Erasmus+

Projekt finansowany w ramach programu:
Erasmus+ / Akcja 2: Współpraca na rzecz innowacji i wymiany dobrych praktyk, Partnerstwa Strategiczne

(Komisja Europejska, EACEA)

E-PORADNIK

DLA MŁODYCH PRZEDSIĘBIORCÓW

Projekt finansowany ze środków Unii Europejskiej. Publikacja została zrealizowana przy wsparciu finansowym Komisji Europejskiej. Publikacja odzwierciedla jedynie stanowisko jej autorów i Komisja Europejska nie ponosi odpowiedzialności za jej zawartość merytoryczną.

Powitanie

Drogi młody przedsiębiorco,

Witaj w e-poradniku DiFens!

Poniżej znajdziesz informacje, przykłady, wskazówki i porady jak wspierać własny biznes w cyfrowej erze. Eksperci z różnych dziedzin przygotowali pięć części składających się na niniejszy e-poradnik, nadając mu tym samym formę treściwą, konkretną i użyteczną, aby można było skupić się na pięciu kluczowych obszarach związanych z cyfrowym bezpieczeństwem każdej firmy:

W **części I** znajdują się informacje wprowadzające jak i szczegółowe o charakterze instruktażowym na temat tego, czym jest digitalizacja biznesowa, jak i gdzie ją wdrożyć, dlaczego i jakie narzędzia mogą pomóc w procesie jej wdrażania.

W **części II** zostały przewidziane informacje na temat innowacji społecznych i przedsiębiorczości społecznej oraz zalet i korzyści płynących z funkcjonowania przedsiębiorstw społecznych, a także konkretnych zagrożeń i szans, jakie pojawiają się w tej sferze biznesu.

Część III koncentruje się na prawnych aspektach cyfrowego zabezpieczenia firmy, w szczególności w kwestii ochrony danych, ochrony konsumentów, handlu elektronicznego i plików cookie.

Części IV i **V** dotyczą cyberbezpieczeństwa i zagrożeń z nim związanych, wyjaśniając, czym one są i jak sobie z nimi radzić, a także określając kompletną strategię, dzięki której będzie można prawidłowo funkcjonować.

Każda część składa się z tożsamych elementów, tj. wszystkie części zawierają w różnych miejscach informacje, przykłady oraz porady. Ponadto e-poradnik zawiera specjalną **listę kontrolną** pomocną w diagnozowaniu stanu własnej firmy pod kątem cyberbezpieczeństwa, **zalecenia** odnośnie literatury uzupełniającej w celu zgłębienia wiedzy na podejmowany temat oraz **glosariusz** z terminologią, który zawsze można otworzyć i sprawdzić, jeśli którykolwiek z zastosowanych terminów jest nieznany.

Spis treści

CZĘŚĆ I

DIGITALIZACJA BIZNESU

Spis zastosowanych skrótów

Skrót	Rozwinięcie
CEO	Dyrektor generalny
IoT	Internet przedmiotów
BI	Analityka biznesowa
ROI	Zwrot z inwestycji
CRM	Zarządzanie relacjami z klientami
IT	Technologie informacyjne
URL	Ujednolicony format adresowania zasobów
CIO	Dyrektor ds. informacji
GPS	Globalny System Pozycjonowania
QR code	Kod QR
ERP	Planowanie zasobów przedsiębiorstwa
SQL	Strukturalny język zapytań
DAP	Platforma cyfrowej adaptacji
POS	Materiały wspierające sprzedaż
SLA	Umowa o gwarantowanym poziomie świadczenia usług
AI	Sztuczna inteligencja
APIs	Interfejs aplikacji
OWASP	Projekt Open Web Application Security

CA	Średni personel - specjaliści ds. komputerów
USB	Uniwersalna magistrala szeregowa
MŚP	Małe i średnie przedsiębiorstwa
RFID	Identyfikacja częstotliwości radiowej
HR	Zasoby ludzkie
ICT	Technologie informacyjno-komunikacyjne

A. Wstęp

Biznes w obliczu cyfrowej ery

Świat stał się bardziej ze sobą powiązany niż kiedykolwiek wcześniej. Możliwość zanurzenia się w dynamicznej, złożonej i ciągle zmieniającej się rzeczywistości staje się koniecznością, zarówno dla systemów gospodarczych, jak i samych przedsiębiorców. Przenikanie technologii do świata biznesu jest kwestią niepodlegającą dyskusji. Głównymi cechami, którym należy się przyjrzeć jest nieuchronna zmiana charakteru samej firmy, której działalność dodatkowo determinowana jest nawykami pracy tzw. Millenialsów. Wśród głównych filarów tzw. digitalizacji biznesu znajduje się wiele potrzeb, na które należy odpowiedzieć.

Każda nowoczesna firma powinna osiągnąć równowagę pomiędzy takimi determinantami jak rozwój, podejmowanie ryzyka i stan zasobów ludzkich. Możliwym scenariuszem staje się wówczas skuteczny wzrost, pnący się w górę niczym startup „jednorożec”. Wykorzystanie technologii w celu zwiększenia wydajności i zabezpieczenia firmy poprzez planowanie z wyprzedzeniem, minimalizuje ryzyko. Na drugim końcu spektrum znajdują się klienci i pracownicy. Ułatwienie dostępu wpływa na wydajność, gdy firma adaptuje nowe technologie i ulepsza jakość życia, które te nowe technologie ze sobą przynoszą.

Bycie konkurencyjnym

Krawędź. Życie, praca i prowadzenie firmy na krawędzi, w harmonii z planowaniem daleko wykraczającym poza wyznaczone horyzonty, czynią je bardziej sprawnymi. Stworzenie przewagi konkurencyjnej i dążenie do tego celu do granic możliwości to jedna strategia, która ilustruje wynik wielu podjętych wcześniej działań. Kamień milowy to solidne ustalanie własnego położenia od pierwszego dnia. Wyróżnianie się z tłumu jako autorytet, ekspert i przywódca może sprawić, że świat się zmieni, a firma się rozrośnie. Era cyfrowa wymaga gruntownej cyfrowej rewolucji.

Powiedziawszy to, nie ma potrzeby wyważać otwartych drzwi. Niezbędna jest jasna misja odzwierciedlająca potrzeby stale zmieniającego się rynku. Nieustanna analiza konkurencji i klientów może umożliwić firmie pozostanie w centrum zainteresowania. Rozwój obsługi klienta to realna potrzeba. Na wierzchołku tego wszystkiego znajduje

się rozwój ludzi, inspirowanie ich i kierowanie nimi, co stoi na równie wysokim filarze. Bycie innowacyjnym na wskroś, pomaga przedsiębiorcy w bezpiecznym przemieszczaniu się we wszystkich wyżej wymienionych sektorach.

Potrzeba adaptacji

Ewolucja podąża za gromadzeniem różnych doświadczeń. Wszyscy mądrzy ludzie uczą się na swoich błędach; jednak mądrzejsi ludzie są w stanie odwrócić krzywą, ucząc się na błędach i zwycięstwach innych. Każda zmiana zawsze wiąże się z ogromnym ryzykiem, tak więc wciąż, czasami, nie ryzykując niczym, ryzykujemy wszystkim.

80% firm zdało sobie sprawę, że technologia zniewolenia, przy przygotowaniu swojej oferty, stała się kluczowa dla ich sukcesu, a tymczasem Czwarta Rewolucja Przemysłowa stoi u naszych bram. Ponownie, tylko 29% firm jest w stanie potwierdzić, że wdrożyły w ostatnim czasie zdobycze nowego tysiąclecia w zakresie zarządzania i nowoczesnych technologii.

Era cyfrowa zrewolucjonizowała świat biznesu. Bycie konkurencyjnym w dzisiejszych czasach idzie w parze z byciem innowacyjnym. Przystosowanie się do tych wszystkich zmian, a zwłaszcza zrobienie tego przed tym jak zajmą się tym konkurenci i na bardziej inteligentne sposoby, może odróżnić firmę na tle konkurencji.

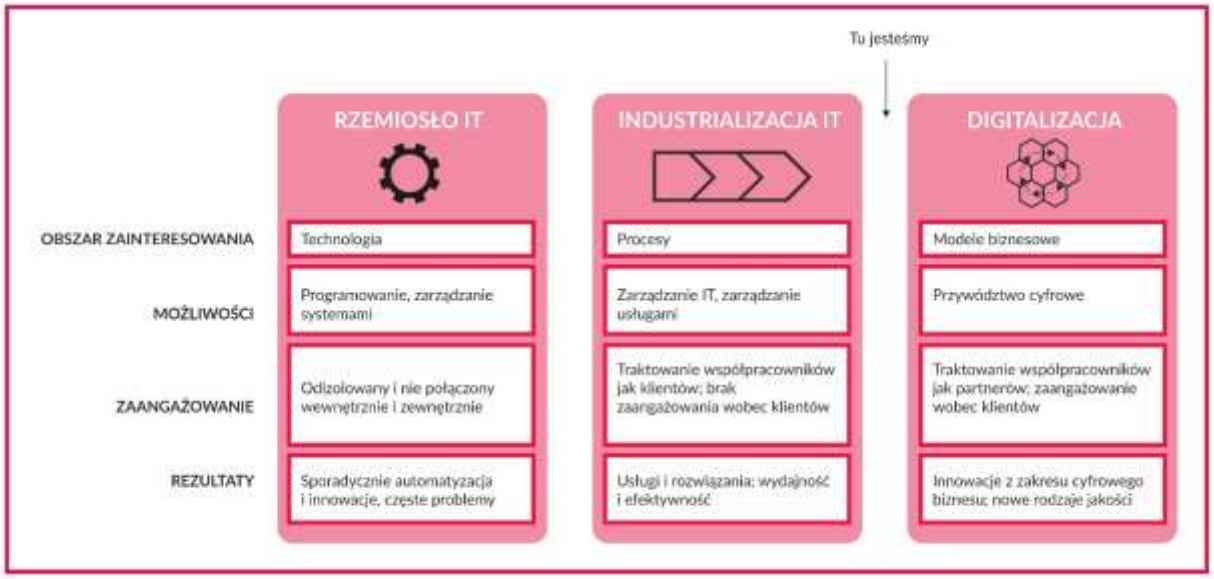
Oczywistym wnioskiem, jaki należy wyciągnąć, jest to, że wszystkie te poczynania są wzmacniane i potęgowane przez digitalizację biznesu.

Ryc. 1: Biznes w gospodarce cyfrowej

Co to jest digitalizacja biznesu?

Często używane zamiennie z cyfryzacją i z zupełną transformacją cyfrową, digitalizacja jest naprawdę czymś innym.

Cyfryzacja oznacza wykorzystanie technologii cyfrowych i danych (cyfrowych i macierzystych) w celu generowania przychodów, usprawnienia działalności, zastąpienia/transformacji procesów biznesowych (a nie tylko ich digitalizacji) oraz stworzenia środowiska dla cyfrowego biznesu, w którym informacje cyfrowe stanowią rdzeń. Poniżej znajdują się trzy definicje lub lepsze konteksty, w których termin ten jest używany.



Ryc. 2: Oś czasu funkcjonowania biznesu

W biznesie, cyfryzacja najczęściej odnosi się do umożliwiania, ulepszania i/lub przekształcania operacji biznesowych i/lub funkcji biznesowych i/lub modeli biznesowych/procesów i/lub działań, poprzez wykorzystanie technologii cyfrowych oraz szerszego wykorzystania i umiejscawiania w kontekście przekształconych danych cyfrowych, najczęściej w formie praktycznej wiedzy, z myślą o konkretnych korzyściach. Wymaga to cyfryzacji informacji, ale oznacza więcej, a jej centralnym punktem są dane. Podczas, gdy digitalizacja dotyczy raczej systemów zapisu i coraz częściej systemów zatrudniania, to cyfryzacja dotyczy systemów zatrudniania i systemów wglądu, wykorzystujących cyfrowe dane i procesy.

Drugim często wymienianym aspektem jest digitalizacja określonego "środowiska" lub obszaru działalności. Przejąć cyfrowe miejsce pracy. Często dąży się do wykorzystania minimum papieru. Ale cyfrowe miejsce pracy dotyczy również innych rzeczy. Oznacza to również, że twoja siła robocza działa inaczej, używając narzędzi cyfrowych, takich jak urządzenia mobilne i technologie, które sprawiają, że są mobilne i/lub korzystają ze współpracy społecznej i zunifikowanych platform komunikacyjnych, które są systemami cyfrowymi, umożliwiając im pracę w bardziej "cyfrowy sposób". To z kolei stwarza nowe możliwości zaangażowania się w inny sposób. I wymaga czegoś więcej niż tylko danych cyfrowych.

Digitalizacja twojej firmy prowadzi do cyfrowego biznesu. Lista tego, co można zdigitalizować (łańcuchy dostaw prowadzące do cyfrowych łańcuchów dostaw itp.) jest długa. Ogólnie rzecz biorąc, cyfryzacja jest postrzegana jako droga zmierzająca w kierunku cyfrowego biznesu i cyfrowej transformacji, a także do tworzenia nowych - cyfrowych - źródeł przychodów i ofert w tym samym czasie. I to wymaga zmiany. To dlatego wiele osób używa zamiennie terminów cyfryzacja i transformacja cyfrowa (tak często to robimy).

Trzecie znaczenie cyfryzacji wykracza poza biznes i odnosi się do stałego wprowadzania technologii cyfrowych we wszystkich możliwych działaniach społecznych i ludzkich. Pomyślmy na przykład o coraz bardziej cyfrowym kliencie, rosnącej cyfrowej opiece zdrowotnej, rosnącej cyfryzacji rządu, marketingu, obsłudze klienta itp. Innymi słowy: bardziej cyfrowy (w różnych możliwych obszarach).

[I-scoop.eu. (2018). Digital business: transformation, disruption, optimization, integration and humanization. [online] Dostępne na: https://www.i-scoop.eu/digital-business]

Korzyści płynące z posiadania cyfrowego biznesu

Ryc. 3. Najczęściej dostrzegane zalety digitalizacji

Choć może to zabrzmieć zabawnie, to słowo „Basic" to termin, który opisuje 20% małych firm w Stanach Zjednoczonych, które nie korzystają w pełni z narzędzi cyfrowych. Deloitte Connected Small Businesses U.S. Research zbadał, w jaki sposób narzędzia cyfrowe pomagają małym firmom i, w konsekwencji, amerykańskiej gospodarce. Badanie sklasyfikowało właścicieli małych firm na cztery poziomy zaangażowania cyfrowego w oparciu o sposób korzystania z narzędzi online. Poniżej znajduje się typowy podział:

- Podstawowy (20%) Małe firmy na tym poziomie mają nierozwiniętą obecność cyfrową. Opierają się na tradycyjnych metodach marketingowych, takich jak bezpośrednia wysyłka i reklama drukowana. Nie mają własnej strony internetowej ani nie są obecni w mediach społecznościowych. Zasadniczo jedynym narzędziem cyfrowym, którego używają, jest firmowy adres e-mail.
- Średniozaawansowany (30%): Na tym poziomie mała firma korzysta z narzędzi cyfrowych, takich jak prosta strona internetowa (bez możliwości prowadzenia handlu elektronicznego lub mobilnego). Posiada niektóre podstawowe narzędzia marketingu online, takie jak wzmianka w katalogach online lub obecność na platformach handlowych należących do innych podmiotów.
- Zaawansowany (30 procent): Zaawansowana firma ma bardziej złożoną stronę internetową, na przykład taką, która oferuje funkcje mobilne, rezerwacje online lub też funkcje związane z handlem elektronicznym. Firma taka angażuje się w wiele mediów społecznościowych i kanałów marketingu online. Wykorzystuje również wewnętrzne narzędzia cyfrowe, takie jak oprogramowanie do wideokonferencji lub oprogramowanie w chmurze, aby zwiększyć swoją wydajność i efektywność.
- Wysoce zaawansowany (20%): Ta prawdziwie cyfrowa firma wykorzystuje wszystkie powyższe narzędzia cyfrowe, jednak na wyższym poziomie. Ponadto firma taka stosuje bardziej wyrafinowane narzędzia cyfrowe, takie jak tworzenie aplikacji mobilnej lub korzystanie z analityki danych, aby dowiedzieć się więcej o preferencjach klientów i trendach sprzedaży.

- Jak wykazują badania, im większe zaangażowanie cyfrowe, tym większe korzyści dla firmy. Jest to prawdą bez względu na to, jak długo pracujesz, gdzie znajduje się twoja firma lub w jakiej branży pracujesz. W rzeczywistości przepaść pomiędzy osiągnięciami podstawowych i zaawansowanych (prawdziwie cyfrowych) małych firm jest ogromna.

Przemyśl:

Cyfrowe małe przedsiębiorstwa są twórcami miejsc pracy. Jest niemal trzykrotnie bardziej prawdopodobne, że zaawansowane i wysoce zaawansowane firmy stworzyły więcej miejsc pracy przeciągu ostatniego roku niż firmy będące na poziomie podstawowym. Ponadto ich pracownicy są bardziej produktywni dzięki wewnętrznym narzędziom cyfrowym, z których korzysta firma.

Cyfrowe małe firmy docierają do nowych rynków. Dzięki większej liczbie kanałów marketingowych są w stanie dotrzeć do bardziej zróżnicowanej grupy klientów i w rezultacie są trzykrotnie bardziej prawdopodobne, że eksportowały więcej produktów lub usług w ciągu ostatniego roku niż firmy na poziomie podstawowym. Ponad 4 na 10 (43&) klientów małych firm cyfrowych to klienci regionalni, krajowi lub międzynarodowi, w porównaniu do 28% w przypadku firm będących na poziomie podstawowym.

Cyfrowe małe firmy kreują innowacje. Firmy zaawansowane są pięciokrotnie bardziej prawdopodobne, a firmy wysoce zaawansowane - dziesięciokrotnie bardziej prawdopodobne, że wprowadziły nowy produkt lub usługę w ubiegłym roku niż firmy na poziomie podstawowym.

Cyfrowe małe firmy docierają do większej liczby klientów. Zaawansowane i wysoce zaawansowane firmy są trzykrotnie bardziej prawdopodobne, że w ubiegłym roku odnotowały zwiększoną liczbę zapytań sprzedażowych niż firmy na poziomie podstawowym. W rzeczywistości małe firmy cyfrowe doświadczają większej aktywności klientów na całej ścieżce sprzedaży, od zainteresowania, przez zapytania do zakupu.

Biorąc pod uwagę wszystkie te czynniki, nic dziwnego, że cyfrowe małe firmy rozwijają się szybciej. W ubiegłym roku, w porównaniu z małymi firmami na poziomie podstawowym, firmy cyfrowe miały dwa razy więcej przychodów na jednego

pracownika, a ich dochody wzrosły prawie czterokrotnie. Poszerzanie rynków, innowacyjne nowe produkty i usługi oraz rosnąca baza klientów naturalnie prowadzą do rozwoju firmy.

Reasumując, jeśli firma chce się rozwijać - lub nawet przetrwać - musi ciągle ulepszać sposób korzystania z narzędzi cyfrowych w różnych aspektach swojej działalności.

[Small Biz Daily. (2018). The Benefits of Being a Digital Business - Small Biz Daily. [online] Dostępne na: https://www.smallbizdaily.com/benefits-digital-business/].

Druga strona monety

Skoro posiadanie firmy cyfrowej jest idylliczną sytuacją lub jednokierunkowym procesem, dlaczego jeszcze nie wszystkie firmy są na drodze do cyfrowej transformacji? Właściwie to mogą na niej być. Cyfryzacja to trudna i czasochłonna procedura, która może również ukrywać wiele zagrożeń i przeszkód, a wielu firmom może nawet nie udać się przekształcić. Co więcej, utrzymanie cyfrowej firmy mogłoby nie być tak proste, jak się wydaje, ponieważ mogą pojawiać się różne zagrożenia, nawet po zakończeniu procesu transformacji i w trakcie codziennej działalności firmy.

Cyfrowe zagrożenia dla twojej firmy

Internet, komputerowa technologia mobilna i reklama online mogą pomóc małym firmom konkurować z większymi rywalami, ale te narzędzia cyfrowe również stanowią duże zagrożenie.

- Oszustwo w transakcjach
- Przykrzy natręci
- Przestępstwo popełnione przez pracownika firmy
- Niekompletne oprogramowanie
- Urządzenia mobilne

Inne kwestie dotyczące bardziej skomplikowanego wyposażenia technicznego i bardziej zaawansowanych cyfrowych modeli biznesowych mogą obejmować:

- Ataki na urządzenia w obszarze Internetu rzeczy
- Ochrona danych
- Ataki na materiały wspierające sprzedaż

[Forbes.com. (2018). [online] Dostępne na: https://www.forbes.com/2007/06/14/microsoft-apple-symantec-ent-tech-cx_df_0614riskdigital]

Ryc. 4. Cyfrowe zagrożenia dla twojej firmy

Technologie cyfrowe wobec cyfryzacji firmy

Technologie cyfrowe są jednym z najważniejszych źródeł wzrostu dla gospodarek krajowych. Umożliwiają one gospodarkom tworzenie nowych miejsc pracy, poprawę życia ludzi i budowanie lepszych i bardziej ekologicznych społeczeństw. Obywatele, przedsiębiorstwa, uniwersytety i rządy stają się coraz bardziej powiązani w cyfrowym świecie. Cyfryzacja zmienia życie ludzi, tj. sposób, w jaki pracują, robią zakupy, prowadzą życie towarzyskie, komunikują się ze sobą, czy kształcą. Zmienia także tradycyjne gałęzie przemysłu i zmienia otoczenie biznesu, od mody po motoryzację, od transportu i logistyki po dystrybucję energii. Nowe osiągnięcia technologiczne przyspieszają i ulepszają sposób, w jaki nowe innowacyjne produkty i usługi są opracowywane, rozwijane, wytwarzane i udostępniane. Umożliwiają firmom szybszy rozwój i wprowadzanie na rynek innowacyjnych produktów i usług, o których wcześniej nie można było pomyśleć.

Technologie cyfrowe pomagają całkowicie od nowa kształtować łańcuchy wartości, wyostrzyć inteligencję rynkową, poprawić wydajność, skrócić czas wprowadzania produktów na rynek i zwiększyć zadowolenie klientów. Ponadto, dzięki technologiom, MŚP mogą zacząć działać globalnie już od pierwszego dnia swojej działalności, docierając natychmiast do rynków zagranicznych i puli talentów. Nic dziwnego, że

organizacje rozwijają się dwa do trzech razy szybciej, gdy są wzmocnione przez technologie cyfrowe.

Nowoczesne technologie kooperacji nie tylko zapewniają o wiele większą i bardziej zróżnicowaną pulę talentów w zasięgu każdego przedsiębiorcy rozpoczynającego lub skalującego swoją firmę, ale również umożliwiają utalentowanym osobom wspólne, bezproblemowe, globalne działanie, pomimo różnych stref czasowych i dystansu geograficznego.

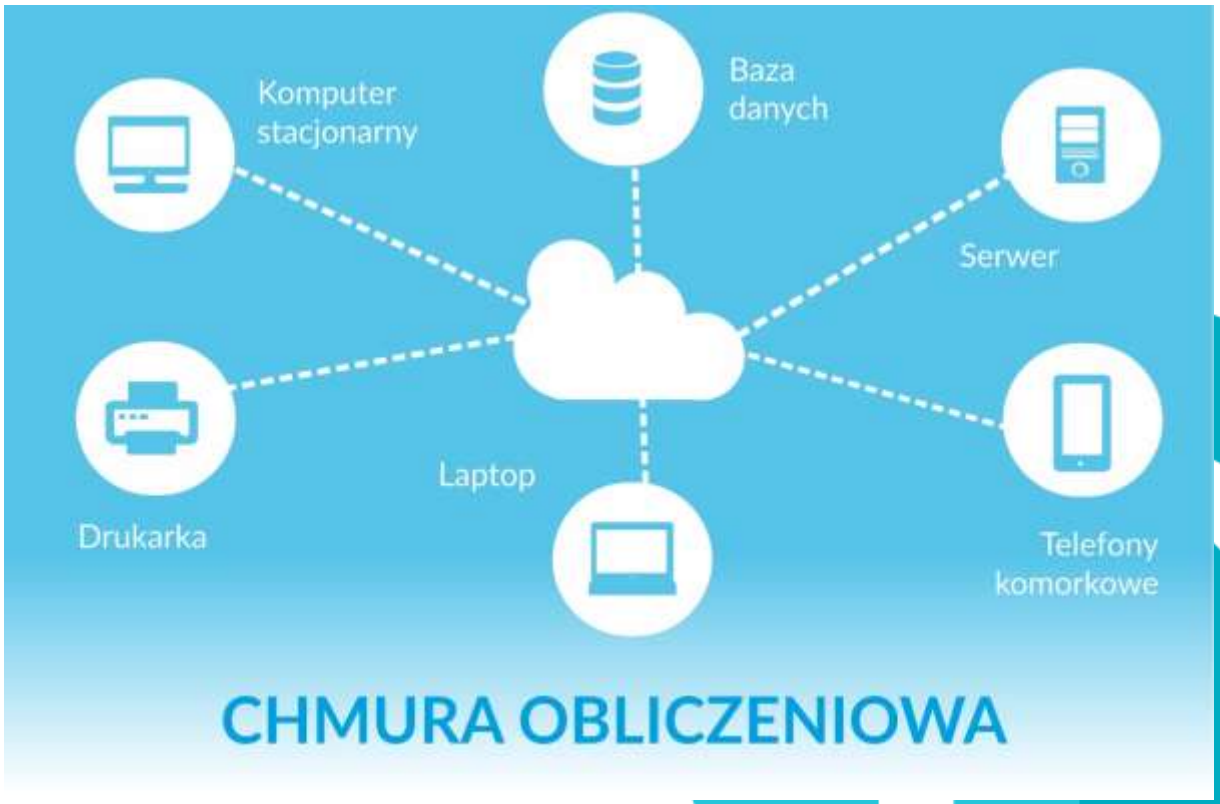
Dwie wciąż rozwijające się i mające wielkie znaczenie technologie cyfrowe dla biznesu to chmury obliczeniowe i duże zbiory danych.

Ryc. 5: Technologie cyfrowe otwierają nowe możliwości

B. Rozwiązania oparte na chmurze - funkcjonalności i zagrożenia

Chmura obliczeniowa a biznes

Przetwarzanie w chmurze umożliwia firmom zarządzanie zasobami obliczeniowymi w Internecie. Termin ten rozwinął się w ciągu ostatnich lat i można nim opisać sposób korzystania z narzędzia należącego do innego podmiotu dla własnych potrzeb informatycznych i tych związanych z gromadzeniem różnych zasobów. „Chmura" odnosi się do Internetu, a operacja w chmurze" opisuje sposób, w jaki firma przechowuje i uzyskuje dostęp do swoich danych za pośrednictwem połączenia internetowego. Przetwarzanie w chmurze umożliwia firmom wirtualny dostęp do ich informacji, tworząc elastyczny i globalny sposób uzyskiwania dostępu do danych w dowolnym miejscu i czasie.



Ryc. 6: Chmura obliczeniowa a biznes

Co to jest chmura obliczeniowa?

Internet zmienia sposób, w jaki prowadzimy firmę i wchodzimy w interakcje jako społeczeństwo. Tradycyjnie sprzęt i oprogramowanie znajdują się w komputerze danego użytkownika. Oznacza to, że uzyskujesz dostęp do swoich danych i programów wyłącznie na swoim komputerze.

Chmura obliczeniowa umożliwia dostęp do danych i programów poza własnym środowiskiem komputerowym. Zamiast przechowywania danych i oprogramowania na komputerze osobistym lub serwerze, wszystko znajduje się w „chmurze". Może to obejmować aplikacje, bazy danych, pocztę e-mail i usługi plików. Może to obejmować aplikacje, bazy danych, pocztę e-mail i serwery plików. Zasadniczo wynajmujesz pojemność (przestrzeń serwera lub dostęp do oprogramowania) od dostawcy usług w chmurze i łączysz się przez Internet. Zamiast sprostać własnym potrzebom IT, wynajmujesz zasoby od usługodawcy i płacisz tylko za te, które zużyjesz.

Chmura obliczeniowa posiada 4 modele pod względem różnych opcji dostępu i bezpieczeństwa. Zanim przeniesiesz swoje dane do chmury, musisz zastanowić się, który model najlepiej pasuje do potrzeb twojej firmy i danych, które są w twoim posiadaniu.

Chmura prywatna

Chmura prywatna to miejsce, w którym usługi i infrastruktura są utrzymywane i zarządzane przez ciebie lub osobę trzecią. Ta opcja zmniejsza potencjalne ryzyko związane z bezpieczeństwem i kontrolą, i będzie ci odpowiadać, jeśli dane i aplikacje są podstawową częścią twojej działalności i potrzebujesz wyższego poziomu bezpieczeństwa lub wymagań dotyczących danych poufnych.

Chmura współdzielona

Chmura współdzielona istnieje wtedy, gdy kilka organizacji, z podobnymi względami bezpieczeństwa, ma dostęp do chmury prywatnej. Na przykład różne systemy franczyzowe mają własne chmury publiczne, ale są one hostowane zdalnie w środowisku prywatnym.

Chmura publiczna

Chmura publiczna to miejsce, w którym usługi są przechowywane poza siedzibą firmy i są dostępne przez Internet. Miejsce, w którym przechowywane są zasoby jest zarządzane przez zewnętrzną organizację, taką jak Google lub Microsoft. Ta usługa oferuje największy poziom elastyczności i oszczędności kosztów, aczkolwiek jest bardziej podatna na ataki niż chmury prywatne.

Chmura hybrydowa

Model chmury hybrydowej wykorzystuje zalety zarówno chmur publicznych, jak i prywatnych. Poprzez zastosowanie opcji z różnych rodzajów chmury, zyskujesz zalety każdego modelu.

Na przykład, możesz użyć chmury publicznej do swoich e-maili, aby zaoszczędzić na dużych kosztach pamięci masowej, a jednocześnie zachować poufne dane za bezpieczną zaporą w chmurze prywatnej.

Jak działa chmura obliczeniowa

Dostępne są 3 główne typy modeli usług przetwarzania w chmurze, powszechnie znane jako:

- Oprogramowanie jako usługa (SaaS)
- Infrastruktura jako usługa (IaaS)
- Platforma jako usługa (PaaS)

W zależności od potrzeb firma może korzystać z jednego z tych modeli usług lub z kombinacji wszystkich trzech.

Oprogramowanie jako usługa (SaaS)

SaaS jest najczęstszą formą chmury obliczeniowej dla małych firm. Możesz uzyskać dostęp do aplikacji internetowych obsługiwanych za pomocą przeglądarki, a nie tradycyjnych aplikacji przechowywanych na komputerze lub serwerze. Host aplikacji jest odpowiedzialny za kontrolowanie i konserwację aplikacji, w tym aktualizacji oprogramowania i ustawień. Ty, jako użytkownik, masz ograniczoną kontrolę nad ustawieniami aplikacji i konfiguracji.

Typowym przykładem SaaS jest internetowa usługa pocztowa lub system zarządzania relacjami z klientami.

Infrastruktura jako usługa (IaaS)

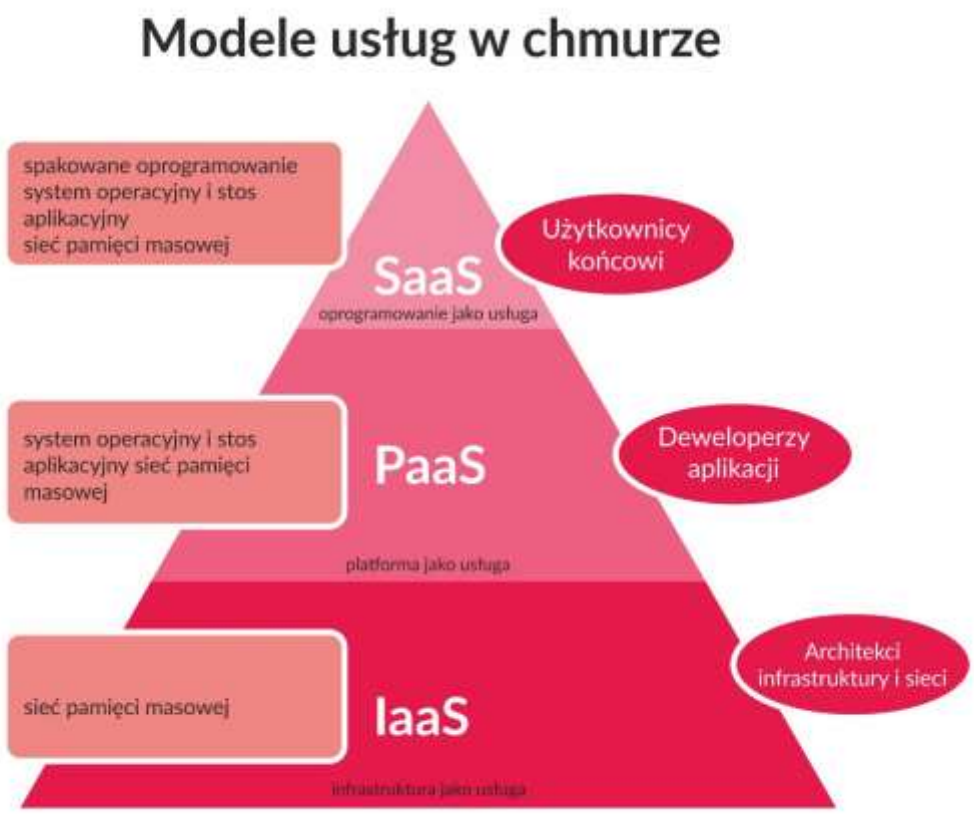
IaaS zazwyczaj wiąże się z zakupem lub dzierżawą mocy komputera i miejsca na dysku od zewnętrznego usługodawcy. Ta opcja umożliwia dostęp przez sieć prywatną lub przez internet. Dostawca usług utrzymuje fizyczny sprzęt komputerowy, w tym przetwarzanie procesora, pamięć, przechowywanie danych i łączność sieciową.

Przykłady IaaS obejmują Amazon EC2, Rackspace i Windows Azure.

Platforma jako usługa (PaaS)

PaaS można opisać jako krzyżówkę zarówno SaaS, jak i IaaS. Zasadniczo wynajmujesz sprzęt, systemy operacyjne, pamięć masową i przepustowość sieci zapewnioną przez IaaS, a także serwery oprogramowania i środowiska aplikacji. PaaS oferuje większą kontrolę nad technicznymi aspektami konfiguracji komputera i możliwością dostosowania do własnych potrzeb.

[DreamHost. (2018). What is Cloud Computing? Can It Help Your Business? - DreamHost.blog. [online] Dostepne na: https://www.dreamhost.com/blog/cloud-computing-for-business]



Ryc. 7: Modele usług w chmurze

Jakie korzyści dla biznesu przynosi chmura obliczeniowa?

Chmura obliczeniowa oferuje twojej firmie wiele korzyści. Umożliwia skonfigurowanie wirtualnego biura, co zapewnia elastyczność łączenia się z firmą w dowolnym miejscu i czasie. Wraz z rosnącą liczbą urządzeń internetowych używanych w dzisiejszym środowisku biznesowym (np. smartfony, tablety), dostęp do danych jest jeszcze łatwiejszy. Poniżej zaprezentowano 8 sposobów w jakich przetwarzanie w chmurze może przynieść korzyści twojej firmie:

Prostota

Instalowanie nowego oprogramowania, śledzenie problemów związanych z bezpieczeństwem, instalowanie poprawek i uaktualnianie do nowych wersji oprogramowania to praca na pełen etat. Jednak wiele małych firm nie może sobie pozwolić na własnego specjalistę IT, więc korzysta z usług konsultantów IT, którzy są

zajęci i nie zawsze są w stanie sprostać potrzebom internetowym firmy. Inne firmy polegają na „mimowolnym" informatyku, takim jak kierownik biura firmy.

Każde podejście angażuje czas, pieniądze i problemy, a nawet może narazić firmę na ryzyko. Jeśli w załodze twojej firmy nie ma specjalisty IT, to korzystanie z oprogramowania chmurowego znacznie ułatwia życie. Wszystkie te aktualizacje są automatycznie przetwarzane poza firmą przez dostawcę usług w chmurze, który ma pełny personel ekspertów IT, aby zapewnić najnowszą technologię. Nawet jeśli twoja firma zatrudnia specjalistów IT, outsourcing usług w chmurze umożliwia pracownikom działu IT poświęcanie mniej czasu na konserwację nakrętek i śrub oraz więcej czasu na opracowywanie innowacyjnych pomysłów na rozwój firmy.

Bezpieczeństwo

Wydaje się, że każdego dnia czytamy o naruszeniach danych dotyczących wielkich korporacji, takich jak Target, Home Depot, Sony, itp. Jeśli tak duże firmy nie są odporne na złośliwe oprogramowanie, hakerów i wirusy, możesz sobie wyobrazić, jak wrażliwy jest twój mały biznes. Podczas gdy duże firmy mogą sobie pozwolić na grzywny i procesy sądowe związane z naruszeniem bezpieczeństwa danych, takie koszty wybiją typowemu przedsiębiorcy biznes z głowy.

Nie zakładaj, że jesteś bezpieczny, ponieważ nikt nie zechce włamać się do twoich danych biznesowych. W rzeczywistości, ponieważ małe firmy są zazwyczaj mniej chronione przed zagrożeniami internetowymi, w rzeczywistości są one preferowanymi celami hakerów online. Renomowani dostawcy usług w chmurze mogą pomóc, oferując znacznie lepsze zabezpieczenia niż zapewnia to przeciętny właściciel małej firmy. Przechowywanie danych w chmurze zapewnia ochronę ekspertów, których zadaniem jest być na bieżąco z najnowszymi zagrożeniami dla twojego bezpieczeństwa.

Ciągłość

Klęski żywiołowe, kradzieże lub wypadki mogą zniszczyć najważniejsze dane firmy, jeśli są przechowywane wyłącznie na dyskach twardych lub serwerach w biurze. W ostatnich latach ekstremalne zjawiska pogodowe, takie jak powodzie, huragany i zamiecie, spowodowały, że wiele małych firm przestało działać, przynajmniej

tymczasowo. Zgodnie ze statystykami FEMA, od 40 do 60% małych przedsiębiorstw dotkniętych katastrofą nigdy nie wznawia swojej działalności.

Usługi przechowywania w chmurze i tworzenia kopii zapasowych mogą przetrzymywać stale aktualizowane kopie danych biznesowych i aplikacji online, dzięki czemu są zawsze bezpieczne od katastrofy i można je przywrócić po całym zajściu. Automatyczne tworzenie kopii zapasowych eliminuje ryzyko błędu ludzkiego podczas procesu tworzenia kopii zapasowej, zwiększając tym samym bezpieczeństwo. Ponadto wiele rozwiązań do tworzenia kopii zapasowych w chmurze oferuje możliwość automatycznego zapisywania wielu wersji dokumentu, dzięki czemu można łatwo wrócić do wcześniejszych wersji.

Mobilność

Praca zdalna jest obecnie dodatkową zaletą dla wielu pracowników. I, oczywiście, zapracowani właściciele małych firm i tak często pracują po nocach w domu. Gdy korzystasz z usług w chmurze, nie musisz wysyłać sobie pocztą e-mail plików na później lub pamiętać o zabraniu do domu pendrive'a. Zamiast tego ty i twój zespół możecie uzyskać dostęp do najnowszych wersji swoich dokumentów i danych z dowolnego miejsca, w którym macie połączenie z Internetem. Usługi w chmurze motywują sprzedawców i innych, którzy często podróżują w interesach, aby osobiście odwiedzić obecnych i przyszłych klientów. Nigdy więcej nie będziesz musiał się martwić o pozostawienie w swoim biurze najnowszej wersji prezentacji, umowy lub oferty.

Efektywność

Oprogramowania w chmurze aktualizuje się automatycznie, bez wysiłku z twojej strony. Bez potrzeby czasochłonnej konserwacji, twój personel zyskuje na wydajności. Pracownicy nie muszą czekać (i nie pracować), podczas gdy specjalista IT aktualizuje lub naprawia komputery. A ponieważ zawsze mają najnowsze wersje oprogramowania, ich komputery zawsze działają z najwyższą wydajnością. Mniej wypadków i szybsze prędkości oznaczają, że twoi pracownicy mogą zrobić więcej w krótszym czasie.

Łączność

Usługi w chmurze oferują nowe sposoby łączenia się ze zdalnymi lub wirtualnymi pracownikami, z obecnymi i potencjalnymi klientami. Na przykład możesz prowadzić wirtualne połączenia konferencyjne lub wideokonferencje online, korzystając z technologii VoIP. Narzędzia do współpracy oparte na chmurze pozwalają zespołom przeglądać, komentować i edytować dokumenty lub prezentacje jednocześnie (prawie) w czasie rzeczywistym. Gdy nie musisz fizycznie odwiedzić konkretnego miejsca, aby zorganizować spotkanie, twoje możliwości interakcji z klientami zwiększają się stopniowo. Oznacza to więcej zadowolonych klientów i silniejsze powiązania z nimi.

Przystępność

Oszczędności to jedna z największych korzyści z chmury dla małych firm. Wielu dostawców usług w chmurze oferuje darmowe wersje oprogramowania, które często są odpowiednie dla małych firm. Zamiast jednorazowo płacić za kosztowne oprogramowanie, płacisz za usługi w chmurze w sposób ciągły, miesięczny lub w ramach subskrypcji. Ten model „pay-as-you-go" pomaga w przepływach pieniężnych, ponieważ koszty rozkładają się w czasie.

Usługi w chmurze również obniżają koszty pracy, ponieważ dostawca usług w chmurze obsługuje zadania, które normalnie wykonałby pracownik IT. No i wreszcie, podczas korzystania z usług w chmurze, płacisz tylko za to, z czego korzystasz. Gwarantuje to, że nie będziesz nadmiernie wydawać pieniędzy na sprzęt, którego nie używasz, lub na oprogramowanie, które szybko stanie się przestarzałe.

Skalowalność

Usługi w chmurze to świetny sposób dla małych firm na zarządzanie planowanym wzrostem. Wraz z rozwojem Twojej firmy możesz łatwo przejść na kolejny poziom usług w chmurze i niemal natychmiast dodawać serwery lub dodawać użytkowników. Nie ma potrzeby kupowania kosztownego nowego oprogramowania lub sprzętu, ponieważ po prostu „wynajmujesz" to, czego potrzebujesz od dostawcy usług w chmurze. Oprócz wspomagania procesu radzenia sobie z planowanym wzrostem, usługi w chmurze umożliwiają także zarządzanie nieoczekiwanymi impulsami wzrostu. Co się stanie, jeśli twój produkt nagle stanie się popularny w mediach

społecznościowych, a witryna Twojej firmy jest przeciążona przez odwiedzających składających zamówienia?

Możesz szybko rozwiązać problem, skalując do następnego poziomu usług w chmurze lub dodając nowe narzędzia oparte na chmurze. Usługi w chmurze mogą również pomóc w nieoczekiwanym lub sezonowym spowolnieniu aktywności firmy. Jeśli firma notuje spadek, wyeliminujesz produkt lub usługę albo musisz zwolnić pracowników, po prostu zmniejsz zakres usług w chmurze, z których używasz. Zapewniając prostą i niedrogą skalowalność, usługi w chmurze umożliwiają małym firmom przeprowadzić ją w mgnieniu oka.

[Business.qld.gov.au. (2018). Cloud computing for business | Business Queensland. [online] Dostępne na: https://www.business.qld.gov.au/running-business/it/cloud-computing]

Dołącz do innych w chmurze

Chmura obliczeniowa z pewnością oferuje wiele korzyści dla właścicieli małych firm. Być może największą zaletą jest to, że pozwoli ci się mniej skupić na sprawach związanych z IT, a bardziej na podstawowej działalności firmy. Dzięki elastyczności i łatwości korzystania z usług w chmurze możesz zacząć działać szybko, aby skorzystać z szansy i rozwinąć swój biznes oraz w pełni wykorzystać jego potencjał.

[Business.qld.gov.au. (2018). Cloud computing for business | Business Queensland. [online] Dostępne na: https://www.business.qld.gov.au/running-business/it/cloud-computing]

Chmura a ochrona danych

Bezpieczeństwo w chmurze polega na znalezieniu odpowiednich dostawców i wdrożeniu technologii, która koncentruje się zarówno na weryfikacji tożsamości, jak i szyfrowaniu danych. Oto 10 pytań dotyczących bezpieczeństwa, które należy zadać dostawcom usług w chmurze przed skorzystaniem z ich usług:

- Kto może zobaczyć moje dane?
- Jeśli moje dane znajdują się w wielorakich centrach danych w różnych lokalizacjach, to czy są one chronione przed lokalnymi atakami?
- Jaką redundancją dysponujesz, aby zabezpieczyć moje dane?
- Jakie konkretne środki podejmiesz, aby zaszyfrować moje dane?
- Jak zarządzasz kluczami szyfrowania?

- Co stanie się z moimi danymi i jak je przywrócisz w przypadku awarii lub cyberataku?
- Jakimi certyfikatami bezpieczeństwa dysponujesz?
- Czy wykazujesz zgodność z najnowszymi protokołami bezpieczeństwa?
- Co może pójść nie tak podczas korzystania z usług?
- Czy jesteś odsprzedawcą usług? Jeśli tak, kto jest odpowiedzialny za obsługę i wsparcie?

C. Wykorzystywanie dużych zbiorów danych Big data - możliwości i zagrożenia

Big data: Co to jest i dlaczego jest to ważne

Ryc. 8. Stosowanie Big Data

Big Data to termin opisujący dużą ilość danych, zarówno ustrukturyzowanych, jak i nieustrukturyzowanych, które codziennie dosłownie zalewają firmę. Ale to nie ilość danych jest ważna. Ważne jest to, co robią z nimi podmioty, które je wykorzystują. Big Data może być analizowane pod kątem wnikliwości, które prowadzą do lepszych decyzji i strategicznych ruchów biznesowych.

Definiując duże zbiory danych, ważne jest również zrozumienie połączenia danych nieustrukturyzowanych i wielowymiarowych, które zawierają informacje.

Dane nieustrukturyzowe pochodzą od informacji, które nie są zorganizowane lub są łatwo interpretowane przez tradycyjne bazy danych lub modele danych, a także posiadają zazwyczaj dużą ilość tekstu. Metadane, tweety na Twitterze i inne posty w mediach społecznościowych to dobre przykłady danych nieustrukturyzowanych.

Dane wielowymiarowe odnoszą się do różnych formatów i typów danych i mogą pochodzić z interakcji między ludźmi i maszynami, takich jak aplikacje internetowe lub sieci społecznościowe. Doskonałym przykładem są dane dziennika sieciowego, które zawierają kombinację tekstu i obrazów oraz danych ustrukturyzowanych, takich jak informacje na temat formy lub transakcjach. Ponieważ zakłócenia cyfrowe zmieniają kanały komunikacji i interakcji tak samo jak sprzedawcy zwiększają zadowolenie klientów z urządzeń, funkcjonalności stron internetowych, bezpośrednich interakcji i platform społecznościowych, dane o wielu strukturach będą nadal ewoluować.

[Forbes.com. (2018). [online] Dostępne na: https://www.forbes.com/sites/lisaarthur/2013/08/15/what-is-big-data]

Czemu Big Data jest ważne?

Znaczenie Big Data nie zależy od tego, ile masz danych, ale co z nimi robisz. Możesz pobierać dane z dowolnego źródła i analizować je, aby znaleźć odpowiedzi, które umożliwiają:

1. obniżenie kosztów,
2. obniżenie wymiaru czasu,
3. nowe produkty i zoptymalizowane oferty, oraz
4. inteligentne podejmowanie decyzji.

Łącząc duże zbiory danych z zaawansowanymi narzędziami analitycznymi, możesz wykonywać zadania związane z biznesem, takie jak:

- Określanie głównych przyczyn awarii, problemów i usterek w czasie zbliżonym do rzeczywistego.
- Generowanie kuponów w punkcie sprzedaży w zależności od nawyków zakupowych klienta.
- Ponowne obliczenie całego portfela ryzyka w ciągu kilku minut.
- Wykrywanie nieuczciwych zachowań, zanim wpłyną one na twoją firmę.

W jaki sposób firmy mogą czerpać korzyści z Big Data?

Ryc. 9: Korzyści dla firm z korzystania z Big Data

- Korzystanie z Big Data obniża twoje koszty

Najnowszy artykuł w Tech Cocktail pokazuje, w jaki sposób Twiddy & Company Realtors obniża swoje koszty o 15%. Firma porównała opłaty eksploatacyjne dla wykonawców względem średniej dla swoich dostawców. Dzięki temu procesowi firma zidentyfikowała i wyeliminowała błędy w przetwarzaniu faktur oraz zautomatyzowane harmonogramy usług.

- Korzystanie z Big Data zwiększa twoją wydajność

Korzystanie z narzędzi technologii cyfrowej zwiększa efektywność twojej firmy. Korzystając z narzędzi takich jak Mapy Google, Google Earth i media społecznościowe, możesz wykonywać wiele zadań bezpośrednio przy biurku, nie ponosząc kosztów podróży. Dzięki tym narzędziom oszczędzasz również dużo czasu.

- Korzystanie z Big Data pozytywnie wpływa na twoje ceny

Użyj narzędzia Business Intelligence, aby ocenić swoje finanse, dzięki czemu uzyskasz dokładniejszy obraz tego, gdzie znajduje się twoja firma.

- Możesz konkurować z dużymi firmami

Korzystanie z tych samych narzędzi, których używają duże firmy, pozwala ci przebywać na tym samym polu gry. Twoja firma staje się bardziej wyrafinowana, korzystając z narzędzi dostępnych dla własnego użytku.

- Korzystanie z Big Data pozwala skupić się na lokalnych preferencjach

Małe firmy powinny skoncentrować się na lokalnym środowisku, do spełniania potrzeb którego zostały one powołane. wielkie dane pozwalają jeszcze lepiej przyjrzeć się upodobaniom i preferencjom lokalnego klienta. Gdy twoja firma pozna preferencje twoich klientów w połączeniu z indywidualnym podejściem, zyskasz przewagę nad konkurencją.

- Korzystanie z Big Data pomaga zwiększyć sprzedaż i lojalność

Cyfrowe ślady, które zostawiamy za sobą, ujawniają spory wgląd w nasze preferencje dotyczące zakupów, przekonań, itp. Dane te umożliwiają firmom dostosowanie produktów i usług dokładnie do tego, czego chce klient. Cyfrowy ślad pozostaje odciśnięty, gdy klienci przeglądają strony internetowe i publikują je w mediach społecznościowych.

- Korzystanie z Big Data zapewnia zatrudnianie odpowiednich pracowników

Firmy rekrutujące mogą skanować życiorysy kandydatów i profile LinkedIn w poszukiwaniu słów kluczowych pasujących do opisu stanowiska. Proces rekrutacji nie opiera się już na tym, jak kandydat wygląda na papierze i jak jest postrzegany subiektywnie.

[King, A. (2018). 7 Benefits to Using Big Data for Small Businesses - IndustriusCFO. [online] IndustriusCFO. Dostępne na: http://www.industriuscfo.com/7-benefits-using-big-data/]

D. Poprawa kompetencji cyfrowych pracowników

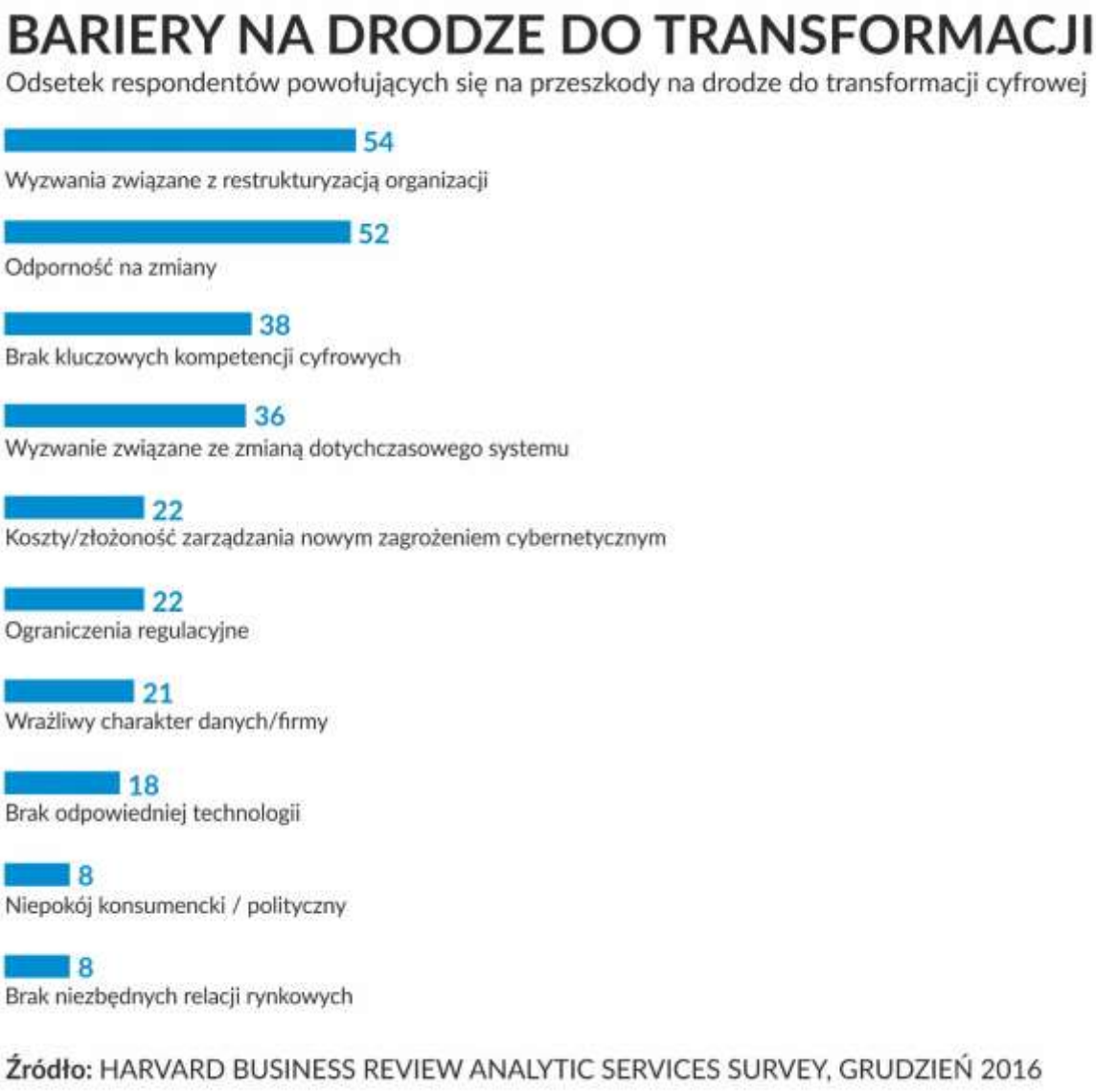
Bariery w digitalizacji biznesu a kompetencje cyfrowe

Cyfrowa transformacja zmienia każdy aspekt krajobrazu biznesowego, pod warunkiem, że liderzy są gotowi go zaakceptować. Jaki jest stan rewolucji cyfrowej i czego firmy powinny oczekiwać?

Doświadczamy już okresu cyfrowej transformacji, a firmy, które już ją dostrzegły, czerpią z tego tytuły korzyści. Czego możemy się jednak spodziewać przez następne kilka lat i jak firmy mogą nadążyć za zmianami wpływającymi na ich branżę?

Firma Harvard Business Review Analytics Services i Microsoft opublikowały raport „Competing in 2020: winners and losers in the digital economy", w którym przedstawiają stan rewolucji cyfrowej i jak na nią reagują liderzy biznesu. Jednym z najbardziej godnych uwagi punktów, które należy wziąć pod uwagę w tym konkretnym badaniu, była próba wykazania związku między barierami cyfryzacji biznesu a kompetencjami cyfrowymi.

Cyfrowa transformacja nie przychodzi bez wyzwań i istnieje wiele barier w jej integracji z biznesem. Respondentów ankiety poproszono o określenie najważniejszych barier w kierunku przystosowania się do transformacji cyfrowej w nadchodzących latach: 54% spośród nich określiło strukturę organizacji jako największe wyzwanie.



Ryc. 10: Bariery wobec przyszłej transformacji

Bardzo podobny odsetek (52%) określił odporność na zmiany jako kluczową barierę dla cyfrowej transformacji w swojej działalności, podczas gdy inne odpowiedzi obejmowały brak kompetencji cyfrowych, zasobów i budżetu. Opór wobec zmian jest prawdopodobnie najciekawszym zidentyfikowanym wyzwaniem, ponieważ wskazuje, że niektóre organizacje nie są otwarte na nowe trendy. Może to wymagać dalszej współpracy i kształcenia w tym kierunku, aby pomóc zrozumieć takim organizacjom korzyści wynikające z rewolucji cyfrowej w ich usługach.

Co więcej, brak zasobów, budżetu i kompetencji nie może być przeoczony, przy czym te ostatnie stwarzają potrzebę, aby każdy rozwijał właściwe cechy, które

ukształtują cyfrowego lidera. Zdaniem respondentów trzecią najważniejszą kompetencją, którą cyfrowi liderzy muszą posiąść do 2020 roku, jest umiejętność pracy ze specjalistycznymi danymi i analizami. Na drugim miejscu uplasowała się umiejętność współpracy, przy czym respondenci wyraźnie dostrzegli potrzebę większej liczby osób w swojej organizacji do rozwijania odpowiednich umiejętności, aby móc sprostać cyfrowej transformacji.

Ryc. 11. Najważniejsze kompetencje na rok 2020

[The rising opportunity of digital transformation: What businesses need to know - ClickZ. [online]. Dostępne na: https://www.clickz.com/the-rising-opportunity-of-digital-transformation-what-businesses-need-to-know/110987/]

Czym są kompetencje cyfrowe?

Kompetencje cyfrowe wywodzą się z warstwowej i złożonej konwergencji kilku kluczowych umiejętności, a mianowicie umiejętności informatycznych, umiejętności informacyjno-komunikacyjnych, alfabetyzmu cyfrowego, zdolności cyfrowych,

płynności w zakresie technologii informacyjno-komunikacyjnych, umiejętności obsługi komputera, umiejętności korzystania z technologii informacyjno-komunikacyjnych, e-umiejętności, umiejętności technologicznych, umiejętności korzystania z mediów, umiejętności przetwarzania informacji, e-alfabetyzacji, umiejętności ogólno-rozwojowych, umiejętności XXI wieku, multi-alfabetyzmu i nowego alfabetyzmu. Glister opisał najpowszechniej stosowane pojęcie kompetencji cyfrowych jako: umiejętności rozumienia i wykorzystywania informacji w wielu formatach z szerokiej gamy źródeł, gdy są one prezentowane za pośrednictwem komputera.

Kompetencje cyfrowe obejmują wiedzę i zdolność do określania potrzeb informacyjnych ze źródeł technologii cyfrowej oraz do odpowiedniego wykorzystywania cyfrowych narzędzi i urządzeń do wprowadzania, uzyskiwania dostępu, organizowania, integracji i oceny zasobów cyfrowych, a także do konstruowania nowej wiedzy, tworzenia wyrażeń medialnych i komunikowania się z innymi. Kompetencje cyfrowe obejmują zarówno umiejętności techniczne związane ze zrozumieniem i korzystaniem z cyfrowych systemów, narzędzi i aplikacji, jak i umiejętności przetwarzania informacji, które są poznawczymi podstawami biegłości cyfrowej.

Ryc. 12. Kategorie kompetencji cyfrowych

Dlaczego twoja firma potrzebuje szkoleń w zakresie kompetencji cyfrowych

Cyfrowy oznacza transformatywny. Konsumenci wspomagają się obecnie wyszukiwarkami i mediami społecznościowymi na każdym etapie swojej podróży zakupowej: 81% z nich przeprowadza badania online przed dokonaniem zakupu, a 70% podróży zakupowych jest zakończonych przed kontaktem ze sprzedawcą. Technologia cyfrowa umożliwiła konsumentom samokształcenie oraz odczuwanie większej skrupulatności przy podejmowaniu ostatecznej decyzji o zakupie.

Stwarza to zobowiązanie dla firmy do uznania i dostosowania się do tego cyfrowego wzrostu, jeśli chce osiągnąć trwały sukces konsumencki i przynosić tak wysokie zyski, jak tylko to możliwe. 76% specjalistów od marketingu uważa, że marketing zmienił się bardziej w ciągu ostatnich dwóch lat niż w całym ubiegłym pięćdziesięcioleciu, co oznacza, że niezbędne jest stałe podnoszenie kwalifikacji.

Organizacje, które podejmą decyzję o zatrzymaniu obecnych i przyciąganiu przyszłych klientów dzięki przemyślanej strategii marketingu cyfrowego, będą łatwiej budować świadomość marki, generować oszczędności, a ostatecznie zwiększać przychody. Właśnie dlatego wykwalifikowani profesjonaliści cyfrowi są nieodzownym atutem.

Jednak pomimo niewątpliwych korzyści płynących z cyfryzacji, duża liczba organizacji pozostaje odporna na stosowanie cyfrowych narzędzi i technologii. Niezależnie od tego, czy chodzi o brak odpowiedniego budżetu i zasobów, strach przed utratą kontroli czy ogólny sceptycyzm, że technologia cyfrowa może zapewnić znaczący zwrot z inwestycji, bariery w zakresie cyfrowej adopcji muszą zostać przezwyciężone, aby zagwarantować trwały sukces organizacyjny.

Odpowiedź jest prosta. Krótkoterminowa inwestycja w szkolenie w zakresie kompetencji cyfrowych spowoduje długoterminową nagrodę - wzmocnienie pozycji organizacji i jej pracowników, utrzymanie przewagi konkurencyjnej i zapewnienie, że nie zostaną pozostawieni w tyle.

Jeśli nadal masz wątpliwości, w jaki sposób twoja firma może skorzystać ze strategicznego, zrównoważonego planu edukacji cyfrowej, zapoznaj się z kilkoma kluczowymi zaletami wymienionymi poniżej:

1. Kompetencje cyfrowe mogą motywować pracowników

Obecnie istnieje niespotykany globalny niedobór kompetencji cyfrowych, który dotknął wszystkie branże. W rezultacie rekrutacja kompetentnych kandydatów stanowi problem dla organizacji każdej wielkości.

Ponieważ konkurują one ze sobą, aby zatrudnić tych kilku dostępnych specjalistów cyfrowych, mniejsze firmy cierpią na brak dopasowania do coraz bardziej lukratywnych wynagrodzeń i pakietów korzyści, które łatwo oferują ich konkurenci korporacyjni.

Jednak pomimo tego pilnego zapotrzebowania, poziom kompetencji cyfrowych na świecie jest oszałamiająco niski. W raporcie na temat kompetencji cyfrowych z 2016 roku specjaliści od marketingu z Irlandii, Wielkiej Brytanii i USA, testowani pod kątem kompetencji cyfrowych, uzyskali średnio zaledwie 38%. Wiąże się to z powszechnym uznaniem, że będą musieli zwiększyć swoje umiejętności w zakresie marketingu internetowego, aby pozostać kompetentnym w swoich rolach (86% Irlandia, 69% Wielka Brytania i USA).

Coraz więcej firm chce zatrudniać wykwalifikowanych specjalistów na całym świecie jako rozwiązanie tego niedoboru talentów. Jednak łatwiejszą i ostatecznie bardziej opłacalną opcją jest pielęgnowanie lokalnej puli talentów.

Według Adobe organizacje mające plan na osiągnięcie swojej dojrzałości cyfrowej dążą do szkolenia i rozwijania umiejętności swoich obecnych pracowników. Uznają, że szkolenie i możliwość rozwoju zawodowego i osobistego jest często głównym priorytetem dla pracowników. Bez tego mogą czuć się niestymulowani i pozbawieni złudzeń.

Jeśli organizacje zapewnią swoim pracownikom edukację cyfrową, nie tylko skorzystają z nowych możliwości cyfrowych i zachęt, ale mogą także wykorzystać szkolenie jako potężne narzędzie retencyjne.

2. Kompetencje cyfrowe mogą przyczynić się do zwiększenia przychodów

Cyfrowe narzędzia i technologie wywarły już głęboki wpływ na globalną gospodarkę. W 2016 r. światowe przychody z reklam online przewyższyły reklamę telewizyjną po raz pierwszy, a całkowite przychody z reklam cyfrowych osiągną w 2020 r. ponad 260 mld dolarów.

Wydatki na reklamę cyfrową i budżety marketingowe systematycznie się powiększają, ponieważ coraz więcej organizacji zaczyna doceniać korzyści biznesowe, jakie może przynieść technologia cyfrowa. Według raportu firmy Capgemini firmy o silniejszej intensywności cyfrowej czerpią więcej przychodów ze swoich aktywów fizycznych i są od 9 do 26% bardziej dochodowe.

Istnieje zbyt wiele postępów technologicznych dla organizacji, aby te mogły się rozwijać wyłącznie w oparciu o tradycyjne metody marketingu i sprzedaży. Tylko 28% potencjalnych klientów, do których zadzwonią akwizytorzy, faktycznie angażuje się w rozmowy, a tylko 1% z tych rozmów zostanie ostatecznie zamienionych na spotkania. Ponieważ konsumenci stają się bardziej uprzywilejowani za pomocą technologii cyfrowej, w mniejszym stopniu polegają na doświadczeniu przedstawicieli handlowych, a bardziej na własnych umiejętnościach badawczych. W odpowiedzi na tę zmianę władzy, organizacje muszą ożywić swoje funkcje sprzedażowe i marketingowe oraz wykorzystywać te same kanały i platformy, z których korzystają ich klienci, aby skutecznie do nich dotrzeć.

Kompetencje cyfrowe mogą umożliwić twojej organizacji lepsze utrzymywanie relacji z klientami, zdobycie pozycji lidera w branży i zyskanie większej liczby kupujących w trakcie podróży zakupowych. Trening kompetencji cyfrowych uwolni ten potencjał.

3. *Kompetencje cyfrowe mogą generować znaczne oszczędności*

Wszyscy słyszeliśmy zwrot „wydawaj pieniądze aby zarabiać pieniądze". Ale co z wydawaniem pieniędzy, aby oszczędzać pieniądze? Dzięki kompletnemu zestawowi kompetencji cyfrowych Twoja organizacja może osiągnąć oba te cele.

Amerykańskie Towarzystwo Szkoleń i Rozwoju (ASTD) zebrało informacje szkoleniowe od ponad 2500 firm i stwierdziło, że organizacje oferujące kompleksowe szkolenia mają o 218% wyższy dochód na pracownika niż te, które nie oferują szkoleń w takim stopniu. Oznacza to, że prosta czynność motywowania pracowników poprzez szkolenie z zakresu kompetencji może zaoszczędzić znaczną ilość pieniędzy dla organizacji. Podobnie, według Amerykańskiego Stowarzyszenia Zarządzania (AMA), koszt zatrudnienia i szkolenia nowego pracownika wynosi od 25 do 200% rocznej rekompensaty, więc szkolenie z zakresu kompetencji może ponownie obniżyć koszty, zmniejszając tym samym niepotrzebną rotację pracowników. Oprócz tego, inne korzyści finansowe mogą obejmować oszczędność siły roboczej, zmniejszenie liczby utraconych dni pracy i wzrost wydajności.

Główne zasady marketingu cyfrowego opierają się na efektywności i opłacalności:

- Precyzyjne opcje ukierunkowywania reklam mogą powodować niższy koszt za lepszy efekt.
- Łatwe i natychmiastowe interakcje online z segmentowaną grupą docelową mogą generować więcej konwersji przy niższych kosztach
- Duża ilość danych z narzędzi analitycznych zapewnia nieoceniony wgląd, który może pomóc w udoskonaleniu strategii cyfrowej i uniknięciu niepotrzebnych wydatków.

Według Gartnera, 40% organizacji twierdziło, że uzyskało znaczne oszczędności dzięki wykorzystaniu cyfrowych metod marketingowych do promowania swoich produktów i usług. Oszczędności te można następnie wykorzystać i ponownie zainwestować w bardziej cyfrowe techniki marketingowe i taktyki, aby powtórzyć sukces dochodu przy niższych ogólnych wydatkach.

4. *Kompetencje cyfrowe mogą pomóc twojej firmie w osiągnięciu przewagi konkurencyjnej*

Silny cyfrowy zestaw kompetencji nie jest już luksusem dla organizacji - jest podstawowym elementem każdego konkurencyjnego modelu biznesowego. Jednak pomimo tego nasz najnowszy raport na temat umiejętności wykazał, że organizacje pozostają w dużej mierze wyłączone z technologii cyfrowej. Tylko 31% organizacji amerykańskich, 25% Wielkiej Brytanii i 40% w Irlandii jest uważanych za rozwiniętych cyfrowo, zaś ich pracownicy jednomyślnie wskazali, że tempo zmian technologicznych i cyfrowych jest zbyt wolne.

Według McKinley'a, 90% wszystkich ról marketingowych wymaga kompetencji cyfrowych. Wynika to z tego, że cyfrowe specjalizacje są nieskończenie bardziej ukierunkowane, wydajne i mierzalne w porównaniu z tradycyjnymi technikami. Technologie cyfrowe umożliwiają osiągnięcie sukcesu. Może usprawnić procesy, przy wymaganym wysiłku ze strony organizacji, jednocześnie zwiększając możliwości. Uzyskanie dokładnych wglądów i przełożenie tych wglądów na działania oznacza, że jeśli uda się je wykorzystać, cyfrowe narzędzia i kanały mogą pomóc organizacjom w rozwoju i utrzymaniu znaczącej przewagi konkurencyjnej.

Media społecznościowe mogą stanowić platformę drobiazgowej obsługi klienta online, która poprawi wskaźniki retencji. Marketing mobilny może pomóc organizacji rozwinąć wszechobecną obecność marki. Marketing e-mailowy może pielęgnować wartościowe relacje za pomocą przydatnych treści na każdym etapie podróży klienta. Każda zbudowana kampania może być mierzona i optymalizowana za pomocą narzędzi analitycznych.

Niektóre z głównych barier utrudniających adopcję cyfrową to brak specjalistycznej wiedzy na miejscu w firmie, a także brak zaangażowania organizacyjnego w tym obszarze. Aby zdać sobie sprawę z potencjału cyfrowej organizacji, niezbędne jest posiadanie odpowiednich umiejętności, aby móc zrozumieć jej znaczące korzyści i podjąć działania.

[Digital Marketing Institute. (2018).Why your organization needs digital skills training. [online] Dostępne na: https://digitalmarketinginstitute.com/blog/why-your-organization-needs-digital-skills-training]

E. Digitalizacja biznesu - lista kontrolna

Czy jesteś gotowy na erę cyfrową?

Wielu właścicieli małych firm uważa, że skutecznie korzystają już z technologii cyfrowej, ponieważ mają stronę internetową i stronę na Facebooku. Istnieje jednak wiele innych sposobów wykorzystania technologii cyfrowej w celu poprawy wyników biznesowych.

Przeprowadzenie audytu cyfrowego pomoże ci ustalić, czy twoja firma jest cyfrowym nowicjuszem, cyfrowo aktywną czy cyfrowo zaawansowaną.

Digitalizacja: 10-stopniowa lista kontrolna „od czego zacząć”

Ścieżka do cyfryzacji może być długa. Aby się upewnić, że się nie zgubisz, powinieneś zacząć od przynajmniej następujących rzeczy:

	✓
Stwórz zespół na pokładzie. Przedstaw główne korzyści, jakie digitalizacja przyniesie nie tylko twojej firmie, ale wszystkim pracownikom. Namaluj obrazek, który przykuje uwagę wszystkich. Jeśli jesteś dyrektorem generalnym, upewnij się, że odgrywasz widoczną rolę w promowaniu zmiany.	
Zaakceptuj wizję. Wyobraź sobie wymierne korzyści, jakie może przynieść cyfrowe rozwiązanie dla ciebie, twojej firmy i społeczności. Zdecyduj, co chcesz osiągnąć, przechodząc w stronę cyfryzacji - i trzymaj się tego.	
Zrozum swoich przyszłych klientów. Miej oko na swoich milenialnych klientów. Używanie technologii w codziennym życiu jest dla nich drugą naturą.	

Opracuj rozwiązania technologiczne, aby zaspokoić potrzeby przyszłych klientów i dotrzymuj kroku przyszłej konkurencji.	
Zaplanuj cyfrową podróż. Zobacz, jak twoi obecni i docelowi klienci korzystają z platform cyfrowych. Pomoże to w zidentyfikowaniu właściwych rozwiązań cyfrowych, aby ich pozyskać.	
Utwórz grupę roboczą ds. cyfryzacji Zaangażuj wszystkich swoich pracowników, tworząc grupę roboczą cyfrowych mistrzów. Pomoże to zabezpieczyć opcję „wpisowego” w obszarach biznesowych. Grupa robocza może współpracować na osi czasu dostawy, utrzymywać harmonogramy projektów i aktualizować ich zespoły na temat postępów.	
Zainwestuj w odpowiednie narzędzia. Zbadaj odpowiednie, specyficzne dla branży oprogramowanie i narzędzia IT dla cyfrowego biznesu. Od księgowości - zarządzanie zapasami, punktem sprzedaży, listami płac i wielu innych - są setki aplikacji, które mogą pomóc twojej firmie. Zapewniają one bezpieczeństwo danych, mobilny dostęp, raportowanie i integrację w czasie rzeczywistym, aby ułatwić płynne przejście.	
Zarejestruj się na platformie SaaS Przejdź na właściwą platformę SaaS (oprogramowanie jako rozwiązanie), aby lepiej wykorzystywać ważne dane biznesowe i zarządzać nimi. Narzędzia SaaS, które komunikują się ze sobą na jednej platformie, mogą wyeliminować ręczne wprowadzanie danych - a to oznacza	

więcej czasu na prowadzenie firmy. Dostawcy usług SaaS mają również najwyższy poziom bezpieczeństwa, więc możesz mieć pewność, że wszystkie twoje informacje znajdują się w bezpiecznych rękach.	
Zmniejsz swoje straty Zademonstruj swoje odważne przywództwo, podejmując trudne decyzje. Wiedza, czy coś można czy nie można jest o wile mniej ważna niż miejsce w twojej strategii transformacji cyfrowej. Jeśli wymaga to spisania na straty kilku nierentownych inwestycji w stare systemy i oprogramowanie - zrób to.	
Mierz wyniki Śledź, jak twoje cyfrowe inicjatywy wpływają na twoje wyniki. Porównaj z pierwotnymi celami i zastanów się, czy twoje podejście konsekwentnie pomaga osiągnąć najlepsze wyniki.	
Podziel się swoją nową wiedzą Trenuj swój zespół, aby zapewnić swoim pracownikom umiejętności, wiedzę i doświadczenie, aby jak najlepiej wykorzystać swoją strategię cyfrową.	

F. Glosariusz terminologii

Big data - wielkie dane to zestawy danych, które są tak obszerne i złożone, że tradycyjne oprogramowanie do przetwarzania danych jest niewystarczające, aby sobie z nimi poradzić. Wyzwania związane z wielkimi danymi obejmują przechwytywanie danych, przechowywanie danych, analizę danych, wyszukiwanie, udostępnianie, przesyłanie, wizualizację, zapytania, aktualizację, prywatność informacji i źródło danych.

Chmura obliczeniowa - przetwarzanie w chmurze to paradygmat technologii informatycznej, który umożliwia powszechny dostęp do pul współużytkowanych z konfigurowalnymi zasobami systemowymi i usługami wyższego poziomu, które można szybko udostępnić przy minimalnym wysiłku zarządzania, często przez Internet. Przetwarzanie w chmurze polega na dzieleniu się zasobami w celu osiągnięcia spójności i ekonomii skali, podobnie do użyteczności publicznej.

Cyfrowy biznes - Cyfrowy biznes to tworzenie nowych projektów biznesowych poprzez zacieśnianie światów cyfrowych i fizycznych.

Rewolucja cyfrowa - rewolucja cyfrowa to efekt, który zmienia podstawowe oczekiwania i zachowania w kulturze, rynku, przemyśle lub procesie, które są spowodowane lub wyrażane poprzez cyfrowe kompetencje, kanały lub zasoby.

Kompetencje cyfrowe - kompetencje cyfrowe to umiejętności związane z umiejętnością czytania cyfrowego.

Digitalizacja - Digitalizacja polega na wykorzystaniu technologii cyfrowych w celu zmiany modelu biznesowego i zapewnienia nowych możliwości generowania przychodów i wartości. Jest to proces przejścia do biznesu cyfrowego.

Uczenie się maszynowe - algorytmy uczenia maszynowego składają się z wielu technologii (głębokie uczenie się, sieci neuronowe i przetwarzanie w języku naturalnym), stosowanych w uczeniu bez nadzoru i nadzorowanym, które działają w oparciu o wnioski z istniejących informacji.

Platforma (Digital Business) - platforma jest produktem, który obsługuje lub umożliwia prezentację innym produktom i usługom. Platformy (w kontekście biznesu cyfrowego) istnieją na wielu poziomach. Platformy różnią się pomiędzy sobą

poziomem, tj. te z wysokim poziomem umożliwiają platformowy model biznesowy platformom niskopoziomowym, zapewniającym zbiór biznesowych i/lub technologicznych możliwości wykorzystywanych przez inne produkty lub usługi do dostarczania własnych możliwości biznesowych Platformy umożliwiające model biznesowy platformy mają powiązane ekosystemy biznesowe.

G. Wnioski i dodatkowe źródła wiedzy

Niewątpliwie transformacja cyfrowa będzie przełomem dla wielu branż. Jest to kolejna faza rewolucji przemysłowej. Cyfryzacja biznesu nie jest cyfrową transformacją działalności gospodarczej, ale jest kluczowym krokiem w tym kierunku.

Pomimo tego, jak ważna wydaje się cyfryzacja biznesu, nie jest to łatwa droga do przebycia. Ponad połowa kadry kierowniczej w Europie twierdzi, że innowacje cyfrowe nie przyniosły dużego wpływu na funkcjonowanie ich organizacji. Często duże firmy uważają, że cyfryzacja jest jedynie nowym kanałem i nie do końca jest jasne, czego mogą się po niej spodziewać.

Z pewnością wyzwaniem jest, aby pozostać na szczycie wielu technologii cyfrowych, takich jak sztuczna inteligencja, biometria, obliczenia kwantowe i robotyka. Jednak, gdy firmy stawiają klienta w samym centrum cyfrowej innowacji i wykorzystują technologie cyfrowe do tworzenia dla nich pozytywnych doświadczeń, raz za razem widzimy, że uzyskujemy w efekcie wysoki wpływ. Firmy często rozpoczynają cyfryzację od projektu, ale ta konfiguracja nie może wywrzeć dużego wpływu na organizację.

Technologie cyfrowe zasadniczo zmieniają sposób, w jaki firmy wchodzą na rynek i organizują się wewnętrznie. Aby technologie cyfrowe mogły wywrzeć duży wpływ, cała organizacja musi zostać wzięta pod uwagę i musi zaadaptować ten nowy sposób myślenia.

Firmy, które uważają, że integracja nowych technologii z istniejącą (starszą) infrastrukturą jest ich kluczowym wyzwaniem w zakresie innowacji cyfrowych, zaczęły od niewłaściwego podejścia. Technologie cyfrowe nie są tutaj po to, aby naprawić coś, co nie działa. Technologie cyfrowe pozwalają firmom na gruntowne przemyślenie tego, z czym trafiają na rynek, w jaki sposób trafiają na rynek i z kim trafiają na rynek.

Kluczowe znaczenie ma również utrzymanie całego zespołu, osób odpowiedzialnych za działalność dostosowaną do tej zmiany. Pracownicy muszą posiadać te określone umiejętności, które pomogą im w przyjęciu zmiany i w skutecznym wykonywaniu działań w nowym środowisku cyfrowym.

Wydaje się, że ludzie są najważniejszym czynnikiem dla nowych technologii, aby z powodzeniem wtopić się w środowisko biznesowe i stać się narzędziem do sukcesu.

Dodatkowe źródła wiedzy:

Aby dokonać cyfrowej transformacji, musisz być całkowicie przesiąknięty działaniem uczenia maszynowego i sztucznej inteligencji. Powinieneś także zdawać sobie sprawę z rewolucji Blockchain oraz jak technologia stojąca za Bitcoin zmienia pieniądze i biznes. Prędzej czy później, każda organizacja będzie musiała zrozumieć i używać blockchain (https://pl.wikipedia.org/wiki/Blockchain) w jakiejś formie. Zdolność do wybierania właściwych członków zespołu, zbliżania ich do wspólnej wizji i motywowania ich do osiągnięcia więcej, niż mogliby sądzić, jest także umiejętnością, którą powinieneś dalej rozwijać. Wielkie dane - obserwujesz, jak wielkie dane zmieniają świat IT i świat biznesu. Ale pod wieloma względami ten trend dopiero zaczyna się kształtować. Wielu liderów wciąż nie rozumie ani nie wykorzystuje siły danych do podejmowania decyzji, dużych i małych. Zapoznaj się z możliwościami, jakie otwierają duże zbiory danych, a także z zagrożeniami, które za nimi stoją. Możesz również przeanalizować sposób, w jaki działają firmy typu start-up i jak wykorzystują ciągłe innowacje, aby stworzyć radykalnie udany biznes. I to jest ten powód dla którego start-upy tak często z sukcesem konkurują z większymi, bardziej ugruntowanymi organizacjami. Zastosowanie zasad „Lean” i „Agile” we własnej organizacji i technologii pomoże Ci dostosować się do szybko zmieniającego się rynku i sprawi, że będziesz mniej podatny na ataki z zewnątrz. Może to nawet pomóc w stworzeniu własnej rewolucji.

H. Źródła:

1. i-scoop: Digitization, digitalization and digital transformation: the differences (https://www.i-scoop.eu/digitization-digitalization-digital-transformation-disruption)
2. Gartner Executive Programs: Taming the Digital Dragon: The 2014 CIO Agenda
3. i-scoop: Digital business: transformation, disruption, optimization, integration and humanization (https://www.i-scoop.eu/digital-business)
4. tieto: How Digitalization is Changing the Face of Business (https://perspectives.tieto.com/blog/2015/07/how-digitalization-is-changing-the-face-of-business)
5. Forbes: Digital Business is Everyone's Business (https://www.forbes.com/sites/gartnergroup/2014/05/07/digital-business-is-everyones-business/#7f60b8b67f82)
6. cio: Digital transformation: Why it's important to your organization (https://www.cio.com/article/3063620/it-strategy/digital-transformation-why-its-important-to-your-organization.html)
7. insightsuccess: Role of Digitization in Today’s Business World (https://www.insightssuccess.com/role-of-digitization-in-todays-business-world)
8. Forbes: Digital Transformation And Innovation In Today's Business World (https://www.forbes.com/sites/brianrashid/2017/06/13/digital-transformation-and-innovation-in-todays-business-world/#341a36e74905)
9. McKinsey & Company: Raising your Digital Quotient (https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/raising-your-digital-quotient)
10. Deloitte: Doing business in the digital age: the impact of new ICT developments in the global business landscape (April 2013)
11. Gartner: The New Risks of Digital Business (https://www.gartner.com/smarterwithgartner/the-new-risks-of-digital-business)
12. i-scoop: Cybersecurity: security risks and solutions in the digital transformation age (https://www.i-scoop.eu/cyber-security-cyber-risks-dx)

13. wired: 5 cloud business benefits (https://www.wired.com/insights/2012/10/5-cloud-business-benefits)

14. dreamhost: What is Cloud Computing and How Can It Help Your Small Business? (https://www.dreamhost.com/blog/cloud-computing-for-business)

15. McKinsey & Company: How companies are using big data and analytics (https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/how-companies-are-using-big-data-and-analytics)

16. Business News Daily: 8 Big Data Solutions for Small Businesses (https://www.businessnewsdaily.com/6358-big-data-solutions.html)

17. sas: How Midsized Businesses Can Take Advantage of Big Data (white paper)

18. Bernard Marr & Co: How Is Big Data Used In Practice? 10 Use Cases Everyone Must Read (https://www.bernardmarr.com/default.asp?contentID=1076)

19. Digital Skills Academy: The Top 10 Digital Skills Tech Companies are Looking for Today (https://digitalskillsacademy.com/blog/the-top-10-digital-skills-tech-companies-are-looking-for-today)

20. Skillsoft: What are digital skills? A comprehensive definition for modern organisations (white paper)

21. Digital Marketing Institute: Why your organization needs digital skills training (https://digitalmarketinginstitute.com/blog/why-your-organization-needs-digital-skills-training)

22. Department for Culture, Media and Sports, France: Digital Skills for the Digital Economy

23. Smallbizdaily.com: The Benefits of Being a Digital Business (https://www.smallbizdaily.com/benefits-digital-business/)

24. Forrester: Why Do Digital Business Transformations Fail? (https://go.forrester.com/blogs/15-04-01-why_do_digital_business_transformations_fail/)

25. Business Queensland: Cloud computing for business (https://www.business.qld.gov.au/running-business/it/cloud-computing)

26. Business News Daily: Cloud Computing: A Small Business Guide (https://www.businessnewsdaily.com/4427-cloud-computing-small-business.html)

CZĘŚĆ II

CYBERBEZPIECZEŃSTWO DLA MŁODYCH INNOWATORÓW SPOŁECZNYCH

Spis zastosowanych skrótów

Skrót	Rozwinięcie
SBI	Inicjatywa na rzecz przedsiębiorczości społecznej
MŚP	Małe i średnie przedsiębiorstwa
IoT	Internet przedmiotów
SEO	Optymalizacja dla wyszukiwarek internetowych (ang. Search Engine Optimization)
IT	Technologie informacyjne (ang. Information Technology)

A. Wstęp

Kolejne rozdziały pozwolą przedsiębiorstwom społecznym i innowatorom społecznym zrozumieć koncepcję przedsiębiorczości społecznej w erze cyfrowej oraz tego, jak zmieniło się środowisko pracy, od tradycyjnego środowiska biurowego do środowiska cyfrowego w sferze Internetu przedmiotów. W rozdziale tym zostaną również przedstawione możliwości i zagrożenia dla przedsiębiorstwa społecznego w środowisku online oraz podpowiemy, jak prawidłowo rozwijać firmę, aby uniknąć szkodliwych skutków prowadzenia działalności w Internecie. Rozdział ten przedstawi innowatorom społecznym i przedsiębiorcom wskazówki i przydatną listę kontrolną do wdrażania zabezpieczeń cyfrowych w ich przedsiębiorstwach społecznych.

„Przedsiębiorstwo może być społeczne tylko wtedy, gdy cele społeczne są główną misją jego działalności.” [11]

B. Przedsiębiorczość społeczna w erze cyfrowej

Jest oczywiste, że przedsiębiorstwa społeczne mają dzisiaj bardzo pozytywny wpływ na społeczeństwo, a nawet więcej, wydają się być buforem dla negatywnych konsekwencji wywołanych kryzysem gospodarczym.

> *„Przedsiębiorczość społeczna była jednym z głównych tematów omawianych na Światowym Forum Ekonomicznym, które odbyło się w Davos w styczniu 2017 r., jako nowy sposób lub narzędzie do przezwyciężenia pewnych problemów społecznych, które nękają współczesne społeczeństwa" [11].*

Ponadto środowisko biznesowe zmieniło się z biurowego, bardziej tradycyjnego środowiska biznesowego na cyfrowe, co zapewnia również inne podejście biznesowe dla firm, które jest znacznie bardziej przystosowalne do zmian niż wcześniej. Cyfrowe środowisko, innowacje i pojawiające się technologie są dla przedsiębiorstw szansą na uwzględnienie w ich codziennej działalności, ale także stanowią zagrożenie, jeśli nie zostaną odpowiednio wdrożone. Jeśli narzędzia te mają mieć odpowiedni wpływ na działalność biznesową, powinny być odpowiednio zintegrowane i z punktu widzenia firmy powinny być zorientowane na odpowiednie zarządzanie ryzykiem cyfrowym i strategię ochrony prywatności [1].

Jednak firmy często nie rozumieją w dostateczny sposób, jak kwestie cyfrowego bezpieczeństwa i prywatności mogą stwarzać ryzyko gospodarcze i mają ograniczoną zdolność reagowania na nie, a także zarządzania nimi. Podczas gdy różne rodzaje MŚP stoją w obliczu różnych wyzwań, to każdy z nich może czerpać korzyści z integracji zarządzania ryzykiem cyfrowym i ryzykiem prywatności przy podejmowaniu decyzji biznesowych.

W obecnej erze cyfrowej usługi w różnych obszarach biznesowych muszą działać nieprzerwanie, 24 godziny na dobę, 365 dni w roku. Chociaż poczyniono postępy w zakresie wydajniejszego świadczenia usług za pomocą technologii takich jak Internet przedmiotów, to metody ataków cybernetycznych stały się coraz bardziej różnorodne i wyrafinowane - a nawet zbliżone do cyberterroryzmu. Właśnie dlatego bezpieczeństwo w systemie jest niezbędne [2].

> *„Internet, serwisy społecznościowe i media społecznościowe stały się kluczowymi zasobami dla sukcesu i współpracy wielu przedsiębiorców*

społecznych. Po 2000 roku Internet stał się szczególnie przydatny w rozpowszechnianiu informacji szerokiemu gronu podobnie myślących osób w krótkim czasie, nawet jeśli osoby te są geograficznie rozproszone. Ponadto Internet umożliwia łączenie zasobów projektowych przy użyciu zasad open source "[3].

Jak już ustalono, każde przedsiębiorstwo, a zwłaszcza przedsiębiorstwa społeczne, muszą dostosować się do prędkości, środowiska i wymagań cyfrowych, a także muszą dostosować swoje produkty, usługi, działalność, partnerstwo i postępowanie do środowiska cyfrowego. Jednak firmy, gdy rozpatrują możliwość przystosowania się do świata cyfrowego, coraz częściej nie dostrzegają tego jakie możliwości mogą zyskać, gdy zdigitalizują swoją działalność. Co może zrobić środowisko cyfrowe dla biznesu?

Takimi przykładami są modele typu wiki lub crowdsourcing, na przykład przedsiębiorstwo społeczne może pozyskać setki osób z całego kraju (lub z wielu krajów) do współpracy przy wspólnych projektach online (np. opracowanie biznesplanu lub strategii marketingowej na przedsięwzięcie przedsiębiorczości społecznej). Oto lista stron crowdfundingowych, które mają na celu wzmocnienie pozycji przedsiębiorców w celu promowania dobra społecznego. Te strony crowdfundingowe finansują projekty typu for-profit i non-profit:

- 33needs to strona crowdfundingowa dla przedsiębiorstw społecznych. Jej celem jest znalezienie firm, które są najbardziej zdolne do tworzenia zmian i pomóc im uzyskać to, czego potrzebują, aby zapewnić inwestowanie z korzyścią dla przedsiębiorców społecznych, przedsiębiorstw społecznych i firm z misją społeczną. Przedsiębiorcy społeczni mają od 30 do 60 dni na osiągnięcie celu.
- Buzzbnk to internetowy portal, który łączy przedsięwzięcia społeczne ze wszystkich środowisk ze zwolennikami, wspomożycielami i fanami. Buzzbank pobiera niewielką opłatę rejestracyjną za dołączenie przedsięwzięcia społecznego.
- CauseVox to witryna crowdfundingowa dla organizacji non-profit i dla celów zarobkowych. Witryna udostępnia niezły zestaw narzędzi i szablonów do

zaprojektowania kampanii, pozyskiwania wsparcia w witrynie lub za pośrednictwem mediów społecznościowych, śledzenia postępów i wykorzystywania danych.

- IndieGoGo oferuje każdemu, kto ma kreatywny, społecznie zaangażowany i przedsiębiorczy pomysł, narzędzia do budowania kampanii i zbierania pieniędzy. Chociaż jest to ogólna strona crowdfundingowa, skupia się ona wyraźnie na projektach dotyczących dobra publicznego.
- ioby pomaga zebrać niezbędne fundusze i znaleźć nowych wolontariuszy. Ioby dba o kwestie środowiskowe na obszarach miejskich oraz wszelkie inne ważne kwestie, które mają wpływ na funkcjonowanie społeczności.
- OpenIDEO jest społecznym motorem zmian społecznych. Po tym, jak wyzwanie zostało postawione, mają miejsce trzy fazy rozwoju - inspiracja, konceptualizacja i ewaluacja. Członkowie społeczności mogą wnosić swój wkład na wiele różnych sposobów, od inspirujących obserwacji i zdjęć, szkiców pomysłów po modele biznesowe i fragmenty kodu.
- Start Some Good jest stroną, na której przedsiębiorcy społeczni gromadzą społeczność i zbierają fundusze potrzebne do wprowadzenia zmian. Zarówno przedsiębiorstwa społeczne nastawione na zysk, jak i non-profit mogą prowadzić na stronie kampanie fundraisingowe.

Takie strony internetowe pomagają przedsiębiorcom społecznym rozpowszechniać swoje pomysły wśród szerszej publiczności, pomagają w tworzeniu i utrzymywaniu sieci osób o podobnych poglądach oraz pomagają powiązać potencjalnych inwestorów, darczyńców lub wolontariuszy z organizacją. Umożliwia to przedsiębiorcom społecznym osiągnięcie ich celów przy niewielkim kapitale rozruchowym lub bez jego udziału, a także z niewielką lub z brakiem siedziby (np. Przy wynajętej powierzchni biurowej). Na przykład rozwój technologii open-source jako trwałego narzędzia umożliwia ludziom na całym świecie współpracę w rozwiązywaniu lokalnych problemów.

W ostatnich latach duży nacisk na wsparcie przedsiębiorstw społecznych znajduje się na wczesnym etapie rozwoju - od początkowej koncepcji, poprzez uruchomienie i inwestycje. Te inicjatywy, często określane jako „inkubatory", działają zazwyczaj

z osobami lub zespołami, które mają pomysł na przedsiębiorstwo społeczne i zapewniają szereg narzędzi pomocniczych, które pomogą im je rozwinąć i uruchomić. Niektóre zapewniają również ciągłe wsparcie dla start-up'ów [4].

WSKAZÓWKI DLA PRZEDSIĘBIORSTW SPOŁECZNYCH:

Skorzystaj z zasobów, jakie zapewnia przestrzeń co-workingowa

Brak przestrzeni biurowej często powstrzymuje ludzi przed założeniem firmy. Przestrzenie co-workingowe rozwiązują ten problem, dając ci miejsce, w którym możesz z łatwością pracować. Wynajem przestrzeni co-workingowej jest tańszy niż wynajem własnego biura. Możliwe jest wyszukiwanie bezpłatnych przestrzeni co-workingowych, również dla start-upów, które może być finansowane lokalnie, regionalnie lub w skali kraju i zapewnia bezpłatne powierzchnie biurowe dla start-upów [5].

Korzystaj z bezpłatnych usług, aby zarabiać na swojej firmie

Przedsiębiorcy społeczni powinni promować swoje firmy za pośrednictwem jednej z wielu bezpłatnych usług, które ostatnio pojawiły się na rynku. Obecnie funkcjonują platformy, na których każdy przedsiębiorca może się zarejestrować i osiągnąć sukces bez zatrudniania sprzedawcy, projektanta lub zespołu do budowy swojej strony internetowej. Takie strony internetowe to rynek internetowy i mobilny, który łączy pracę freelancerów z lokalnym popytem, umożliwiając konsumentom lub firmom znalezienie natychmiastowej pomocy [5]. Strony, które pomagają każdemu zarabiać lub sprzedawać swoje usługi online: TaskRabbit, Crowdsite, Envato studio, …

Użyj crowdfundingu

Przedsiębiorcy społeczni mogą również czerpać korzyści z platform finansowania społecznościowego, dzięki którym twój produkt stanie się globalną sceną i niech świat stanie się twoim fundatorem. Przykłady takich platform i strony internetowej zostały opisane powyżej [5].

Dostrzeż innowacje

Czytając to udowadniasz, że jesteś innowatorem społecznym, ale ważne jest, aby zwiększyć innowacyjność i pozwolić każdemu w firmie na bezpośredni dostęp do osób podejmujących ważne decyzje. Zatrudnij wspaniałych ludzi i daj im szansę na innowacje. Innowacja niekoniecznie oznacza następny wielki pomysł. Innowacja może być w sposobie, w jaki się komunikujesz wewnątrz firmy lub w jaki sposób działa twój proces biznesowy, a nawet technologia, z której korzystasz. W tym sensie powinieneś rozważyć innowację jako kogokolwiek lub cokolwiek, co usprawni twój proces biznesowy, aby był lepszy niż dotąd. Aby odnieść sukces jako cyfrowy biznes społeczny, konieczne jest ponowne ocenienie wszystkich procesów biznesowych. Jeśli nie, ostatecznie nastąpi rozłączenie pod względem wydajności, dostępu do danych i widoczności w całym kompleksowym procesie - co spowoduje opóźnienia i błędy, które nie są akceptowane w nowym cyfrowym świecie [5].

> *„Technologie cyfrowe otwierają nową i być może nieograniczoną dziedzinę innowacyjnych strategii ... "[11]*

Bądź przedsiębiorcą społecznym opartym na danych

Podejmowanie decyzji opartych na danych jest kluczem do rozwoju każdej firmy. Korzystaj z dostępnych danych i wykorzystuj je, aby dowiedzieć się, co działa najlepiej. Małe zmiany w danych mogą mieć ogromny wpływ na sukces firmy. Zaleca się korzystanie z usług takich jak Google Analytics do statystyk ruchu i Google AdWords w celu poprawy SEO na rynku docelowym [5].

Spraw, aby produkt był częścią twojego zespołu

Przekonaj się, kim są twoi zwolennicy i wykorzystaj ich do zaangażowania się w twoją społeczność. Po znalezieniu tych influencerów, należy ciężko się napracować, aby ich zaangażować. Jeśli ktoś lubi produkt, będzie produktywny dla danego przedsięwzięcia, czyniąc produkt częścią jego życia i dzieląc się nim ze swoimi przyjaciółmi [5].

Youtuberzy, vlogerzy i blogerzy stają się coraz ważniejszymi ambasadorami marki, jeśli chodzi o lokowanie produktu lub reklamę firmową, a także angażują zupełnie różnych obserwatorów w stosunku do zwykłej grupy docelowej. Nie oznacza to, że

koniecznie musisz mieć ambasadora marki. To tylko sposób na zaangażowanie większej liczby różnych docelowych odbiorców.

C. Cyfrowe wdrażanie koncepcji społecznej przedsiębiorczości

Przedsiębiorczość społeczna to innowacyjna forma przedsiębiorczości z naciskiem na solidarność społeczną, współpracę i odpowiedzialne zachowanie wobec społeczeństwa i ludzi [6]. Przedsiębiorczość społeczna mocno zakotwiczyła w świecie biznesu i musi, jak każda inna firma, dostosować się do obecnego świata cyfrowego. Zagrożenie polega na tym, że firmy i osoby zaangażowane w ich działalność nie są w stanie tak szybko przystosować się do zmian w cyfrowym świecie i to tak szybko, jak zmienia się sfera cyfrowa i technologia. Przedsiębiorstwa społeczne nie różnią się w tej kwestii.

Na dzisiejszym ciągle zmieniającym się rynku możemy zadać sobie pytanie: Jak firmy społeczne przetrwają w erze cyfrowej? Większość firm społecznych uważa, że wystarczy mieć stronę internetową lub profile w mediach społecznościowych. Aby zaistnieć w marketingu cyfrowym, trzeba przeciwstawić się konkurencji, a co ważniejsze, przyciągnąć więcej klientów do swojej firmy.

> *„Zachowania konsumentów ewoluują w szybszym tempie, niż wiele firm może sobie z tym poradzić. W związku z tym tradycyjne firmy ze wszystkich branż nie dostarczają tego, czego chcą i oczekują klienci w erze cyfrowej. A dla tych, którzy nie nadążają, wpływ może być znaczny. Dzięki technologii zmieniającej sposób funkcjonowania firm, istnieją pewne znaczące trendy, które mogą pomóc utrzymać pozycję firmom społecznym na czele."* [7]

Nie ma jednego uniwersalnego wzorca lub harmonogramu tworzenia zmian biznesowych i adaptacji do świata cyfrowego, jednak badania przewidują kilka kluczowych kroków, które firmy powinny rozważyć, dostosowując się do świata cyfrowego.

Komunikuj strategię: przedsiębiorstwa i ludzie nie mogą się zmienić bez poczucia celu i wspólnego zrozumienia oraz zatwierdzenia strategii komunikacji dla gospodarki cyfrowej. Tradycyjna komunikacja w biurze nie działa, jeśli ty i twoi współpracownicy są całkowicie cyfrowi i komunikujesz się za pośrednictwem Skype, Viber, e-maili, a nawet za pośrednictwem intranetu. Strategia komunikacji musi zostać ponownie oceniona i przystosowana do środowiska cyfrowego. Poprzez strategię komunikacji

można rozumieć wszystkie strategie komunikacyjne, jakie może mieć społeczny biznes (z konsumentami, z interesariuszami, współpracownikami i wszystkimi innymi beneficjentami) [8].

Buduj nowe struktury: Biznes społeczny działający w świecie cyfrowym może potrzebować innej struktury organizacyjnej niż tradycyjnie działająca firma. Ponieważ uwaga w środowisku cyfrowym przesunęła się bardziej w stronę wizualizacji, fotografii, wideo, przesyłania strumieniowego, mediów społecznościowych, potrzebnych może być więcej projektantów, fotografów lub edytorów wideo niż w tradycyjnym biznesie społecznym, dlatego też struktura organizacyjna w firmie musi zostać odnowiona, oceniona i ponownie zaprojektowana wokół potrzeb organizacji w środowisku cyfrowym. Może to oznaczać, że musisz stworzyć nowe struktury lub zespoły do obsługi operacji cyfrowych i modeli biznesowych [8].

Przeanalizuj zespoły: Podczas burzy mózgów dotyczących wszelkiego rodzaju problemów lub rozwiązań wskazane jest uwzględnienie w zespołach grup projektowych pracowników z różnych działów o różnych umiejętnościach i dogłębnej wiedzy na temat polityki, komunikacji, analityki, itp. Taka odmienna współpraca ludzi jest o wiele bardziej innowacyjna i sprawna w poszukiwaniu rozwiązania [8].

Eksperymentuj i ucz się: Cyfrowa innowacja oznacza pracę z danymi i ich wykorzystywanie w zupełnie nowy sposób. Cyfrowe firmy społeczne muszą zacząć cechować się szybkością i chęcią do eksperymentowania, dzięki czemu można szybciej reagować na potrzeby konsumentów i zmiany na rynku [8].

Przeanalizuj ponownie system IT Wiele systemów IT jest zbyt wolnych i sztywnych dla biznesu cyfrowego. W miarę modernizacji infrastruktury informatycznej firmy dążą do uzyskania elastyczności, szybkości i bezpieczeństwa [8].

WSKAZÓWKI NA WDROŻENIE CYFRYZACJI

- Start-up Power Text Solutions zapewnia zestaw internetowych narzędzi badawczych, takich jak kategoryzacja i podsumowanie informacji. Jego celem jest stworzenie niespotykanej dotąd platformy wspierającej wspólne badania internetowe.

- Google Wave - ma na celu umożliwienie ludziom z całego świata wzajemnej interakcji, współpracy i wymiany niemal każdego rodzaju informacji w czasie rzeczywistym.

D. Cyfrowe zagrożenia i możliwości dla przedsiębiorstw społecznych

Komisja Europejska i Europejski Komitet Ekonomiczno-Społeczny zajęły się ważną potrzebą przedsiębiorstw społecznych, tj. aby wykorzystać możliwości digitalizacji do osiągnięcia celów społecznych i środowiskowych. *„Gospodarka społeczna i przedsiębiorstwa społeczne muszą wykorzystywać cyfryzację i technologie cyfrowe jako dźwignię transformacji gospodarczej i społecznej oraz większego wpływu społecznego w całej Europie" [9].*

Szansa, jaką oferuje technologia cyfrowa, jest znacznie większa dla małych i średnich przedsiębiorstw społecznych i firm społecznych, często ograniczonych zasobami. Dobre narzędzia cyfrowe w połączeniu z prostą, ale inteligentną zintegrowaną strategią cyfrową i informatyczną umożliwiają znaczną optymalizację zasobów. *"Upewnij się, że ostateczny cel wdrożenia nowego rozwiązania jest przejrzysty, że masz wyższe kierownictwo lub opiekunów i że wszyscy kluczowi interesariusze są zaangażowani w testowanie różnych rozwiązań. Jeśli zrobione poprawnie, możesz zaoszczędzić pieniądze, czas i skoncentrować się na uzyskaniu większego wpływu" [10].*

Cyfrowe możliwości dla przedsiębiorstw społecznych

+ potencjał angażowania znacznie większej publiczności w interaktywnym środowisku.

+ media społecznościowe jako odniesienie dla danych osobowych (interesy, potrzeby, opinie i nastroje danej jednostki).

+ to świetny sposób, aby zachęcić ludzi do mówienia o swojej marce kosztowo.

+ przekazywanie wiadomości za darmo do grupy docelowej

+ mając sklep internetowy, twoi klienci mogą pochodzić z całego świata [7].

Cyfrowe zagrożenia dla przedsiębiorstw społecznych

- czasochłonność;

- dodatkowe koszty personelu, jeśli jest zarządzany wewnętrznie;

- narażenie na naruszenie bezpieczeństwa (wrażliwe dane osobowe lub firmowe);

- oszustwo/Phishing, złośliwe oprogramowanie/konie trojańskie, oprogramowanie szantażujące, cyberataki;

- problemy ze zgodnością.

Przydatną wskazówką przy dostosowywaniu firmy do środowiska online jest utworzenie wewnętrznej listy kontrolnej. To nie tylko zapewnia przejrzystość, jakie polityki, procedury i procesy przeszła organizacja, dostosowując się do środowiska cyfrowego, ale jest także świetnym i łatwym sposobem spojrzenia na słabe punkty organizacji, ponieważ oczywiste będzie, co zostało zaniedbane lub pominięte w procesie adaptacji.

Dla firm w środowisku cyfrowym ważne jest posiadanie odpowiedniego i wystarczającego sprzętu, ale przede wszystkim ścisłych i bezpiecznych programów komputerowych oraz stosowanych zabezpieczeń sieciowych i polityk takich jak: program antywirusowy, hasło i szyfrowanie. W organizacji pracuje wiele osób na różnych stanowiskach, które mają dostęp do poufnych lub strzeżonych informacji, które muszą być odpowiednio zabezpieczone, nie tylko przed zewnętrznymi potencjalnymi hakerami, ale także aby zapobiegać wszelkiemu niewłaściwemu użyciu w obrębie personelu organizacji. Tak proste i skuteczne zasady dotyczące haseł i szyfrowania są zalecane dla pierwszych kroków, w jaki sposób chronić swoje informacje, dane i prywatność. Organizacja, a dokładniej dyrektor lub przedstawiciel, musi przypisać prawa użytkowników wszystkim członkom zespołu i potwierdzić je w systemie. Konieczne jest uzgodnienie i wyjaśnienie, do których plików, informacji lub danych pracownicy mają dostęp, a do których nie. Powinien również istnieć protokół, jeśli członek zespołu potrzebuje określonych informacji, które są obecnie odmawiane przez użytkownika. Ponadto jakie są procedury uzyskiwania takich informacji i kto jest osobą kontaktową, która zatwierdza aktualizację uprawnień.

Wysokiej rangi menedżerowie, dyrektorzy lub niektórzy znaczący członkowie personelu mogą mieć zdalny dostęp do serwerów komputerowych i do istniejących danych. Twoja organizacja musi stosować politykę, w której wymieniono szczegółowo członków zespołu oraz jakie dokumenty i informacje są im zdalnie dostępne. Wszystkie wyżej wymienione kroki w zakresie bezpieczeństwa cyfrowego nie będą działać, jeśli organizacja nie ustanowiła sposobów ich monitorowania. Jeśli organizacja nie wyznaczy jasnego systemu monitorowania z określonym członkiem zespołu i jeśli kary za jakiekolwiek naruszenie nie są wszystkim znane, to lista kontrolna zagrożeń jest bezcelowa.

E. Lista kontrolna cyfrowego bezpieczeństwa

	✓
Bezpieczeństwo sieci	
Polityka antywirusowa	
Polityka hasłowa	
Polityka szyfrowania	
Polityka dostępu zdalnego	
Ochrona danych	
Ochrona prywatności	
Zarządzanie uprawnieniami użytkownika	
Edukacja użytkowników, świadomość pracowników	
Zarządzanie ryzykiem	
Monitoring	

F. Glosariusz terminologii

Crowdsourcing - to model, w którym osoby lub organizacje uzyskują towary i usługi, w tym pomysły i finanse, od dużej, stosunkowo otwartej i często szybko ewoluującej grupy użytkowników Internetu. Dzieli pracę pomiędzy uczestnikami, aby osiągnąć skumulowany wynik. Jako sposób pozyskiwania, crowdsourcing istniał przed erą cyfrową (tj. "Offline").

Przedsiębiorczość cyfrowa - Przedsiębiorczość cyfrowa może być zdefiniowana jako przedsiębiorczość, w której niektóre lub wszystkie przedsięwzięcia odbywają się cyfrowo zamiast w bardziej tradycyjnych formatach. Produkty, dystrybucja, miejsce pracy - każde z nich i więcej może przybrać formę cyfrową w przedsiębiorczym przedsięwzięciu.

Rynek cyfrowy - Internet udostępnia ogromny asortyment produktów i usług wszystkim na świecie dzięki połączeniu z Internetem. W przypadku produktów cyfrowych, takich jak muzyka czy oprogramowanie, dystrybucja produktu staje się natychmiastowa i bezpłatna. Wraz z wprowadzeniem strony internetowej każde przedsięwzięcie rozprzestrzenia się natychmiast po świecie.

Cyfrowe miejsce pracy - Zasięg Internetu umożliwia przedsiębiorcom cyfrowym korzystanie z potencjału potencjalnych pracowników i partnerstw na całym świecie bez zmuszania do relokacji. Globalne wirtualne zespoły mogą przynieść znaczne korzyści przedsiębiorcy cyfrowemu, ułatwiając lokalizację i zatrudnianie talentów, wykorzystywanie różnorodności kulturowej, poprawę wykorzystania zasobów oraz zwiększenie elastyczności i szybkości reagowania.

Oprogramowanie open source - oprogramowanie komputerowe z kodem źródłowym, który można zobaczyć, modyfikować i rozpowszechniać bezpłatnie. Oprogramowanie open source jest ogólnie uważane za bezpieczniejszą alternatywę niż oprogramowanie własne, ponieważ programiści mogą przetestować go w celu wykrycia wszelkich backdoorów.

Ransomware to rodzaj złośliwego oprogramowania pochodzącego z wirusów kryptograficznych, który może publikować dane ofiary lub blokować dostęp do niej, chyba że zostanie opłacony okup.

Spyware - oprogramowanie zbierające informacje o komputerze i sposobie korzystania z niego, a następnie przekazujące te informacje komuś innemu za pośrednictwem Internetu. Oprogramowanie szpiegujące zwykle działa w tle i często instaluje się na komputerze bez wiedzy i pozwolenia.

Wirus - program lub kod, który jest replikowany na inne pliki, z którymi ma styczność. Większość wirusów replikuje się, chociaż wiele z nich może uszkodzić system komputerowy lub dane użytkownika.

G. Wnioski i dodatkowe źródła wiedzy

Przedsiębiorstwa społeczne muszą dostosowywać się do wymagań stale zmieniającej się gospodarki cyfrowej, aby pozostać na rynku i dalej działać. Zmieniające się środowisko cyfrowe i postęp technologiczny stają się istotnym aspektem przedsiębiorstw, a źródła i zasoby muszą być przydzielane szybciej niż inne aspekty biznesowe. Niektóre firmy społeczne dokonały tych postępów i dokonały transformacji przy niewielkim nakładzie lub bez inwestycji czy wysiłków, podczas gdy inne firmy potrzebują dodatkowej pomocy. Środowisko cyfrowe zmusza firmy społeczne do ponownej oceny strategii biznesowych i modyfikowania ich środowiska cyfrowego, w którym obecnie się znajdują. Obejmuje to również ocenę wszystkich procesów biznesowych, które zostały ustanowione przed transformacją. Ponowne przemyślenie i zdefiniowanie nowych strategii może spowodować, że niektóre firmy również przejdą zmiany w strukturach kadry organizacyjnej. Mobilność i elastyczność są kluczowe, aby pracownicy mogli pozostać ważni w gospodarce cyfrowej. Aby utrzymać transformację cyfrową, przedsiębiorstwa muszą stosować nowe technologie, nowe procesy biznesowe i zwracać szczególną uwagę na systemy wspomagające i bezpieczeństwo. Niemniej jednak przedsiębiorstwa nie mogą zmieniać, modyfikować ani dostosowywać tylko systemów i procesów sprzętowych bez zmiany ludzi. Jeśli zmienia się miejsce pracy, pracownicy również muszą.

Dodatkowe źródła wiedzy na ten temat:

Digital business strategy: toward a next generation of insights

MIS Quarterly

From social enterprise to social innovation

5th Italian Business Forum 2017

Cybersecurity - threats, challenge, opportunities

ACS

Digital security: a Financial Services perspective

Ernst & Young

Growing a Digital Social Innovation Ecosystem for Europe

NESTA

Social enterprises

KOMISJA EUROPEJSKA

The impact of the digital world on management and marketing

KOZMINSKI UNIVERSITY

New technologies and digitalisation: opportunities and challenges for social economy and social enterprise

EECS

Boosting Social Enterprise Development: Good Practice Compendium

OECD

H. Źródła:

[1] OECD, 2016 Ministerial meeting: Managing Digital Security and Privacy Risk for Economic and Social Prosperity, https://www.oecd.org/internet/ministerial/meeting/Managing-Digital-Security-and-Privacy-Risk-discussion-paper.pdf

[2] Growing a Digital Social Innovation Ecosystem for Europe (2015), European Union, https://www.nesta.org.uk/sites/default/files/dsireport.pdf

[3] Durieux, Mark & Stebbins, Robert (2010): Social Entrepreneurship for Dummies, Wiley Publishing, Inc., Hoboken, *http://socialnaekonomija.si/wp-content/uploads/2015/03/Social-Entrepreneurship-For-Dummies-Mark-Durieux.pdf*

[4] British Council (2015): Social Enterprise in the UK – Developing a thriving social enterprise sector, https://www.britishcouncil.org/sites/default/files/social_enterprise_in_the_uk_final_web_spreads.pdf

[5] Rupa Rathee (2017): ENTREPRENEURSHIP IN THE DIGITAL ERA, Asia Pacific Journal of Research in Business Management, Vol. 8, Issue 6, June 2017 Impact Factor: 5.16, ISSN: (2229-4104), https://www.academia.edu/33640590/ENTREPRENEURSHIP_IN_THE_DIGITAL_ERA?auto=download

[6] Socialnopodjetništvo za začetnike, Ljubljana: ŠOU

[7] Rossi, Ben (2016): How companies must adapt to the digital revolution, http://www.information-age.com/how-companies-must-adapt-digital-revolution-123461760/

[8] Harward Business Review, Is Your Company Adapting Fast Enough to Thrive in an Increasingly Digital World?, October 2017, https://hbr.org/sponsored/2017/10/is-your-company-adapting-fast-enough-to-thrive-in-an-increasingly-digital-world

[9] New technologies and digitalisation: opportunities and challenges for Social Economy and Social Enterprise, https://www.eesc.europa.eu/en/agenda/our-events/events/new-technologies-and-digitalisation-opportunities-and-challenges-social-economy-and-social-enterprise

[10] Violo, Marc (2017): Digital Tool Box for Social Enterprises & Charities, https://medium.com/on-purpose-stories/digital-tool-box-for-social-enterprises-charities-b4bc3f4c4184

[11] Prodanov, Hristo (2018): Social Enterpreneurship And Digital Technologies, Economic Alternatives, 2018, Issue 1, pp. 123-138, https://www.unwe.bg/uploads/Alternatives/9_Prodanov_EAlternativi_en_1_2018.pdf

CZĘŚĆ III

KWESTIE PRAWNE DOTYCZĄCE CYBERBEZPIECZEŃSTWA

Spis zastosowanych skrótów

Skrót	Rozwinięcie
UE	Unia Europejska
RODO	Ogólne rozporządzenie o ochronie danych 2016/679 (ang. General Data Protection Regulation 2016/679)
CRD	Dyrektywa w sprawie praw konsumenckich 2018/83 (ang. Consumers Right Directive 2018/83)
EPD	Dyrektywa o prywatności i łączności elektronicznej (ang. e-Privacy Directive)
HTTP	Protokół przesyłania dokumentów hipertekstowych (ang. Hypertext Transfer Protocol)

A. Wstęp

Stworzenie prawdziwego, właściwie działającego jednolitego rynku cyfrowego z odporną europejską gospodarką opartą na danych jest jednym z głównych priorytetów Unii Europejskiej. Oznacza to, że zasadniczo powinien istnieć skuteczny transgraniczny swobodny przepływ danych. Europejskie przedsiębiorstwa coraz częściej dostrzegają rozwój technologii cyfrowej i zaczynają włączać cyfrowe modele biznesowe, aby w pełni korzystać z analityki danych, jak i samych danych.

Właściwe funkcjonowanie sieci i systemów informatycznych w całej UE jest niezbędne do utrzymania gospodarki internetowej i zapewnienia dobrobytu. W tym celu UE działa na wielu frontach, aby promować odporność cybernetyczną.

Ale te nowe modele biznesowe nie są powszechne. Aby naprawdę z nich skorzystać, należy wziąć pod uwagę reżim regulacyjny aplikacji. W bieżącej części zapoznasz się z europejskimi ramami prawnymi związanymi z bezpieczeństwem cyfrowym. Pierwsze strony tej części poświęcone są najnowszym zmianom w prawodawstwie UE, które spowodowały zawirowania w społeczeństwie europejskim - a mianowicie ogólne rozporządzenie o ochronie danych (RODO). Po dokładnej analizie rozporządzenia następuje przegląd dyrektywy w sprawie praw konsumentów (CRD), dyrektywy o handlu elektronicznym oraz dyrektywy o prywatności i łączności elektronicznej (EPD).

B. Wytyczne w zakresie ochrony danych

Od 25 maja 2018 r. Obowiązują nowe wymagania prawne dla firm przetwarzających dane osobowe.

Być może słyszałeś o ogólnym rozporządzeniu o ochronie danych 2016/679, znanym również jako RODO. Jest to rozporządzenie UE, które ma zastosowanie do każdej firmy prowadzącej działalność gospodarczą z klientami w UE, oferującym towary lub usługi na terytorium UE oraz zajmującymi się danymi związanymi z obywatelami UE, w tym z jej pracownikami. Głównym celem RODO jest ochrona danych osobowych mieszkańców UE poprzez rygorystyczne wymogi mające wpływ na cały cykl życia danych w większości organizacji. Ponieważ to najważniejszy zbiór zasad i przepisów regulujących wykorzystanie danych osobowych w UE, RODO ma ogromne znaczenie dla większości przedsiębiorstw w regionie.

Jak ważne dla przedsiębiorstwa jest GDPR, można dostrzec na podstawie grzywien, za nieprzestrzeganie prawa. W przypadku nieprzestrzegania przepisów organizacje, nawet jeśli nie mają siedziby w UE, mogą otrzymać grzywnę w wysokości do 20 milionów EUR lub 4% łącznych przychodów globalnych za poprzedni rok podatkowy - w zależności od tego, która z tych wartości jest wyższa. Oznacza to, że jeśli firma ma klientów lub pracowników w UE, wymogi RODO muszą być traktowane poważnie.

Oznacza to, że jeśli firma ma klientów lub pracowników w UE, wymogi RODO muszą być traktowane poważnie.

Ryc. 1: Obszary, w których należy dążyć do osiągnięcia zgodności z RODO

Dane osobowe

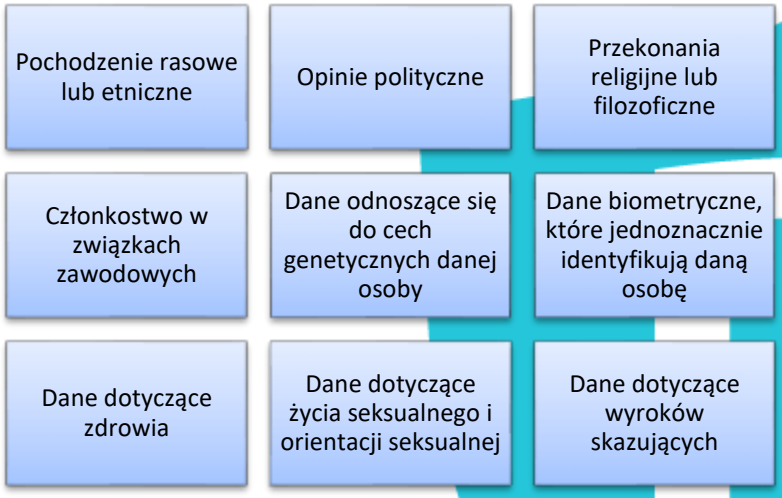
Przede wszystkim, aby osiągnąć zgodność z RODO, niezwykle ważne jest zrozumienie, do której informacji - lub danych - odnosi się i chroni RODO, a mianowicie, jakie są dane osobowe.

Po pierwsze: dane osobowe nie są danymi odnoszącymi się do osoby prawnej i nie są danymi osoby zmarłej.

Dane osobowe oznaczają wszelkie informacje dotyczące podmiotu danych, którym jest:

- zidentyfikowana osoba fizyczna - osoba, którą można odróżnić od innych członków określonej grupy, na przykład według nazwiska lub zdjęcia;
- dająca się zidentyfikować osoba fizyczna - osoba, która może być bezpośrednio lub pośrednio zidentyfikowana, na przykład na podstawie informacji umożliwiających identyfikację osoby za pomocą rozsądnych dostępnych środków, takich jak jej głos lub adres IP.

specjalne kategorie danych osobowych, często nazywane "danymi wrażliwymi", obejmują ujawnianie danych osobowych:



Ryc. 2: Specjalne kategorie danych osobowych

Zasadniczo zabrania się przetwarzania tych szczególnych kategorii danych, chyba że osoba, której dotyczą dane, wyraża swoją wyraźną zgodę, lub przetwarzanie dotyczy danych osobowych, które zostały w sposób jawny upublicznione przez osobę, której dane dotyczą, lub wymagane przez prawo do przetwarzania takich

danych osobistych Dotyczy to, w większości przypadków, dokumentacji medycznej osób.

Pod względem zatrudnienia istnieją pewne wyjątki, ponieważ pracodawcy mają prawo (jeśli to konieczne) do przetwarzania wrażliwych danych pracowników. Jednak jako pracodawca powinieneś upewnić się, że nie przechowujesz wrażliwych informacji, które pozwalają na identyfikację pracowników, dłużej niż jest to uzasadnione, i nie powinieneś opierać żadnej decyzji wyłącznie na automatycznych procesach i ocenach (w tym profilowaniu).

Ważną podkategorią danych osobowych są dane pseudonimizowane, które nie mogą być przypisane do konkretnego podmiotu danych bez wykorzystania dodatkowych informacji, o ile takie dodatkowe informacje są zabezpieczane i przechowywane oddzielnie. Innymi słowy, chodzi tu o dane osobowe, które są związane z możliwą do zidentyfikowania osobą fizyczną za pomocą rozsądnych środków (co określają koszty i czas potrzebny na identyfikację, a także dostępna technologia w momencie przetwarzania). Pseudonimizacja jest sposobem na ograniczenie ryzyka związanego z przetwarzaniem danych osobowych.

Z drugiej strony, anonimowe informacje to te, które nie mogą w jakikolwiek sposób zidentyfikować osoby, której dotyczą dane, a jej przetwarzanie nie jest regulowane przez RODO. Ważna uwaga: dane mogą być uważane za anonimowe, jeśli ponowna identyfikacja jest praktycznie niemożliwa, co oznacza, że ponowne zidentyfikowanie danej osoby jest niemożliwe przez którąkolwiek ze stron i przy wykorzystaniu wszelkich dostępnych środków.

Więcej praktycznych informacji na temat pseudonimizacji i anonimizacji danych można znaleźć w częściach IV i V niniejszego e-Poradnika.

Przetwarzanie

Aby zachować zgodność z RODO, powinieneś wiedzieć, co to jest przetwarzanie danych osobowych. Zgodnie z rozporządzeniem przetwarzanie to każda operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych, niezależnie od tego, czy odbywa się to w sposób zautomatyzowany, takie jak **zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptacja lub zmiana, wyszukiwanie, konsultowanie,**

wykorzystanie, ujawnienie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie.

Odnosi się to do wszystkich całkowicie lub częściowo zautomatyzowanych systemów, a nawet do całkowicie niezautomatyzowanych środków, które stanowią część zbioru danych lub mają stanowić część zbioru danych. Definicja „zbioru danych" jest podana w ramach RODO i oznacza każdy uporządkowany zestaw danych osobowych, które są dostępne zgodnie z określonymi kryteriami, czy to scentralizowane, zdecentralizowane czy rozproszone funkcjonalnie lub geograficznie. Przykładem takiego systemu może być nawet wizytówka, którą otrzymujesz od partnerów biznesowych: zbieranie ich przez właściciela karty tworzy system archiwizacji.

Należy również wyjaśnić, że przetwarzanie danych osobowych przez osobę fizyczną w ramach działalności o charakterze wyłącznie osobistym lub domowym, a zatem bez związku z działalnością zawodową lub handlową, nie jest objęte RODO. Na przykład, nawet przesyłane na Facebooku dane są traktowane jako przetwarzanie danych osobowych, jednak ponieważ jest to wyłącznie do użytku osobistego i bez celu komercyjnego, nie jest kontrolowane przez RODO. Jednak, gdy komunikujesz się z ludźmi w mediach społecznościowych, ale w celach komercyjnych (np. sprzedając produkty na Instagramie), obowiązuje cię RODO.

	TAK	**NIE**
Czy dane dotyczą osoby fizycznej?	RODO obowiązuje ✓	RODO nie obowiązuje ✗
Czy te dane w jakiś sposób identyfikują osobę fizyczną?	RODO obowiązuje ✓	RODO nie obowiązuje ✗
Czy mogę oddzielić lub przesegregować te identyfikowalne	RODO nie obowiązuje ✗	RODO obowiązuje ✓

dane od tego, co zostało?		
Czy planuję w jakiś sposób zarabiać na tych danych?	RODO obowiązuje ✓	RODO nie obowiązuje ✗ (w celach osobistych lub domowych)

Ryc. 3: Podsumowanie zastosowania RODO

Podstawowe zasady przetwarzania danych osobowych

Zgodnie z RODO wszelkie przetwarzanie danych osobowych, objętych niniejszym rozporządzeniem, musi być zgodne z następującymi zasadami:

Legalność	- **Przetwarzaj dane osobowe na podstawie art. 6 RODO;**
Uczciwość **Transparentność**	- **Poinformuj podmiot, którego dotyczą dane o zaistnieniu i charakterze przetwarzania;** - **Udostępnij informacje na temat przetwarzania danych osobowych w łatwy i zrozumiały sposób (w tym informacje o tożsamości administratora danych i celach przetwarzania oraz o zagrożeniach, zasadach, zabezpieczeniach, prawach związanych z przetwarzaniem);** - **Poinformuj podmiot, którego dane dotyczą o zaistnieniu profilowania i jego konsekwencjach;** - **Poinformuj podmiot, którego dane dotyczą, czy jest on zobowiązany do podania danych osobowych i jakie są tego konsekwencje.**
Określone **Doprecyzowane cele** **Prawnie uzasadnione**	- Jeżeli dane osobowe są przetwarzane na podstawie zgodnego z prawem celu, należy w określony i wyraźny sposób określić, jaki jest to uzasadniony cel w momencie gromadzenia danych; - Nie przetwarzaj dalej udostępnionych ci danych, gdy są niezgodne z tymi celami; - Gdy kontroler zamierza przetwarzać dane osobowe do celów innych niż te, dla których zostały zgromadzone, administrator

	powinien przekazać osobie, której dane dotyczą (przed dalszym przetwarzaniem) informacje o tym, jaki jest ten inny cel i inne niezbędne informacje; - To nowe przetwarzanie powinno również odbywać się według powyższych zasad.
Minimalizacja danych **Ograniczone przechowywanie**	- Zebrane dane osobowe muszą być adekwatne, istotne i ograniczone do tego, co jest ściśle niezbędne w związku z celami przetwarzania; - Dane osobowe należy przechowywać w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy niż jest to konieczne do celów, dla których przetwarzane są dane osobowe (zwolnione jest przechowywanie informacji do celów archiwizacji w interesie publicznym, badania naukowe lub historyczne lub celów statystycznych, uzupełnionych o konkretne środki ochrony praw i wolności osób, których dane dotyczą).
Dokładność	- Dane osobowe muszą być dokładne i w razie konieczności, aktualizowane; - Przy użyciu rozsądnych środków, upewnij się, że wszystkie dane osobowe są dokładne, a jeśli nie, popraw w odpowiednim czasie wszystkie nieścisłości.
Integralność **Poufność**	- Zapewnij odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed nieautoryzowanym lub niezgodnym z prawem przetwarzaniem oraz przed przypadkową utratą, zniszczeniem lub uszkodzeniem; - Upewnij się, że przetwarzane dane osobowe są chronione przed potencjalnym wyciekiem, jak również, że nie zostaną utracone, zniszczone lub uszkodzone; - W przypadku jakiegokolwiek incydentu to administrator ponosi odpowiedzialność za powstałe szkody i może zostać pociągnięty do wypłaty odszkodowania, jeżeli nie jest w stanie udowodnić, że nie jest w żaden sposób odpowiedzialny za powstałą szkodę

	oraz że przedsięwziął wszelkie odpowiednie środki techniczne i organizacyjne mające na celu ochronę baz danych; - Aby zapewnić odpowiedni poziom bezpieczeństwa, upewnij się, że: o pseudonimizujesz i szyfrujesz dane osobowe; o zapewniasz ciągłą poufność, integralność, dostępność i odporność systemów przetwarzania i usług; o zapewniasz możliwość przywrócenia dostępności i dostępu do danych w odpowiednim czasie w razie jakiegokolwiek incydentu; o regularnie testujesz i poddajesz ewaluacji skuteczność technicznych i organizacyjnych środków bezpieczeństwa.
Powiadomienie organu nadzoru	- Naruszenie danych osobowych stanowi naruszenie bezpieczeństwa, które prowadzi do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmiany, nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych lub przetwarzanych w inny sposób. Naruszenie może zaistnieć pojedynczo lub w kombinacji poszczególnych wariantów: o „Naruszenie poufności" - nieuprawnione lub przypadkowe ujawnienie lub dostęp do danych osobowych; o „Naruszenie dostępności" - przypadkowa lub nieautoryzowana utrata dostępu do danych osobowych lub ich zniszczenie; o „Naruszenie integralności” - nieautoryzowana lub przypadkowa zmiana danych osobowych; - Powiadomienie o naruszeniu ochrony danych do właściwego organu nadzorczego (organu ochrony danych) powinno zostać sporządzone nie później niż w ciągu 72 godzin od powzięcia informacji na ten temat; - Konieczne jest dostarczenie organowi ochrony danych informacji na temat: charakteru naruszenia; kategorii

	i przybliżonej liczby osób i danych, których dotyczą dane; imienia i nazwiska oraz danych kontaktowych inspektora ochrony danych; prawdopodobnych konsekwencji naruszenia; proponowanych środków zaradczych. W przypadku opóźnienia w zgłoszeniu, musi być ono uzasadnione; - Naruszenia, które prawdopodobnie nie spowodują ryzyka dla osób, których dane dotyczą, nie wymagają zgłaszania organowi nadzorującemu (na przykład publicznie dostępnych danych osobowych, lub mieszanych i losowych danych, które wciąż mają nienaruszony klucz).
Komunikacja z osobą, której dane dotyczą	- W przypadku dużej szansy na negatywne skutki wynikające z naruszenia danych, dane dotyczące naruszenia powinny być przekazywane zainteresowanym osobom tak szybko, jak to jest racjonalnie wykonalne; - Należy podać konkretne informacje o prawdopodobnych konsekwencjach i krokach, jakie należy podjąć, aby się chronić, a także opis charakteru naruszenia, nazwiska i danych kontaktowych inspektora ochrony danych lub innej osoby do kontaktu; - Spraw aby komunikacja była transparentna i wolna od innych informacji, takich jak regularne aktualizacje, newslettery itp.; - Korzystaj z więcej niż jednego kanału komunikacji (SMS, e-mail, banery na stronie internetowej, ważne reklamy itp.), aby skutecznie dotrzeć do osób, których potencjalnie dotyczą skutki wynikające z naruszenia danych; - Powiadomienie nie jest wymagane, jeśli wszystkie trzy poniższe warunki są spełnione: o Jeśli dane są nieczytelne dla osób nieuprawnionych do uzyskania dostępu (na przykład, jeśli są bezpiecznie zaszyfrowane); o Natychmiast po naruszeniu podejmowane są niezbędne kroki w celu zapewnienia, że ryzyko prawdopodobnie nie

	wystąpi; ○ Wymagałoby to niewspółmiernego wysiłku, aby skontaktować się z osobami (jeśli ich kontakty zostały utracone lub nie były wcześniej znane).
Ryzyko i Wysokie ryzyko	- Po wystąpieniu naruszenia ważne jest, aby ocenić ryzyko, które może z tego wyniknąć, a więc prawdopodobieństwo i dotkliwość wpływu na osoby, a także to czy wymagane jest ich powiadomienie; - Ryzyko ma miejsce, gdy naruszenie może prowadzić do fizycznych, materialnych lub niematerialnych szkód dla osób, których dane zostały naruszone; - Kryteria, które należy wziąć pod uwagę: ○ Rodzaj naruszenia; ○ Charakter, wrażliwość i ilość danych osobowych; ○ Łatwość identyfikacji osób; ○ Dotkliwość konsekwencji dla osób; ○ Szczególne cechy osoby; ○ Liczba dotkniętych osób; ○ Szczególne cechy kontrolera danych.
Odpowiedzialność Ewidencjonowanie	- Bez względu na potrzebę powiadomienia, administrator musi prowadzić dokumentację wszystkich naruszeń; - Zaleca się ustanowienie wewnętrznego rejestru naruszeń, który obejmuje przyczyny, opis, skutki, podjęte działania zaradcze; - Zaleca się wprowadzenie i utrzymanie procedury, która obejmuje sposób ograniczania i zarządzania incydentami oraz odzyskiwania danych po ich zaistnieniu, oceny ryzyka i wymaganych powiadomień oraz informowania pracowników o procedurze.

Ryc. 4: Podstawowe zasady przetwarzania danych osobowych

C. Wytyczne ochrony konsumentów

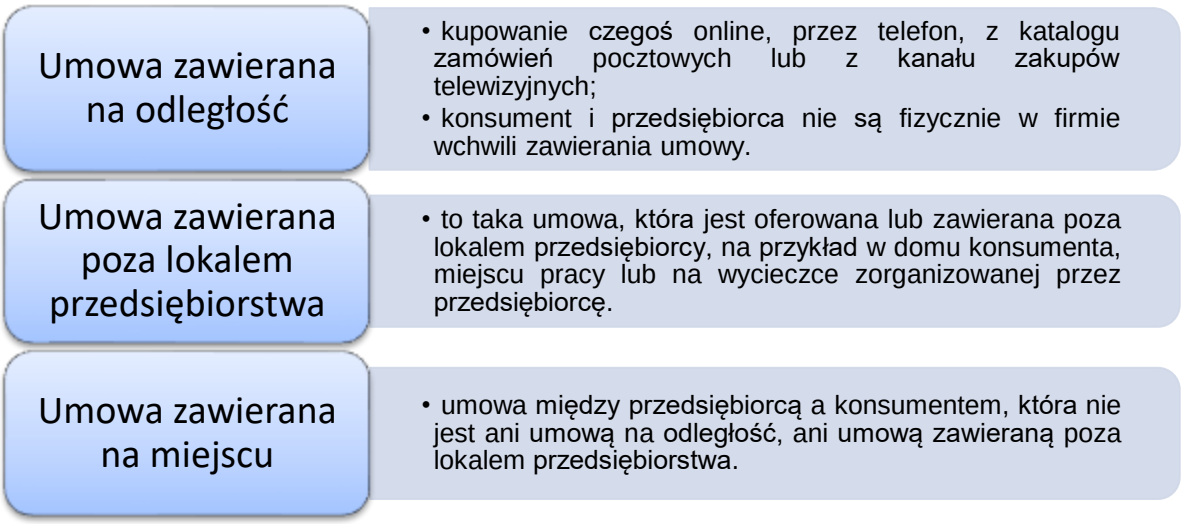
Podobnie jak w przypadku ochrony danych zgodnie z RODO, ochrona konsumentów jest regulowana dyrektywą UE 2011/83/UE Parlamentu Europejskiego i Rady z dnia 25 października 2011 r. w sprawie praw konsumentów (znaną również jako dyrektywa o prawach konsumenta). Zastępuje ona dwie poprzednie dyrektywy - jedną (dyrektywa Rady 85/577/EWG) w sprawie ochrony konsumenta w przypadku umów wynegocjowanych poza lokalem przedsiębiorstwa, a drugą (dyrektywę 97/7/WE Parlamentu Europejskiego i Rady) w sprawie ochrony konsumentów w odniesieniu do umów zawieranych na odległość.

Celem dyrektywy jest osiągnięcie wysokiego poziomu ochrony konsumentów w całej UE i przyczynienie się do właściwego funkcjonowania rynku wewnętrznego. Dyrektywa ma zastosowanie do każdej umowy zawartej między przedsiębiorcą a konsumentem.

Państwa członkowskie były zobowiązane do wdrożenia jej w swoim prawie krajowym do dnia 13 grudnia 2013 r., zaś wszystkie krajowe środki transpozycji ustanowiono od dnia 13 czerwca 2014 roku.

Dyrektywa jest wdrażana z maksymalną harmonizacją, zwaną również „pełną harmonizacją", co oznacza, że państwa członkowskie nie mogą przyjąć bardziej restrykcyjnych przepisów w tym obszarze - przepisy dyrektywy przewidują maksymalne zastosowanie. Dyrektywa ustanawia pewne kluczowe prawa konsumenckie i określa zasady dotyczące umów między konsumentami a przedsiębiorstwami, które mają bezpośredni wpływ na codzienne życie konsumentów w całej UE.

Rodzaje umów wyodrębnionych na mocy dyrektywy to trzy: umowy zawierane poza lokalem przedsiębiorstwa, umowy zawierane na odległość i umowy zawierane na miejscu.



Ryc. 5: Różne rodzaje umów zgodnie z dyrektywą 2011/83/UE

W dyrektywie dokonano dodatkowo kategoryzacji umów na cztery kategorie: umowy sprzedaży, umowy o świadczenie usług, umowy na treści cyfrowe online oraz umowy na dostawy usług użyteczności publicznej. Klasyfikacja umowy jako "sprzedaży" lub "umowy o świadczenie usług" określa sposób obliczania okresu karencji (art. 9). Okres karencji definiowany jest jako okres, w którym klient może wypowiedzieć umowę bez podania przyczyny i bez ponoszenia dodatkowych kosztów. W przypadku umów o świadczenie usług, treści cyfrowych i umów o świadczenie usług użyteczności publicznej, 14-dniowy okres odstąpienia rozpoczyna bieg od momentu zawarcia umowy. W przypadku umów sprzedaży okres wypłaty rozpoczyna się dopiero po otrzymaniu towarów.

Zgodnie z dyrektywą, w szczególności w odniesieniu do towarów cyfrowych każdy, kto kupuje treści cyfrowe, musi być w stanie uzyskać jasne i jednoznaczne informacje, w tym szczegóły dotyczące oprogramowania i sprzętu oraz treści, z którą pracuje, a także informacje o prawie autorskim. Konsumenci muszą mieć możliwość wycofania zakupów treści cyfrowych do momentu, w którym rozpoczyna się pobieranie lub przesyłanie strumieniowe treści.

Dyrektywa wyłącza niektóre kategorie umów z zakresu jej stosowania, w tym:

Ryc. 6: Kategorie działań wyłączone z dyrektywy o prawach konsumenta

Dyrektywa w sprawie praw konsumentów w pigułce

Celem dyrektywy jest osiągnięcie wysokiego poziomu ochrony konsumentów w całej UE i przyczynienie się do właściwego funkcjonowania rynku wewnętrznego poprzez zbliżanie niektórych aspektów przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących umów zawieranych między konsumentami a przedsiębiorcami.

To, co dyrektywa oznacza dla firm i konsumentów, podsumowano w poniższej tabeli:

Korzyści dla konsumentów	– **Informacje, które konsumenci muszą uzyskać przed dokonaniem zakupu, a prawo konsumentów do anulowania zakupów online jest teraz takie samo we wszystkich krajach UE;** – **Konsumenci mogą polegać na tych samych prawach, niezależnie od tego, gdzie dokonują zakupów w UE;** – **Większe prawa konsumenckie i wyższy poziom ochrony niezależnie od miejsca i sposobu dokonywania zakupów;** – **Pełne informacje na temat całkowitego kosztu**

	produktu lub usługi, w tym wszelkich dodatkowych opłat (np. kosztów dostawy).
Nowe zasady dla firmy	– Żadnych pułapek odnośnie kosztów w Internecie: kupujący online muszą potwierdzić, że akceptują płacenie za coś, zanim zostaną obciążeni (cena powinna być jasno wskazana). Klienci nie muszą płacić za żadne opłaty, o których nie zostali jasno poinformowani przed dokonaniem zakupu; – Brak wcześniej zaznaczonych pól: dyrektywa wprowadza wyraźny zakaz dotyczący wstępnie zaznaczonych pól na stronach internetowych, które wiążą się z pobieraniem dodatkowych płatności; – Sprzedawcy nie mogą pobierać więcej opłat za płatności kartą kredytową, niż ich to kosztuje w przypadku takiej opcji płatności; – Stawki za numery interwencyjne reklamacji lub pytań klientów nie powinny być wyższe niż stawki bazowe za takie połączenia.
	Reguły zwrotów: – Okres, w którym konsumenci mogą wycofać się z zakupu na odległość (np. przez Internet) lub zakupu poza lokalem przedsiębiorstwa (gdy sprzedawca odwiedzi dom konsumenta) zostanie przedłużony z poprzednich siedmiu dni do jednolitego w całej UE okresu 14 dni; – Te 14 dni zaczynają się licząc od dnia, w którym konsument otrzyma towar. W ciągu tego okresu konsument ma prawo do anulowania zakupu z dowolnego powodu. Jeżeli sprzedawca nie poinformował konsumenta w sposób wyraźny o prawie do anulowania zakupów, okres zwrotu zostaje przedłużony do jednego roku;

	– Sprzedawcy muszą zwrócić koszty zakupu konsumentom w ciągu 14 dni od dnia anulowania, wliczając w to standardowe koszty dostawy. Jeżeli chodzi o towary, przedsiębiorca może odroczyć zwrot do czasu, aż towary zostaną zwrócone przez konsumenta lub konsument przedstawi dowody, że towary te zostały wysłane do przedsiębiorcy. Nie dotyczy to produktów wykonanych na zamówienie lub produktów łatwo psujących się (takich jak produkty mleczne); – Konsumenci otrzymują standardowy unijny formularz do wykorzystania, jeśli chcą anulować zakupy, mimo że nie są zobowiązani do korzystania z niego. Jeżeli przedsiębiorcy chcą, aby konsument zapłacił za przesyłkę towarów po anulowaniu zakupu, muszą wyraźnie poinformować ich o tym przed wysłaniem towarów, podając konkretną lub szacunkową kwotę związaną ze zwrotem.
Ważne konsekwencje dla firm	– Wspólne reguły dla przedsiębiorstw ułatwiają wymianę handlową w całej Europie; – Firmy dokonujące sprzedaży telefonicznie, pocztą lub online lub poza lokalem mają jeden zestaw zasad, które mają stosować. Zapewnia to równe szanse i zmniejsza transgraniczne koszty transakcji; – W odniesieniu do małych przedsiębiorstw i rzemieślników nie ma prawa do zawierania umów na pilne naprawy i prace konserwacyjne. Państwa członkowskie mogą również zwolnić przedsiębiorców wykonujących naprawy lub prace konserwacyjne w domach klientów za mniej niż 200 euro z pewnych wymogów informacyjnych

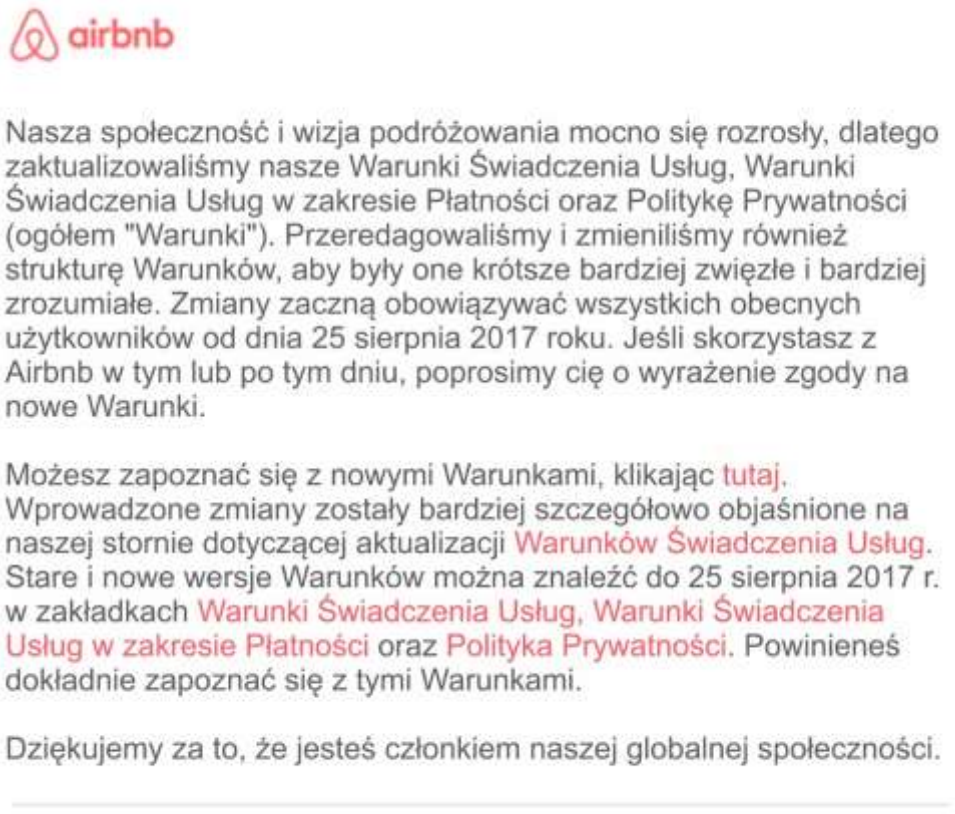
Ryc. 7: Konsekwencje wynikające z dyrektywy o prawach konsumenta

Firmy a zgodność z dyrektywą

Aby być w zgodzie ze wszystkimi aspektami dyrektywy, oto kilka przydatnych wskazówek, które również zostaną podsumowane w pełnej liście kontrolnej sprawdzającej zgodność z prawem na końcu tej części e-Poradnika.

1) Upewnij się, że twoja strona internetowa zawiera regulamin, który informuje klientów o wszystkich istotnych prawach i obowiązkach. Niektóre z tych informacji należy również uwzględnić w polityce zamówień lub na stronach, z których klienci korzystają przy zamawianiu produktów lub usług. Dołącz informacje o zwrotach towarów, anulowaniach zakupów, zwrotach kosztów, itp.

2) Po wprowadzeniu zmian w regulaminie korzystania z usługi postaraj się poinformować o tym swoich klientów. Na przykład, po tym jak Airbnb.com zmieniło swój regulamin w czerwcu 2017 r., użytkownicy otrzymali ten e-mail:



airbnb

Nasza społeczność i wizja podróżowania mocno się rozrosły, dlatego zaktualizowaliśmy nasze Warunki Świadczenia Usług, Warunki Świadczenia Usług w zakresie Płatności oraz Politykę Prywatności (ogółem "Warunki"). Przeredagowaliśmy i zmieniliśmy również strukturę Warunków, aby były one krótsze bardziej zwięzłe i bardziej zrozumiałe. Zmiany zaczną obowiązywać wszystkich obecnych użytkowników od dnia 25 sierpnia 2017 roku. Jeśli skorzystasz z Airbnb w tym lub po tym dniu, poprosimy cię o wyrażenie zgody na nowe Warunki.

Możesz zapoznać się z nowymi Warunkami, klikając tutaj. Wprowadzone zmiany zostały bardziej szczegółowo objaśnione na naszej stronie dotyczącej aktualizacji Warunków Świadczenia Usług. Stare i nowe wersje Warunków można znaleźć do 25 sierpnia 2017 r. w zakładkach Warunki Świadczenia Usług, Warunki Świadczenia Usług w zakresie Płatności oraz Polityka Prywatności. Powinieneś dokładnie zapoznać się z tymi Warunkami.

Dziękujemy za to, że jesteś członkiem naszej globalnej społeczności.

3) Stwórz sposób, w którym twoi klienci wykazaliby, że rozumieją swoje prawa i obowiązki - co zwykle dzieje się przy polu, które należy zaznaczyć przed rejestracją lub przed sfinalizowaniem zamówienia.
4) W związku z poprzednim punktem, pamiętaj, że wstępne zaznaczanie pola jest całkowicie zabronione.
5) Upewnij się, że klienci mogą się z tobą skontaktować bez ponoszenia dodatkowych opłat (linie o podwyższonej opłacie itp.).
6) Zapewnij swoim klientom łatwo dostępny formularz anulowania rezerwacji.

D. Wytyczne dotyczące e-handlu

W zakresie, w jakim ochrona danych jest regulowana przez RODO, a ochrona konsumentów jest regulowana przez dyrektywę UE 2011/83/UE, handel elektroniczny (e-handel) jest regulowany dyrektywą 2000/31/EO Parlamentu Europejskiego Rady z 8 czerwca 2000 r., znaną również jako dyrektywa o handlu elektronicznym.

Państwa członkowskie musiały dokonać transpozycji do swoich przepisów krajowych do 17 stycznia 2002 roku. Celem dyrektywy jest stworzenie ram prawnych zapewniających swobodny przepływ usług społeczeństwa informacyjnego między państwami członkowskimi. Dyrektywa ustanawia standardowe zasady w UE dotyczące różnych kwestii związanych z handlem elektronicznym. Niniejsza dyrektywa jest zbliżona do niektórych przepisów krajowych dotyczących usług społeczeństwa informacyjnego odnoszących się do rynku wewnętrznego, ustanawiania usługodawców, informacji handlowych, umów elektronicznych, odpowiedzialności pośredników, kodeksów postępowania, pozasądowych sposobów rozstrzygania sporów, działań sądowych i współpracy między sądami w państwach członkowskich UE.

	Czego tyczy się dyrektywa?
Serwisów informacyjnych (takie jak strony z wiadomościami)	✓
Sprzedaży (książki, usługi finansowe, usługi turystyczne itp.)	✓
Podatków	✗
Reklamy	✓

Usług profesjonalnych (prawnicy, lekarze, pośrednicy w obrocie nieruchomościami)	✓
Gier hazardowych polegających na obstawianiu stawki w grach losowych, w tym w loteriach i transakcjach bukmacherskich.	✗
Działalność notariuszy lub równoważnych zawodów do w zakresie, w jakim dotyczą one bezpośredniego i konkretnego związku z wykonywaniem władzy publicznej,	✗
Usług rozrywkowych	✓
Pytań dotyczących usług społeczeństwa informacyjnego	✗
Podstawowych usług pośrednictwa (dostęp do Internetu, transmisja i hosting informacji)	✓
Bezpłatnych usług finansowanych przez reklamę, sponsoring itp.	✓
Pytań dotyczących porozumień lub praktyk regulowanych przez prawo kartelowe	✗

Ryc. 8: Zastosowanie dyrektywy o handlu elektronicznym

Odpowiedzialność pośredników

Dyrektywa o handlu elektronicznym zawiera kilka przepisów dotyczących odpowiedzialności pośredników. Ustanawia zharmonizowane zasady dotyczące takich kwestii, jak wymogi dotyczące przejrzystości i informacji dotyczące dostawców

usług internetowych, informacji handlowych, umów elektronicznych i ograniczeń odpowiedzialności usługodawców będących pośrednikami.

„Zwykły przekaz”

Usługodawcy, których rola polega wyłącznie na przekazywaniu informacji pochodzących od stron trzecich i zapewnieniu dostępu za pośrednictwem sieci komunikacyjnej, nie mogą zostać pociągnięci do odpowiedzialności za nielegalne treści przekazywane przez strony trzecie, jeżeli:

- Nie inicjują transmisji;
- Nie selekcjonują odbiorcy transmisji ;oraz
- Nie selekcjonują lub nie modyfikują transmitowanych treści.

Automatyczne, pośrednie i przejściowe przechowywanie informacji, które ma miejsce podczas przekazywania informacji w celu przetworzenia transmisji, objęte są zwolnieniem z odpowiedzialności.

„Buforowanie"

Usługodawcy nie mogą być pociągani do odpowiedzialności za nielegalne treści należące do stron trzecich podczas zapewniania możliwości buforowania pod warunkiem, że:

- Nie modyfikują treści;
- Przestrzegają warunków dotyczących dostępu do informacji i zasad dotyczących aktualizacji treści;
- Nie zakłócają zgodnego z prawem korzystania z technologii w celu uzyskania danych na temat wykorzystania informacji;
- Szybko podjęli działania w celu usunięcia dostępu do przechowywanych informacji, gdy zostaną poinformowani, że informacje zostały usunięte z sieci, gdy dostęp do niej został wyłączony lub gdy organ odpowiedzialny zlecił usunięcie.

“Hosting”

Usługodawcy, którzy przechowują informacje dostarczone przez odbiorcę usługi i na ich żądanie, nie ponoszą odpowiedzialności, jeżeli:

- Nie posiadają faktycznej wiedzy na temat nielegalnej działalności lub informacji oraz w odniesieniu do roszczeń odszkodowawczych i nie są świadomi faktów ani okoliczności, z których wynika nielegalna działalność lub informacje,
  lub
- Gdy dostawca, po uzyskaniu takiej wiedzy lub świadomości, działa szybko w celu usunięcia lub uniemożliwienia dostępu do informacji.

E. Pliki cookie

Czym są pliki cookie?

Plik HTTP cookie, określany również jako ciasteczko internetowe, plik cookie w Internecie, plik cookie przeglądarki, magiczny plik cookie lub po prostu plik cookie to niewielki fragment danych przechowywanych na komputerze lub telefonie komórkowym użytkownika, który można odczytać za pomocą Notatnika. Plik cookie umożliwia stronie "zapamiętanie" twoich działań lub preferencji w czasie (na przykład, jeśli umieściłeś przedmioty w koszyku online, możesz uzyskać do nich dostęp podczas następnych wizyt na stronie internetowej). Może również rejestrować aktywność użytkownika, w tym klikanie historii przycisków, logowanie informacji, nazw, adresów, haseł, itp. Większość przeglądarek obsługuje pliki cookie, ale użytkownicy mogą decydować, czy je akceptują, a także usuwać je w dowolnym momencie.

Różne rodzaje plików cookie

Istnieją dwa podstawowe typy plików cookie sklasyfikowane według długości życia i domeny, do której należą. Są to:

- **Sesyjne pliki cookie** (pliki cookie w pamięci, przejściowe pliki cookie lub nietrwałe pliki cookie) istnieją tylko w pamięci tymczasowej, podczas gdy użytkownik porusza się po stronie internetowej. Zwykle są usuwane, gdy użytkownik opuszcza przeglądarkę.
- **Stałe pliki cookie** wygasają w określonym dniu lub po określonym czasie, w przeciwieństwie do sesyjnych plików cookie, w zależności od życzeń ich twórcy. Informacje, które zawierają, są przekazywane do serwera za każdym razem, gdy użytkownik odwiedza stronę, do której należy. Są one również określane jako śledzące pliki cookie, ponieważ mogą być wykorzystywane przez reklamodawców do rejestrowania informacji o zwyczajach przeglądania użytkownika.

Jeśli chodzi o domenę, do której należą, to dzielą się na:

- **Własne pliki cookie**, które są ustawiane przez serwer www odwiedzanej strony i mają tę samą domenę, co oznacza, że atrybut domeny pliku cookie będzie zgodny z domeną wyświetlaną na pasku adresu przeglądarki internetowej.
- **Obce pliki cookie** przechowywane w innej domenie niż domena odwiedzanej strony. Ten rodzaj plików cookie zwykle pojawia się, gdy strony internetowe zawierają treści z zewnętrznych stron internetowych, takich jak banery reklamowe. Daje to możliwość śledzenia historii przeglądania użytkownika i jest często wykorzystywana przez reklamodawców w celu wyświetlania odpowiednich reklam każdemu użytkownikowi.

Istnieją również bezpieczne pliki cookie, pliki http-only cookie, pliki super-cookie, pliki cookie zombie.

W normalnych okolicznościach pliki cookie nie mogą przenosić wirusów ani złośliwego oprogramowania na komputer. Ponieważ dane w pliku cookie nie zmieniają się, gdy jest przenoszony tam i z powrotem, nie ma możliwości wpływania na sposób działania komputera. Jednak niektóre wirusy i złośliwe oprogramowanie mogą być zamaskowane jako pliki cookie. Na przykład „pliki super-cookie" mogą być zagrożeniem dla bezpieczeństwa, ale wiele przeglądarek oferuje sposób ich blokowania. „Plik cookie zombie" to plik cookie, który pojawia się ponownie po usunięciu, sprawiając, że pliki cookie zombie są trudne do zarządzania. Obce pliki cookie mogą również powodować problemy z bezpieczeństwem, ponieważ ułatwiają stronom, których nie możesz zidentyfikować, śledzenie, dokąd zmierzasz i co robisz online.

Dyrektywa o prywatności i łączności elektronicznej

Korzystanie z plików cookie powoduje obawy związane z prywatnością. W maju 2011 r. Przyjęto dyrektywę UE w celu ochrony prywatności konsumentów w Internecie. Tak brzmi dyrektywa 2009/136/WE, która stała się znana jako dyrektywa o plikach cookie - o prywatności i łączności elektronicznej. Obowiązuje ona każdą osobę lub organizację, która jest fizycznie zlokalizowana w UE i ma stronę

internetową i/lub dowolną stronę internetową skierowaną do konsumentów w UE, które korzysta z plików cookie.

Ustawodawstwo wymaga, aby strony internetowe:

- ✓ Informowały użytkowników, czy używają plików cookie;
- ✓ Wyjaśniały, jakie dane są zbierane za pomocą plików cookie i w jaki sposób wykorzystywane są te dane;
- ✓ Zbierają zgodę użytkownika na korzystanie z plików cookie.

Jeśli posiadasz stronę internetową, musisz upewnić się, że jest ona zgodna z prawem, a to zwykle oznacza wprowadzenie pewnych zmian. Zgodność z dyrektywą o sprowadza się do trzech podstawowych kroków:

- ✓ Informuj użytkowników, że używasz plików cookie;
- ✓ Podaj link, pod którym mogą dowiedzieć się więcej o tym, jak korzystasz z zebranych danych;
- ✓ Zapewnij użytkownikom możliwość wyrażenia zgody na korzystanie z plików cookie.

Najczęstszym sposobem na zrobienie tego jest wyświetlenie małego baneru u góry lub u dołu strony internetowej z linkiem do szczegółowej polityki prywatności/ ochrony danych oraz przycisk do wyrażenia zgody na wykorzystanie plików cookie i ukrycie banera.

Istnieją dwa rodzaje zgody, które strony mogą gromadzić:

- **Wyraźne wyrażenie zgody** - użytkownicy muszą kliknąć przycisk, zaznaczyć pole wyboru lub wykonać inne określone działanie, aby wyrazić zgodę na korzystanie z plików cookie. Po uzyskaniu wyraźnej zgody użytkownicy nie mogą okazjonalnie wyrażać zgody na używanie plików cookie.
- Domniemane wyrażenie zgody - jeden z najpopularniejszych sposobów, w który zbierana jest domniemana zgoda, to wyświetlanie ważnego powiadomienia cookie, które kończy się stwierdzeniem: „Kontynuując korzystanie z tej strony, zgadzasz się na użycie plików cookie." Ważne jest, aby jednoznaczne powiadomienie zostało przekazane, a użytkownik był

świadomy, że niektóre z jego działań będą rozumiane jako domniemana zgoda na użycie plików cookie.

Przepisy obowiązują niezależnie od tego, czy użytkownik jest na komputerze, smartfonie, tablecie lub jakimkolwiek innym urządzeniu. Dlatego też podczas konfigurowania powiadomienia o plikach cookie ważne jest, aby zawiadomienie było wyświetlane i działało poprawnie na wszystkich urządzeniach.

RODO i pliki cookie

Celem RODO jest ochrona "osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu takich danych", innymi słowy użytkowników strony internetowej. Pliki cookie są wymienione raz w preambule RODO. Jednak to co w niej jest zapisane ma znaczący wpływ na zgodność plików cookie z dyrektywą:

(30)

Osoby fizyczne mogą być powiązane z identyfikatorami online dostarczanymi przez ich urządzenia, aplikacje, narzędzia i protokoły, takie jak adresy protokołów internetowych, identyfikatory plików cookie lub inne identyfikatory, takie jak znaczniki identyfikacji radiowej. Może to pozostawiać ślady, które w szczególności w połączeniu z unikalnymi identyfikatorami i innymi informacjami otrzymanymi przez serwery mogą być wykorzystywane do tworzenia profili osób fizycznych i ich identyfikacji.

Innymi słowy, kiedy pliki cookie mogą zidentyfikować osobę, uznaje się ją za dane osobowe.

Nie wszystkie pliki cookie są używane w sposób umożliwiający identyfikację użytkowników, ale większość jest i będzie podlegać RODO. Obejmuje to pliki cookie do celów analitycznych, reklamowych i usług funkcjonalnych, takich jak narzędzia ankiet i czatów.

Aby zachować zgodność, organizacje muszą albo zaprzestać zbierania plików cookie naruszających zasady, albo znaleźć zgodne z prawem podstawy do gromadzenia i przetwarzania tych danych. Większość organizacji opiera się na zgodzie

(dorozumianej lub opt-in), ale wzmocnione wymagania RODO oznaczają, że uzyskanie zgody prawnej będzie znacznie trudniejsze.

- **Domniemana zgoda nie jest już wystarczająca.** Zgoda musi być wyrażona wyraźnym akcentem, takim jak kliknięcie pola wyboru lub wybranie ustawień lub preferencji w menu ustawień. Po prostu odwiedzenie strony nie jest równoznaczne z wyrażeniem zgody.
- **Komunikaty typu „Korzystając z tej strony, akceptujesz pliki cookie" również nie są wystarczające z tych samych powodów.** Jeśli nie ma prawdziwego i wolnego wyboru, to nie ma ważnej zgody. Musisz umożliwić zarówno akceptowanie, jak i odrzucanie plików cookie. To oznacza:
    - **Musi być tak samo łatwo wycofać zgodę, jak jej udzielić.** Jeśli organizacje chcą, aby ludzie blokowali pliki cookie, jeśli nie wyrażą na to zgody, muszą najpierw zaakceptować pliki cookie.
    - **Strony będą musiały zapewnić opcję opt-out.** Nawet po uzyskaniu ważnej zgody strony muszą dać ludziom możliwość zmiany zdania. Jeśli poprosisz o zgodę za pomocą opcji akceptacji w menu ustawień, użytkownicy muszą zawsze mieć możliwość powrotu do tego menu, aby dostosować swoje preferencje.

F. Lista kontrolna - zgodność z prawem

	✓
Moja strona internetowa zawiera:	
Regulamin	
Prawa i obowiązki	
BRAK wstępnie zaznaczonych pól	
BEZPŁATNY kontakt	
Formularz rezygnacji	
Nie przechowuję danych wrażliwych dłużej niż jest to uzasadnione	
Wiem, co stanowi przetwarzanie danych osobowych	
Podczas przetwarzania danych osobowych przestrzegam zasad:	
Legalności	
Uczciwości i przejrzystości	
Legalności	
Minimalizacji danych i ograniczonego przechowywania	
Dokładności	
Integralności i poufności	
Powiadomienie organu nadzoru	
Komunikacja z osobą, której dane dotyczą	

Ryzyka i wysokiego ryzyka	
Odpowiedzialności i prowadzenia dokumentacji	
Oferowana usługa / produkt zawiera pełne informacje o całkowitych kosztach, w tym wszelkich dodatkowych opłatach	
Nie pobieram opłat za płatności kartą kredytową	
Infolinia dla moich klientów jest ustalana na podstawie stawki bazowej	
Informuję użytkowników o tym, że używam plików cookie	
Zbieram zgody użytkowników na korzystanie z plików cookie	
Wyjaśniam, jakie dane są gromadzone podczas wyrażania zgody na używanie plików cookie.	

G. Glosariusz terminologii

Rozporządzenie UE - rozporządzenie jest aktem prawnym UE, który staje się natychmiast wykonalny jako prawo we wszystkich państwach członkowskich jednocześnie.

Dyrektywa UE - Dyrektywa jest aktem prawnym UE, który wymaga od państw członkowskich osiągnięcia określonego rezultatu bez narzucania środków do osiągnięcia tego rezultatu. Można ją odróżnić od przepisów, które są samo-wykonalne i nie wymagają żadnych środków wykonawczych. Dyrektywy zwykle pozostawiają państwom członkowskim pewien margines swobody w zakresie dokładnych przepisów prawnych, które należy przyjąć. Dyrektywy można przyjmować za pomocą różnych procedur legislacyjnych w zależności od ich przedmiotu.

Środki transpozycji - w prawie UE transpozycja to proces, w którym państwa członkowskie UE wprowadzają dyrektywę w życie, wprowadzając odpowiednie środki wykonawcze. Transpozycja jest zazwyczaj dokonywana przez prawodawstwo pierwotne lub wtórne.

Rynek wewnętrzny - zwany również jednolitym rynkiem europejskim lub wspólnym rynkiem. Rynek wewnętrzny jest jednolitym rynkiem, który ma na celu zagwarantowanie swobodnego przepływu towarów, kapitału, usług i pracy - "czterech swobód" - w obrębie UE.

Zgodność - Zgodne z obowiązującymi przepisami, zarówno krajowymi, jak i międzynarodowymi.

H. Wnioski i dodatkowe źródła wiedzy

W niniejszej części e-Poradnika opisano szczegółowo niezbędne informacje na temat ogólnego rozporządzenia o ochronie danych (RODO), a następnie analizę dyrektywy w sprawie praw konsumentów (CRD), dyrektywy o handlu elektronicznym oraz dyrektywy o prywatności i łączności elektronicznej (EPD).

Na podstawie omówionych tematów i po przejrzeniu listy kontrolnej twoja firma funkcjonuje teraz zgodnie z przepisami UE. Ważne jest, aby nigdy nie przeoczyć, na co wskazują regulacje unijne i krajowe, nie tylko dlatego, żeby ubezpieczyć się od kar pieniężnych, ale także po to, aby być odpowiedzialnym społecznie.

Porady prawne są często uważane za drogie i trudno dostępne, ale należy skonsultować się z ludźmi, którzy są świadomi tego, co firmy potrzebują, aby być w zgodzie z prawem i unikać obchodzenia niektórych zasad tylko, dlatego, żeby zmniejszyć wydatki, ponieważ te "luki" mogą cię kosztować znacznie więcej w przyszłości!

Aby uzyskać bezpłatny mentoring i porady na ten temat, możesz skorzystać z platformy mentoringu DiFens dostępnej pod adresem: http://www.difens.eu/, gdzie eksperci prawni mogą pomóc ci rozwiązać konkretny przypadek.

Dodatkowe źródła wiedzy:

Are you ready for tomorrow's data compliance challenges? **FORBES**	Is your website legal? **YFS Magazine**	The lifecycle of data protection is evolving. Here's what you need to know. **FORBES**
Legal regulations for e-commerce **KOMISJA EUROPEJSKA**	Summary of adoption of e-commerce legislation worldwide **UNCTAD**	Why cookie alternatives are vital for the future of mobile advertising? **CLEARCODE**

I. Źródła:

Competition and Consumer Protection Commission (2017) The Consumer Rights Directive: A guide for traders dealing with consumers. Dostępne na: https://www.ccpc.ie/business/wp-content/uploads/sites/3/2017/03/CRD-Guidance_FINAL.pdf

European Commission (2014) DG JUSTICE: Guidance document concerning Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council. Dostępne na: https://ec.europa.eu/info/sites/info/files/crd_guidance_en_0.pdf

Jelowicki, L. (2014)The EU Consumer Rights Directive 2014 explained. Practicology.com. Dostępne na: https://www.practicology.com/thinking/blog/eu-consumer-rights-directive-2014-explained

Lindahl, F. (2013)The Consumer Rights Directive. Improved as a cross-border-only Regulation and toward a European Consumer Code, influenced by the Common Frame of Reference? Master's thesis in Commercial and Tax Law. Jönköping International Business School. Dostępne na: https://www.diva-portal.org/smash/get/diva2:623054/FULLTEXT01.pdf

Schmon, C. (2016) Review of the Consumer Rights Directive. BEUC Comments. Dostępne na: http://www.beuc.eu/publications/beuc-x-2016-093_csc_beucs_comment_to_review_of_consumer_rights_directive.pdf

CZĘŚĆ IV

CYBERBEZPIECZEŃSTWO

A. Wstęp

Istnieje wiele definicji dla cyberbezpieczeństwa. Najbardziej znana brzmi: "**Bezpieczeństwo komputerowe,** zwane również **bezpieczeństwem cybernetycznym** lub **bezpieczeństwem informatycznym**, jest ochroną systemów komputerowych przed kradzieżą lub uszkodzeniem ich sprzętu, oprogramowania lub informacji, a także przed zakłóceniami lub błędnym kierowaniem świadczonych usług" [1].

Cyberbezpieczeństwo to duża i interesująca dziedzina badawcza w społeczności informatyków. W tej części zajmiemy się głównie praktycznym bezpieczeństwem komputerowym, co oznacza sposób, w jaki bezpieczeństwo komputerowe jest stosowane w codziennych ustawieniach. Bardziej konkretnie zajmiemy się bezpieczeństwem codziennych procesów w przedsiębiorstwie, nawet najmniejszym lub najnowszym.

Zwykle mamy do czynienia z pewnymi właściwościami, które wpływają na systemy komputerowe. Te właściwości mogą być związane ze sprzętem, oprogramowaniem lub nawet siecią. Pogorszenie tej właściwości może prowadzić do takich konsekwencji, jak kradzież, uszkodzenie, zakłócenie lub błędne ukierunkowanie danych i procesów biznesowych. Zniszczenie tej właściwości może być celowe, tj. atak lub przypadkowe, tj. uszkodzenie. Najczęstsza sytuacja polega na tym, że osoba atakująca celowo osłabia bezpieczeństwo systemu komputerowego.

To brzmi jak naprawdę przerażający i skomplikowany problem, i zazwyczaj tak jest. Niemniej jednak ludzie nie powinni wpadać w panikę lub działać niepoprawnie. Umieszczenie wszystkich możliwych istniejących mechanizmów kontroli bezpieczeństwa na miejscu może być równie niepoprawne, jak w przypadku nie robienia niczego. Posiadanie zbyt wielu środków bezpieczeństwa może wywołać kilka problemów. Oznacza to dodatkową pracę dla działów IT i bezpieczeństwa. Bycie przedsiębiorcą oznacza, że prawdopodobnie nie masz przywileju posiadania dedykowanego personelu do tego, co może prowadzić do wydawania zbyt dużo pieniędzy i czasu na partnera zewnętrznego, który dostarcza ci oprogramowanie lub środki bezpieczeństwa. Ponadto zbyt wiele środków bezpieczeństwa i metod zero-jedynkowych, ich projektowanie i przestrzeganie, wiąże się z dodatkową pracą dla

twoich pracowników. Jeśli, na przykład, muszą przejść przez wiele kroków za każdym razem, gdy chcą połączyć się z oprogramowaniem do wystawiania faktur, trudno będzie im faktycznie pracować, a zatem jest to czasochłonne. Zawsze istnieje możliwość, że ludzie spróbują znaleźć inne, łatwiejsze rozwiązanie, obejście tego problemu. Takie rozwiązania byłyby najprawdopodobniej całkowicie niepewne i niewłaściwe. Dla firm ważne jest, aby zachować równowagę między bezpieczeństwem a wydajnością. Ważnym aspektem, który wpływa na wydajność w tym zakresie, jest użyteczność. Konfiguracja bezpieczeństwa w oprogramowaniu i podejmowanie decyzji związanych z bezpieczeństwem jest trudnym zadaniem dla wielu użytkowników. Sposób przedstawienia aspektów bezpieczeństwa pod względem ich konstrukcji i użyteczności sprawia, że jest to skomplikowany proces, który użytkownicy wolą unikać, a w większości przypadków nawet go ignorować [21]. Raporty identyfikują błąd człowieka jako jedną z najczęstszych przyczyn błędów konfiguracji zabezpieczeń, głównie ze względu na nieprzydatne projektowanie systemów zabezpieczeń [21], [22]. Ponadto stosowanie systemów bezpieczeństwa, które nie są przydatne, prowadzi do błędów popełnianych przez użytkowników, które podważają ogólne bezpieczeństwo [23].

Wszystkie powyższe można przełożyć na koszty związane z działalnością gospodarczą. Oczywiste jest, że istnieje potrzeba bardziej elastycznych rozwiązań, które zapewnią spersonalizowane metody utrzymania bezpieczeństwa zgodnie ze specyficznymi potrzebami każdej firmy lub organizacji. Możemy śmiało powiedzieć, że istnieje kilka aspektów, które należy uwzględnić przy stosowaniu zabezpieczeń komputerowych.

Kolejną kwestią, o której warto wspomnieć, jest to, że bezpieczeństwo w przedsiębiorstwie w odniesieniu do cyfrowych danych i procesów obejmuje również aspekt fizyczny, a nie tylko techniczny. Systemy komputerowe obejmują również urządzenia sprzętowe, które mogą zostać w jakiś sposób skradzione lub zniszczone. Można podjąć pewne środki bezpieczeństwa w celu ich ochrony, takie jak posiadanie ich w odpowiednich obiektach, zawsze zamykanie pomieszczenia, w którym się znajdują itd. Fizyczne i techniczne (wirtualne) zabezpieczenia można zazwyczaj łączyć w celu zapewnienia rozwiązań w niektórych sytuacjach. Na przykład, jeśli laptop zostanie skradziony lub serwer zostanie zniszczony z powodu

pożaru, to jeśli prawidłowo wykonałeś kopię zapasową danych, będziesz mógł je przywrócić i uruchomić system przy użyciu innego urządzenia. Mogą wystąpić straty, ale nie będą one dla firmy fatalne w skutkach.

Dodatkowym krokiem, jaki może obrać każda firma, jest poświęcenie czasu na edukowanie użytkowników (tj. pracowników, dostawców lub kogokolwiek innego używającego systemu) na temat tego, dlaczego i jak właściwie korzystać ze środków i narzędzi bezpieczeństwa. To może zaoszczędzić im czasu w pracy, uniemożliwić im dokonywanie prób znalezienia obejścia i stworzenia świadomości bezpieczeństwa w środowisku pracy.

Cyberbezpieczeństwo jest bardzo ważne, nie tylko ze względu na utratę danych, czasu lub pieniędzy, które firma może napotkać w przypadku naruszenia bezpieczeństwa, ale także ze względu na przepisy UE dotyczące ochrony danych, które przedsiębiorstwa będą musiały spełnić, ponieważ 25 maja 2018 r. zostało wprowadzone w życie RODO [19]. Można znaleźć się w trudnej sytuacji nie tylko w obliczu utraty biznesu, ale także mając do czynienia ze sprawami sądowymi, grzywnami i sądami.

W następnych sekcjach przedstawiamy następujące tematy: Bezpieczeństwo cyfrowe jako kwestia techniczna; Wpływ naruszeń zabezpieczeń cyfrowych na procesy biznesowe; rozwiązania w obszarze bezpieczeństwa cybernetycznego wraz z listę kontrolną dotyczą cyberbezpieczeństwa oraz glosariusz terminologii.

B. Bezpieczeństwo cyfrowe jako kwestia techniczna

I. Wprowadzenie

Na początek musimy wspomnieć, że cyberbezpieczeństwo to nie tylko kwestia techniczna. Co się stanie, jeśli cały system telefoniczny przestanie działać? Dotyczy to nie tylko technicznej części działalności, ale także procesów takich jak sprzedaż lub zakupy, inwentaryzacja, komunikacja z klientami, itp.

Jak wykazano powyżej, techniczne aspekty bezpieczeństwa cybernetycznego mogą mieć bezpośredni wpływ na cały biznes. To jest praktyczna strona cyberbezpieczeństwa. W związku z tym zdobywanie większej wiedzy na temat jej aspektów technicznych ma zasadnicze znaczenie dla sprostania kryzysowi tego rodzaju.

Różne aplikacje mają różne wymagania względem bezpieczeństwa, które można pogrupować według następujących zasad: Poufność, integralność, dostępność, uwierzytelnianie, niezaprzeczalność, odpowiedzialność, prywatność i inne. Trzy najważniejsze zasady, zwane Triadą CIA, to poufność (confidentiality), uczciwość (integrity) i dostępność (availability). Systemy komputerowe firm muszą być chronione na wszystkich trzech poziomach przez cały czas. Zaniedbanie któregokolwiek z nich oznacza większe ryzyko w systemach bezpieczeństwa.

II. Zasady Triady CIA

Jak wyjaśniono powyżej, jest to za każdym razem bardzo ważne, gdy próbujemy analizować, oceniać lub wdrażać zabezpieczenia w każdym systemie komputerowym, aby uwzględnić wszystkie aspekty zasad triady CIA. Każda z nich poniżej jest opisana bardziej szczegółowo, aby zapewnić lepsze zrozumienie.

Poufność

Zgodnie z zasadą poufności informacje nie są udostępniane ani ujawniane nieupoważnionym osobom, systemom lub procesom. W prostszych słowach, rzeczy,

które powinny być trzymane w tajemnicy, muszą być w tej tajemnicy trzymane. Jak możemy je chronić? Jak ważna jest ich ochrona? Czy te tajemnice mogą być użyte przeciwko osobie, której dotyczą? Na przykład wyobraź sobie, że ktoś kradnie informacje o karcie kredytowej klienta twojego sklepu internetowego. Ponadto istnieje wiele innych danych, które zazwyczaj muszą być utrzymywane w tajemnicy, w tym własność intelektualna, informacje finansowe, tajemnice państwowe, dane studentów i inne. Poufność jest bardzo ważna, ponieważ opiera się na niej prawo i przepisy. Szkody spowodowane utratą poufności, na przykład w wyniku naruszenia danych, mogą być poważne. Jest to najbardziej pożądana zasada triady CIA, z którą zazwyczaj ludzie są najbardziej zaznajomieni. Jest mnóstwo przykładów na to jak codzienne korzystamy i ochraniamy poufność. Jednym z przykładów jest wykorzystanie zaszyfrowanych kanałów do komunikacji w Internecie, tak jak w sytuacji, gdy mamy dane logowania przechodzące przez „https" zamiast „http", aby utrzymać całkowicie zaszyfrowaną komunikację między klientem a serwerem, aby zachowa ich poufność. Właściciel strony musi uzyskać certyfikat "https" i użyć go, aby skorzystać z tej bezpiecznej komunikacji. Szyfrowanie jest już zaimplementowane przez protokół https. Zgodnie z informacjami podanymi przez Google: Począwszy od lipca 2018 roku w wersji Chrome 68, Chrome zaznaczy wszystkie witryny „http" jako „niebezpieczne". Czytaj więcej na oficjalnym ogłoszeniu Google w [8].

Innym przykładem jest użycie wirtualnej sieci prywatnej - sieci VPN do połączenia, jeśli podróżujemy, a nie tylko korzystania z dowolnego niezaufanego dostępnego Wi-Fi, które może być niebezpieczne. VPN to „tunelowana" zabezpieczona sieć za pośrednictwem sieci rozległej (WAN - Wide Area Network), takiej jak Internet, która umożliwia bezpieczną komunikację między swoimi punktami końcowymi. Osoba podłączona do VPN jest w rzeczywistości bezpiecznie połączona z (zabezpieczoną) siecią lokalną (LAN) swojej firmy podczas pobytu poza domem, co oznacza, że nie musi być faktycznie zlokalizowana w fizycznej lokalizacji sieci LAN firmy w celu zabezpieczenia [2]. VPN oferuje szyfrowaną komunikację między klientem, a serwerem i jest własnością organizacji w celu kontrolowania i monitorowania przechodzącego przez nią ruchu. W przypadku ataku organizacja będzie mogła znaleźć za pośrednictwem sieci VPN żądania, które są przekazywane do niego lub z niego, co zwykle ujawnia, kim jest atakujący.

Innym przykładem jest użycie oprogramowania szyfrującego do szyfrowania woluminów danych. Takie oprogramowanie to funkcja BitLocker, która jest technologią Windows i FileVault, która jest rozwiązaniem dla komputerów Mac. Szyfrowanie może faktycznie być postrzegane jako techniczna implementacja poufności. Posiadanie naprawdę ważnych danych zaszyfrowanych może sprawić, że pozostaną one tajne nawet w przypadku, gdy zostaną skradzione, ponieważ pliki będą nieczytelne dla każdego, kto nie posiada odpowiedniego klucza do odszyfrowywania.

Istnieje kilka algorytmów i metod szyfrowania, które można wykorzystać do szyfrowania i ochrony danych. Metoda AES jest najbardziej znaną i najnowszą. Jak więc ktoś może wykorzystać tę wiedzę?

Jak pokazano na Rycinie 1 poniżej, kroki są następujące:

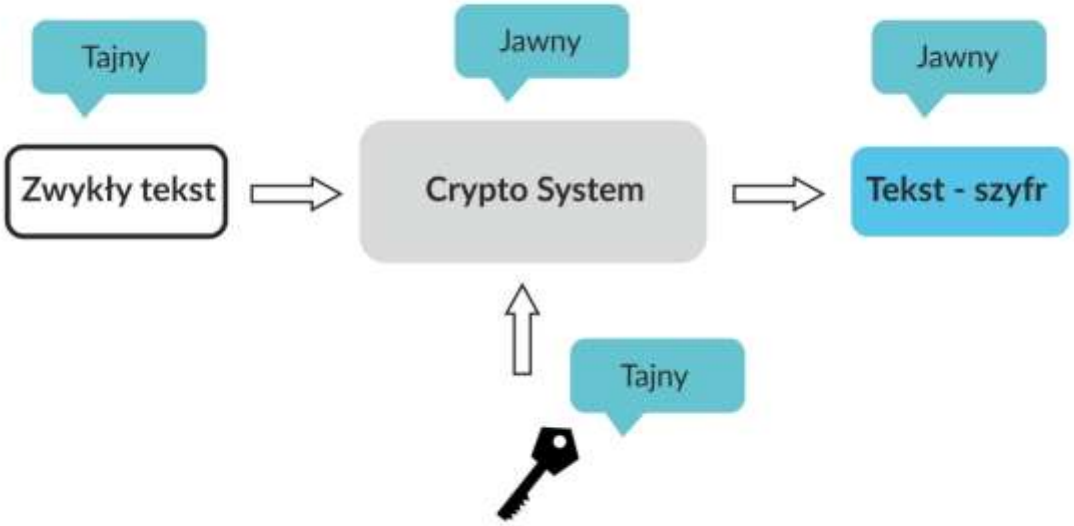
Pierwszą rzeczą do zrobienia jest wybranie algorytmu kryptograficznego do zastosowania, który ma w sobie System Crypto. Algorytm kryptograficzny jest publiczny i znany każdemu, nie wpływając na bezpieczeństwo szyfrowania.

Po drugie, wybierz klucz do szyfrowania, który spowoduje, że dane staną się nieczytelne. Klucz powinien zdecydowanie być trzymany jako tajemnica, w przeciwieństwie do algorytmu kryptograficznego.

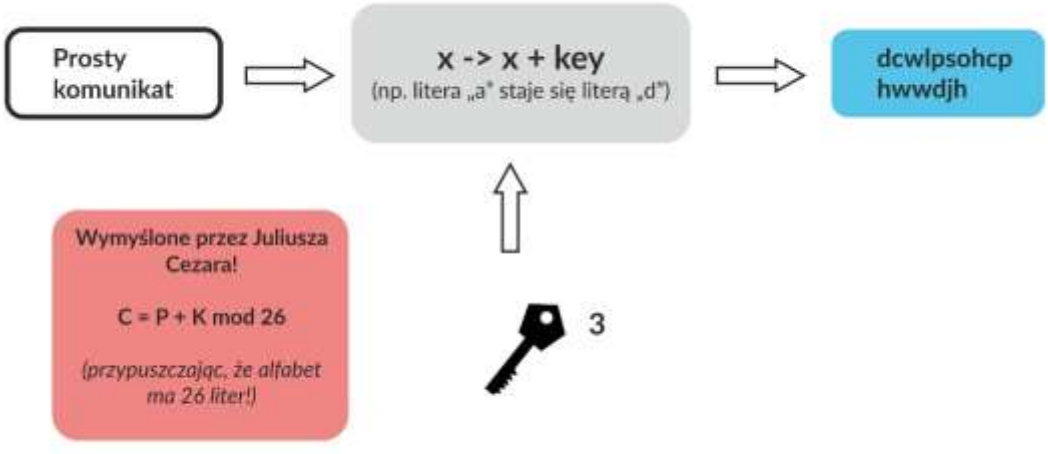
Teraz jako następny krok, mając klucz i informacje, które chcesz zaszyfrować, możesz przekazać je do Systemu Crypto, który wygeneruje zaszyfrowane dane zwane szyfrogramem.

Możesz teraz wysyłać lub przechowywać szyfrogram. Nawet publicznie, nikt bez klucza odszyfrowywania nie ma do niego dostępu.

Jeśli chcesz użyć tych danych, odszyfruj je za pomocą pasującego klucza.


Tajny
Jawny
Jawny
Zwykły tekst
Crypto System
Tekst - szyfr
Tajny

Ryc. 1 ([6])


Prosty komunikat
x -> x + key
(np. litera „a" staje się literą „d")
dcwlpsohcp hwwdjh
Wymyślone przez Juliusza Cezara!
C = P + K mod 26
(przypuszczając, że alfabet ma 26 liter!)
3

Ryc. 2 ([6])

Załóżmy, że mamy następujący tekst, który chcemy zaszyfrować: „prosta wiadomość". Tekst jest teraz znaczący i wszyscy rozumieją, co mówi. Jeśli ktoś uzyska nieautoryzowany dostęp do serwera w celu wyświetlenia lub pozyskania z niego danych, zobaczy tekst „prosta wiadomość". Zdecydowaliśmy się na użycie Caesar Cipher jako naszego algorytmu kryptograficznego. Algorytm ten zasadniczo przesuwa litery w alfabetycznym cyklu. Zdecydowaliśmy również, że naszym kluczem jest liczba „3". Należy pamiętać, że chociaż klucze muszą być skomplikowane, to jest to tylko prosty przykład. Aby być w cyklu, każda postać w tekście „prosta wiadomość" zostanie przesunięta o +3 litery. Na początku dzielimy klucz (k = 3) przez 26 (litery w alfabecie angielskim). Następnie przesuwamy literę zgodnie z resztą podziału i tak dalej. W rezultacie otrzymamy wiadomość jako "dcwlpsohcphwwdjh". To zdecydowanie nie jest czytelne! Możemy go gdzieś schować lub wysłać na inny koniec. Jeśli chcemy przeczytać tę wiadomość za pomocą naszego klucza, po prostu stosujemy opisany powyżej proces w odwrotnej kolejności. Oznacza to, że odejmujemy nasz klucz od każdej litery, itd. [Rycina 2]

Zobaczmy teraz na przykładzie, jak mierzymy siłę klucza szyfrującego. Ataki Brute-Force w zasadzie oznaczają próbowanie wszystkich możliwych kombinacji w celu osiągnięcia czegoś (np. złamanie hasła lub znalezienie klucza szyfrującego z zakresem możliwych kombinacji). Czterobitowy klucz szyfrowania ma 2^4 możliwe kombinacje i jest równy 16 kluczowym próbom złamania szyfrowania. Jest to naprawdę łatwe do złamania, zamiast 32-bitowego klucza szyfrowania, który ma 2^{32} możliwe kombinacje równe 4 294 967 296 próbom złamania szyfrowania. Wyobraź sobie użycie jeszcze większego klucza o długości 64 bitów! Zajmie to niewiarygodnie dużo czasu, przez co nie da się złamać szyfrowania. Teraz rozważmy nasz przykład na Rycinie 2, gdzie używany klucz wymaga tylko 2 bitów do przedstawienia: z 2 bitami możemy uzyskać liczbę od 0 do 3, tj. tylko $2^2 = 4$ kombinacje. Osoba atakująca, posługując się atakiem brute-force, będzie potrzebowała w najgorszym przypadku tylko 4 prób odnalezienia naszego klucza.

Do tej pory powinno być już całkowicie jasne, dlaczego musimy przestrzegać zasady poufności. Może chronić nas przed ludźmi umyślnie lub przypadkowo wyciekającymi nasze tajne lub wrażliwe dane i zapewniać dostęp tylko upoważnionym osobom.

Integralność

Zasada integralności stanowi, że dane lub informacje nie zostały zmienione, zniszczone lub w jakikolwiek sposób zmodyfikowane lub utracone w sposób nieuprawniony lub przypadkowy.

W prostych słowach informacja musi być dokładna i kompletna, zawierająca „prawdę" pochodzącą od źródła. Aby porozmawiać o codziennych przykładach wykorzystania i ochrony integralności, możemy zacząć od stwierdzenia, że integralność pozwala nam weryfikować dane przechodzące przez sieć i specjalnie sprawdzać pakiety pod kątem błędów za pomocą metody cyklicznej kontroli nadmiarowej (CRC, Cyclical Redundancy Check). CRC to funkcja mieszająca, która wykrywa przypadkowe zmiany w surowych danych komputerowych powszechnie stosowanych w cyfrowych sieciach telekomunikacyjnych [20]. Jeśli występują błędy, informacje są ponownie wysyłane i ponownie sprawdzane, itd. Innym przykładem jest podpis cyfrowy, algorytm kryptograficzny zapewniający, że osoba, która faktycznie wysłała informacje, była tą, która miała go wysłać. Kolejnym przykładem są algorytmy kryptograficznego mieszania, takie jak MD5 lub SHA1. Porównują pobierany plik, na przykład oprogramowanie, z pierwotnie oferowanym pobieraniem, tworząc wartość skrótu o stałej długości, będący skrótem. Nawet niewielka zmiana w pliku przyniesie ogromną zmianę w wynikach (skrócie).

Jednym z przykładów jest atak phpMyAdmin. Atakujący może zastąpić niektóre pliki binarne tego bardzo często używanego oprogramowania, co zapobiega powodzeniu sprawdzania skrótu i sumy kontrolnej.

Integralność i dokładność są naprawdę ważne i potrzebne. Jeśli nie możemy zweryfikować, czy otrzymana wiadomość jest "dobra", jaki jest cel jej otrzymania? Wyobraź sobie, że oglądasz film ze zniekształconą informacją. Czy możesz później wykorzystać tę wiedzę nabytą jako poprawną lub czy przegapiłeś jakieś ważne informacje?

Dostępność

Zasada dostępności stwierdza, że system informacyjny lub zasób systemowy, tj. informacja pozostaje dostępna i użyteczna na żądanie przez uprawnioną jednostkę systemu, na przykład użytkownika, zgodnie ze specyfikacją wydajności dla

systemu. System jest dostępny, jeśli świadczy usługi zgodnie z jego projektem na żądanie użytkowników lub w sposób ciągły.

Mówiąc najprościej, systemy muszą być dostępne i funkcjonować, a do danych powinniśmy mieć dostęp zawsze, gdy ich potrzebujemy. Zastanówmy się nad przykładem komputera, który psuje się podczas wykonywania przez niego ważnej pracy lub katastrofalnego wirusa wymazującego cały system komputerowy. Może to być nawet sytuacja życiowa i śmiertelna, na przykład w przypadku, gdy dokumentacja medyczna pacjenta nie jest dostępna w nagłym przypadku.

A co jeśli dojdzie do całkowitego zniszczenia urządzeń, a co za tym idzie, utraty danych? Czy masz ich kopię zapasową, aby przywrócić je tak szybko, jak to możliwe, przywracając w ten sposób również ich dostępność? A co z przypadkiem, w którym dane z kopii zapasowej były przechowywane w tej samej fizycznej lokalizacji co oryginał, a wszystkie zostały zniszczone podczas pożaru? Czy potrzebujesz więcej kopii zapasowych w różnych lokalizacjach, urządzeniach lub centrach danych?

Niektóre sposoby, które możemy wykorzystać do zapewnienia lepszego i bardziej odpowiedniego tworzenia kopii zapasowych w celu zwiększenia dostępności danych, obejmują: włączenie poziomów RAID, które są danymi grupowymi na poziomy w serwerach centrów danych, w zależności od tego, ile potrzebujemy, aby te dane były dostępne, a klastrowanie serwerów oznacza różne centra danych, ale wszystkie dostarczają dane na tę samą stronę internetową, a użytkownik nie ma o tym pojęcia, a także za pomocą mechanizmów równoważenia obciążenia, aby dane użytkowników trafiały na dostępne serwery, na przykład w przypadku, gdy jeden z nich nie działa.

Przykładem ataku na system komputerowy, który prowadzi do niepowodzenia dostępności, jest atak Denial of Service (odmowa usługi). Odmowa usługi to cyberatak w której atakujący dąży do unieruchomienia maszyny lub sieci, aby żaden użytkownik nie mógł jej normalnie używać. Może zakłócać doświadczenie użytkownika za pośrednictwem usługi. Usługa jest więc zasadniczo "nieczynna" i nie może być regularnie używana przez klientów.

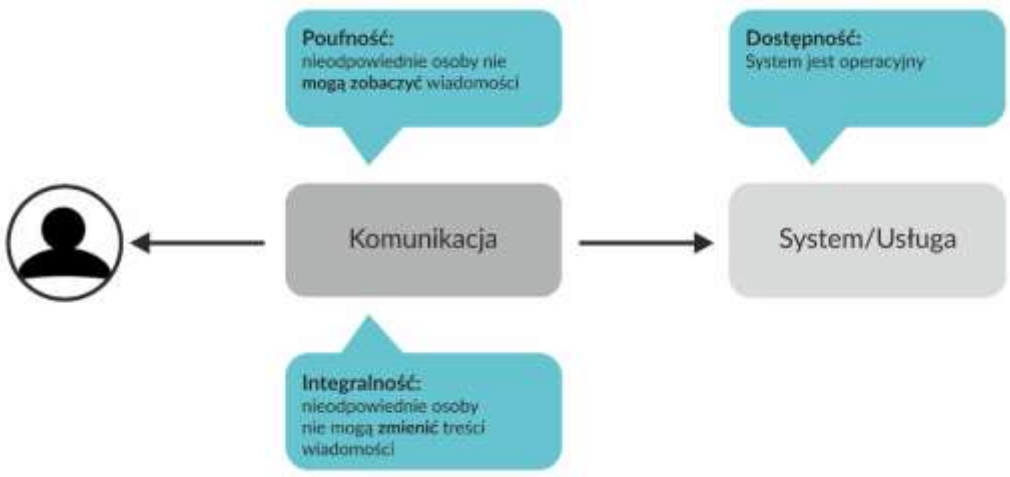
Atak DoS jest realizowany poprzez przeciążenie docelowej maszyny lub sieci ogromną liczbą żądań próbujących przeciążyć te systemy i całkowicie lub częściowo uniemożliwić ukończenie niektórych żądań.

Natomiast podczas ataku rozproszonej odmowy usługi (atak DDoS) ruch przychodzący przeciążający system docelowy pochodzi z wielu różnych źródeł. To uniemożliwia zatrzymanie ataku, ponieważ aby to osiągnąć, będziemy musieli zablokować każdego atakującego nasz system.

Atak DoS lub DDoS jest podobny do tłumu próbującego uzyskać dostęp do drzwi wejściowych lub bramy do sklepu lub firmy, a tym samym nie dopuszczając do wejścia odpowiednich osób. Może to zakłócić normalne funkcjonowanie sklepu lub firmy. Atakujący używający metody DoS często atakują witryny lub usługi hostowane na wysokim poziomie serwery internetowe takie jak te należące do banku, np. bramki płatności kartą kredytową.

Poniżej przedstawiamy w formie graficznej przykład zastosowania trzech zasad, o których mówiliśmy, wpływających na komunikację między systemem, a użytkownikiem oraz na to, jak ważne są one dla bezpieczeństwa tej komunikacji.

Załóżmy, że użytkownik chce komunikować się przez Internet z systemem lub usługą. Może to być twój klient komunikujący się z usługą sklepu internetowego. Użytkownik musi mieć oferowaną usługę bez żadnych problemów, które mogłyby spowodować nieprawidłowe działanie usługi (dostępność). Użytkownik chce potajemnie wysyłać wiadomości do systemu / usługi bez niechcianych oczu czytających ich wiadomości (poufność). Oprócz tego, nikt nie powinien mieć możliwości zmiany tych wiadomości w jakikolwiek sposób, a tym samym zmieniać oryginalnych danych wysyłanych lub otrzymywanych przez użytkownika (integralność). [Rycina 3]



Ryc. 3 ([6])

III. Ryzyko

Ryzyko w systemie można mierzyć prawdopodobieństwem utraty jednej z trzech analizowanych powyżej zasad bezpieczeństwa CIA. Nie myśl, że ryzyko odnosi się tylko do wielkich zagrożeń lub ataków. Ryzyko może być wszędzie, nawet w najprostszych rzeczach.

Bardziej szczegółowa dyskusja na temat ryzyka znajduje się w części V.

IV. Przegląd najpowszechniejszych rodzajów ataków

Złośliwe oprogramowanie

Termin „złośliwe oprogramowanie” jest połączeniem słów „złośliwy” i „oprogramowanie". Mówiąc najprościej, złośliwym oprogramowaniem jest jakikolwiek program zamierzający wyrządzić szkody na danych, urządzeniach lub ludziom. Takie oprogramowanie jest zaprojektowane i opracowane w celu niszczenia danych, wpływając na wydajność komputera, powodując awarię lub szpiegując prywatne informacje.

Historycznie złośliwe oprogramowanie było rozpowszechniane wśród użytkowników za pośrednictwem załączników do wiadomości e-mail. E-mail bezpośrednio otrzymany przez użytkownika prosił go o pobranie załącznika. Kliknięcie aktywowało i instalowało złośliwe oprogramowanie, a ostatecznie powodowało zamierzoną szkodę [7].

Każdy rodzaj złośliwego oprogramowania działa w inny sposób, aby zainfekować komputery i dane, a zatem każdy z nich wymaga innej metody usuwania Najlepszą praktyką, którą można zastosować, jest użycie oprogramowania antywirusowego zawierającego narzędzia do usuwania złośliwego oprogramowania. Nie zapomnij też o unikaniu podejrzanych e-maili i linków [17].

Różne znane typy złośliwego oprogramowania to wirusy, trojany, oprogramowanie szpiegujące (Spyware), robaki komputerowe, oprogramowanie szantażujące (Ransomware), oprogramowanie reklamowe (Adware) i BotNets. Pokrótce:

Wirus, jak sugeruje jego nazwa, dołącza się do niezainfekowanych plików, kopiuje się i propaguje poprzez infekowanie innych czystych plików i systemów komputerowych. Ta propagacja może być niekontrolowana. Uszkodzenie wywołane taką infekcją może być poważne lub nawet nieodwracalne, np. uszkodzenie w podstawowej funkcjonalności systemu, niszczenie i usuwanie plików itp. Wirus zazwyczaj ma postać pliku wykonywalnego i zostaje aktywowany po uruchomieniu (klikając na niego) [7], [17].

Trojan, podszywa się pod legalne oprogramowanie lub znajduje się w jednym z takich, które zostały wcześniej zmodyfikowane. Jak sama nazwa wskazuje, działa dyskretnie i tworzy backdoory w zabezpieczeniach systemu, aby umożliwić wejście innym złośliwym oprogramowaniom [17].

Spyware, to złośliwe oprogramowanie zaprojektowane do szpiegowania twoich informacji. Jest prawie zawsze w pakiecie z bezpłatnym oprogramowaniem i często jest to cena, którą musisz zapłacić za używanie tego oprogramowania. Może to być niewielka uciążliwość, np. wyświetlanie wyskakujących reklam, zmiana ustawień bez twojej zgody lub działania. Może też mieć poważny wpływ na system komputerowy, np. drastycznie spowalnia działanie systemu. Może się również zdarzyć, że program szpiegujący ukryje się w tle i zanotuje, co robisz w Internecie, w tym hasła, numery

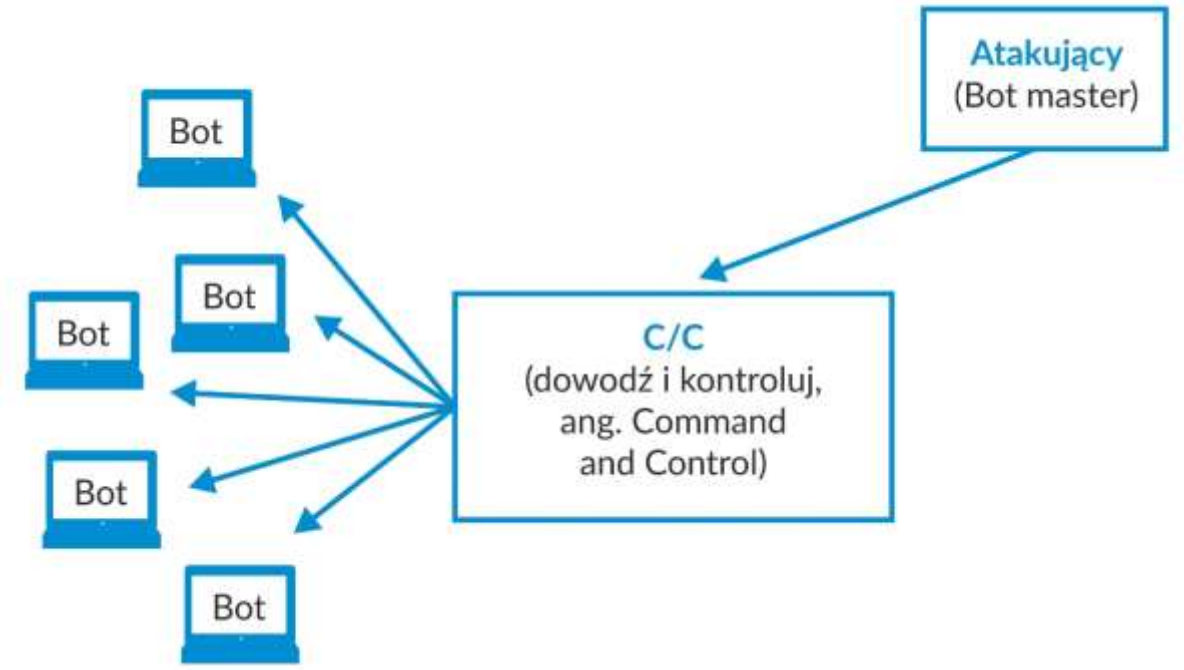
kart kredytowych, nawyki surfowania, informacje osobiste i finansowe, itp. Ponadto może przejąć zdalną kontrolę nad komputerem w celu uzyskania dostępu do plików i danych, zainstalować oprogramowanie lub korzystać z komputera w celu rozprzestrzeniania wirusów [7], [17].

Robaki komputerowe: Robak jest rodzajem wirusa, ale z podstawową różnicą, że ma zdolność rozprzestrzeniania się automatycznie bez inicjacji człowieka (podczas gdy typowy wirus rozprzestrzenia się poprzez działalność człowieka, na przykład poprzez uruchomienie pliku instalacyjnego). Robak może rozprzestrzeniać się z komputera na komputer, wykorzystując luki w oprogramowaniu i sprzęcie, wykorzystując każdą kolejną zainfekowaną maszynę, aby zainfekować ich więcej [17], [18].

***Ransomware*:** Oprogramowanie to jest złośliwe, ponieważ uzyskuje nieautoryzowany dostęp do systemów komputerowych i szyfruje pliki. W ten sposób może zatrzymać je jako „zakładników" wraz z całym systemem lub urządzeniem, blokując dostęp do nich, dopóki nie zapłacisz żądanego okupu w zamian za klucz odszyfrowywania [4]. Ransomware jest wyjaśnione bardziej szczegółowo w dalszej części e-poradnika.

***Adware*:** Adware nie zagraża bezpośrednio systemowi komputerowemu, tak jak inne złośliwe oprogramowania, ponieważ jest to oprogramowanie reklamowe. Problem polega na tym, że może on podważyć twoje bezpieczeństwo, aby dążyć do osiągnięcia swoich celów i tym samym otwierając twój system na działanie innych złośliwych oprogramowań [17].

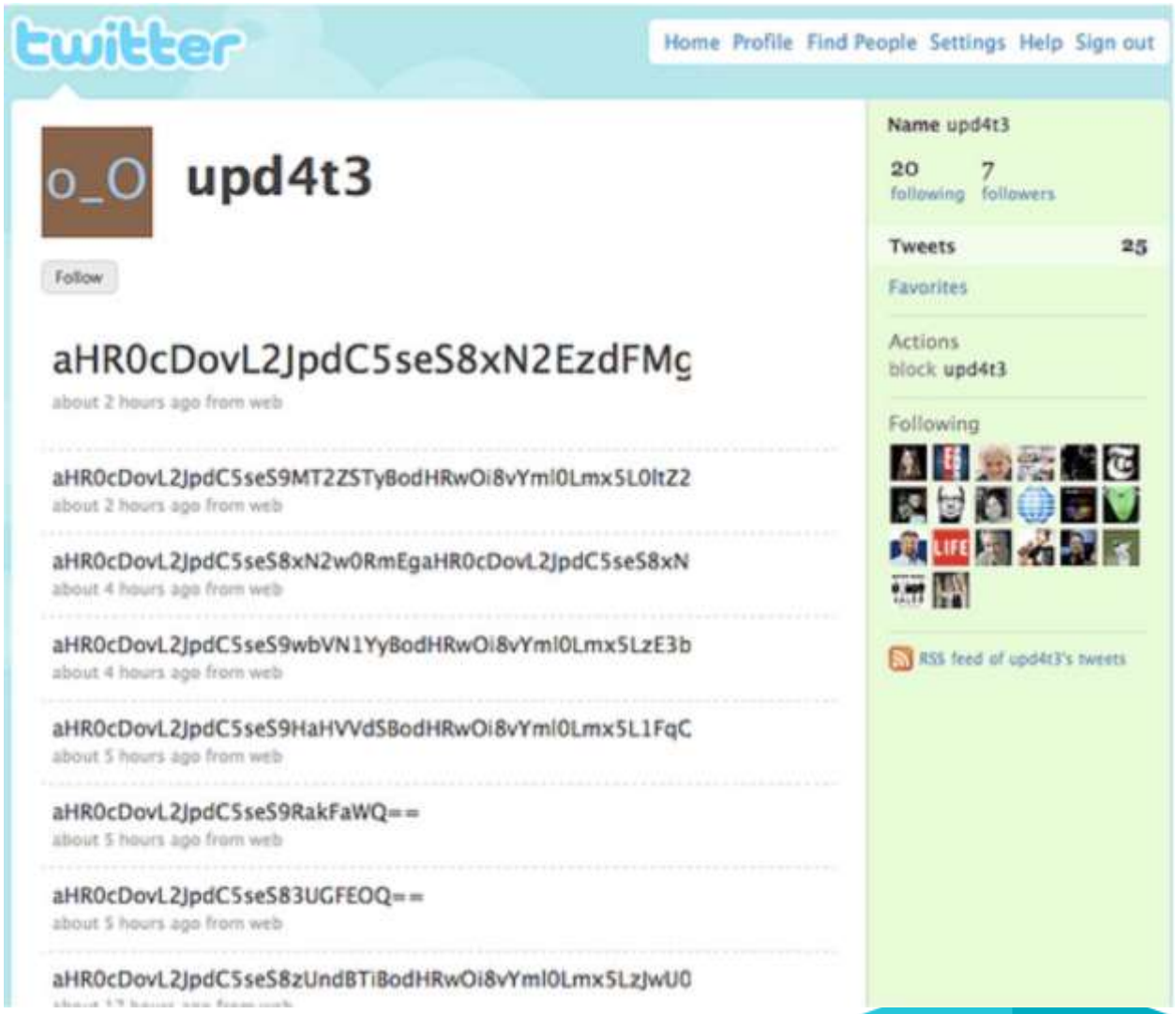
***Atak BotNet*:** Atakujący zazwyczaj próbują zagrozić serwerom zawierającym cenne dane o firmie lub jej użytkownikach. Sposobem na zaszkodzenie lub wykorzystanie zaatakowanego serwera jest kontrolowanie kilku zwykłych hostów (na przykład komputera) jako botów. Boty te mogą zawierać BotNet (jak armię upośledzonych maszyn, patrz Rycina 4) [6], które mogą być używane na różne sposoby atakowania innych hostów, zachowując anonimowość atakującego.



Ryc. 4

BotNet to w zasadzie duża grupa upośledzonych hostów, które mogą być kontrolowane przez atakującego, tzw. Bot Mastera. Sieci te są często wynajmowane do przeprowadzania wszelkiego rodzaju złośliwych działań. Na przykład, ktoś może znaleźć Bot Matsera i poprosić go, aby użył BotNet do kliknięcia oszustwa na łączu w celu zarobienia większej ilości pieniędzy lub fałszywego ruchu, wysyłania wiadomości e-mail SPAM do wielu e-maili, zdobywania fałszywych komentarzy na Facebooku / Twitterze lub do retweetów . Jednym z najbardziej popularnych działań atakującego, który wynajmuje BotNet od Bot Mastera są ataki DDoS (Distributed Denial of Service) skierowane do hosta (ów).

Bot Master kontroluje BotNet poprzez ukryty kanał poleceń i kontroli (BotNet C/C). Boty okresowo sprawdzają ten kanał, aby otrzymywać nowe polecenia. Polecenia często pochodzą z innych źródeł, zobacz Rycinę 5 [6]. Na przykład konto na Twitterze stworzono właśnie do tego rodzaju ataków. Atakujący wysyła tweety z zaszyfrowanymi poleceniami, aby nikt nie wiedział, co w nich jest. BotNet C/C może odczytać polecenie, używając klucza atakującego do odszyfrowania go, a następnie jego wykonania.



Ryc. 5

Zobaczmy kilka znanych przykładów z powyższych oprogramowań:

W 2000 r. wirus „ILOVEYOU" był najbardziej szkodliwym przykładem złośliwego oprogramowania wszechczasów. Wirus przychodził na skrzynkę e-mail w wiadomości zatytułowanej „Kocham cię". „ILOVEYOU" nadpisuje pliki systemowe i pliki osobiste i błyskawicznie się rozprzestrzenia [24].

„Storm Worm" natomiast był koniem trojańskim, który infekował komputery, czasami zmieniając je w zombie lub boty, aby kontynuować rozprzestrzenianie się wirusa i wysyłać ogromną ilość spamu. Urządzenia były infekowane, gdy ktoś otwierał e-mail z napisem „230 zabitych przez burze nękające Europę" i klikał w link. Do lipca 2007 r., Storm Worm został odebrany w ponad 200 milionach e-maili [24].

Bardzo znanym przykładem oprogramowania szantażującego jest CryptoLocker wydany we wrześniu 2013 r. i rozpowszechniany za pośrednictwem załączników wiadomości e-mail oraz szyfrowany w plikach użytkownika, aby nie mogli uzyskać do nich dostępu [24].

Ataki na sieci internetowe

Ataki oparte na sieci to te, które korzystają z systemów i usług internetowych, w tym: przeglądarek (wraz z ich rozszerzeniami), stron internetowych (w tym CMS - systemy zarządzania treścią) oraz komponentów informatycznych usług sieciowych i aplikacji internetowych.

Istnieją różne rodzaje tych ataków, takie jak:

- exploity w przeglądarkach internetowych (lub w ich rozszerzeniach),
- exploity w serwerach sieciowych i usługach internetowych,
- ataki typu drive-by,
- ataki metodą wodopoju
- przekierowania i ataki typu „człowiek w przeglądarce"

Exploity w przeglądarkach internetowych to formy złośliwego kodu, który wykorzystuje lukę w zabezpieczeniach systemu operacyjnego lub zainstalowanego oprogramowania, z zamiarem złamania zabezpieczeń przeglądarki i zmiany ustawień przeglądarki użytkownika bez jego wiedzy [32].

Serwery www i exploity usług internetowych to oprogramowanie lub fragment danych, który wykorzystuje błąd lub lukę w zabezpieczeniach serwera internetowego lub usług internetowych, aby spowodować niezamierzone lub nieprzewidziane zachowanie. Takie zachowanie może umożliwić atakującym na przykład zdalne przejęcie kontroli nad zaatakowanym serwerem lub usługą internetową, przez Internet, i umożliwia im zdalne wykonanie złośliwego kodu.

Ataki typu drive-by dotyczą niezamierzonego pobierania oprogramowania komputerowego z Internetu i mają na celu dwie rzeczy:

- pobrania, które użytkownik uruchomił, ale bez zrozumienia tego konsekwencji. Na przykład pobranie, które automatycznie zainstalowało nieznany program, jak składnik ActiveX lub aplet Java,
- pobrania, które nastąpiły bez wiedzy użytkownika. Takie pobrania można zainicjować po prostu odwiedzając stronę internetową lub przeglądając wiadomość e-mail w formacie html, z zaimplementowanym szkodliwym skryptem do kodu HTTP lub PHP [33].

Ataki metodą wodopoju to ataki, w których atakujący odgaduje lub obserwuje, które witryny są często odwiedzane przez ofiarę lub określoną grupę (tj. organizację, branżę lub region) i infekuje jedną lub więcej takich witryn złośliwym oprogramowaniem. Atak ten to rodzaj strategii ataku komputerowego, w którym ofiarą jest określoną grupą użytkowników. Atak taki może potencjalnie zainfekować członków grupy docelowej poprzez określone konfiguracje szkodliwego oprogramowania, aby móc wybrać docelowych użytkowników spośród zarażonych użytkowników [34].

Przekierowanie użytkowników legalnej witryny do innej witryny jest możliwe dzięki umieszczeniu złośliwego kodu w pliku konfiguracyjnym serwera www. Następnie atakujący chce, aby użytkownicy wprowadzali poufne informacje do złośliwej witryny podczas pozornego nawigowania w zaufanej witrynie. Ataki typu „człowiek w przeglądarce" mają na celu przechwycenie danych podczas przechodzenia przez bezpieczną komunikację między użytkownikiem a aplikacją online [35].

Ataki na aplikacje internetowe

Ataki na aplikacje webowe są skierowane przeciwko dostępnym aplikacjom internetowym, usługom sieciowym, a także aplikacjom mobilnym. Takie ataki próbują nadużywać interfejsów API wbudowanych w aplikacje internetowe. Ataki w aplikacjach internetowych są zwykle skierowane na dobrze znane zasoby i projekty oparte na otwartym lub publicznym źródle, takie jak wtyczki Joomla i Wordpress, witryny Magento, itp.

Można wymienić następujące ataki aplikacji internetowych:

- SQL Injection (SQLi),

- Local File Inclusion (LFI),
- Remote File inclusion (RFI),
- Cross-site Scripting (XSS),
- PHP injection (PHPi) lub PHP Object Injection [36].

Atak typu SQL Injection (SQLi) to technika wstrzykiwania kodu. Służy do atakowania aplikacji opartych na danych, w których nikczemne instrukcje SQL są wstawiane do pola wejściowego w celu ich wykonania. SQL Injection jest jedną z najbardziej krytycznych luk w zabezpieczeniach. Atak oparty na luce SQL Injection pozwala na zrzut zawartości bazy danych, takich jak: nazwiska, numery kart kredytowych i wszelkich innych poufnych i wrażliwych danych handlowych [37].

Local File Inclusion (LFI) to atak polegający na włączeniu, w którym osoba atakująca może oszukać aplikację internetową, w tym pliki na serwerze internetowym, wykorzystując funkcje, które dynamicznie zawierają lokalne pliki lub skrypty. Konsekwencją takiego ataku jest: Przekazywanie katalogów i ujawnianie informacji, a nawet zdalne wykonywanie kodu. Local File Inclusion jest bardzo podobny do Remote File Inclusion (RFI).

W RFI atakujący w porównaniu do LFI może nie tylko zawierać pliki lokalne, ale także pliki zdalne [38].

Cross-site Scripting (XSS) to rodzaj ataku polegającego na wstrzykiwaniu kodu po stronie klienta, w którym osoba atakująca może wykonywać złośliwe skrypty w legalnej witrynie lub aplikacji sieciowej [39].

Wstrzykiwanie PHP (PHPi) lub PHP Object Injection jest luką w poziomie aplikacji, która w rzeczywistości pozwala atakującemu na różnego rodzaju złośliwe ataki, takie jak: SQL Injection, Application Denial of Service, Code Injection i Path Traversal w oparciu o kontekst [40].

Atak typu Denial of Service

Atak typu DoS (Denial of Service) to atak z zamiarem wyłączenia komputera lub sieci, przez co jest niedostępny dla użytkowników. Ataki tego typu są zwykle realizowane przez kierowanie dużym ruchem lub wysyłanie informacji powodujących awarię. W obu przypadkach atak ten odmawia pracownikom, członkom lub

posiadaczom kont, a więc rzeczywistym uzasadnionym użytkownikom, usługi lub zasobu. Do najczęstszych ofiar ataków typu DoS należą banki, firmy handlowe, agencje medialne lub organizacje rządowe i handlowe, a także inne prestiżowe organizacje. Ataki typu DoS zwykle nie skutkują kradzieżą lub utratą informacji lub innych aktywów, ale wiążą się z utratą czasu i pieniędzy. Innym typem ataku DoS jest atak DDoS (Distributed Denial of Service). Atak typu DDoS ma miejsce, gdy wiele systemów przeprowadza zsynchronizowany atak DoS na pojedynczy cel. Różnica polega na tym, że cel jest atakowany z wielu lokalizacji jednocześnie [41].

Spam

Spam jest tak stary, jak sam Internet. Ale nadal pozostaje głównym środkiem dostarczania szkodliwego oprogramowania, wykorzystując złośliwe załączniki i szkodliwe linki. Spam to ponad 85% wszystkich wysłanych wiadomości e-mail, a konta spamowe stanowią ponad 50% wolumenu adresów e-mail. Spam jest wysyłany przez duże botnety lub zainfekowane wirusem komputery, a także może być kanałem reklamującym produkty zdrowotne lub usługi erotyczne/randkowe. Ważne jest, aby użytkownicy zadawali sobie pytanie przed otwarciem wiadomości e-mail, jeśli znają nadawcę, czy format załącznika i treść są poprawne, czy rozpoznają temat wiadomości e-mail [42].

Phishing

Phishing wykorzystuje przede wszystkim techniki socjotechniczne do atakowania użytkowników końcowych. Techniki te służą do oszukiwania użytkowników i wykorzystywania słabych stron w bezpieczeństwie sieci. Ataki Phishingowe zwykle rozpoczynają się od złośliwej wiadomości e-mail, którą otrzymują użytkownicy, w której są przekonani, że odwiedzają fałszywą witrynę internetową, która próbuje uzyskać poufne informacje, takie jak nazwy użytkowników, hasła i dane karty kredytowej. Na przykład e-mail z Phishingiem może zawierać informację od pracownika banku i prosić o podanie danych logowania do bankowości internetowej, aby pomóc ci rozwiązać problem, który uznał, że masz, lub wolontariusz Czerwonego Krzyża z prośbą o podanie numeru karty kredytowej, aby zaakceptować darowiznę dla potrzebujących i tak dalej. Będziesz musiał być bardzo ostrożny, logicznie do wszystkiego podchodzić i pamiętać, że organizacje nigdy nie będą prosić o twoje dane uwierzytelniające przez e-mail. Nie wszystko jest wiarygodne.

Istnieje duże prawdopodobieństwo, że może to być osoba atakująca, która próbuje okraść cię z cennych informacji.

Phishing staje się coraz bardziej wyrafinowany i ukierunkowany, co utrudnia jego wykrywanie. Zamiast e-maili często używane są również komunikatory.

Wyłudzanie informacji może również pojawić się na fałszywej stronie internetowej, która wygląda bardzo podobnie do innych, tych bardziej popularnych. Co ważne, te fałszywe strony zwykle wyglądają identycznie jak te prawdziwe a jedyną różnicą jest adres URL witryny. Na przykład, w jakiś sposób lub ktoś może przekierować cię do strony o nazwie www.bankofvvvest.com zamiast www.bankofwest.com. Wyglądają podobnie, ale pierwsza z nich to fałszywa kontrolowana strona internetowa atakującego w celu uzyskania osobistych informacji, rachunków bankowych, kart kredytowych itp. Ten drugi przykład można by uniknąć, stosując odpowiednie certyfikaty, które zostaną opisane w dalszej części. Ogólnie kampanie Phishingowe zwiększyły się zarówno pod względem wielkości, jak i zaawansowania. Phishing jest zwykle wykorzystywany jako pierwszy krok w cyberatakach. Z tego powodu Phishingu jest powiązany z większością zagrożeń cybernetycznych, takich jak: botnety, złośliwe oprogramowanie, ataki internetowe, zestawy exploitów, cyber-szpiegostwa itp. [43]

Insider Threat

Zagrożenie wewnętrzne, zgodnie z definicją, odnosi się do zagrożenia, że użytkownik wewnątrz danej organizacji poprzez autoryzowany dostęp wykorzysta poufne informacje, umyślnie lub nieumyślnie, aby zaszkodzić bezpieczeństwu danej organizacji. Z tego powodu zagrożenia wewnętrzne są poważnym zagrożeniem dla różnych instytucji i organizacji, niezależnie od ich lokalizacji, wielkości czy sektora. Dla większości organizacji trudno jest odróżnić to działanie od całkowicie niegroźnej działalności. Incydenty tego typu mogą być celowe lub nieumyślne. Należy jednak wspomnieć, że straty spowodowane takim zagrożeniem są w dużej mierze nieznane. Ale to uprzywilejowani użytkownicy, w tym menedżerowie z dostępem do poufnych informacji, stanowią największe zagrożenia dla organizacji [44].

Fałszerstwo tożsamości

Kradzież tożsamości jest szczególnym przypadkiem naruszenia bezpieczeństwa danych. Jest to atak mający na celu uzyskanie poufnych informacji, które mogą być wykorzystane do identyfikacji osoby lub nawet systemu komputerowego. Informacje te można następnie wykorzystać do podszywania się pod właściciela tożsamości. Celem ataków jest uzyskanie takich informacji, jak: możliwe do zidentyfikowania nazwiska, adresy, dane kontaktowe, dane uwierzytelniające, dane finansowe, dane dotyczące zdrowia, dzienniki, itp. Gdy osoba atakująca posiada dane osobowe, może opróżnić rachunek bankowy ofiary, naliczyć opłaty na karcie kredytowej ofiary, otworzyć nowy rachunek. Atakujący może nawet uzyskać leczenie medyczne kosztem ubezpieczenia zdrowotnego ofiary. Złodziej może nawet podać nazwisko ofiary policji podczas aresztowania. Według Federalnej Komisji ds. Handlu, niezależnej agencji rządu Stanów Zjednoczonych, kradzież tożsamości mieści się w sześciu głównych kategoriach: oszustwo związane z zatrudnieniem lub podatkowe (wykorzystanie danych osobowych innej osoby w celu uzyskania zatrudnienia lub złożenia zeznania podatkowego), oszustwa związane z kartami kredytowymi (wykorzystujące cudzą kartę kredytową lub numer karty kredytowej w celu dokonywania nieuczciwych zakupów), oszustwo telefoniczne lub narzędzia (przy użyciu danych osobowych innej osoby w celu otwarcia telefonu komórkowego lub konta usługowego), oszustwo bankowe (wykorzystanie danych osobowych innej osoby do przejęcia istniejącego rachunku finansowego lub otwarcia nowego rachunku pod czyimś nazwiskiem), oszustwo pożyczkowe lub leasingowe (wykorzystujące czyjeś informacje do uzyskania pożyczki lub leasingu), dokumenty rządowe lub oszustwa świadczeń (wykorzystujące skradzione dane osobowe w celu uzyskania korzyści rządowych) [45].

Wyciek informacji

Wyciek informacji jest głównym zagrożeniem bezpieczeństwa cybernetycznego. Wyciek informacji oznacza różne rodzaje wycieków danych, począwszy od danych osobowych gromadzonych przez internetowych gigantów i usługi online, a nawet danych biznesowych przechowywanych w infrastrukturach informatycznych przedsiębiorstw [46].

Cyber-szpiegostwo

Cyber-szpiegostwo oznacza kradzież tajemnic i informacji przechowywanych w formatach cyfrowych lub na komputerach i sieciach informatycznych, bez zgody i wiedzy posiadacza informacji, od osób indywidualnych, konkurentów, rywali, grup, rządów i wrogów w celach osobistych, ekonomicznych, politycznych lub aby uzyskać przewagę militarną. Cyber-szpiegostwo obejmuje zazwyczaj wykorzystywanie tajemnic i informacji, a nawet kontrolę nad poszczególnymi komputerami/całymi sieciami, dla korzyści strategicznych lub dla działań psychologicznych, politycznych i sabotażu. Ostatnio cyber-szpiegostwo obejmuje również analizę publicznej aktywności na portalach społecznościowych, w tym na Facebooku i Twitterze [47]. W większości przypadków użytkownicy lub organizacje, których bezpieczeństwo cyfrowe zostało naruszone, nie są nawet tego świadomi. Ale jakie są najlepsze formy ochrony przed zagrożeniami technicznymi w odniesieniu do bezpieczeństwa cyfrowego, takimi jak: złośliwe oprogramowanie, ataki sieciowe, ataki aplikacji internetowych, Phishing, spam, odmowa usługi, oprogramowanie Ransomware, botnety, zagrożenie wewnętrzne, manipulacja fizyczna, naruszenia bezpieczeństwa danych, kradzież tożsamości, wyciek informacji, zestawy exploitów, cyber-szpiegostwo? Proste, zdroworozsądkowe środki ostrożności podczas korzystania z Internetu i innych nowych technologii mogą zapobiec narażeniu na wyżej wspomniane zagrożenia techniczne. System operacyjny komputera powinien zostać jak najszybciej zaktualizowany (należy wziąć pod uwagę automatyczne aktualizacje), ponieważ hakerzy często wykorzystują znane luki w bezpieczeństwie systemu operacyjnego do swoich celów. Regularne aktualizacje mają również duże znaczenie dla różnych aplikacji na komputerach, smartfonach, tabletach czy nawet urządzeniach Internetu przedmiotów, ponieważ gdy tylko okaże się, że firmy produkujące oprogramowanie wykryły słabości, hakerzy zaczynają tworzyć programy, które wykorzystują te słabości. Aplikacje internetowe, usługi sieciowe, strony internetowe (w tym CMS - systemy zarządzania treścią) również powinny być regularnie aktualizowane. Przeglądarki i wtyczki powinny również zostać zaktualizowane do najnowszej wersji. Użytkownicy nie powinni pobierać załączników ani klikać odsyłaczy z podejrzanych wiadomości e-mail, szczególnie pochodzących z nieznanych im adresów e-mail. Oprogramowanie zapory sieciowej i pakiet zabezpieczeń internetowych, oprogramowanie antywirusowe powinno być używane

i regularnie aktualizowane, zwłaszcza podczas przeglądania Internetu. Podejrzane witryny nie powinny być odwiedzane. Hasła nie powinny być proste, a także sugeruje się ich częste wymiany (co 4 tygodnie). Regularnie twórz kopie zapasowe danych i przechowuj je w bezpiecznym miejscu. Administratorzy IT powinni upewnić się, że wszystkie systemy w sieci są załatane i zaktualizowane. Powinieneś uważać na to, co udostępniasz w mediach społecznościowych. Nie powinieneś zawierać zbyt wielu informacji na temat swoich profili [48].

V. Więcej potencjalnych problemów dla firm

Istnieją różne zagrożenia, które próbują oszukać ludzi, wykorzystując nowe, ale i twórcze sposoby. Takie jak:

- Oszustwa telefoniczne, które są podobne do wiadomości Phishingowych. Ludzie bardzo przekonująco mówią, że będą potrzebować od ciebie pewnych informacji dotyczących fałszywego problemu. Na przykład mogą powiedzieć, że dzwonią od firmy Microsoft i odkryli, że masz wirusa w swoim systemie. Aby móc Ci pomóc, będą potrzebować twoich danych logowania i innych informacji.
- Fizyczna obecność nieautoryzowanych osób w pokoju z centrum danych lub przed komputerem lub laptopem. Może to być ktoś, kto włamał się do twoich lokali w celu kradzieży danych, a nawet ktoś, kto udaje klienta, ale w rzeczywistości patrzy na dane prezentowane na ekranie, podczas gdy przeglądasz system, próbując odpowiedzieć na jego pytania dotyczące cen i zapasów.
- Ransomware to naprawdę duże zagrożenie dla wszystkich przedsiębiorstw, od najmniejszego przedsiębiorcy do największego. Jest to atak, w którym agent zagrożenia uzyskuje dostęp do komputera, szyfruje wszystkie dane w taki sposób, że nie można ich już używać, a następnie prosi o okup w celu odszyfrowania ich. Szczegółowy przykład zostanie podany w dwóch następnych sekcjach.
- Wreszcie, bardziej inteligentne i bardziej elastyczne wirusy i inne złośliwe oprogramowanie pojawiają się cały czas jako zagrożenie. Inwestowanie

w dobre oprogramowanie antywirusowe, które stale aktualizuje bazę wirusów, byłoby bardzo dobrym i skutecznym rozwiązaniem.

C. Wpływ naruszeń zabezpieczeń cyfrowych na procesy biznesowe

I. Wpływ

Opisaliśmy już powyższe przypadki, w których błąd techniczny w systemie komputera biznesowego spowodowany brakiem bezpieczeństwa może doprowadzić do zakłócenia procesów biznesowych. Tak czy inaczej, jeśli system lub jego część załamie się, oznacza to koszt dla firmy. Koszt nie zawsze oznacza pieniądze, może to oznaczać stratę czasu lub wysiłku, utratę przyszłych lub obecnych klientów, utratę cennych danych, a nawet stawienie czoła procesowi sądowemu.

Od najprostszych rzeczy, takich jak brak dostępu do Internetu przez kilka minut, aż po najpoważniejsze przypadki, takie jak kradzież informacji o kliencie, mogą się zdarzyć złe rzeczy.

Nie dotrzymanie terminu, brak możliwości wystawienia faktury lub pokwitowania, niemożność zrealizowania transakcji lub sprzedaży, niedostarczenie zamówienia w terminie, ujawnienie lub wykorzystanie wrażliwych danych, utrata wszystkich danych księgowych po kradzieży danych uwierzytelniających to tylko kilka sytuacji, w których przedsiębiorcy mogą się znaleźć ze względu na nieodpowiednią konfigurację zabezpieczeń ich systemu.

Co się stanie, jeśli ktoś ukradnie twoje dane uwierzytelniające, zaloguje się do twojego sklepu internetowego i przejmie kontrolę nad nim? Jeśli nie masz planu awaryjnego, możesz nawet stracić całą firmę.

Jak wcześniej wspomniano, atak za pomocą oprogramowania szantażującego (Ransomware) jest poważną sytuacją. Wykorzystajmy ten przykład jako studium przypadku w tej części e-Poradnika.

II. Studium przypadków: Ransomware:

Ransomware jest rodzajem złośliwego oprogramowania, które uzyskuje dostęp do systemów komputerowych, a szyfrowanie plików może przechowywać je wraz z całym systemem lub urządzeniem jako "zakładnikami", blokując dostęp do nich, dopóki nie zapłacisz żądanego okupu w zamian za klucz deszyfrowania. Jak wyjaśniliśmy w poprzedniej części, zaszyfrowane dane są nieczytelne, chyba że

posiadasz klucz [4]. Oczywiście, nawet jeśli okup zostanie zapłacony, nikt nie może zagwarantować, że klucz odszyfrowywania zostanie ostatecznie dostarczony. Pamiętaj, że masz do czynienia z przestępcami, którzy dbają tylko o twoje pieniądze, a nie o twoje dane. Jeśli poproszą o dane bankowe lub dane karty kredytowej, a ty je im dostarczysz, być może spróbują zmaksymalizować zysk, używając tych informacji nawet po wysłaniu klucza deszyfrującego (jeśli to w ogóle zrobią). Mogą też wysłać plik zatytułowany „odblokuj", który może zainfekować Twój komputer jeszcze bardziej złośliwym oprogramowaniem [28].

Ransomware możesz otrzymać z załącznika wiadomości e-mail, pobranego złośliwego pliku, zhakowanej strony internetowej lub pozornie niewinnej, ale w rzeczywistości złośliwej reklamy. Używanie scrackowanego oprogramowania, sieci P2P lub USB zainfekowanego oprogramowaniem Ransomware może potencjalnie zainfekować twoje urządzenie [29] Po zainfekowaniu Ransomware zauważysz, że twoje pliki, obrazy i dane zostały zaszyfrowane i nie możesz ich otworzyć. Możesz również zobaczyć ekran z groźbą i prośbą o zapłacenie okupu.

Ataki typu Ransomware istnieją od dziesięcioleci, ale utrzymują się jako jedno z największych zagrożeń, przed którymi stoją dziś firmy i osoby prywatne. W miarę jak zapobiegamy używaniu poprzedniego oprogramowania Ransomware, ich różnorodność jest coraz bardziej zaawansowana w rozprzestrzenianiu możliwości, unikaniu wykrycia, szyfrowaniu plików i zmuszaniu użytkowników do płacenia okupów. Każde nowe oprogramowanie jest bardziej wyrafinowane, trudniejsze do uniknięcia i bardziej szkodliwe dla ofiary.

Historycznym faktem jest, że pierwszy atak typu Ransomware, o którym wiemy, że miał miejsce w 1989 r., dotyczył branży opieki zdrowotnej, która wciąż jest jednym z głównych celów takich ataków. Niektórzy zaawansowani cyberprzestępcy tworzą w oparciu i Ransomware dobrze zarabiające firmy, oferując programy typu „Ransomware-as-a-service". Niektóre z najbardziej znanych Rnsomware to CryptoLocker, CryptoWall, Locky i TeslaCrypt. Sam CryptoWall wygenerował ponad 320 milionów dolarów przychodów.

Średni okup jaki należy opłacić wynosi około 500 dolarów. Zwykle ofiary są zobowiązane do zapłaty okupu, stwierdzając, że w ostatecznym terminie okup

ulegnie podwojeniu lub pliki staną się trwale niedostępne lub zniszczone lub nawet ujawnione publicznie.

Dlatego oczywiste jest, że atak typu Ransomware może wywrzeć znaczący i bardzo negatywny wpływ na firmę, niezależnie od tego, czy jest ona własnością przedsiębiorcy, czy jest ogromną, dobrze działającą korporacją. Dostępność staje się ogromnym problemem, a jeśli nie jesteś przygotowany i gotowy do odzyskania danych, to będzie to albo utrata tych danych lub utrata pieniędzy, a wraz z nimi wszelkie konsekwencje.

Jeśli potrzebujesz więcej informacji, możesz przeczytać szczegóły na temat 10 najgorszych ataków z wykorzystaniem Ransomware w roku 2017 w [9].

Pod koniec następnej części omówimy działania, które można podjąć w celu odparcia takiego ataku spowodowanego przez Ransomware.

D. Rozwiązania w obszarze cyberbezpieczeństwa

I. Ramy bezpieczeństwa

Wprowadzanie zabezpieczeń w systemach komputerowych może być frustrujące i mylące. Aby pomóc w tym zadaniu, można skorzystać z przewodników, takich jak ramy i standardy bezpieczeństwa, które wyjaśniają, jak zachować bezpieczeństwo, a także wskazać, czego należy unikać. Postępując zgodnie z tymi instrukcjami, możesz poprawić i potwierdzić swoje bezpieczeństwo. Bardziej ogólne ramy można zastosować do prawie każdej firmy. Można wybrać dowolne wskazówki. Przykłady takich ram obejmują ramy NIST [25], ramy ISO [26] i ramy CIS [27].

Decydując się na wybór ram, należy rozważyć takie, które jest stosunkowo łatwy do naśladowania i wydają się bardziej odpowiednie dla Ciebie. Po wybraniu ram zdecyduj, które formanty najlepiej pasują do twojej firmy. W zależności od procesów i potrzeb twojej firmy może nie być konieczne przestrzeganie wszystkiego lub wdrożenie wszystkich środków od samego początku. To prowadzi do tworzenia własnej polityki bezpieczeństwa, którą można stosować i dopracowywać.

II. Pozostałe środki bezpieczeństwa

W poprzednich sekcjach liczne środki bezpieczeństwa zostały przedstawione głównie jako przykłady. Podsumowując, niektóre środki, które mogą zapewnić rozwiązania dla wątków cybernetycznych, są następujące:

- Właściwe i regularne tworzenie kopii zapasowych wszystkich danych;
- Instalacja oprogramowania antywirusowego i zapory sieciowej z odpowiednimi specyfikacjami dla każdego urządzenia. Należy pamiętać, że czasami warto kupować tego rodzaju oprogramowanie, zamiast korzystać z ich bezpłatnych lub próbnych wersji;
- Regularna aktualizacja systemów;
- Zgodność z ramami bezpieczeństwa lub ich częścią;
- Wybieranie silnych haseł i ochrona ich przez nie dzielenie się nimi z nikim i nie pozwalanie im na ujawnienie;
- Uzyskanie certyfikatu https dla swojej witryny;

- Zapobieganie działań nieuprawnionych osób mających fizyczny dostęp do pomieszczeń lub urządzeń;
- Korzystaj wyłącznie z oprogramowania pochodzącego z zaufanych źródeł, które jest sprawdzane i weryfikowane oraz zawiera wszystkie niezbędne techniczne środki bezpieczeństwa.

Istnieje wiele narzędzi online, z których możesz skorzystać, aby ocenić swoje bezpieczeństwo lub określić, czy twoje bezpieczeństwo zostało naruszone.

- Narzędzia oceny bezpieczeństwa mogą być przydatne do sprawdzenia, jak dobrze wdrożyłeś środki bezpieczeństwa w swojej firmie. Jednym z przykładów jest narzędzie Microsoft Security Assessment Tool, które można znaleźć i pobrać na [10]
- Narzędzia, które pomogą Ci dowiedzieć się o wszelkich zagrożeniach na twoich kontach e-mail. Niektóre z nich podkreślają także ryzyko ataków na dzisiejszy Internet. Jednym z przykładów jest narzędzie Microsoft Security Assessment Tool, które można znaleźć i pobrać na [11] Wszystkie dane na temat tego narzędzia pochodzą z „naruszeń" które wyciekły publicznie lub, innymi słowy, danych konta osobistego, które zostały nielegalnie udostępnione, a następnie udostępnione publicznie. „Have I been pwned?" agreguje go i umożliwia łatwe wyszukiwanie.

III. Studium przypadków - część II

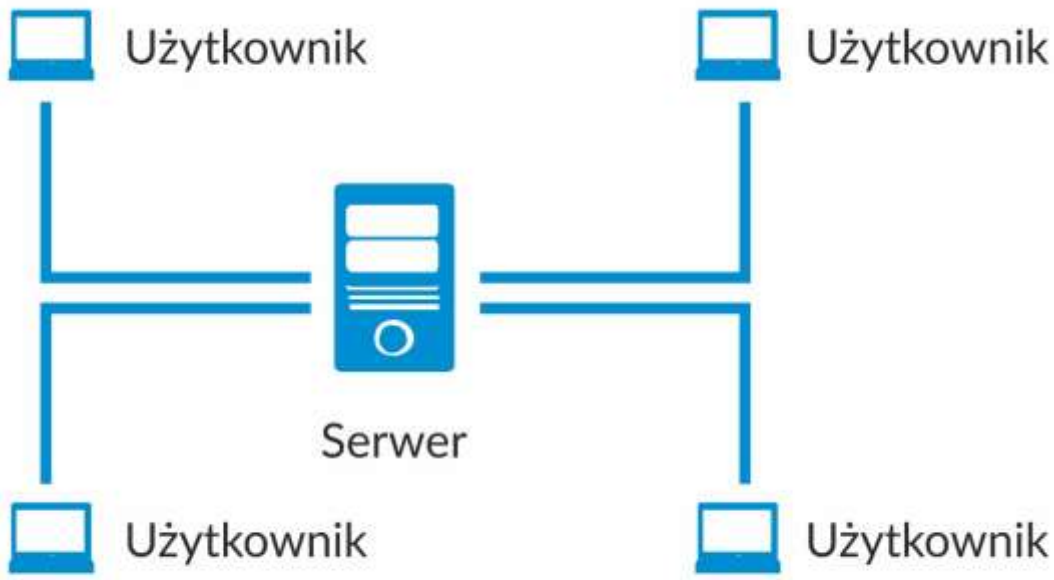
Wracając do studium przypadku dotyczącego Ransomware, możemy przeanalizować kroki, które są potrzebne, aby rozwiązać taki problem.

Przede wszystkim musisz zrozumieć, że zanim zdasz sobie sprawę, że jesteś atakowany przez takie oprogramowanie, twoje pliki (wszystkie lub niektóre z nich) będą już odszyfrowane. Jak więc zareagować?

Pierwszym krokiem jest zatrzymanie ataku. W tym celu należy odciąć dostęp zainfekowanego urządzenia do sieci. Jeśli istnieje scentralizowany katalog plików, czyli serwer z wszystkimi znajdującymi się tam dokumentami i użytkownicy podłączeni do niego z oddzielnych urządzeń, należy odciąć użytkownikowi „prawa zapisu" do tego serwera dla wszystkich użytkowników. Musisz to zrobić, ponieważ

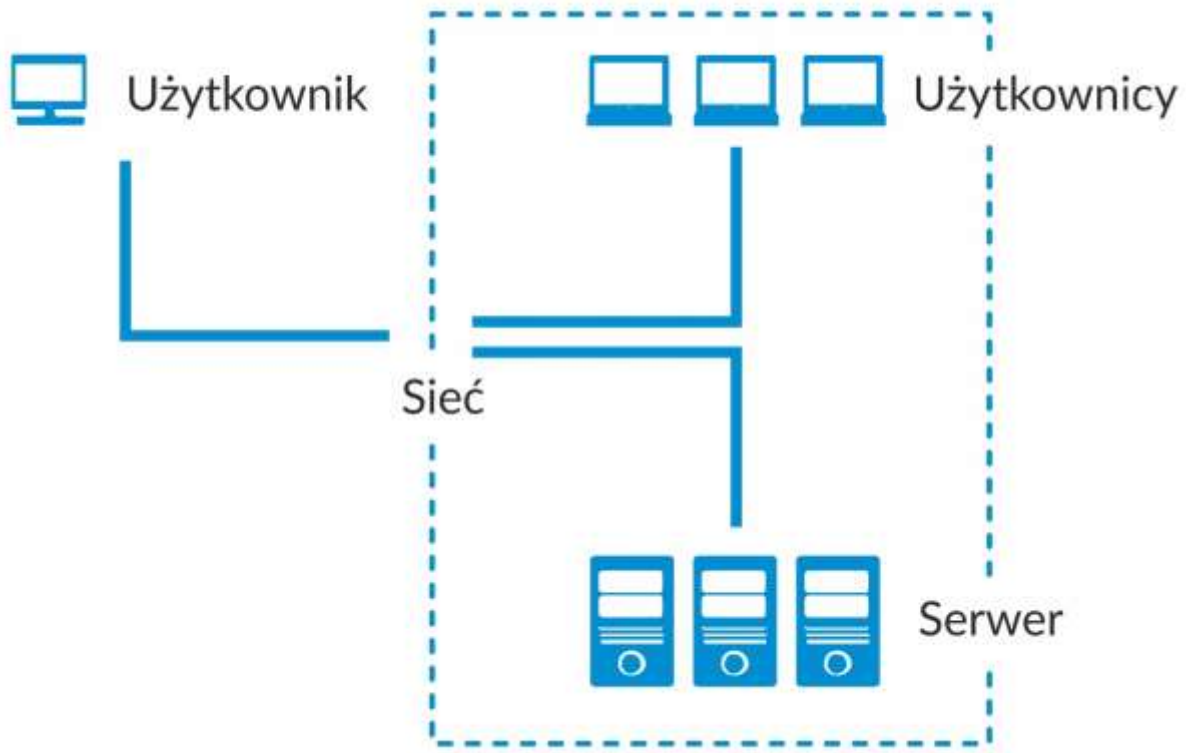
oprogramowanie Ransomware działa przez infekcję użytkownika, a więc musisz powstrzymać zainfekowanego użytkownika przed dostępem do jakichkolwiek danych na serwerze. Aby to zrobić, należy ustawić serwer jako „Tylko do odczytu”, aby żaden użytkownik nie mógł go nadpisywać. Oczywiście będzie to miało negatywny wpływ wyłączenia dostępu do zapisu dla wszystkich "niewinnych" użytkowników. Naprawdę ważne jest, aby nie wyłączać serwera. Konieczne jest uruchomienie wszystkich dostępnych ostatnio dzienników.

Musisz teraz znaleźć zainfekowanego użytkownika, aby utrzymywać dla niego ograniczenia dostępu do serwera i zezwolić innym użytkownikom na dostęp. Możesz sprawdzić, kim jest ta osoba, sprawdzając, kto ma uprawnienia do zaatakowanych plików i kto miał dostęp do nich przed atakiem. Zainfekowanego użytkownika należy poinstruować, aby natychmiast odłączył kabel ethernetowy, żeby odłączyć się od sieci (lub odłączyć od sieci Wi-Fi). Wtedy atak zostanie zatrzymany. Należy pamiętać, że użytkownik nie powinien wyłączać komputera, ponieważ mogą istnieć ważne informacje o ataku w pamięci komputera, które zostaną usunięte podczas odłączania zasilania.



Ryc. 8 - Scentralizowany katalog plików

Jeśli jesteś użytkownikiem jednego urządzenia z plikami znajdującymi się na twoim urządzeniu, usuń urządzenie z sieci, ale nie wyłączaj go z tych samych powodów, które wyjaśniono powyżej.



Ryc. 9 - Pliki zlokalizowane na jednym urządzeniu

W drugim kroku musisz ocenić wyrządzone szkody. Jeśli przestrzegasz zasady poufności, prawdopodobnie doznasz mniejszych szkód. W przypadku scentralizowanego katalogu plików oznacza to, że jeśli każdy z twoich użytkowników ma pozwolenie na dostęp tylko do kilku całkowitych danych serwera, a atakujący przeszedł przez jednego użytkownika, to tylko jego pliki zostaną uszkodzone . Jeśli przestrzegasz zasady integralności, możesz mieć pewność, które pliki zostały uszkodzone podczas ataku, porównując je z poprzednim stanem (np. ostatnią zapisaną kopią zapasową). Oceniając szkody, możesz utworzyć kopię dysku lub zainfekowanych plików do późniejszej analizy.

Trzeci i ostatni krok dotyczy odzyskiwania W tym studium przypadku w wyniku ataku ucierpiała zasada dostępności. Najlepszą praktyką jest wyczyszczenie systemu, a następnie przywrócenie wszystkich danych przy użyciu najnowszych kopii

zapasowych. Aby wyczyścić system przed przywróceniem danych, można sformatować i ponownie zainstalować system operacyjny lub spróbować zdezynfekować urządzenie, uruchamiając tryb awaryjny i rozpoczynając głębokie skanowanie oprogramowaniem antywirusowym. To nie pomoże odszyfrować danych, ale może wyczyścić system z infekcji, aby przywrócona kopia zapasowa mogła być bezpiecznie używana. Teraz możesz zrozumieć znaczenie regularnych kopii zapasowych. Stąd dostępność jawi się jako rozwiązanie. Nie zapomnij również przywrócić dostęp do serwera.

Jeśli nie masz dostępnej kopii zapasowej, oto lista niektórych rzeczy, które możesz wypróbować [30], [31]:

- wróć do momentu, w którym twój system nie był zainfekowany, jeśli to możliwe;
- spróbuj odzyskać starszą wersję plików za pomocą oprogramowania shadow explorer lub narzędzia do odzyskiwania danych;
- spróbuj zidentyfikować określony typ oprogramowania typu Ransomware (dostępne są niektóre narzędzia online) i jeśli zostanie zidentyfikowany, sprawdź, czy narzędzie deszyfrujące jest już dostępne i użyj go.

Powyższy scenariusz brzmi przerażająco, ale można go rozwiązać stosunkowo łatwo, jeśli przestrzegasz trzech zasad i rozwiązań, które omówiliśmy w tej części.

E. Lista kontrolna dotycząca cyberbezpieczeństwa

	✓
Komputery regularnie tworzą kopie zapasowe	
Systemy są regularnie i na czas aktualizowane	
Oprogramowanie antywirusowe zostało zainstalowane poprawnie i zgodnie z ocenionymi potrzebami	
Zapora została zainstalowana	
Ocena ryzyka wykonana i monitorowana	
Postępuj zgodnie z ramami bezpieczeństwa, aby stać się bezpieczniejszym	
Stwórz sieć VPN, z której użytkownicy będą korzystać w razie potrzeby	
Uzyskaj zweryfikowany bezpieczny certyfikat dla swojej witryny (https)	
Nie otwieraj stron internetowych oznaczonych jako niezabezpieczone w przeglądarce	
Używaj silnych haseł i zabezpieczaj je przed nieautoryzowanymi osobami	
Nadzoruj fizyczny dostęp do pomieszczeń i urządzeń	
Potwierdzaj tożsamość nadawcy wiadomości e-mail przed podaniem jakichkolwiek danych lub kliknięciem dowolnych plików w wiadomości e-mail	
Szyfruj wszelkie przechowywane przez siebie wrażliwe dane	

(np. za pomocą dedykowanego oprogramowania)	
Nie pobieraj niezaufanego oprogramowania	
Lista kontrolna ustawień zapory	
Używaj tych reguł, które są dozwolone w twojej zaporze sieciowej	
Sprawdzaj nagłówki pakietów	
Egzekwuj reguły	
Lista kontrolna monitorowania sieci	
Używaj szyfrowanej komunikacji do poważnych transakcji twojej firmy	
Nagrywaj i przetwarzaj ruch w sieci	
Wykrywaj znane ataki	
Wykrywaj anomalie	
Wykrywaj złośliwe ruchy	

F. Glosariusz terminologii

Zasoby: za zasoby możemy uznać wszystkie informacje, dane, urządzenia, systemy komputerowe, urządzenia i usługi, które wspierają działania związane z informacją. W ten sposób możemy włączyć do tej definicji ludzi, którzy również pracują na systemie informatycznym. W kontekście cyberbezpieczeństwa wszystkie zasoby muszą być chronione.

Zagrożenie: Każde możliwe naruszenie, które może naruszyć bezpieczeństwo i spowodować szkodę dla zasobu. Może to być celowe, przypadkowe lub nawet konsekwencją klęski żywiołowej.

Agent zagrożenia: Każda osoba lub podmiot, który celowo lub przypadkowo wyrządził szkodę w zasobach np. ktoś odłącza serwer przez pomyłkę lub uderza w niego fizycznie.

Luka w zabezpieczeniach: wada lub słabość w projektowaniu lub wdrażaniu zasobu, który może narazić go na działanie zagrożenia lub agenta zagrożenia, umożliwiając mu wykorzystanie go w celu podważenia bezpieczeństwa. Przykłady mogą się dotyczyć problemów wysokiego poziomu, takich jak słabe kopie zapasowe lub problemów niskiego poziomu, takich jak słabe kodowanie.

Exploit: wszelkie oprogramowanie lub narzędzia celowo wykorzystywane do skorzystania z luki w zabezpieczeniach w celu spowodowania nieprawidłowego działania lub zaburzenia funkcjonalności. Oczywistym przykładem mogą być narzędzia hakerskie.

Zapora sieciowa: W przypadku komputerów, zapora sieciowa to system bezpieczeństwa sieci, który monitoruje i kontroluje przychodzący i wychodzący ruch sieciowy na podstawie wcześniej określonych reguł bezpieczeństwa. Zapora zwykle ustanawia barierę między zaufaną siecią wewnętrzną a niezaufaną siecią zewnętrzną, taką jak Internet.

Ryzyko: prawdopodobieństwo, że zagrożenie wykorzysta lukę w zabezpieczeniu i spowoduje szkodę. Jak we wszystkich teoriach probabilistycznych, ryzyko może być większe lub mniejsze w zależności od wystąpienia różnych warunków. Na przykład, możemy powiedzieć, że istnieje większe ryzyko utraty niektórych danych, jeśli

istnieje tylko jedna kopia zapasowa, lub istnieje większe ryzyko, że ktoś zaatakuje serwer danych banku, zamiast atakować serwer, na którym gromadzone są zdjęcia.

Atak: dowolne celowe zdarzenie, które szkodzi lub ma zamiar zaszkodzić zasobie albo przez samo uzyskanie do nie dostępu (atak bierny), albo edytując go, niszcząc, usuwając lub nawet ujawniając go bez upoważnienia (atak aktywny). Przykładem może być atak typu DoS lub naruszenie danych.

Usterka: każde przypadkowe zdarzenie, które szkodzi zasobie, na przykład fizyczne zniszczenie sprzętu.

Zmniejszanie ryzyka: każde narzędzie, usługa lub system zmniejszające ryzyko ataku.

Kompensujący punkt kontrolny: dowolne narzędzie, usługa lub system, które zmniejszają ryzyko ataku na zasób, celowo zapobiegając zagrożeniu. Przykładem jest zapora sieciowa między Internetem a systemem komputerowym.

Osoba powiązana: osoba kluczowa mająca dostęp do informacji.

Glosariusz został stworzony przy użyciu definicji z [5] oraz [12], [13], [14], [15], [16], [20]

G. Wnioski

Utrzymanie systemu w sieci jest skomplikowanym zagadnieniem, ale można się z nim zmierzyć wdrażając określone środki ostrożności, stosując krok po kroku certyfikowane procedury i protokoły oraz stosując określone rozwiązania w przypadku wystąpienia problemu.

Co najważniejsze, wszystkie systemy powinny w każdym czasie spełniać trzy główne zasady triady CIA: poufność, integralność i dostępność. Jeśli nie możesz dokładnie potwierdzić, czy zastosowałeś triadę CIA w każdym systemie i procesie w twoim biznesie, to tak czy owak będziesz mieć w przyszłości problemy. Aby zminimalizować wszelkie przyszłe problemy i ryzyka, trzeba myśleć o zasadach na każdym etapie cyklu życia systemu, regularnie oceniać swoje bezpieczeństwo, tak aby za każdym razem stawało się ono jeszcze większe.

H. Źródła:

[1] Gasser, Morrie (1988). Building a Secure Computer System (PDF). Van Nostrand Reinhold. p. 3. ISBN 0-442- 23022-2,

[2] TechTerms - https://techterms.com/definition/vpn

[3] Denial-of-Service Attack - https://en.wikipedia.org/wiki/Denial-of-service_attack

[4]https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time

[5] Introduction to Cybersecurity for Business, University of Colorado System on Coursera, Taught by: Greg Williams, Lecturer Department of Computer Science

[6] CS682: Advanced Security Topics Course by Dr. Elias Athanasopoulos, University of Cyprus (2018, https://www.cs.ucy.ac.cy/courses/EPL682/)

[7] V-Alert Project, LLP Funded

[8] https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html

[9] https://www.techrepublic.com/article/the-top-10-worst-ransomware-attacks-of-2017-so-far/

[10] https://www.microsoft.com/en-us/download/details.aspx?id=12273

[11] https://haveibeenpwned.com

[12] https://en.wikipedia.org/wiki/Asset_(computer_security)

[13] https://en.wikipedia.org/wiki/Threat_(computer)

[14] https://en.wikipedia.org/wiki/Vulnerability_(computing)

[15] https://en.wikipedia.org/wiki/Exploit_(computer_security)

[16] https://www.techopedia.com/definition/6060/attack

[17] https://www.avg.com/en/signal/what-is-malware

[18] https://www.veracode.com/security/computer-worm

[19] https://www.eugdpr.org/

[20] https://www.techopedia.com/definition/1793/cyclic-redundancy-check-crc

[21] Furnell, S.M., Jusoh, A. &Katsabas D. (2006). The challenges of understanding and using security: A survey of end-users. Computers & Security, Vol.25: 27–35. Retrieved 10 March 2009 from http://linkinghub.elsevier.com/retrieve/pii/S0167404805002038

[22] Whitten, A. &Tygar, J.D. (2005). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In: Cranor, L. & Garfinkel, S. (Eds.), Security and usability: Designing secure systems that people can use. Sebastopol, CA: O'Reilly, pp 669–692.

[23] Flenchais, I. &Sasse, M.A. (2007). Stakeholder involvement, motivation, responsibility, communication: How to design usable security in e-Science. International Journal of Human Computer Studies. DOI:10.1016/j.ijhcs.2007.10.002

[24] https://uk.norton.com/norton-blog/2016/02/the_8_most_famousco.html

[25] https://www.nist.gov/cyberframework

[26] https://www.iso.org/isoiec-27001-information-security.html

[27] https://www.cisecurity.org/

[28] http://www.alphr.com/realworld/380632/how-to-deal-with-a-ransomware-attack

[29] http://www.thewindowsclub.com/what-to-do-after-ransomware-attack

[30] https://www.quora.com/How-do-I-use-my-computer-after-a-Ransomware-attack

[31] https://www.tomsguide.com/us/ransomware-what-to-do-next,news-25107.html

[32] The European Union Agency for Network and Information Security (ENISA), Threat Landscape Report 2017, January 2018, p. 31-35

[33] https://en.wikipedia.org/wiki/Drive-by_download, access 27.01.2018

[34] https://en.wikipedia.org/wiki/Watering_hole_attack, access 27.01.2018

[35]https://www.rsa.com/content/dam/rsa/PDF/Making_Sense_of_Man_in_the_browser_attacks.pdf, access 27.01.2018

[36] The European Union Agency for Network and Information Security (ENISA), Threat Landscape Report 2017, January 2018, p. 36-39

[37] https://en.wikipedia.org/wiki/SQL_injection, access 27.01.2018

[38] https://www.acunetix.com/blog/articles/local-file-inclusion-lfi/, access 27.01.2018

[39] https://www.acunetix.com/websitesecurity/cross-site-scripting/, access 27.01.2018

[40] https://blog.udemy.com/php-injection/, access 27.01.2018

[41] https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos, access 27.01.2018

[42] The European Union Agency for Network and Information Security (ENISA), Threat Landscape Report 2017, January 2018, p. 45-48

[43] Zulfikar Ramzan, Phishing attacks and countermeasures, Mark Stamp, Peter Stavroulakis, Handbook of Information and Communication Security, Springer, https://books.google.com/books?id=I-9P1EkTkigC&pg=PA433, p. 433-447

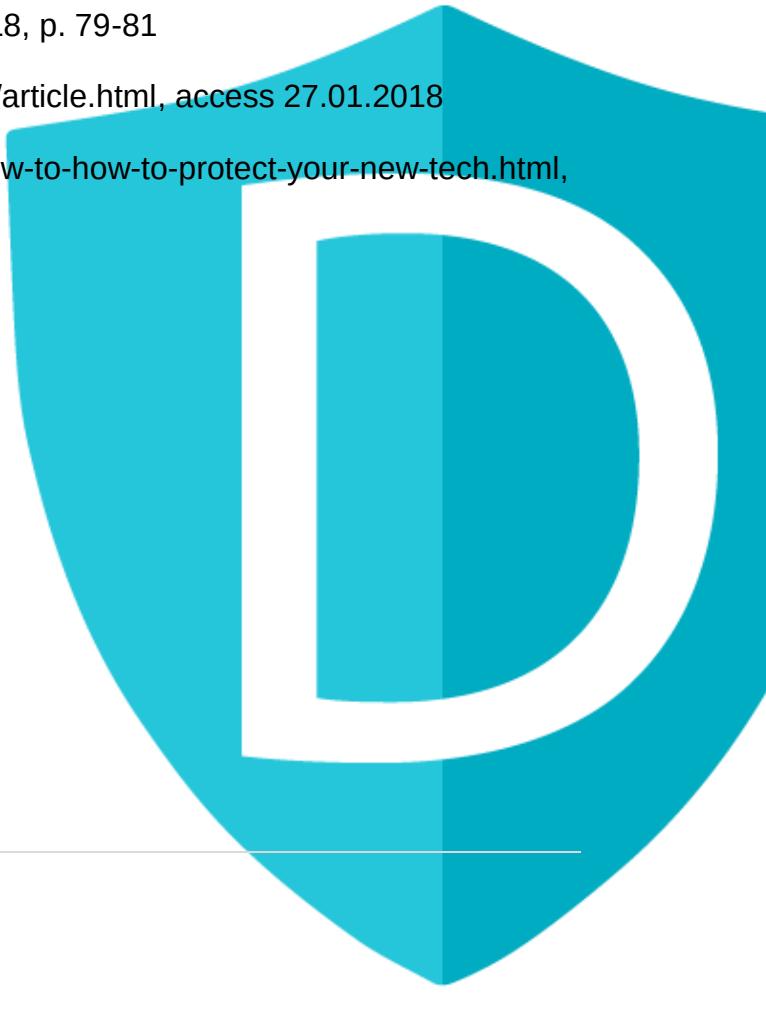
[44] The European Union Agency for Network and Information Security (ENISA), Threat Landscape Report 2017, January 2018, p. 64-67

[45] https://www.lifelock.com/education/how-common-is-identity-theft/, access 27.01.2018

[46] The European Union Agency for Network and Information Security (ENISA), Threat Landscape Report 2017, January 2018, p. 79-81

[47] https://www.pcworld.com/article/141474/article.html, access 27.01.2018

[48] https://us.norton.com/internetsecurity-how-to-how-to-protect-your-new-tech.html, access 27.01.2018



CZĘŚĆ V

OCENA RYZYKA W ZAKRESIE CYBERBEZPIECZEŃSTWA

Spis zastosowanych skrótów

Skrót	Rozwinięcie
DDoS	Rozproszona odmowa usługi (ang. Distributed Denial of Service)
DoS	Odmowa usługi (ang. Denial of service)
ICT	Technologie informacyjno-komunikacyjne
LFI	Local File Inclusion
PHPi	PHP injection or PHP Object Injection
RFI	Remote File inclusion
SQLi	SQL Injection attacks
XSS	Cross-site Scripting

A. Wstęp

W ciągu ostatnich lat znacznie wzrosły cyfrowe zagrożenia bezpieczeństwa i różne incydenty związane z bezpieczeństwem cyfrowym. Te różne zagrożenia i incydenty związane z bezpieczeństwem cyfrowym powodują realne konsekwencje, zarówno gospodarcze, jak i społeczne, dla sektora publicznego, organizacji prywatnych, nie wspominając o osobach fizycznych. Można podać różne przykłady tych konsekwencji, takie jak: straty finansowe, utrata klientów i/lub zaufania partnerów, uszkodzenie reputacji organizacji, nieporządek w działaniach organizacyjnych itp. Obecnie działalność gospodarcza jest silnie powiązana i opiera się na danych. Technologie informacyjne i komunikacyjne (ICT), a zwłaszcza Internet, mają obecnie zasadnicze znaczenie dla funkcjonowania gospodarki. Rządy, organizacje publiczne i prywatne, osoby fizyczne są dziś uzależnione, w taki czy inny sposób, od narzędzi cyfrowych. Takie kwestie, jak „wielkie dane" i "Internet przedmiotów", zapewniają duży potencjał innowacji w zakresie produktów i usług. Ale mają również wpływ na skalę i zakres bezpieczeństwa cyfrowego. Nie wspominając o liczbie zhakowanych stron internetowych każdego dnia i liczbie wirusów tworzonych każdego miesiąca. Potrzebne są strategie zarządzania bezpieczeństwem cyfrowym, które mają zasadnicze znaczenie dla działalności gospodarczej i społecznej. W związku z tym wdrożenie procedur oceny ryzyka może zapewnić bezpieczeństwo cyfrowe zarówno w działalności gospodarczej, jak i społecznej.

Ocena ryzyka jest procesem identyfikowania, analizowania i oceny potencjalnych zagrożeń, na które może napotkać organizacja i wpływać na jej zdolność do prowadzenia działalności. Ocena ryzyka powinna również zapewniać środki, procesy i kontrole, aby zminimalizować wpływ tych zagrożeń na bieżące i przyszłe operacje gospodarcze [1]. Aby móc przeprowadzić ocenę ryzyka, organizacja musi zidentyfikować potencjalne ryzyko i określić prawdopodobieństwo takich zagrożeń. Ocena ryzyka jest przydatna, gdy mamy do czynienia z planowaniem projektów, poprawą bezpieczeństwa miejsca pracy, przygotowywaniem wydarzeń, planowaniem zmian w swoim środowisku (nowi konkurenci, zmiany w polityce rządu) itp. [2].

Gospodarka cyfrowa pozwala organizacjom powiększać się i rozwijać się, ale także z powodu szybkiego tempa technologii, powoduje nowe wyzwania związane z bezpieczeństwem i prywatnością. Cyfrowe zagrożenia bezpieczeństwa stanowią

problem zarówno dla mniejszych podmiotów, jak i dużych organizacji. Dlatego ocena ryzyka jest również jedynym sposobem, aby upewnić się, że wybrane kontrole cyberbezpieczeństwa pasują do ryzyka, przed którym stoi organizacja. W ocenie ryzyka organizacja szacuje prawdopodobieństwo wystąpienia ryzyka i koszty dla organizacji w przypadku wystąpienia ryzyka [3]. Ocena ryzyka bezpieczeństwa cyfrowego zapewnia, że czas, wysiłek i zasoby nie są marnowane na wdrażanie metod ochrony przed zagrożeniami, które są mało prawdopodobne lub nie będą miały znaczącego wpływu na organizację [4].

Ekosystem cyfrowy jest obecnie niezbędny dla gospodarki, a ze względu na incydenty związane z bezpieczeństwem cyfrowym na dużą skalę, OECD twierdzi, że prezesi firm i rządy państw powinni traktować cyfrowe bezpieczeństwo jako ekonomiczne ryzyko: "Ryzyko związane z bezpieczeństwem cyfrowym należy traktować raczej jako kwestię ekonomiczną niż techniczną (...)" [5]. Oznacza to, że ważne jest zintegrowanie oceny ryzyka bezpieczeństwa cyfrowego w ogólnym zarządzaniu ryzykiem w organizacji i procesami decyzyjnymi.

Głównym celem tego rozdziału jest dostarczenie pełnego przeglądu podejść do oceny ryzyka cyfrowego, które powinny być przestrzegane przez potencjalnych i obecnych młodych przedsiębiorców w ich cyfrowych przedsięwzięciach biznesowych oraz aby podkreślić znaczenie wdrożenia strategii oceny ryzyka bezpieczeństwa cyfrowego w przedsięwzięciach internetowych.

Celem tej części jest wyposażenie potencjalnych i obecnych młodych przedsiębiorców w praktyczną wiedzę na temat aspektów technicznych (bezpieczeństwo cyfrowe jako ryzyko techniczne), a także aspektów ekonomicznych (bezpieczeństwo cyfrowe jako ryzyko ekonomiczne) bezpieczeństwa cyfrowego. Niniejsza część zawiera przegląd zalet i wad wynikających z wdrożenia lub niewdrożenia oceny ryzyka bezpieczeństwa cyfrowego.

Przedstawiono również praktyczne porady i nakreślono przykłady dobrych praktyk dotyczących planowania i przeprowadzania oceny ryzyka bezpieczeństwa cyfrowego. Niniejsza część zawiera również przykłady, jak strategia cyfrowej oceny ryzyka dla bezpieczeństwa działa i jak powinna być wdrażana na poziomie organizacyjnym, aby być częścią ogólnego zarządzania ryzykiem i procesów

decyzyjnych organizacji. Ponadto wskazano możliwe niedociągnięcia i luki, których należy unikać, a także sposoby ich przezwyciężenia.

Ta część zawiera obszerny słownik terminologiczny, a także listę kontrolną do oceny ryzyka bezpieczeństwa cyfrowego, ponieważ są one niezbędne, aby uzyskać pełną wiedzę na temat prezentowanego tematu.

B. Bezpieczeństwo cyfrowe jako ryzyko techniczne

Mając na uwadze znaczenie oceny ryzyka bezpieczeństwa cyfrowego oraz potrzebę, aby ocena ryzyka bezpieczeństwa cyfrowego była częścią ogólnego zarządzania ryzykiem i procesów decyzyjnych organizacji, w niniejszej sekcji skupimy się na wymiarze technicznym, ponieważ ocena ryzyka bezpieczeństwa cyfrowego ma zarówno wymiar techniczny, jak i ekonomiczny. W tej sekcji opisano różne ryzyka techniczne związane z bezpieczeństwem cyfrowym oraz wybór odpowiednich mechanizmów kontroli w celu rozpoznania zidentyfikowanego ryzyka. Treść jest zorganizowana w oparciu o przeciwstawne zestawienie zalet i wad w wyniku wdrożenia / niewdrożenia takich strategii.

Istnieje wiele zagrożeń cyfrowych dla biznesu i organizacji, które mogą wynikać z różnych branż i sektorów i mogą być różnej wielkości, a także z różnym zaawansowaniem zabezpieczeń. Jednak wszystkie rządy, organizacje publiczne i prywatne, a także osoby fizyczne, muszą zarządzać ryzykiem cyfrowym i łagodzić je. Bezpieczeństwo cyfrowe jako ryzyko techniczne powinno również mieć wielkie znaczenie dla potencjalnych i obecnych młodych przedsiębiorców w ich cyfrowych przedsięwzięciach biznesowych. Ryzyko techniczne stwarza zagrożenia dla przedsiębiorstw, takie jak utrata aktywów gospodarczych i nadszarpnięcie ich reputacji.

W tej sekcji opisano różne ryzyka techniczne związane z bezpieczeństwem cyfrowym, związane z: złośliwym oprogramowaniem, atakami sieciowymi, atakami na aplikacje internetowe, Phishingiem, spamem, odmową usługi, oprogramowaniem Ransomware, botnetami, zagrożeniami wewnętrznymi, manipulacją fizyczną, naruszeniem bezpieczeństwa danych, kradzieżą tożsamości, wyciekiem informacji, zestawami exploitów, cyber-szpiegostwem, które zostały już opisane w poprzedniej części zatytułowanej „Cyberbezpieczeństwo”.

Wymienione powyżej różne rodzaje ryzyka technicznego to zbiór aktualnych zagrożeń z 2017 r., oparty na Raporcie o zagrożeniach w 2017 roku wydanym przez Agencję Zagrożeń Sieci i Informacji (ENISA) [6].

Znając definicję złośliwego oprogramowania, dostępną w rozdziale „Cyberbezpieczeństwo” i popularnych typów złośliwego oprogramowania, takich jak: wirusy (które infekują pliki programów i/lub pliki osobiste), robaki (które mogą się replikować w sieci), programy szpiegujące i programy rejestrujące naciśnięcia klawiszy (które zbierają dane osobowe użytkownika), konie trojańskie (które wyglądają i mogą nawet działać, jako legalne oprogramowanie), rootkity (które uzyskują prawa administracyjne do systemu operacyjnego w celu złośliwego działania), porywacze przeglądarki (co modyfikuje ustawienia przeglądarki internetowej), malvertising (wykorzystanie legalnych systemów reklamowych online w celu rozprzestrzeniania złośliwego oprogramowania), przejdźmy do opisania różnych ryzyk technicznych związanych z nimi aspektów bezpieczeństwa cyfrowego [7].

Gdy wymienione powyżej zagrożenia występują na urządzeniu lub są przesyłane przez sieć, mogą wydrenować z informacji urządzenie lub zasoby sieciowe i spowolnić połączenie internetowe. Istnieją również inne zagrożenia techniczne wynikające z tych zagrożeń, ponieważ złośliwe oprogramowanie może:

- niszczyć lub uszkadzać pliki osobiste lub biznesowe,
- dezaktywować oprogramowanie antywirusowe lub nawet utrudniać działanie przeglądarki, aby uniemożliwić pobieranie narzędzi do usuwania wirusów,
- zbierać skróty klawiaturowe, które mogą służyć do przechwytywania numerów kart kredytowych i haseł,
- przechwytywać przeglądarkę lub urządzenie w celach złośliwych lub komercyjnych lub skierowania użytkownika na stronę internetową, która próbuje nakłonić go do wprowadzenia haseł na swoich kontach,
- wysyłać swoje kopie na twoje kontakty mailowe [8].

Poniżej znajduje się lista najważniejszych mechanizmów kontrolnych, które zapobiegają zidentyfikowanym zagrożeniom pochodzącym od złośliwego oprogramowania:

- używaj wyłącznie licencjonowanych kopii oprogramowania i/lub oprogramowania pochodzącego ze znanych i zaufanych źródeł,

- instaluj tylko oprogramowanie, które jest potrzebne na urządzeniu, ponieważ dodatkowe nieużywane oprogramowanie powoduje dodatkowe zagrożenie,
- przechowywać oryginalne kopie oprogramowania w bezpiecznym miejscu,
- regularnie wykonuj kopię zapasową plików i systemu i przechowuj kopie w bezpiecznym miejscu,
- regularnie aktualizuj: system operacyjny, przeglądarkę internetową, definicje antywirusowe, oprogramowanie antyszpiegowskie, wszelkie inne zainstalowane oprogramowanie,
- nie używaj oprogramowania, dysków, przenośnych dysków itp. z systemów domowych.

Ataki na sieć internetową, które korzystają z systemów i usług internetowych, są również opisane w części „Cyberbezpieczeństwo". Po przeczytaniu poprzedniej części znasz już różne typy tych ataków, tj.: exploity przeglądarki internetowej (złośliwy kod wykorzystujący lukę w systemie operacyjnym lub zainstalowane oprogramowanie), exploity serwerów internetowych i usług internetowych (wykorzystujące błąd lub wrażliwość serwera internetowego lub usług internetowych), ataki drive-by (niezamierzone pobieranie oprogramowania komputerowego z Internetu), ataki metodą wodopoju (infekowanie wybranych stron internetowych złośliwym oprogramowaniem), ataki typu „człowiek w przeglądarce" (przechwytywanie poufnych informacji i danych). Teraz możemy opisać różne zagrożenia techniczne w odniesieniu do tego aspektu bezpieczeństwa cyfrowego:

- exploity do przeglądarek internetowych mogą wykonywać na przykład fałszowanie paska adresu, co oznacza, że użytkownik widzi zaufany adres URL (na przykład bank internetowy) na pasku, ale zawartość witryny jest kontrolowana przez atakującego. Może to służyć do kradzieży danych logowania i dostępu [9],
- exploity serwerów internetowych i usług internetowych mogą na przykład korzystać z luki Cross Site Scripting, co oznacza, że osoba atakująca może wykonać złośliwe skrypty w legalnej witrynie lub aplikacji sieciowej. Może to

służyć do zbierania danych ze strony, przejęcia sesji użytkownika, przekierowania użytkowników, zebrania informacji o użytkowniku przeglądającym witrynę [10],

- ataki typu drive-by mogą instalować keyloggery, oprogramowanie Ransomware na urządzeniu lub nawet tworzyć backdoory, które umożliwią atakującemu zainstalowanie jeszcze większej ilości złośliwego oprogramowania. Może to służyć do szyfrowania danych na urządzeniu i żądania okupu oraz zbierania naciśnięć klawiszy lub wyszukiwania haseł, informacji o koncie i innych poufnych informacji w celu uzyskania nieautoryzowanego dostępu lub przeprowadzenia nieautoryzowanych transakcji [11],
- ataki metodą wodopoju są wykorzystywane do atakowania profilowanej grupy użytkowników za pomocą złośliwego kodu w celu kradzieży danych lub przejęcia kontroli nad systemami organizacji, branży lub w regionie (grupa profilowana). Może to prowadzić do zagrożeń w wielu organizacjach, w tym w służbie zdrowia, technologiach, edukacji, administracji itp. [12],
- ataki typu "człowiek w przeglądarce" są często wykorzystywane do kradzieży jednorazowych kodów haseł (SMS), które banki używają do uwierzytelniania przelewów pieniężnych użytkownika. Kiedy urządzenie jest zainfekowane trojanem typu „człowiek w przeglądarce”, a użytkownik przechodzi do witryny bankowości internetowej, ta sesja uruchamia trojana, który może zmienić numer konta i/lub kwotę przelewu bankowego, jednocześnie wyświetlając użytkownikowi stronę internetową zawierającą uzasadnienie i szczegóły transakcji [13].

Jak widać powyżej ataki internetowe są często wykorzystywane do kradzieży danych logowania, haseł i innych informacji dostępowych / jednorazowych kodów hasłowych w celu uzyskania nieautoryzowanego dostępu do systemów lub przeprowadzenia nieautoryzowanych transakcji za pośrednictwem bankowości internetowej. Powodują one poważne zagrożenie zarówno dla użytkowników, jak i organizacji, dlatego ważne jest, aby podjąć odpowiednie działania kontrolne w celu zapobiegania i ograniczania zidentyfikowanych zagrożeń. Oto, co możesz zrobić, aby zapobiegać i ograniczać te zagrożenia:

- instaluj oprogramowanie antywirusowe oraz antyszpiegowskie i aktualizuj je,
- zawsze aktualizuj swój system operacyjny i przeglądarkę internetową,

- konfiguruj opcje bezpieczeństwa w przeglądarce internetowej (na przykład: skorzystaj z wyskakującego okienka, nie zapisuj swoich haseł i informacji o formularzu),
- korzystaj z Internetu jako użytkownik zalogowany na komputerze, który nie ma praw administracyjnych,
- przeglądaj wiadomości e-mail w postaci zwykłego tekstu, a nie w widoku HTML,
- korzystaj z pre-paidowej karty kredytowej przy zakupach w Internecie,
- nie korzystaj z bankowości internetowej na niezaufanych urządzeniach lub sieciach,
- wpisuj adres strony internetowej ręcznie i nie zawsze ufaj paskowi statusu [14].

Popularność takich zasobów i projektów opartych na otwartym kodzie źródłowym lub źródłach publicznych, takich jak wtyczki Joomla i Wordpress, witryny Magento itp., ma również duże znaczenie z punktu widzenia bezpieczeństwa cyfrowego. Jak już wiesz z części „Cyberbezpieczeństwo" ataki na aplikacje internetowe najczęściej dotyczą interfejsów programowania aplikacji (API). Tam możesz również przeczytać więcej o rodzajach takich ataków: Injection SQL (SQLi - technika wprowadzania kodu), Local/Remote File Inclusion (LFI/RFI - aplikacja internetowa zawierająca pliki na serwerze www), Cross-site Scripting (XSS - uruchamianie złośliwych skryptów, w legalnej witrynie), PHP Injection lub PHP Object Injection (PHPi - robienie różnego rodzaju złośliwych ataków).

Aplikacje internetowe nie są już ograniczone do przedstawiania tylko tekstu i obrazów, tak jak papierowa broszura. Zagrożenia bezpieczeństwa aplikacji internetowych mogą stanowić bezpośrednie zagrożenie dla organizacji, ponieważ obecnie wszyscy użytkownicy prywatni i biznesowi codziennie korzystają z aplikacji internetowych. Aplikacje internetowe są kluczowymi narzędziami umożliwiającymi prywatnym użytkownikom, organizacjom, klientom, a nawet krajom komunikację, dostęp i przetwarzanie informacji. Informacje te mogą obejmować na przykład: informacje finansowe, dokumentację medyczną, dane dotyczące bezpieczeństwa narodowego, itp. [15].

Oto kilka technicznych zagrożeń związanych z tym aspektem bezpieczeństwa cyfrowego:

- naruszenie mechanizmów ochrony systemu,
- przechwytywanie informacji, które nie powinny być dostępne poza aplikacją i/lub organizacją (np. własność intelektualna),
- uzyskanie nieautoryzowanego dostępu do aplikacji internetowych i przechowywanych danych (na przykład: nazwiska, numery kart kredytowych i wszelkie inne poufne i wrażliwe dane handlowe),
- szpiegowanie przeglądarki (manipulowanie plikami cookie może pozwolić nieautoryzowanemu użytkownikowi udawać autoryzowanego użytkownika),
- podniesienie uprawnień do autoryzowanego użytkownika,
- kradzież tożsamości, kradzież usług lub treści oraz oszustwo związane z kartami kredytowymi,
- odmowa usługi.

Ponieważ aplikacje internetowe ewoluowały, a zabezpieczanie aplikacji internetowych stało się ważne, musimy wymienić najważniejsze odpowiednie mechanizmy kontrolne, aby zapobiegać zidentyfikowanym ryzykom i je ograniczać:

- konieczny jest program zarządzania ryzykiem, a zasady i procedury powinny powstrzymać wdrażanie aplikacji internetowych z lukami,
- szkolenie programistów w zakresie bezpiecznych metod kodowania,
- aplikacje internetowe muszą być testowane przez profesjonalnych testerów bezpieczeństwa przed ich wdrożeniem [16],
- aktualizowanie poprawek zabezpieczeń dla serwerów i aplikacji internetowych,
- korzystanie z systemów wykrywania włamań (ang. Intrusion Detection Systems - IDS) i systemów zapobiegania włamaniom (ang. Intrusion Prevention Systems - IPS),
- korzystanie z zaawansowanych zapór sieciowych (które oferują możliwość odrzucania szkodliwych pakietów),

- skanowanie pod kątem luk w kodowaniu po zbudowaniu aplikacji za pomocą specjalistycznego oprogramowania,
- używanie skanerów serwerów www do wyszukiwania niebezpiecznych plików na serwerach internetowych. [15].

Ważne jest również podkreślenie, że takie kwestie jak:

- osierocone aplikacje internetowe (opracowane przez zespoły, które nie są już w firmie lub aplikacje internetowe, które nie są już aktualizowane),
- starsze aplikacje sieciowe (stare aplikacje internetowe tworzone przed wdrożeniem zasad bezpieczeństwa),
- krótki czas wdrożenia na rynek aplikacji internetowych,
- niestandardowe aplikacje internetowe (aplikacje internetowe opracowywane przez firmę są narażone na wysoki błąd ludzki),
- prowadzą do zwiększenia ryzyka zagrożenia bezpieczeństwa aplikacji internetowych [17].

Ponieważ wyłudzanie informacji jest niestety bardzo popularnym oszustwem internetowym, ważne jest włączenie **Phishingu** do oceny ryzyka bezpieczeństwa cyfrowego.

Udany atak Phishingowy może prowadzić do takich technicznych zagrożeń, jak:

- używanie twojego komputera do instalowania wirusów i robaków,
- wysyłanie wiadomości Phishingowych do wszystkich kontaktów e-mailowych,
- wykorzystanie skradzionych danych w celu uzyskania dostępu do systemu organizacji, naruszenie mechanizmów ochrony systemu,
- wykorzystywanie skradzionych danych osobowych do otwierania fałszywych kont bankowych lub kart kredytowych, a następnie wykorzystywanie ich w nielegalnych transakcjach,
- korzystanie z konta bankowego online do dokonywania przelewów bankowych lub zakupów on-line.

Powyższe ryzyka techniczne mogą prowadzić do takich zagrożeń gospodarczych, jak: straty finansowe i szkody wizerunkowe.

Aby zmniejszyć powyższe zagrożenia, należy wdrożyć następujące środki:

- zidentyfikować działy, które najprawdopodobniej mogą zostać dotknięte przez Phishing,
- opracować plan ochrony i przeciwdziałania Phishingowi,
- przekazywać plan zarówno pracownikom organizacji, jak i podmiotom zewnętrznym (partnerom, klientom itp.),
- przeszkolić swoich pracowników [18].

Spam może być wysyłany przez botnety lub zainfekowane wirusem komputery, ale spam jest także problemem w mediach społecznościowych, takich jak: Facebook, Twitter i LinkedIn. Dzięki atakom spamowym na media społecznościowe można uzyskać dostęp do stron profilu użytkownika, na których można umieszczać niepokojące linki, obrazy lub filmy. Spam jest również problemem w komunikatorach w mediach społecznościowych. Możemy zauważyć, że spamerzy przenoszą swoją aktywność z poczty e-mail do mediów społecznościowych. Więc jakie są techniczne zagrożenia ze strony spamu:

- infekowanie komputerów, aplikacji internetowych, serwerów i sieci za pomocą wirusów i/lub złośliwego kodu,
- wiadomości spamowe zajmują miejsce na serwerach pocztowych,
- wiadomości spamowe mogą generować dużą liczbę żądań serwera, a czasami mogą nawet spowodować awarię serwera, pozostawiając organizację bez poczty elektronicznej,
- urządzenia zainfekowane za pomocą spamu mogą stać się częścią botnetu, uruchamiać złośliwe oprogramowanie, wysyłać spam lub brać udział w atakach typu DDoS (rozproszona odmowa usługi).

Organizacje mogą chronić się przed spamem i różnymi negatywnymi skutkami spamu poprzez:

- używanie silnika antyspamowego na swoich serwerach pocztowych i aktualizowanie na bieżąco. Silnik antyspamowy powinien skanować wszystkie przychodzące i wychodzące wiadomości e-mail pod kątem spamu i złośliwego oprogramowania,
- mechanizm antyspamowy powinien wykorzystywać takie techniki, jak: filtrowanie reputacji lub dopasowywanie wzorców do wykrywania nowych i pojawiających się kampanii,
- ustawianie alertów, gdy serwer pocztowy organizacji stał się częścią botnetu, aby zapewnić korzystanie z infrastruktury organizacji tylko w uzasadniony sposób [19],
- także użytkownicy powinni być przeszkoleni, aby: nie odpowiadać na wiadomości spamowe, nie klikać żadnych linków ani pobierać / otwierać plików w wiadomościach spamowych, nie przekazywać wiadomości od kogoś, kogo nie znają, używać filtra antyspamowego, zgłaszać spam [20],
- w mediach społecznościowych nie powinieneś używać aplikacji, którym nie ufasz, uważać na podejrzane linki zamieszczane w mediach społecznościowych lub wysyłane przez komunikatory,
- zawsze usuwaj aplikacje na koncie społecznościowym, których nie znasz,
- usuń wszystkie posty / wiadomości wysłane przez ciebie lub w twoim imieniu przez aplikacje i powiadom kontakty, do których zostały przesłane, że prawdopodobnie jest to spam [21].

Ponieważ większość organizacji korzysta z aplikacji internetowych i infrastruktur serwerowych w swoich zwykłych operacjach, ochrona aplikacji internetowych i serwerów przed atakami typu DoS i DDoS jest czymś, o co organizacje muszą się zatroszczyć. Ataki typu DoS lub DDoS odmawiają pracownikom, członkom lub posiadaczom kont, a więc rzeczywistym uzasadnionym użytkownikom, usługi lub zasobu. Ale te ataki niosą za sobą również inne techniczne ryzyko:

- wysoka przepustowość lub zużycie energii obliczeniowej,

- koncentrują one personel IT na rozwiązaniu tego problemu, ponieważ atakujący może przeprowadzić inny atak, chcąc na przykład ukraść dane,

jak również pozatechniczne ryzyka związane z utratą przychodów i szkodą dla reputacji organizacji [22].

Jaka powinna być reakcja na atak typu DoS i DDoS oraz jak zmniejszyć ryzyko takich ataków:

- pochłonięcie ataku, za pomocą zapory sieciowej, jest najprostszą reakcją,
- możliwość ograniczenia: ruchu przychodzącego z określonych regionów IP, liczby koszyków, które użytkownicy mogą tworzyć, liczby zapytań do wyszukiwania w witrynie,
- tworzenie stron internetowych, aplikacji internetowych i systemów bardziej wydajnych pod względem mocy obliczeniowej,
- zachęcanie do stosowania najlepszych praktyk w zakresie kodowania (na przykład, aby zachować bezpieczeństwo przed zalewaniem witryny masą zapytań),
- używanie narzędzi do monitorowania, analizowania ruchu przychodzącego i identyfikacji złośliwych żądań,
- zgłębienie informacji z wyprzedzeniem, jakie środki oferuje usługodawca, firma zajmująca się hostingiem internetowym podczas ataku DoS / DDoS [23].

W części „Cyberbezpieczeństwo”, a także na początku tej części, pojawiło się słowo „botnet". Ale jakie są zagrożenia techniczne wynikające z tego zagrożenia - gdy urządzenie jest zainfekowane:

- boty wyczerpują moc obliczeniową urządzenia lub zasoby sieciowe, aby wykonać zadania atakującego,
- wysokie zużycie przepustowości,
- kradzież wrażliwych danych.

jak również nietechniczne ryzyko związane z wysokimi kosztami przepustowości i szkodą dla reputacji organizacji, zarówno gdy infrastruktura działa lub jest celem botnetu.

Organizacje mogą podejmować różne środki w celu zapobiegania zagrożeniom ze strony botnetów:

- monitorowanie wydajności sieci i ruchu w sieci w celu wykrycia nieregularnego zachowania sieci,
- wszystkie sieci, serwery i urządzenia powinny być regularnie aktualizowane,
- używanie narzędzi anty-botnetowych (zapory sieciowe, oprogramowanie antywirusowe, pakiety wykrywania rootkitów, sniffery sieciowe i specjalistyczne programy antywirusowe) do znajdowania i blokowania wirusów botów,
- szybkie usuwanie wirusów z botów i eliminowanie luk w zabezpieczeniach,
- także użytkownicy powinni być przeszkoleni: nie klikać żadnych linków ani pobierać/otwierać plików w wiadomościach spamowych [24].

Kolejnym zagrożeniem w cyberbezpieczeństwie są **zagrożenia wewnętrzne**, którymi również zajmowaliśmy się w części „Cyberbezpieczeństwo". Dlaczego te zagrożenia są tak ważne? Jest wiele powodów, ale powinniśmy wspomnieć przynajmniej: o tym, że

- ciężko jest wykryć umyślne działania, ponieważ trudno odróżnić je od niegroźnej działalności - regularnej pracy pracowników,
- zazwyczaj złośliwi pracownicy wiedzą, jak ukryć swoje działania, co utrudnia udowodnienie ich winy (będą próbowali wyjaśnić, że to był błąd).

Jak wykryć takich złośliwych pracowników:

- pracownicy pobierający dane na dyski zewnętrzne,
- pracownicy uzyskujący dostęp do danych niezwiązanych z ich pracą,
- pracownicy wysyłający dane do osobistych kont e-mailowych,
- pracownicy żądający dostępu na wyższym poziomie bez uzasadnienia tego,

- pracownicy często przebywający w biurze poza godzinami pracy,
- pracownicy naruszający zasady organizacji,
- pracownicy nadmiernie korzystający z drukarek i skanerów,
- pracownicy instalujący oprogramowanie niezwiązane z ich pracą,
- pracownicy próbujący uzyskać dostęp do obszarów o ograniczonym dostępie [25].

Naruszenie danych i **kradzież tożsamości**, jako szczególny przypadek naruszenia bezpieczeństwa danych, sąpoważnymi konsekwencjami wielu z wyżej wymienionych problemów związanych z zagrożeniami bezpieczeństwa cyfrowego. Oba tematy zostały poruszone w części „Cyberbezpieczeństwo". W tej sekcji przedstawimy wybrane środki kontroli, aby zapobiec tym zagrożeniom, tj.:

- opracowanie i wdrożeni planu ochrony przed utratą danych,
- edukowanie pracowników w zakresie przetwarzania i ochrony danych, zapewnienie im również wsparcie techniczne,
- nie gromadź danych, których nie potrzebujesz
- nie przechowuj danych w wielu miejscach,
- zawsze aktualizuj aplikacje i systemy,
- pamiętaj, że szyfrowanie danych nie powinno być jedyną metodą obrony,
- wymagaj tych samych standardów od dostawców i partnerów [26].

Należy również zwrócić szczególną uwagę na zmniejszenie ryzyka zostania ofiarą kradzieży tożsamości, a więc powinieneś:

- zmniejszyć liczbę posiadanych kart kredytowych i debetowych,
- zmniejszyć liczbę instytucji finansowych, z których usług korzystasz,
- używać prepaidowej karty w czasie zakupów online,
- nigdy nie podawać numeru karty kredytowej lub debetowej, danych osobowych, itp. przez telefon, pocztę lub przez niezabezpieczone strony internetowe,

- skontaktować się z wystawcą swojej karty kredytowej lub debetowej, kiedy spodziewasz się nowej lub ponownie wydanej karty, tak aby nie znajdowała się ona w twojej skrzynce pocztowej,
- corocznie sprawdzaj swoje raporty kredytowe [27].

Niestety, nie możesz się całkowicie zabezpieczyć, a jeśli złodziej chce ukraść twoje informacje, jego szanse i tak są bardzo wysokie [28].

C. Bezpieczeństwo cyfrowe jako ryzyko ekonomiczne

Znając techniczny wymiar ryzyka związanego z bezpieczeństwem cyfrowym, jego ekonomiczny wymiar wymaga dalszego omówienia. W tej sekcji wyjaśniono wpływ bezpieczeństwa cyfrowego na wymiar ekonomiczny, ponieważ takie specjalne ukierunkowanie na działalność gospodarczą i społeczną jest potrzebne, zamiast patrzeć na ryzyko wyłącznie z perspektywy infrastruktury cyfrowej.

Aspekt ekonomiczny bezpieczeństwa cyfrowego powinien również być bardzo interesujący dla potencjalnych i obecnych młodych przedsiębiorców w ich cyfrowych przedsięwzięciach biznesowych, ponieważ powinno być ono traktowane jako kwestia ekonomiczna, a nie wyłącznie techniczna. Oznacza to, że ważne jest zintegrowanie procedur oceny ryzyka cyfrowego w ogólnym zarządzaniu ryzykiem w organizacji i procesami decyzyjnymi. Wszystkie zainteresowane strony, w tym potencjalni i obecni młodzi przedsiębiorcy, powinni mieć świadomość, że zagrożenia bezpieczeństwa cyfrowego mogą wpływać na osiągnięcie ich celów gospodarczych i społecznych. W szczególności potencjalnym i obecnym młodym przedsiębiorcom należy zapewnić możliwość kształcenia i nabycia umiejętności niezbędnych do zrozumienia tego ryzyka i wpływu decyzji dotyczących zarządzania ryzykiem w zakresie bezpieczeństwa cyfrowego na działalność gospodarczą. Ponadto powinni mieć świadomość, że nie mogą się całkowicie uchronić, więc muszą sobie radzić z pewnym poziomem ryzyka związanego z bezpieczeństwem cyfrowym, aby osiągnąć swoje cele gospodarcze i społeczne. Co więcej, zarządzanie ryzykiem cyfrowym w zakresie bezpieczeństwa powinno respektować interesy innych stron i społeczeństwa jako całości [29].

Do bezpieczeństwa cyfrowego można podejść z co najmniej czterech różnych perspektyw, takich jak: technologia, egzekwowanie prawa, bezpieczeństwo narodowe i międzynarodowe, a także dobrobyt gospodarczy i społeczny. W tej sekcji wyjaśniono wpływ bezpieczeństwa cyfrowego na wymiar gospodarczy, zaś następna obejmuje zagadnienia związane z „tworzeniem dobrobytu, innowacjami, rozwojem, konkurencyjnością i zatrudnieniem we wszystkich sektorach gospodarki, a także innymi aspektami jak: indywidualne swobody, zdrowie, edukacja, kultura,

partycypacja demokratyczna, nauka, rozrywka i inne aspekty dobrobytu, w których środowisko cyfrowe napędza postęp” [30]. Dzieje się tak dlatego, że środowisko cyfrowe ma zasadnicze znaczenie dla funkcjonowania dzisiejszych gospodarek i społeczeństw oraz jest źródłem innowacji.

Incydenty związane z bezpieczeństwem cyfrowym powodują różne konsekwencje dla dotkniętych nimi organizacji, takie jak: osłabienie reputacji (gdy marka organizacji jest narażona), utrata konkurencyjności (w przypadku kradzieży tajemnic handlowych), straty finansowe wynikające z samego ataku (na przykład wyrafinowane oszustwa) z powodu utraconego kontraktu, zakłóceń w prowadzeniu działalności (na przykład sabotażu), kosztów związanych z odrabianiem strat, postępowaniami sądowymi i grzywnami. Trudno jest również oszacować faktyczne koszty incydentów związanych z bezpieczeństwem cyfrowym, ponieważ często organizacje nie udostępniają tego rodzaju informacji, ponieważ są postrzegane jako potencjalnie szkodliwe informacje. Z tego powodu nie ma statystyk ani źródeł danych dotyczących rzeczywistych kosztów incydentów związanych z bezpieczeństwem cyfrowym. „Dotknięte organizacje mogą skończyć płacąc grzywny, opłaty prawne i koszty rekompensaty". Inną ekonomiczną konsekwencją ryzyka bezpieczeństwa cyfrowego są zmiany w zarządzaniu organizacjami po takich incydentach. W przeszłości wielu dyrektorów generalnych lub dyrektorów ustąpiło, a kierownictwo różnych szczebli straciło pracę w wyniku naruszenia bezpieczeństwa, które zostało ujawnione przez media. Ponadto osoby fizyczne oraz małe i średnie przedsiębiorstwa mogą ponieść straty finansowe, kradzież tożsamości, a także inne skutki ekonomiczne z powodu naruszenia danych. Osoby fizyczne jako konsumenci mogą również stracić zaufanie do całego sektora / systemu, a nie tylko zaufanie do danej instytucji (31).

Organizacje, a zwłaszcza potencjalni i obecni młodzi przedsiębiorcy, powinni zadbać o to, aby ich cyfrowe środki bezpieczeństwa wspierały działalność gospodarczą i społeczną. Niemożliwe jest wyeliminowanie każdego potencjalnego ryzyka, należy więc podjąć pewne decyzje, biorąc pod uwagę fakt, że cyfrowe środki bezpieczeństwa „mogą podnieść koszty finansowe, złożoność systemu i czas wprowadzenia na rynek, a także zmniejszyć wydajność, użyteczność, możliwości ewoluowania, innowacyjność i wygodę dla użytkownika". A wszystkie powyżej wymienione kwestie wiążą się z kosztami. [32].

Zarządzanie cyfrowymi zagrożeniami bezpieczeństwa wymaga wzięcia pod uwagę, że takie zagrożenia rzeczywiście istnieją, a pewne umiejętności, które można zdobyć dzięki wykształceniu (niektóre z tych umiejętności można zdobyć za pośrednictwem naszego e-Poradnika), praktyce, doświadczeniu, a wszystko to pociąga za sobą koszty dla organizacji.

D. Integracja bezpieczeństwa cyfrowego w ramach ogólnego zarządzania ryzykiem i procesów decyzyjnych w organizacji

Znając różne zagrożenia techniczne i ekonomiczne, powinniśmy zauważyć wyraźną potrzebę integracji bezpieczeństwa cyfrowego w ramach ogólnego zarządzania ryzykiem i procesów decyzyjnych w organizacji.

Ale co dokładnie oznacza ryzyko? Możemy pomyśleć o następującym przykładzie: klient złożył zamówienie w naszym sklepie internetowym na pół godziny przed południem, a nasza polityka dostawy mówi, że jeśli ktoś zamówi przed południem, wtedy ich zamówienie zostanie dostarczone tego samego dnia. Spieszymy do wystawienia i wydrukowania faktury, aby móc przekazać paczkę kurierowi przed wyjazdem na popołudniowe przesyłki, aby zamówienie zostało dostarczone na czas, a zatem zgodne z naszą polityką. Jest to codzienna, bardzo możliwa sytuacja „awaryjna". Istnieje ryzyko zerwania połączenia z Internetem, co uniemożliwi nam wystawienie faktury z naszego sklepu internetowego. Istnieje również ryzyko zepsucia się urządzeń (komputera lub drukarki), więc nie będziemy mogli wydrukować faktury. Nie jest to wielki kryzys bezpieczeństwa, ale może prowadzić do niezadowolenia klientów, anulowania zamówienia i utraty dobrej reputacji.

Dobrym sposobem analizy i zrozumienia ryzyka jest rozbicie go w następujących obszarach:

a) To, do czego mamy dostęp, może zwiększyć ryzyko naruszenia bezpieczeństwa. Czy wiemy, że strony internetowe, do których uzyskujemy dostęp za pośrednictwem Internetu, są bezpieczne? Czasami, gdy odwiedzasz stronę internetową, możesz otrzymać powiadomienie z przeglądarki, że ta witryna ma niezaufany certyfikat Masz możliwość pozostać na stronie lub ją opuścić. Co zrobisz?

   A co z oprogramowaniem? Czy wiemy, że oprogramowanie, które chcemy zainstalować, jest bezpieczne? Nawet jeśli jest to absolutnie bezpieczne, czy jest możliwe, że mamy zainstalowanych zbyt wiele aplikacji na naszych urządzeniach,

które spowalniają wydajność? Czy jest możliwe, że nie mamy dostępu do najlepszego oprogramowania do zadań, które musimy wykonać, a które pozwolą nam na mniejszą produktywność? Czy łączymy nasze osobiste urządzenia z siecią firmową? Czy wykorzystujemy firmowe komputery do celów prywatnych? Czy uzyskujemy dostęp do nielegalnych materiałów lub je pobieramy?

b) To gdzie i z czym się łączymy może zwiększyć ryzyko naruszenia integralności i poufności naszych systemów. Czy możemy mieć pewność, że sieć, do której jesteśmy podłączeni, jest zaufana? Korzystanie z naszych urządzeń mobilnych w niezaufanych sieciach, takich jak Wi-Fi na lotnisku lub prosty przykład podłączenia się do sieci w kawiarni może być niebezpieczne i szkodliwe dla naszych danych i naszych urządzeń.

c) Kiedy mają miejsca różne wydarzenia to ryzyko wzrasta. Na przykład, jeśli wydarzyła się katastrofa i otrzymujesz e-mail z informacją nadesłaną z Czerwonego Krzyża z prośbą o wpłacenie darowizny to czy możemy od razu w to uwierzyć? Najpierw musimy to sprawdzić.

d) W jaki sposób przestrzegamy najlepszych praktyk bezpieczeństwa? Czy postępujemy zgodnie z najlepszymi praktykami? Czy mamy wystarczającą wiedzę, zanim coś zrobimy? Jeśli nie, będziemy musieli zgłębić swoją wiedzę przed podjęciem jakichkolwiek działań. Większa wiedza oznacza mniejsze ryzyko.

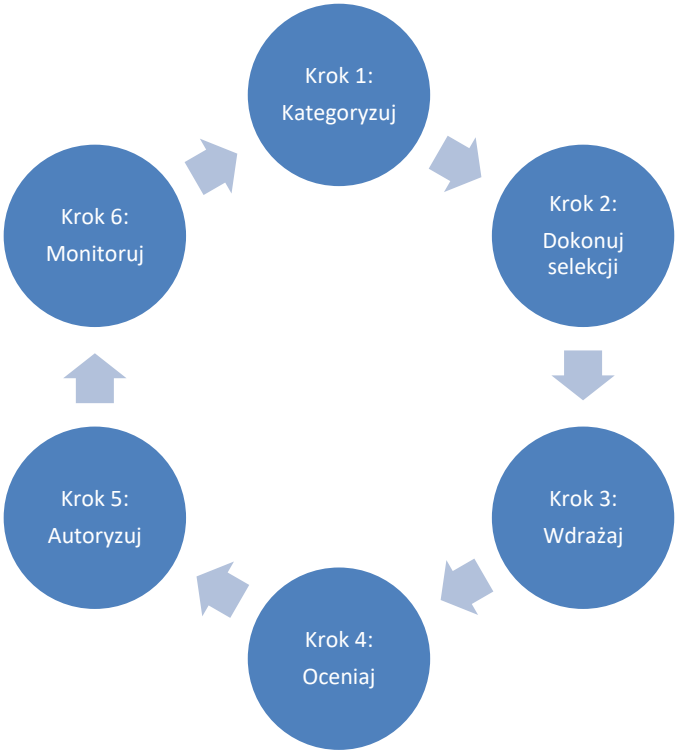
e) Dlaczego używamy tych najlepszych praktyk? Musimy być w stanie logicznie rozumieć i wiedzieć o wszelkich podejmowanych przez nas środkach dotyczących cyberbezpieczeństwa. Nie podążaj tylko za tłumem, czy za tym, co jest napisane na jednej stronie. Badaj, dociekaj, pytaj, ucz się, rozum. Może niektóre środki będą dobre dla twojej firmy, a inne będą szkodliwe. Wiedząc, dlaczego coś robisz, zmniejszasz ryzyko. Na przykład, gdy otrzymasz link do kliknięcia lub e-maila do przeczytania, nie rób tego po prostu bez zrozumienia dlaczego to robisz. Innym przykładem jest niepotrzebne korzystanie z usług udostępniania plików do przechowywania danych tylko dlatego, że jest to łatwiejsze, bez znajomości zagrożeń, które się za tym kryją. Co się stanie, jeśli twoje hasło zostanie skradzione, a jeśli zapomnisz na zawsze wszystkie twoje certyfikaty?

Ponadto, aby zrozumieć ryzyko, musisz wziąć pod uwagę niektóre czynniki ryzyka, których nie będziesz w stanie zmienić. Na przykład nie będzie można zmienić sposobu działania systemów operacyjnych lub zakupionego oprogramowania i związanych z nimi luk. Będziesz mógł je ulepszyć tylko za pomocą innych środków. Mogą istnieć użytkownicy, którzy odmówią przestrzegania najlepszych praktyk, które ustanowisz dla bezpieczeństwa swojej firmy. Będziesz musiał zająć się nimi na innym poziomie, bez uszczerbku dla środków bezpieczeństwa i cyberbezpieczeństwa.

Aby zarządzać ryzykiem operacyjnym i organizacyjnym, możesz skorzystać z Ram Zarządzania Ryzykiem, który pomaga w zarządzaniu nimi. Ale jaka jest różnica między ryzykiem operacyjnym a organizacyjnym. Usługi operacyjne, systemy lub funkcje w organizacji odnoszą się do ryzyka operacyjnego, podczas gdy ogólna struktura organizacji jako całości odnosi się do ryzyka organizacyjnego. W Ramach Zarządzania Ryzykiem działania związane z bezpieczeństwem i zarządzaniem ryzykiem są zintegrowane w całym cyklu życia systemu lub usługi, co stanowi znaczący krok w zapewnianiu skutecznego programu bezpieczeństwa informacji.

Wewnętrzną częścią ogólnej strategii dla Twojej firmy / organizacji musi być zarządzanie ryzykiem. Pomoże ci odpowiedzieć na pytania typu „Jak rozpoznać ryzyko?” i „Jak sobie z nim poradzić?". Przykładem jest NIST 800-37, który stanowi ramy dla ciągłego zarządzania ryzykiem w czasie rzeczywistym dla cyklów życia systemu.

Jak skonfigurować strukturę zarządzania ryzykiem? Cykl życia w ramach zarządzania ryzykiem zawiera szereg kroków, które można zastosować w celu ustawienia własnych ram zarządzania ryzykiem (zob. Rycinę 1). Te kroki zostały pokrótce opisane poniżej:



Ryc. 1: Ramy Zarządzania Ryzykiem [33]

Krok 1: Kategoryzuj / Definiuj system i sposób jego użycia. Należy również wziąć pod uwagę znaczenie systemu, np. czy to serwer ze zdjęciami czy systemem kart kredytowych? W przypadku, gdy jest to system kart kredytowych, czy jest to serwer kart kredytowych lub terminal? W przypadku awarii, jak możemy sobie z nimi poradzić? W tym kroku musisz przypisać role osobom odpowiedzialnym (np. właścicielowi systemu).

Krok 2: Wybierz środki bezpieczeństwa, które zostaną umieszczone w systemie na podstawie stopnia krytyczności (tj. niski, średni i wysoki). Należy pamiętać, że wysokiej krytyczności nie można przypisać do wszystkich środków bezpieczeństwa. Jak już wspomniano, nie jest dobrą praktyką kontrolowanie bezpieczeństwa we wszystkich aspektach działalności firmy, ponieważ może to powodować problemy z wydajnością, np. dla stanowisk pracy dla pracowników będą musiały zostać określone wymagania antywirusowe lub też trzeba określić, czy pracownicy wymagają określonego uwierzytelnienia w celu uzyskania dostępu do systemów finansowych (oczywiście, że tak).

W tym kroku również musisz przypisać role osobom odpowiedzialnym (np. pracownikowi ds. bezpieczeństwa informacji).

Krok 3: Po wybraniu środków bezpieczeństwa w kroku 2, musisz wdrożyć je w tym kroku (np. zainstalować wybrane oprogramowanie antywirusowe w systemach). Również i w tym kroku musisz przypisać role osobom odpowiedzialnym (np. właścicielowi systemu informatycznego).

Krok 4: Po wdrożeniu kontroli bezpieczeństwa informacji w poprzednim kroku będziesz musiał opracować kilka procesów na tym etapie, aby upewnić się, że są na miejscu i nie są zagrożone, np. sprawdzenie, czy twój program antywirusowy faktycznie chroni twój system(y) przed zagrożeniami lub zdaje sobie sprawę z nowych zagrożeń, które nie były początkowo brane pod uwagę. W tym kroku musisz także przypisać role osobom odpowiedzialnym (np. Może to być biuro ds. audytu / bezpieczeństwa informacji w twojej firmie / organizacji lub w firmie zewnętrznej).

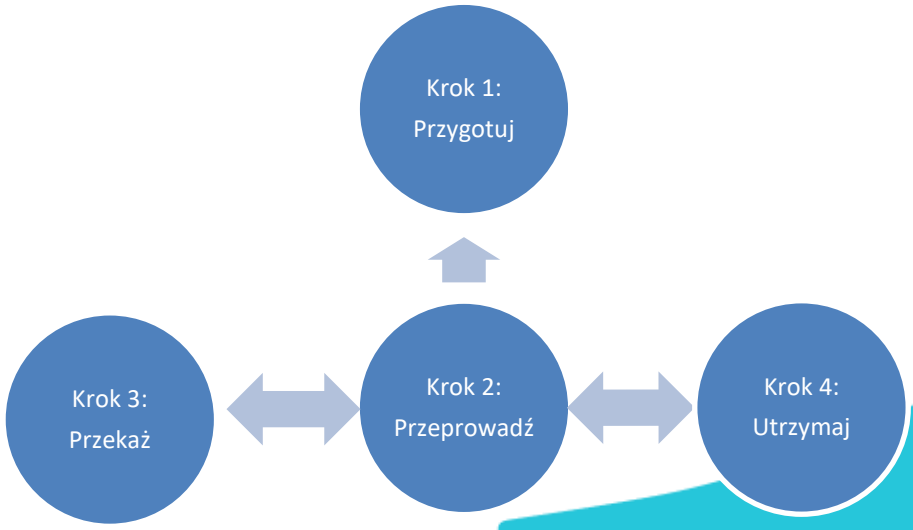
Krok 5: Zakładając, że już zidentyfikowałeś ryzyko, jakie działania podejmiesz, aby je złagodzić? Co więcej, czy możliwe jest zastosowanie tych działań, o których myślisz? Czy istnieje jakikolwiek powód, dla którego akceptujesz ryzyko (w przypadku, gdy jesteś upoważniony do podjęcia takich działań), np. niektóre programy antywirusowe nie mogą być instalowane w terminalach punktów sprzedaży? W związku z tym akceptujesz ryzyko braku oprogramowania antywirusowego lub szukasz rozwiązania kompromitującego. W tym kroku musisz także przypisać role osobom odpowiedzialnym (np. Może to być biuro ds. audytu / bezpieczeństwa informacji w twojej firmie / organizacji).

Krok 6: Ciągły monitoring systemu informatycznego i środków kontroli bezpieczeństwa stosowanych pod kątem ich skuteczności odbywa się w końcowym etapie cyklu życia. Typową metodą jest rejestrowanie każdego działania systemu, pakietu ruchu sieciowego, transakcji systemowej, sesji użytkownika itp. Jest to określane jako rejestrowanie i pomaga monitorować zidentyfikowane zagrożenia lub naruszenia całego systemu, przeglądając pliki dziennika. Umożliwia to podjęcie natychmiastowych działań w razie potrzeby. W tym kroku musisz także przypisać role osobom odpowiedzialnym

(np. wiele różnych osób lub specjalistów specjalizujących się w danej dziedzinie w twojej firmie / organizacji).

Podjęcie decyzji w sprawie odpowiednich Ram Zarządzania Ryzykiem wymaga głębokiego przemyślenia. Musisz zbudować kompletną strukturę, która będzie działać w twoim środowisku biznesowym.

Znacząca rola w procesie zarządzania ryzykiem została przypisana do **oceny ryzyka**. Proces oceny ryzyka składa się z kilku etapów: przygotowania do oceny, przeprowadzenia oceny, przekazania wyników oceny i utrzymania oceny. Rycina 2 ilustruje te kroki. Proces oceny ryzyka został dokładniej omówiony poniżej.



Ryc. 2: Ocena ryzyka [34]

Krok 1: Przygotowanie do oceny. Najpierw określ cel oceny. Zastanów się, na czym polega ocena i jaki jest zakres. Trzeba będzie zdefiniować założenia i ograniczenia związane z oceną. Ponadto należy zadeklarować źródła informacji, które należy wykorzystać jako dane wejściowe do oceny. Ostatecznym działaniem jest określenie modelu ryzyka i metod analitycznych.

Krok 2: Przeprowadzenie oceny. Rozważ źródła zagrożeń i zdarzenia, które mogą być przez nie wytwarzane. Wykrywaj luki w swoim systemie biznesowym/organizacyjnym, co pociąga za sobą przestrzeganie określonego planu, który zawiera możliwe do wystąpienia zagrożenia i warunki sprzyjające wykorzystaniu tych luk. Następnie należy określić prawdopodobieństwo zidentyfikowanych źródeł zagrożeń, które mogą przyczynić się do powstania określonych zdarzeń, zakładając, że te zdarzenia zaistnieją. Będą musiały zostać określone skutki uboczne takie jak wpływ na działalność organizacyjną i majątek, osoby fizyczne, inne organizacje, nawet na poziomie krajowym. Może to być spowodowane wykorzystaniem luk w zabezpieczeniach za pośrednictwem źródeł zagrożeń w określonych zdarzeniach. Potrzebne są wyjaśnienia, w których można znaleźć zagrożenia dla bezpieczeństwa jako połączenie potencjalnej groźby wykorzystania słabych punktów i ich wpływu, w tym niepewności związanej z określaniem ryzyka.

Krok 3: Przekazanie wyników oceny. Należy dobrze zrozumieć wyniki oceny. Tylko wtedy możesz udostępnić je razem z informacjami, które zostały użyte jako dane wejściowe na początku oceny. Przekazując wyniki, będziesz wspierać inne działania związane z zarządzaniem ryzykiem.

Krok 4: Utrzymanie wyników oceny. Czynniki ryzyka, które zostały określone podczas oceny ryzyka, muszą być stale monitorowane, aby zrozumieć wszelkie późniejsze zmiany tych czynników. Pamiętaj o aktualizacji składników oceny ryzyka, aby odzwierciedlały działania monitorujące prowadzone przez twoją firmę [34].

E. OCENA RYZYKA W ZAKRESIE CYBERBEZPIECZEŃSTWA - LISTA KONTROLNA

	✓
Krok 1: Przygotowanie do oceny ryzyka	
Określ cel oceny	
Zidentyfikuj zakres oceny	
Zidentyfikuj założenia i ograniczenia związane z oceną	
Określ źródło informacji, które mają być wykorzystane jako dane wejściowe do oceny	
Określ model ryzyka i podejścia analityczne, które należy zastosować podczas oceny	
Krok 2: Przeprowadzanie oceny ryzyka	
Zidentyfikuj odpowiednie źródła zagrożeń	
Określ zagrożenia, które mogą być generowane przez te źródła zagrożeń	
Zidentyfikuj luki w organizacji, które mogą być wykorzystane przez te źródła zagrożeń, przez pochodzące z nich zagrożenia oraz warunki sprzyjające wykorzystaniu tych luk	
Określ prawdopodobieństwo, że zidentyfikowane źródła zagrożeń doprowadzą do wystąpienia konkretnych zagrożeń oraz prawdopodobieństwo zaistnienia takich zagrożeń	
Określ niekorzystny wpływ na działalność i aktywa organizacji	

Określ ryzyka związane z cyberbezpieczeństwem łącząc prawdopodobieństwo wystąpienia zagrożenia wykorzystania luk w zabezpieczeniach oraz związanych z tym konsekwencji	
Krok 3: Przekazywanie i dzielenie się informacjami na temat oceny ryzyka	
Przekazuj wyniki oceny ryzyka	
Udostępniaj informacje opracowane podczas przeprowadzania oceny ryzyka	
Krok 4: Utrzymywanie wyników oceny	
Monitoruj na bieżąco czynniki ryzyka zidentyfikowane w ocenach ryzyka i zrozum	
późniejsze zmiany tych czynników, aktualizuj elementy oceny ryzyka odzwierciedlających działania monitorujące [34]	

F. Glosariusz terminologii

Ryzyko - potencjalne zyskanie lub utrata czegoś wartościowego [35].

Ocena ryzyka - proces identyfikacji ryzyka związanego z dobrze zdefiniowaną sytuacją i określeniem prawdopodobieństwa wystąpienia tego ryzyka, konsekwencje wystąpienia ryzyka oraz dodatkowe zabezpieczenia, które mogłyby złagodzić powstałe konsekwencje. Ocena ryzyka jest wyrazem synonimicznym dla analizy ryzyka [34].

Zarządzanie ryzykiem - cały proces identyfikowania, kontrolowania i ograniczania ryzyka. Obejmuje ocenę ryzyka [34].

Zagrożenie - potencjał źródła zagrożeń do wykorzystania określonej luki [34].

G. Wnioski i dodatkowe źródła wiedzy

Po zapoznaniu się z powyższym tekstem, wiesz już jak ważne jest zintegrowanie oceny ryzyka bezpieczeństwa cyfrowego w ogólnym zarządzaniu ryzykiem w organizacji i procesami decyzyjnymi. W tej części dokonaliśmy pełnego przeglądu podejść do oceny ryzyka cyfrowego, które powinny być przestrzegane przez potencjalnych i obecnych młodych przedsiębiorców w ich cyfrowych przedsięwzięciach biznesowych oraz aby podkreślić znaczenie wdrożenia strategii oceny ryzyka bezpieczeństwa cyfrowego w przedsięwzięciach internetowych. Naszym celem było wyposażenie potencjalnych i obecnych młodych przedsiębiorców w praktyczną wiedzę na temat aspektów technicznych (bezpieczeństwo cyfrowe jako ryzyko techniczne), a także aspektów ekonomicznych (bezpieczeństwo cyfrowe jako ryzyko ekonomiczne) bezpieczeństwa cyfrowego.

Ponadto w razie potrzeby zalecamy dalsze zgłębianie wiedzy na ten temat.

H. Źródła:

[1] http://searchcompliance.techtarget.com/definition/risk-assessment, dostęp: 13.11.2017

[2] https://www.mindtools.com/pages/article/newTMC_07.htm, dostęp: 13.11.2017

[3] http://www.genre.com/knowledge/blog/steps-to-a-good-risk-assessment-en.html, dostęp: 13.11.2017

[4] https://www.itgovernance.co.uk/cyber-security-risk-assessments-10-steps-to-cyber-security, dostęp: 13.11.2017

[5] http://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm, dostęp: 13.11.2017

[6] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017/at_download/fullReport, dostęp: 27.01.2018

[7] https://www.lifewire.com/what-is-malware-2625933, dostęp: 27.01.2018

[8] https://oit.ncsu.edu/it-security/safe-computing/viruses/, dostęp: 16.05.2018

[9] https://www.trendmicro.com/vinfo/us/security/definition/address-bar-spoofing, dostęp: 16.05.2018

[10] https://www.acunetix.com/websitesecurity/cross-site-scripting/, dostęp: 27.01.2018

[11] https://www.lastline.com/blog/drive-by-download/, dostęp: 16.05.2018

[12] https://searchsecurity.techtarget.com/feature/Targeted-Cyber-Attacks, dostęp: 16.05.2018

[13] https://www.rsa.com/content/dam/rsa/PDF/Making_Sense_of_Man_in_the_browser_attacks.pdf, dostęp: 16.05.2018

[14] https://www.sans.org/reading-room/whitepapers/application/web-browser-insecurity-1637, dostęp: 16.05.2018

[15] https://www.sans.org/reading-room/whitepapers/application/web-based-attacks-2053, dostęp: 16.05.2018

[16] https://www.business.att.com/learn/operational-effectiveness/the-top-10-web-application-security-risks.html, dostęp: 16.05.2018

[17] http://www.trendmicro.it/media/misc/web-application-vulnerabilities-en.pdf, dostęp: 16.05.2018

[18] http://resources.infosecinstitute.com/category/enterprise/phishing/phishing-as-a-risk-damages-from-phishing/#gref, dostęp: 16.05.2018

[19] https://www.bloxx.com/media/1356/bloxx_whitepaper_increasingemailthreats_us.pdf, dostęp: 17.05.2018

[20] https://www.techsoup.org/support/articles-and-how-tos/things-you-can-do-to-prevent-spam, dostęp: 17.05.2018

[21] https://www.facebook.com/help/217854714899185, dostęp: 17.05.2018

[22] https://www.quora.com/How-dangerous-is-a-DDoS-attack, dostęp: 17.05.2018

[23] https://www.computerweekly.com/feature/DDoS-attack-threat-cannot-be-ignored, dostęp: 17.05.2018

[23] https://www.computerweekly.com/feature/DDoS-attack-threat-cannot-be-ignored, dostęp: 17.05.2018

[24] https://www.veracode.com/security/botnet, dostęp: 17.05.2018

[25] https://securityintelligence.com/the-cisos-guide-to-managing-insider-threats/, dostęp: 17.05.2018

[26] https://www.kroll.com/en-us/what-we-do/cyber-security/prepare-and-prevent/cyber-risk-assessments/data-breach-prevention-tips, dostęp: 17.05.2018

[27] https://www.privacyrights.org/consumer-guides/how-reduce-your-risk-identity-theft, dostęp: 17.05.2018

[28] https://www.thebalance.com/prevent-identity-theft-1947624, dostęp: 17.05.2018

[29] OECD, Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, http://dx.doi.org/10.1787/9789264245471-e, p. 9

[30] OECD, Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, http://dx.doi.org/10.1787/9789264245471-e, p. 19-20

[31] OECD, Managing Digital Security and Privacy Risk for Economic and Social Prosperity, OECD Publishing, http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2016)1/FINAL&docLanguage=En, p. 14-15

[32] OECD, Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, http://dx.doi.org/10.1787/9789264245471-e, p. 35

[33] https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-37r1.pdf, dostęp: 11.06.2018

[34] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf, dostęp: 11.06.2018

[35] https://en.wikipedia.org/wiki/Risk, dostęp: 11.06.2018

Podziękowania od zespołu DiFens

Mamy nadzieję, że niniejszy e-Poradnik spełnił swój cel i pomógł ci łatwiej wkroczyć w świat cyfrowego bezpieczeństwa dla twojej obecnej lub przyszłej firmy, wskazując ci właściwy kierunek, jakim powinieneś podążać.

Zachęcamy do dalszego zgłębiania tematu ze stron zatytułowanych „Dodatkowe źródła wiedzy" Dalsze czytanie" części e-Poradnika, a także poprzez zaznajomienie się z dodatkową literaturą związaną z własnym polem działania.

Jeśli potrzebujesz dodatkowych wskazówek, możesz skorzystać z mentoringu w zakresie przedsiębiorczości i bezpieczeństwa cyfrowego na platformie mentorskiej DiFens, dostępnej pod adresem: http://www.difens.eu/ Jeśli czujesz się wystarczająco pewny siebie, możesz również zostać mentorem i pomóc innym młodym przedsiębiorcom w ich staraniach, dzieląc się z nimi swoją wiedzą i doświadczeniem.

Aby uzyskać więcej informacji na temat projektu i zespołu stojącego za nim, odwiedź http://difens-project.eu/ lub skontaktuj się z nami poprzez adres e-mail:difensproject@gmail.com

Dziękujemy za przyłączenie się do nas i życzymy powodzenia w zabezpieczaniu swoich firm!