CYBERBEZPIECZEŃSTWO
– WYZWANIA DLA BIZNESU

Pracodawcy RP
Rok założenia 1989

Pragmatic Solutions

DAGMA
BEZPIECZEŃSTWO IT

Pracodawcy Rzeczypospolitej Polskiej

tel: 22 518 87 00

ul. Berneńska 8
03-976 Warszawa

e-mail: sekretariat@pracodawcyrp.pl

W dzisiejszym społeczeństwie, coraz bardziej uzależnionym od technologii, cyberbezpieczeństwo stało się kluczowym aspektem działalności biznesowej. Przedsiębiorcy i pracodawcy muszą być w pełni świadomi, że cyberataki stanowią realne zagrożenie dla ich firm i mogą mieć poważne konsekwencje zarówno dla produkcji, funkcjonowania firmy, jak i dla reputacji przedsiębiorców. Niezależnie od branży czy rozmiaru przedsiębiorstwa, żadna firma nie jest w stu procentach odporna na ryzyko ataku cybernetycznego.

Zagrożenia, które płyną z cyberataków, są szczególnie istotne w kontekście obecnej sytuacji geopolitycznej na wschodniej granicy. Wzrost konfliktów międzynarodowych i rozwój zaawansowanych technologii informatycznych powodują, że cyberprzestępcy mają dostęp do coraz większej liczby narzędzi i zasobów, których mogą użyć przeciwko firmom. Ataki mogą prowadzić do kradzieży poufnych danych, zakłóceń w funkcjonowaniu sieci informatycznych, utraty informacji handlowych, a nawet manipulacji systemami i infrastrukturą biznesową.

Przedsiębiorcy i pracodawcy muszą być gotowi i zdolni do zapobiegania, wykrywania oraz skutecznego reagowania w przypadku takich zagrożeń. Inwestowanie w cyberbezpieczeństwo nie jest już luksusem, ale koniecznością. Ochrona przed cyberatakami wymaga kompleksowego podejścia, które obejmuje nie tylko technologiczne środki ochrony, ale także edukację pracowników, świadomość zagrożeń i procedury reagowania w przypadku takich incydentów.

W opracowniu, które oddajemy w Państwa ręce, szczegółowo przedstawiamy zarówno praktyczne jak i prawne aspekty, które mogą pomóc przedsiębiorcom i pracodawcom w ochronie swoich firm przed cyberzagrożeniami. Analizujemy zmieniające się prawo oraz nowoczesne techniki ataków, trendy w dziedzinie cyberbezpieczeństwa, najważniejsze obszary ryzyka i skuteczne metody ochrony.

Wnioski i rekomendacje, które wynikną z naszego opracowania, będą miały na celu zapewnienie Państwa firmom lepszej cyberochrony, a także zwiększenie świadomości na temat zagrożeń związanych z cyberbezpieczeństwem. Ponadto zwracamy uwagę na znaczenie współpracy między przedsiębiorstwami, rządem i innymi zainteresowanymi podmiotami w walce z cyberprzestępczością. Wierzymy, że dostarczone informacje będą pomocne i skłonią Państwa do podjęcia działań w celu wzmocnienia cyberochrony w Waszych firmach.

dr Rafał Dutkiewicz
Prezes Pracodawców RP

178% – o tyle w 2022 roku wzrosła liczba zgłoszeń naruszenia cyberbezpieczeństwa w porównaniu z rokiem 2021. Jest to część dłuższego trendu, który obserwujemy od lat. Cyberbezpieczeństwo może wydawać się typowo technologicznym wyzwaniem, jednak prawo staje się coraz bardziej istotnym elementem architektury gwarantującej odpowiednie zabezpieczenie danych. Regulacje zarówno na poziomie europejskim, jak i krajowym starają się nadążyć za wirtualnym światem. Jak wskazujemy w Raporcie, już niebawem przed nami duże zmiany w tym kontekście – wejście w życie unijnego Rozporządzenia DORA i Dyrektywy NIS2.

Z jednej strony regulacje dotyczące cyberbezpieczeństwa są pożądane, bo służą wspólnemu dobru, jakim jest odpowiednie przechowywanie danych. Z drugiej jednak, ich wdrożenie i dostosowanie procedur jest dużym wyzwaniem dla przedsiębiorstw. Przepisy określają nie tylko technologiczne zabezpieczenia czy procedury, ale także czysto praktyczne i fizyczne obowiązki, które mają gwarantować bezpieczeństwo danych. W niniejszym Raporcie znajdą Państwo podsumowanie najważniejszych, już obowiązujących regulacji w tym obszarze, jak i nadchodzących unijnych aktów prawnych.

Mec. Piotr Spaczyński,
Partner Zarządzający w SSW Pragmatic Solutions

Intensyfikacja cyberataków, zmiany prawne na poziomie europejskim i krajowym, praca hybrydowa, wojna za wschodnią granicą – ostatnie lata przyniosły wyjątkowe tempo zmian, nawet dla tak dynamicznej branży jak cyberbezpieczeństwo.

Nowe wyzwania sprawiły, że wielu zarządzających firmami poczuło potrzebę zweryfikowania na nowo sprawności swoich organizacji w aspekcie bezpieczeństwa informatycznego. Dyrektywy europejskie i zmieniające się prawo krajowe mogą służyć wyciągnięciu wniosków co do kierunków działania, nawet jeśli Państwa organizacja jeszcze tym regulacjom nie podlega bezpośrednio.

Dla zapewnienia należytej odporności organizacji na ataki, kluczowe jest osiągnięcie równowagi w wielu aspektach – analizy ryzyka, odpowiedniego planowania procesów, kultury cyberbezpieczeństwa wśród pracowników, aż po zabezpieczenia techniczne i procedury postępowania w wypadku skutecznego ataku. Dlatego bezpowrotnie minęły czasy, w których o zabezpieczeniach decydowało grono kilku informatyków w oderwaniu od reszty organizacji.

Dla zapewnienia cyberbezpieczeństwa niezbędne jest, aby w tę tematykę zaangażowali się również menedżerowie najwyższego szczebla. Stawia to przed nimi nowe wyzwania – zrozumienie podstaw myślenia o cyberbezpieczeństwie i nauczenie się dialogu z osobami odpowiedzialnymi za procesy, aspekty prawne i technologię. Tak, aby wspólnie stworzyć kulturę bezpieczeństwa, zasady, procedury i zastosować optymalne dla organizacji rozwiązania techniczne.

Oddajemy w Państwa ręce krótki przegląd tej tematyki. Jeśli po jego przeczytaniu poczują Państwo niedosyt lub pojawią się wątpliwości – oznacza to, że osiągnęliśmy cel. Czas poważnie porozmawiać o cyberbezpieczeństwie!

Paweł Jurek
Dyrektor ds. rozwoju biznesu w DAGMA Bezpieczeństwo IT

SPIS TREŚCI

I. CYBERBEZPIECZEŃSTWO – ASPEKTY PRAWNE

Wstęp

1. WSTĘP

Dynamiczny rozwój technologii bez wątpienia ma wpływ na rynek towarów i usług oraz rozwój społeczno-gospodarczy każdego państwa. Nie tylko korzystanie z rozbudowanych systemów informatycznych, gromadzących olbrzymie zasoby danych, ale również korzystanie z usług świadczonych w chmurze obliczeniowej, skutkuje wzmożoną aktywnością cyberprzestępców.

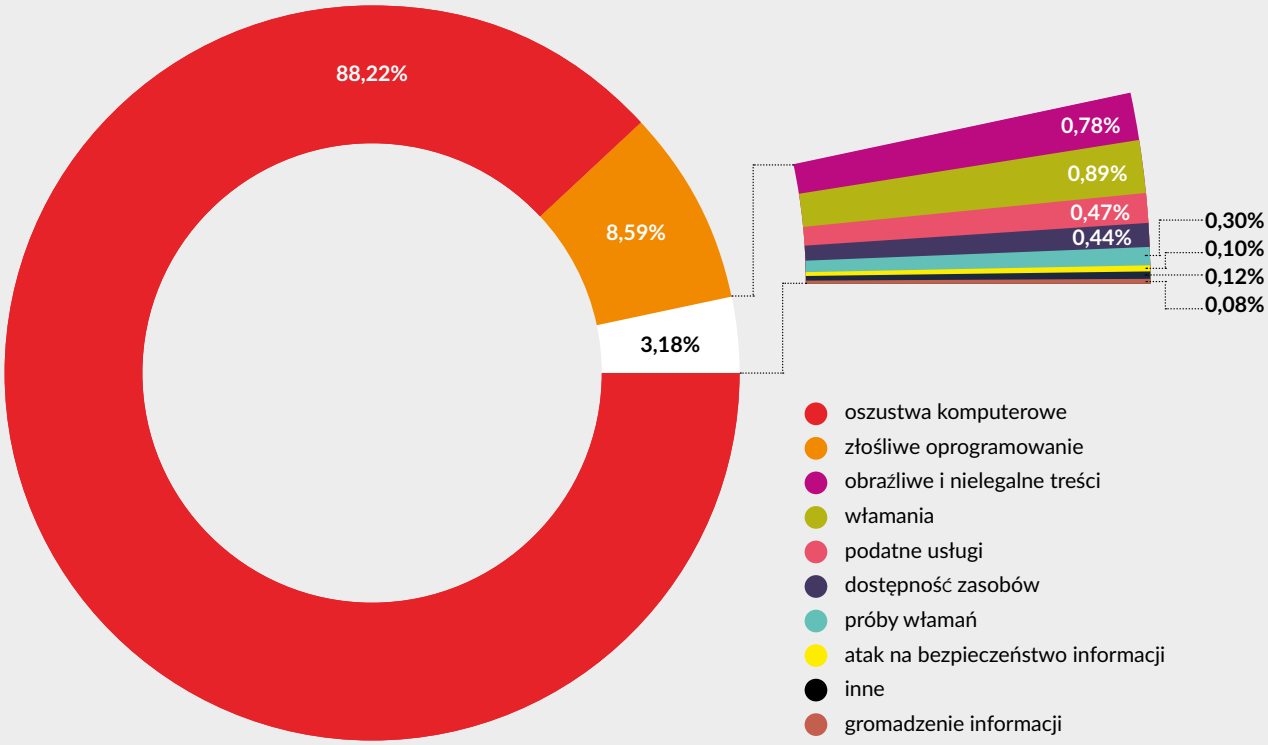
Jak podaje CERT, pierwszy polski zespół reagowania na incydenty działający w strukturach NASK, w swym raporcie: *W 2022 r. odnotowano 322 479 zgłoszeń incydentów cyberbezpieczeństwa. Wśród nich występowały również takie, które nie zostały uznane za incydent. CERT Polska dokonał starannej klasyfikacji, na podstawie której wytypował 115 164 zgłoszeń, z których zarejestrował 39 683 incydentów cyberbezpieczeństwa.*

Dla porównania, w roku poprzednim, *CERT Polska zarejestrował 116 071 zgłoszeń. Spośród wszystkich zgłoszeń nasi specjaliści wytypowali 65 586, na podstawie których zarejestrowano łącznie 29 483 unikalnych incydentów cyberbezpieczeństwa*[1].

Odnotowano zatem wzrost incydentów cyberbezpieczeństwa na poziomie 182% porównując rok 2021 do roku 2020 oraz 178% porównując rok 2022 do roku 2021. Na chwilę obecną nie są znane statystki za 2023 r., należy jednak zakładać dalszy wzrost tendencji. Skala dynamiki wskazuje, że cyberbezpieczeństwo przestało być kojarzone z filmami science-fiction, a stało się chlebem powszednim nie tylko dużych korporacji, ale i każdego przedsiębiorcy. Można nawet zaryzykować stwierdzenie, że równie łatwo jest popełnić przestępstwo gospodarcze w sieci, co w rzeczywistości, o ile nie łatwiej.

CERT w 2022 r. odnotował następujące kategorie cyberataków:

kategorie incydentów



Cyberprzestępczość nieustannie rozwija się, przestępcy doskonalą swoje metody, jak i sięgają po nowe, dotychczas nieznane środki. Ataki przeprowadzane są w różnorodny sposób, począwszy od podszywania się, kradzieży tożsamości, po zaawansowane sztuczki socjotechniczne.

[1] Raport roczny z działalności CERT POLSKA z 2022 r., Krajobraz bezpieczeństwa polskiego internetu; https://cert.pl/uploads/docs/Raport_CP_2022.pdf oraz Raport roczny z działalności CERT POLSKA z 2021 r., https://cert.pl/uploads/docs/Raport_CP_2021.pdf

Znaczenie cyberbezpieczeństwa

2. ZNACZENIE CYBERBEZPIECZEŃSTWA

Przedsiębiorcy postawieni przed powyższymi okolicznościami faktycznymi powinni rozważyć wdrożenie środków cyberbezpieczeństwa. W niektórych przypadkach są lub będą prawnie zobowiązani do wdrożenia środków mających służyć odporności systemów informatycznych na działania naruszające:

- poufność
- integralność
- dostępność
- autentyczność danych

Jesteśmy w czasie wzrostu wartości danych takich jak listy dostawców, klientów, danych telemetrycznych z taśm produkcyjnych, danych technologicznych, receptur itp. To zjawisko, niekiedy określane mianem Big Data, powstało jako skutek działań przedsiębiorcy w celu uzyskania przewagi konkurencyjnej na gruncie danych.

Zbieranie, agregowanie, integracja, tworzenie powiązań, struktur oraz w kolejnym kroku analiza, weryfikacja, tworzenie predykcji na podstawie danych – taka aktywność przedsiębiorcy służy temu, aby dane stały się najbardziej wartościowym aktywem przedsiębiorcy. Przedsiębiorca operujący w tak rozwiniętej gospodarce dokonuje czynności prawnych, zawiera umowy o korzystanie z tych danych, i ma spory o dane, i o dostęp do nich.

PRZYKŁAD: Producent wózków sklepowych z wmontowanymi beaconami, rejestrującym zachowania klientów w sklepach, ma wyższe przychody z tytułu udzielania dostępu do danych zbieranych przez wózki, aniżeli ze sprzedaży samych wózków.

PRZYKŁAD: Dystrybutor energii, który outsourcował utrzymanie bazy danych klientów (m.in. dane o zużyciu) korzysta z domniemania prawnego wyłączności w prawie do korzystania z bazy danych (np. pobieranie danych) – jako podmiot, który poniósł ryzyko nakładu inwestycyjnego związanego z bazą danych.

Uzyskanie przewagi konkurencyjnej dzięki danym jest związane z wyzwaniami: dane mogą być na tyle wartościowe, że może istnieć podmiot, który zechce uzyskać do nich dostęp w sposób nieuprawniony – wtedy niejako w zwierciadle wzrostu wagi danych, wzrasta znaczenie cyberbezpieczeństwa.

Z powyższych przykładów biją konkretne wnioski – z jednej strony wartość (majątkowy charakter praw do baz danych), z drugiej szanse i zagrożenia oraz z trzeciej strony regulacje i best practices w zakresie osiągnięcia cyberbezpieczeństwa.

Ta tematyka, przede wszystkim prawna, jakże ważna dla przedsiębiorców, została przedstawiona w niniejszym opracowaniu.

Aktualny stan prawny

3. AKTUALNY STAN PRAWNY

Prawo wydaje się emanacją rozwoju społeczeństwa – to oczywiście przewrotne twierdzenie. Istotnie bowiem, przy najszczerszych chęciach, świadomość społeczeństwa nie nadąża za wolą ustawodawców – i odwrotnie, ustawodawcy nie nadążają za rozwojem technicznym i społecznym.

Efektem jest opór społeczeństwa wobec regulacji – najbardziej aktualnym przykładem jest ogólna niechęć do ochrony danych osobowych (RODO). Wydaje się, że ów opór ma charakter przejściowy, wszak obecnie nie budzi sprzeciwu regulacja czasu pracy czy przepisy antymonopolowe.

Do wspólnego orszaku regulacji co RODO zalicza się dyrektywa NIS, która nałożyła na państwa członkowskie obowiązek wdrożenia do krajowych porządków prawnych ustaw do dnia 10 maja 2018 roku (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii – czyli tzw. Dyrektywa NIS).

Dyrektywa NIS wyznacza podstawowe ramy cyberbezpieczeństwa na poziomie UE i nakłada na Państwa Członkowskie UE implementację do porządku prawnego aktów prawnych. W Polsce cyberbezpieczeństwo regulowane jest na mocy m. in. następujących aktów prawnych:

- Ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Ustawa o KSC);
- Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz. U. poz. 1806);
- Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. poz. 2180);
- Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. poz. 2080);
- Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz.U. 2019 poz. 2479);
- Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie wzoru formularza do przekazywania informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych, które miało istotny wpływ na funkcjonowanie sieci lub usług (Dz. U. poz. 1831);
- Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług (Dz. U. poz. 1830);
- Rozporządzenie Wykonawcze Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiające zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ.

Nadrzędne znaczenie ma ustawa o Krajowym Systemie Cyberbezpieczeństwa (dalej jako „ustawa o KSC") i stanowi ona podstawowy instrument określający prawa i obowiązki podmiotów stanowiących krajowy system cyberbezpieczeństwa.

W kolejnych latach, czeka nas aktualizacja stanu prawnego, tj.:

- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2);
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Rozporządzenie DORA).

Nowe przepisy wchodzą w życie wraz z przełomem 2024 i 2025 roku (Dyrektywa NIS2 – obowiązek transpozycji do krajowego porządku prawnego do 16 października 2024 roku; Rozporządzenie DORA – 17 stycznia 2025 roku, obowiązujące bezpośrednio).

Ostatnim elementem orszaku legislacji razem z RODO i NIS jest projekt rozporządzenia ePrivacy. Pomimo tego, że zakładał, że wejdzie pod koniec maja 2018, projekt nadal jest przedmiotem prac legislacyjnych na poziomie instytucji UE.

Wartość stanu prawnego jest nie do przecenienia. Dyrektywa NIS, Rozporządzenie DORA i Dyrektywa NIS2 stanowią nie tylko źródło obowiązków dla podmiotów zobowiązanych, ale też źródło standardu cyberbezpieczeństwa dla podmiotów nie będących przedmiotem wymogów prawnych.

3.1. Podmioty zobowiązane na gruncie ustawy o KSC

Ustawa o KSC nakłada prawa i obowiązki na:

operatorów usług kluczowych | dostawców usług cyfrowych | podmioty publiczne

Operator usługi kluczowej ma status kwalifikowany, gdyż może nim być wyłącznie podmiot, wobec którego organ właściwy, tj. minister odpowiedzialny za dany dział administracji rządowej, wydał decyzję administracyjną o uznaniu za operatora usługi kluczowej. Są to podmioty należące do sektorów takich jak sektor energii, transportu, bankowość i infrastruktura rynków finansowych, ochrona zdrowia, zaopatrzenie w wodę pitną i jej dystrybucja i infrastruktura cyfrowa. Zatem są to podmioty które mogą być kojarzone jako obiekty szeroko rozumianego sabotażu.

Samo świadczenie usługi kluczowej nie jest wystarczającą przesłanką do wydania decyzji administracyjnej o uznaniu podmiotu za operatora usługi kluczowej, niezbędne jest także, by:

- świadczenie usługi kluczowej w jednym z ww. sektorów zależało od systemów informacyjnych;
- incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej przez tego operatora.

Próg istotności skutku zakłócającego incydentu ustala się biorąc pod uwagę m. in. liczbę użytkowników usługi kluczowej, udział podmiotu świadczącego usługę kluczową w rynku, czy też wpływ, jaki mógłby mieć incydent, ze względu na jego skalę i czas trwania, na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne.

Drugim adresatem praw i obowiązków wynikających z ustawy o KSC jest **dostawca usługi cyfrowej,** którym jest z kolei osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, mająca siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, świadcząca usługę cyfrową.

Usługą cyfrową jest:

INTERNETOWA PLATFORMA HANDLOWA	Usługa, która umożliwia konsumentom lub przedsiębiorcom zawieranie umów drogą elektroniczną z przedsiębiorcami na stronie internetowej platformy handlowej albo na stronie internetowej przedsiębiorcy, który korzysta z usług świadczonych przez internetową platformę handlową. Jest to zatem każdy serwis internetowy, który umożliwia przedsiębiorcom zawieranie umów drogą elektroniczną – jednym słowem, nawet najprostszy marketplace.
USŁUGA PRZETWARZANIA W CHMURZE	Usługa umożliwiająca dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników. Zatem, nie jest to chmura prywatna.
WYSZUKIWARKA INTERNETOWA	Usługa, która umożliwia użytkownikom wyszukiwanie wszystkich stron internetowych lub stron internetowych w danym języku za pomocą zapytania przez podanie słowa kluczowego, wyrażenia lub innego elementu, przedstawiającą w wyniku odnośniki, odnoszące się do informacji związanych z zapytaniem.

Ustawa o KSC przewiduje jeden wyjątek od uznania, że mamy do czynienia z dostawcą usługi cyfrowej, mianowicie posiadanie statusu mikroprzedsiębiorcy lub małego przedsiębiorcy, tj.:

Mikroprzedsiębiorcą jesteś, jeżeli w co najmniej jednym z dwóch ostatnich lat obrotowych:

- zatrudniałeś mniej niż 10 pracowników;
- roczny obrót netto (czyli sprzedaż usług, towarów, wyrobów i operacji finansowych) nie przekroczył równowartości w złotych 2 milionów euro;
- suma aktywów bilansu sporządzonego na koniec jednego z tych lat nie przekroczyła równowartości w złotych 2 milionów euro.

Małym przedsiębiorcą jesteś, jeżeli co najmniej w jednym z dwóch ostatnich lat obrotowych:

- zatrudniałeś mniej niż 50 pracowników;
- roczny obrót netto (czyli sprzedaż usług, towarów, wyrobów i operacji finansowych) nie przekroczył równowartości w złotych 10 milionów euro;
- suma aktywów bilansu sporządzonego na koniec jednego z tych lat nie przekroczyły równowartości w złotych 10 milionów euro.

A zatem np. działalność w postaci prowadzenia internetowej platformy umożliwiającej zakup towarów, prowadzona przez małego przedsiębiorcę, nie będzie kwalifikowana jako usługa cyfrowa w rozumieniu ustawy o KSC.

Ustawa o KSC przewiduje wyłączenia podmiotowe, gdyż **nie stosuje** się jej do:

- przedsiębiorców telekomunikacyjnych w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów;
- kwalifikowanych i niekwalifikowanych dostawców usług zaufania w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej

i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE;

- podmiotów wykonujących działalność leczniczą, tworzonych przez Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu.

3.2. Obowiązki przedsiębiorców na gruncie ustawy o KSC

Przedsiębiorca może być adresatem praw i obowiązków wynikających z ustawy o KSC, występując w roli:
- operatora usługi kluczowej;
- dostawcy usługi cyfrowej.

3.2.1. Incydent

Aby zrozumieć istotę obowiązków przedsiębiorców na gruncie ustawy o KSC należy przede wszystkim wyjaśnić kluczowe pojęcie, tj. incydent.

Definicja tego pojęcia jest bardzo szeroka, gdyż incydentem jest:

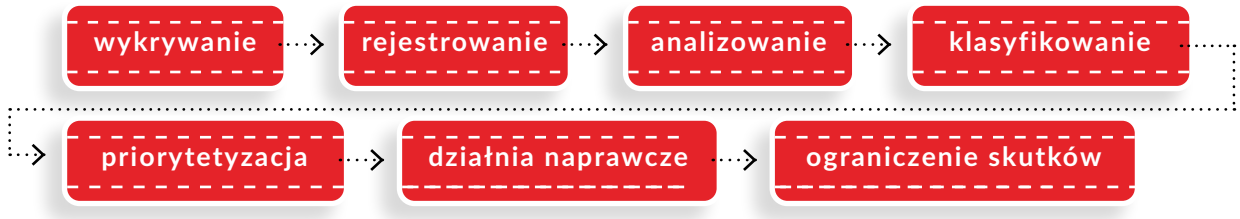
incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo, tj. na odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

Ustawa o KSC wskazuje następujące incydenty:

KRYTYCZNY	• incydent o najpoważniejszym charakterze, skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi; • klasyfikowane przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV;
POWAŻNY	• zgłaszany przez operatora usługi kluczowej; • powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej;
ISTOTNY	• zgłaszany przez dostawców usług cyfrowych; • ma istotny wpływ na świadczenie usługi cyfrowej.

Jak wynika z powyższego, incydent istotny może wystąpić wyłącznie w przypadku usługi cyfrowej, a incydent poważny wyłącznie w przypadku usługi kluczowej. Natomiast incydent krytyczny występuje w obu przypadkach, ale decyzja o przyznaniu takiej kategorii nie leży w gestii przedsiębiorcy, a w gestii właściwego CSIRT.

Obsługa incydentu, jako ustrukturyzowany proces, składa się z kilku faz i obejmuje następujące po sobie czynności począwszy od wykrycia aż do usunięcia jego skutków:



3.2.2. Obowiązki operatora usługi kluczowej

Z racji pełnionej funkcji obowiązki operatora usługi kluczowej są znacznie bardziej rozbudowane niż obowiązki dostawcy usługi cyfrowej.

W terminie **3 miesięcy** od doręczenia decyzji o uznaniu za OUK	• prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem; • zarządzanie incydentami; • wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami KSC; • zapewnienie użytkownikowi usługi kluczowej dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową, w szczególności przez publikowanie informacji na ten temat na swojej stronie internetowej; • przekazanie organowi właściwemu do spraw cyberbezpieczeństwa dane, o których mowa w art. 7 ust. 2 pkt 8 i 9 ustawy o KSC, nie później niż w terminie 3 miesięcy od zmiany tych danych; • obsługę incydentu i klasyfikacja incydentu jako poważny; • zapewnienie dostępu do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV; • zgłoszenie incydentu poważnego niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV; • współdziałanie podczas obsługi incydentu poważnego i krytycznego z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV; • usuwanie podatności oraz informowanie o ich usunięciu organu właściwego do spraw cyberbezpieczeństwa; • powołanie wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo lub zawarcie umowy z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa.
W terminie **6 miesięcy** od doręczenia decyzji o uznaniu za OUK	• wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych; • zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej; • stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej; • stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa; • opracowanie, stosowanie i aktualizacja dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego; • ustanowienia nadzoru nad dokumentacją dotyczącą cyberbezpieczeństwa systemu informacyjnego; • zapewnienie przechowywania dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego przez co najmniej 2 lata od dnia jej wycofania z użytkowania lub zakończenia świadczenia usługi kluczowej.
W terminie **1 roku** od doręczenia decyzji o uznaniu za OUK	• zapewnienie przeprowadzenia, co najmniej raz na 2 lata, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej.

3.2.3. Obowiązki dostawcy usługi cyfrowej

Do głównych obowiązków dostawcy usługi cyfrowej należy:

- wdrożenie właściwych i proporcjonalnych środków technicznych i organizacyjnych w celu zarządzania ryzykiem, na jakie narażone są systemy informacyjne wykorzystywane do świadczenia usługi cyfrowej;
- przeprowadzenie czynności umożliwiających wykrywanie, rejestrowanie, analizowanie oraz klasyfikowanie incydentów;
- zapewnienie w niezbędnym zakresie dostępu do informacji właściwemu CSIRT o incydentach zakwalifikowanych jako krytyczne przez właściwy CSIRT;
- klasyfikacja incydentu jako istotny;
- zgłaszanie incydentu istotnego niezwłocznie, nie później jednak niż w ciągu 24h od momentu wykrycia, do właściwego CSIRT, chyba że nie posiada on informacji pozwalających na ocenę istotności wpływu incydentu na świadczenie usługi cyfrowej;
- zapewnienie obsługi incydentu istotnego i incydentu krytycznego we współpracy z właściwym CSIRT;
- usuwanie podatności;
- przekazywanie operatorowi usługi kluczowej, który świadczy usługę kluczową za pośrednictwem tego dostawcy usługi cyfrowej, informacje dotyczące incydentu mającego wpływ na ciągłość świadczenia usługi kluczowej tego operatora;
- podejmowanie środków zapobiegających i minimalizujących wpływ incydentów na usługę cyfrową i zapewnienie jej ciągłości.

3.3. Spółka świadczy usługi nie mieszczące się w wykazie usług objętych ustawą o KSC – czy cyberbezpieczeństwo jej nie dotyczy?

Wdrożenie środków z zakresu cyberbezpieczeństwa powinno być elementem funkcjonowania każdej firmy. Ustawa o KSC wprawdzie nakłada obowiązki wyłącznie na określone podmioty, nie oznacza to jednak, że inni przedsiębiorcy nie są zagrożeni cyberprzestępczością. O ile w takim przypadku nie musimy stosować przepisów ustawy o KSC, dbałość o interes firmy nakazuje zachowanie szczególnej staranności.

Celem cyberataku mogą być bowiem zasoby informatyczne, mienie, wiedza, dane czy też przewaga rynkowa każdej firmy. Nie bez znaczenia jest także atak Rosji na Ukrainę, który skutkował wzmożonym zagrożeniem w sferze cyfrowej, w konsekwencji czego wprowadzono stopień alarmowy CHARLIE-CRP.[2]

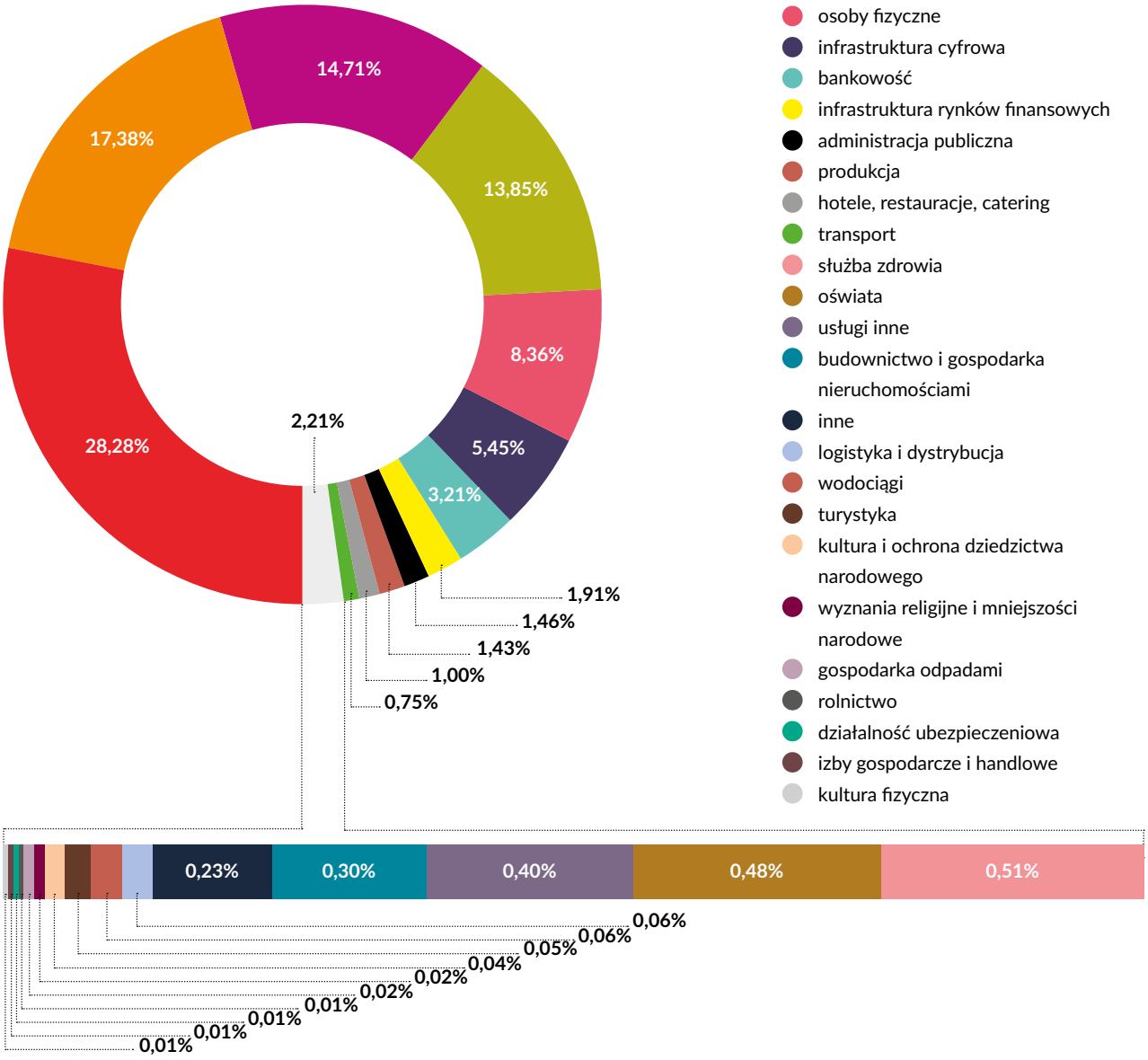
Jak wskazał w swym raporcie CERT, nie istnieje właściwie branża, która nie byłaby narażona na ataki cyberbezpieczeństwa. W 2021 r. najwięcej incydentów odnotowano w sektorze:

- mediów;
- handlu hurtowego i detalicznego;
- usług pocztowych (w tym poczty elektronicznej) i kurierskich.

[2] UWAGA – wprowadzono 3 stopień alarmowy CHARLIE-CRP - Baza wiedzy - Portal Gov.pl (www.gov.pl)

Nie oznacza to, że przedstawiciele innych branż mogli spać spokojnie:

sektory gospodarki



Powyższa tabela pokazuje, że praktycznie nie istnieje sektor gospodarki wolny od cyberataków. Nie tylko każdy przedsiębiorca, ale przede wszystkim każdy użytkownik Internetu powinien zadbać o swoje bezpieczeństwo informatyczne.

A zatem:

- cyberprzestępczość grozi nie tylko podmiotom wskazanym w ustawie o KSC ale każdej firmie, zwłaszcza takiej która ma swoje zasoby w chmurze obliczeniowej lub korzysta z internetu;
- na cyberataki narażone są zwłaszcza systemy informatyczne i aplikacje (na przykład system CRM, MS Office, system do zarządzania księgowością, aplikacje służące do wewnętrznej obsługi firmy), urządzenia mobilne i laptopy oraz serwery i sieć;
- cyberatak może zagrażać każdemu działowi w firmie: sprzedaży, marketingu, księgowości, prawnemu czy też finansów.

Zmiany w prawie

4. ZMIANY W PRAWIE

4.1. DORA

Rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniającego rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 („**DORA**") **rozpocznie stosowanie po upływie 24 miesięcy od jego wejścia w życie, czyli od 17 stycznia 2025 roku.**

DORA obejmie:

- instytucje finansowe, w tym m.in.:
  - instytucje kredytowe i płatnicze;
  - dostawców świadczących usługę dostępu do informacji o rachunku;
  - instytucje pieniądza elektronicznego;
  - dostawców usług w zakresie kryptoaktywów, którzy uzyskali zezwolenie na mocy rozporządzenia w sprawie rynków kryptoaktywów;
  - emitentów tokenów powiązanych z aktywami;
- zarządzających alternatywnymi funduszami inwestycyjnymi;
- spółki zarządzające[3];
- zewnętrznych dostawców usług technologii informacyjno-telekomunikacyjnych (information and communication technologies – **ICT**)[4].

Należy przy tym zaznaczyć, że dokładne definicje powyższych podmiotów znajdują się w DORA oraz powiązanych aktach prawnych, do których odniesienia znajdują się w DORA, tj. MICA[5].

Zgodnie z DORA, wyżej wymienione podmioty powinny:

- wprowadzić ramowe zasady zarządzania ryzykiem ICT;
- używać i utrzymywać zaktualizowane systemy ICT;
- utworzyć i wdrożyć polityki i procedury związane z bezpieczeństwem ICT;
- utworzyć i wdrożyć procedury, które pozwolą zarządzać incydentami związanymi z ICT;
- zgłaszać poważne incydenty związane z ICT do odpowiednich organów w czasie uzależnionym od sytuacji;
- przeprowadzać regularne testy operacyjnej odporności cyfrowej.

Niedopełnienie obowiązków skutkować może użyciem przez organy nadzorcze środków zapobiegawczych (zakaz prowadzenia działalności, publiczne ogłoszenie sankcji) i nałożeniem administracyjnych kar pieniężnych. Z uwagi na okoliczność, że DORA jest rozporządzeniem unijnym, będzie stosowana bezpośrednio we wszystkich państwach UE.

[3] „spółka zarządzająca" oznacza spółkę zarządzającą w rozumieniu art. 2 ust. 1 lit. b) dyrektywy 2009/65/WE;
[4] „zewnętrzny dostawca usług ICT" oznacza przedsiębiorstwo świadczące usługi cyfrowe i usługi w zakresie danych, w tym dostawców usług w chmurze, oprogramowania, usług analizy danych, ośrodków przetwarzania danych, ale z wyłączeniem dostawców komponentów sprzętowych i przedsiębiorstw, które uzyskały zezwolenie na mocy prawa Unii i świadczą usługi łączności elektronicznej, o których mowa w art. 2 pkt 4 of dyrektywy Parlamentu Europejskiego i Rady (UE), 2018/1972
[5] ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY w sprawie rynków kryptoaktywów i zmieniające dyrektywę (UE) 2019/1937

4.2. NIS2

27 grudnia 2022 r. w Dzienniku Urzędowym Unii Europejskiej opublikowano Dyrektywę NIS2.

Od wejścia dyrektywy w życie, państwa członkowskie będą miały 21 miesięcy na jej wprowadzenie do krajowych porządków prawnych – termin upływa 16 października 2024 roku.

Kogo obejmie NIS2 (**Podmioty NIS2**)?

- Podmioty kluczowe z następujących sektorów:
  - energetyka;
  - transport;
  - bankowość;
  - infrastruktura rynków finansowych;
  - opieka zdrowotna;
  - woda pitna;
  - ścieki;
  - infrastruktura cyfrowa;
  - zarządzanie usługami ICT;
  - administracja publiczna;
  - przestrzeń kosmiczna.

- Podmioty ważne z następujących sektorów:
  - usługi **pocztowe** i kurierskie;
  - gospodarowanie **odpadami**;
  - produkcja, wytwarzanie i dystrybucja **chemikaliów**;
  - produkcja, przetwarzanie i dystrybucja **żywności**;
  - produkcja;
  - usługi cyfrowe;
  - badania naukowe.

Najważniejsze postanowienia NIS2:

- wprowadzono obowiązki organów zarządzających Podmiotów NIS2:
  - zatwierdzanie środków zarządzania ryzykiem w zakresie cyberbezpieczeństwa;
  - nadzorowanie wdrażania środków zarządzania ryzykiem;
  - uczestnictwo w regularnych szkoleniach dotyczących rozumienia i oceny ryzyka związanego z cyberbezpieczeństwem;
  - ponoszenie odpowiedzialności za nieprzestrzeganie postanowień dyrektywy;

- wprowadzono dla Podmiotów NIS2 obowiązek wprowadzenia środków zarządzania ryzykiem w cyberprzestrzeni:
  - analiza ryzyka i polityka bezpieczeństwa systemów informacyjnych;
  - procedura postępowania w przypadku incydentów (zapobieganie incydentom, wykrywanie ich i reagowanie na nie);
  - ciągłość działania i zarządzanie kryzysowe;
  - bezpieczeństwo łańcucha dostaw, w tym bezpieczeństwo stosunków między Podmiotem NIS2 a jego bezpośrednimi dostawcami lub usługodawcami;
  - bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym postępowanie w przypadku podatności i ich identyfikacja;
  - polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie;
  - podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa;

- polityki i procedury stosowania kryptografii i w stosownych przypadkach szyfrowania;
- bezpieczeństwo zasobów ludzkich, politykę kontroli dostępu i zarządzanie aktywami;
- w stosownych przypadkach – stosowanie uwierzytelniania wieloskładnikowego lub ciągłego, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych;

- nałożenie na Podmioty NIS2 obowiązku zgłaszania istotnych incydentów właściwym organom w ciągu 24 godzin od uzyskania informacji o incydentach istotnych.

Podmioty NIS2 naruszające obowiązki wynikające z NIS2 będą podlegały administracyjnym karom pieniężnym w wysokości do 10 000 000 EUR lub 2% całkowitego rocznego światowego obrotu przedsiębiorstwa. NIS2 jako dyrektywa pozostawia organom krajowym swobodę wyboru formy i środków jej wdrożenia do krajowego systemu prawnego (nie musi być stosowana bezpośrednio).

Zagrożenia wynikające z cyberprzestępczości dla przedsiębiorców

5. ZAGROŻENIA WYNIKAJĄCE Z CYBERPRZESTĘPCZOŚCI DLA PRZEDSIĘBIORCÓW

Cyberataki wymierzone są w podstawowe zasoby firmy takie jak dane techniczne, dane pracowników i klientów, konta bankowe czy wszelkie inne informacje mające postać cyfrową. Skutki dostępu do takich informacji osób trzecich mogą być wielorakie:

- paraliż firmy i utrata ciągłości działania firmy, a w konsekwencji straty finansowe;
- utrata przewagi rynkowej;
- naruszenie zawartych z kontrahentami umów o ochronie informacji niejawnych na skutek niezachowania bezpieczeństwa informacji;
- utrata danych;
- szkody w mieniu w postaci np. uszkodzenia serwerów;
- konieczność zakupu nowych systemów, dodatkowych zabezpieczeń i urządzeń;
- szkodliwy wpływ na wizerunek firmy.

Najczęstsze formy ataków na firmy to:

Phishing	• polega ona na podszywaniu się „przestępcy" pod całkowicie inną osobę bądź instytucję; • celem ataku jest nakłonienie użytkownika do podjęcia określonego działania, na przykład kliknięcia w zainfekowany link lub pobrania dokumentu w celu zainfekowania systemu; • celem jest wyłudzenie informacji, np. danych logowania, danych osobistych lub innych, poufnych informacji.
Ransomware/ szkodliwe oprogramowanie	• większość ataków zaczyna się od złośliwej wiadomości e-mail, której otworzenie powoduje instalację złośliwego oprogramowania w celu przejęcia zasobów firmy; • wykorzystywane do szyfrowania danych; • celem takiego ataku jest wymuszenie okupu za odzyskanie danych.
DoS (Denial of Service)	Polega na „zalaniu" dużej liczby danych, zapytań i informacji z wielu (nawet setek tysięcy) komputerów z całego świata, co powoduje przeciążenie systemu a w konsekwencji awarii serwerów.

5.1. Przykłady incydentów cyberbezpieczeństwa

O tym, jakie mogą być praktyczne skutki cyberataków, najdobitniej pokazują przykłady praktyczne. Poniżej opisane przykłady pokazują, że cyberataki grożą zarówno gigantom jak i małym firmom.

Przykład nr 1:
Jedna z polskich firm zawarła umowę na świadczenie usług utrzymania jednego z systemów informatycznych z zewnętrznym, profesjonalnym wykonawcą usług IT. Na skutek braku zachowania właściwych środków bezpieczeństwa przez wykonawcę usług IT, dostęp do wszystkich zasobów informatycznych firmy uzyskali cyberprzestępcy, wykorzystując tzw. tunelowanie i fakt połączenia zdalnego wykonawcy usług IT z systemami firmy. Sprawców cyberataku nie udało się ustalić, a na jego skutek:

- firma utraciła bezpowrotnie część danych biznesowych;
- firma zmuszona była zamówić dodatkowe usługi mające na celu odtworzenie danych i zabezpieczenie dowodów;
- firma zmuszona była wdrożyć w trybie natychmiastowym dodatkowe zabezpieczenia, nieprzewidziane w budżecie;
- wyrządzone zostały szkody majątkowe.

Łączne straty wyceniono na kilkaset tysięcy złotych.

Przykład nr 2:
W maju 2022 r. operator sieci rurociągów paliwowych, dostarczających benzynę i paliwo lotnicze, był celem ataku ransomware, polegającego na infekowaniu systemów złośliwym oprogramowaniem zaprojektowanym do blokowania tych systemów poprzez szyfrowanie danych. W konsekwencji ataku, systemy informatyczne firmy zostały całkowicie wyłączone na 6 dni, co spowodowało całkowite zawieszenie działalności firmy. Przerwa spowodowała panikę wśród kupujących, skok cen paliwa oraz brak paliwa na wielu stacjach w południowo-wschodnich stanach USA.

Przedsiębiorca zmuszony był do zapłacenia przestępcom okupu wynoszącego ok. 5 mln USD, po zapłaceniu którego otrzymała narzędzie do deszyfracji zakodowanych przez wirusa danych. Deszyfryzacja przebiegała bardzo powoli, co generowało dodatkowe straty po stronie firmy. Mimo oferowania przez rząd USA nagrody w wysokości $10 mln, nie udało się schwytać sprawców ataku. Atak stał się przyczyną zapowiedzi zmian legislacyjnych w zakresie cyberbezpieczeństwa w prawie USA.

Prawa wyłączne służące ochronie cyberbezpieczeństwa

6. PRAWA WYŁĄCZNE SŁUŻĄCE OCHRONIE CYBERBEZPIECZEŃSTWA

Poza warstwą regulacyjną, wyznaczoną reżimem NIS, NIS2, DORA, nie należy zapominać o kontekście praw wyłącznych, które odgrywają ważną rolę w każdym procesie wdrożenia cyberbezpieczeństwa oraz w razie zaistnienia cyberincydentu. Są to również narzędzia ochrony prawnej – prawa te stanowią podstawę roszczeń w razie ewentualnych naruszeń w toku cyberincydentu.

6.1. Tajemnica przedsiębiorstwa

Kluczem powodzenia biznesu jest pomysł na działalność gospodarczą i know-how. Tajemnica przedsiębiorstwa i regulacja ustawy o zwalnianiu nieuczciwej konkurencji są środkami, które z prawnego punktu widzenia zapewniają ochronę know-how. Przewaga rynkowa często wynika ze specjalistycznych informacji, którymi dysponuje dany przedsiębiorca, a zatem powinien on podjąć wszelkie środki zapewniające jej ochronę, przede wszystkim w środowisku cyfrowym, narażonym na cyberataki.

Zgodnie z ustawą o zwalczaniu nieuczciwej konkurencji, przez tajemnicę przedsiębiorstwa należy rozumieć: *informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów* ***nie są powszechnie znane*** *osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób,* ***o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności***[6].

Jak widać, w tajemnicę przedsiębiorstwa zaszyty jest element poufności i obowiązek podjęcia przez przedsiębiorcę środków w celu zachowania informacji w tajemnicy.

Cyberprzestępczość jest realnym zagrożeniem dla tajemnicy przedsiębiorstwa, gdyż:

- ujawnienie informacji poufnych w drodze cyberataku powoduje, że trudniej przedsiębiorcy na drodze sądowej chronić swoje know-how, gdyż mogą nie być spełnione wymagania ustawowe braku powszechnej znajomości tych informacji;
- przedsiębiorca zobowiązany jest, z zachowaniem należytej staranności, podjąć środki w celu utrzymania poufności informacji, w szczególności środków i zabezpieczeń technologicznych i organizacyjnych, np. kontrola dostępu, blokady informatyczne, zawieranie umów o zachowaniu poufności, tzw. NDA, ostrzeżenia umieszczone na dokumentach, dostęp jedynie wybranych osób do informacji, ograniczony dostęp do pomieszczeń, dysków lub folderów, w których znajduje się poufna informacja, monitoring dostępu, zabezpieczenia hasłami, inne zabezpieczenia techniczne;
- ujawnienie tajemnicy przedsiębiorcy może mieć realny wpływ na jego przewagę rynkową i powodzenie prowadzonej działalności gospodarczej. Tajemnica przedsiębiorstwa ma wartość gospodarczą, czyli taką wartość, która pozwala choćby minimalnie na zwiększenie produkcji, zmniejszenie kosztów, itp.

Ustawa o zwalczaniu nieuczciwej konkurencji daje ochronę prawną tajemnicy przedsiębiorstwa przed jej:

- przekazaniem;
- ujawnieniem;
- wykorzystaniem;
- nabyciem od osoby nieuprawnionej.

Odpowiedzialna będzie także osoba, która była związana umową o pracę, o dzieło, zlecenia lub inną.
Jest to **odpowiedzialność cywilna**, jednak ustawa również przewiduje **odpowiedzialność karną** za naruszenie tajemnicy przedsiębiorstwa – do dwóch lat pozbawienia wolności.

[6] art. 11 ustawy o zwalczaniu nieuczciwej konkurencji

Pamiętać należy, że **prawa własności przemysłowej**, takie jak patenty, znaki towarowe, wzory przemysłowe, wraz ze zgłoszeniem i rejestracją są publikowane, więc także **stają się publiczne**. Istotne jest zaznaczenie, iż nawet jeżeli jeden lub kilka elementów urządzenia są jawne, gdyż chociażby są przedmiotem patentu na wynalazek, to informacje dotyczące całości urządzenia lub np. jego złożenia mogą być objęte tajemnicą przedsiębiorstwa. Te kwestie powinny być uwzględnione przy podejmowaniu decyzji o tym, jak chronić informacje istotne z punktu widzenia przedsiębiorcy.

Umowa o korzystanie z informacji poufnych lub know-how lub tajemnicy przedsiębiorstwa, w zależności od decyzji stron może zawierac szereg postanowień. Z reguły postanowienia takiej umowy dotyczą:

- otrzymywania informacji przez jedną ze stron;
- uzyskania uprawnienia do konkretnego korzystania z tych informacji;
- wysokości lub braku wynagrodzenia;
- zobowiązania do zachowania informacji w poufności pod groźbą zapłaty kar umownych.

6.2. Prawa autorskie

Niewiele warunków musi być spełnionych do objęcia jakiegoś wytworu intelektu ludzkiego ochroną prawno-autorską. Ochrona z tytułu prawa autorskiego przysługuje twórcom utworów, a utworem jest:

- każdy przejaw działalności twórczej o indywidualnym charakterze; wymagany jest warunek twórczości – procesu polegającego na ustaleniu przez człowieka jego twórczej natury. Jest to warunek subiektywny – tj. twórca musi być wewnętrznie przeświadczony o tym, że tworzy coś indywidualnego (nie musi być to utwór nowy) a utwór musi mieć tzw. indywidualne piętno twórcy;
- ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia;
- ochroną objęty może być wyłącznie sposób wyrażenia; nie są objęte ochroną odkrycia, idee, procedury, metody i zasady działania oraz koncepcje matematyczne;
- im bardziej techniczne wymogi wpływają na treść przedmiotu, tym mniejsza jest twórczość;
- brak wymogu rejestracji – prawa powstają poprzez ustalenie utworu.

Co więcej, ochroną prawno-autorską mogą być objęte bazy danych (tzw. twórcze bazy danych).

Zatem, w kontekście cyberbezpieczeństwa to sposoby wyrażenia danych (raporty, wykresy, dokumentacja itp.) mogą być przedmiotem ochrony prawa autorskiego. Osoba nieuprawniona do ich wykorzystania może być adresatem odpowiednich roszczeń.

6.3. Prawa do baz danych

Oprócz ochrony prawnoautorskiej, ustawodawca daje ochronę bazom, które nie będą chronione jak utwory (tj. nie są twórcze i nie podlegają ochronie jak utwory).

Bazy danych to ustrukturyzowane zestawienia danych, wymagające istotnego nakładu inwestycyjnego w celu sporządzenia, weryfikacji lub prezentacji ich zawartości.

Prawa producentów baz danych stanowią odrębny przedmiot praw i obrotu gospodarczego. Wyłącznymi i zbywalnymi prawami producentów baz danych są prawa do pobierania danych i wtórnego ich wykorzystania w całości lub w istotnej części, co do jakości lub ilości. Osoba nieuprawniona do ich wykorzystania może być adresatem odpowiednich roszczeń.

Cyberbezpieczeństwo – dobre praktyki dla przedsiębiorców

7. CYBERBEZPIECZEŃSTWO – DOBRE PRAKTYKI DLA PRZEDSIĘBIORCÓW

Wskazanie wyczerpującego katalogu środków, jakie należy podjąć w celu ochrony przed cyberatakami nie jest możliwe – stałe doskonalenie narzędzi przez hakerów powoduje, że raz podjęte środki muszą podlegać aktualizacji. W przeciwnym razie może okazać się, że wdrożone środki po upływie np. 5 lat okażą się niewystarczające by ochronić zasoby firmy.

Przygotowania firmy do cyberbezpieczeństwa powinny przebiegać w dwóch kierunkach:

PRZYGOTOWANIA ORGANIZACYJNE:
procedury wewnętrzne, szkolenia personelu

PRZYGOTOWANIA TECHNOLOGICZNE:
zakup sprzętu i systemów

Rekomendowany schemat przygotowania firmy:

I. INWENTARYZACJA DANYCH	• Przegląd informacji pod kątem zidentyfikowania tych, które wymagają zapewnienia szczególnych środków bezpieczeństwa; • Zapewnienie odpowiedniego poziomu ochrony krytycznym informacjom.
⋮	
II. MAPOWANIE SYSTEMÓW I INFRASTRUKTURY	• Przegląd zabezpieczeń sieci, systemów i baz danych; • Przegląd oprogramowania pod kątem braku wsparcia i aktualizacji; • Przegląd zabezpieczeń komputerów, laptopów i innych urządzeń mobilnych; • Przegląd systemu tworzenia kopii zapasowych; • Testy penetracyjne mające na celu wykrycie luk i podatności w systemach IT.
⋮	
III. WDROŻENIE ŚRODKÓW TECHNICZNYCH	• Zapewnienie bezpieczeństwa na etapie projektowania i zamawiania systemów IT; • Utworzenie systemu kopii zapasowych; • Zapewnienie bezpiecznych kanałów komunikacji, w tym wprowadzenie obowiązku szyfrowania poczty elektronicznej, szyfrowanego kanału komunikacji (SSL); • Stały monitoring sieci; • Aktualizacja oprogramowania; • Zapewnienie bezpieczeństwa fizycznego budynków.
⋮	
IV. MAPOWANIE UMÓW	• Weryfikacja zawartych umów pod kątem potrzeby dodania postanowień przewidujących obowiązek zapewnienia przez kontrahentów bezpieczeństwa udostępnionych przez nas informacji; • Zawieranie umów o ochronie informacji niejawnych już na etapie negocjacji umów przewidujących m. in. obowiązek zapewnienia bezpieczeństwa danych i kary umowne za naruszenie poufności danych.
⋮	
V. PROCEDURY I STRUKTURA	• Powołanie zespołu reagowania na incydenty cyberbezpieczeństwa; • Wdrożenie procedury postępowania na wypadek incydentu; • Cykliczne testy procedury postępowania na wypadek incydentu; • Wdrożenie polityk i reguł zarządzania dostępem do danych, systemów i aplikacji; • Wdrożenie planu ciągłości działania firmy.
⋮	

VI. SZKOLENIA PERSONELU	• Szkolenia nowych pracowników i cykliczne szkolenia całego personelu z wewnętrznych procedur dotyczących cyberbezpieczeństwa; • Cykliczne szkolenia personelu w celu poszerzenie świadomości i wiedzy na temat cyberataków; • Ćwiczenia na podatność pracowników na socjotechnikę (np. podatność na otwieranie zainfekowanej korespondencji mailowej, udostępnianie haseł nieupoważnionym osobom).
VII. CYKLICZNY PRZEGLĄD I MONITORING PROCEDUR I SUSTEMÓW	• Weryfikacja adekwatności procedur wewnętrznych; • Reakcja na zmiany w środowisku prawny i technologicznym; • Testy bezpieczeństwa i podatności pracowników na socjotechnikę.

O czym należy pamiętać?

- Największą podatnością na cyberatak jest człowiek, dlatego ważne jest cykliczne szkolenie personelu.
- Należy zwracać uwagę na wczesne symptomy cyberataku:
  - spowolnione działanie urządzeń i aplikacji;
  - niewyjaśnione znikanie plików lub pojawianie się nowych plików;
  - rozsyłanie spamu przez pracowników.
- Należy pamiętać o bieżącej aktualizacji oprogramowania, wykonywaniu kopii zapasowych danych i wprowadzeniu polityki haseł, w szczególności:
  - uwierzytelnianie silnym hasłem lub uwierzytelnianie dwuskładniowe;
  - cykliczne, wymuszone zmiany haseł;
  - zakaz ujawniania haseł, np. zapisywania na karteczkach przyklejonych do monitora;
  - konieczności stosowania różnych haseł do różnych urządzeń i systemów.
- Kopia zapasowa danych powinna być składowana w innym miejscu lub urządzeniu, niż to, w którym zazwyczaj dane te są przetwarzane.
- Wykwalifikowany personel IT jest podstawą bezpieczeństwa IT w firmie.
- W przypadku dużych firm ręczne zarządzanie dostępem i tożsamością może nie być możliwe, warto zainwestować w systemy typu IAM (Identity and Access Management), system zautomatyzowanego zarządzania tożsamością i dostępem.
- Urządzenia mobilne (smartfony, tablety itp.) częściej ulegają zniszczeniu czy zagubieniu niż atakowi, należy ograniczyć ich użycie i rodzaj przetwarzanych w nich danych.
- Należy zapewnić system pozwalający zarządzenie użytkownikami i ich uprawnieniami dostępowymi do systemów; należy kierować się zasadą „dostępu koniecznego" a więc przyznania uprawnień tylko tym członkom personelu i do tych procesów, do których jest to konieczne.
- Po odejściu pracownika z pracy należy usunąć jego konto i zmienić hasła do wszystkich usług, do których miał dostęp, jego konto może być wykorzystane do przeprowadzenia ataku.

Praktyczne aspekty wdrożenia wymogów cyberbezpieczeństwa

8. PRAKTYCZNE ASPEKTY WDROŻENIA WYMOGÓW CYBERBEZPIECZEŃSTWA

Przede wszystkim należy sobie odpowiedzieć na pytanie jak ważne jest dla podmiotu cyberbezpieczeństwo. Dla przykładu, na pierwszy rzut oka dystrybutor blachy stalowej nie jest wystawiony na ryzyko cyberincydentu. Brak obecności on-line, zamówienia przyjmowane mailowo, listownie, telefonicznie. Niemniej jednak, nawet taka spółka ma magazyny, składa zamówienia do producentów, realizuje zamówienia klientów.

Podczas procesu mapowania okazało się, że wdrożono system ERP, połączony z EDI magazynowo-zamówieniowym. Podatności tych systemów zwiększają ryzyko niedostępności usług i całej działalności podmiotu.

Tym samym, w każdym przypadku indywidualnie należy ocenić wpierw o jakim ryzyku mówimy. W obecnych czasach pracy zdalnej i wzmożonego rozwoju handlu elektronicznego, trudno jest wyobrazić sobie system przedsiębiorstwa bez jakichkolwiek zabezpieczeń.

Oczywiście należy mierzyć siły na zamiary – w większości przypadków wystarczy wydzielenie etatu lub jego części w celu zapewnienia bezpieczeństwa, jednak to wszystko musi być poprzedzone analizą zapotrzebowania. Taka analiza powinna przede wszystkim obejmować wiedzę na temat stanu organizacji i uwzględniać poziom wiedzy poszczególnych pracowników, ich relacji i wrażliwości. W takim wypadku możliwa do zastosowania jest analiza SWOT (Strengths, Weaknesses, Opportunities, Threats – Siły, słabości, szanse i zagrożenia).

Istotnym etapem takiego procesu jest określenie misji i zadań, które mają być prowadzone przez zespół. Zasadniczo są to dwa główne cele:

- wdrażanie proaktywnych środków w celu zmniejszenia zagrożeń komputerowych incydenty bezpieczeństwa;
- reagowanie na takie incydenty, gdy się pojawią.

Wdrożenie cyberbezpieczeństwa to oczywiście koszty – podmiot wdrażający cyberbezpieczeństwo powinien rozważyć jaki zakres ochrony będzie wymagany w jego organizacji, przede wszystkim w zakresie czasowym (czy 24 godziny na dobę, czy tylko w czasie prowadzenia działalności).

ZESPOŁ CSIRT

Liczba osób, które ma być zaagażowana jest oczywiście uzależniona od rodzajów i ilości systemów informatycznych wystawionych na podatności.

Może się bowiem okazać, że wystarczającym będzie wyznaczenie dodatkowych całych etatów lub ustalenie nowych obowiązków wśród obecnych pracowników.

Ważne, by, jak wskazuje ENISA (europejska agencja ds. cyberbezpieczeństwa), osoby zaangażowane w prace zespołu reagowania na incydenty były z różnych departamentów przedsiębiorstwa. Osoba zarządzająca powinna być odpowiedzialna za kierunek przygotowań i reakcji na cyberincydenty. To oczywiście wpływa na koszta (księgowa/CFO); komunikację zewnętrzną (należy poinformować publikę o zagrożeniu); oraz działania prawne (zarówno przygotowanie dokumentacji jak i reakcja na cyberincydenty wymaga wiedzy i zaangażowania prawnika). Naturalnie, to zespół techniczny będzie odpowiedzialny za identyfikację zagrożeń i zaproponowanie rozwiązania.

Role zespołów CSIRT

Działania przed incydentem:

- zbieranie informacji o podatnościach;
- ocena ryzyka związana z podatnościami – (1) zbadanie skąd pochodzi informacja (od producenta oprogramowania, zaufanej osoby trzeciej?) (2) odniesienie do systemów w przedsiębiorstwie (3) klasyfikację zagrożenia i ryzyka związanego z brakiem działania;

- wdrożenie zabezpieczeń;
- informowanie użytkowników o zagrożeniach (w tym dystrybucja rozwiązania).

Działania po incydencie:

- zbieranie informacji o zgłoszeniach;
- ocena zagrożenia;
- ustanowienie ticketu, poszukiwanie i wdrożenie rozwiązania;
- informowanie użytkowników/członków zespołu CSIRT.

Taka inwestycja w zespól CSIRT może być zrównoważona zyskami z potencjalnego outsourcingu takich zespołów. Ustanowiony zespół i sporządzona dokumentacja może być przedmiotem usług na zewnątrz przedsiębiorstwa.

NORMY ISO

Narzędziem, które może być pomocne we wdrażaniu cyberbezpieczeństwa są normy ISO. Normy ISO są przedmiotem realizacji zadań podmiotów zobowiązanych z ustawy o krajowym systemie cyberbezpieczeństwa, ale mogą stanowić pewną busolę dla podmiotów, które wdrażają cyberbezpieczeństwo poza reżimem ustawowym.

Podstawowa norma standaryzująca systemy zarządzania bezpieczeństwem informacji to ISO/IEC 27001. Norma ta zawiera ustrukturyzowane cele organizacji związane z bezpieczeństwem informacji oraz określa:

- cele pozyskanie wiedzy o kontekście organizacji, zrozumienia potrzeb i oczekiwań zainteresowanych;
- zakres systemu bezpieczeństwa (to jest kluczowy element każdego projektu cyberbezpieczeństwa – jakie dane maja być chronione i w jaki sposób)
- role kierownictwa, odpowiedzialność i uprawnienia innych podmiotów w organizacji;
- ustanowienie polityki bezpieczeństwa informacji;
- planowanie – szacowanie/ocena ryzyka, polegające na wyborze odpowiednich opcji postępowania, określeniu opcji zabezpieczeń;
- cele bezpieczeństwa informacji – co ma być zrobione, przy pomocy jakich zasobów, kto będzie odpowiedzialny, kiedy będzie to zakończone i jak będą oceniane wyniki;
- wsparcie – określenie zasoby i kompetencje potrzebne do ustanowienia, wdrożenia, utrzymywania i ciągłego doskonalenia SZBI.

Co do dokumentacji, powinna ona odpowiadać na podstawowe kwestie:

- w jaki sposób przetwarzane są informacje, zwłaszcza w odniesieniu do poufności?
- jakie środki są wdrażane przy ujawnianiu informacji, zwłaszcza jeśli informacje związane z incydentami są przekazywane innym zespołom lub stronom?

- czy istnieją względy prawne, które należy wziąć pod uwagę w odniesieniu do obsługi informacji? Przykładowo – czy są przetwarzane dane osobowe?

- czy wdrożono wymogi dotyczące korzystania z kryptografii w celu ochrony wyłączności i integralności w archiwach, w komunikacja danych, zwłaszcza pocztą elektroniczną?

Z innych przykładów, prawo nakłada na podmioty świadczące usługi z zakresu cyberbezpieczeństwa obowiązki organizacyjne:

- posiadanie, utrzymywanie i aktualizowanie systemu zarządzania bezpieczeństwem informacji spełniającym wymagania Polskiej Normy PN-EN ISO/IEC 27001 w zakresie obejmującym co najmniej świadczone usługi;

- posiadanie i udostępnianie w języku polskim i angielskim deklaracji swojej polityki działania w zakresie określonym dokumentem RFC 2350;

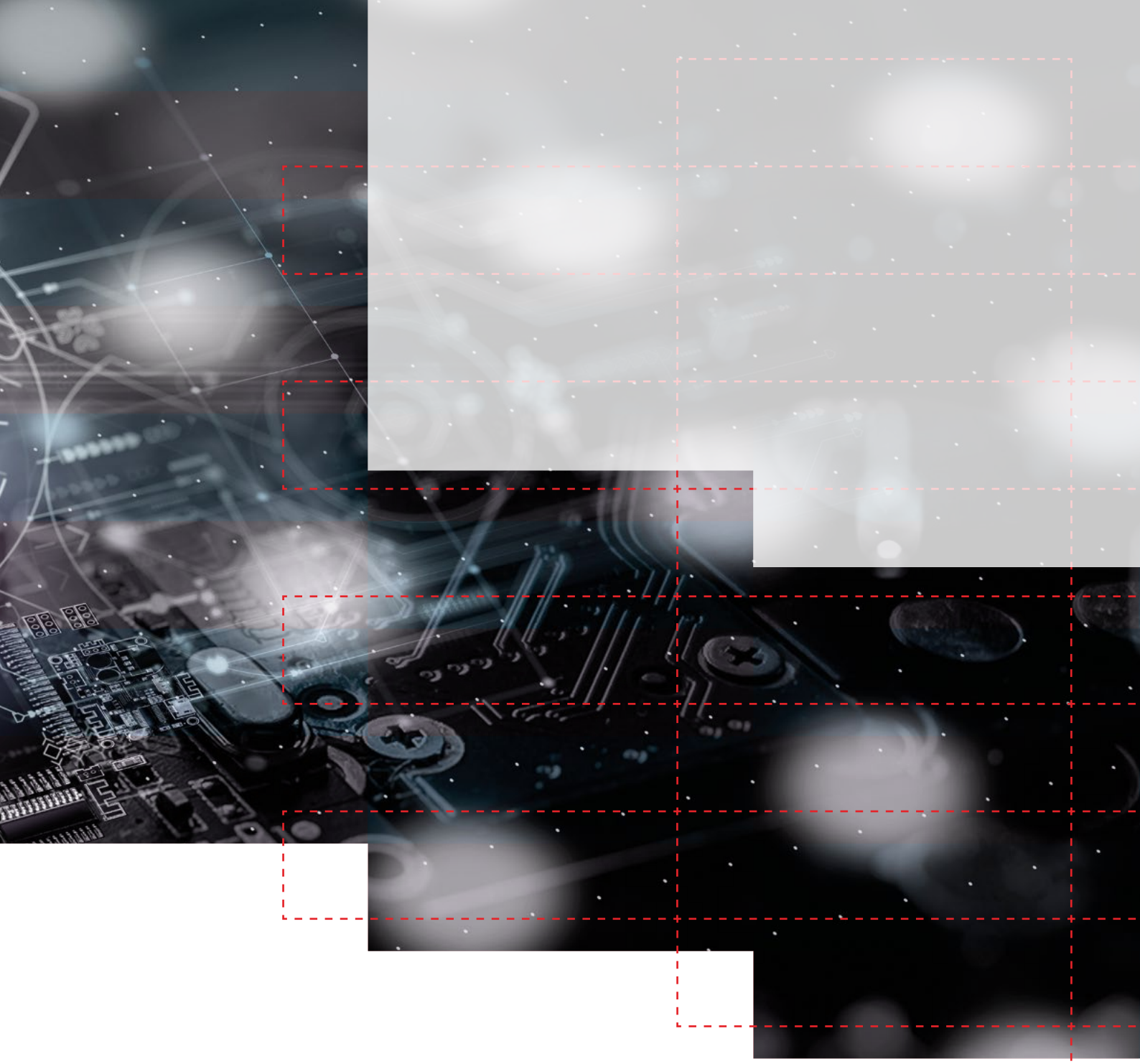
- stosowanie następującego zabezpieczenia pomieszczenia lub zespołu pomieszczeń adekwatnego do przeprowadzonego szacowania ryzyka, w tym co najmniej:
  - ściany i stropy pomieszczenia lub zespołu pomieszczeń, w których będą świadczone usługi z zakresu cyberbezpieczeństwa, powinny mieć klasę odporności ogniowej co najmniej EI 60, określoną w Polskiej Normie PN-EN 13501, a budynek, w którym będą świadczone usługi z zakresu cyberbezpieczeństwa, powinien mieć klasę odporności pożarowej nie niższą niż klasa B, określoną w przepisach wydanych na podstawie art. 7 ust. 2 pkt 1 ustawy z dnia 7 lipca 1994 r. – Prawo budowlane (Dz.U. z 2019 r. poz. 1186, z późn. zm.2));
  - drzwi do pomieszczenia lub zespołu pomieszczeń spełniające co najmniej wymagania klasy 2 określone w Polskiej Normie PN-EN 1627, wyposażone w zamek spełniający co najmniej wymagania klasy 4 określone w Polskiej Normie PN-EN 12209, o ile na podstawie przeprowadzonego szacowania ryzyka dostęp do nich rodziłby nieakceptowalne ryzyko nieuprawnionego wejścia do pomieszczenia lub zespołu pomieszczeń;
  - konstrukcję pomieszczenia lub zespołu pomieszczeń zapewniającą odporność na próbę nieuprawnionego dostępu;
  - okna spełniające co najmniej wymagania klasy 2 określone w Polskiej Normie PN-EN 1627, o ile na podstawie przeprowadzonego szacowania ryzyka dostęp do nich niesie nieakceptowalne ryzyko nieuprawnionego wejścia do pomieszczenia lub zespołu pomieszczeń;
  - szafy o podwyższonej odporności ogniowej, zabezpieczające przed próbami włamań oraz pożarami, odpowiednio do wartości danych oraz ewentualnych innych zagrożeń, na podstawie przeprowadzonego szacowanego ryzyka, służące do przechowywania dokumentacji papierowej oraz informatycznych nośników danych mających istotne znaczenie dla prowadzonej działalności;
  - system kontroli dostępu obejmujący wszystkie wejścia i wyjścia kontrolowanego obszaru, w którym co najmniej rozpoznanie osoby uprawnionej następuje w wyniku odczytu identyfikatora lub odczytu cech biometrycznych, oraz rejestrujący zdarzenia;
  - stały nadzór osoby uprawnionej nad osobami niewykonującymi czynności związanych z realizacją obowiązków, o których mowa w art. 8 pkt 4 i 6, art. 11 ust. 1 pkt 1-5, art. 12 i art. 13 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, przebywającymi w pomieszczeniu lub zespole pomieszczeń, w których wykonywane są te czynności;
  - system sygnalizacji napadu i włamania spełniający co najmniej wymagania systemu stopnia 2 określone w Polskiej Normie PN-EN 50131-1, stale monitorowany przez personel bezpieczeństwa oraz

wyposażony w rezerwowe źródło zasilania i obejmujący ochroną wejścia i wyjścia kontrolowanego obszaru oraz sygnalizujący co najmniej:

- otwarcie drzwi, okien i innych zamknięć chronionego obszaru;
- poruszanie się w chronionym obszarze;
- stan systemu, w tym generujący ostrzeżenia i alarmy;
- system sygnalizacji pożarowej obejmujący urządzenia sygnalizacyjno-alarmowe, służące do samoczynnego wykrywania i przekazywania informacji o pożarze, a także urządzenia odbiorcze alarmów pożarowych i urządzenia odbiorcze sygnałów uszkodzeniowych, przy czym obiekty wyposażone w stałe urządzenia gaśnicze i objęte całodobowym nadzorem co najmniej jednej osoby nie muszą być wyposażone w system sygnalizacji pożarowej.

Zatem widzimy, że pomimo tego, że Normy są stosowane we wdrożeniach wykonujących obowiązki ustawy o krajowym systemie cyberbezpieczeństwa, są one bazą tego, aby:

- podjąć działania dokumentacyjne – sporządzenie odpowiednich polityk, wyznaczających kompetencje, obowiązki, standardy;
- podjąć działania organizacyjne – wyznaczenie osób odpowiedzialnych;
- podjąć działania techniczne – wdrożenie zabezpieczeń fizycznych i cyfrowych.



Działania po incydencie – *case study* – opowieści z krypty

9. DZIAŁANIA PO INCYDENCIE – *CASE STUDY* – OPOWIEŚCI Z KRYPTY

„Bank okrada ludzi"

Zaczęło się niewinnie, od kolportażu buńczucznych ulotek z hasłem „Bank okrada ludzi". Okazało się, że robił to pracownik jednego z oddziałów banku. Dodatkowo okazało się, że ów pracownik pobierał rozmaite bazy danych klientów ze szczegółowymi informacjami dotyczącymi ich zdolności kredytowej, zaciągniętych zobowiązań, itp. a przy okazji poszczególne dane z bazy danych banku usunął. Po czym zaczął pisać do klientów banku.

W ten sposób naruszył szereg zaciągniętych przez siebie obowiązków. Dzięki prawidłowo sformułowanym i wdrożonym politykom bezpieczeństwa, zawartym zobowiązaniom do zachowania informacji w poufności, nieużywania określonych urządzeń, udało się postawić temu człowiekowi kilka zarzutów, m.in. z kodeksu karnego z rozdziału o przestępstwach przeciwko ochronie informacji (tam, niektóre znamiona przestępstwa wymagają przyjęcia zobowiązania przez sprawcę), przepisów karnych ustawy o ochronie danych osobowych oraz ustawy prawo bankowe.

Atak DDoS

Bliżej nieokreślone osoby (jak to zwykle bywa w tego rodzaju przypadkach), lub może jedna osoba korzystająca z przejętych innych komputerów przeprowadziła atak Rejected Amplifcation DDoS, na system rezerwacji biletów jednego z przewoźników lotniczych.

Atak DDoS (Distributed Denial of Service) to atak polegający na wyczerpaniu zasobów sieciowych lub obliczeniowych atakowanego serwisu tak, by uniemożliwić mu realizację normalnych czynności. W ten sposób przy pomocy niewielkiego nakładu środków (mały ruch z zapytaniami) można bardzo efektywnie (bo z pomocą wielu serwerów) wygenerować olbrzymi ruch. Ataki takie są jedną z najpowszechniejszych metod przeprowadzania DDoS.

Okazało się, że nie skonfigurowano poprawnie narzędzia raportowania. Nie wdrożono także monitorowania ruchu na styku z sieci. Zaś przy wdrożeniu zapory sieciowej, nie przeniesiono reguł filtrujących z poprzednio używanych urządzeń. To wszystko wbrew postanowieniom umowy z podwykonawcą. Na tej podstawie zawarto ugodę z wykonawcą IT.

Atak na kancelarii prawnej

W polskiej kancelarii wprowadzono outsourcing usług IT. Niestety, podobnie jak powyżej, jedno z urządzeń zapory było nieprawidłowo skonfigurowane, a mówiąc ściślej – pozostawiono ustawienia fabryczne (dostępne na stronie internetowej producenta). Haker dostał się do sieci i ściągnął kilkadziesiąt gigabajtów danych, maili z klientami, umów, pism. Następnie publicznie zaszantażował kancelarię, żeby zapłaciła za te dane – 10% przychodu rocznego firmy[7].

Kazus Morele

Efektem wycieku danych ze sklepu internetowego Morele była nałożona we wrześniu 2019 roku kara w wysokości prawie 3 mln zł[8].

Kazus phishing

W lutym 2018 roku ofiarą phishingu padła Polska Grupa Zbrojeniowa. Koszt? 4 mln zł[9].

Podsumowując

Z analiz wynika, że cyberprzestępcy oczekiwali zazwyczaj okupu na poziomie od 0,7 do 5% rocznych przychodów przedsiębiorstwa, zaś niektóre źródła podają, że średni koszt cyberincydentu w 2023 roku to 5 mln dolarów[10].

[7] https://www.rp.pl/zawody-prawnicze/art4337991-hakerzy-w-wielkiej-kancelarii-adwokackiej
[8] https://wyborcza.biz/biznes/7,177150,25210543,2-8-mln-zl-kary-dla-morele-net-za-atak-hakerski.html
[9] https://www.computerworld.pl/news/Atak-phishingowy-na-spolke-Polskiej-Grupy-Zbrojeniowej,412093.html
[10] https://itreseller.com.pl/szkody-wywolywane-przez-cyberataki-beda-stale-rosly-w-2025-roku-maja-siegac-10-bilionow-dolarow/

Zdaniem autorów, wniosek z niniejszego opracowania płynie taki, że warto zweryfikować cele i budżety na cyberbezpieczeństwo w znaczeniu technicznym, ale i prawnym.

Autorzy:
Jakub Kubalski
Marta Pasztaleniec
Kacper Krawczyński

II. CYBERBEZPIECZEŃSTWO MOJEJ FIRMY. SKORO I TAK BĘDZIE DROGO, CZY PRZYNAJMNIEJ WIEM, ZA CO PŁACĘ?

Wstęp

1. WSTĘP

Niezależnie od tego, czy czytają Państwo ten raport w Katowicach, Warszawie, Chełmnie czy Zielonej Górze, gdzieś w Polsce dochodzi w tym momencie do próby cyberataku. Cyberprzestępcy nie znają granic, nie mają wyrozumiałości i atakują bez żadnych skrupułów. Ataki ze strony internetowych przestępców dotykają największych i najmniejszych, duże koncerny międzynarodowe, ale i małe, lokalne biznesy. Dowodzą temu coroczne raporty, które pokazują wyraźną tendencję – cyberataków jest coraz więcej i dochodzi do nich coraz częściej. *(...) przestępcy wykorzystywali rozwój technologii cyfrowych do przeprowadzenia zaawansowanych kampanii phishingowych i infekowania szkodliwym oprogramowaniem, które, tak jak w przypadku działań z wcześniejszych lat, miały na celu wyłudzenie danych uwierzytelniających do bankowości elektronicznej, ale również do kont pocztowych i społecznościowych* – czytamy w Raporcie rocznym z działalności CERT Polska w 2022 roku[1]. Hakerzy wykorzystują przy tym ludzkie emocje, słabości i nawyki. Popularnym problemem jest posiadanie jednego hasła do różnych serwisów, dzięki czemu przestępcy uzyskują dostęp do kilku kont jednocześnie. Brzmi znajomo? Ten problem jest wciąż aktualny, a człowiek nadal pozostaje najsłabszym ogniwem, które udaje się przełamywać cyberprzestępcom.

Aż 59% polskich firm doświadczyło incydentu związanego z bezpieczeństwem IT w ciągu ostatnich 12 miesięcy – to alarmujące wyniki badania MŚP[2], które przeprowadził specjalizujący się w cyberbezpieczeństwie ESET. Dlaczego aż tyle? Nie odpowiemy na to pytanie w tym Raporcie. Ale zaprezentujemy katalog podpowiedzi na różnym poziomie zaawansowania, aby w miarę możliwości, każdy z czytających odnalazł coś interesującego dla siebie.

Jeśli chodzi o cyberbezpieczeństwo w Polsce, organizacje podobnej wielkości często bardzo różnią się poziomem myślenia o bezpieczeństwie i zaawansowaniem swoich zabezpieczeń. Dlatego w tym poradniku, zaczęliśmy od najczęstszych bolączek inwestycji w cyberbezpieczeństwo polskich firm, scenariuszy ataków i prostych, być może oczywistych porad praktycznych. Następnie pokazujemy jak podejść do badania naszych słabych stron i ustalania priorytetów zabezpieczeń. Na kolejnym poziomie – w skrócie pokazujemy, jak podejść do wdrożenia kompletnego systemu zarządzania bezpieczeństwem organizacji. Na koniec omawiamy najczęściej stosowane modele współpracy z zewnętrznymi partnerami – aż po zyskujący na popularności w ostatnich latach model, w którym organizacja zleca monitorowanie swojego bezpieczeństwa zewnętrznemu partnerowi (Security Operations Center).

[1] Raport roczny z działalności CERT Polska 2022
https://cert.pl/uploads/docs/Raport_CP_2022.pdf

[2] ESET SMB Digital Security Sentiment Report 2022
https://in.eset.pl/storage/www_nowyeset/doc/raporty/ESET_Digital_security_sentiment_report_2022.pdf

Typowe problemy i mity inwestycji w cyberbezpieczeństwo

2. TYPOWE PROBLEMY I MITY INWESTYCJI W CYBERBEZPIECZEŃSTWO

Niedocenianie wagi problemu – brak zabezpieczeń lub tylko najtańszy antywirus; „najwyżej od nowa zainstalujemy Windowsa"

Wiele, szczególnie mniejszych organizacji uznaje, że udział w „wyścigu zbrojeń" między światem cyberprzestępców a osobami odpowiedzialnymi za zabezpieczenia nie ma sensu, jedynie generuje koszty i nie warto brać w nim udziału. Z jednej strony jesteśmy bombardowani informacjami medialnymi o kolejnych atakach hakerskich. Z drugiej, koszty zatrudnienia ludzi odpowiedzialnych za cyberbezpieczeństwo i koszty ewentualnego zakupu dobrej jakości rozwiązań ochronnych są również niemałe. Są menedżerowie, którzy ten dylemat rozwiązują decydując się na radykalne oszczędności w zabezpieczeniach. Na pytanie czy coś chroni komputery ich pracowników, odpowiadają, że pozostali przy darmowych antywirusach lub najtańszych, które znaleźli na rynku. Często w takich organizacjach styk sieci firmowej i sieci internet jest chroniony przez stary firewall z oprogramowaniem nieaktualizowanym od lat.

Jeśli chodzi o świadomość zarządzających taką organizacją – mamy dwie typowe sytuacje. Czasem nie zwracają oni w ogóle uwagi na cyberbezpieczeństwo, prowadząc swój biznes od lat według utartych nawyków. Czasem wręcz niski stopień informatyzacji organizacji paradoksalnie sprawia, że stopień zagrożenia jest niższy – skoro wiele rzeczy załatwia się na papierze i offline, to również tematyka bezpieczeństwa informatycznego schodzi na dalszy plan.

Część organizacji z tej kategorii ma menedżerów, którzy są świadomi, że takie podejście radykalnie zwiększa ryzyko. Że nawet przypadkowy, masowy atak przez rozprzestrzeniające się w sieci ataki ransomware może zatrzymać działanie takiej organizacji. Zwolennicy opisywanego podejścia zakładają, że jeśli już dojdzie do takiego ataku, to po prostu przez kilka dni nie będą pracować, a systemy operacyjne na komputerach pracowników w przypadku zaszyfrowania, trzeba będzie zainstalować na nowo. Po kilku dniach przerwy, firma zacznie działać ponownie. Ale być może bez dostępu do kluczowych zasobów.

Tego typu podejście spotykane jest coraz rzadziej. Jednak szczególnie w segmencie małych firm, możemy nadal znaleźć jego przedstawicieli.

Kupowanie tylko ze względu na cenę rozwiązań słabej jakości, bez świadomości potrzeb

Jeśli menedżerowie dochodzą do wniosku, że warto się zabezpieczyć, nie mają często kompetencji wyboru rozwiązań, ani specjalistów wewnątrz organizacji. Dochodzi do sytuacji, w której organizacja "wybiera się na zakupy", nie mając jednak wiedzy, jakie zabezpieczenia powinno się w danej organizacji wdrożyć. W tej sytuacji są często organizacje naśladujące wybory innych lub też bezkrytycznie podążające za sugestiami sprzedawców rozwiązań. Organizacja, która nie ma wiedzy i świadomości własnych potrzeb w zakresie bezpieczeństwa informatycznego, jest podatna na różnego rodzaju chwyty marketingowe, kupując często to, co najszybciej zostanie zaproponowane przez kontaktujących się z organizacją sprzedawców.

Niestety trzeba przyznać, że branża cyberbezpieczeństwa nie ułatwia życia takim potencjalnym klientom. Mamy w niej do czynienia z dużym stopniem skomplikowania rozwiązań i szybkim rozwojem zabezpieczeń w czasie. Wiedza pozyskana przez organizację w ciągu kilku lat może w istotnej części ulec dezaktualizacji. To sprawia, że wiele informacji podawanych przez dostawców technologii jest trudnych do sprawdzenia bez wiedzy fachowej. Słowem – „kupujemy kota w worku" i nie mamy w organizacji kogoś, kto będzie w stanie oddzielić informacyjny szum od faktów oraz pomóc nam wybrać świadomie.

Tego typu klienci mogą być wrażliwi na oddziaływanie sprzedawców technologii cyberbezpieczeństwa, stosujących różnego rodzaju sztuczki i wątpliwe etycznie techniki. Zainteresowani spotkają się z teoretycznie bezstronnymi rankingami rozwiązań, które tworzone są przez organizacje powiązane z danym producentem. Mogą

zwrócić uwagę na mało istotne funkcjonalności rozwiązań, a pominąć w procesie wyboru parametry naprawdę kluczowe. Czy powinniśmy wybrać system antywirusowy o „najwyższej wykrywalności zagrożeń"? Dla laika odpowiedź wydaje się oczywista – tak. Jeśli jednak ten system generuje ogromne liczby fałszywych alarmów, blokując pracę na bezpiecznych plikach w firmie, już po miesiącu od zakupu zostanie wyłączony ze względu na skargi pracowników. To samo spotka system, który wprawdzie na papierze świetnie wypadł w testach wykrywalności, ale potrzebuje do swojego działania tyle zasobów, że znacznie spowalnia pracę komputerów, które chroni i uniemożliwia pracownikom realizowanie ich obowiązków.

Dla tej grupy organizacji konfrontacja z podjętymi wyborami, jeśli chodzi o rozwiązania również bywa bolesna. Jeden problem, to sytuacja, w której na skutek chaotycznie wybieranych zabezpieczeń, mimo ich wprowadzenia, organizacja stanie się celem skutecznego ataku. Drugi rodzaj bolesnej konfrontacji, to sytuacja, w której firma jest zmuszona do szybkiego poszukiwania alternatywnej technologii lub dostawcy, bo pierwszy wybór został podjęty w oparciu o złe kryteria i dopiero po wdrożeniu, doszło do „zderzenia" z rzeczywistością.

Utrzymywanie systemów bez ludzi potrafiących nimi zarządzać – „wydaliśmy majątek, a więc jesteśmy bezpieczni"

Osiągnięcie przez organizację wysokiego poziomu bezpieczeństwa informatycznego, to efekt złożonych działań – na poziomie stworzenia odpowiedniej kultury bezpieczeństwa, wdrożenia norm i polityk, nawyków ludzkich, aż po wybór, wdrożenie i utrzymanie odpowiednich rozwiązań technicznych. W warunkach szybko zmieniających się wyzwań, odpowiedni balans między tymi składnikami jest bardzo istotny dla osiągnięcia celu finalnego, czyli możliwie jak najbardziej bezpiecznej organizacji.

Zwykle nie da się osiągnąć wysokiego poziomu bezpieczeństwa dbając jedynie o normy i kulturę, bez zastosowania rozwiązań technicznych. Jednak również odwrotna sytuacja nie jest optymalna. Jeśli organizacja decyduje się przeznaczyć większe zasoby finansowe na swoje bezpieczeństwo informatyczne, należy zachować odpowiednie proporcje.

W sytuacji, w której w firmie wewnętrznie brakuje kompetencji, a pojawiają się środki na zakup zaawansowanych rozwiązań ochronnych, możemy mieć do czynienia z sytuacją, w której organizacja dysponuje bardzo zaawansowanymi systemami, o ogromnych możliwościach, jednak nie potrafi z tych systemów efektywnie korzystać. Dlatego bardzo ważne jest, aby decydując się na zaawansowane systemy bezpieczeństwa, zweryfikować, czy mamy odpowiednie zasoby ludzkie i czy nasz personel ma odpowiednie kompetencje.

W praktyce przekłada się to na przeprowadzeniu szkoleń dla zespołu administratorów tych systemów, a być może zatrudnieniu dodatkowych specjalistów cybersecurity. Alternatywne rozwiązanie, to wybór zewnętrznego partnera, który tego typu zadania może dla nas realizować – zarządzać zakupionymi przez nas rozwiązaniami ochronnymi.

Brak kontroli nad lukami w funkcjonujących systemach, nieaktualne wersje zabezpieczeń – „nie mam czasu się tym zajmować"

Wyścig pomiędzy atakującymi, a obrońcami firmowych sieci zmienił się istotnie w 2001 roku, kiedy pierwszy raz na masową skalę wykorzystano lukę w oprogramowaniu serwerowym Microsoft. Korzystający z tej luki robak internetowy, nazwany potem "Code Red" zaatakował skutecznie tysiące firm i organizacji. Ogromne pod względem skali ataki wykorzystujące luki w oprogramowaniu w kolejnych latach (aż po słynny atak WannaCry w 2017 roku), doprowadziły do sytuacji, w której możemy uznać, że obecnie nie ma czegoś takiego jak gotowe i skończone oprogramowanie. Mamy również do czynienia z niecodziennym wyścigiem. Atakujący starają się znaleźć błędy i luki w działającym oprogramowaniu, które można następnie wykorzystać w przełamywaniu firmowych zabezpieczeń. Z kolei dostawcy oprogramowania regularnie dodają nowe funkcjonalności, popełniając przy tym nowe błędy. Mimo, że starają się aktualizować swoje oprogramowanie również w zakresie bezpieczeństwa, to po latach osiągnęliśmy stan, w którym trudno uznać, że dane oprogramowanie zostało dostarczone w skończonej, finalnej formie.

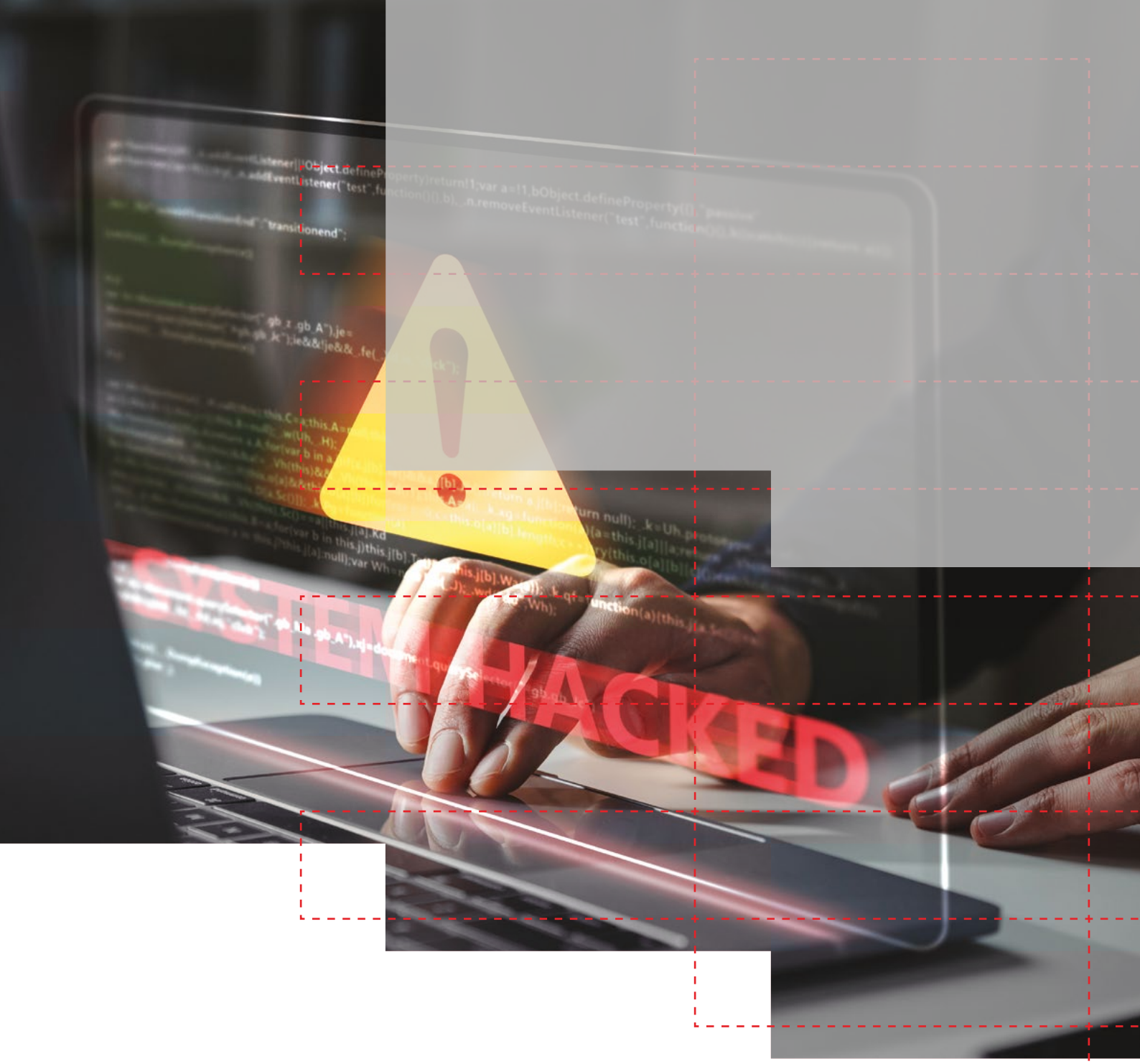
Według zajmującej się wykrywaniem luk szwedzkiej firmy Holm Security każdego miesiąca identyfikowanych jest ok. 300 nowych podatności, przy czym należy pamiętać, że nawet jedna „dziura" w oprogramowaniu może spowodować gigantyczne problemy w ciągłości pracy organizacji.

Ta sytuacja sprawiła, że aktualizowanie używanego w firmach oprogramowania, stało się niezbędne dla zapewnienia należytego bezpieczeństwa organizacji. Nie jest to już tylko decyzja uzależniona od tego, czy organizacja potrzebuje jakiejś nowej funkcjonalności, ale konieczność dla zapewnienia bezpieczeństwa. Proces tworzenia oprogramowania stał się na tyle skomplikowany, że stworzenie aplikacji aktualnej, zupełnie pozbawionej błędów i podatności, uznaje się za praktycznie niemożliwe.

„Co właściwie mamy chronić?" – brak określenia tego co najcenniejsze. Jeśli zostaniemy zaatakowani, co jest dla nas najważniejsze dla zachowania ciągłości działania?

Bardzo wiele średnich i dużych organizacji w Polsce potrafi już wybrać najpopularniejsze techniczne zabezpieczenia w kategoriach uznawanych za standardowe w branży. Organizacje mają już podstawowe środki techniczne – tzn. dbają o ochronę antywirusową komputerów pracowników, dostęp do firmy jest chroniony przez firewall, dostępy pracowników z zewnątrz są szyfrowane za pomocą tuneli VPN, organizacja wdraża podwójne uwierzytelnianie dla pracowników itd. Często administratorzy odpowiadający za techniczną warstwę zabezpieczeń są przekonani, że osiągnięto całkiem niezły poziom bezpieczeństwa. Niestety to nie wystarcza. Nawet jeśli podejmiemy dobre decyzje, jeśli chodzi o wybór i wdrożenie rozwiązań ochronnych, a zabraknie szerszej analizy ryzyk związanych z włamaniem i wyciągnięcia wniosków z tej analizy, to nie można uznać, że organizacja dojrzale myśli o swoim bezpieczeństwie informatycznym.

Kluczowe jest rozpoczęcie od analizy ryzyka. Jeśli założymy, że cyberprzestępcy włamali się do naszej organizacji i nasze systemy przestały działać, a dane wyciekły – co taki fakt oznacza dla nas? Które z systemów są niezbędne dla działania naszej organizacji? Czy i jak długo firma może działać bez sprawnej poczty elektronicznej? Jak długo możemy pracować bez sprawnego systemu do zarządzania relacjami z klientami (CRM)? Jeśli przestępcy zyskają dostęp do baz danych naszego sklepu internetowego, to jakie informacje tam znajdą? Czy jako firma potrafimy realizować zamówienia od naszych kontrahentów bez sprawnego portalu internetowego? Jak długo? Żeby organizacja potrafiła sobie odpowiedzieć na te pytania, często trzeba zacząć od ustrukturyzowania procesów i zależności działających w średniej firmie. Bardzo często, procesy te nie istnieją w spisanej formie lub nie są zrozumiałe dla osób odpowiedzialnych za cyberbezpieczeństwo organizacji. Żeby przeprowadzić należytą analizę ryzyka, potrzebna jest więc interakcja zespołów odpowiedzialnych za cyberbezpieczeństwo z zespołami odpowiedzialnymi za procesy biznesowe i z osobami decyzyjnymi w organizacji. Dopiero po pełnej analizie ryzyka, zespół osób odpowiedzialnych za wdrażanie rozwiązań ochronnych ma pełną wiedzę, gdzie organizacja przechowuje swoje "srebra rodowe", a więc najcenniejsze zasoby oraz które procesy są kluczowe dla przetrwania organizacji. Po takiej analizie może okazać się, że nie wystarczy wdrożenie zabezpieczeń, ale być może potrzebne jest przeprojektowanie pewnych procesów biznesowych, aby zmniejszyć ryzyko dla organizacji, w wypadku skutecznego włamania.



Najczęstsze scenariusze cyberataków i możliwe sposoby zapobiegania

3. NAJCZĘSTSZE SCENARIUSZE CYBERATAKÓW I MOŻLIWE SPOSOBY ZAPOBIEGANIA

Jeśli chcemy podjąć dobre decyzje na temat wyboru zabezpieczeń dla swojej organizacji, warto poznać najczęstsze scenariusze ataków i techniki stosowane przez przeciwnika. Musimy jednak brać pod uwagę, że współcześnie przeprowadzane ataki to najczęściej kombinacja wielu technik. Aby przełamać zabezpieczenia hakerzy planują atak wieloetapowo, używając różnych narzędzi, w różnych fazach swojej „akcji". Problematyczna staje się więc prosta, logiczna kategoryzacja zagrożeń, gdyż najczęściej, kiedy atak się powiedzie, okazuje się, że przestępcy korzystali z całego wachlarza dostępnych technik. Najczęściej jest to jakiś rodzaj ataku phishingowego, powiązany ze znajomością socjotechniki. To sytuacja, w której do ataku wykorzystuje się wiedzę o organizacji, aby przygotować na tyle wiarygodny e-mail, aby pracownik mógł uznać go za prawdziwy i otworzyć jego załącznik lub kliknąć w przesłany link. Pierwszym etapem może więc być phishing.

Kiedy pracownik klika w link lub otwiera załącznik, najczęściej do akcji wkracza złośliwe oprogramowanie (wirus, malware), które wykonuje przygotowane przez atakujących instrukcje na komputerze pierwszej „ofiary" wewnątrz organizacji. Jeśli organizacja ma niezałatane luki w swoich aplikacjach, taka operacja staje się łatwiejsza. Złośliwe oprogramowanie może rozprzestrzenić się wewnątrz organizacji na kolejne komputery i serwery. Często atak to misterny, wieloetapowy plan, w którym obecność złośliwego oprogramowania wewnątrz organizacji pozostaje przez nią niewykryta przez wiele tygodni. To powoduje problemy w badaniu, w jaki sposób do ataku doszło, gdyż analiza ruchu z ostatnich dni, może nic nie pokazać.

Ataki według podobnych scenariuszy mogą dotyczyć podmiotów niezależnie od ich wielkości. Jednak bardzo często małe i średnie firmy są znacznie gorzej zabezpieczone. Potwierdzają to raporty. Według badania przeprowadzonego przez ESET, jednego z największych dostawców rozwiązań ochronnych, aż 74% małych i średnich przedsiębiorstw uważa, że są bardziej podatne na cyberataki niż duże firmy. Biznes najczęściej obawia się ataków wirusów i złośliwego oprogramowania. Najczęstszym kierunkiem, z jakiego do takich ataków dochodzi jest sieć WWW – ataki w jakimś momencie wiążą się z wizytą na specjalnie spreparowanej stronie internetowej[3].

opinia MŚP o cyberbezpieczeństwie

Firmy są świadome wielu rodzajów ryzyka i zagrożeń na polu cyberbezpieczeństwa, lecz nie wierzą, że są w stanie poradzić sobie ze wszystkimi. Największe obawy budzi kwestia narażenia pracowników na ataki malware, zwłaszcza poprzez sieć web; na drugim miejscu są ataki ransomware i braki w zabezpieczeniach u osób trzecich.

Największe obawy wobec cyberbezpieczeństwa na kolejny rok

[3] ESET SMB Digital Security Sentiment Report 2022
https://in.eset.pl/storage/www_nowyeset/doc/raporty/ESET_Digital_security_sentiment_report_2022.pdf

Złośliwe oprogramowanie – przez sieć lub e-mail (phishing)

Najczęstszym obecnie kierunkiem, z którego rozpoczyna się atak na organizację jest uruchomienie złośliwego kodu, wykorzystującego lukę w oprogramowaniu organizacji. Złośliwe oprogramowanie jest zwykle dostarczane w formie linku w odpowiednio spreparowanej wiadomości e-mail, wyglądającej na zaufaną i pochodzącą od wiarygodnego nadawcy (phishing). Druga, często występująca sytuacja, to sprowokowanie pracownika do wizyty na zawierającej złośliwe oprogramowanie stronie internetowej bez użycia e-maila. Link do niebezpiecznej lokalizacji może być rozprzestrzeniany na wiele innych sposobów.

Oprócz wdrażania zabezpieczeń, które pozwolą odpowiednio monitorować i filtrować przychodzące wiadomości e-mail czy odwiedzane przez pracowników strony internetowe, kluczowa staje się edukacja zespołu. Poziom bezpieczeństwa w organizacji można wydatnie podnieść, regularnie szkoląc pracowników na temat tego czym jest phishing, jak zauważyć potencjalny atak i jak zareagować na podejrzaną wiadomość.

Ransomware

Oprogramowanie wymuszające okup (ang. ransom) to szczególny rodzaj złośliwego oprogramowania, który wyjątkowo mocno daje się we znaki osobom odpowiedzialnym za cyberbezpieczeństwo. Przestępcy starają się umieścić złośliwe oprogramowanie wewnątrz organizacji i to najlepiej w systemach przechowujących kluczowe dla organizacji dane. Następnie ransomware uruchamia się i zaczyna swoją pracę, szyfrując wszystko do czego ma dostęp wewnątrz organizacji. Jeśli dane zostaną skutecznie zaszyfrowane, to w ciągu kilku minut, organizacja może zostać zupełnie odcięta od dostępu do swoich niezbędnych do działania systemów. Zwykle atak tego typu skutkuje zatrzymaniem działania systemów. Organizacja staje przed wyborem: zapłacić okup, aby uzyskać klucze pozwalające na odszyfrowanie danych lub też mozolnie odtwarzać wszystkie systemy ze swoich kopii bezpieczeństwa. Pamiętajmy, że opcja zapłaty okupu to jak negocjacje z terrorystami, a płacąc, nie wiemy, czy osiągniemy pożądany efekt. Z kolei na rozsądniejszą opcję drugą, czyli odtwarzanie systemów z kopii bezpieczeństwa mogą pozwolić sobie tylko przezorne organizacje, które mają wdrożoną należytą politykę tworzenia takich kopii. Jeśli organizacja to zaniedbała, zaliczamy „twarde lądowanie", które może zakończyć się poważnymi stratami finansowymi (długi przestój organizacji), a nawet upadłością firmy na skutek ataku ransomware, kiedy straty i czas na przywrócenie działalności jest na tyle długi, że eliminuje firmę z rynku.

Głośny przykład na Śląsku

Znanym przykładem takiego działania cyberprzestępców jest przeprowadzony w lutym 2023 roku atak na infrastrukturę Śląskiej Karty Usług Publicznych. Na skutek ataku ransomware pasażerowie miejskiego transportu na terenie aglomeracji śląskiej napotkali na szereg utrudnień. Stracili dostęp do aplikacji pozwalającej płacić za przejazdy komunikacją miejską, a na przystankach przestały działać tablice informacyjne pokazujące godziny odjazdów. Co gorsza, nie działały również czytniki kart w autobusach, co spowodowało spore problemy z kasowaniem biletów. Władze samorządowe odebrały szereg skarg od mieszkańców, którzy nie mogli dojechać na czas z powodu braku informacji czy problemów z zakupem biletów. Przywracanie kluczowych dla pasażerów funkcjonalności systemu trwało ponad tydzień. Cyberatak na Śląską Kartę Usług Publicznych jest przykładem, w którym problemy z bezpieczeństwem infrastruktury informatycznej mają namacalny wpływ na codzienne życie mieszkańców.

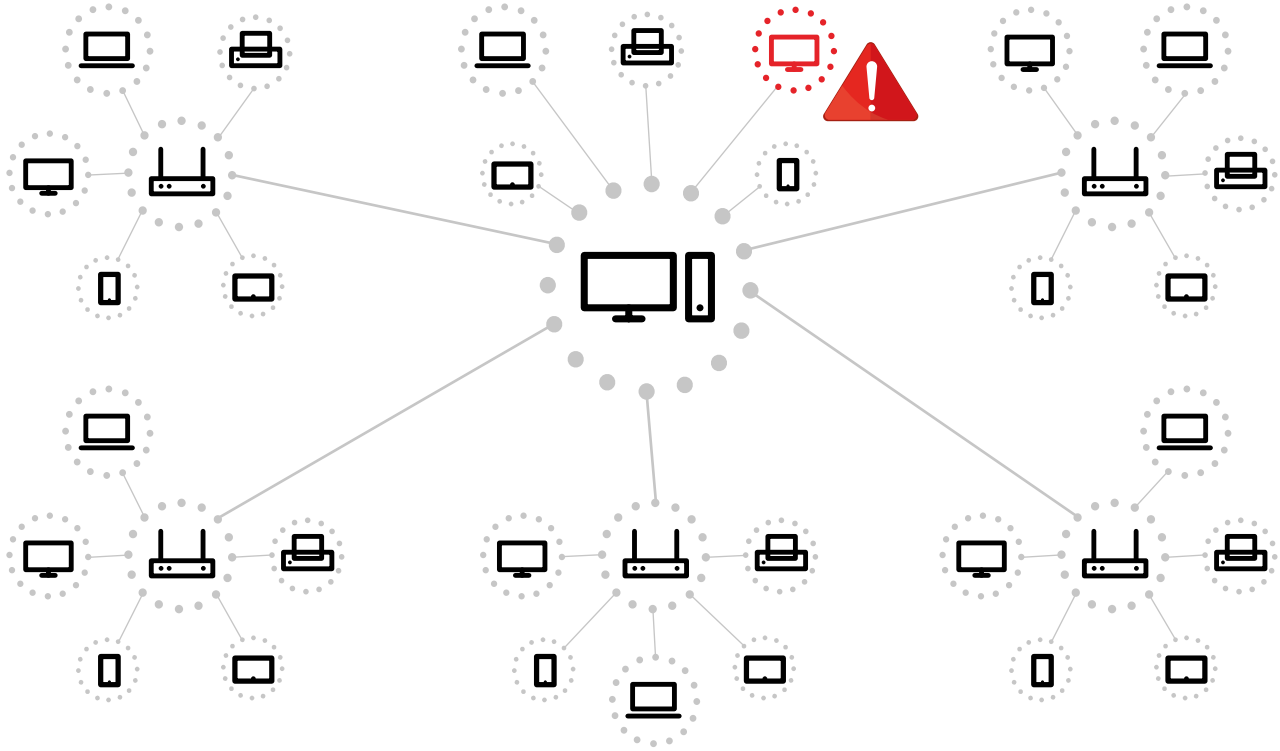
Błędy w zabezpieczeniach kontrahentów (ataki na łańcuch dostaw)

Biznes tworzą ludzie. Ale współczesna i efektywna firma, to nie forteca otoczona wysokim murem, ale często fizycznie rozproszone zespoły osób realizujące wspólne cele, z pomocą wielu zewnętrznych systemów i partnerów technologicznych. Bez płynnej współpracy systemów IT, nigdy nie osiągnęlibyśmy wystarczającej efektywności. Wspieramy więc nasze procesy różnego rodzaju specjalistycznymi systemami, bardzo często do-

starczanymi bardzo często od zewnętrznych kontrahentów dostarczających np. systemy księgowe, kadrowe, systemy CRM, logistyczne, marketing automation czy business intelligence. Biznes żąda efektywności. Chce więc maksymalnie zintegrować dostawców z organizacją, aby uprościć codzienność jej pracowników. Lepiej zintegrowani, działamy szybciej i zyskujemy przewagę konkurencyjną. W ten sposób jednak rosną wyzwania w aspekcie cyberbezpieczeństwa. Jeśli cyberprzestępcy skutecznie zaatakują naszego zaufanego kontrahenta i dostaną się do jego wewnętrznych zasobów, mogą następnie wykorzystać jego systemy, aby dostać się do naszej organizacji. Co gorsza, nasze zabezpieczenia długo mogą okazywać się bezbronne; przecież w naszym systemie pracuje zaufany dostawca, więc wydaje się, że nie ma problemu. W ten sposób organizacja może stać się ofiarą wyrafinowanego, długo niewykrywanego ataku. Jeśli przestępcom udało się w ten sposób wniknąć do naszej organizacji, grozi nam np. wyciek danych, którego długo możemy nie być świadomi. Atak może być celowany w naszego kontrahenta. Jednak drugą możliwością jest zaatakowanie dostawcy oprogramowania, z którego rozwiązań korzysta nasza organizacja. Wtedy pobierając jego aktualizację, sami nieświadomie tworzymy lukę w zabezpieczeniach.

Wstrząsająca infiltracja...

Spektakularnym przykładem tego typu działania, które wstrząsnęło branżą, był cyberatak na firmę SolarWinds. W zasadzie głównym celem ataku byli klienci tej firmy. SolarWinds to ogromny dostawca rozwiązań służących do monitorowania infrastruktury informatycznej i zarządzania nią. Skoro rozwiązanie monitoruje systemy i jest wdrożone w organizacji, ma szeroki dostęp do jej zasobów. Atakujący wprowadzili złośliwe oprogramowanie do aplikacji autorstwa SolarWinds. Następnie oprogramowanie SolarWinds, będące swego rodzaju „nosicielem ataku", aktualizując się u swoich klientów rozprzestrzeniło atak na ponad 18 tys. (!) organizacji. Wśród zaatakowanych było kilka agencji federalnych USA, amerykańska administracja zarządzająca bezpieczeństwem nuklearnym, prywatne firmy takie jak Microsoft, Intel czy nawet specjalizujące się w zabezpieczeniach FireEye. Co gorsza, atak pozostawał niewykryty przez kilka miesięcy i wiązał się z trudnym do określenia wyciekiem danych. Kto stał za tym cyberprzestępczym majstersztykiem? Amerykańskie agendy rządowe wskazują na działania rosyjskiego wywiadu. Jak łatwo się domyślić Rosja zaprzeczyła zarzutom, a szczegółowe dowody pozostają w rękach wywiadów państw i globalnych firm specjalizujących się w cyberbezpieczeństwie.



Ataki przeciążające systemy (DDoS)

Mechanizm takiego ataku polega na wygenerowaniu bardzo dużej liczby sztucznych zapytań do systemu czy strony internetowej organizacji. Skala zapytań przekracza możliwości odpowiedzi i wskutek takiego działania systemy ofiary stają się niedostępne dla ich normalnych użytkowników.
Atak tego typu bywa spektakularny i szybko staje się obiektem zainteresowania mediów. Bardzo łatwo bowiem spróbować załadować daną stronę internetową i potwierdzić jej niedostępność. Powoduje więc czasowy przestój, pytania zaniepokojonych klientów, ale zwykle nie wiąże się z uzyskaniem dostępu do wewnętrznych zasobów organizacji.

Estonia – przykład ataku na firmy i instytucje
Jednym z najbardziej znanych cyberataków tego typu był przeprowadzony w 2007 roku atak na instytucje w Estonii. Zmasowane działania rozpoczęły się natychmiast po ostrym sporze politycznym wokół usunięcia rosyjskiego pomnika z centrum Tallina. Zaatakowane i niedostępne w związku z tym stały się serwisy internetowe parlamentu Estonii, banków, ministerstw i mediów. Ataki były ponawiane przez kilkadziesiąt dni. Bezpośrednią reakcją na tego typu działania cyberprzestępców było utworzenie w Tallinie Centrum Doskonalenia Cyberobrony NATO, a techniki używane wobec Estonii były szeroko dyskutowane przez kilka kolejnych lat.

Wycieki danych – na skutek ataku lub „insider threat”

W dzisiejszych czasach, gdy większość firm działa w oparciu o różnorodne systemy informatyczne oraz korzysta z usług zewnętrznych partnerów, zagrożenia związane z wyciekiem danych z organizacji stają się coraz bardziej realne i powszechne.

Niebezpieczeństwo może płynąć zarówno od wewnątrz, jak i z zewnątrz firmy. W przypadku wycieków spowodowanych od zewnątrz, mamy do czynienia z rosnącą liczbą ataków hakerskich, wyrafinowanych kampanii phishingowych, a także, coraz popularniejsze w Polsce szpiegostwo przemysłowe.

Z informacji Safetica wynika, że aż 80% firm traci dane w wyniku błędów pracowników lub ich świadomego działania[4].

Mogą to być pracownicy niefrasobliwi, czyli tacy którzy przypadkiem doprowadzają do wycieku danych lub pracownicy celowo działający na szkodę firmy. Mamy wtedy np. do czynienia z „insider threat” – zagrożeniem, które polega na wykorzystaniu wewnętrznej pozycji w organizacji do celów szkodliwych, takich jak kradzież poufnych informacji lub przekazywanie ich osobom trzecim. W takim przypadku ryzyko związane z wyciekiem danych jest szczególnie duże, ponieważ osoba, która dopuszcza się takiego przestępstwa, ma bezpośredni dostęp do wrażliwych danych.

Świetnym przykładem jest historia prezes jednej z największych firm spedycyjnych w Gdańsku. W pewnym momencie firma zaczęła rejestrować coraz to większe straty. Okazało się, że 4 pracowników, którzy odeszli z firmy jakiś czas wcześniej, wykradło i przywłaszczyło sobie ponad półtora terabajta danych swojego byłego pracodawcy. Dzięki temu, stworzyli konkurencję dla poprzedniej firmy spedycyjnej i zaczęli przejmować kontrahentów oraz proponować im niższe ceny. W rezultacie firma spedycyjna w pewnym momencie liczyła straty w milionach.

Takie incydenty są niezwykle kosztowne dla firmy. Według raportu „Cost of Data Breach Report 2022” opublikowanego przez technologicznego giganta IBM, średni koszt naruszenia danych wynosił w 2022 roku rekordowe 4,35 miliona dolarów. Ponadto, raport wykazał, że średni czas wykrycia i zażegnania wycieku danych wyniósł aż około 6 miesięcy[5].

[4] https://www.verizon.com/business/resources/reports/dbir/
[5] https://www.ibm.com/downloads/cas/3R8N1DZJ

Garść porad praktycznych na początek

4. GARŚĆ PORAD PRAKTYCZNYCH NA POCZĄTEK

Skuteczne zapewnienie bezpieczeństwa informatycznego to rozległy temat. Zacznijmy jednak od najprostszych, fundamentalnych rekomendacji, aktualnych w zasadzie dla każdej organizacji.

Zadbaj o skuteczną ochronę antywirusową

Dobrej jakości system ochrony antywirusowej działający na komputerach pracowników i serwerach to współcześnie podstawa i niezbędny element zabezpieczeń technicznych w każdej organizacji. Przy wyborze takiego rozwiązania kieruj się zdefiniowanymi wewnętrznie w organizacji kryteriami – trzeba określić, jakie systemy operacyjne należy chronić, jak zapewnić bezpieczeństwo urządzeń mobilnych, jak organizacja chce zarządzać taką ochroną, ale również jakie technologie detekcji są stosowane. Pod potocznym pojęciem „antywirus" kryją się również bardzo zaawansowane systemy łączące wiele technologii. Rywalizacja dostawców oraz tworzone na potrzeby pokazania sztucznych przewag typologie rozwiązań sprawiają, że określenie jakimi kryteriami należy się kierować wybierając tego typu technologię, przekracza ramy niniejszego opracowania.

Aby łatwo zmieniać ustawienia ochrony antywirusowej najprościej wybierać rozwiązania, które zapewniają centralną konfigurację ochrony antywirusowej za pomocą portalu producenta, dostępnego w chmurze. Nie ma wtedy konieczności instalowania serwerów do centralnego zarządzania wewnątrz organizacji, łatwiej również zapewnić aktualną ochronę antywirusową pracownikom zdalnym.

Należy pamiętać, że oprogramowanie antywirusowe mocno ingeruje w system operacyjny, a wysyłając próbki podejrzanych plików do analizy, może mieć dostęp do poufnych danych przetwarzanych na naszych komputerach. Dlatego szczególnie ważna jest dobra reputacja i zaufanie do dostawcy tego typu oprogramowania. Oprócz jakości rozwiązania dowiedzionej w niezależnych testach, należy brać również pod uwagę geopolityczne pochodzenie dostawców. Przykładem radykalnej zmiany był 2022 rok, w którym wiele firm i organizacji zmieniało stosowane u siebie zabezpieczenia, ponieważ po wybuchu wojny w Ukrainie używanie rozwiązań pochodzenia rosyjskiego zostało uznane za ryzykowne.

Firmy chcące zapewnić sobie wyższy poziom bezpieczeństwa powinny rozważyć system klasy „Endpoint Detection & Response". Tego rodzaju rozwiązanie zapewnia szerokie informacje o wszystkich plikach i procesach uruchamianych na komputerach pracowników, pozwala śledzić zależności między nimi, nawet po kilku miesiącach. W rękach zaawansowanego zespołu administratorów lub zewnętrznego partnera (np. świadczącego dla nas usługę Security Operations Center) to narzędzie o ogromnych możliwościach. Możemy z niego skorzystać zarządzając takim rozwiązaniem również wewnątrz organizacji, jednak decyzja o jego zakupie powinna być połączona z gruntownym szkoleniem pracowników.

Odizoluj sieć wewnętrzną za pomocą firewalla i zapewnij zdalny dostęp pracownikom

Współcześnie, w warunkach coraz częściej stosowanych aplikacji działających w chmurze, kwestia rozdzielenia zasobów w wewnętrznej sieci firmowej oraz zasobów poza nią, staje się coraz bardziej problematyczna. Podstawą jest dobrej klasy firewall, którym jest zazwyczaj tzw. system Unified Threat Management. Oznacza to wielofunkcyjne rozwiązanie, które oprócz klasycznych funkcji firewalla może również wykrywać włamania, zapewnić segmentację sieci, filtrować odwiedzane przez pracowników strony internetowe, zapewniać priorytetyzację ruchu sieciowego oraz bezpieczny, szyfrowany dostęp do zasobów firmy pracownikom zdalnym.

Oprócz wyboru dobrej klasy technologii, kluczowa jest zaawansowana konfiguracja takiego rozwiązania. Niestety bardzo często klienci kupują zaawansowany firewall, ale zespół informatyków obsługujących sprzęt nie posiada wystarczającej wiedzy, aby je należycie skonfigurować. Następnie przez kilka lat firewall pracuje na ustawieniach "domyślnych", realizując minimum funkcji bezpieczeństwa, ponieważ aby uruchomić te bardziej zawansowane, należało posiadać odpowiednią wiedzę i znać kontekst działania organizacji, a na to już nigdy

nie wystarczyło czasu. Ważne jest również zapewnienie regularnej analizy incydentów oraz aktualizowanie oprogramowania tego rozwiązania.

Dbaj o aktualność oprogramowania

Instalowanie bieżących aktualizacji jest współcześnie niezbędnym składnikiem każdej strategii cyberbezpieczeństwa. Wspominaliśmy wcześniej, że co roku odkrywane są tysiące nowych podatności, które wymagają od organizacji podjęcia kroków w celu ich wykrycia i usunięcia. Dbanie o aktualność oprogramowania staje się współcześnie na tyle skomplikowanym wyzwaniem, że tworzone są specjalne rozwiązania służące do wyszukiwania luk kryjących się w nieaktualnych wersjach aplikacji i wspierające administratorów w łataniu tych luk. Ta kategoria narzędzi nazywana jest rozwiązaniami klasy Vulnerability Management.

Brak wiedzy jakie są potencjalne zagrożenia dla naszych systemów i sprzętu wcale nie oznacza, że one nie występują. W rezultacie takiego podejścia może pojawić się mylne wrażenie, że "wszystko jest ok". Jednak kwestią czasu będzie to, kiedy ktoś potrafiący posługiwać się odpowiednimi narzędziami, uzyska nieautoryzowany dostęp do naszych zasobów.

Rozwiązania klasy Vulnerability Management pozwalają na cykliczne sprawdzanie naszych aplikacji i systemów pod kątem luk i nieaktualnych wersji. Szybkie identyfikowanie i naprawianie podatności w zabezpieczeniach oznacza, że potencjalni atakujący mają mniej czasu na ich wykrycie i wykorzystanie.

Dlaczego to takie ważne? Możemy wdrażać różne systemy do obrony, lecz bez narzędzia monitorowania i ocenienia sytuacji możemy mieć złudne wyobrażenie. Zdrowe jedzenie i bieganie daje nam poczucie, że będziemy żyć 100 lat. Lecz dopiero pójście na badania kontrolne, pokaże nam prawdziwy obraz sytuacji i wskaże obszary do poprawy np. wysoki cukier. Bez tego, pomimo zdrowego trybu życia, nie unikniemy problemu. Podobnie jest z cyberbezpieczeństwem.

Wprowadź środki ochrony danych

Wyciek z organizacji jej poufnych danych, może w pewnych przypadkach zakończyć się nawet zamknięciem działalności. Dlatego warto rozważyć dwa podstawowe aspekty.

Pierwsze to szyfrowanie danych. Problematyczne w organizacji jest zwykle należyte sklasyfikowanie zasobów pod kątem tego, które są szczególnie cenne. Dlatego najprościej jako standard uznać szyfrowanie wszystkich nośników – szczególnie dane na komputerach pracowników w wypadku np. zagubienia lub kradzieży laptopa są narażone na wyciek. Jeśli mamy zdefiniowane, gdzie dane są przechowywane i mamy je zabezpieczone przez szyfrowanie, spełniony mamy pierwszy warunek – zabezpieczenia danych w spoczynku (at rest). Pozostaje do rozstrzygnięcia drugie wyzwanie, czyli jak zabezpieczyć zasoby w trakcie przesyłania (in transit). Można to osiągnąć przez dodatkowe rozwiązania do szyfrowania przesyłanej poczty elektronicznej lub zastosowanie innych, bezpiecznych sposobów ich wymiany.

Zastosuj oprogramowanie klasy Data Leak Prevention wobec pracowników przetwarzających newralgiczne dane. Aplikacja działa w tle na komputerach pracowników i monitoruje ich aktywność wobec przetwarzanych danych. Jeśli pracownik, na skutek roztargnienia lub złej woli podejmie próbę wysłania poufnych danych poza organizację, rozwiązanie DLP (w zależności od konfiguracji) od razu taką próbę zablokuje i zaalarmuje administratorów albo zarejestruje w logach taką aktywność. Wybierając rozwiązanie klasy DLP należy zwrócić uwagę na łatwość jego wdrożenia w organizacji. Zwykle firmy mają duży kłopot z określeniem, które dane są newralgiczne i jak tak naprawdę są przetwarzane wewnątrz organizacji. Problem ten rozwiązuje wdrożenie całego systemu zarządzania bezpieczeństwem informacji (SZBI), o którym piszemy na kolejnych stronach. Ale nawet jeśli organizacja takiego systemu jeszcze nie stosuje, są dostępne na rynku łatwe we wdrożeniu rozwiązania DLP, które można najpierw uruchomić w trybie monitorowania i audytu, aby uzyskać pełną wiedzę jakie dane przesyłają poszczególni pracownicy. Po wykonaniu takiego wstępnego audytu, można następnie wdrożyć pewne zasady i ograniczenia, aby zapewnić należyty poziom bezpieczeństwa zasobów, bez blokowania i utrudniania zachowań pożądanych.

Zaplanuj politykę tworzenia kopii zapasowych

Wybierz rozwiązanie tworzące regularnie kopie zapasowe (backup) oraz zdecyduj, które dane są najcenniejsze z punktu widzenia biznesowego oraz zachowania ciągłości działania. Do tego znów potrzebujemy analizy ryzyka, ale też zrozumienia procesów biznesowych w twojej organizacji. Rozumienie procesów biznesowych jest kluczowe, aby odpowiedzieć sobie na pytania: jak często powinna być tworzona kopia zapasowa i jak długo należy ją przechowywać? Pamiętajmy, że w wypadku utraty danych (atak, pożar, awaria) dane, które zostaną odzyskane z kopii zapasowej, będą aktualne na moment jej wykonywania, a wszystko to, co wydarzyło się później, zostanie utracone. Być może część operacji trzeba będzie powtórzyć. Dopiero rozumiejąc procesy biznesowe, zespół odpowiedzialny za tworzenie kopii bezpieczeństwa może odpowiednio dobrać częstotliwość ich zapisu.

Dobrą praktyką jest też regularne testowanie procesu odzyskiwania danych z backupu, aby być pewnym, że proces odzyskiwania działa prawidłowo i kopie można odtworzyć w dowolnym momencie.

Ponadto należy rozważyć opcję przechowywania kopii danych w chmurze internetowej lub innej lokalizacji geograficznej na wypadek fizycznego zniszczenia lokalizacji, w której dane są zwykle przetwarzane. Dostawcy takich rozwiązań zapewniają obecnie możliwość tworzenia kilku kopii w różnych lokalizacjach fizycznych i chmurowych oraz automatycznej synchronizacji tych kopii. Ponadto, w wypadku fizycznego zniszczenia serwerów, na których były one zwykle przetwarzane, istnieje możliwość ponownego uruchomienia kopii tych systemów na innych urządzeniach (tzw. bare metal restore). Oczywiście tak zaawansowane możliwości to dodatkowe koszty. Należy więc kierować się wcześniej wykonaną analizą ryzyka.

Przeanalizuj bezpieczeństwo używanych aplikacji chmurowych i świadomie zdecyduj, które dane możesz przetwarzać w chmurze, a które chcesz przetwarzać jedynie lokalnie

Obecnie wykorzystanie rozwiązań chmurowych radykalnie upraszcza pewne zagadnienia. Pracownicy działu IT opierając się na nich nie muszą martwić się o bieżące aktualizowanie działającego oprogramowania, gdyż dostawca usługi chmurowej wykonuje te operacje automatycznie ze swojej strony. Znacznie upraszcza się również praca zdalna, w sytuacji, kiedy firma działa w strukturze rozproszonej.

Z drugiej strony, jeśli decydujesz się na rozwiązania chmurowe warto sprawdzić, gdzie dane są przetwarzane, jakie dane będą wysyłane z organizacji i jaką dostępność gwarantuje dostawca usługi. Wybieraj dostawcę rozwiązań chmurowych biorąc pod uwagę również przepisy prawne. W zależności od sytuacji może być konieczne podpisanie umowy o powierzeniu przetwarzania danych osobowych.

Sprawdź proces autoryzacji użytkowników: polityki tworzenia haseł i dwuskładnikowe uwierzytelnianie, nadawanie i odbieranie uprawnień

Podstawą bezpieczeństwa systemów jest zapewnienie, aby tylko uprawnione osoby miały dostęp do informacji i systemów. Niezbędny jest do tego właściwy proces autoryzacji użytkownika, a więc upewnienia się przez organizację, że ktoś, kto próbuje uzyskać dostęp do informacji jest do tego uprawiony oraz że to faktycznie jest właściwa osoba.

Współcześnie funkcję tę realizuje zwykle uzyskiwanie dostępu za pomocą podania odpowiedniej nazwy użytkownika i hasła. W celu zapewnienia podstawowej ochrony należy wdrożyć w firmie zasady tworzenia i aktualizacji haseł (np. dopuszczanie haseł o pewnej minimalnej długości i cykliczną zmianę haseł). Ogromną rolę w tym procesie odgrywa szkolenie pracowników. Należy uświadomić zespół, że nie wolno dopuszczać do sytuacji, w której pracownicy korzystają z kont dostępu swoich kolegów, notują hasła zostawiając je w widocznym miejscu lub przesyłają otwartą pocztą elektroniczną.

Związane jest z tym również zagadnienie stworzenia właściwego systemu uprawnień w organizacji i kontroli procesu nadawania uprawnień nowym pracownikom. Obejmuje to cykliczne przeglądanie sytuacji, w których

pracownicy uzyskują nowe, szersze uprawnienia aż po sytuację, w której należy wyłączyć wszystkie dostępy osobom, które opuszczają firmę. Niestety problem, w którym były pracownik nadal może zyskać dostęp do poufnych systemów organizacji potęguje się w sytuacji coraz powszechniejszego wykorzystania systemów w chmurze. Jeśli były pracownik ma dostęp do takiego systemu, to nawet jeśli jest już odcięty od wewnętrznej sieci firmowej, może okazać się, że nadal ma dostęp do systemu przez przeglądarkę internetową.
Wyższym poziomem zabezpieczeń jest zastosowanie tzw. uwierzytelnienia dwuskładnikowego (2FA – Two Factor Authentication). To uwierzytelnienie zapewnia nieporównywalnie wyższy poziom bezpieczeństwa, niż nawet skomplikowane hasło. Mechanizm łączy to co pracownik wie (hasło) z tym, co pracownik posiada – może to być np. jednorazowy kod wygenerowany na jego telefonie komórkowym lub dane biometryczne np. skan odcisku palca lub tęczówki oka.

Zaplanuj systematyczne szkolenia pracowników

Rozwiązania techniczne, normy ISO, skany tęczówki i inne najbardziej zaawansowane systemy będą niewiele warte, jeśli pominiemy budowanie kultury bezpieczeństwa w organizacji. Dlatego nieodzownym elementem myślenia o bezpieczeństwie są cykliczne szkolenia pracowników na temat zasad obowiązujących w firmie.

Szkolenia powinny obejmować nie tylko ogólne zasady polityki bezpieczeństwa przyjętej w firmie, ale również standardy zachowania w konkretnych sytuacjach, jak np. reguły wpuszczania gości na teren firmy, zasady zarządzania hasłami czy w szczególności otwierania e-maili z nieznanych źródeł. W szkoleniach należy położyć szczególny nacisk na aspekt praktyczny i sprawdzanie wiedzy.

Świetnym motywatorem dla pracowników są dostępne obecnie na rynku platformy służące do symulowania kampanii phishingowych wobec osób zatrudnionych w firmie. Stosując taką platformę, zespół odpowiedzialny za cyberbezpieczeństwo może rozesłać symulowany „atak phishingowy" do pracowników, np. e-mail udający wiadomość od kontrahenta czy przełożonego i nakazujący otwarcie jakiegoś załącznika lub zarejestrowanie się na stronie internetowej w celu pobrania np. faktury. Następnie prowadzący taką akcję edukacyjną zyskuje dostęp do pełnych raportów. Wiemy, którzy z pracowników otwarli spreparowany e-mail, którzy kliknęli w link w nim zawarty i którzy zarejestrowali się na fałszywej witrynie internetowej. Jest to angażująca forma sprawdzania skuteczności szkoleń prowadzonych dla personelu, która pod względem funkcjonalności, przypomina akcje typu „tajemniczy klient" stosowane wobec pracowników struktur sprzedażowych.

Wprowadź całościowy system zarządzania bezpieczeństwem informacji

Objętość tej publikacji pozwala na przytoczenie jedynie najważniejszych, oczywistych rekomendacji, które będą aktualne dla każdej firmy. Jeśli jednak firma chce zagwarantować sobie najwyższy poziom bezpieczeństwa, nie wystarczy opierać się na ogólnych rekomendacjach, ale należy we współpracy z profesjonalistami, najczęściej zewnętrznymi partnerami stworzyć i wdrożyć całościowy system zarządzania bezpieczeństwem informacji.

Podstawowym efektem takiego wdrożenia będzie podjęcie decyzji na podstawie realnych ryzyk, stworzenie praktycznych zasad indywidualnych dla danej organizacji i uwzględniających jej specyfikę oraz potrzeby. To swego rodzaju „wyższy poziom wtajemniczenia". Aby go osiągnąć, należy stworzyć w organizacji odrębną komórkę odpowiadającą za bezpieczeństwo i planować takie wdrożenie w porozumieniu z kierownictwem najwyższego szczebla.

Poziom wyżej – jak sprawdzić słabe strony?

5. POZIOM WYŻEJ – JAK SPRAWDZIĆ SŁABE STRONY?

Zastosowanie rekomendacji z poprzedniego punktu, to pewne minimum. Jednak, aby organizacja mogła skupić się na ochronie tego, co dla niej najważniejsze, przed etapem konfigurowania zabezpieczeń należy wykonać pracę analityczną. Współcześnie określenie ważności i potrzeb cyberbezpieczeństwa zaczyna się zwykle wewnątrz danej organizacji. Przynajmniej tak powinno być. Niektóre z firm stają się coraz bardziej świadome cyberzagrożeń, a na inne nakładane są pewne wymagania, które muszą zostać spełnione np. europejska dyrektywa NIS2. Są też firmy, które padły ofiarą cyberataku i dopiero w jego wyniku zmieniają swoje podejście, profesjonalizując swoje myślenie o cyberbezpieczeństwie.

Niezależnie od grupy, do której zalicza się firma, aby osiągnąć odpowiedni poziom cyberbezpieczeństwa należy sięgnąć do podstaw określających cyberbezpieczeństwo, czyli tzw. triady CIA a nawet CIAA. Co to takiego? Są to pewne atrybuty (własności), które muszą zostać spełnione, aby zapewnić bezpieczeństwo informacji. Jakie to atrybuty?

- Confidentiality (poufność) – czyli zapewnienie, że do informacji nie ma dostępu nikt, kto tego dostępu mieć nie powinien lub innymi słowy, dostęp mają tylko osoby uprawnione.
- Integrity (integralność) – to zapewnienie, że informacja nie zostanie zmieniona inaczej niż w celowy dla organizacji sposób (czyli np. żadna osoba trzecia nie będzie w stanie podmienic pewnych danych na fałszywe).
- Availability (dostępność) – to zapewnienie, że informacje mogą być wykorzystywane przez określone osoby w wyznaczonym czasie.
- Accountability (odpowiedzialność) – to zapewnienie, że możliwe będzie ustalenie osób odpowiedzialnych za dane operacje.

Zrozumienie CIA/CIAA jest ważne przy wyznaczaniu mapy naszej organizacji, którą powinniśmy zrobić w pierwszej kolejności, aby określić procesy, procedury, dokumenty oraz systemy, które są wykorzystywane w tych procesach.

Przy określaniu wymagań powinniśmy zadać sobie wiele pytań, w tym m.in.:

- Które poufne dane nie mogą wyciec oraz w którym miejscu moja firma te dane przetwarza?
- Które dane nie mogą zostać zmienione i musi zostać zachowana ich integralność?
- W którym miejscu brak dostępności działania systemów lub posiadania danych ma ogromny wpływ na działanie organizacji?
- Kto za dane działania jest odpowiedzialny?

Mając określone procesy/elementy kluczowe dla organizacji, można przystąpić do mapowania infrastruktury informatycznej. Pozwoli to określić jakie systemy informatyczne działają w kluczowych obszarach, które są krytyczne oraz jak łączą się i jaki mają wpływ na pozostałe elementy działające w organizacji. Mapowanie infrastruktury pozwala nam określić, co powinniśmy zabezpieczać i jest jednym z pierwszych elementów budowania cyberbezpieczeństwa. Im więcej pracy włożymy w ten proces i wykonamy go dokładniej, tym lepsze efekty możemy osiągnąć tworząc i utrzymując bezpieczeństwo cyfrowe firmy.

W rzeczywistości wygląda to następująco. Tworzymy mapę tego, co jest technicznie wykorzystywane w kluczowych obszarach działania organizacji np. system CRM lub poczta email i na podstawie tego, określamy w jaki sposób np. nasz CRM łączy się z innym programem w firmie i jaki wpływ może mieć na niego ten inny system. Na podstawie określenia wpływów i zależności przechodzimy do analizy, aby oszacować poziom ryzyka. Posiadając te dane, ustalamy co powinno być chronione od strony technicznej i w jaki sposób możemy to chronić.

Praktycznie każda działająca firma posiada już pewne zastosowane zabezpieczenia techniczne oraz proceduralne. Dlatego ważne jest, aby weryfikować ich aktualny stan i porównać go z mapą procesów, sprawdzając czy i w jaki sposób do niej pasuje. Taka weryfikacja może dotyczyć zarówno części technicznej jak i dokumentacyjnej oraz może być wykonana na wiele sposobów. Dla niektórych skan podatności w infrastrukturze sieciowej będzie w zupełności wystarczający. Dla innych będą to testy penetracyjne razem z analizą kodu źródłowego aplikacji.

Na postawie porównania aktualnego stanu z mapą procesów krytycznych można dowiedzieć się, w którym miejscu aktualnie się znajdujemy oraz ustalić priorytety działań, które mają na celu podniesienie poziomu bezpieczeństwa cyfrowego firmy.

Ważnym elementem jest zachowanie równowagi pomiędzy poziomem zastosowanych zabezpieczeń, a możliwością korzystania z systemów, danych oraz kosztem użytych zabezpieczeń. Dlatego modelując proces cyberbezpieczeństwa dobrze jest pracować na tzw. “suwaku”, w którym musimy znaleźć odpowiedni balans pomiędzy tym, jakie zastosujemy środki bezpieczeństwa, a jaki będzie to miało wpływ na codzienną pracę oraz działanie firmy.

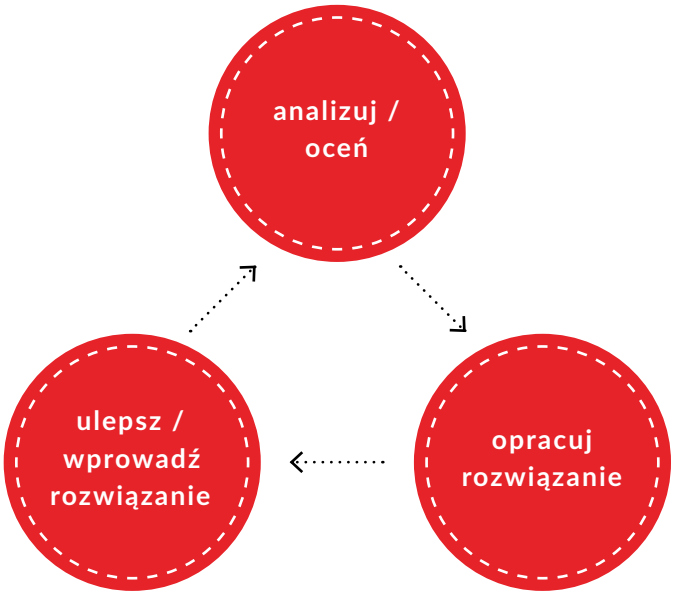
Niski poziom cyberbezpieczeństwa:
- unikanie kosztów
- brak ograniczeń w działalności zespołu
- ryzyko wystąpienia cyberataków i straty z nimi związane

Wysoki poziom cyberbezpieczeństwa:
- koszty
- odporność na cyberincydenty
- utrudniona praca organizacji

Przykładowe kategorie testów/audytów pozwalające ustalić stan faktyczny

Analiza cyberbezpieczeństwa to ciągły proces, który przynosi najlepsze rezultaty, jeżeli jest wykonywany cyklicznie. Każdą organizację można podzielić na trzy główne obszary, które są ze sobą połączone:

1. Bezpieczeństwo tzw. korporacyjne, czyli bezpieczeństwo informacji, w którego skład wchodzą polityki, procedury oraz ich stosowanie,
2. Bezpieczeństwo techniczne, do którego zaliczyć można zabezpieczenia infrastruktury informatycznej sieciowej, aplikacyjnej, sprzętowej,
3. Bezpieczeństwo czynnika ludzkiego, czyli to jaką wiedzę posiadają pracownicy w kontekście cyberbezpieczeństwa oraz jak stosują ją w codziennej pracy.



Wszystkie te elementy łączą się ze sobą i mają wzajemny wpływ. Prostym przykładem może być polityka tworzenia haseł, która w dokumentacji i procedurach określa, że długość hasła powinna zawierać minimum 12 znaków. Tak określone wytyczne, powinny być zastosowane we wszystkich używanych systemach w organizacji, aby realnie pracownik nie mógł ustawić krótszego hasła. Wymaganie wiedzy o cyberbezpieczeństwie od pracowników musi wiązać się z cyklicznymi szkoleniami i podnoszeniem świadomości. To tylko przykłady wzajemnych relacji, które pokazują, że do bezpieczeństwa i jego weryfikacji, należy podchodzić całościowo, skupiając się na kluczowych aspektach dla danej firmy.

Analizę cyberbezpieczeństwa można przeprowadzać na wiele różnych sposobów, poniżej przedstawiamy kilka z nich.

1) **Audyt bezpieczeństwa informacji** – polega na przeglądzie procedur i polityk bezpieczeństwa. Ocenia, czy i w jaki sposób organizacja stosuje skuteczne działania prewencyjne, mające chronić przed cyberatakami. Podczas takiego audytu weryfikuje się również czy zostało zastosowane dane rozwiązanie, jeżeli jest wymagane lub jakie inne środki zaradcze zostały wdrożone.

Przykład: Kontrola dostępu, w której możemy sprawdzić w jaki sposób są nadawane uprawniania do systemu, w jaki sposób odbierane i jak często należy wykonać przegląd uprawnień.

2) **Testy penetracyjne** – jest to kontrolowana symulacja realnego ataku hakerskiego, którego głównym celem jest próba przełamania zabezpieczeń. Wykonuje się je po to, aby odnaleźć luki, przez które prawdziwy atakujący mógłby dostać się do testowanego systemu lub infrastruktury. Testom penetracyjnym może podlegać między innymi infrastruktura sieciowa, aplikacja webowa, desktopowa, mobilna.

Przykład: Próba zmiany uprawnień z użytkownika na administratora albo próba wykonania jak największej liczby zalogowań różnymi danymi w celu dostania się do aplikacji.

3) **Testy socjotechniczne** – to symulowany atak wobec pracowników firmy, aby uzyskać nieautoryzowany dostęp do danych. Najczęstszym rodzajem są testy phishingowe, gdzie wykorzystywany jest fałszywy mail łudząco podobny do znanej instytucji, osoby jak również firmy, w której pracujemy. Do takich testów należy też szereg innych działań lub kontakt bezpośredni albo pośredni np. rozmowa telefoniczna, wiadomość SMS. Testy pozwalają nam zweryfikować, jak pracownicy mogliby zachować się przy realnym ataku skierowanym bezpośrednio w ich stronę.

Przykład: Mail z domeny przypominającej naszą firmową informujący o wynikach finansowych, zmianach personalnych lub całkowicie zewnętrzny, który swoim tematem ma zaciekawić pracownika jak np. możliwość wygrania biletów na mundial.

4) **Audyt konfiguracji** – polega na przeglądzie aktualnej konfiguracji urządzeń i oprogramowania w celu sprawdzenia czy zastosowana konfiguracja spełnia zalecenia producenta. Taka weryfikacja powinna być wykonywana przez certyfikowanych inżynierów danego rozwiązania. Celem sprawdzenia konfiguracji jest zapewnienie najwyższego standardu bezpieczeństwa w zastosowanych produktach, zgodnie z wytycznymi stawianymi przez producenta.

Przykład: Sprawdzenie czy nie zostały zastosowane domyślne hasła dla kont administratora, czy system nie obciąża zasobów serwera albo czy reguły zostały wprowadzone w odpowiedni sposób, który pozwala na ich działanie.

Rodzajów testów i audytów jest znacznie więcej, podobnie jak standardów, według których można je przeprowadzać, dlatego ważne jest, aby zdefiniować co chcemy poddać analizie i na podstawie tego odpowiednio dopasować konkretne rozwiązanie.

Wynikiem każdej analizy musi być raport, który ma określić co zostało wykonane podczas analizy oraz wskazać aktualny stan badanego obszaru. Obowiązkowo powinien zawierać informacje, co i w jaki sposób należy poprawić, aby podnieść poziom bezpieczeństwa. Dzięki temu jesteśmy w stanie zaplanować działania naprawcze lub usprawniające, następnie je wdrożyć i po określonym czasie ponownie przeprowadzić analizę. Warto bowiem pamiętać, że cyberbezpieczeństwo to ciągły proces.

Wdrożenie systemu zarządzania bezpieczeństwem informacji

6. WDROŻENIE SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Jeśli w naszej organizacji mamy wdrożone podstawowe rekomendacje, jeśli jesteśmy w stanie ustalić nasze słabe strony i to co dla naszej organizacji jest ważne, być może to nasza firma jest gotowa na kolejny poziom – wprowadzenie wystandaryzowanego systemu bezpieczeństwa informacji. System bezpieczeństwa informacji (SZBI) to nic innego jak pewna strategia działania, spójna na poziomie całej firmy. Zapewnia właściwą ochronę informacji, a także cykliczne sprawdzanie procedur organizacji, aby adaptować jej działanie do nowopowstających zagrożeń. Jest to standard kojarzony najczęściej z normą ISO 27001, jednak wdrażając tego rodzaju metodykę postępowania, niekoniecznie jesteśmy zobowiązani do wykonywania formalnej certyfikacji.

Jak zacząć, etapy wdrażania, sposób pracy poprawny metodycznie

Wdrożenie systemu zarządzania bezpieczeństwem informacji (SZBI) jest zawsze procesem złożonym i zazwyczaj długotrwałym w każdej organizacji. To, jak bardzo będzie wymagający system i jak długo będzie trwał projekt wdrożeniowy, zależy od kilku czynników:

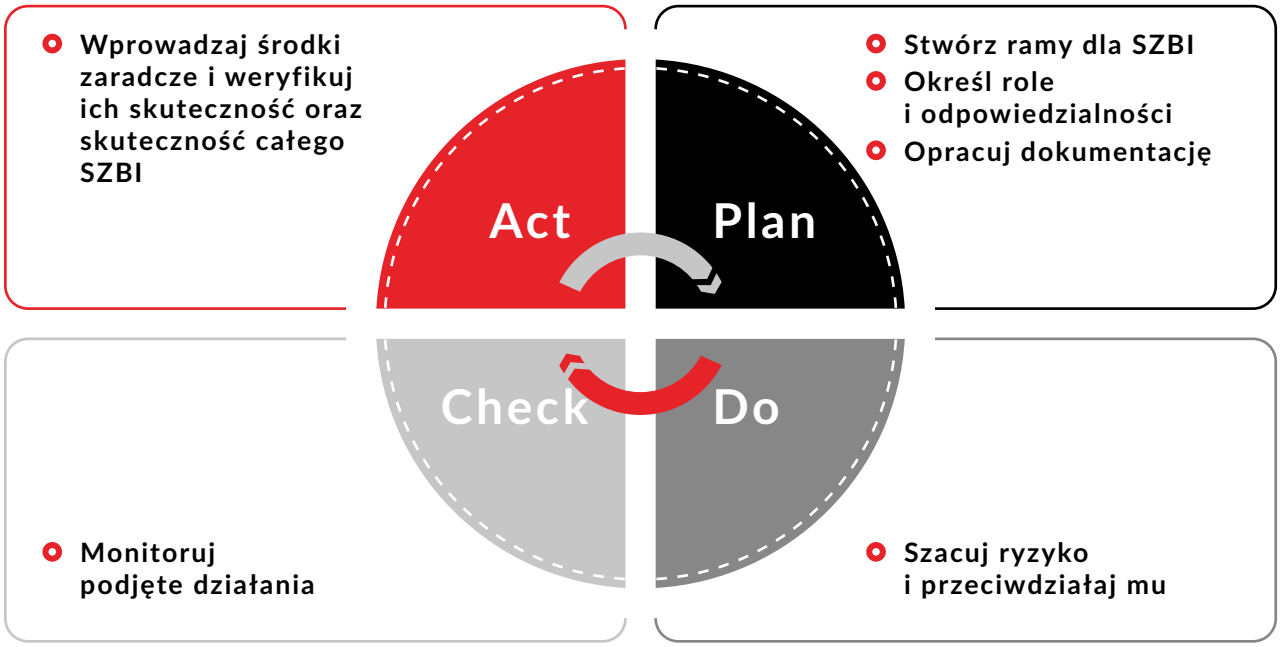
- branża, w której funkcjonuje organizacja;
- złożoność procesów w firmie;
- wielkość organizacji;
- podmioty z którymi organizacja współpracuje oraz ich wzajemne wymagania;
- specyficzne wymagania względem przepisów prawa;
- dojrzałość organizacji w zakresie bezpieczeństwa informacji (dojrzałość systemów IT/istniejących procedur eksploatacyjnych).

Niestety, ale nie istnieje jedna recepta na zbudowanie systemu SZBI, który będzie użyteczny, ale przede wszystkim skuteczny, a to właśnie skuteczność jest miarą sprawnego systemu i podlega szczególnej weryfikacji, w tym przez niezależne jednostki certyfikujące w trakcie audytów III strony.

Jak w każdym systemie SZBI, ważnym czynnikiem jest odpowiednie zaplanowanie i zapewnienie zasobów w zakresie IT (infrastruktura, systemy i zabezpieczenia), administracji (budynki – ich lokalizacja oraz zabezpieczenia fizyczne), ludzi (personel z odpowiednimi kompetencjami) oraz wiedzy na temat istniejących międzynarodowych standardów bezpieczeństwa informacji, zgodnie z którymi organizacja będzie chciała zbudować system.

Zanim organizacja przystąpi do wdrażania systemu zarządzania bezpieczeństwem informacji, powinna określić standard, na podstawie którego zamierza budować system zarządzania bezpieczeństwem informacji. Do najbardziej popularnych standardów zaliczamy ISO/IEC 27001, którego podejście oparte jest na ryzyku, a który doczekał się nowego wydania pod koniec 2022 roku.

Wdrożenie systemu SZBI opiera się o cykl Deminga (cykl PDCA), którego celem jest ciągłe doskonalenie – wymusza na organizacji stałe monitorowanie wdrożonego systemu w zakresie zmieniającego się otoczenia, wymagań branżowych oraz rynku. Cykl ten składa się z 4 faz: Plan (zaplanuj), Do (wykonaj), Check (zweryfikuj), Act (udoskonalaj).



Sprawne i skuteczne wdrożenie systemu SZBI zapewnią działania wsparte poniższymi krokami:

- **Zrozumienie kim jesteśmy** – czyli określenie tzw. kontekstu organizacji. Krok ten poświęcony jest identyfikacji tego, jakie są wymagania wobec branży, w której działa firma oraz zidentyfikowanie podmiotów zewnętrznych, z którymi dana organizacja współpracuje, aby osiągać cele biznesowe. Ważnym czynnikiem jest także zidentyfikowanie potrzeb organizacji względem tych podmiotów zewnętrznych, ale także potrzeb i wymagań jakie te podmioty mają wobec naszej organizacji. Innym ważnym czynnikiem jest identyfikacja czy organizacja nie podlega specyficznym przepisom prawa i jakie wiążą się w związku z tym ryzyka wobec niej. Otoczenie (położenie geograficzne, najbliższe sąsiedztwo), w którym funkcjonuje firma jest kolejnym czynnikiem, który należy brać pod uwagę, a który może negatywnie wpływać na jej działanie. Do kontekstu będziemy wracać przy każdym przeglądzie systemu zarządzania oraz w sytuacji znaczących zmian, które będą miały wpływ na jej funkcjonowanie oraz w zakresie procesów bezpieczeństwa informacji.

- **Określenie zakresu systemu zarządzania** – systemem można objąć całą organizację (wraz z podległymi lokalizacjami, jeśli istnieją) bądź tylko jej część (konkretne piony/komórki organizacyjne). Mogą to być tylko konkretne procesy funkcjonujące w danej firmie. Przy określaniu granic systemu, należy zawsze brać pod uwagę kontekst organizacji oraz współzależności pomiędzy organizacją a podmiotami trzecimi.

- **Zapewnienie wsparcia najwyższego kierownictwa** – aby system mógł powstać i być ciągle doskonalony, musi być zapewnione wsparcie oraz zaangażowanie z najwyższego poziomu w organizacji. Dzięki temu zostaną zapewnione niezbędne zasoby potrzebne w jego budowaniu oraz utrzymywaniu, czyli: zasoby ludzkie (kompetentny zespół), techniczne i organizacyjne oraz pewność, że zbudowana polityka oraz cele bezpieczeństwa informacji będą wspierały i będą zgodne z celami biznesowymi organizacji (jej strategią) oraz że wymagania systemu zarządzania będą zintegrowane z zidentyfikowanymi głównymi procesami funkcjonującymi w firmie.

- **Określenie kryteriów w zakresie szacowania ryzyk występujących w bezpieczeństwie informacji** – jednym z najważniejszych elementów budowania skutecznego systemu SZBI jest zidentyfikowanie luk i podatności występujących w firmie na poziomie organizacyjnym, osobowym, fizycznym i technicznym[6] (wg nowych kategorii zabezpieczeń normy ISO/IEC 27001:2022). Organizacja powinna zatem określić kryteria akceptacji ryzyk (akceptowalne i nieakceptowalne poziomy, względem których powinna wdrożyć działania zapobiegające wystąpieniu ryzyk). Należy pamiętać, że proces szacowania ryzyka powinien uwzględniać te związane z utratą podstawowych atrybutów bezpieczeństwa, czyli poufności, dostępności i integralności informacji (tzw. triada CIA). W zależności od wyników pierwszego szacowania ryzyka, organizacja powinna opracować i wdrożyć proces postępowania z ryzykiem w bezpieczeństwie informacji, aby:
  - dobrać odpowiednie działania względem zidentyfikowanych ryzyk (akceptacja, redukcja, współdzielenie, unikanie);
  - dobrać adekwatne zabezpieczenia (techniczne, fizyczne, organizacyjne);
  - porównać wybrane zabezpieczenia z tymi, jakie zostały zawarte w załączniku normatywnym A[7] (nowa norma ISO/IEC 27001:2022 przewiduje 93 zabezpieczenia, w tym 11 nowych);
  - opracować Deklarację Stosowania (na podstawie wdrożonych zabezpieczeń) – czyli wykaz zabezpieczeń, które zostały zastosowane w organizacji;
  - stworzyć plan postępowania z ryzykiem – czyli „pomysł" organizacji w jaki sposób, kiedy, jakimi zasobami zamierza wdrożyć zabezpieczenia;
  - określić cele bezpieczeństwa informacji, które będą spójne z przyjętą w organizacji polityką bezpieczeństwa informacji.

- **Zaplanowanie i zapewnienie odpowiednich zasobów** – bardzo ważnym krokiem jest przekazanie budowania i doskonalenia systemu osobom posiadającym odpowiednią wiedzę oraz kompetencje w zakresie ustanawiania, wdrażania, utrzymywania i ciągłego doskonalenia systemu zarządzania w organizacji.

- **Zinwentaryzowanie aktywów** – czyli wszystkiego, co ma wartość dla organizacji (głównie informacji), aby firma miała świadomość, co posiada i jaką te aktywa mają dla niej wartość, a co za tym idzie, jakie ryzyka z ich posiadaniem/przetwarzaniem są związane i w jaki sposób je zabezpieczać. Inwentaryzacja zasobów jest bardzo ważnym elementem, który ma swoje następstwa w procesie szacowania ryzyka. Aktywa (sprzętowe i informacyjne) powinny być cyklicznie weryfikowane, a zabezpieczenia dla nich dobierane na podstawie kolejnych wyników procesu szacowania ryzyka.

- **Sformułowanie dokumentacji wchodzącej w skład systemu zarządzania** – w tym tzw. dokumentów systemowych (ściśle wymaganych przez normę ISO/IEC 27001), ale także wszelkich dokumentów (w tym procedur eksploatacyjnych), które zostały stworzone przez organizację na potrzeby budowania systemu SZBI. To również określenie sposobów ich nadzorowania oraz aktualizowania wraz z zmieniającym się otoczeniem, w którym funkcjonuje firma bądź innymi czynnikami zewnętrznymi lub wewnętrznymi, które mają wpływ na jej działanie oraz bezpieczeństwo.

- **Wdrażanie działań związanych z zidentyfikowanymi ryzykami** – organizacja powinna cyklicznie prowadzić szacowanie ryzyka w bezpieczeństwie informacji oraz wdrażać plany postępowania z takim ryzykiem. Każda, istotna z punktu widzenia firmy zmiana, mająca bezpośredni wpływ na wdrożony system SZBI, np. zmiany w procesach biznesowych czy rozszerzenie zakresu usług oferowanych przez organizację, powinna być bodźcem do ponownej analizy szacowania ryzyk.

[6] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection https://www.iso.org/standard/27001
[7] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection https://www.iso.org/standard/27001

- **Monitorowanie wprowadzonych działań** – firma powinna ustalić w jaki sposób zamierza weryfikować, czy wprowadzone działania są skuteczne i pozwalają doskonalić wdrożony system SZBI. Organizacja we własnym zakresie powinna określić sposoby monitorowania swoich działań. Najczęstszymi działaniami są:
  - weryfikacja, czy cele bezpieczeństwa są realizowane;
  - analizowanie występujących incydentów bezpieczeństwa informacji i czy są wyciągane z nich wnioski, a także wprowadzane działania korygujące, które powinny minimalizować ponowne wystąpienie podobnych incydentów w przyszłości;
  - analizowanie bezpieczeństwa teleinformatycznego w oparciu o informacje pochodzące z systemów organizacji (np. firewalle, IDS/IPS, SIEM, SOAR, DLP);
  - analizowanie wyników skanowania podatności technicznych (z wykorzystaniem zatwierdzonych skanerów podatności, np. w oparciu o bazy międzynarodowe CVE, NVD);
  - analizowanie wyników testów penetracyjnych oraz testów socjotechnicznych;
  - analizowanie raportów dotyczących naruszeń ochrony danych osobowych;
  - analizowanie wyników testów i ćwiczeń planów ciągłości działania;
  - analizowanie skuteczności planów postępowania z ryzykiem w bezpieczeństwie informacji.

- **Przeprowadzanie audytów wewnętrznych** – organizacja powinna cyklicznie sprawdzać wdrożony system SZBI własnymi siłami lub wykorzystywać do tego celu podmioty, które specjalizują się w weryfikacji zgodności systemu SZBI z wymogami ISO/IEC 27001. To, jak często audyty wewnętrzne będą przeprowadzane w organizacji, będzie zależało od kontekstu organizacji, jej wielkości i złożoności procesów biznesowych oraz ogólnych potrzeb organizacji.

- **Wprowadzanie działań korygujących i doskonalenie systemu** – jeśli w trakcie audytów wewnętrznych zostały zidentyfikowane obszary do doskonalenia lub niezgodności z wymogami normy, firma powinna podjąć adekwatne działania (systemowe, techniczne, organizacyjne) w celu ich wyeliminowania. Bardzo ważnym aspektem jest, aby organizacja dokonywała przeglądów skuteczności podjętych działań korygujących oraz wprowadzała zmiany w systemie zarządzania, w sytuacjach, gdy jest to wymagane.

Szacuje się, że wdrażanie systemu SZBI trwa od 4 do 9 miesięcy, jednak proces ten może być dłuższy i zależny od ww. czynników wpływających na organizację.

Wdrożenie i utrzymywanie certyfikowanego systemu SZBI daje organizacji wiele korzyści

- Zbudowanie wizerunku silnej i świadomej firmy w zakresie cyberbezpieczeństwa.
- Uzyskanie zaufania wśród klientów oraz potencjalnych klientów.
- Spełnienie wymagań klientów i stron zainteresowanych.
- Większą kontrolę nad spoczywającymi wymaganiami prawnymi, specyficznymi dla danej branży.
- Nacisk na budowanie własnej świadomości cyberbezpieczeństwa.

- Większą kontrolę nad informacjami, które organizacja tworzy oraz pozyskuje (przetwarza i przechowuje) od swoich klientów i kontrahentów.
- Obniżenie kosztów powodowanych incydentami wynikającymi m.in. z braku świadomości pracowników.
- Usystematyzowane działania związane z reagowaniem na pojawiające się incydenty w organizacji.
- Zidentyfikowanie informacji wymagających szczególnej ochrony w firmie.
- Systematyczne doskonalenie zabezpieczeń stosowanych w organizacji, przy uwzględnieniu ich podatności i zmieniających się w trybie ciągłym zagrożeń.

To skomplikowane... Zatrudnić więcej ludzi czy postawić na zewnętrznego partnera?

7. TO SKOMPLIKOWANE... ZATRUDNIĆ WIĘCEJ LUDZI CZY POSTAWIĆ NA ZEWNĘTRZNEGO PARTNERA?

Opisane w poprzednich punktach rekomendacje – niezależnie do tego, na jakim poziomie zdecydujemy się je wdrażać – wymagają zwykle współpracy z firmami zewnętrznymi, specjalizującymi się w tematyce cyberbezpieczeństwa. Firmy wdrażające jedynie podstawowe rekomendacje zwykle poszukują po prostu dostawców rozwiązań. Jednak organizacje bardziej świadome, starające się przeanalizować swoje słabe strony, czy też wdrożyć pełen system zarządzania bezpieczeństwem organizacji, potrzebują znacznie bardziej zaawansowanych partnerów. Kilka przykładowych modeli współpracy opisujemy poniżej.

Partner dostarczający rozwiązania – najpopularniejszy w średnich firmach. Czy damy radę zrobić dobrze resztę?

Prawdopodobnie najpopularniejszym modelem współpracy z zewnętrznymi partnerami zajmującymi się cyberbezpieczeństwem jest model, w którym większość decyzji dotyczących bezpieczeństwa informatycznego podejmowanych jest wewnątrz organizacji. Do tego uogólnienia nie pasują mikrofirmy, zbyt małe na zatrudnianie własnych specjalistów IT i z tego powodu zlecające te zadania w całości na zewnątrz (co sprowadza się do tego, że informatyk na części etatu instaluje oprogramowanie antywirusowe lub konfiguruje firewall i zdalny dostęp) oraz największe organizacje, które z powodu znaczących wymagań decydują się na stałą współpracę z dużymi, wyspecjalizowanymi w tematyce cyberbezpieczeństwa jednostkami.

W typowej średniej wielkości organizacji to zatrudnieni wewnątrz specjaliści porównują technologie dostępne na rynku, często w długim i żmudnym procesie testowania, starając się dopasować dostępne rozwiązania do konkretnych potrzeb. Niestety w polskich realiach średnich firm, osoby odpowiedzialne za cyberbezpieczeństwo danej organizacji, często równocześnie odpowiadają za całe bieżące funkcjonowanie infrastruktury informatycznej. Personel jest zmuszony rozstrzygać dylemat; czy zajmować się niedziałającą drukarką w gabinecie prezesa, bieżącymi problemami z funkcjonowaniem poczty internetowej, czy też zająć się tematami ważnymi strategicznie, których jednak organizacja nie docenia, dopóki nie dojdzie do skutecznego ataku. Jeśli w organizacji nie rozdzielono skutecznie zespołu odpowiedzialnego za bezpieczeństwo informacji, od zespołu odpowiedzialnego za utrzymanie bieżącego funkcjonowania systemów IT, najczęściej dochodzi do sytuacji, w której nigdy nie starcza czasu na należyte przygotowanie i wdrożenie polityk bezpieczeństwa. Oznacza to, że firma powierza ważne decyzje dotyczące zaplanowania bezpieczeństwa własnym pracownikom. Jednak oni, z powodu braku czasu lub braku kompetencji, swoje działania sprowadzają do wyboru rozwiązań ochronnych i wyboru partnera, który takie rozwiązania dostarczy.

Zewnętrzny partner to tak naprawdę sprzedawca konkretnych rozwiązań – sprzętu, serwerów, oprogramowania antywirusowego, firewalli.

Wyzwaniem w sytuacji takiego podziału prac są duże wymagania stojące przed wewnętrznym zespołem danej organizacji. Model ten grozi występującą niestety często sytuacją, w której wprawdzie firma zakupiła rozwiązania, ale nie ma pełnej wiedzy na temat ich poprawnego stosowania lub jej pracownicy nie mają czasu na zajmowanie się funkcjami cyberbezpieczeństwa.

Partner łączący doradztwo, dostarczanie rozwiązań, ich konfigurację i szkolenia pracowników – pożądany model dla większości firm

Jak zwracaliśmy uwagę, typowym problemem w wielu polskich organizacjach jest stosowanie rozwiązań, dla których pracownicy nie mają należytych kompetencji, by skutecznie je wdrożyć i stosować. Drugim bardzo częstym problemem jest korzystanie z partnerów, którzy jedynie dostarczają rozwiązania, podczas gdy organizacja nie potrafi samodzielnie zidentyfikować, co przede wszystkim powinna chronić i jakie są najsłabsze punkty w jej zabezpieczeniach. Nawet, jeśli firma nie jest gotowa na wdrożenie pełnego systemu zarządzania

bezpieczeństwem informacji, to dobrym rozwiązaniem pośrednim jest związanie się z zewnętrznym, zaufanym partnerem o większych kompetencjach. Taki partner pomoże naszej organizacji przynajmniej w ograniczonym stopniu przeanalizować, jakie kierunki ataków są dla nas największym zagrożeniem. Następnie przeprowadzi z nami przynajmniej podstawowe mapowanie procesów i infrastruktury oraz oceni, jakie rodzaje zabezpieczeń należy wdrożyć w pierwszej kolejności. Dobrze, jeśli usługodawca zajmujący się cyberbezpieczeństwem będzie w stanie zapewnić pełen pakiet szkoleń dla pracowników, aby w wypadku wdrożenia nowych systemów upewnić się, że administratorzy potrafią je w pełni wykorzystać.

Partner konsultujący wdrożenie systemu zarządzania bezpieczeństwem informacji

Jeśli nasza organizacja decyduje się na wdrożenie pełnego systemu tego rodzaju, warto rozpocząć od wyboru właściwego partnera. Firma, która przymierza się do wdrożenia systemu SZBI, nie musi realizować wszystkich związanych z tym działań samodzielnie. Może skorzystać z pomocy doświadczonych firm, które pomogą w skuteczny sposób opracować system SZBI, w tym wspomóc organizację przy właściwej identyfikacji głównych procesów biznesowych, które mają znaczenie dla bezpieczeństwa informacji, a także wspólnie wypracować mechanizmy i narzędzia z zakresu ciągłości działania, optymalne z punktu widzenia specyfiki organizacji.

Jak taka współpraca mogłaby wyglądać?

Działania w tym zakresie można podzielić na kilka faz:

- **Faza I – formułowanie dokumentacji systemu SZBI:**
  Podstawowym założeniem jest bezpośrednia współpraca pomiędzy firmą, a pracownikami. Dzięki temu możliwe jest uzyskanie koordynacji w zakresie wiedzy i zaangażowania obydwu stron. Głównymi elementami tej fazy są:
  - przeprowadzenie niezbędnych szkoleń dotyczących wymagań normy ISO/IEC 27001;
  - wsparcie przy identyfikowaniu procesów biznesowych oraz kontekstu organizacji;
  - wsparcie przy przeprowadzeniu szacowania ryzyka oraz wynikających z niej planów postępowania z ryzykiem;
  - wsparcie przy opracowaniu polityki bezpieczeństwa informacji, a także celów bezpieczeństwa informacji;
  - stworzenie procedur systemowych oraz wszelkich innych procedur eksploatacyjnych, w tym procedur dotyczących ciągłości działania procesów biznesowych.

- **Faza II – Weryfikacja i doskonalenie systemu SZBI:**
  Ten etap poświęcony jest wspólnemu wypracowaniu właściwych metod doskonalenia funkcjonującego systemu SZBI. Do elementów tej fazy należą:
  - wsparcie przy przeprowadzaniu działań korygujących;
  - wsparcie przy planowaniu audytów wewnętrznych;
  - wsparcie przy przeprowadzaniu przeglądu zarządzania systemu SZBI.

Wdrożenie systemu SZBI przy współpracy z właściwymi partnerami zapewni firmie wiele korzyści. Oprócz zwiększenia poziomu bezpieczeństwa, może znacznie wpłynąć na zwiększenie świadomości wśród pracowników. Pozwoli również na uzyskanie pełnego rozpoznania specyfiki biznesu oraz wpłynie pozytywnie na wzmocnienie wizerunku oraz autorytetu organizacji na rynku.

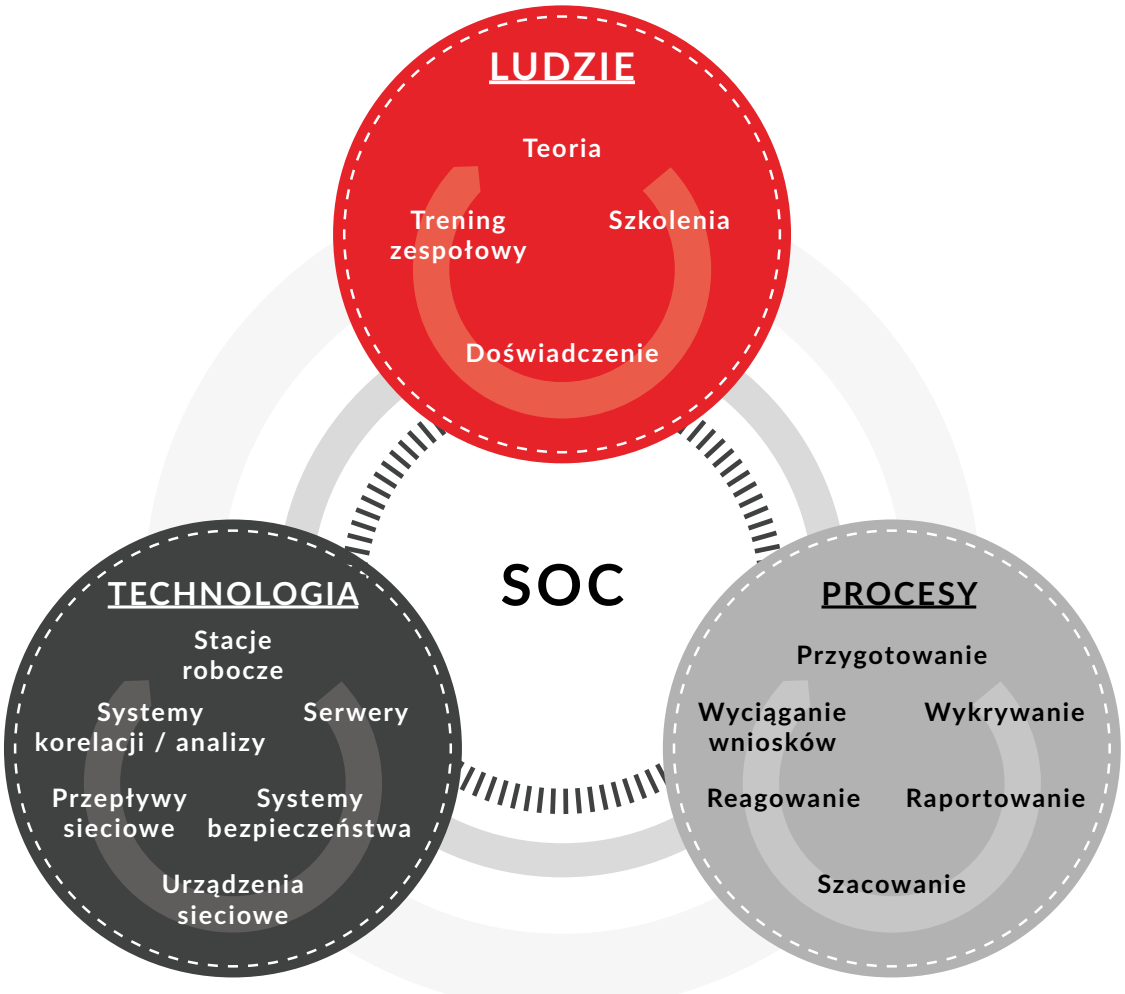
W efekcie wdrożenia takiego systemu organizacja zyskuje również konkretną wiedzę, jakiego rodzaju rozwiązania techniczne należy zastosować. Może więc następnie poszukać partnerów wyspecjalizowanych w konkretnych kategoriach rozwiązań i zapewniających oprócz samego ich dostarczenia – cały pakiet wsparcia (wdrożenie, szkolenia, wsparcie serwisowe).

Opcja dla zaawansowanych – współpraca z zewnętrznym Security Operations Centre. Czym się kierować wybierając partnera?

Najwyższym poziomem cyberbezpieczeństwa jest związanie się z zewnętrznym partnerem, który zapewni nam tzw. usługę Security Operations Center (SOC). Jest to usługa bieżącego monitorowania stanu bezpieczeństwa firmy, a więc wykrywania, analizowania i reagowania na incydenty za pomocą kombinacji rozwiązań technologicznych i zestawu procesów. W polskich realiach, na tego rodzaju współpracę decydują się obecnie tylko organizacje o najwyższych wymaganiach w zakresie bezpieczeństwa, ale model ten zyskuje w ostatnich latach coraz większą popularność również wśród mniejszych biznesów.

Elementy usługi SOC

Wybierając SOC zwróćmy uwagę czy usługa pokryje wskazane obszary.



Szukając firmy świadczącej usługi Security Operations Center dopytujmy o to, co stoi za samą ofertą jaką otrzymamy. Sama informacja o tym jak zwymiarowana jest usługa to jedno. Czasy reakcji, liczba obsługiwanych zdarzeń, sposób raportowania, dostępność kolejnych linii SOC, oferowany dodatkowo system jak SIEM (system zapewniający szeroki wgląd w to, co dzieje się wewnątrz organizacji przez zbieranie logów z różnych rozwiązań i ich korelowanie) czy SOAR (umożliwiający automatyzację reakcji na zagrożenia) – to powtarzalne, konkretne składniki ofert. To co jest jednak niezwykle istotnym elementem zewnętrznej usługi SOC, to kwestie związane z przygotowaniem wdrożenia usługi, wdrożeniem usługi i jej rozwojem w trakcie współpracy z klientem. I to na te obszary powinniśmy w szczególności zwrócić uwagę.

Źródła – co konkretnie ma analizować partner zewnętrzny w ramach SOC?

Aby SOC mógł właściwie chronić firmę w obszarze cyberprzestrzeni, musi „patrzeć" we właściwe miejsca naszej infrastruktury. Techniczna realizacja takich „oczu" dla Security Operations Center to źródła, czyli konkretne systemy, urządzenia czy też inne elementy powiązane z naszym środowiskiem IT czy OT. To od źródeł zależy czy SOC będzie miał precyzyjne dane do dalszej analizy i czy monitorowane są obszary najważniejsze, powiązane z najistotniejszymi dla organizacji ryzykami. Jeśli sami nie mamy odrobionej pracy domowej z tych tematów, sama usługa SOC może być niestety nietrafionym pomysłem, gdyż wykonawca będzie od nas wymagał wskazania źródeł, a wtedy najczęściej wybiera się te, które albo są łatwe do integracji np. z systemem klasy SIEM, albo wydają się być atrakcyjnymi z punktu widzenia obszarów do monitorowania. Przypomina to próbę trafienia strzałą do celu, przy czym łucznik ma opaskę na oczach, a celem jest jabłko ustawione na głowie naszej firmy. Czasami się udaje. A czasami nie. Ponadto nasza infrastruktura, systemy, sposób pracy zmienia się w czasie. Dlatego i źródła powinny podlegać przeglądom, tak aby mieć pewność, że SOC nadal patrzy we właściwe dla nas miejsca. Jeśli zakontraktowane mamy monitorowanie konkretnej liczby, konkretnego typu źródeł na początku umowy, to upewnijmy się, że mamy od usługodawcy wsparcie w okresowych przeglądach i czy aby nie trzeba zmienić ich konfiguracji lub w ogóle nie zmienić źródeł. Wyobraźmy sobie nie tak rzadko spotykany scenariusz, gdy rozpoczynamy współpracę z firmą świadczącą usługę SOC w momencie gdy system pocztowy mamy umieszczony lokalnie, w naszej infrastrukturze IT. Po kilku kwartałach przenosimy nasz system w całości do rozwiązania w chmurze. Jak wtedy wygląda sprawa monitorowania tego obszaru przez SOC? Czy możemy liczyć na realne wsparcie usługodawcy, czy jednak musimy zatrudnić dodatkowo integratora, który wykona dla nas niezbędne prace związane z konfiguracją takiego nowego źródła? Szukajmy na rynku takich firm świadczących usługę SOC, które mają szerokie kompetencje i realne zaplecze w postaci wykwalifikowanych inżynierów. Zaoszczędzimy sobie typowego ping-ponga pomiędzy naszym zespołem IT, usługodawcą SOC i integratorem wdrażającym nowy system lub utrzymującym konkretny obszar naszej infrastruktury.

Rozwijaj myślenie o cyberbezpieczeństwie

Wybierając firmę świadczącą Security Operations Center przedyskutujmy w jaki sposób będzie testowana skuteczność wdrożonych elementów usługi i jak będzie wyglądał proces jej doskonalenia. Umowy na tego rodzaju usługi podpisywane są zazwyczaj na 2–3 lata. W dobie dynamicznych zmian i szybkiego rozwoju technologii to okres bardzo długi, w którym z dużym prawdopodobieństwem w naszej firmie nastąpią istotne zmiany. Czy to związane z ryzykami, infrastrukturą IT/OT, czy też regulacjami zewnętrznymi. Za takimi zmianami musi podążać cała infrastruktura naszego cyberbezpieczeństwa.

Mając silne wsparcie wyspecjalizowanej grupy ekspertów z ramienia zewnętrznego usługodawcy SOC, dopytajmy na etapie wyboru takiego partnera, jak taka firma będzie współpracowała z nami w celu podniesienia naszego poziomu dojrzałości w obszarze cybersecurity. Samo wysyłanie cyklicznych raportów oraz informowanie nas o incydentach najwyższego poziomu nie powoduje, że jako organizacja stajemy się bardziej dojrzali w tym obszarze. Mapy i zalecenia dotyczące rozwoju, transfer wiedzy, współpraca warsztatowa, przegląd architektury cyberbezpiczeństwa, szkolenia z technologii oraz z bezpieczeństwa cyfrowego – im szersza potencjalna możliwość współpracy i gwarancja dostępności takich narzędzi w ramach umowy, tym większa korzyść dla naszej organizacji. Unikniemy w ten sposób sytuacji, w której po kilku latach płacenia za SOC zostajemy

z pokaźnym zbiorem raportów, informujących o tych samych, nierozwiązanych problemach z naszym cyberbezpieczeństwem.

Autorzy:
Paweł Jurek
Karolina Kraśniewska
Dawid Zięcina
Krystian Paszek
Marcin Mazur

DAGMA
BEZPIECZEŃSTWO IT

Pracodawcy RP
Rok założenia 1989

Pragmatic Solutions

DAGMA
BEZPIECZEŃSTWO IT

ISBN 978-83-956155-8-0