GAZETA FINANSOWA
14 – 20 grudnia 2018 r.

FIRMA BEZPIECZNA W SIECI

Cyberbezpieczeństwo – co nam grozi?

W ciągu najbliższych lat będziemy świadkami rozwoju przestrzeni cyberataków, przy jednoczesnym zmniejszaniu widoczności i kontroli nad infrastrukturą informatyczną. Powszechność urządzeń podłączonych od sieci, które uzyskują dostęp do danych osobistych i finansowych – armii urządzeń IoT i infrastruktury krytycznej stosowanych w samochodach, domach, biurach i inteligentnych miastach – oraz rosnąca sieć wzajemnych połączeń stwarzają nowe możliwości dla cyberprzestępców.

Jolanta **Malak**

dyrektor sprzedaży Fortinet na Polskę, Białoruś i Ukrainę

Cyfrowi kryminaliści są coraz bieglejsi w wykorzystywaniu takich osiągnięć jak sztuczna inteligencja, co czyni ataki jeszcze bardziej skutecznymi. Ten trend zapewne jeszcze przyspieszy w 2018 roku. Co nas czeka w tym zakresie?

Wzrost samouczących się sieci hivenet i swarmbots

Bazując na wyrafinowanych atakach, takich jak Hajime oraz Devil's Ivy lub Reaper, można przewidywać, że cyberprzestępcy zastąpią botnety inteligentnymi klastrami zainfekowanych urządzeń, nazywanych hivenetami, aby otworzyć skuteczniejsze wektory ataku. Hivenety wykorzystują metodę samouczenia, aby skutecznie docierać do zagrożonych systemów na niespotykaną dotąd skalę. Będą one w stanie komunikować się ze sobą oraz podejmować działania na bazie analizy lokalnie zbieranych danych. Hivenety będą rosły wykładniczo, co zwiększy ich zdolność do jednoczesnego ataku na wiele ofiar i znacznie utrudni podjęcie przeciwdziałań. Laboratorium FortiGuard Labs odnotowało w tym roku 2,9 mld prób komunikacji botnetowej tylko w ciągu jednego kwartału.

Ransomware to wielki biznes

Chociaż dzięki nowym typom oprogramowania, jak np. ransomworm, liczba ataków ransomware wzrosła w ciągu ostatniego roku aż 35-krotnie, to nie należy sądzić, że to ostatnie słowo cyfrowych wyłudzaczy. Następnym wielkim celem dla tego typu ataków będą prawdopodobnie dostawcy usług w chmurze. Złożone hiperpołączenia sieciowe, które tworzą dostawcy usług w chmurach, mogą skutkować tym, że pojedynczy punkt awarii dotknie setki firm, instytucji państwowych, organizacji opieki zdrowotnej oraz infrastrukturę krytyczną. Cyberprzestępcy zaczną łączyć technologie sztucznej inteligencji z wielowymiarowymi metodami ataku, aby skanować, wykrywać i wykorzystywać słabości dostawcy rozwiązań chmurowych.

Morphic Malware następnej generacji

Jeśli nie w przyszłym roku, to wkrótce po nim, zaczniemy dostrzegać złośliwe oprogramowanie stworzone całkowicie przez maszyny oparte na automatycznym wykrywaniu luk i skomplikowanej analizie danych. Polimorficzne złośliwe oprogramowanie nie jest nowe, ale przybierze inne oblicze. Poprzez wykorzystanie sztucznej inteligencji, zacznie tworzyć nowy, wyrafinowany kod, który za pomocą maszynowych procedur będzie w stanie nauczyć się, jak unikać wykrycia. Dzięki ewolucji istniejących narzędzi, przestępcy będą mogli rozwinąć najlepszy możliwy exploit w oparciu o charakterystykę każdej unikalnej słabości. Złośliwe oprogramowanie jest już w stanie używać modeli uczenia się, aby ominąć zabezpieczenia, a co za tym idzie, może wyprodukować nawet ponad milion odmian wirusa w ciągu dnia. Jak do tej pory wszystko to opiera się tylko na algorytmie, co ogranicza poziom zaawansowania i kontroli nad wynikiem. Eksperci Fortinet wykryli 62 miliony szkodliwych programów w jednym kwartale 2017 r. – wśród nich 16 582 warianty pochodzące z 2 534 rodzin malware'u. Z kolei 20 proc. organizacji stwierdza, że doświadczyła aktywności malware'u atakującego urządzenia mobilne. Zwiększona automatyzacja szkodliwego oprogramowania sprawi, że te statystyki staną się jeszcze bardziej niepokojące w nadchodzącym roku.

Infrastruktura krytyczna na pierwszy plan

Ze względu na kwestie strategiczne i ekonomiczne dostawcy i użytkownicy infrastruktury krytycznej nadal znajdują się na pierwszym miejscu listy najbardziej zagrożonych atakami. Organizacje te prowadzą sieci, które chronią ważne usługi i informacje. Jednak najbardziej krytyczna infrastruktura i operacyjne sieci technologiczne są kruche, ponieważ zostały pierwotnie zaprojektowane jako szczelne i izolowane. Oczekiwanie szybkiego reagowania na potrzeby pracowników i konsumentów zaczęło zmieniać wymagania wobec tych sieci, napędzając potrzebę zastosowania w nich zaawansowanych zabezpieczeń. Biorąc pod uwagę znaczenie tych sieci i potencjał niszczycielskich rezultatów ich naruszeń, dostawcy infrastruktury krytycznej dołączyli do wyścigu cyfrowych zbrojeń z organizacjami państwowymi, przestępczymi i terrorystycznymi.

Nowe usługi wykorzystujące automatyzację oferowane przez cyberprzestępców i Darkweb

Wraz ze zmianami w cyberprzestępczym półświatku, ewoluuje również Darkweb. Można się spodziewać, że wkrótce zobaczymy nowe oferty w modelu C-a-a-S (Cybercrime-as-a-service) pochodzące z Darkwebu, ponieważ już teraz widzimy tam zaawansowane usługi, wykorzystujące uczenie maszynowe. Na przykład usługa znana jako FUD (Fully Undetectable) jest już częścią kilku ofert. Umożliwia ona programistom zajmującym się cyberprzestępczością sprawdzenie, czy ich ataki i złośliwe oprogramowanie będą wykryte przez narzędzia bezpieczeństwa pochodzące od różnych dostawców. Dodatkowo w ramach usługi zwiększony zostanie poziom wykorzystania uczenia maszynowego, które służy do modyfikowania i podnoszenia skuteczności analizowanego kodu.

Stawiaj czoła zagrożeniom

Dzięki postępowi w dziedzinie automatyzacji i sztucznej inteligencji istnieje szansa dla przedsiębiorczych cyberprzestępców, aby wykorzystać odpowiednie narzędzia do poważnego naruszenia gospodarki cyfrowej. Rozwiązania bezpieczeństwa muszą być w odpowiedzi budowane wokół zintegrowanych technologii bezpieczeństwa, użytecznych informacji o zagrożeniach oraz dynamicznie konfigurowalnych systemów zabezpieczających. Ochrona powinna działać szybko, automatyzując reakcje, a także stosując inteligencję i samokształcenie, aby sieci mogły podejmować skuteczne i autonomiczne decyzje. Pozwoli to nie tylko zwiększyć widoczność i scentralizować kontrolę, ale także umożliwi strategiczną segmentację, podnoszącą poziom bezpieczeństwa. Ponadto podstawowe procedury bezpieczeństwa muszą stać się częścią polityki ochrony IT. Jest to wciąż często pomijane, ale kluczowe dla ograniczenia konsekwencji cyberataków.

FIRMA BEZPIECZNA W SIECI

Bezpiecznie założyć spółkę przez Internet?

W dobie powszechnego dostępu do Internetu coraz więcej spraw można załatwić w sieci. Oczywistym stało się robienie w ten sposób zakupów, opłacanie rachunków czy zamawianie jedzenia, ale coraz chętniej korzystamy też z możliwości przeprowadzania online działań natury urzędowej, nawet takich, jak założenie spółki. Choć to bardzo praktyczne rozwiązanie, warto skorzystać wcześniej z konsultacji doświadczonych prawników, by ustrzec się przed popełnieniem błędów, a w efekcie stratą czasu i pieniędzy Jak zatem założyć spółkę online, ile trwa takie przedsięwzięcie i na jakie trudności możemy natrafić?

Piotr **Pruś**

radca prawny z ECOVIS
Milczarek i Wspólnicy Kancelaria Prawna

Możliwość samodzielnego założenia spółki drogą elektroniczną jest kusząca i na pewno stanowi duże ułatwienie. Zanim przystąpimy do działania musimy jednak odpowiedzieć sobie na szereg pytań związanych z jej formą prawną, zasadami organizacji, przedmiotem działania czy rolą poszczególnych wspólników. Rejestracja firmy rodzi określone konsekwencje natury prawnej, finansowej i biznesowej, stąd wskazane jest w pierwszej kolejności zasięgnąć informacji u doświadczonego prawnika. Mimo wszystkich ułatwień, które niesie za sobą założenie spółki przez Internet, warto ten krok skonsultować z radcą prawnym. Doświadczony specjalista może nie tylko uchronić przed popełnieniem błędów i rozjaśnić wątpliwości pojawiające się w trakcie procesu rejestracji, ale przede wszystkim doradzić najlepsze rozwiązania dla planowanej działalności. Wyposażeni w niezbędną wiedzę, „świadomi swoich praw i obowiązków", możemy przystąpić do założenia spółki.

Najpierw EPUAP

Pierwszym krokiem w procesie założenia spółki jest utworzenie konta na epuap.gov.pl. Jest to niezbędne, gdyż dzięki możliwości zalogowania się na tej platformie będziemy mogli złożyć podpisy w końcowej fazie rejestracji spółki oraz dokonać wszelkich opłat. Sama rejestracja konta na EPUAP nie jest skomplikowana i zajmuje około 10 minut. Wystarczy wpisać swoje podstawowe dane, wybrać nazwę użytkownika i hasło. Kiedy konto jest już utworzone, należy je potwierdzić w ciągu 14 dni w najbliższym punkcie np. w banku. Lista miejsc, gdzie można tego dokonać jest długa i dopasowana do rejestrującego. Sam proces potwierdzania profilu trwa około 5-6 minut, a w jego trakcie wystarczy złożyć dwa podpisy.

Konto na stronie ministerstwa sprawiedliwości

W celu założenia wybranej przez nas spółki konieczne jest zarejestrowanie się na stronie Ministerstwa Sprawiedliwości, gdyż konto na platformie EPUAP nie wystarcza. Przysparza to nieco trudności – mniej doświadczona osoba może stracić około 10-15 minut na znalezienie miejsca, w którym może się zarejestrować, a także na weryfikację adresu e-mail.

Podstawowe dane spółki

Kiedy już uda nam się założyć to konto, można przystąpić do wypełniania rubryk z podstawowymi informacjami na temat spółki: jej nazwą, formą prawną, siedzibą, przedmiotem działalności. Wpisanie tych informacji zajmuje niewiele więcej niż 5-6 minut.

Kapitał zakładowy

Kolejny krok to wpisanie kapitału zakładowego oraz liczby udziałów w spółce. Jest to zaledwie kilka rubryk, ale mogą one nastręczyć pewne trudności, gdyż nigdzie nie ma podanej informacji jaka jest minimalna wymagana wartość owego kapitału. Wypełnienie tych rubryk zajmuje około 6-7 minut. Wpisanie zbyt niskiej kwoty spowoduje, że nie będzie możliwe złożenie podpisu w EPUAP. Trzeba wtedy wrócić do etapu określania kapitału.

Wspólnicy, udziały, organy spółki

Następnie wypełniamy rubryki dotyczące organów spółki takich jak Zarząd czy Rada Nadzorcza oraz zasad zbywania udziałów przez wspólników. Jest tu kilka opcji do wyboru, ale brakuje szczegółowych informacji na ich temat. Na przykład w przypadku zbycia udziałów mamy cztery opcje – od „Zbycie oraz zastawienie udziału wymaga zgody Spółki" aż po „ 1. Zbycie oraz zastawienie udziału nie wymaga zgody Spółki. 2. Zastawnik i użytkownik mogą wykonywać prawo głosu z udziału, na którym ustanowiono zastaw lub użytkowanie, jeżeli przewiduje to czynność prawna ustanawiająca ograniczone prawo rzeczowe oraz gdy w księdze udziałów dokonano wzmianki o jego ustanowieniu i o upoważnieniu do wykonywania prawda głosu". Bez specjalistycznej wiedzy może być trudno wybrać najkorzystniejszą opcję dla rejestrującego. Potencjalnie wybierze on więc opcję najbezpieczniejszą, czyli najprostszą do zrozumienia. Przejście przez te trzy kroki zajmuje około 15 minut.

Etap końcowy

Rejestracja, bez złożenia podpisów, zajmuje nieco ponad 43 minuty. Kolejnym krokiem jest złożenie podpisów w profilu na EPUAP, uiszczenie opłat oraz oczekiwanie na rejestrację. Warto przypomnieć, że ewentualne błędy popełnione w trakcie wypełniania poszczególnych rubryk np. wpisanie zbyt niskiej kwoty kapitału zakładowego pokazują się dopiero w końcowej fazie wypełniania wniosku, przez co trzeba wracać do wcześniejszych etapów, co może spowolnić cały proces.

Zmiana świadomości polskich przedsiębiorców

Popyt na rozwiązania z zakresu analityki danych może nad Wisłą wzrosnąć w 2019 roku nawet o 25-30 proc., wynika z szacunków TogetherData. Do czynników, które będą katalizatorami popytu należy zakwalifikować dywersyfikacje usług i oferty wykorzystania chmury publicznej. 73 proc. europejskich firm przetwarza już swoje dane w chmurze, dowodzi badanie przeprowadzone przez firmę Qubole. Jest to ponad 15 proc. więcej niż rok temu. Wynika to z faktu, że rozwiązania chmury publicznej wygrywają funkcjonalnością i ekonomiką z tradycyjnymi czystymi platformami danych.

Zdaniem IDC już w przyszłym roku dziewięć na dziesięć przedsiębiorstw będzie korzystać z rozwiązań opartych w części lub w całości na chmurze obliczeniowej. W 2025 roku biznes będzie tam umieszczał już 60 proc. ogółu swoich cyfrowych informacji. TogetherData szacuje, iż w Polsce w ciągu najbliższych 5 lat ten odsetek może wynieść od 40 do 50 proc. Godną uwagi siłą napędową rosnącego popytu na rozwiązania analityczne będzie zmiana świadomości polskich przedsiębiorców. Rodzimy biznes zaczyna przechodzić od ogółu do szczegółu, od fazy eksperymentów i weryfikacji poprawności koncepcji do realnych wdrożeń. Przyczyną tego są widoczne korzyści biznesowe. – mówi Michał Grams, prezes zarządu TogetherData. Nie mówi się już tylko o Big Data jako o efektywnym narzędziu, ale o konkretnych wdrożeniach i efektach. Mogą nimi być zwiększające się przychody w sklepach internetowych, optymalizacja kosztów procesów likwidacji szkód w ubezpieczalniach czy spadki fluktuacji pracowników w zakładach produkcyjnych. Wyzwaniem pozostaje wciąż strategia doboru danych, wynikająca z ich wielośródłowości. Różnorodność dostępnych źródeł danych stwarza trudności w stosowaniu i wdrażaniu systemów analitycznych. Zdaniem ekspertów TogetherData, tylko cztery na dziesięć firm w Polsce nie skarży się na brak specjalistycznej wiedzy, aby móc wykorzystać duże zbiory danych do dalszej analizy. Uporządkowanie zetabajtów informacji pochodzących zarówno ze źródeł online jak i offline, jest największym wyzwaniem dla podmiotów z branży zdrowotnej, przemysłowej oraz finansowej. Najlepiej w tym zakresie radzą sobie firmy technologiczne, telekomunikacyjne oraz handlowe. W przyszłym roku wyzwaniem dla polskich przedsiębiorców nie będzie sama kwestia wdrożenia narzędzi analizujących dane, tylko sprytnej i efektywnej strategii ich badania i wykorzystania. Moda na Big Data zmieni się w trend Smart Data. – tłumaczy Michał Grams, prezes zarządu TogetherData. Firmy muszą w zmienić swoje podejście. Nie liczy się bowiem ilość badanych i wykorzystanych biznesowo danych, lecz ich odpowiedni dobór. Technologia, rodzaj i forma narzędzi jest dopiero następnym krokiem.

CloudGuard SaaS – ochrona aplikacji w chmurze

CloudGuard SaaS, jeden z najnowszych dodatków do portfolio produktów bezpieczeństwa w chmurze - Check Point CloudGuard, chroni przedsiębiorstwa korzystające z aplikacji SaaS i poczty elektronicznej w chmurze (w tym Office 365, GSuite i OneDrive) oraz zapobiega ukierunkowanym atakom mającym na celu kradzież poufnych danych. W odpowiedzi na zaawansowane zagrożenia SaaS, usługa ta zapewnia 360-stopniową ochronę przed złośliwym oprogramowaniem, zagrożeniami typu zero-day, atakami typu phishing, a także przejęciami kont pracowników.

– W dzisiejszej piątej generacji cyberataków cybernetycznych kluczowe znaczenie ma wdrożenie technologii radzących sobie z coraz większą ilością zagrożeń dla aplikacji biznesowych opartych na chmurze – twierdzi Itai Greenberg, wiceprezes ds. zarządzania produktem w Check Point Software Technologies.

CloudGuard SaaS może być niezbędnym rozwiązaniem, które wyposaża firmy w niezbędne zabezpieczenia prewencyjne dla wielu aplikacji SaaS dla przedsiębiorstw w ciągu kilku min zaledwie kilku minut.

CloudGuard SaaS jest najskuteczniejszym rozwiązaniem zapobiegania naruszeniom w przypadku złośliwego oprogramowania i ataków zero-day na aplikacje SaaS, wykorzystującym wiodącą w branży technologię SandBlast Check Point. SandBlast uzyskał 100 proc. wskaźnik blokowania i najwyższy wskaźnik unikania testów z NSS Labs, uznanym na całym świecie zaufanym źródłem niezależnych, opartych na faktach testów bezpieczeństwa cybernetycznego.

Usługa blokuje przejęcia kont SaaS, uniemożliwiając nieautoryzowanym użytkownikom logowanie się, nawet jeśli urządzenie jest już narażone. Korzystając z nowej technologii ID-GuardTM, identyfikuje fałszywy dostęp poprzez wyszukiwanie błędnych loginów i centralizację uwierzytelniania wieloczynnikowego. Ponadto CloudGuard SaaS może uwierzytelniać użytkowników w dowolnej aplikacji SaaS na dowolnym urządzeniu mobilnym lub komputerze PC. CloudGuard SaaS powstrzymuje również wyrafinowane ataki phishingowe, które mogą ominąć inne rozwiązania.

FIRMA BEZPIECZNA W SIECI

Posypią się kary finansowe

Problemy z interpretacją przepisów ustawy o krajowym systemie cyberbezpieczeństwa oraz bardzo krótki czas na wypełnienie zadań nałożonych przez ustawodawcę przysporzą przedsiębiorcom sporo problemów. Kary finansowe za niewykonanie obowiązków wynikających z ustawy grożą zarówno firmom objętym legislacją, jak i osobom zajmującym kierownicze stanowiska.

Dawid **Bałut**

CEO TestArmy CyberForces

Od początku roku tylko do września 2018 w polskiej sieci doszło do ponad 2,5 tysiąca incydentów związanych z naruszeniem bezpieczeństwa (dane NASK). Teraz atak cyberprzestępcy będzie kosztował przedsiębiorców jeszcze więcej. Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa, która weszła w życie 28.08.2018 r., sankcje finansowe grożą OUK – objętym ustawą operatorom usług kluczowych oraz osobom zajmującym kierownicze stanowiska, którzy nie dopełnili swoich obowiązków.

Najbardziej zagrożone sektory

Oczywiście zdecydowana większość firm objętych ustawą już posiada odpowiednie wdrożenia oraz własne zespoły ludzi czuwających nad ochroną infrastruktury – to przede wszystkim sektor bankowości, finansów i operatorzy sieci. Natomiast brakuje rzetelnych danych, które pokazywałyby na ile bezpieczne są systemy wykorzystywane przez urzędy i jak często jednostki administracji publicznej stykają się z zagrożeniami. Publicznie niewiele wiadomo o stanie bezpieczeństwa w przedsiębiorstwach energetycznych, transportowych i z sektora zdrowotnego. Ukrywanie tych informacji przez organizacje zazwyczaj sugeruje, że poziom bezpieczeństwa jest niższy niż byśmy sobie życzyli. Zachowują takie informacje dla siebie w obawie o negatywną krytykę społeczeństwa oraz ściągniecie na siebie większej uwagi cyberprzestępców. Dlatego mierzymy się dzisiaj także z wyzwaniem kulturowym, wymagającym zrozumienia i zaakceptowania tego, że choć cyberbezpieczeństwo nie generuje bezpośrednich zysków, służy do minimalizowania strat finansowych oraz reputacyjnych w przypadku skutecznego ataku hakerskiego.

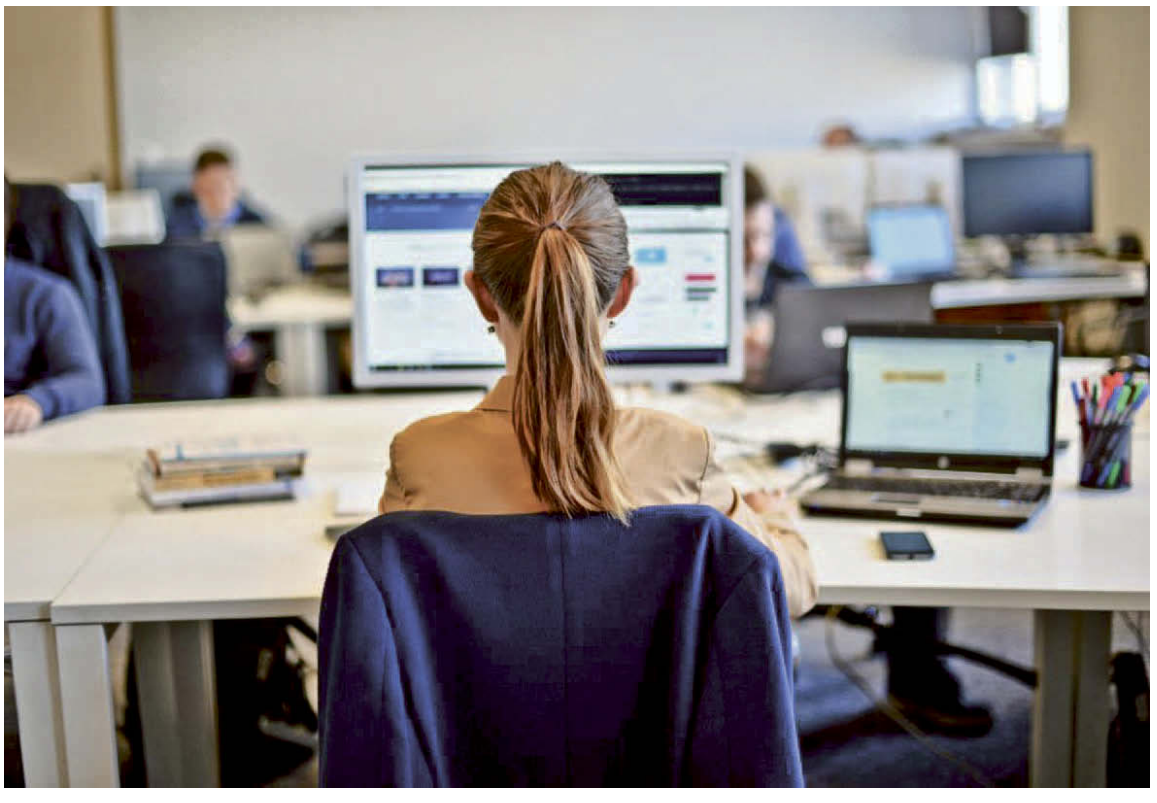
Trzy miesiące na wdrożenie przepisów w życie

Do tej pory brakowało regulacji państwowych w kwestii cyberbezpieczeństwa. Dlatego, choć dla części przedsiębiorców jest to temat nowy, jego realizacja nie może być rozciągnięta w czasie. Wdrożenia rozwiązań poprawiających stan bezpieczeństwa oczekuje się już teraz. Za niewykonanie obowiązków – grożą kary finansowe. Odliczanie czasu rozpoczyna się w momencie otrzymania decyzji administracyjnej o uznaniu podmiotu za operatora usług kluczowych (OUK) i wpisania go do wykazu – organy państwowe miały na to czas do 9 listopada 2018 r. Od tego dnia przedsiębiorstwo ma zaledwie trzy miesiące na wdrożenie rozwiązań, które będą umożliwiać dokonywanie szacunku ryzyka dla usług kluczowych. Musi też być w stanie sprawnie zarządzać, zgłaszać i usuwać wszystkie incydenty związane z bezpieczeństwem, posiadać osobę odpowiedzialną na cyberbezpieczeństwo i prowadzić aktywne działania edukacyjne wobec użytkowników. Tymczasem problemem wielu organizacji jest choćby interpretacja przepisów ustawy o krajowym systemie cyberbezpieczeństwa. Może dojść do sytuacji, w której podmioty nierozumiejące wymagań zaniżą wagę incydentu, nie zgłaszając go do odpowiednich urzędów. Dlatego ważne jest, aby instytucje państwowe zaczęły tworzyć mocne więzi z firmami, które będą wspierać działania zabezpieczające oraz rozwijać know-how w dziedzinie bezpieczeństwa. Nawet ważniejsze niż aspekty techniczne jest to, aby organy państwowe budowały oparte na zaufaniu relacje z biznesem, dzięki którym ten sektor nie będzie obawiał się komunikacji w sprawie incydentów. Strach i chaos są dla nas największym wrogiem, na którego musimy się przygotować.

Na tym nie koniec obowiązków. Ustawa daje podmiotom sześć miesięcy na wdrożenie adekwatnych do oszacowanego ryzyka środków technicznych i organizacyjnych pozwalających zbierać dane o zagrożeniach i podatnościach. Organizacja musi też już stosować środki, które będą zapobiegać incydentom i minimalizować skutki potencjalnego nadużycia systemów. Po dwunastu miesiącach od otrzymania decyzji, podmiot musi przygotować i przekazać pierwszy kompletny audyt.

Posypią się kary?

Obowiązków jest sporo, a proces ich wdrożenia trudny, wysoce niestandardowy, wymagający specjalistycznej wiedzy i doświadczenia. Tymczasem kary finansowe za niedopełnienie obowiązków wynikających z ustawy wynoszą od tysiąca do nawet miliona złotych! 200 tys. zł zapłacą firmy, które nie przeprowadziły audytu lub nie wykonały zaleceń pokontrolnych w wyznaczonym terminie. 150 tys. zł – gdy OUK nie będzie systematycznie przeprowadzał zarządzania ryzykiem wystąpienia incydentu i szacowania takiego ryzyka. 100 tys. zł grozi w momencie niewdrożenia środków technicznych i organizacyjnych uwzględniających wymagania ustawy. Karami finansowymi objęte są również osoby zajmujące kierownicze stanowiska, które nie dopełnili swoich obowiązków – do 200 proc. miesięcznego wynagrodzenia. Minimalna kara finansowa wynosi tysiąc złotych. Maksymalna – 1 milion złotych! Taka sankcja grozi w przypadku stwierdzenia uporczywego naruszania przepisów ustawy. Czy podmioty zdążą w czasie wyznaczonym przez ustawodawcę i unikną słonych sankcji finansowych? Ustawa to pierwszy krok do zwiększenia poziomu bezpieczeństwa całego kraju. Choć potrzeba ochrony cyberprzestrzeni jest krytyczna, trzeba pamiętać, że do tej pory Polska nie podejmowała znacznych inwestycji w zarządzanie cyberbezpieczeństwem. Dlatego w mojej opinii większość organizacji nie będzie w stanie wykonać nałożonych zadań w terminie wyznaczonym przez ustawodawcę i będzie mierzyć się z ryzykiem wysokich kar finansowych. Trzymam kciuki za realizację tego jakże potrzebnego projektu, jednak apeluję do organów rządowych o praktyczność i zdrowy rozsądek. Jeśli chcemy czegoś od firm oczekiwać, to musimy je najpierw odpowiednio wyedukować oraz wspierać.



Jak działa STIR?

Śledzenie operacji na koncie, możliwość blokady każdego rachunku na 72 godziny – wokół STIR, czyli nowego narzędzia administracji skarbowej pojawia się wiele pytań i kontrowersji. Czym jest to narzędzie i czy rzeczywiście przedsiębiorcy mogą mieć powody do obaw.

Czym jest STIR?

STIR to System Teleinformatyczny Izby Rozliczeniowej. Wykorzystuje niejawne algorytmy do analizy danych pochodzących m.in. z JPK_VAT, CEIDG, KRS oraz danych o zakładanych rachunkach bankowych. Banki oraz SKOKi są zobowiązane dostarczać izbie rozliczeniowej informacje o nowo otwieranych oraz prowadzonych dla podmiotów kwalifikowanych rachunkach bankowych. STIR ma z założenia być jednym z elementów składających się na większy program uszczelnienia systemu podatkowego w Polsce. (…)

Czy jest się czego bać?

Szef Krajowej Administracji Skarbowej (KAS) jest upoważniony do zarządzenia blokady rachunku na czas nie dłuższy niż 72 godziny. Dzieje się tak, jeśli dane wskazują, że podmiot kwalifikowany może wykorzystywać banki lub SKOK-i do wyłudzeń skarbowych lub do czynności, które mogą do nich bezpośrednio prowadzić. Na takie postanowienie nie przysługuje zażalenie. Ponadto szef KAS może przedłużyć czas blokady rachunku do 3 miesięcy w przypadku uzasadnionej obawy, że podmiot nie wykona zobowiązania podatkowego przekraczającego równowartość 10 tys. euro. W tym wypadku podmiot już będzie mógł złożyć zażalenie. – Jeśli nie będzie można zaskarżyć działania szefa KAS, to wówczas będzie on mógł dowolnie blokować rachunki bankowe przedsiębiorców, dla których został wyliczony podwyższony wskaźnik ryzyka – zauważa Piotr Ciszewski, ekspert ds. podatków w firmie inFakt, oferującej nowoczesne rozwiązania księgowe.

Precyzja

Warto również podkreślić, że algorytmy stosowane przez STIR są niejawne. – Obecnie system monitoruje ponad 5,6 mln rachunków podmiotów kwalifikowanych. Na podstawie tych danych system „uczy się" działania i być może jego pierwsze analizy nie będą do końca trafione. Z danych na październik wynika, że w wyniku działania STIR dokonano blokady 20 rachunków bankowych, w tym 17 na więcej niż 72 godziny. W wyniku blokady zabezpieczono około 6 mln zł, co pokazuje skalę działania danego mechanizmu – wyjaśnia Piotr Ciszewski. – Pamiętajmy jednak, że STIR działa w oparciu o uczenie maszynowe, więc w miarę funkcjonowania i uzupełniania go coraz większą ilością danych powinien być coraz bardziej precyzyjny.

Do tej pory, zgodnie z informacją Ministerstwa Finansów, STIR wskazał około 26 tysięcy podmiotów wysokiego i podwyższonego ryzyka wykorzystania sektora finansowego do wyłudzeń skarbowych.