Cyberatak może dotknąć każdego

Wiele mówi się o potrzebie edukacji i krzewienia wiedzy na temat bezpieczeństwa w internecie. To oczywiście niezwykle ważne, ale w praktyce stopień skomplikowania usług cyfrowych oraz fakt, że przenikają one niemal wszystkie sfery życia, sprawia, że właściwe zarządzanie bezpieczeństwem wymaga kompetencji przekraczających możliwości przeciętnego indywidualnego użytkownika. Wobec tego obowiązek zapewnienia bezpieczeństwa spoczywa na biznesie, czyli firmach świadczących usługi oraz na instytucjach państwowych. I tu leży prawdziwe wyzwanie, związane ze zdobywaniem wiedzy i kompetencji.

Urszula **Rybicka**

ekspert instytutu badawczego NASK

W tym celu w ubiegłym roku utworzono Narodowe Centrum Cyberbezpieczeństwa (NC Cyber), ulokowane w instytucie badawczym NASK. W sytuacji zagrożenia NC Cyber może też stanowić zaplecze eksperckie dla narażonych podmiotów. -Trwa wyścig między przestępcami a specjalistami ds. bezpieczeństwa. Wyścig o to, kto pierwszy zdobędzie informację pozwalającą dokonać przestępstwa lub mu zapobiec - mówi Wojciech Kamieniecki, dyrektor instytutu badawczego NASK, zajmującego się od ponad 20 lat problematyką bezpieczeństwa teleinformatycznego. - Naszą rolą, jako instytutu badawczego i jednocześnie gospodarza NC Cyber, jest inicjowanie i promowanie współpracy i wymiany informacji, a także analiza nowych źródeł ryzyka i wypracowywanie środków zaradczych. Tylko informowanie się o zagrożeniach i wzajemne ostrzeganie w połączeniu z eksperckim zapleczem dają szansę na ochronę polskich firm, instytucji i zwykłych internautów przed naprawdę poważnymi problemami.

Kluczowe narzędzia

Organizacje działające w branży IT od dawna mają świadomość, że wiedza, informacja, jest kluczowym narzędziem poprawy bezpieczeństwa. Wiele firm, dla których bezpieczeństwo teleinformatyczne jest elementem kluczowym (np. banki lub operatorzy telekomunikacyjni) mają własne jednostki tzw. threat intelligence (ang. wywiad ds. zagrożeń). Takie zespoły ma też policja, wojsko, instytucje państwowe oraz oczywiście firmy, które specjalizują się w cyberbezpieczeństwie, np. oferują oprogramowanie antywirusowe. Jednostki te analizują wszystkie zarejestrowane próby nielegalnych operacji, badają nowo odkryte rodzaje malware'u, analizują sposoby jego dystrybucji i prognozują możliwe trendy i scenariusze rozwoju sytuacji. Ogólnie rzecz biorąc, starają się jak najwcześniej wykryć pojawiające się nowe zagrożenia i opracować środki zapobiegawcze. Im więcej mają danych, tym szybciej i skuteczniej mogą reagować.

Niezbędna jest współpraca

Jasne jest, że nikt nie pozyska kompletnych danych o zagrożeniach w globalnej sieci w pojedynkę. Niezbędna jest współpraca między firmami, instytucjami publicznymi, organami ścigania i środowiskiem naukowo-eksperckim. Tylko wymiana informacji i wzajemne ostrzeganie się, najlepiej na skalę globalną, przybliży nas do zapewnienia bezpieczeństwa na optymalnym poziomie. Rozumie to Unia Europejska, która w 2016 r. wydała dyrektywę o nazwie NIS (w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych). W myśl jej zapisów pod szczególną ochroną znajdą się przedsiębiorstwa z kluczowych sektorów gospodarki (ochrona zdrowia, finanse, energetyka, transport i telekomunikacja) oraz urzędy państwowe. Dyrektywa nakłada na państwa członkowskie obowiązek utworzenia centrów koordynacyjnych, które będą zbierały informacje o zaistniałych problemach, monitorowały poziom zagrożenia i w razie potrzeby ostrzegały zainteresowanych.

Konieczność raportowania

Dyrektywa NIS nakłada też na firmy z kluczowych branż obowiązek raportowania krajowemu punktowi kontaktowemu incydentów zakłócających bezpieczeństwo. Krajowe centra będą się następnie dzielić tą wiedzą z partnerami z innych państw członkowskich. Na pełne wdrożenie tych przepisów mamy dwa lata. Do tego czasu będziemy musieli przełamać barierę nieufności i lęku. Albowiem dziś wiele instytucji obawia się ujawnienia informacji, że padły ofiarą hakerów. Rzeczywiście upublicznienie takiej informacji może niekorzystnie wpłynąć na reputację. Niemniej, przy aktualnej skali zagrożeń w internecie, bez wymiany informacji wysiłki zmierzające do zapewnienia bezpieczeństwa publicznego będą skazane na niepowodzenie. - Naszą, być może najważniejszą, misją jako Narodowego Centrum Cyberbezpieczeństwa, będzie zapewnienie, aby ta wymiana informacji odbywała się sprawnie, a jednocześnie w sposób poufny i chroniący interesy ofiar ataków - Juliusz Brzostek, dyrektor Narodowego Centrum Cyberbezpieczeństwa w NASK.

Rosnąca świadomość

Już teraz obserwujemy przejawy rosnącego zaufania i świadomości, jak konieczne jest dzielenie się informacjami o zagrożeniach. Działający w NASK od 1996 r. Zespół CERT Polska, który został włączony do NC Cyber, w ubiegłym roku CERT Polska obsłużył 1926 incydentów, o 32 proc. więcej niż w 2015. Wynika to z coraz większej liczby zgłoszeń. Cyberatak może dotknąć każdego. Totalne zabezpieczenie sieci, odgrodzenie jej firewallami i uodpornienie na wszelkie zagrożenia nie jest możliwe w żadnej cywilnej firmie ani instytucji. Nie istnieją całkowicie odporne na atak urządzenia i programy i nie można całkowicie wyeliminować błędów ludzi, posługujących się nimi. - Choć do Polski dotarły wszystkie globalne nowości wykorzystywane przez cyberprzestępców, to jednak w 2016 roku najpowszechniejsze były zagrożenia tradycyjne - oszustwa, wykorzystujące niewiedzę lub nieuwagę internautów – mówi dyrektor Juliusz Brzostek. - Najczęstszym typem incydentu był phishing, stanowiący ponad połowę wszystkich przypadków - dodaje szef NC Cyber. Phishing to metoda wyłudzenia cennych informacji. Najczęściej zbierająca żniwo wśród klientów bankowości elektronicznej. Przestępcy rozsyłają maile łudząco przypominające bankową korespondencję, prosząc o potwierdzenie loginu i hasła. Banki prowadzą kampanie informacyjne, jednak wciąż wiele osób pada ofiarą tego typu przestępstwa. Coraz więcej jest też niebezpiecznych aplikacji na smartfony.

Jedyne, co można zrobić, to identyfikować nowe zagrożenia i ostrzegać przed nimi, zanim ucierpi więcej osób. A będzie to możliwe dopiero wtedy, kiedy nauczymy się współpracy i wymiany informacji. Tylko informowanie się o zagrożeniach i wzajemne ostrzeganie w połączeniu z eksperckim zapleczem dają szansę na ochronę polskich firm i instytucji przed naprawdę poważnymi problemami.

BIZNES RAPORT

GAZETA FINANSOWA
12 – 18 maja 2017 r.

SECURITY AS A SERVICE, CZYLI BEZPIECZEŃSTWO W PAKIECIE

Cięcie kosztów przestało być głównym powodem sięgania po outsourcing. Niezależnie od kondycji finansowej firm nadal wiele innych aspektów, takich jak jakość usług czy wydajność procesów, skłania je do wyboru tego modelu biznesowego. Dodatkowo pojawił się inny problem: niedobór specjalistów na rynku pracy, który w dobie rosnącej cyberprzestępczości grozi poważnymi konsekwencjami.

Robert **Mikołajski**

ekspert Atmana

Zdaniem 80 proc. badanych przez Uniwersytet Duke'a i Międzynarodowe Stowarzyszenie Profesjonalistów Outsourcingu (IAOP) główną korzyścią wynikającą z outsourcingu bynajmniej nie jest optymalizacja kosztów, ale poprawa wydajności operacji biznesowych. O co chodzi? Ankietowani zwrócili uwagę m.in. na możliwość szybszej realizacji założonej strategii, poprawę jakości produktów czy usług, ale także dostęp do wykwalifikowanych specjalistów. Ta ostatnia kwestia wskazana przez uczestników badania ma szczególne znaczenie w obliczu niedoboru talentów z branży IT. Komisja Europejska szacuje, że do 2020 r. na specjalistów IT będzie czekało już ponad 750 tys. wakatów. Szczególnie dotkliwy może być brak ekspertów ds. cyberbezpieczeństwa, bo firmy nie dość, że borykają się z rosnącą skalą cyberzagrożeń, to jeszcze stoją przed wyzwaniami związanymi z cyfrową transformacją biznesu. Jej sukces w dużej mierze zależał będzie od kompetencji i doświadczenia zespołu. Nic więc dziwnego, że jak wynika z danych firmy analitycznej IDC, do końca 2017 roku ponad 70 proc. przedsiębiorstw spośród 500 największych organizacji będzie chciało zatrudnić zespoły wyspecjalizowane w cyfrowej transformacji i innowacjach, a do 2018 r. wzrost zatrudnienia w działach programistycznych ma wzrosnąć dwu- lub trzykrotnie. Czy te przewidywania się sprawdzą, czas pokaże, analitycy IDC mówią jednak wprost: z jednej strony firmy będą budować odpowiednie zespoły wewnętrzne, ale z drugiej – będą musiały nauczyć się współpracy i korzystania z zewnętrznych zasobów programistycznych. Outsourcing coraz częściej staje się polisą bezpieczeństwa w czasach deficytu specjalistów.

Daleko od Bahrajnu

Azjatyckie Królestwo Bahrajnu to jeden z nielicznych przykładów właściwego podejścia do kwestii kształcenia ekspertów IT i współpracy nauki z biznesem. W kraju funkcjonują liczne centra szkoleniowe, w których programy nauczania są na bieżąco aktualizowane zgodnie z sygnalizowanymi przez przedsiębiorstwa potrzebami. Dzięki temu państwo o 1,3-milionowej populacji może pochwalić się 12 000 wykwalifikowanych specjalistów ICT. Co więcej, ich liczba będzie systematycznie rosnąć. Bahrajn to doskonały, lecz niestety, odosobniony przykład kraju, który nie ma problemów z niedoborem talentów z branży informatycznej. Od Bahrajnu jesteśmy daleko nie tylko geograficznie, ale także pod względem dostępności specjalistów IT. Zapewne wiele osób pamięta problem z obsadzeniem stanowiska wiceministra cyfryzacji odpowiedzialnego za cyberbezpieczeństwo. Nic w tym dziwnego, skoro polski rynek mógłby „wchłonąć" od zaraz kilkanaście tysięcy takich specjalistów, a zdaniem analityków z Biura Bezpieczeństwa Narodowego to i tak ostrożne szacunki.

Niedobór ekspertów IT, w tym specjalistów ds. cyberzagrożeń, nie jest jedynie polskim problemem. Firma Vanson Bourne postanowiła zbadać to zjawisko w szerszym ujęciu, zwracając się do menadżerów IT z całego świata, w tym USA, Wielkiej Brytanii, Niemiec, Francji, Japonii i Australii, z pytaniem dotyczącym braków kadrowych. Wyniki? 82 proc. respondentów przyznało, że w ich organizacjach brakuje niezbędnych umiejętności w zakresie walki z cyberprzestępczością. Co ciekawe, aż 76 proc. stwierdziło, że rządy ich państw nie robią nic w kierunku poprawy tej sytuacji, choćby poprzez modyfikację systemów edukacyjnych.

Dział IT czy firma IT?

Choć według danych GUS liczba absolwentów kierunków informatycznych spada, to każdego roku na polski rynek pracy trafia nadal po kilkanaście tysięcy świeżo wykształconych specjalistów IT. To jednak zdecydowanie za mało. Deficyt wynika jednak nie tylko z liczby absolwentów kończących kierunki informatyczne. Specjaliści wolą pracować w firmie o typowym informatycznym DNA niż w nawet renomowanym przedsiębiorstwie, w którym IT pełni jedynie funkcje wspomagającą. Powód? Przede wszystkim możliwości rozwoju i nabywania kompetencji – w firmach IT czekają na nich zadania trudniejsze, ale też pozwalające nabyć cennego doświadczenia. Poza tym takie doświadczenie zdobywane „u źródeł" jest bardziej cenione przez ewentualnych przyszłych pracodawców. W przypadku wewnętrznych działów IT droga rozwoju kariery jest często bardzo ograniczona. Brak ekspertów ds. cyberzagrożeń to jeden z istotniejszych czynników skłaniających przedsiębiorstwa do poszukiwania wsparcia na zewnątrz, ale nie jedyny. Do ważnych argumentów przemawiających za outsourcingiem należy dodać jeszcze możliwość skupienia się na swoim biznesie, bez potrzeby stałego nadzorowania infrastruktury, tworzenia mechanizmów kontroli czy śledzenia trendów z zakresu cyberbezpieczeństwa, gdy z roku na rok rośnie liczba incydentów, a cyberprzestępcy stosują coraz bardziej wyrafinowane metody i narzędzia.

Nie mamy płaszcza

Zrealizowane niedawno przez należącą do IBM firmę Resillent badanie pokazało, że 66% globalnych firm jest nieprzygotowanych, by umieć „podnieść się" po cyberataku. Ponad połowa badanych przyznała, że co najmniej raz padła ofiarą incydentu wymierzonego w minimum 1000 cyfrowych rekordów zawierających m.in. dane personalne, więc ryzyko jest rzeczywiste i naprawdę duże. Co ciekawe, 70 proc. ankietowanych stwierdziło, że walka z cyberprzestępczością zabiera im tyle samo bądź więcej czasu niż przed rokiem, przez co nierzadko zdarza się, że menadżerowie zamiast angażować się pełni w realizację planów strategicznych, muszą skupiać się na zupełnie innych kwestiach. W rezultacie zwykle cierpi na tym biznes. Outsourcing ma tutaj zasadniczą przewagę. Dział wewnętrzny w skrajnych przypadkach powie: „nie mamy pańskiego płaszcza i co pan nam zrobi", co wcale nie musi wynikać ze złych intencji, tylko z niedofinansowania i ograniczonych kwalifikacji działu IT, który jest tylko jednostką wspierającą core business. W przypadku korzystania z usług zewnętrznych, narzucamy dostawcy pewne standardy jakości zabezpieczone karami umownymi, a w skrajnym przypadku możemy wypowiedzieć umowę i zmienić wykonawcę. To znacznie bezpieczniejsze rozwiązanie.

Pozostaje jeszcze temat kosztów. Zdaniem autorów raportu badane firmy byłyby w stanie oszczędzić w budżecie nawet 400 tys. dolarów, gdyby prawidłowo zareagowały na cyberatak. Oczywiście bezpieczeństwo nie wiąże się jedynie z ich odpieraniem. Tutaj pojawia się jeszcze kwestia ciągłości funkcjonowania biznesu i zagrożenia natury techniczno-środowiskowej. Awarii czy to zasilania, czy dostępu do Internetu nie sposób przewidzieć, a zwykle oznaczają one konieczność wstrzymania działania firmy nawet na kilka dni. To oznacza straty, które w Polsce według Veeam Software wynoszą nawet kilkanaście milionów dolarów. Dzieje się tak m.in. dlatego, że firmy mają zwykle złudne poczucie kontroli nad wszystkimi procesami. Obecnie ich złożoność jest tak duża, że szczególnie w przypadku przedsiębiorstw MSP, brakuje zarówno zespołów, jak i regulacji pozwalających nad nimi zapanować i stworzyć skuteczny plan działania w przypadku awarii. Trudno znaleźć decyzyjną osobę z działu IT, która natychmiast odpowie, jak często prowadzić rozruchy agregatów prądotwórczych, jak i gdzie robione są backupy danych sprzedażowych, a także, czy firewall zabezpieczający wewnętrzną sieć firmy ma aktualny firmware.

Czas na SECaaS

Zdaniem analityków IT wraz z popularyzacją rozwiązań dostarczanych jako usługi i wzrostem zainteresowania firm outsourcingiem bezpieczeństwa, coraz częściej sięgać będą one po kolejny segment rozwiązań w modelu XaaS: Security as a Service (SECaaS). Z analizy firmy Markets and Markets wynika, że globalny rynek rozwiązań z zakresu bezpieczeństwa przedsiębiorstw, dostarczanych w modelu usługowym, do 2020 roku wzrośnie do wartości ponad 8,5 miliarda dolarów z 3,12 mld w 2015 roku, a jego roczne tempo wzrostu przekroczy 22 proc. Podstawowa działalność sprzedażowa firmy jest zawsze jej oczkiem w głowie. We własnej firmie obszary wspierające biznes są często zaniedbywane, traktowane po macoszemu. Natomiast te same obszary, które dla nas są wspierające, dla innej firmy są podstawowym źródłem przychodu, a więc podlegają ciągłej optymalizacji, poprawianiu i rozwijaniu. To tłumaczy popyt na usługi bezpieczeństwa.

GAZETA FINANSOWA
12 – 18 maja 2017 r.

BIZNES RAPORT

Alternatywne rozwiązania IT zwiększą bezpieczeństwo

Posiadanie systemu informatycznego w przedsiębiorstwie jest niezbędne do jego poprawnego funkcjonowania. Dlatego też zapewnienie bezpieczeństwa firmowej sieci powinno być absolutnym priorytetem. Poniżej prezentujemy alternatywne rozwiązania IT, których wprowadzenie podniesie poziom zabezpieczeń w organizacji.

Łukasz **Laskowski**

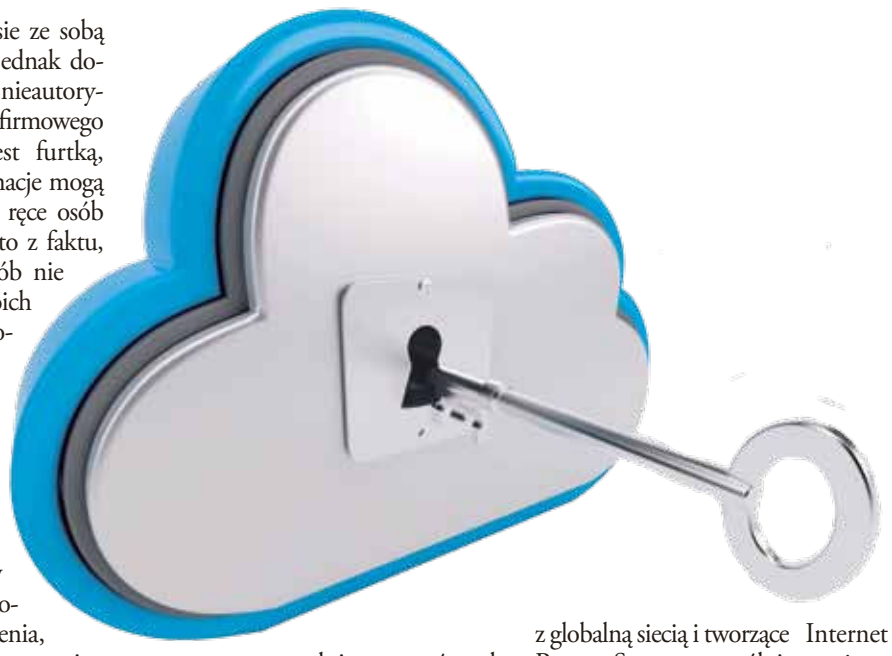
prezes zarządu Ediko

Bezpieczeństwo informatyczne przedsiębiorstwa przestaje być tylko jednym z aspektów pracy działu IT, a staje się kwestią kluczową, bez której nie ma mowy o poprawnym funkcjonowaniu firmy. Potwierdzają to badania PwC, przeprowadzone na przestrzeni ostatnich lat, według których wydatki polskich przedsiębiorstw na cyberbezpieczeństwo z roku na rok systematycznie rosną. W 2013 r. było to zaledwie 2,7 proc. budżetu IT, natomiast w 2016 wartość ta wyniosła już 10 proc. Jest to odpowiedź na rosnącą liczbę ataków na infrastrukturę komputerową firm, których w 2016 r. było w Polsce o 46 proc. więcej niż w poprzednim roku. Przez ataki hakerskie, z którymi związana była m.in. utrata klientów, danych, bądź przestój w działaniu, 4 proc. zaatakowanych przedsiębiorstw odnotowało straty w wysokości powyżej miliona złotych.

Bring Your Own Device – tu potrzebna jest kontrola!

Przekazywanie pracownikom dostępu do firmowej sieci z poziomu ich prywatnych urządzeń, czyli rozwiązanie o nazwie Bring Your Own Device (BYOD), jest już zjawiskiem powszechnym. Takie działanie pozwala zaoszczędzić pieniądze niezbędne do kupienia odpowiedniego sprzętu, a także czas, ponieważ dzięki ciągłemu dostępowi do firmowych danych pracownik może elastycznie reagować na potrzeby firmy. Z raportu „Nowoczesne IT dla MŚP" opublikowanego przez Ipsos Mori w 2015 r. wynika, że w niemal połowie (46 proc.) małych i średnich przedsiębiorstw w Polsce pracownicy korzystają z własnych urządzeń. Używają ich oni przede wszystkim do dostępu do służbowej skrzynki e-mail, edytują na nich firmowe dokumenty oraz korzystają z potrzebnych do pracy aplikacji.

Lista zagrożeń, jakie niesie ze sobą rozwiązanie BYOD jest jednak dosyć długa. Wpuszczenie nieautoryzowanego urządzenia do firmowego obiegu dokumentów jest furtką, przez którą istotne informacje mogą w łatwy sposób trafić w ręce osób niepożądanych. Wynika to z faktu, że znaczna większość osób nie dba o bezpieczeństwo swoich prywatnych urządzeń mobilnych lub komputerów. Jeżeli chodzi o smartphone'y, to najnowsze badania przeprowadzone przez Consumer Reports w Stanach Zjednoczonych pokazały, że aż 64 proc. użytkowników nie używa PIN-u do odblokowania swojego urządzenia, tylko 14 proc. ma oprogramowanie antywirusowe, a raptem 8 proc. posiada narzędzia do usuwania danych ze swoich telefonów.



Alternatywą dla BYOD jest standard zwany POCE (Personally Owned, Company Enabled) który zakłada, że prywatne urządzenie zostanie włączone w sieć wewnętrzną firmy. Główną różnicą Pomiędzy BYOD a POCE są nałożone w tym drugim ograniczenia, które kontrolują, do jakich danych, aplikacji i urządzeń prywatny sprzęt będzie miał dostęp, a także wprowadzają na nim system zabezpieczeń i weryfikacji, aby w pełni panować nad przepływem informacji. Wybór tego rozwiązania nie wygeneruje tylu kosztów, co np. zapewnienie wszystkim pracownikom nowego, służbowego sprzętu, a z pewnością podniesie poziom bezpieczeństwa wrażliwych, firmowych danych.

Chmura a Internet of Things

Zabezpieczenie urządzeń użytkowników końcowych jest istotne, jednak coraz więcej analiz zwraca uwagę na konieczność zabezpieczenia innego aspektu firmowego IT. Chodzi o przedmioty samoistnie łączące się z globalną siecią i tworzące Internet Rzeczy. Są one szczególnie narażone na ataki, ponieważ, jeżeli korzystają z cloud computingu, mogą stanowić spore ułatwienie przy próbie włamania się do sieci firmy. Ze świata napływają informacje o udanych próbach ataku na takie urządzenia jak lodówka, inteligenta toaleta, czy nawet żarówka, która dzięki połączeniu z Internetem mogła być obsługiwana z poziomu smartphone'a.

Rozwiązaniem zwiększającym poziom bezpieczeństwa jest wybór tych urządzeń IoT, które działają np. w oparciu tylko o firmową sieć LAN. Pozwalają one zminimalizo-

Testy penetracyjne, etyczny hacking i informatyka śledcza to nie science fiction, a konieczność we współczesnym biznesie

Obecnie odpowiedzialny za Rapid Detection Center oraz rozwijanie produktów związanych z wykrywaniem ataków i podatności w firmie F-Secure. Posiada wieloletnie doświadczenie w przeprowadzaniu testów penetracyjnych oraz analiz powłamaniowych, głównie dla europejskiego sektora finansowego. Entuzjasta zastosowań sztucznej inteligencji w wykrywaniu cyberataków. Absolwent Informatyki, Ekonomii oraz MBA.

Leszek **Tasiemski**

lider specjalnej jednostki RDC w firmie F-Secure (VP, Rapid Detection Center, R&D Radar & RDS w firmie F-Secure)

Każda minuta pracy pentesterów jest na wagę złota, bo potencjalne ataki mogą narazić firmy nie tylko na ogromne straty pieniędzy, ale także na utratę reputacji. W grę wchodzą kluczowe elementy funkcjonowania biznesu takie jak bazy danych projektów inżynierskich, numery kart kredytowych czy konta klientów, oczywiście zdarzają się także kary umowne czy konsekwencje pozwów. Kontrolowane ataki opierają się na serii testów zaprojektowanych, by wykazać, co dana firma robi dobrze, a co źle w zakresie bezpieczeństwa. Działania sprawdzają, czy przedsiębiorstwo odpowiednio wykrywa i odpowiada na symulowane ataki.

Praca pentestera od kuchni

Szczegóły codziennej pracy pentesterów przywodzą na myśl scenariusz filmu sensacyjnego. Szukanie wydruków maili w śmietnikach, podrzucanie zainfekowanego pendrive'a na parkingu firmowym czy próby zdobycia haseł do sieci bezprzewodowej od recepcjonistki, podając się za nowego pracownika to tylko kilka przykładów działalności jednostek F-Secure zajmujących się pentestami. Spora część pracy opiera się także na działaniach badawczo-rozwojowych i tworzeniu narzędzi pozwalających analizować (audyt), zapobiegać (prewencja) oraz zwalczać cyberzagrożenia.

Czasami gramy policjantów, czasami złodziei – zawsze po dobrej stronie. Kiedy gramy złodziei, to wcielamy się w rolę hakerów na zlecenie naszych klientów. Próbujemy zdalnie włamać się do systemu, a wielokrotnie nawet fizycznie dostać się do budynku – to wszystko w celu wykazania braków w zabezpieczeniach. Następnie prezentujemy raport z tego, co udało nam się osiągnąć i wraz z klientem pracujemy nad poprawieniem poziomu ochrony. Kiedy gramy policjantów, to ścigamy hakerów. Gdy u naszego klienta wydarzy się incydent, staramy się dociec, w jaki sposób atakujący dostali się do systemu, co zrobili i od jak dawna mają dostęp. W niektórych przypadkach udaje się wytropić cyberprzestępców i postawić ich przed sądem.

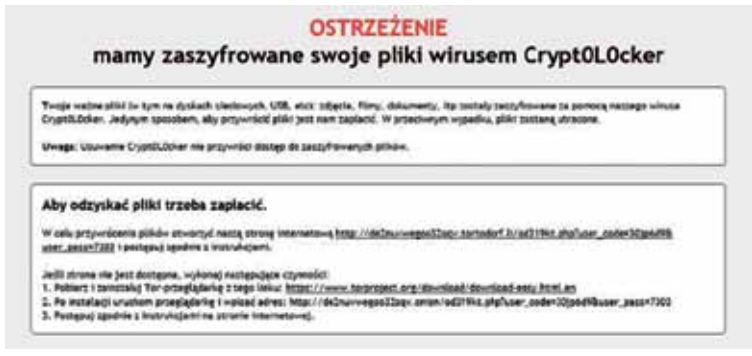
Cyberataki na firmy

Rozwój technologii jest tak szybki, że kwestia bezpieczeństwa za nim nie nadąża, a największymi beneficjentami pędzącego rozwoju są cyberprzestępcy. Wystarczy jedno źle skonfigurowane urządzenie, by uzyskać dostęp do firmy.

Mimo medialnej widowiskowości najgroźniejsze ataki na systemy finansowe i szpiegostwo przemysłowe są stosunkowo rzadkie. Z praktycznego punktu widzenia, najpowszechniejsze i bardzo niebezpieczne są ataki typu ransomware. Takie oprogramowanie szyfruje pliki i żąda okupu (w walucie Bitcoin) za ich odszyfrowanie. Ofiarami takich ataków padają zarówno indywidualni użytkownicy, jak również firmy. Niedawno zidentyfikowaliśmy przypadek firmy, w której oprogramowanie ransomware „rozlało się" po sieci i zaszyfrowało setki stacji roboczych (zaatakowane zostały również kopie zapasowe). Straty wynikające z zablokowania dostępu do istotnych firmowych danych były szacowane na setki tysięcy Euro dziennie.

Socjotechnika podstawową bronią hakera

Cyberprzestępcy coraz częściej skupiają się na firmach, które pokładają zbyt duże nadzieje w zautomatyzowanych rozwiązaniach chroniących ich sieci. Hakerzy ciągle doskonalą umiejętności socjotechniczne, aby przechytrzyć osoby zatrudnione w firmach. Zapewnianie pracowników o tym, że są bezpieczni, jest działaniem na niekorzyść, bo może prowadzić do uśpie-



BIZNES RAPORT
GAZETA FINANSOWA
12 – 18 maja 2017 r.

przedsiębiorstwa

wać ryzyko wycieku oraz włamania przez komunikację i przetwarzanie danych tylko w obrębie zabezpieczonej struktury informatycznej firmy. W tym momencie technologia ta cieszy się szczególnym zainteresowaniem. Rozwiązania IoT tego typu znajdują już zastosowanie przede wszystkim w monitoringu, kontroli i gromadzeniu oraz analizie danych z ważnego dla firm zakresu Big Data. Zainteresowane są nimi różne branże, takie jak transport i handel, ale także i przemysł, nazywany często Industry 4.0. Taki Internet Rzeczy sprawdza się także we wspomaganiu i optymalizacji procesów biurowych, m.in. monitorując pracę firmowych drukarek.

Bezpieczeństwo na zlecenie

Według najnowszego raportu „HP dla Biznesu. Bezpieczeństwo. Ryzyko. Dostępność" aż 70 proc. polskich przedsiębiorstw zapewnia, że bezpieczeństwo ma dla nich najwyższy priorytet, jeżeli chodzi o strefę IT. Jednocześnie w więcej niż co trzeciej firmie, odpowiedzialność za bezpieczeństwo w tej kwestii jest rozproszona po różnych działach, co znacznie osłabia skuteczność działania. W prawie połowie firm dbanie o bezpieczeństwo jest po prostu jednym z obowiązków działu IT, natomiast tylko 11 proc. posiada do tego oddzielną komórkę. Dodatkowo, 54 proc. nie przeprowadza regularnych kontroli bezpieczeństwa swojej sieci wewnętrznej.

Sposobem, który pozwala nawet mniejszym firmom zabezpieczyć się przed cyberatakami, jest outsourcing zarządzania bezpieczeństwem danych. Oznacza to zlecenie audytu oraz ochrony firmowej struktury informatycznej specjalnemu przedsiębiorstwu. – W tym momencie na działania outsourcingowe w kwestii bezpieczeństwa zdecydowało się około 9 proc. polskich firm. Takie rozwiązanie to szansa, szczególnie dla tych firm z sektora MSP, dla których działania informatyczne są kluczowe dla funkcjonowania, ale ze względu na wysoki koszt utrzymania, nie mogą sobie pozwolić na samodzielne zapewnienie bezpieczeństwa – mówi Alan Pajek, ekspert w temacie bezpieczeństwa danych w przedsiębiorstwach.

Ze względu na rosnące zagrożenia związane z cyberatakami, firmy muszą nieustannie ulepszać swoje systemy zabezpieczeń oraz nie dopuszczać do powstawania luk, przez które do ich sieci miałyby dostęp osoby niepożądane. Trzeba jednak pamiętać, że przedsiębiorstwo odpowiednią ochronę zyska dopiero wtedy, kiedy wraz z technologią o bezpieczeństwo będą dbać także odpowiednio wyedukowani pracownicy. Czasami bowiem najlepszym zabezpieczeniem jest ludzki, zdrowy rozsądek.

nia ich czujności, a na to właśnie liczą hakerzy. Technologia nie zawsze jest w stanie ustrzec przed niebezpieczeństwem i powinna raczej pełnić funkcję wspomagającą ochronę.

Przykładem zastosowania socjotechnik w ataku jest phishing, czyli wysyłanie sfałszowanych wiadomości i podszywanie się pod osobę lub instytucję, w celu wyłudzenia określonych informacji. Phishing cieszy się bardzo wysoką skutecznością podczas kontrolowanych ataków, które przeprowadzamy w przedsiębiorstwach. Pracownicy najczęściej nie spodziewają się, że e-mail, który dostają lub witryna, z której powszechnie korzystają, mogą być sfałszowane. Podczas przeprowadzania pentestu jedna z naszych jednostek w F-Secure rozesłała sfałszowany mail udający wiadomość z serwisu LinkedIn, żeby sprawdzić, ilu pracowników kliknie w link podany w mailu. Wynik był zatrważający, bo kliknęło aż 52 proc. osób. W innym eksperymencie grupa stworzyła mail prowadzący do sfałszowanego portalu. W tym przypadku w przekierowujący link kliknęło 26 proc. osób, a 13 proc. osób zalogowało się na sfałszowanej stronie, używając swoich danych logowania.

Istnieją także gotowe platformy, na których można w łatwy sposób stworzyć własną kampanię phishingową, czy „zaprojektować" złośliwe oprogramowanie z gotowych modułów. Rynek złośliwego oprogramowania stał się bardzo zorganizowany, w podziemiu działają wirtualne giełdy, na których przestępcy mogą w łatwy sposób kupować narzędzia. Dostępne są nawet specjalne systemy raportujące przestępcom ile złośliwe oprogramowanie zarobiło dla nich pieniędzy. Dostawcy gotowych komponentów konkurują ze sobą funkcjonalnością, stabilnością, niewykrywalnością, a nawet – oferowanym wsparciem technicznym.

Ryzyko zawodowe

Pentesty najczęściej zaskakują firmy, obnażając, w jak wielkim stopniu są one narażone na ataki. Przekonanie przedsiębiorstw o ich bezpieczeństwie najczęściej zgoła różni się od faktycznego poziomu ochrony i tego, co dostrzegają cyberprzestępcy. Testy wykazują całą powierzchnię ataku, czyli newralgiczne punkty, które mogą stanowić cel hakerów – nie tylko w cyfrowym, ale również w fizycznym wydaniu.

Najczęściej po przeprowadzeniu kontrolowanego ataku prezesi otwierają oczy i zdają sobie sprawę, że ryzyko jest realne. Niektórzy prezesi reagują zaskoczeniem, inni niedowierzaniem, a pewna grupa nie jest zdziwiona, bo poddaje się kontrolowanemu atakowi kolejny raz. Testy penetracyjne warto ponawiać, ponieważ bezpieczeństwo nie jest dane raz na zawsze.

Pięta achillesowa biznesu

Specjaliści zajmujący się cyberbezpieczeństwem przewidują, że ataki hakerskie w 2017 roku spowodują 24-godzinną blokadę Internetu. Może to mieć katastrofalne skutki dla rynków finansowych na całym globie. A jak pokazują wyniki raportu Capgemini „Waluta Zaufania: Dlaczego Banki i Firmy Ubezpieczeniowe muszą lepiej dbać o bezpieczeństwo Danych swoich Klientów" opublikowanego przez Digital Transformation Institute Capgemini (2017), tylko jeden na pięciu dyrektorów (21 proc.) jest wysoce przekonany o możliwościach branży w zakresie wykrywania ewentualnych włamań. Czy mamy się czego obawiać?

Karolina **Wójcik**
junior consultant Linkleaders

Pomimo tego, że instytucje finansowe, a w szczególności banki, wydają zawrotne sumy, by zabezpieczyć swoje systemy, liczba i częstotliwość wycieków danych wciąż rośnie. Co istotne, większość konsumentów (65 proc.) wskazuje bezpieczeństwo systemów mających chronić prywatność danych jako niezwykle ważny czynnik podczas wyboru docelowego banku, wynika z raportu Capgemini. Badania dotyczące bezpieczeństwa wskazują też na duże rozbieżności pomiędzy wysokim poziomem zaufania społeczeństwa wobec banków, a rzeczywistą niezawodnością systemów.

Cyberbezpieczeństwo idzie w parze z zarządzaniem ryzykiem

Mądre zarządzanie ryzykiem do dziś jeden z priorytetów biznesowych każdej organizacji, bez względu na reprezentowaną branżę. Jest to wypadkowa między innymi dynamicznych zmian technologicznych, które mogą narazić przedsiębiorstwa na poważne konsekwencje biznesowe, jeśli te nie będą w stanie za nimi nadążyć. Najnowszy raport CIMA Ensuring corporate viability in an uncertain world – Framing the board conversation on risk zwraca uwagę, ze firmy powinny podnieść temat ryzyka biznesowego do poziomu strategicznego, zwłaszcza w czasach rosnącej złożoności i niepewności na globalnych rynkach. Dla przykładu, wraz z wprowadzeniem w Wielkiej Brytanii nowych wymogów sprawozdawczych związanych z ryzykiem, zarządy firm coraz częściej poszukują sposobów umożliwiających integrację procesów zarządzania ryzykiem, upewniając się, że dywizje odpowiedzialne za finanse i zarządzanie ryzykiem nie działają autonomicznie. Mimo to praktyki z zakresu ERM, czyli koncepcji zintegrowanego zarzadzania ryzykiem, wymagają popularyzacji i ciągłej aktualizacji, wynika z badań CIMA. Ma to szczególne znaczenie nie tylko w dążeniu do osiągnięcia przewagi konkurencyjnej w skali mikro, ale także w zapewnieniu stabilizacji w ujęciu globalnym, gdzie czynniki ryzyka występujące w danym regionie mogą negatywnie wpływać na organizacje jedynie prowadzące tam interesy, a posiadające swoje siedziby w innej części świata. W odpowiedzi na coraz więcej wyzwań przedsiębiorstwa decydują się na wprowadzenie koncepcji ERM, by ulepszyć strategiczną ewaluację zagrożeń wpływających na sukces biznesu. Badania przeprowadzone przez Instytut CIMA wykazują jednak, że zaledwie 1/3 europejskich firm udało się wdrożyć zaawansowany model ERM, nad którym pieczę sprawują komitety audytu lub specjalnie powoływane komitety ryzyka. – Aż 60 proc. organizacji reprezentujących różne branże mierzy się z coraz trudniejszymi wyzwaniami, które w sposób znaczący mogą wpłynąć na strategiczny sukces ich przedsięwzięć. Efektywną implementację modelu identyfikacji zagrożeń spowalniają także inne czynniki. Do najważniejszych przeszkód należy ustalanie priorytetów. 2 na 5 respondentów uważa, że nie posiada odpowiednich zasobów, by zoptymalizować nadzór nad ryzykiem. Raport CIMA pokazuje, że niemal drugie tyle odczuwa konieczność przeznaczenia budżetu na inne, nadrzędne wydatki. Ryzyko jest też jednym z priorytetowych tematów dla branży technologicznej – tłumaczy Jakub Bejnarowicz, Szef CIMA w Europie Środkowo-Wschodniej.

Zmiany monitorujące etyczne zachowania świat finansów przyjmuje z zadowoleniem. Dla przykładu JPMorgan Chase & Co. specjalizujący się w bankowości inwestycyjnej, zaadaptował już w tej chwili program eliminujący wątpliwe etyczne zachowania swoich bankowców. W efekcie ma się zmniejszyć liczba ryzykownych giełdowych zagrań, co będzie powodowane wizją zastąpienia bankierów sprawniejszymi i popełniającymi mniej błędów maszynami.

Ochrona danych na celowniku biznesu

Rozporządzenie o ochronie danych (ang. General Data Protection Regulation, GDPR), regulacja unijna mająca wejść w życie w maju 2018 roku, zmusi wiele organizacji do ujawnienia wycieku danych w ciągu 72 godzin, a w przypadku zaniechania – zapłacenia wysokich kar. Nowe regulacje wpłyną na wszystkie obszary działalności firmy, w których dochodzi do przetwarzania danych. Wymogi będą musiały zostać uwzględnione między innymi w obszarze sprzedaży, obsługi posprzedażowej, wsparcia i backoffice (podczas oceny ryzyka operacyjnego czy audytu wewnętrznych procesów). Choć przestrzeganie zapisów rozporządzenia będzie miało zasadnicze znaczenie i pozostał nieco ponad rok od jego wdrożenia, tylko jedna trzecia badanych wśród kadry kierowniczej banków i firm ubezpieczeniowych (32 proc.), określiła swoją organizację jako taką, która zrobiła duże postępy w realizacji wytycznych projektu. - Wprowadzenie w życie unijnego rozporządzenia jest szansą dla wielu organizacji na zapewnienie bezpieczeństwa swoim klientom. Z raportu Capgemini wynika, że na istotność tego aspektu wskazuje aż 65 proc. konsumentów. Zmieniający się charakter zagrożeń i niejasności wśród liderów z branży może tłumaczyć, dlaczego pomimo wysokiego poziomu inwestycji, około 71 proc. organizacji wciąż nie posiada zrównoważonej strategii bezpieczeństwa ani silnych zasad ochrony prywatności danych – zauważa Piotr Siuda, dyrektor projektów w Capgemini.

Według badań firmy Accenture Operations trzy kluczowe kompetencje współczesnych pracowników to wiedza technologiczna, umiejętność rozwiązywania skomplikowanych problemów oraz gotowość do zmiany. Podobne cechy będą coraz ważniejsze w kontekście cyberbezpieczeństwa i ochrony przed atakami hakerskimi. We wdrożenie zmian w zakresie bezpieczeństwa danych powinni być zaangażowani bowiem przedstawiciele z wielu działów firm, m.in. prawnego, IT, bezpieczeństwa, obsługi klienta, marketingu oraz HR. Zmiany powinny zaczynać się już na etapie odpowiedzialnego podejścia do przekazywanych treści oraz właściwego poziomu wiedzy pracowników. Choć wielu konsumentów instynktownie powierza swoje dane instytucjom finansowym, kiedy ich zaufanie zostanie zachwiane, aż trzy czwarte konsumentów zmieni swojego dostawcę – podaje raport Capgemini.

> **Rozporządzenie o ochronie danych (ang. General Data Protection Regulation, GDPR), regulacja unijna mająca wejść w życie w maju 2018 roku, zmusi wiele organizacji do ujawnienia wycieku danych w ciągu 72 godzin, a w przypadku zaniechania – zapłacenia wysokich kar. Nowe regulacje wpłyną na wszystkie obszary działalności firmy, w których dochodzi do przetwarzania danych.**

GAZETA FINANSOWA
12 – 18 maja 2017 r.

BIZNES RAPORT

Cyberprzestępcy coraz bardziej pomysłowi

Jednym z najpoważniejszych problemów, z jakim borykają się w dzisiejszych czasach przedsiębiorcy, są cyberataki. Z dnia na dzień rośnie ilość publikacji i poradników mówiących o tym, jak skutecznie zabezpieczać się przed atakami w sieci. Rosnąca liczba artykułów na temat ataków hakerskich, które doprowadzają firmy do poważnych strat finansowych i wizerunkowych sprawiają, że przedsiębiorcy poświęcają coraz więcej uwagi kwestiom bezpieczeństwa w sieci, inwestując tym samym w specjalistyczne zabezpieczenia i systemy. Ekspert Loando.pl, Maciej Suwik podpowiada, na jakie rozwiązania przedsiębiorcy z sektora fintech powinni szczególnie zwrócić uwagę, by uchronić swą firmę przed cyberatakiem.

Inwestycja w bezpieczeństwo

Najnowszy raport „Światowe Badanie Bezpieczeństwa Informacji" wskazuje na znaczny wzrost zainteresowania przedsiębiorców tematem cyberbezpieczeństwa oraz sposobami walki z atakami hakerów. Ponad połowa ankietowanych firm deklaruje skuteczność w wykrywaniu nawet bardzo skomplikowanych cyberataków, co jest najwyższym od 2013 roku, wskaźnikiem. Przekonanie to wynika przede wszystkim z inwestycji w wyspecjalizowane zespoły IT, monitorujące zagrożenia w sieci (tzw. SOC – Security Operations Center), ale też w mechanizmy zapobiegające atakom w sieci. Pomimo znacznego polepszenia sytuacji, wciąż spory odsetek firm przyznaje się do korzystania z przestarzałych środków bezpieczeństwa online (48 proc.), natomiast 44 proc. w ogóle nie posiada zespołu SOC. Poważny problem stanowi również poziom wiedzy pracowników w tej kwestii – aż 86 proc. ankietowanych uważa, że ich kompetencje w zakresie cyberbezpieczeństwa nie do końca spełniają potrzeby organizacji, w której pracują. Znaczące są również ograniczenia budżetowe (61 proc.), brak wyspecjalizowanych kadr (56 proc.) oraz brak świadomości lub wsparcia ze strony zarządu (32 proc.).

Serwer dedykowany czy własny?

„Inwestując we własne przedsiębiorstwo, należy również wziąć pod uwagę wydatki związane z bezpieczeństwem w sieci i postawić na rozwiązania, które uchronią firmę nie tylko przed stratami finansowymi, ale też wizerunkowymi. Szczególnie ważne jest to w przypadku instytucji zaufania publicznego, takich jak banki czy firmy pożyczkowe. Cyberprzestępcy coraz częściej – oprócz spamu skrzynki pocztowej – hakują również oficjalne strony internetowe czy kasują całą jej zawartość, co w efekcie może skutkować zaburzeniem komunikacji z klientami. Wpływ na wizerunek firmy mają także wirusy umieszczane na stronie. Klient, wchodząc na stronę danej firmy, otrzymuje komunikat o zagrożeniu, przez co usługodawca traci na wiarygodności, a tym samym – spada liczba potencjalnych klientów. Coraz więcej firm, m.in. start-upy fintechowe, dążą do zwiększenia ochrony danych poprzez wdrażanie zabezpieczeń online. Jednym z nich jest inwestycja w serwer dedykowany" – komentuje

Maciej Suwik, ekspert Loando.pl

Serwer dedykowany to najbezpieczniejsze, ale jednocześnie jedne z najdroższych rozwiązań, dedykowane szczególnie firmom, których klienci wprowadzają swoje dane na oficjalnej stronie internetowej (e-commerce, bankowość internetowa czy pożyczki online). Tego typu rozwiązania oferowane są przez firmy usług SLA, zajmujących się raportowaniem i oceną osiąganych wyników na stronie www. Wykupiony serwer jest dostosowywany do potrzeb administratora strony oraz skonfigurowany z jego działaniami.

Alternatywą dla serwerów dedykowanych są również własne serwerownie, które dają przedsiębiorcy swobodę w zarządzaniu oferowanymi usługami. Choć wymaga ona dużych nakładów finansowych, własna serwerownia gwarantuje wyłączność dostępu do panelu administracyjnego strony tylko upoważnionym osobom. Korzystanie z zewnętrznych usług SLA nie jest już wtedy potrzebne.

Ochrona przed spamem

Jedną z podstawowych form ataków hakerskich jest wspomniane wcześniej, spamowanie skrzynki pocztowej. Każdy z przedsiębiorców odbiera codziennie ogromną ilość wiadomości e-mail, z których znaczna część może stanowić poważne zagrożenie dla firmy. Coraz częściej hakerzy stosują tzw. phishing, czyli metodę pozyskiwania haseł bezpośrednio od użytkowników za pomocą wiadomości e-mail. Treść takiej wiadomości zawiera link odsyłający nas na stronę, która na pierwszy rzut oka wydaje się być zaufaną stroną sklepu internetowego czy witryny bankowej. Informacje wpisane na stronę zostają natychmiastowo wykorzystane przez hakerów. Warto również podkreślić, że znaczna część osób nie zwraca uwagi, bądź nie potrafi poprawnie odróżnić normalnej wiadomości e-mail od tej zawirusowanej. Istnieje natomiast wiele prostych sposobów pomocnych w weryfikacji wiadomości przesyłanych przez hakerów. „Tego typu wiadomości trafiają przede wszystkim do spamu i pochodzą od nieznanego nadawcy. Ich tytuły również mogą zdradzać ich pochodzenie – są bowiem bardzo chwytliwe, mówią o korzystnych ofertach, promocjach czy nagrodach" – wyjaśnia Maciej Suwik, ekspert Loando.pl

> **Inwestując we własne przedsiębiorstwo, należy również wziąć pod uwagę wydatki związane z bezpieczeństwem w sieci i postawić na rozwiązania, które uchronią firmę nie tylko przed stratami finansowymi, ale też wizerunkowymi**

Przedmiotem ataków cyberprzestępców stały się również faktury wysyłane drogą e-mailową, w których hakerzy podszywają się pod dostawcę usług telekomunikacyjnych czy instytucję finansową. Na ataki narażone są szczególnie osoby, które korzystają z innowacji finansowych i decydują się na regulowanie zobowiązań finansowych drogą internetową. Tak jak w przypadku wiadomości e-mail, istnieje kilka sposobów umożliwiających weryfikację i odróżnienie oryginalnej faktury od podrobionej. Jednym z podstawowych zabiegów jest upewnienie się, że w wiadomości znajduje się załącznik „smime.p7s", świadczący o oryginalności faktury. Ponadto wiadomość z e-fakturą, jak i sam dokument powinny być podpisane elektronicznie. Na rynku dostępne są również darmowe programy umożliwiające weryfikację podpisów elektronicznych (np. WebNotarius), które pomogą określić pochodzenie dokumentu.

„Wszystkie z wymienionych rozwiązań podnoszą poziom bezpieczeństwa w sieci. Należy mieć jednak świadomość, iż istnieją oprogramowania, z których korzystania lepiej zrezygnować. Jednym z nich jest Java, której odinstalowanie znacznie zmniejsza powierzchnię potencjalnego ataku hakerskiego. Jest ona bowiem bardzo podatna na ataki oraz wykorzystywanie luk 0-day – podatności, na które nie wymyślono jeszcze odpowiednich rozwiązań gwarantujących bezpieczeństwo w sieci. Według danych statystycznych, 193 na 200 luk znaleźć można właśnie w Javie". – dodaje Maciej Suwik, ekspert Loando.pl