RAPORT

CYBER-BEZPIECZEŃSTWO

CZERWIEC 2018

POD PATRONATEM

WP GAZETA.PL interia onet BUSINESS INSIDER POLSKA

WYDAWCA

interaktywnie.com

SPIS TREŚCI

Zbawienne RODO

Wszędzie słyszę narzekanie na unijne Rozporządzenie o ochronie danych osobowych - tzw. RODO. Że złe, niepotrzebne, przesadzone. Że teraz wszyscy się boją kar i wielu spraw nie można załatwić szybko i sprawnie.

Powiem z przekorą: - no i dobrze! Fakt, faktem - prawo obowiązujące przed wejściem w życie nowych regulacji było bardzo dobre. Mnóstwo spraw regulowała Ustawa o ochronie danych osobowych oraz ta o świadczeniu usług drogą elektroniczną. Czy zdajecie sobie sprawę z tego, że w zasadzie RODO niewiele zmieniło w porządku prawnym i zasadach, co do których trzeba się stosować? Ale wywołało też burzę, która przyczyni się do poprawy bezpieczeństwa danych, finansów, biznesu itp., itd.

Firmy i instytucje zostały w końcu nastraszone, że jeśli się nie przystosują do nowych regulacji, mogą zostać ukarane wielomilionowymi karami. To określenie mocno na wyrost, ale - trzeba przyznać - jest skuteczne. Strach padł na banki, telekomy, firmy ubezpieczeniowe, szpitale i przychodnie, ale też na małe - nawet osiedlowe - biznesy. W końcu wszyscy zdaliśmy sobie sprawę z tego, że w zasadzie nie ma na rynku takiego podmiotu, który nie przetwarza danych osobowych, stanowiących przecież ogromną wartością dla ich właścicieli, w związku z czym muszą one podlegać ochronie. Nie można więc do nich podchodzić frywolnie.

W końcu sklepy internetowe i wydawcy zaczęli więc masowo instalować certyfikaty SSL. Wzrosła sprzedaż podpisów elektronicznych i rozwiązań chmurowych. Przedsiębiorcy przeprowadzili audyty, a w wielu firmach dokumenty przestały się walać po biurkach. To prawdziwy cud nad Wisłą.

Jak dbać o bezpieczeństwo firm i danych. Jakie zagrożenia płyną z sieci - o tym wszystkim przeczytacie w tym raporcie.

A po lekturze zapoznajcie się koniecznie z ofertą firm, które postanowiły zaprezentować się w tym opracowaniu: Autenti, Dagma, LogicalTrust, Optima Partners i zadbajcie o swoje cyberbezpieczeństwo.

Tomasz Bonek,
redaktor naczelny i prezes zarządu Interaktywnie.com

WIZYTÓWKI FIRM

Autenti Sp. z o.o.

Adres
ul. Święty Marcin 29/8
61-806 Poznań

Dane kontaktowe
bok@autenti.com
www.autenti.com
+48 22 29 05 112

Opis działalności
Autenti to platforma do autoryzacji dokumentów i zawierania umów przez internet. Dzięki Autenti podpisywanie dokumentów możliwe jest na komputerze, tablecie lub smartfonie - w dowolnym miejscu i czasie. Platforma to wyjątkowe połączenie podpisu elektronicznego, innowacyjnej technologii oraz przepisów prawa europejskiego. Z usługi korzystać można w relacjach z partnerami biznesowymi, konsumentami, a także pracownikami.

Wybrani klienci
Lens Finance, Work Service, Siemens Finance, Pizza Portal

SecurityInside

Dane kontaktowe
kontakt@securityinside.pl
www.securityinside.pl
+48 71 738 24 35

Opis działalności
Poszukujesz atrakcyjnej i przystępnej edukacji o cyberzagrożeniach dla Ciebie i Twojej Firmy? Sprawdź SecurityInside.pl!

Rabat 15% na hasło „interaktywnie-2018-si”

Wybrani klienci
Getin Bank, Bank Credit Agricole, Mennica Polska, MPWiK Wrocław, PLAY, Kruk

Optima Partners

Adres
ul. P. Gintrowskiego 53
02-697 Warszawa

Dane kontaktowe
biuro@optimapartners.pl
www.securityhub.eu
+48 22 395 51 87

Opis działalności
Świadczymy profesjonalne usługi IT i security – m.in.:
· Testy penetracyjne aplikacji webowych / API / aplikacji mobilnych wg OWASP
· Testy penetracyjne infrastruktury wg OSSTMM
· Testy DoS / DDoS
· Audyt konfiguracji bezpieczeństwa
· Audyt kodu źródłowego
· Testy socjotechniczne
· Analiza powłamaniowa

Projekty realizowane są przez doświadczonych inżynierów bezpieczeństwa.

Wybrani klienci
xTrade Brokers DM S.A., TMS Brokers S.A., NN Investment Partners TFI, Moventum, BGŻ BNP Paribas, Imperial Tobacco

CYBERBEZPIECZEŃSTWO. CO GROZI FIRMOM I JAK DUŻY JEST TO PROBLEM

Kaja Grzybowska
redaktor Interaktywnie.com

kg@interaktywnie.com

1

W 2017 roku 82 proc. przedsiębiorstw zanotowało co najmniej jedno naruszenie bezpieczeństwa, a co czwarta firma zaobserwowała ich co najmniej 10 - wynika z raportu KPMG „Barometr cyberbezpieczeństwa. Świat, mogłoby się więc wydawać, na milion sposobów udowodnił, że zagrożenia związane z cyberbezpieczeństwem nie ograniczają się do rozsiewania niechcianych filmików na Facebooku, ale mimo tego polscy przedsiębiorcy pozostają sceptyczni do ostrzeżeń i je lekceważą.

Polskie firmy regulacje traktują jak fanaberie nieznających życia urzędników, a nowe technologie jedynie jako sposób na zwiększenie konkurencyjności. Niewielu z nich dostrzega korelacje między rozbudowaną infrastrukturą IT i automatyzacją procesów biznesowych z koniecznością ich odpowiedniego i nieustannego zabezpieczania. A co najciekawsze, ich podejścia nie są w stanie zrewidować nawet własne kiepskie, doświadczenia.

Tymczasem już na Facebooku cyberprzestpcy atakują prymitywnym clickbaitem - w stylu „Nie uwierzysz, co zrobiła na swoim wieczorze panieńskim!". W mailu przypominają o rzekomo niezapłaconych fakturach, a w mobile'u zachęcają do pobrania zainfekowanych aplikacji. To jednak waga piórkowa hakerskich ataków w porównaniu z tym, co dzieje się za zamkniętymi drzwiami banków, firm produkcyjnych, szpitali, szkół i - niestety - ośrodków rządowej administracji. Bo cyberbezpieczeństwo, choć powinno być już regulowane na poziomie unijnym, w Polsce wciąż kuleje.

O cyberbezpieczeństwie, tak samo jak o innowacjach, przedsiębiorczości, polskich start-upach i dolinach krzemowych, administracje wszystkich rządów uwielbiają mówić. Powstają więc śmiałe plany, długofalowe

strategie i prezentacje w Power Poincie, ale dochodzenie do konkretnych wniosków i praktycznych ustaleń, zwykle grzęźnie na mieliźnie międzyresortowych konfliktów i personalnych przepychanek. Cyberbezpieczeństwo nie jest wyjątkiem.

Ustawa o krajowym systemie cyberbezpieczeństwa, która wykuwała się w Ministerstwie Cyfryzacji jeszcze za czasów Anny Streżyńskiej, najpierw stała się zarzewiem głośnego sporu z Ministerstwem Obrony Narodowej, a potem przedmiotem krytyki organizacji biznesowych, którym w proponowanych zapisach brakowało centralizacji ośrodka decyzyjnego.

Czym grozi brak aktualizacji systemu?

Przykład ransomware'u WannaCry pokazał czym grozi brak aktualizacji systemu operacyjnego (powinna być, wraz z aktualizacjami oprogramowania antywirusowego, traktowana priorytetowo w każdej instytucji). W wyniku wspomnianego ataku zainfekowanych zostało około 200 tysięcy komputerów na całym świecie – zagrożenie szyfrowało dane znajdujące się na dysku, a następnie żądało okupu. Znane są przypadki instytucji, które po infekcji zagrożeniem ransomware zdecydowały się zapłacić okup cyberprzestępcom. Tak było w przypadku amerykańskiej szkoły publicznej w Leominster, która, ze względu na brak backupu danych, zdecydowała się przekazać 10 tysięcy dolarów za odblokowanie dostępu do zaszyfrowanych plików. Jak poinformowali dziennikarze stacji CBS News, szkoła do tej pory nie odzyskała dostępu do danych.

Kamil Sadkowski
analityk zagrożeń z ESET

W końcu trafiła jednak do Sejmu. W międzyczasie jednak ofiarą ataków inspirowanych najprawdopodobniej z Rosji padły ważne, światowe organizacje - padła amerykańska sieć elektroenergetyczna i infrastruktura lotnicza, wirus WannaCry zaszyfrował maszyny w brytyjskich szpitalach, banki w Rosji i instytucje państwowe na Ukrainie, a firma Kaspersky została oskarżona o działania wywiadowcze. Do tego jeszcze dane użytkowników Facebooka zostały bezprawnie wykorzystane do celów politycznych, a w Europie Rozporządzenie o ochronie danych osobowych (RODO) uruchomiło lawinę pytań i wątpliwości związanych z przetwarzaniem wrażliwych informacji.

Skala cyber ataków na firmy

44% firm poniosło straty finansowe na skutek ataków
62% spółek odnotowało zakłócenia i przestoje funkcjonowania
31% padło ofiarą zaszyfrowania dysku (ransomware)
20% średnich i dużych firm nie posiada nikogo od cyberbezpieczeństwa
46% spółek nie posiada operacyjnych procedur reakcji na incydenty
3% budżetu IT stanowią średnio wydatki na bezpieczeństwo – to co najmniej trzy razy za mało

źródło: raport PwC pt.: „Cyber-ruletka po polsku. Dlaczego firmy w walce z cyberprzestępcami liczą na szczęście"

Cyberatak jest zjawiskiem powszechnym, a specjslistyczne badania tezę nonszalanckim podejściu do sieciowych zagrożeń tylko potwierdzają.

Jak zabezpieczyć się przed zagrożeniami?

Specjaliści podkreślają, że żaden system nie jest w 100 procentach na nie oodporny, ale szkolenie pracowników i uświadomienie im potencjalnych zagrożeń to minimum, którego lekceważenie nie znajduje usprawiedliwienia.

Przyczyny incydentów związanych z naruszeniem bezpieczeństwa:

Błąd użytkownika	**41%**
Wykorzystanie danych/informacji	**24%**
Błędy konfiguracji komponentów	**21%**
Atak phishingowy	**20%**
Wykorzystanie znanych podatności oprogramowania	**18%**
Wykorzystanie pracownika (socjotechnika)	**15%**
Błędy projektowe systemów	**13%**
Wykorzystanie sieci	**13%**
Wykorzystanie aplikacji	**13%**
Wykorzystanie systemu IT	**12%**

źródło: raport PwC pt.: „Cyber-ruletka po polsku. Dlaczego firmy w walce z cyberprzestępcami liczą na szczęście"

- Podstawą cyberbezpieczeństwa są i zawsze będą ludzie. Niestety, stanowią w nim także najsłabsze ogniwo i ten fakt jest najczęściej wykorzystywany przez przestępców. Błędy, które popełniają pracownicy wynikają z rutyny, zaniedbań, niezrozumienia technologii oraz z braku świadomości zagrożeń - mówi Pawel Jacewicz, ztarszy konsultant w dziale cyberbezpieczeństwa Deloitte. - Przestępcy korzystając z bogatego arsenału ataków socjotechnicznych są w stanie uzyskać pewną formę kontroli nad zachowaniem osób i w konsekwencji przełamać nawet najbardziej zaawansowane zabezpieczenia techniczne.

Na szczycie skali zagrożeń niepodzielnie panują te będące skutkiem działań pracowników. Błędy, zaniedbania i brak kompetencji to jednak tylko jedna strona medalu. Druga, to ich sprytne wykorzystanie przez cyberprzestępców, którzy by spowodować wielomilionowe straty wcale nie muszą się wysilać. Phishing, czyli tzw. „łowienie", trudno przecież uznać za wysublimowaną metodę działania, a jednak - wciąż działa.

- Powszechnym zagrożeniem w naszym kraju są ukierunkowane ataki phishingowe, w których oszuści podszywają się pod kontrahenta, przesyłając fałszywą fakturę lub dokument o rzekomej zmianie numeru konta, nakłaniając w ten sposób atakowaną firmę do przetransferowania pieniędzy na fałszywy rachunek bankowy, kontrolowany przez cyberprzestępców - mówi Kamil Sadkowski. - Dla przykładu, jeden z zarządców dróg wojewódzkich został w taki sposób oszukany na kwotę 3,7 mln złotych. Pieniędzy nigdy nie odzyskał - dodaje.

Phishing nie jest jednak jedyny. Nad Wisłą nie brakuje też bardziej wyrachowanych przykładów wymuszania okupu za pomocą złośliwego oprogramowania typu ransomware. I choć wiele

instytucji, w obawie przed wyciekiem danych, a także przed wyciekiem informacji o wycieku, decyduje się płacić, to niewiele z nich dane odzyskuje, a jeszcze mniej wyciąga z tego odpowiednie wnioski. Nie tylko zresztą w Polsce. Specjaliści z PwC zwrócili uwagę na to, że zaledwie miesiąc po tym, jak udało się opanować epidemię WannaCry, rozszalała się Petya, działająca w bliźniaczy sposób. Straty związane z drugim atakiem w przypadku niektórych globalnych przedsiębiorstw sięgnęły nawet dziesiątek milionów dolarów.

Straty finansowe

Strategia typu: „jakoś to będzie" jest coraz bardziej ryzykowna i nie tylko o straty finansowe chodzi, choć te są ogromne. Z raportu Global Terrorism Index 2015 wynika, że tylko w 2014 roku świat stracił 52,9 mld dolarów w wyniku działalności cyberterrorystów. Z nowszych badań Check Point, że w Polsce ponad 90% firm doświadczyło co najmniej kilkudziesięciu ataków w ciągu roku, a średni koszt jednego (w przypadku firmy średniej wielkości) sięga 1,5 mln złotych.

Straty finansowe są jednak trudne do precyzyjnego oszacowania, bo w wielu firmach incydenty polegające na naruszeniu systemu zabezpieczeń są pilnie strzeżoną tajemnicą. Warto wspomnieć, że o włamaniach do Yahoo! świat dowiedział się dopiero po trzech latach od zdarzenia, w momencie gdy spółka przechodziła na własność Verizona. O większości pomniejszych przypadków zapewne więc nie dowiemy się nigdy.

Paraliż systemów produkcyjnych czy przerwa w ciągłości dostarczanych usług wymuszona przez działania zewnętrzne - oprócz strat finansowych - skutkują jednak także utratą reputacji zarówno wśród kontrahentów, jak i klientów. I warto zwrócić na to uwagę.

Dotychczas pokrzywdzeni użytkownicy mogli co najwyżej jednoczyć się w świętym oburzeniu na Facebooku lub dochodzić swoich praw w sądzie, co było trudne, ale RODO dało im prostą ścieżkę i narzędzia do domagania się zadośćuczynienia za utratę danych. Blamaż na tym polu może więc kosztować podwójnie. Bo Rozporządzenie przewiduje też kary za jego złamanie.

Uważaj! Jest 100 tys. luk w programach

Niewidocznym na pierwszy rzut oka zagrożeniem są podatności systemów, aplikacji i urządzeń wykorzystywanych przez przedsiębiorstwa. Liczba znanych luk przekroczyła już 100 tysięcy, z czego ponad 14 tysięcy jest oznaczonych jako te najbardziej krytyczne, a kolejne będą odkrywane. Jest to naturalny stan cyfrowego świata. Największym grzechem przedsiębiorstw jest jednak brak działań ograniczających ich wpływ na firmę. Automaty wyszukujące podatne elementy identyfikują je szybko, precyzyjnie i na wielką skalę, a następnie infekują w sposób niewidoczny dla użytkownika lub przy jego minimalnym udziale. Zarażone systemy i urządzenia są następnie wykorzystywane do rozwoju ataku na firmę lub kolejnych ataków na inne przedsiębiorstwa lub osoby prywatne.

Adam Lisowski
ekspert w zespole ds. cyberbezpieczeństwa w PwC

ARTYKUŁ PROMOCYJNY

W CYBERSFERZE JAK W KRYMINALNYM FILMIE. ZA WSZELKĄ CENĘ TRZEBA SIĘ BRONIĆ

POLICJANCI I ZŁODZIEJE W SIECI

Katarzyna Pilawa
specjalista ds. PR i marketingu w firmie DAGMA Bezpieczeństwo IT

2

Ten wyścig nieustannie trwa: od czasów pojawienia się komputerów i tworzenia sieci, będących podstawą dzisiejszej internetowej sfery, znajdowali się tacy ludzie, którzy pragnęli przeniknąć ich zagadkę. Historia komputeryzacji jest opowieścią o walce dwóch typów innowatorów - wynalazców zabezpieczeń i miłośników ich łamania. Przeciwnicy zawsze są blisko siebie, depczą sobie po piętach.

Sposobów na atakowanie sieci jest mnóstwo, na dodatek ciągle ich przybywa. Są wśród nich exploity i cyberataki wykorzystujące socjotechnikę. Każdy z nich może zagrażać danym, paraliżować pracę oraz wystawiać na szwank reputację firmy.

Najpopularniejsze cele ataków to wirtualne serwery, publiczne witryny webowe i urządzenia mobilne. Cyberkryminaliści nie cofają się przed niczym, są doskonale przygotowani, pomysłowi i zdeterminowani. Mogą działać na wiele sposobów.

(R)ewolucja ransomware

Kwestie bezpieczeństwa w sieci nie schodzą z nagłówków największych portali oraz magazynów na całym świecie. Wystarczy przypomnieć głośne ataki szyfrujące dane na komputerach ransomware – Petya oraz Wannacry, które wyłudzały pieniądze od zwykłych użytkowników oraz mniejszych i większych instytucji.

Wannacry - najgłośniejszy atak ransomware, którego największa aktywność przypadła na maj 2017 roku, był jednym z największych cyberataków w historii, który infekował setki tysięcy komputerów na całym świecie, również w Polsce. Złośliwe oprogramowanie blokowało dostęp do komputera z systemem Windows. WannaCry nie pozwalał otworzyć ani skopiować żadnych znajdujących się na nim plików. Użytkownik widział tylko

planszę z instrukcją, informującą o bezskuteczności prób usunięcia wirusa i oczekiwaniu okupu. Wirus szyfrował wszystkie pliki zapisane na dyskach użytkownika, niemal nieodwracalnie blokując do nich dostęp. Za odszyfrowanie należało zapłacić bitcoinami, a koszt zdjęcia blokady wzrastał wraz z upływem czasu. Jeśli użytkownik nie wpłacił okupu do zdefiniowanej daty, możliwość odzyskania dostępu do plików przepadała bezpowrotnie.

Drugi, równie poważny atak ransomware nastąpił niespełna miesiąc po pierwszym. Zagrożenie, znane jako Petya, uderzyło w firmy i instytucje znajdujące się głównie na Ukrainie.

Prawidłowość serii ataków wskazał jako pierwszy Anton Cherepanov, analityk zagrożeń z firmy ESET. Jego teza opierała się na analizie cyberincydentów z dwóch lat - pierwszy atak z tej serii miał mieć miejsce w 2015 roku, kiedy to na cel wzięto ukraińskie przedsiębiorstwo energetyczne. Prawdopodobnie ta sama grupa hakerów w grudniu 2016 roku znów zaatakowała ukraińskie instytucje finansowe i infrastrukturę krytyczną tego państwa.

Cyberprzestępcy wykorzystali złośliwą aktualizację popularnego na Ukrainie programu do rozliczeń finansowych M.E.Doc, którą udostępnili na kontrolowanych przez siebie serwerach producenta. Dzięki automatycznemu procesowi pobierania aktualizacji błyskawicznie dotarli do olbrzymiej grupy ukraińskich celów, niszcząc dane w większości tamtejszych firm i organizacji.

W opinii Davida Harleya z ESET, wspomniane zagrożenia zaczynają ewoluować, poszerzając tym samym zasięg ataków oraz formę. Zdaniem eksperta, ataki targetowane w dalszym ciągu będą nam zagrażać. Niektóre instytucje nawet już teraz zabezpieczają środki w swoich budżetach na zapłatę okupu potencjalnego ataku ransomware, w ramach specyficznej „strategii backupu". Część z nich dochodzi do wniosku, że lepiej zapłacić okup, niż wydać żądaną przez cyberprzestępców kwotę na poprawę swojego cyberbezpieczeństwa. Harley przewiduje, że w przypadku urządzeń mobilnych coraz mniej ataków będzie koncentrować się na kradzieży danych. Zwiększy się natomiast liczba zagrożeń, które będą dotyczyć przejęcia kontroli nad telefonem i jego poszczególnymi funkcjami.

Duże instytucje na celowniku hakerów

Przykład ataku na ukraińską elektrownię sprzed dwóch lat, który na kilka godzin pozbawił prądu niemal milion mieszkańców, pokazuje, że duże instytucje przemysłowe mogą stać się ofiarami cyberprzestępców. Wymierzone w przemysł ataki potrafią obejść zaawansowane systemy kontrolne. Do jednych z nich należał Industroyer, który atakował między innymi elektrownie, wodociągi, rozdzielnie gazu, bezpośrednio kontrolując znajdujące się w podstacjach elektrycznych przełączniki i wyłączniki. W tym celu wykorzystywał przemysłowe protokoły komunikacyjne stosowane w infrastrukturze zasilania, systemach kontroli

transportu i innych ważnych systemach infrastruktury krytycznej (woda, gaz), które są używane na całym świecie. Eksperci z ESET prognozują, że kolejne miesiące będą sporym wyzwaniem dla osób, zajmujących się poprawą bezpieczeństwa przestarzałych systemów kontroli (ICS). Duże organizacje będą musiały nie tylko zweryfikować system kontroli sieci, ale również wprowadzić odpowiednie oprogramowanie oraz hardware, chroniące przed atakami hakerów.

Wciąż aktualne ataki DDoS

Poważne niebezpieczeństwo stwarzają także botnety. Maszyny zombie, wykorzystywane bez wiedzy ich właścicieli, stwarzają zagrożenie skoordynowanego ataku na sieć przedsiębiorstwa czy instytucji, mogą spamować i infekować następne urządzenia.

Według badania A10 Networks, w zeszłym roku ataki realizowane za pośrednictwem botnetów osiągnęły masę krytyczną - na całym świecie dochodzi do nich prawie 4 tysięcy razy dziennie. Celem ataków DDoS padają strony internetowe banków, sklepów internetowych. Jedną z takich stron, która kilka miesięcy temu przestała działać w wyniku ataku DDoS, była witryna internetowa brytyjskiej loterii narodowej. W efekcie miliony Brytyjczyków w dniu ataku nie mogło zakupić losu na loterii.

Walkę z cyberprzestępcami toczą twórcy antywirusów, współpracując przy tym ze stróżami prawa. Do takiej sytuacji doszło przy okazji likwidacji botnetu Windigo, który zaczął działać w 2011 roku, przez trzy lata funkcjonował niewykryty. Odpowiadał za wysyłkę 35 milionów wiadomości spamowych dziennie.

Dzięki współpracy firmy ESET z amerykańskim Federalnym Biurem Śledczym (FBI) udało się zidentyfikować i aresztować jednego z twórców Windigo. Eksperci z ESET wówczas ustalili, że za sprawą wielu specjalnie zaprojektowanych zagrożeń komputerowych zostało zainfekowanych kilkadziesiąt tysięcy serwerów na całym świecie.

Ataki na naszą prywatność

Rozwój nowych technologii sprawia, że producenci coraz chętniej wymagają od swoich użytkowników podania danych osobowych, które zostaną przez twórców aplikacji zmonetyzowane. Ten trend, zdaniem Tony'ego Anscombe'a z ESET, będzie utrzymywał się w najbliższych latach, zwiększając ryzyko związane z prywatnością danych, ich wyciekiem lub sprzedażą innym podmiotom.

W 2018 roku nasza prywatność może zostać poddana próbie. Wszystko za sprawą urządzeń Internetu Rzeczy (IoT). Podczas jazdy samochodem nasz smartfon pokazuje nam aktualne natężenie ruchu, za pomocą telefonu kontrolujemy termostat w domu, pracę piekarnika, czy nawet pralki. Cyberprzestępcy, na podstawie zgromadzonych przez smart-urządzenia

informacji, są w stanie zebrać szereg danych na nasz temat - mogą wiedzieć, gdzie jesteśmy, co jemy, a nawet kiedy uprawiamy seks. Analizy Gartnera wskazują, że w 2018 roku będzie ponad 11 miliardów urządzeń podłączonych do sieci, z czego liczba ta wzrośnie do ponad 20 miliardów w 2020 roku.

Jak radzi ekspert z ESET, w najbliższym czasie konsumenci IoT powinni wnikliwie analizować politykę prywatności, czytać dotyczące jej komunikaty oraz podejmować bardziej racjonalne decyzje w kontekście zakupu nowoczesnych gadżetów. Przepisy RODO wprowadziły nowe obostrzenia dla firm z zakresu przetwarzania danych osobowych. Wymusza to na przedsiębiorcach jeszcze większą dbałość o dane swoich użytkowników, co będzie miało zdecydowany wpływ na poprawę bezpieczeństwa, a co za tym idzie - zmniejszenia liczby potencjalnego wycieku wrażliwych danych.

Jak się bronić?

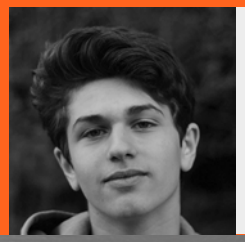
Zagrożeniom można stawiać opór, choć nie jest to łatwe. Wobec tego, że po drugiej stronie barykady staje czasem wielu kreatywnych „fachowców", którzy postanowili przejść na stronę złych mocy, co sprawia, że niebezpieczeństwo ewoluuje w szybkim tempie, istotną rolę odgrywają dwie sprawy. Potrzebna jest permanentna analiza zagrożeń, pozwalająca na opracowywanie systemów blokad. Ważna jest również współpraca twórców antywirusów z organami ścigania. Dzięki niej udaje się coraz skuteczniej wymierzać sprawiedliwość wśród cyberprzestępców. Eksperci z firm antywirusowych wielokrotnie pomagali m.in. FBI, Interpolowi, Europolowi przy namierzaniu hakerów, dostarczając funkcjonariuszom specyfikacje oraz raporty dotyczące przeprowadzanych przez cyberprzestępców ataków. Taka współpraca może mieć znaczący wpływ na wzrost poziomu cyberbezpieczeństwa. Może w niedalekiej przyszłości doprowadzić do większej ilości aresztowań przestępców odpowiadających za naruszanie bezpieczeństwa w sieci oraz zwiększyć świadomość użytkowników o braku anonimowości w Internecie. W opinii ekspertów w tym roku zwiększy się ilość aresztowań, które sprawią, że Internet będzie bezpiecznym miejscem dla wszystkich, z wyjątkiem cyberprzestępców.

Szansą na większe bezpieczeństwo sieci korporacyjnych są inteligentne technologie. Na rynku od dawna funkcjonują rozwiązania bezpieczeństwa oparte na uczeniu maszynowym. Tworzą one ochronę użytkowników biznesowych poprzez analizowanie sieci, uczenie się jej prawidłowości i wykrywanie anomalii. Machine learning stanowi sedno koncepcji behawioralnej, choć to maszyny uczą się poprzez obserwowanie zachowań i definiowanie profilu standardowej aktywności użytkownika.

Najważniejsze kryterium tego, czy rozwiązanie antywirusowe spełnia swoją rolę, są dwa czynniki - dokładność detekcji i szybkość działania. Jeśli chodzi o kombinację wykrywalności i szybkości działania - rozwiązania ESET są liderem większości niezależnych testów. Dlaczego tak jest? Uczenie maszynowe i technologie sztucznej inteligencji to obecnie w branży bezpieczeństwa kierunek rozwoju, z którym wiąże się największe nadzieje. W tym kierunku swoje badania R&D prowadzi większość kluczowych graczy w branży. Co ciekawe - to, na co stawiają dziś eksperci, stało u fundamentów założenia firmy ESET. Od początku swojego istnienia ESET budował i rozwijał technologie, które miały zbudować produkt, który w możliwie największym stopniu będzie w stanie samodzielnie wykryć nowy atak. ESET nazywał wtedy tę technologię „zaawansowaną analizą heurystyczną". Już 10 lat temu ESET realizował w Polsce dużą kampanię reklamową mówiąc o stosowaniu sztucznej inteligencji w swoich produktach. W tamtym okresie podejście było unikalne, bo większość innych graczy poprawiała detekcję zatrudniając po prostu więcej pracowników, którzy szybciej mogli tworzyć nowe sygnatury wykrywające nowe ataki. Dziś po latach daje to ogromną przewagę, ponieważ firma zbiera doświadczenia w wykorzystaniu sztucznej inteligencji do wykrywania zagrożeń znacznie dłużej niż konkurenci. To widać w wynikach testów.

Paweł Jurek
wicedyrektor ds. rozwoju w firmie DAGMA Bezpieczeństwo IT

JAK UCHRONIĆ SIĘ PRZED ATAKAMI?



Robert Cieszawski
redaktor Interaktywnie.com

redakcja@interaktywnie.com

3

Aż 80 proc. prezesów największych światowych organizacji przyznaje, że cyberataki są jednym z największych zagrożeń dla rozwoju ich biznesu - czytamy w raporcie PwC z 2018 roku. Ochrona firmy przed cyberatakami może być bardziej lub mniej ścisła, a pracownicy lepiej lub gorzej przeszkoleni, ale ryzyko przełamania zabezpieczeń zawsze będzie istniało. Nie ma bowiem organizacji w 100 procentach na nie odpornych i perfekcyjnie chronionych.

Niestety, w regionie Europy Środkowo-Wschodniej odsetek przekonanych o tym szefów firm jest jeszcze niższy i wynosi obecnie 77 proc. Choć świadomość wzrasta i widoczny jest pewien postęp w deklarowanym poziomie gotowości, z analiz PwC wynika, że polskie firmy wciąż nie są w pełni przygotowane na przeciwdziałanie współczesnym zagrożeniom i metodom ataków. Ogólną strategię bezpieczeństwa opracowało zaledwie 65 proc. badanych przez PwC firm, a procesy reagowania na incydenty już nieznacznie co drugie przedsiębiorstwo.

Jak chronić przedsiębiorstwa

Nie ma jednego panaceum na wszelkie zagrożenie cybernetyczne. Potrzebna jest zawsze sieć różnych zabezpieczeń, wzajemnie się przenikających, utrudniających tym samym przedostanie się do twierdzy, jaką być powinny systemy informatyczne firm i instytucji.

Mimo tego, jak podkreślają eksperci, w kwestii bezpieczeństwa stuprocentowej odporności na atak nikomu nie udało się dotąd osiągnąć. Potwierdziły to głośne ataki na rządowe sieci komputerowe, instytucje finansowe, czy wielkie koncerny i filmy. Sparaliżowanie japońskiego koncernu samochodowego Nissan czy francuskiego Reanult, niemieckich kolei Deutche Bahn czy brytyjskich szpitali przez wirus WannaCry w maju ubiegłego roku, dowiodło, że nawet potężne i bogate firmy mogą stać się ofiarami.

Instytucje państwowe i tzw. infrastruktura krytyczna, która powinna być solidnie zabezpieczona, również padła pod naporem następcy wspomnianego złośliwego oprogramowania, wirusa Petya, który zaledwie miesiąc później zainfekował najważniejsze ukraińskie lotniska, ciepłownie i elektrownie. Nie oparł mu się również rosyjski, państwowy gigant naftowy, Rosnieft czy amerykański koncern farmaceutyczny Merck.

Potrzebny audyt

Podstawowym powodem, dla którego audyt bezpieczeństwa informacji staje się niemalże koniecznością zarówno dla małych, średnich, jak i dużych przedsiębiorstw jest przejście ze stanu „nie wiem, czego nie wiem" do „wiem, czego nie wiem".

Liczba cyberzagrożeń wzrasta z każdym dniem i niezwykle ciężko jest nadążyć za pomysłowością cyberprzestępców. Tak więc jedynym sposobem na skuteczną ochronę jest skorzystanie ze wsparcia ekspertów w dziedzinie bezpieczeństwa. Ekspertów, którzy obok części teoretycznej, czyli np. stworzenia odpowiednich procedur i dokumentacji w zgodzie z RODO, sprawdzą też realny poziom bezpieczeństwa organizacji. Służą temu testy penetracyjne - czyli kontrolowane ataki na infrastrukturę sieciową - i socjotechniczne, to jest sprawdzenie reakcji pracowników na próby wyłudzenia informacji. Nawet jeżeli firma posiada własny dział IT, to bezpieczeństwo informacji jest na tyle wąską i skomplikowaną specjalizacją, że skorzystanie ze wsparcia zewnętrznych doradców może okazać się niezbędne. Z usług niezależnych audytorów korzystają zarówno przedsiębiorcy, jak i jednostki administracji publicznej, a zainteresowanie takimi rozwiązaniami nieustannie rośnie – 59 proc. respondentów raportu „20th Global Information Security Survey 2017–18" firmy Ernst & Young twierdzi, że ich budżet na przeciwdziałanie cyberprzestępstwom wzrósł w ciągu ostatnich 12 miesięcy.

Anna Piechocka
dyrektor zarządzająca DAGMA Bezpieczeństwo IT, posiadająca prestiżowy certyfikat bezpieczeństwa CISSP

Pomoże technologia czyli rozwiązania software i hardware

Zwalczaj wroga jego własną bronią - brzmi wojenne powiedzenie. Nie bez przyczyny jednym z najważniejszych elementów tak zwanej architektury bezpieczeństwa są odpowiednie programy, czyli rozwiązania software i sprzętowe - hardware. Na rynku oprogramowania i sprzętu oferta jest bogata. Pozostaje pytanie, w co warto inwestować?

Jak przekonuje Paweł Jurek, wicedyrektor ds. rozwoju w firmie DAGMA Bezpieczeństwo IT, w oderwaniu od sytuacji konkretnej firmy, bez analizy procesów w niej działających trudno określić model, jaki powinna ona przyjąć, aby poprawić poziom bezpieczeństwa.

- Na to pytanie można odpowiedzieć analizując sytuację konkretnej firmy, prowadząc w niej testy bezpieczeństwa i analizując wszystkie ryzyka, na jakie firma jest narażona. Dopiero po wykonaniu takiej pracy można określić, jaką część ryzyk można zmniejszyć, inwestując we właściwy sprzęt i oprogramowanie, a jaką część należy rozwiązać w inny sposób, np. przez zmianę uprawnień - podkreśla ekspert DAGMA.

Jakie programy najczęściej stosują przedsiębiorcy? Okazuje się, że w firmach najczęściej wykorzystywanym zabezpieczaniem - ich wdrożenie potwierdza pond połowa przedsiębiorstw

- są aplikacje typu WAF - Web Applickation FireWall. Więcej niż co drugie przedsiębiorstwo stosuje także mechanizmy web proxy, czyli filtrowania ruchu ze storn www - wynika z badań PwC.

Na podobnym poziomie stosowe są również Systemy Detekcji Włamań (tzw. IPS/IDS). Kłopot w tym, że jak wyjaśniają eksperci, są one nieskuteczne przy wysoko rozwiniętych systemach informatycznych. Nie są przeszkodą dla ataków phishingowych, a co dopiero działań hackerskich określanych jako APT, czyli zawansowanych, uporczywych zagrożeń (z ang. Advanced Persistent Threat).

Te specjalistyczne oprogramowania anty ATP wykorzystuje dziś 46 proc. polskich firm, co i tak można uznać za sukces, bowiem jeszcze rok wcześniej, tylko co czwarty przedsiębiorca deklarował w badaniu PwC jego posiadanie. Ich włączenie do struktury pomaga przedsiębiorstwom skutecznie ograniczyć zagrożenia. Dzięki tym zabezpieczeniom liczba ataków phishingowych znacznie się zmniejszyła - z 39 proc. w roku poprzednim, do 18 proc. obecnie.

Jeszcze mniejszy odsetek organizacji w Polsce stosuje systemy do zarządzania informacją i zdarzeniami bezpieczeństwa (tzw. SIEM) - czyli, upraszczając, system wczesnego ostrzegania. Jak wielu? Według badań, niewiele więcej niż co trzecia firma. Dodatkowo, tylko 14 proc. w ubiegłym roku uruchomiło tzw. Centra Operacji Bezpieczeństwa SOC (Security Operations Center), które zbierają informacje z różnych powiązanych ze sobą systemów bezpieczeństwa, analizują je, co pozwala na wykrycie szeregu problemów z bezpieczeństwem i reakcję.

- Mechanizmy zabezpieczające, tworzące architekturę bezpieczeństwa, w które inwestują firmy, można podzielić na 3 typy: prewencyjne, detekcyjne i reakcyjne. Technologia SIEM zalicza się do mechanizmów detekcyjnych, z kolei SOC do mechanizmów reakcyjnych związanych z monitorowaniem i reagowaniem na identyfikowane incydenty bezpieczeństwa. Odpowiednio zaplanowana i wdrożona architektura bezpieczeństwa to zestaw wzajemnie połączonych ze sobą mechanizmów, stanowiących jednolity system obronny, które

Przeczytaj zanim zainwestujesz

- Zanim wybierzemy się na zakupy, musimy wiedzieć, co należy kupić i gdzie to zainstalować. Bez tej wiedzy, przekażemy tylko nasze budżety na bezpieczeństwo – prawdopodobnie udostępnimy je tym dostawcom, którzy najzręczniej zaprezentują swój produkt. Dlatego na początku należy zainwestować w wiedzę! Należy wyszkolić ludzi, którzy odpowiadają za bezpieczeństwo lub związać się na stałe z partnerem, który ma odpowiedni know-how i będzie nam w tym procesie doradzał. Dopiero, kiedy wiemy, co należy zrobić, żeby się zabezpieczyć, przychodzi czas na zakupy.

Paweł Jurek
wicedyrektor ds. rozwoju w firmie DAGMA Bezpieczeństwo IT

powinny działać jak sprawny system immunologiczny - tłumaczy Tomasz Sawiak, wicedyrektor Zespołu Cyber Security. - W przypadku infrastruktury IT jest podobnie – wnioski z incydentów należy odpowiednio sformułować i wdrożyć doskonaląc zabezpieczenia.

Według Ponemon Institute, liczba użytkowników modułów bezpieczeństwa HSM (Hardware Security Module), które wykorzystuje się przede wszystkim do szyfrowania danych w chmurze z roku na rok rośnie. Zgodnie badaniami instytutu, wykorzystanie HSM od ubiegłego roku wzrosło do 41 proc. Zwykle te rozwiązanie stosuje się w SSL / TLS i szyfrowania na poziomie aplikacji. Co piąty respondent przyznał, że używa HSM z aplikacjami typu blockchain.

Które rozwiązania są niezbędne? Jak wyjaśnia Paweł Jurek, wicedyrektor ds. rozwoju w firmie DAGMA, zwykle firma powinna posiadać rozwiązania typu „endpoint protection" chroniące stacje robocze, odpowiednią ochronę poczty firmowej i własnych serwerów.

- Ochronę danych na poziomie konkretnych rozwiązań technicznych może zapewnić odpowiedni system DLP (Data Loss Prevention) i szyfrowanie zasobów - zaznacza Jurek.

Człowiek, najsłabsze ogniwo w firmie

Mogłoby się wydać, że inwestycja w zawansowane systemy informatyczne - programy, sprzęt - będące obwarowaniem firmy zapewni jej bezpieczeństwo.

- Często obserwowane przez nas podejście firm w tym obszarze, to niezachwiana wiara w zaimplementowane rozwiązania techniczne – zapory, systemy antyAPT, NextGen, Network Behaviour Analizer itp. Najczęściej - w około 95 proc. przypadków - okazuje się, że to są bardzo dobrze wykonane drzwi w domu, w którym, od podwórka, istnieje wielka dziura w ścianie. Taka sytuacja wynika z tego, że najsłabszym ogniwem jest człowiek - przyznaje Jacek Michałek, menedżer w dziale cyberbezpieczeństwa firmy Deloitte.

Potwierdzają to niestety również niezależne badania. Według Kaspersky Lab i B2B International, najczęstszym źródłem wycieku poufnych informacji w firmach na całym świecie - aż w 42 proc. z nich - w 2016 roku okazali się pracownicy.

Również w 30 proc. polskich spółek, główną przyczyną wystąpienia incydentu były przeoczenia czy wręcz błędy własnej kadry. Te często prowadziły do utraty danych, co dla 44 proc. naszych firm oznaczało straty finansowe - wykazuje raport PwC z 2018 roku.

- Pracownicy są najsłabszym ogniwem w obronie przed cyberatakami, szczególnie w typowych atakach socjotechnicznych czyli: phishingu, smishingu, czy vishingu - przyznaje specjalista w kwestii cyberbezpieczeństwa firmy Deloitte.

Dlaczego? Bowiem, jak wyjaśnia ekspert, w przypadku ataków socjotechnicznych, wykorzystuje się słabość ludzkiej natury - ludzie generalnie są dobrzy i starają się pomóc innym,

również nieznajomemu, który prosi ich o otwarcie załącznika, mimo że Excel wyświetla ostrzeżenia o niezaufanych markach i potencjalnie niebezpiecznej treści.

- Atakującemu zwykle wystarczy jedna osoba, która wykona działania prowadzące finalnie do włamania: wejdzie na stronę, do której odnośnik dostała poprzez email, otworzy złośliwy plik otrzymany z niezaufanego źródła lub wykona polecenie rzekomego informatyka ze swojej firmy, który kontaktuje się w pilnej sprawie przez telefon – note bene z numeru również nieznanego - zaznacza inny ekspert Deloitte, Marcin Ludwiszewski, lider ds. cyberbezpieczeństwa.

Trudno uwierzyć? Administrator w dużej wrocławskiej firmie o zasięgu ogólnopolskim, a działającej w branży internetowej, postanowił zbadać poziom bezpieczeństwa. To była prosta prowokacja. Założył maila w popularnej domenie Gmail na swoje nazwisko, ale celowo popełnił w nim błąd. Następnie rozesłał do pracowników maile z prośbą, by w odpowiedzi podesłali mu loginy i hasła do poczty korporacyjnej, motywując to prowadzonymi aktualizacjami w firmie. Efekt? Tylko jeden pracownik nie udostępnił mu danych. Odpisywanie na maila było dla niego zbyt angażujące, więc postanowił zadzwonić i podać hasło oraz login telefonicznie.

Sprytniejsi hackerzy zawężają obszar ataku do mniejszej grupy pracowników.

- Wybierają osoby, które z racji zajmowanych stanowisk, generalnie nie posiadają specjalistycznej wiedzy i mogą mieć małą świadomości zagrożeń bezpieczeństwa, a zarazem współpracują z zewnętrznymi podmiotami - zaznacza Jacek Michałek.

O jakich pracowników może chodzić? Na przykład z działu HR, zakupów czy z recepcji. To często najbardziej podatna na atak grupa.

Atakującym pomagają też informacje, które na co dzień, niemal dla każdego dostępne są w sieci. Mogą oni garściami czerpać wiedzę o pracownikach czy firmie. Służą temu sieci społecznościowe, atrakcyjne akcje promocyjne, czy otwarcie komunikowane publicznie wydarzenia w firmach. Wszystko to może posłużyć za okazję do ataku oraz uwiarygodnienia osoby próbującej przełamać zabezpieczania firmy.

- Przygotowanie ataku przez zdeterminowaną jednostkę lub organizację przestępczą - nie wspominając już o służbach specjalnych - nie nastręcza problemów - zaznacza Marcin Ludwiszewski z Deloitte. - A jeśli nawet zaczyna być kłopotliwe, to zawsze można zmienić cel lub scenariusz ataku - dodaje.

Czy chmura może być receptą na obronę przed atakami?

Rosnąca świadomość zagrożeń cybernetycznych dla biznesu powoduje, że wzrasta zapotrzebowanie na specjalistów

do spraw bezpieczeństwa. Duże firmy, zwłaszcza z sektora finansów, telekomunikacji czy energetyki mocno inwestują w rozbudowane zespoły IT.

W trudniejszej sytuacji są jednak mniejsze spółki, których nie stać jest na stworzenie własnych komórek monitorowania bezpieczeństwa, pozyskania specjalistów i technologii. Zmiana istniejących procesów, jak i wdrożenie dodatkowych, wymaga bowiem nakładów finansowych.

- Bardzo łatwo jest uzasadnić potrzebę instalacji nowych systemów bezpieczeństwa, ale dużo trudniej zapewnić środki i zespół do utrzymania tej infrastruktury czy na praktyczne przetestowanie tych systemów (np. testami penetracyjnymi lub red teaming). Problemem jest też skuteczne i zdeterminowane tych testów przeprowadzenie - zaznacza ekspert Deloitte, Marcin Ludwiszewski.

Rozwiązaniem może okazać się skorzystanie z zewnętrznych usług, na przykład wykorzystanie coraz bardziej popularnej chmury. Zgodnie z danymi International Data Corporation (IDC), w 2018 wydatki na usługi oraz infrastrukturę w chmurze mają sięgnąć 160 mld dolarów, a do 2021 roku wrosnąć do 277 mld dolarów. To pokazuje skalę rozwoju tej usługi.

- Rozwiązania techniczne, w tym outsourcing oraz usługi w chmurze, bardzo pomagają w podniesieniu poprzeczki dla atakującego - przyznaje ekspert bezpieczeństwa Deloitte. - Zakup gotowych usług i zarządzanych przez zewnętrzny podmiot zasobów zdejmuje z organizacji część obowiązków i kosztów, które należałoby ponosić przy samodzielnym ich utrzymaniu - argumentuje.

Najbardziej zaawansowane typy chmury to tzw. SaaS (Software as a Service). W tym modelu to dostawca odpowiada za oprogramowanie i dostarcza gotową usługę. Poza tym rozwiązaniem są jeszcze PaaS (Platform as a Service), któr umożliwiają dostęp do platformy i oferują narzędzia deweloperskie, a użytkownik wspomaga zarządzanie swoimi bazami danych, przepływem danych czy diagnozą problemów.

Trzeci model to IaaS (Infrastructure as a Service), gdzie usługodawca odpowiada jedynie za infrastrukturę, a oprogramowanie pozostaje w gestii użytkownika.

Jak pisał niedawno Interkatywnie.com, chmura w wielu przypadkach przypadkach to jeden z najbezpieczniejszych modeli, bowiem rzadko która firma jest w stanie pozwolić sobie na takie zabezpieczenia własnych serwerów, jakie mają firmy oferujące usługi chmurowe.

Firmy, które profesjonalnie zajmują się dostarczaniem takich rozwiązań - zwłaszcza biznesowi - muszą dbać o najwyższe bezpieczeństwo danych, co potwierdzają certyfikatami norm ISO czy CSA STAR. Mają wyspecjalizowane systemy

bezpieczeństwa, wykorzystują wyższe szyfrowanie danych oraz połączenia VPN między firmą a dostawcą chmury.

Czy są absolutnie bezpieczne? To, że stają się one powszechne i coraz więcej klientów biznesowych powierza im swoje dane, powoduje, że są coraz częściej stają się celami atakujących. Nie są więc one wolne od cyberzagrożeń i muszą odpierać ataki hackerskie podobnie, jak tradycyjne centra danych. Ale jednocześnie pracuje nad nimi nieustannie sztab specjalistów od niwelowania zagrożeń.

Firma Alert Logi w ubiegłym roku wydała raport, w którym przeanalizowała 2,2 mln incydentów, które wystąpiły na przestrzeni 18 miesięcy wśród 3,8 tys. firm korzystających z usług chmurowych. Średnio na firmę przypadały 684 incydenty, które dotyczyły chmur prywatnych i 612 dotyczących firmowych centrów danych. W trzech czwartych przypadków były to ataki na aplikacje webowe.

Jak wynika z najnowszego badania PwC, w przypadku chmury obliczeniowej strategię bezpieczeństwa posiada 27 proc. badanych polskich spółek, a 17 proc. ma w planach jej stworzenie w ciągu najbliższego roku.

- Niestety, bardzo często zakup zewnętrznych usług nie jest poprzedzany analizą ryzyka i wpływu na bezpieczeństwo. Wielokrotnie podjęte decyzje biznesowe wywołują popłoch w działach bezpieczeństwa, postawionych przed faktami dokonanymi i na gwałt szukającymi rozwiązań dla kwestii nieuwzględnionych w umowach z dostawcami. Przykład? Odpowiedzialność za przetwarzanie danych, minimalne wymagania bezpieczeństwa i zgoda na audytowanie dostawcy, wymagania techniczne odnośnie bezpieczeństwa komunikacji i przetwarzania wrażliwych danych i inne kwestie - wylicza Jacek Michałek, ekspert w dziale cyberbezpieczeństwa Deloitte. - Decyzje biznesowe, nieuwzględniające od początku kwestii bezpieczeństwa mogą podnieść ryzyko powodzenia cyberataków, które coraz częściej mają miejsce.

ARTYKUŁ PROMOCYJNY

TWÓJ PRACOWNIK ZGUBIŁ LAPTOP. SPOKOJNIE, WSZYSTKIE DANE BYŁY ZASZYFROWANE

HISTORIA STRACONEGO LAPTOPA

Katarzyna Pilawa
specjalista ds. PR i marketingu w firmie DAGMA Bezpieczeństwo IT

4

To były sekundy. Wystarczyło, że pracownik korporacji nie zamknął auta po tym, jak zatrzymał się na stacji benzynowej, zatankował i poszedł zapłacić. Z tylnego siedzenia zniknęła torba ze służbowym laptopem. Incydent przybrał rozmiary tragedii. Dlaczego? Razem z urządzeniem zniknęły wszystkie cenne firmowe dane.

Firmowa komórka lub komputer to dziś już standardowe wyposażenie powierzane przez pracodawców w wielu branżach. To normalne, że pracownik nie musi inwestować w taki sprzęt mobilny i wydawać własnych pieniędzy na narzędzia swojej pracy.

Jednak takie urządzenia są warte więcej, niż mogłoby się wydawać.

To nie fotki, to strategiczne skarby

Mowa tu oczywiście nie o rynkowej cenie laptopa czy smartfona, lecz o wartości danych przechowywanych w swojej pamięci. W przypadku kradzieży, czy też zagubienia, bo i w taki sposób sprzęt może przepaść i dostać się w niepowołane ręce, firma nie tylko traci pewien zasób danych biznesowych, ale jeszcze narażona jest na to, że równocześnie to zdarzenie wiązać się może z dużym prawdopodobieństwem wycieku informacji i baz danych na zewnątrz. Nic więc dziwnego, że europejscy managerowie IT zgodnie przyznają, że modele pracy mobilnej wiążą się ze zbyt wielkim ryzykiem, mimo oczywistych korzyści związanych ze wzrostem produktywności, jakie mogą zapewnić firmie takie urządzenia.

Wraz z laptopem przepaść przecież mogą faktury, zamówienia, korespondencja, a co najgorsze - bazy danych klientów

lub partnerów, które nieodpowiednio zabezpieczone, mogą przysporzyć firmie wiele problemów, szczególnie finansowych, ponieważ w grę wchodzi RODO. Zatem potrzeba szczelności wynika nie tylko z obawy o działania konkurencji, ale również o ochronę w obliczu nowych przepisów.

Blokuj

Nierzadko sami właściciele firm nie wiedzą, jaką niematerialną wartość gromadzą telefony i laptopy, którymi posługują się pracownicy. Ci ostatni ustawiają ewentualnie kod PIN lub prostą blokadę graficzną w postaci łatwego do odgadnięcia wzoru.

Dane i informacje zapisane w naszych sprzętach mogą zostać sprzedane firmom konkurencyjnym lub nabywcom na czarnym rynku.

Utrata ważnych danych to nie tylko kryzys strategiczny i wizerunkowy, ale także groźba poważnych konsekwencji prawnych. Zmiany w podejściu do ochrony danych osobowych będą dopasowane do dzisiejszych, „zdigitalizowanych" realiów, a sankcje nakładane na przedsiębiorstwa, które naruszą przepisy, są wyjątkowo wysokie.

Jedynym pocieszeniem w tej sytuacji jest fakt, że większość złodziei kradnie telefony i laptopy dla samego sprzętu. Interesuje ich tylko sprzedaż urządzenia, nie zajmują się danymi, nie weryfikują ich i nie wyceniają. Prawdziwi złodzieje danych, którym zależy na ich cyfrowej wartości, wcale nie potrzebują zdobywać fizycznego urządzenia. Cyfrowi bandyci stosują coraz bardziej wyrafinowane metody wykradania informacji z mobilnych urządzeń.

Oficjalnie żadna firma takich danych nigdy by nie kupiła, jednak pokusa uzyskania informacji o podmiotach konkurencyjnych jest bez wątpienia ogromna. Złodziej może też próbować „sprzedać" skradziony sprzęt jego właścicielowi. Zastosuje szantaż: albo pieniądze, albo twoje zdjęcia, filmy, wiadomości, adresy mailowe lądują w sieci.

Jak chronić dane?

Istnieje już wiele technologicznych zabezpieczeń - haseł, VPN-ów, systemów szyfrujących, blokad otwieranych poprzez odcisk palca, nakładek pozwalających pracować w osobnym środowisku systemowym oraz rozwiązań chmurowych. Warte rozważenia są szczególnie te ostatnie; przechowywanie danych w chmurze, a nie na fizycznym urządzeniu, które wówczas jest tylko narzędziem, to bardzo rozsądne wyjście, jednak pod jednym warunkiem - zabezpieczenie musi być naprawdę trudne do złamania. System chmurowy umożliwia natychmiastowe odcięcie dostępu do danych w przypadku utraty fizycznego urządzenia bądź zdalnego zhakowania. Chmura umożliwia także robienie kopii zapasowych. Te powinno wykonywać się często i w miarę regularnie.

Szyfruj

Przeniesienie całej naszej pracy do chmury jest na ten moment niemożliwe. Dlatego warto zapewnić ochronę dysków służbowych komputerów za pomocą szyfrowania znajdujących się na nich danych.

- Szyfrowanie danych odgrywa niezwykle ważną rolę w kontekście bezpieczeństwa każdej organizacji. Dostępne w Polsce rozwiązania szyfrujące, w szczególności DESlock+, chroni nasze dane poprzez pełne szyfrowanie dysku (FDE) - uważa Mikołaj Sikorski, product manager DESLock+ w firmie DAGMA Bezpieczeństwo IT.

- Co oznacza to dla polskiego przedsiębiorcy? Dzięki takiemu rozwiązaniu szyfrowane są całe zasoby naszego dysku wraz z obszarami, w których nie znajdują się na razie żadne informacje, ale znajdą się w przyszłości. Tego typu zabezpieczenie jest bardzo istotne dla przedsiębiorców, ponieważ na przykład w sytuacji kradzieży laptopa zapewni, że nikt niepowołany nie dostanie się do naszych danych.

Zdaniem eksperta szyfrowanie jest najlepszym antidotum na kryzysy, które mogą wiązać się z nieumyślnym naruszeniem przepisów RODO. - Zostało one wskazane w motywie 83 preambuły do RODO, jako jedna z nielicznych wymienionych technologii, która umożliwia zachowanie odpowiedniego poziomu bezpieczeństwa - zauważa Mikołaj Sikorski. - Ważnym elementem w kontekście unijnego rozporządzenia jest również fakt wykazania, że nasz komputer - w sytuacji zagrożenia danych osobowych - został we właściwy sposób zabezpieczony.

Larum nad laptopem

Przypomnijmy: jesteśmy na stacji benzynowej, na której pracownik korporacji stracił laptopa, w kilkanaście sekund zabranego z tylnego siedzenia niezamkniętego pojazdu. Co dalej?

- W przytoczonym przykładzie kradzieży laptopa, na którym znajdowały się dane osobowe, musimy każdorazowo zgłosić taki incydent organowi nadzorczemu – UODO (Urząd Ochrony Danych Osobowych), chyba że jesteśmy w stanie udowodnić, że zaistniały incydent nie naraził danych osobowych na ich wyciek - mówi Mikołaj Sikorski. - Z pomocą przychodzi nam konsola centralnego zarządzania DESlock+, w której, w przypadku takiego incydentu, możemy udowodnić, że skradziony laptop był zaszyfrowany, że odpowiedzialny za to proces został wykonany w 100% i tym samym nie musieliśmy zgłaszać tego incydentu.

Kompleksowe rozwiązanie

Dlaczego firmy w ogóle powinny inwestować w szyfrowanie danych, gdy mają do dyspozycji darmowe rozwiązania?

- Polscy przedsiębiorcy powinni inwestować w szyfrowanie danych nie tylko ze względu na kwestie spełnienia wymogów RODO, ale również, by usprawnić ich codzienną pracę - zwraca uwagę Mikołaj Sikorski. - Jest to możliwe dzięki kluczom szyfrującym, których użycie nie wpływa w żadnym stopniu na pracę pracowników. Sprawiają, że praca z danymi zaszyfrowanymi lub nie, praktycznie niczym się między sobą nie różni. Transparentne przypisywanie użytkownikom kluczy szyfrujących daje możliwość administratorom kontroli nad tym, do których danych użytkownik ma dostęp, a do których nie.

Ekspert zaznacza, że zdarzają się sytuacje szczególne: - Jeżeli w ręce pracownika trafi pendrive, z którego nie powinien korzystać, będzie on dla niego całkowicie nieczytelny. Jeżeli jednak ten sam dysk przenośny trafi do osoby, która ma uprawnienia dostępu, to DESlock+ sam zidentyfikuje, że użytkownik posiada właściwy klucz szyfrujący i automatycznie udzieli zezwolenia do korzystania z danych, bez potrzeby dodatkowej autoryzacji, na przykład przez hasło - tłumaczy Mikołaj Sikorski. - Dzięki temu uzyskujemy bardzo wysoki poziom bezpieczeństwa przy utrzymaniu prostoty użytkowania niezaszyfrowanych nośników wymiennych. Analogiczna sytuacja będzie mieć miejsce dla pojedynczych plików lub dla współdzielonych między użytkownikami archiwów, znajdujących się na naszych zasobach sieciowych.

PODPIS ELEKTRONICZNY I CERTYFIKATY SSL

Paweł Musiał
redaktor Interaktywnie.com

redakcja@interaktywnie.com

5

Deklaracje podatkowe i do ZUS bez wychodzenia z domu, zawieranie umów na odległość czy elektroniczne podpisywanie faktur, albo nawet dokumentacji medycznej. Sprawdziliśmy, jak działa podpis elektroniczny, rozwiązanie stosowane powszechnie w Europie Zachodniej, w Polsce zdobywające coraz więcej klientów. Przyjrzeliśmy się także certyfikatom SSL. Podpowiadamy, kto powinien w nie zainwestować i ile to kosztuje.

Od kilkunastu lat i w Polsce nie trzeba już wszystkich dokumentów podpisywać odręcznie. Bezpieczny podpis elektroniczny jest równoważny pod względem skutków prawnych z podpisem własnoręcznym.

Jak podaje na swoich stronach internetowych Ministerstwo Gospodarki, można go używać do:

- elektronicznego podpisywania umów i dokumentów w obrocie handlowym i cywilno-prawnym,
- w korespondencji z urzędami oraz do podpisywania pism i decyzji administracyjnych przez urzędy,
- podpisywania faktur elektronicznych,
- zarejestrowania działalności gospodarczej (CEIDG),
- składania deklaracji celnych i podatkowych,
- zgłoszeń ubezpieczenia społecznego (również system PUE ZUS),
- podpisywania wniosków do Krajowego Rejestru Sądowego,
- podpisywania raportów dla Generalnego Inspektora Informacji Finansowej,

- korespondencji z Urzędem Ochrony Danych Osobowych,
- podpisywania dokumentacji medycznej.

Ile to kosztuje?

Aby móc składać na dokumentach bezpieczny podpis elektroniczny trzeba liczyć się ze stałymi, rocznymi kosztami. Najpierw należy kupić zestaw z odpowiednim urządzeniem, którego koszt wynosi około 300 zł brutto.

W kolejnych latach wystarczy już tylko odnawiać abonament, dokładnie tak, jak w przypadku np. domeny internetowej. Koszt to około 120 zł.

Sam podpis zwykle jest składany przy pomocy specjalnej karty procesorowej lub tokena USB oraz oprogramowania służącego. Zestawy do składania bezpiecznego podpisu elektronicznego można kupić w Polsce tylko w pięciu, certyfikowanych przez państwo firmach: Unizeto - Certum, PWPW, Krajowa Izba Rozliczeniowa, CenCert oraz Euro Cert.

Są oczywiście platformy, które oferuję bardziej kompleksowe usługi, ale są one oparte właśnie na produkcie bazowym dostarczonym przez wyżej wymienione firmy.

Warto wiedzieć, że zakup podpisu elektronicznego na potrzeby działalności gospodarczej może być zakwalifikowany jako koszt uzyskania przychodu w ramach prowadzonej działalności gospodarczej.

Test podpisu przeprowadzony przez Interaktywnie.com

Przetestowaliśmy certyfikat Unizeto sprzedawany pod marką Certum. Zarówno urządzenie, jak i sam podpis można zamówić na stronach internetowych producentów. Certum zbudowało do tego bardzo prosty moduł sklepu internetowego. Podobne przygotowali wszyscy dostawcy tego rozwiązania.

Do testów wybraliśmy najprostsze zestaw, z modemem USB. Paczka od Unizeto przyszła już po kilku dniach, a w niej karta kryptograficzna (niemal identyczna z SIM do telefonu), czytnik podłączany do komputera przez USB oraz płyta z oprogramowaniem.

O ile instalacja czytnika na komputerach z systemem Windows okazała się banalnie prosta, na komputerach Apple nie było już tak łatwo - tu musieliśmy skorzystać ze wsparcia infolinii Certum, która okazała się bardzo pomocna i skuteczna.

Niestety, zakup zestawu, zainstalowanie oprogramowania i podłączenie modemu to dopiero połowa drogi do podpisywania dokumentów podpisem elektronicznym. Aby móc korzystać z tego rozwiązania należy najpierw uzyskać certyfikat i wgrać go na kartę kryptograficzną. W zestawie, który otrzymujemy go nie ma i być nie może - musi zostać dopiero dla nas przygotowany i uwiarygodniony tak, aby nie było najmniejszych wątpliwości, że należy właśnie do nas, a nie do kogoś, kto się pod nas podszywa. Przecież będziemy nim sygnować najważniejsze dokumenty, dokładnie tak, jak własnoręcznym.

Kiedy zainstalujemy oprogramowanie, czytnik z kartą, będziemy mieć możliwość wygenerowania dokumentów, w tym tych opisujących, jakie dane ma zawierać certyfikat. Te trzeba będzie wydrukować i dostarczyć do wystawcy podpisu. Można to zrobić osobiście w punkcie weryfikacji tożsamości Unizeto w Warszawie, bądź pocztą.

W tym drugim przypadku należy jednak wcześniej dokonać weryfikacji swojej tożsamości i podpisu u notariusza lub w wybranym punkcie partnerskim - to koszt około 20 zł. Po wysłaniu dokumentów trzeba jeszcze poczekać na przygotowanie certyfikatu. Kiedy będzie on, gotowy otrzymamy potwierdzenie na podany przy wypełnianiu formularzy email. Wówczas wystarczy już tylko dopełnić kilku formalności rejestracyjnych na stronie www operatora, by zacząć korzystać z podpisu. Samo jego użytkowanie jest już banalnie proste. Wystarczy w specjalnej aplikacji wybrać dokumenty, które chce się opatrzyć podpisem i kliknąć „podpisz".

Rozwiązanie dostarczane przez Unizeto/Certum jest sprzęgnięte z systemem eDeklaracje oraz programem Płatnik, co umożliwia sprawne składanie deklaracji podatkowych, ZUS oraz innych dokumentów, znacznie pomagając w prowadzeniu żmudnych procesów w księgowości.

Jak kupić podpis kwalifikowany

Kwalifikowany podpis elektroniczny możesz kupić u jednego z dostawców - firm nadzorowanych przez Ministerstwo Cyfryzacji. Aktualną listę tych firm znajdziesz na stronie Narodowego Centrum Certyfikacji. Możliwe jest także korzystanie e-podpisu wydanego przez kwalifikowane podmioty w dowolnym kraju UE.

Usługi certyfikacyjne mają charakter komercyjny, a wysokość opłat określają podmioty świadczące te usługi. Ceny zestawów różnią się w zależności od

długości ważności certyfikatu (rok lub dwa lata) i rodzaju urządzenia do składania podpisu elektronicznego (czytnik kart usb, token usb lub pcmcia). Możliwy jest zakup karty z certyfikatem bez czytnika, albo samych czytników i dodatkowych licencji na oprogramowanie. Kupujący zawiera z kwalifikowanym podmiotem umowę subskrybencką, której warunki określa polityka certyfikacji lub kodeks postępowania certyfikacyjnego.

Rodzaje podpisów elektronicznych

Podpis elektroniczny, potocznie zwany zwykłym, to narzędzie służące do potwierdzenia tożsamości autora dokumentu przesyłanego drogą elektroniczną. Ma on postać danych elektronicznych, które pozwalają jednoznacznie wskazać osobę składającą podpis elektroniczny. Stosowany jest m.in. do podpisywania dokumentów w systemach bankowych i niektórych wniosków w systemie e-government.

Trzeba go odróżnić od bezpiecznego podpisu elektronicznego, który jest przyporządkowany wyłącznie do osoby składającej ten podpis i sporządzany przy pomocy tylko jej dostępnych bezpiecznych urządzeń i danych. Użycie bezpiecznego podpisu elektronicznego daje gwarancję, że wszystkie zmiany wprowadzone w dokumencie po jego podpisaniu będą od razu widoczne.

W odróżnieniu od zwykłego podpisu elektronicznego, podpis bezpieczny musi mieć określoną w przepisach strukturę oraz powstawać przy użyciu odpowiednich algorytmów kryptograficznych (tzw. kluczy prywatnych i publicznych).

Certyfikat niekwalifikowany służy natomiast do potwierdzenia tożsamości użytkownika zwykłego podpisu elektronicznego w różnych systemach informatycznych. Znajduje zastosowanie m.in. przy szyfrowaniu wiadomości i plików przesyłanych pocztą elektroniczną. Może być wystawiany przez różne podmioty.

Zalety stosowanie podpisu elektronicznego

Podpis elektroniczny gwarantuje oszczędność czasu i pieniędzy oraz wygodę w prowadzeniu biznesu. Dzięki jego zastosowaniu, możliwe jest zawieranie umów na odległość, co znacząco zwiększa sprzedaż. Jest uznanym prawnie w UE sposobem akceptacji treści i składania oświadczeń woli, a w szczególności musi zostać wzięty pod uwagę w postępowaniach sądowych. Dzięki realizacji usługi podpisu elektronicznego poprzez usługę zaufania - zaufaną stronę trzecią - transakcje elektroniczne zyskują niezależnego obserwatora, który potwierdza tożsamość oraz czynności uczestników transakcji.

Michał Tabor
Autenti.com

Certyfikat kwalifikowany to z kolei certyfikat zawierający dane pozwalające jednoznacznie wskazać użytkownika bezpiecznego podpisu elektronicznego. Jest on wystawiany wyłącznie osobom fizycznym przez kwalifikowane podmioty świadczące usługi certyfikacyjne - w Polsce pięć firm akredytowanych przez państwo. Są to kwalifikowane podmioty świadczące usługi certyfikacyjne - firmy oferujące podpis elektroniczny spełniające wymogi bezpieczeństwa określone w ustawie. Podmioty takie są wpisane do rejestru Ministerstwa Gospodarki prowadzonego przez Narodowe Centrum Certyfikacji.

Od 1 lipca 2016 r. obowiązuje Rozporządzenie Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS). Nowa regulacja wprowadziła jednolite w całej Unii Europejskiej podejście do świadczenia usług zaufania, których zadaniem jest zapewnienie bezpieczeństwa transakcji elektronicznych realizowanych w internecie.

Rozporządzenie wprowadziło także powszechnie rozpoznawalne mechanizmy identyfikacji elektronicznej (eID), umożliwiające jednoznaczną weryfikację tożsamości użytkowników usług online. Oprócz podpisów elektronicznych i znakowania czasem wprowadziło ono także możliwość stosowanie także tzw. pieczęci elektronicznych, doręczeń elektronicznych, zabezpieczenia stron WWW oraz walidacji i konserwacji pieczęci i podpisów elektronicznych.

Definicje podpisu elektronicznego i kwalifikowanego podpisu elektronicznego zawarte w Rozporządzeniu eIDAS obowiązuje bezpośrednio na terytorium Polski. W prawie polskim pojęcie podpisu elektronicznego wprowadzone zostało w uchylonej ustawie z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. z 2013 r. poz. 262, z późn. zm). Zgodnie z art. 3 pkt 1 tej ustawy podpis elektroniczny stanowiły dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny. Od 7 października 2016 obowiązuje natomiast ustawa z 5 września 2016 o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2016 r. poz. 1579). Zgodnie z nią dokument opatrzony podpisem elektronicznym może być – przy spełnieniu dodatkowych przesłanek – równoważny pod względem skutków prawnych dokumentowi opatrzonemu podpisem własnoręcznym.

Do 6 października 2016 r. podpis elektroniczny mógł być uznany za równoważny podpisowi własnoręcznemu, jeśli spełniał warunki umożliwiające uznanie go za podpis elektroniczny bezpieczny. Zgodnie z uchyloną ustawą bezpieczny podpis elektroniczny to podpis elektroniczny, który:

- jest przyporządkowany wyłącznie do osoby składającej ten podpis,
- jest sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych

urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego,

- jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna.

Skutki prawne związane ze złożeniem oświadczenia woli w formie elektronicznej opatrzonego kwalifikowanym podpisie elektronicznym określa art. 781 § 2 kodeksu cywilnego. Zgodnie z tym przepisem oświadczenie woli złożone w formie elektronicznej jest równoważne z oświadczeniem woli złożonym w formie pisemnej.

Profil zaufany do załatwiania spraw urzędowych

Profil Zaufany (eGO) to bezpłatna metoda potwierdzania tożsamości obywatela w systemach elektronicznej administracji. Nie zastępuje kwalifikowanego podpisu elektronicznego w kontaktach biznesowych, ale działa jak odręczny podpis w przypadku kontaktu z wieloma instytucjami państwowymi. Możesz dzięki niemu wysyłać przez internet dokumenty i wnioski do różnych urzędów (np. wnieść podanie, odwołanie, skargę), bo potwierdza tożsamość.

Podpis potwierdzony profilem zaufanym, podobnie jak kwalifikowany podpis elektroniczny, skutecznie zastępuje w kontaktach z podmiotami publicznymi podpis własnoręczny. Jest ważny (wywołuje skutki prawne), jeżeli został utworzony lub złożony w okresie ważności tego profilu (3 lata). Każdy obywatel może posiadać tylko jeden Profil Zaufany.

Co załatwisz dzięki Profilowi Zaufanemu? Złożysz wniosek o wydanie dowodu osobistego, sprawdzisz, czy dowód osobisty jest gotowy do odbioru, sprawdzisz swoje punkty karne, złożysz wniosek o świadczenie 500+, złożysz deklaracje podatkowe PIT-WZ, PIT-OP, PIT-37 i PIT-38 na portalu podatkowym, wystąpisz o Europejską Kartę Ubezpieczenia Zdrowotnego, złożysz wniosek o rejestrację działalności gospodarczej, wyślesz pismo do podmiotu publicznego i załatwisz wiele innych spraw urzędowych wymagających potwierdzenia tożsamości.

Profil Zaufany można założyć w urzędach miejskich lub w poniższych serwisach bankowych: PKO BP, ING Bank Śląski, Bank Millennium, Inteligo, Bank Pekao, mBank, BZWBK oraz w serwisie Envelo.

Platformy do zawierania umów i korzystania z podpisów

W 2016 r. światowy rynek podpisu elektronicznego wynosił 631,5 mln dolarów. Analitycy spodziewają się, że rynek ten będzie wzrastał w ujęciu CAGR o 26,40% w latach 2017-2025 i osiągnie 4,98 mld dolarów przed końcem roku 2025.

- Idea depapieryzacji w organizacjach to już nie moda, a paląca potrzeba. Nasze rozmowy o e-podpisach w firmach nie kończą się pytaniem "czy?", ale "kiedy u nas?" - mówił w listopadzie 2017 roku Interaktywnie.com Grzegorz Wójcik, CEO Autenti, firmy która pozyskała wówczas finansowanie na rozwój swojej platformy do autoryzacji dokumentów i zawierania umów przez internet. - Dzięki wsparciu Innovation Nest i Black Pearls VC, mamy szansę wykorzystać właściwy moment, aby znacząco przyspieszyć, realizując ambitne plany ekspansji za granicą oraz podnosząc standardy bezpieczeństwa danych. To właśnie kompetencje, doświadczenie i międzynarodowe kontakty naszych partnerów są kluczowe dla dynamicznego rozwoju Autenti - tłumaczył Wójcik pozyskanie finansowania w wysokości 6,3 miliona złotych od funduszy Innovation Nest i Black Pearls VC.

Rozwój podpisu elektronicznego umożliwił właśnie usprawnienie procesów biznesowych w firmach. Teraz mogą one podpisywać umowy przez internet, także z osobami fizycznymi. A to dzięki własnym rozwiązaniom lub specjalistycznym, gotowym platformom, które oferują swoje usługi także w Polsce. Przykładem jest właśnie Autenti. Co daje użytkownikom? Wygodny i prosty interfejs, tak na komputerze, jak i na urządzeniu mobilnym, szybką i prostę funkcję podpisywania dokumentu online, akceptację treści jednym kliknięciem bez zakładania konta na platformie, logowania się czy dodatkowych opłat.

Jak to działa? Autenti przekonuje, że wystarczy założyć konto:
- Zakładasz konto podając swój adres email lub korzystasz z uproszczonego logowania (Google, Microsoft, Facebook) - czytamy na stronach platformy. - Dokumenty podpisujesz online w imieniu własnym lub w imieniu organizacji, którą reprezentujesz – korzystasz wówczas z profilu firmowego przypisanego do Twojej

Zalety korzystania z platformy Autenti

Platforma Autenti dostarcza kompleksową usługę składania podpisu elektronicznego, w łatwy i wygodny sposób prowadzi użytkownika przez proces podpisywania oraz zabezpiecza dowody z realizowanej online transakcji. To wyjątkowe połączenie podpisu elektronicznego, innowacyjnej technologii oraz środowiska prawnego w oparciu o przepisy europejskie i krajowe. Z usługi korzystać można nie tylko w relacjach z partnerami biznesowymi, ale również z konsumentami i pracownikami. To pierwsze tego typu rozwiązanie w Polsce i jedno z nielicznych w Europie.

Michał Tabor
Autenti.com

tożsamości. Jeśli potrzebujesz dodatkowej pewności, że dokument zostanie podpisany przez właściwą osobę, korzystasz z możliwości wysłania mu niepowtarzalnego kodu SMS. Możesz zamówić również opcję weryfikacji odbiorcy za pomocą konta bankowego. Potwierdzeniem złożenia podpisów online jest certyfikat Autenti. To cyfrowy dowód na to, że na platformie, zaufanej stronie trzeciej, spotkały się strony i zawarły porozumienie. Zawiera wszystkie, niezbędne informacje o przebiegu procesu i jego stronach. Potwierdza też integralność i autentyczność podpisanych plików.

W Autenti można podpisać dokumenty dowolnej treści. Bez względu na rodzaj pliku, w którym zostały zapisane. Dokument tekstowy, obraz lub skoroszyt – wystarczy przeciągnąć na platformę i nadać do odbiorcy. Pliki bindowane są do formatu .pdf i wyświetlane na urządzeniu odbiorcy w wygodnej formie, bez względu na ilość nadanych stron. Platforma oferuje możliwość stworzenia własnego obiegu dokumentów w ramach procesu podpisywania.

Certyfikaty SSL

Prawdziwą rewolucję w internecie przeprowadziło Google, kiedy ogłosiło, że strony internetowe bez słynnego https czyli zainstalowanego certyfikatu SSL będzie przy pozycjonowaniu traktował gorzej. Następnie przeglądarka Chrome zaczęła ostrzgać przed nimi, a w ślad za nimi poszła Mozilla Firefox.

W roku 2018 doszło do tego jeszcze RODO, które na właścicielach witryn, które w jakikolwiek sposób przetwarzają dane osobowe wręcz wymusza zainstalowanie certyfikatu. A chodzi przecież nawet o małe sklepy internetowe czy firmy zbierające zapisy na newsletter.

Dlaczego są aż tak istotne?

- Certyfikaty SSL są narzędziem zapewniającym ochronę witryn internetowych, a także gwarantem zachowania poufności danych przesyłanych drogą elektroniczną. Pełne bezpieczeństwo jest efektem zastosowania szyfrowania komunikacji pomiędzy komputerami. Certyfikaty SSL rejestrowane są na określoną nazwę domeny, zawierają informacje o właścicielu domeny, jego adresie itp. Dane te są zabezpieczone kryptograficznie i nie można ich samodzielnie zmienić - czytamy na stronach Certum.

Historia certyfikatów SSL sięga roku 1994, kiedy to firma Netscape stworzyła protokół Secure Socket Layer, służący do bezpiecznej transmisji zaszyfrowanego strumienia danych. Dzięki swojej skuteczności oraz prostej obsłudze i instalacji bardzo szybko znalazł on zastosowanie zwłaszcza przy zabezpieczaniu transakcji realizowanych w bankowości elektronicznej, podczas aukcji internetowych oraz w systemach płatności online.

Tymczasem tylko niewielki odsetek użytkowników internetu ma świadomość, w jaki sposób komunikują się i wymieniają ze sobą dane komputery będące on-line. Upraszczając w dużym stopniu – cała procedura odbywa się za pomocą protokołów, czyli swego rodzaju języka.

- Zasada jego działania pozostaje w dużej mierze poza gestią każdego użytkownika internetu - pisze na swoich stronach internetowych Certum. - O ile jest to sytuacja wygodna, o tyle rodzi szereg zasadniczych pytań o naturę bezpiecznego korzystania z zasobów sieci. Jednym z najpowszechniejszych sposobów zabezpieczenia transmisji danych w internecie jest protokół SSL/TLS. Zastosowanie technologii kryptograficznych oraz certyfikatów klucza publicznego, nazywanych w tym przypadku certyfikatami SSL, umożliwia nawiązanie szyfrowanego połączenia pomiędzy serwerem a łączącym się z nim komputerem użytkownika. Protokół SSL/TLS gwarantuje bezpieczeństwo przez wykorzystanie technologii Infrastruktury Klucza Publicznego (PKI). W trakcie nawiązywania połączenia tworzony jest klucz symetryczny, który będzie wykorzystany do zabezpieczenia wymiany danych pomiędzy stronami w ramach utworzonej sesji. Dla porównania zwykłego protokołu z protokołem SSL/TLS wyobraźmy sobie sytuację, w której płacąc kartą kredytową w sklepie internetowym, informujemy wszystkich innych kupujących jaki jest nasz numer karty, data ważności oraz kod CVS, pozwalając tym samym dowolnie korzystać z naszych środków. W przypadku zastosowania połączeń szyfrowanych nikt nie ma możliwości pozyskania tak ważnych danych.

Certyfikaty SSL są niezbędne dla wszystkich podmiotów udostępniających swoje usługi za pośrednictwem internetu lub sieci lokalnych w celu zapewnienia:

- bezpieczeństwa – szyfrowanie połączeń,
- bezpiecznego przekazywanie danych osobowych,
- wiarygodności – potwierdzenie tożsamości strony WWW lub serwera w internecie,
- zaufania – świadczenie usług zgodnie ze światowymi standardami.

W Polsce jedynie CERTUM Powszechne Centrum Certyfikacji wydaje zaufane certyfikaty SSL.

Potrzebujesz SSL, jeśli:

- pobierasz i przetwarzasz dane osobowe przez internet,
- prowadzisz sprzedaż w internecie,
- publikujesz informacje wymagające uwiarygodnienia,

- prowadzisz aktywną działalność w internecie,
- przekazujesz swoim współpracownikom i partnerom poufne informacje za pośrednictwem sieci.

Certyfikat SSL ma zastosowanie dla:

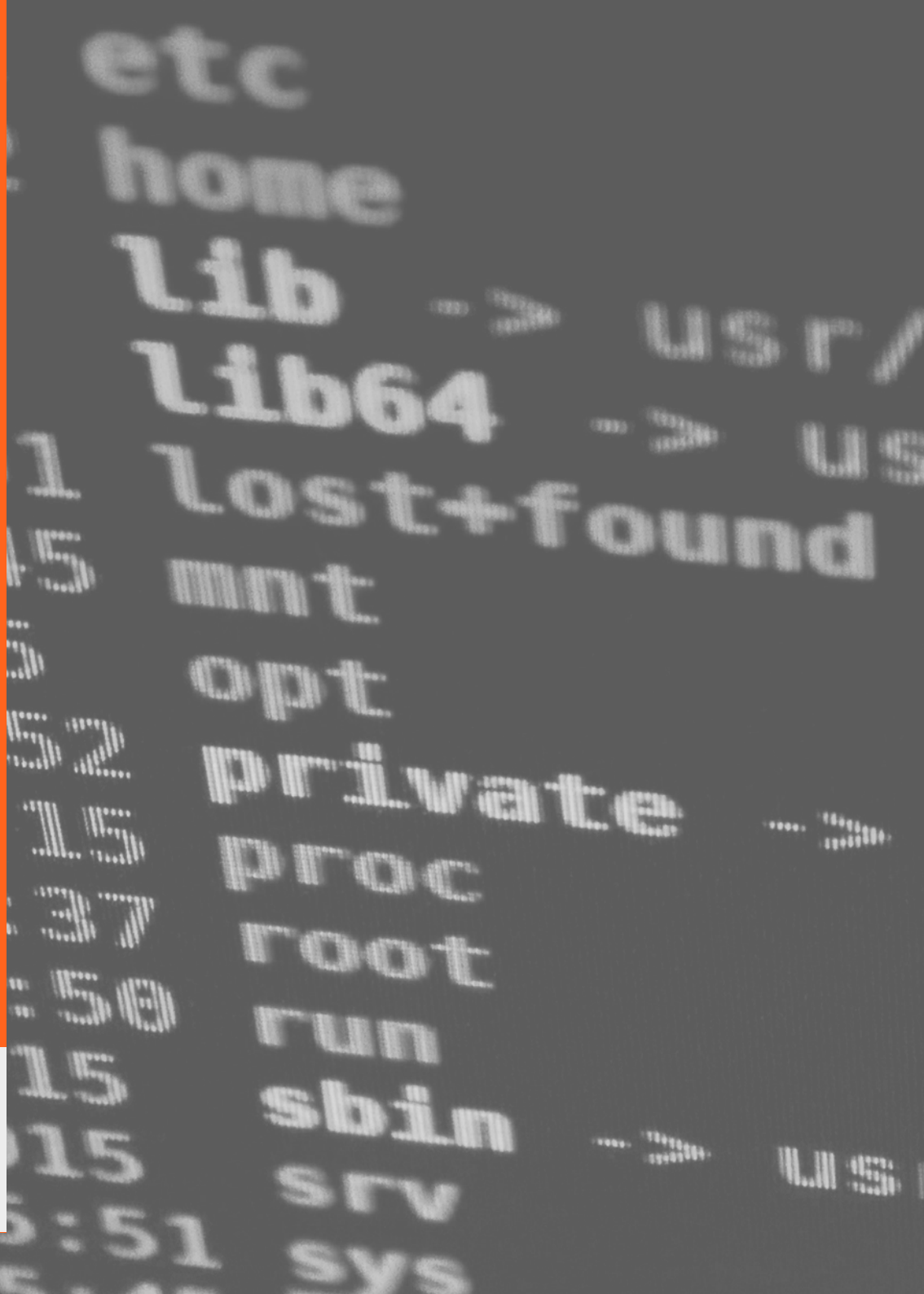
- banków i instytucji finansowych,
- sklepów internetowych (e-commerce),
- serwisów aukcyjnych,
- stron internetowych administracji publicznej
- serwisów internetowych przetwarzających i udostępniających dane na temat zdrowia pacjentów,
- biznesowych serwisów internetowych i portali korporacyjnych,
- serwisów internetowych szkół i uczelni,
- serwerów pocztowych i serwerów baz danych,
- aplikacji typu klient-serwer,
- komunikacji w ramach sieci intranet i ekstranet,
- zabezpieczenia serwerów udostępniających pliki (SFTP).

źródło: Certum

PRACOWNIK TO NAJSŁABSZE OGNIWO.

ZAGROŻENIE SIEDZI PRZY BIURKU

Katarzyna Pilawa
specjalista ds. PR i marketingu w firmie DAGMA Bezpieczeństwo IT



6

Rynek szkoleń przeżywa prawdziwy boom. Nowe przepisy, określane jako zmiana filozofii podejścia do danych osobowych, budzą respekt i niepokój. Bo tak naprawdę nie wiadomo, jak nowe prawo będzie funkcjonowało w praktyce. Tymczasem, najrozsądniejszym krokiem jest przeanalizowanie wszelkich wariantów zdarzeń z punktu widzenia każdego stanowiska w firmie i uporządkowanie zasad - nowe przepisy RODO wydają się demoniczne, póki nie są zestawione z naszym biznesem i codziennymi zadaniami.

Zestaw informacji o tym, jak przetwarzane są dane osobowe w serwisach, do czego są potrzebne, jak są chronione i jakie prawa ma ich właściciel, daje gwarancję wszystkim stronom i zapewnia jasność zasad dotyczących naszej prywatności m.in. może doprowadzić do ukrócenia oszustw i nadużyć.

Szkolenia z zakresu ochrony danych są potrzebne i przydatne, jednak nie mogą odbywać się w oderwaniu od konkretnych metod funkcjonowania firmy. Informacje o przepisach, przekazane pracownikom, muszą odnosić się do konkretnych działań operacyjnych.

RODOodporność

Jedynie prześledzenie studiów przypadków może dać wyobrażenie o tym, czym w praktyce może być działanie zasad narzuconych literą prawa. I tu faktycznie przydadzą się szkolenia, których istotą rzeczy będzie dzielenie się doświadczeniem, jak innowację widzi się zza poszczególnych biurek. Pracownicy zazwyczaj mają jednakowy dostęp do zabezpieczonych i wewnętrznych zasobów firmowych. Do wycieku danych może dojść w przypadku wykonywania codziennych obowiązków i nieumyślności, a nie nieodpowiednich zabezpieczeń.

Zatem zasadne będzie przeprowadzenie, na użytek edukacji pracowników w zakresie obwiązujących przepisów o ochronie danych, analizy praktycznej, uświadamiającej jakich mechanizmów i czynności należy w praktyce unikać.

W każdych okolicznościach może dojść do kradzieży danych z systemu IT przez hakera. Wystarczy wyobrazić sobie sytuację, w której dochodzi do wysyłki e-maila z adresami klientów w polu DW. Dane może wykraść tymczasowy pracownik, albo w ich posiadanie może wejść złodziej, który połakomi się na źle strzeżony i źle zabezpieczony firmowy laptop.

Zatem, aby zyskać pełną RODOodporność, firmy muszą nieustająco szkolić pracowników w zakresie najlepszych praktyk bezpieczeństwa, prowadzić audyty i aktualizować zasady dotyczące przetwarzania danych.

- Unijne rozporządzenie nakazuje przedsiębiorcom „wdrożenie odpowiednich środków technicznych i organizacyjnych" w celu zapewnienia bezpieczeństwa informacji. Co to naprawdę dla nich znaczy? O tyle, o ile „środki techniczne" to po prostu stan zabezpieczeń na poziomie fizycznym i sieciowym, który należy ustalić (audyt bezpieczeństwa informacji - rekonesans), zweryfikować (testy penetracyjne - kontrolowany atak) i zaktualizować (wdrażając np. rozwiązania szyfrujące czy backup'owe), tak „środki organizacyjne" są dużo trudniejszym do zdefiniowania pojęciem - tłumaczy Jarosław Mackiewicz, kierownik zespołu ds. audytów w firmie DAGMA. - Kryją się pod nim zarówno takie elementy jak właściwe procedury i dokumentacja, do których możemy zaliczyć Politykę Bezpieczeństwa Informacji, czy rejestr upoważnień do przetwarzania danych osobowych, jak i dbanie o poziom świadomości zagrożeń wśród pracowników.

Zdaniem eksperta, powołującego się na raport IBM X-Force Threat Intelligence Index, większość zagrożeń płynie z wnętrza organizacji, a rosnącym problemem są incydenty wywołane przez nieświadomych użytkowników.

- Tutaj z pomocą przychodzą rozwiązania takie jak testy socjotechniczne, które polegają na przeprowadzeniu prowokacji mającej na celu sprawdzenie reakcji pracowników na próby wyłudzenia informacji. Warto też zainwestować w dodatkowe szkolenia, które pokażą pracownikom jak w praktyce chronić dane firmy i jej klientów, zaczynając od wysyłania mailingu do większych grup z użyciem ukrytej kopii, poprzez „politykę czystego biurka", aż po właściwe korzystanie z używanego w organizacji oprogramowania - wyjaśnia Jarosław Mackiewicz. - Tylko takie, całościowe podejście, pozwoli nam odpowiednio się zabezpieczyć, zarówno przed faktycznymi zagrożeniami, jak i potencjalnymi drakońskimi karami przewidzianymi w RODO.

Uczciwość i jasne intencje w zbieraniu i przetwarzaniu danych, kontrolowany i przemyślany proces przepływu danych w firmie i stałe podnoszenie świadomości pracowników w zakresie

traktowania wrażliwych zasobów - to najprostszy przepis na funkcjonowanie firmy zgodne z rozporządzeniem.

Straże na murach obronnych

Jednak transparentność to nie wszystko. Cyberświat, tak jak i rzeczywistość, nie jest bowiem dobrym, bezpiecznym miejscem. Wszędzie potrzebna jest czujność. W obliczu wartości, jaką stanowią dane, bardzo ważna jest gotowość do obrony przed zewnętrznym atakiem.

- Systemy informatyczne polskich firm są w różnym stopniu zabezpieczone, bardzo często trudne do złamania przez cyberprzestępców - zauważa Justyna Puchała, kierownik Autoryzowanego Centrum Szkoleniowego DAGMA. - Inaczej jest w przypadku pojedynczego pracownika organizacji, który ma dostęp do służbowego komputera, drukarek, faxu, loginu lub kodu PIN do drzwi wejściowych, baz danych, i który może zupełnie nieświadomie pomóc w przeprowadzeniu ataku na organizację przez cyberprzestępcę. Niezależnie od tego, w jakim dziale firmy pracuje, warto zadbać o jego wiedzę oraz świadomość z zakresu technik wykorzystywanych przez hakerów. Wyczulić na sytuacje, w których jego czujność może zostać uśpiona i narazić firmę na ogromne straty finansowe, np. w przypadku otwarcia zainfekowanego załącznika, który może sparaliżować pracę całej organizacji.

Trzymać rękę na pulsie

Justyna Puchała z z Centrum Szkoleniowego DAGMA zauważa, że szkolenia powinny obejmować wszystkie rodzaje niebezpieczeństw, jakie za przyczyną cyberprzestępców mogą pojawiać się w sieci, także i te najnowsze.

- Trzeba nieustannie szkolić z zakresu pułapek phishingowych, zagrożeń oraz najnowszych metod ataków, np. z tzw. „spear phishingu", który polega na przesłaniu wiadomości od rzekomego, zaufanego nadawcy. Uważam, że niestety w dzisiejszych czasach nie ma gwarancji, że nasza firma nie padnie ofiarą cyberataku - stwierdza Justyna Puchała. - Możemy za to, i powinniśmy, skutecznie się przed nim chronić. Tylko wiedza, świadomość pracowników oraz naprawdę dobre, przetestowane rozwiązania systemów IT dadzą nam najwyższy poziom ochrony.

RODO I BEZPIECZEŃSTWO DANYCH. 10 NAJWAŻNIEJSZYCH ZASAD

Paweł Musiał
redaktor Interaktywnie.com

redakcja@interaktywnie.com

7

Dane osobowe można pozyskiwać i wykorzystywać tylko w niezbędnym zakresie. Trzeba mieć na to wyraźną i świadomą zgodę każdej osoby, której one dotyczą. Ale najważniejsze jest to, że wszystkie trzeba pilnie chronić. Kto tego nie zrobi, a dojdzie do ich wycieku, może zostać ukarany ogromną grzywnę. Jej wysokość będzie zależała nie tylko o skali awarii, ale także od tego czy przedsiębiorca zrobił wszystko by do niej nie doszło. W Polsce już obowiązuje i jest egzekwowane RODO (GDPR) czyli unijne Rozporządzenie o ochronie danych osobowych.

RODO ujednoliciło zasady i nałożyło szereg obowiązków na przedsiębiorców. Weszo w życie 25 maja 2018 roku, a dzień wcześniej zaczęła obowiązywać powiązana z nim nowa Ustawa o ochronie danych osobowych. Jeszcze tego lata ma natomiast pojawić się specustawa, która ureguluje 200 innych, w których są regulacje dotyczące właśnie danych osobowych.

Przepisy RODO dotyczą przetwarzania danych osobowych – zarówno zapisanych w bazach danych, jak i rozproszonych na dowolnych nośnikach – w poczcie elektronicznej pracowników, w dokumentach zapisanych w komputerach, na serwerach lub zewnętrznych dyskach, a nawet list kontaktów w urządzeniach mobilnych.

W praktyce dotyczą więc każdej firmy, która działa na terytorium Unii Europejskiej, niezależnie od formy prawnej. Z obowiązków w zakresie ochrony danych muszą wywiązać się zarówno duże spółki, jak i osoby prowadzące działalność gospodarczą.

Odkryj potencjał narzędzi marketingu internetowego

semahead
tyle do odkrycia

Jesteśmy częścią

Google Partner · interia · BAUER · iab. · IZBA GOSPODARKI ELEKTRONICZNEJ

RODO a bezpieczeństwo

Wprowadzenie RODO zwiększyło świadomość z zakresu bezpieczeństwa IT głównie wśród właścicieli małych i średnich firm. Często utrzymywali oni serwisy swoich biznesów, nie inwestowali jednak w zabezpieczenia. Łatwość tworzenia formularzy kontaktowych sprawiła, że wiele organizacji zbierało dane osobowe swoich potencjalnych klientów - nie zabiegając jednak o właściwy poziom ich ochrony. Po wprowadzeniu regulacji możemy zaobserwować rosnące inwestycje w certyfikaty SSL, zapewniające bezpieczną transmisję danych.

Mateusz Pękala
securityinside.pl

Przedstawiamy 10 najważniejszych zasad RODO.

1. Należy pozyskać świadomą zgodę na przetwarzanie danych osobowych

Czym są dane osobowe? To nie tylko imię i nazwisko, numer pesel, ale także adres e-mail czy w niektórych przypadkach pliki cookies. Dane osobowe są w RODO zdefiniowane jako „informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Możliwa do zidentyfikowania osoba fizyczna to ta, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej."

Osoby zidentyfikowane to na przykład pracownicy albo kontrahenci przedsiębiorcy. Z kolei osoby niezidentyfikowane, których dane również muszą być chronione zgodnie z przepisami RODO, to kandydaci do pracy przysyłający CV, osoby, do których firma wysyła oferty handlowe, klienci sklepu internetowego lub użytkownicy zapisani na newsletter itd.

Zgodnie z RODO, osoby prawne nie mają danych osobowych, ale mają je ich pracownicy, będący osobami fizycznymi. Ogólny firmowy e-mail, na przykład kontakt@firmaX.pl, nie podlega więc ochronie, ale podlegają jej adresy imienne pracowników, czyli jankowalski@firmaX.pl.

Przetwarzanie danych osobowych oznacza jakiekolwiek czynności wykonywane na nich: gromadzenie, przechowywanie, usuwanie, opracowywanie lub udostępnianie.

Zgodnie z RODO **dane osób fizycznych przedsiębiorca można przetwarzać tylko w określonych warunkach i celach.** W przypadku danych zwykłych – czyli takich, które nie są związane ze sferą wrażliwą (przynależność rasowa, poglądy religijne lub polityczne, dane genetyczne lub biometryczne, orientacja seksualna itd.) – są to głównie następujące sytuacje:

- osoba, której dane dotyczą, **wyraziła zgodę na przetwarzanie swoich danych osobowych** w określonych celach,

- **przetwarzanie jest niezbędne do wykonania umowy,** której stroną jest osoba, której dane dotyczą, lub do podjęcia na jej żądanie działań zmierzających do zawarcia umowy,

- przetwarzanie jest niezbędne do **wypełnienia obowiązku prawnego ciążącego na administratorze,**

- przetwarzanie jest niezbędne do celów wynikających z **prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią**, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, w szczególności dziecka.

Przedsiębiorcy powinni pamiętać o tym, że to na nich – jako administratorach – ciąży obowiązek wykazania, że dysponują odpowiednią podstawą prawną do przetwarzania danych. Jeżeli podstawą jest zgoda użytkownika, to w razie wątpliwości administrator danych musi wykazać, że taką zgodę uzyskał. Dlatego jeśli firma buduje bazę danych użytkowników, to powinna archiwizować w niej dane o tym, kiedy i na jaki zakres przetwarzania wyraziła zgodę dana osoba.

Zgoda na przetwarzanie danych musi być wyrażona dobrowolnie i świadomie, w drodze jednoznacznej, potwierdzającej czynności.

RODO mówi wyraźnie: milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny oznaczać zgody. Użytkownik podający swoje dane na stronie internetowej musi wyrazić ją świadomie i czynnie, na przykład poprzez zaznaczenie odpowiedniego pola - tak zwanego checkboksa. Nie wystarczy zatem wyświetlić użytkownikowi informację o tym, że firma będzie przetwarzała jego dane osobowe, nie można też stosować checkboksów, które są domyślnie zaznaczone.

Jeśli dane osobowe są zbierane w różnych celach, to przedsiębiorca musi pozyskać osobne zgody na każdy z nich. Przykładowo, jeśli chcemy rejestrować użytkowników z zamiarem wykorzystania ich danych do celów marketingowych oraz w celu opracowywania danych, powinno być to zapisane w odrębnych formułach zgód, które zostaną wyświetlone obok zgody na przetwarzanie danych. Użytkownik powinien zaznaczyć każdą z nich z osobna.

2. Trzeba dać możliwość usunięcia danych osobowych

Osobie, której dotyczą dane osobowe, w każdym momencie przysługuje prawo cofnięcia zgody na ich przetwarzanie. RODO mówi o tym, że odwołanie zgody powinno być co najmniej tak samo łatwe, jak jej udzielenie. Jeśli użytkownicy strony internetowej

przekazują dane osobowe podczas wypełnienia formularza rejestracyjnego, na przykład zapisując się na newsletter albo biorąc udział w konkursie, to powinni móc cofnąć zgodę tą samą drogą.

Administrator ma obowiązek usunąć dane niezwłocznie, ze wszystkich nośników, na których były przechowywane. Dotyczy to nie tylko baz danych, ale także wszelkich innych miejsc, w których są one zapisywane – poczty elektronicznej, zestawień w plikach excel itd. Przedsiębiorcy powinni zadbać o wdrożenie rozwiązań informatycznych, które pozwolą na skuteczne usuwanie danych na żądanie osoby, której one dotyczą.

Administratorzy danych mają obowiązek udzielania na życzenie właściciela danych informacji o tym, jakie jego dane przetwarzają, w jakim celu i zakresie, jakim innym podmiotom je przekazują itd. Muszą też sprostować nieprawidłowe dane na wniosek osoby, której one dotyczą.

3. Nie można zbierać za dużo danych

RODO mówi, że dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Przedsiębiorca może zbierać i przetwarzać tylko takie informacje, które są niezbędne do świadczenia usług klientom. Nie może gromadzić danych nadmiarowo, na przykład po to, by wykorzystać je w przyszłości, jeśli nie są mu one potrzebne do realizacji usługi.

Zgodnie z regułą **privacy by default** (prywatność w ustawieniach domyślnych) RODO pozwala przetwarzać dane tylko w minimalnym zakresie, zarówno jeśli chodzi o rodzaj danych, jak i czas ich przechowywania: „Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności."

Przykładowo, przedsiębiorca prowadzący sklep internetowy w celu realizacji zamówienia może przetwarzać tylko te dane, które są niezbędne do jego obsługi. Na ogół jest to imię i nazwisko, adres dostawy, e-mail i numer telefonu klienta. Dane te mogą być wykorzystane tylko do realizacji zamówienia. Jeśli firma chciałaby wykorzystywać je w celach marketingowych, do wysyłania newslettera z promocjami, to odrębnie musi pozyskać na to zgodę, która powinna być wyrażona przez klienta świadomie i dobrowolnie.

RODO wymaga także **ograniczenia okresu przechowywania danych do minimum.** Jeśli podstawą przetwarzania jest umowa z klientem, wówczas jego dane mogą być przechowywane do czasu zakończenia świadczeń usług z niej wynikających oraz ewentualnego okresu roszczeń przysługujących stronom umowy. Co do zasady, okres ten nie powinien być dłuższy niż trzy lata, choć szczególne przepisy mogą stanowić inaczej.

Jeśli podstawą prawną jest zgoda właściciela danych, to przedsiębiorca może przetwarzać je do czasu jej odwołania.

Aby zapobiec przechowywaniu danych osobowych dłużej, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu.

4. W chwili projektowania systemu musisz myśleć o RODO

Zasada privacy by design (ochrona w fazie projektowania) mówi o tym, że na każdym etapie projektowania nowego systemu albo technologii, służących do przetwarzania danych osobowych, muszą być respektowane zasady ich ochrony. RODO definiuje ją tak: „Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania - wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą."

5. Nie można profilować danych bez wyraźnej zgody

Dane osobowe przetwarzane w celach marketingowych mogą podlegać profilowaniu. Ma to miejsce na przykład wtedy, gdy firma w sposób zautomatyzowany emituje użytkownikowi internetu reklamy w oparciu o jego zachowanie, zainteresowania lub wcześniej dokonane zakupy.

Przedsiębiorca może przetwarzać dane osobowe w ten sposób tylko w określonych przez RODO przypadkach:

a) jeśli uzyska wyraźną zgodę osoby, której dane dotyczą,

b) gdy jest to niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem,

c) gdy jest to dozwolone przez szczególne przepisy prawa.

6. Dane trzeba dobrze zabezpieczyć

RODO zobowiązuje administratorów i podmioty przetwarzające dane osobowe do ich odpowiedniego zabezpieczenia. W rozporządzeniu wymienione są następujące praktyki, które powinny być w tym celu stosowane:

a) szyfrowanie i pseudonimizacja danych,

b) ciągłe zapewnienie poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,

d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

RODO wymienia szereg potencjalnych ryzyk związanych z przetwarzaniem danych: przypadkowe lub niezgodne z prawem zniszczenie, utrata, modyfikacja, nieuprawnione ujawnienie lub nieuprawniony dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Narzędzie niezbędne dla IOD

W artykule 39 p. b) RODO poświęconym zadaniom Inspektora Ochrony Danych możemy przeczytać, że należą do nich m. in. działania zwiększające świadomość i szkolenia personelu uczestniczącego w operacjach przetwarzania. Z normy ISO 27001, zał. A.7.2.2 dowiadujemy się, że wszyscy pracownicy organizacji powinni otrzymać odpowiednie uświadamiające przeszkolenie. Z pomocą przychodzi platforma SecurityInside.pl. Wygodny system regularnych powiadomień pozwala zautomatyzować i oszczędzić czas IOD.

Mateusz Pękala
securityinside.pl

Każdy podmiot przetwarzający dane osobowe powinien samodzielnie określić, jakie konkretne środki zabezpieczenia danych powinien wdrożyć. Inne są zakresy i ryzyka związane z przetwarzaniem danych osobowych na przykład przez szpitale i sklepy internetowe. Te pierwsze przechowują dane wrażliwe pacjentów, w związku z tym do ich ochrony powinny podchodzić w sposób bardzo restrykcyjny. Rozporządzenie wskazuje, że w celu zapewnienia odpowiedniego stopnia bezpieczeństwa danych ich administrator powinien brać pod uwagę stan wiedzy technicznej, charakter, zakres, kontekst i cele przetwarzania, koszt wdrożenia oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

Aby zminimalizować ryzyka związane z ochroną danych osobowych, przedsiębiorca powinien zastosować odpowiednie środki techniczne, związane z używanymi systemami informatycznymi i infrastrukturą IT.

7. Należy rejestrować przetwarzanie danych

Administratorzy mają obowiązek prowadzić rejestr czynności przetwarzania. Obejmuje on firmy zatrudniające powyżej 250 pracowników, a mniejszych przedsiębiorców w kilku przypadkach:

jeśli przetwarzanie może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych – mogą to być na przykład dane kadrowe.

Rejestr czynności przetwarzania powinien zawierać:

a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych

b) cele przetwarzania;

c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;

d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;

e) gdy ma to zastosowanie, informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej;

f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;

g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Rejestr czynności może być prowadzony pisemnie, także w formie elektronicznej. Przedsiębiorca musi okazać go na żądanie organu nadzorczego.

8. Pracownicy firmy muszą mieć stosowne upoważnienia

Przedsiębiorca powinien upoważnić do przetwarzania danych osoby fizyczne, które mają do nich dostęp – swoich pracowników lub współpracowników.

W szczególnych przypadkach RODO zobowiązuje administratorów do wyznaczenia inspektora ochrony danych. Obowiązek ten obejmuje:

a) organy lub podmioty sektora publicznego,

b) firmy, których główna działalność polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę,

c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę

szczególnych kategorii danych osobowych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

Do tych podmiotów zaliczyć można szpitale, banki, firmy ubezpieczeniowe, firmy przetwarzające dane internautów w celu behawioralnego targetowania reklam.

9. Jeśli przekazujesz dane dalej, musisz podpisać umowę na ich powierzenie

Większości przedsiębiorców dotyczy ten fakt, choć niewielu zdaje sobie z tego sprawę. Tak jest na przykład wtedy, gdy firma dzierżawi serwer lub korzysta z hostingu oferowanego przez inny podmiot, albo gdy przekazuje dane kadrowe pracowników do zewnętrznego biura rachunkowego.

W takich sytuacjach administrator musi podpisać ze swoim partnerem umowę o powierzeniu przetwarzania danych. Powinna ona zobowiązać podmiot przetwarzający do tego, by:

a) przetwarzał dane osobowe wyłącznie na udokumentowane polecenie administratora,

b) zapewnił, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,

c) podejmował wszelkie środki zabezpieczenia danych osobowych wymagane przez RODO,

d) uzyskał zgodę administratora na podpowierzenie przetwarzania danych innemu podmiotowi, jeśli jest taka konieczność,

e) pomagał administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w RODO,

f) usunął lub zwrócił administratorowi wszelkie dane osobowe po zakończeniu świadczenia usług związanych z przetwarzaniem oraz usunął wszelkie ich istniejące kopie,

g) udostępniał administratorowi wszelkie informacje niezbędne do wykazania spełnienia jego obowiązków oraz umożliwił mu przeprowadzenie audytu.

10. Wycieki danych należy zgłaszać

Każda firma przetwarzająca dane osobowe jest narażona na incydenty bezpieczeństwa, takie jak utrata lub zniszczenie danych wskutek awarii systemu informatycznego, uzyskanie dostępu do danych przez osoby nieuprawnione lub kradzież danych.

W przypadku naruszenia bezpieczeństwa danych RODO nakłada na administratorów obowiązek zgłoszenia tego do organu nadzorczego – w Polsce jest nim Prezes Urzędu Ochrony Danych Osobowych (PUODO) – nie później niż 72 godziny od zaistnienia incydentu. Jeżeli jest on na tyle poważny, że może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator zawiadamia o tym również osoby, których dane dotyczą.

Obowiązek zgłaszania incydentów nie obowiązuje w sytuacjach, gdy jest mało prawdopodobne, by incydent skutkował ryzykiem naruszenia praw lub wolności osób fizycznych.

RAPORTY INTERAKTYWNIE.COM 2018

Styczeń

Raport: E-commerce

Luty

Raport: Agencje interaktywne - kto jest kim na polskim rynku

Marzec

Raport: Sieci afiliacyjne i programy partnerskie

Kwiecień

Poradnik: RODO w marketingu i nie tylko. Jak przygotować się na nowe przepisy

Raport: Marketing w wyszukiwarkach SEO i SEM

Maj

Raport: Content marketing. Jak prowadzić kampanie i z jakich agencji warto korzystać. Case studies kampanii

Czerwiec

Almanach polskiego internetu (nowość)

Raport: Lead generation. Najpowszechniejszy trend w internecie. Jak generować leady w różnych branżach. Jak zwiększać konwersję

Lipiec

Raport: e-Mail marketing i marketing automation

Marketing szeptany i wirusowy

Sierpień

Raport: Wideo w internecie

Raport: Studia, studia podyplomowe dot. marketingu - oferty uczelni wyższych

Wrzesień

Raport: Programmatic Buying. Czyli rewolucji w reklamie internetowej ciąg dalszy.

Raport: Finanse w internecie

Październik

Raport: Projektowanie stron internetowych, sklepów, aplikacji. Domeny, hosting, wdrożenia

Raport: Narzędzia niezbędne w marketingu i PR

Listopad

Raport: Najważniejsze sklepy internetowe w Polsce

Grudzień

Raport: Reklama w internecie

Rezerwacja powierzchni reklamowej
reklama@interaktywnie.com
+48 693 710 118, +48 510 304 576, +48 661 878 882

interaktywnie.com

JAK ZADBAĆ O BEZPIECZEŃSTWO IT W FIRMACH?

Kaja Grzybowska
redaktor Interaktywnie.com

kg@interaktywnie.com

8

Ani chmura, ani blockchain nie są remedium na bolączki związane z bezpieczeństwem IT, ale mogą pozytywnie wpłynąć na jego poprawę. Firmy nie powinny jednak koncentrować się na pojedynczych rozwiązaniach i punktowych zabezpieczeniach, a zamiast tego stworzyć kompleksową strategię uwzględniającą nie tylko technologie, ale i procedury. Najsłabszym ogniwem wszystkich zabezpieczeń niezmiennie pozostaje bowiem człowiek. Pytania o bezpieczeństwo zadaliśmy ekspertom. Udzielili rad.

Czy chmura może być sposobem na poprawę bezpieczeństwa IT w firmach?

***W obecnych realiach** często spotykamy się z poglądem, że najbardziej zadbamy o bezpieczeństwo IT, jeśli zainstalujemy systemy **we własnych ośrodkach** i będziemy mieć nad nimi pełną kontrolę. Czasami ma to swoje logiczne uzasadnienie, natomiast **uważam**, że **w zdecydowanej** większości przypadków możemy to bezpieczeństwo znacząco zwiększyć i uzyskać lepszy efekt **kosztowy** za **pomocą** rozwiązań chmurowych.*

***Jeśli weźmiemy** pod uwagę chociażby rozwiązania bezpieczeństwa klasy SIEM, monitorujące systemy IT pod kątem ewentualnych podatności i incydentów, to można taki system posiadać na własność, jednak są one dość kosztowne. W modelu chmurowym można skorzystać z efektu skali i korzystać z nich po prostu znacznie taniej. Co więcej, przy tego typu rozwiązaniach kluczowym elementem jest odpowiedni zespół ekspertów potrafiących ustawić właściwe polityki bezpieczeństwa, zaimplementować je i nimi zarządzać. Przy obecnym popycie na specjalistów cyber- i bezpieczeństwa zatrudnienie takiej osoby może zająć długie miesiące, a firmy oferujące te rozwiązania z chmury zazwyczaj już posiadają odpowiednie zaplecze personalne.*

Innym aspektem bezpieczeństwa jest zapewnienie ciągłości działania przedsiębiorstwa na wypadek awarii. Nierzadko jeszcze spotykamy się z klientami, u których kluczowe systemy - transakcyjne, produkcyjne, CRM, etc. – są zainstalowane tylko w jednym miejscu. Brakuje infrastruktury zapasowej na wypadek awarii, brakuje backupu danych, a firmy często korzystają tylko z jednego łącza do internetu lub jednego źródła energii. W przypadku awarii łącza internetowego lub przerwy w dostawie prądu systemy przestają działać, a firma nie jest w stanie kontynuować produkcji i nie realizuje sprzedaży co oznacza wymierne i często bolesne straty finansowe. W takich przypadkach zdecydowanie rekomendowałbym rozwiązania chmurowe ponieważ infrastruktura jest skonfigurowana w sposób minimalizujący ryzyko awarii i w znaczący sposób przyczynia się do poprawy bezpieczeństwa.

Jarosław Modrzewski
kierownik ds. produktu z departamentu wsparcia biznesowego sieci Plus.

Czy blockchain może być odpowiedzią na zagrożenia cybernetyczne?

Blockchain nie jest panaceum na zagrożenia cybernetyczne, nie korzysta również z innowacyjnych technologii, a świat kryptowalut niejednokrotnie padał ofiarą przestępców choć nie była temu winna sama technologia, a jej implementacja.

Ofiarami ataków padły oparte na blockchainie platformy DAO, serwis crowdfundingowy, który umożliwiał wspieranie innowacji za pomocą kryptowaluty i Bitfinex, kantor do wymiany walut wirtualnych.

Zalety technologii rozproszonych rejestrów można jednak wykorzystać, aby poprawić bezpieczeństwo. Decentralizacja usług eliminuje pojedyncze punkty ataku/awarii, złośliwie zmodyfikowane dane są odrzucane przez sieć użytkowników, a sposób uwierzytelnienia stron transakcji zapewnia ich bezpieczeństwo.

Robert Grabowski
kierownik CERT Orange Polska

Jakie są najbardziej oczywiste cyberzagrożenia, które firmy powinny brać pod uwagę?

Do najistotniejszych cyber zagrożeń należą wszelkiego rodzaju ataki przestępców w celu zdobycia wrażliwych danych klientów. Skutki takich ataków mogą być bardzo dotkliwe.

Włamania do systemów IT mogą też służyć uzyskaniu nieautoryzowanych dostępów pozwalających na realizację transakcji finansowych w imieniu firmy i kradzieży jej środków. Ataki mogą być przeprowadzane z użyciem złośliwego oprogramowania, często rozsyłanego w emailach. Oprogramowanie to pomaga przestępcom realizacji ataków lub pozyskiwania okupu pod groźbą braku dostępu do danych (oprogramowanie złośliwe ransomware).

W swoich atakach przestępcy często stosują również socjotechnikę, która polega na wykorzystaniu łatwowierności lub niewiedzy pracowników nieprzeszkolonych w tym zakresie w celu uzyskania poufnych informacji (przy użyciu telefonu, e-mail, fałszywych stron Internetowych, komunikatorów etc.) lub nakłonienia do wykonania określonych czynności, prowadzących do dostępu przestępców do systemów IT lub kradzieży środków finansowych.

Inną kategorią zagrożeń są ataki DoS/DDoS polegające na wygenerowaniu tak dużego ruchu do systemu IT (np. sklepu Internetowego), że ten przestaje odpowiadać na żądania zwykłych klientów. Należy pamiętać, że z cyberbezpieczeństwem jest jak ze zdrowiem - lepiej zapobiegać, niż leczyć i dobrze trafić na dobrego specjalistę.

Mariusz Pawłowski
Optima Partners, CISSP, ITIL, Prince2 Practitioner, REQB

Czy człowiek to wciąż najsłabsze ogniwo wszystkich zabezpieczeń?

Jednym z najbardziej istotnych zagrożeń, z którymi borykają się wszelkiego rodzaju instytucje jest wykorzystanie ich pracowników oraz systemów, jako celów ataków. Wiążą się nim straty finansowe. Podstawą cyberbezpieczeństwa są i zawsze będą ludzie. Niestety, stanowią najsłabsze ogniwo i ten fakt jest najczęściej wykorzystywany przez przestępców.

Błędy, które popełniają pracownicy wynikają z rutyny, zaniedbań, nierozumienia technologii oraz z braku świadomości zagrożeń. Przestępcy korzystając z bogatego arsenału ataków socjotechnicznych są w stanie uzyskać pewną formę kontroli nad zachowaniem osób, i w konsekwencji, przełamać nawet najbardziej zaawansowane zabezpieczenia techniczne.

W zależności od motywów działań, w kolejnych krokach celem przestępców mogą stać się aktywa finansowe, np. w przypadku coraz popularniejszych ataków BEC (Business Email Compromise) lub korporacyjne systemy wewnętrzne.

W bardziej prozaicznych przypadkach są to infekcje za pomocą botów wysyłających spam, kopiących kryptowaluty czy klikających w reklamy, co nie niesie za sobą zbyt poważnych konsekwencji dla ciągłości działania – poza stratą czasu potrzebną na przywrócenie systemów do stanu sprzed infekcji.

Poważniejszym zagrożeniem są infekcje oprogramowaniem typu RAT (Remote Access Trojan) pozwalającym na zdalny dostęp do wewnętrznych sieci, lub ransomware blokującym dostęp do zasobów, które żąda okupu za przywrócenie dostępu do danych.

Pawel Jacewicz
starszy konsultant w dziale cyberbezpieczeństwa Deloitte

Jakie mogą być skutki biznesowe naruszeń związanych z cyberbezpieczeństwem?

Najbardziej spektakularnym skutkiem cyberataku na firmę jest zakłócenie lub nawet całkowite zatrzymanie jej działalności. Zaszyfrowane dyski serwerów czy komputery wyświetlające komunikat o konieczności zapłacenia okupu, oznaczają spore problemy: od trywialnych kłopotów z komunikacją firmową, poprzez kilkudniowy brak możliwości wykorzystania komputera w pracy, trwałą utratę danych, do zatrzymania linii produkcyjnych włącznie. Taki stan co najmniej utrudnia wywiązywanie się z zobowiązań, a to oznacza konkretne straty finansowe, zagrażające nawet istnieniu firmy.

Efektem skutecznego ataku bywa też wyciek danych firmowych, stąd w internecie można odnaleźć bazy danych klientów lub kontrahentów. Przed pojawieniem się RODO miało to znaczenie wizerunkowe, jednak po wejściu w życie nowych przepisów w maju br. firmie grożą poważne kary finansowe.

Dla internetowych złodziei coraz atrakcyjniejsze stają się informacje wewnętrzne firmy: dokumenty ujawniające stan finansowy, raporty, korespondencja, know-how czy szczegóły dotyczące łańcucha dostaw. Przekazanie tych informacji konkurencji lub ujawnienie ich publicznie to często być albo nie być przedsiębiorstw.

Innym rezultatem jest kradzież pieniędzy bezpośrednio z kont firmowych. Nie zawsze jest to związane z uzyskaniem dostępu do konta – czasem wystarczy zmiana numeru w dyspozycji przelewu. Znane są przypadki, gdy atakujący informował pocztą elektroniczną o zmianie numeru konta, na który należało wykonać przelew - i był on realizowany, a pieniądze przepadały bezpowrotnie.

Negatywny wpływ na wizerunek przedsiębiorstwa i utarta wartości marki to kolejne możliwe efekty cyberataku. Firmowe strony atakujące potencjalnych klientów złośliwym oprogramowaniem, czy wykorzystujące ich komputery do tzw. „kopania" kryptowalut, mogą spowodować całkowitą utratę zaufania klientów, a informacje o takich zdarzeniach są szybko rozpowszechniane przez media społecznościowe i nagłaśniane w prasie.

Adam Lisowski
ekspert w zespole ds. cyberbezpieczeństwa w PwC

Jakie działania mogą podjąć firmy, by zminimalizować ew. skutki cyberataku?

Niedawne przypadki naruszenia bezpieczeństwa wyraźnie pokazują, że niezależnie od wielkości, przedsiębiorstwa nie wdrażają kompleksowych programów przeciwdziałających cyberatakom. Oznacza to, że firmy często wykorzystują dużą liczbę narzędzi do wykrywania różnych zagrożeń cybernetycznych, które w dodatku rzadko się ze sobą komunikują. Przy braku wymiany informacji między takimi systemami, rzeczywista ochrona całej sieci jest prawie niemożliwa i prowadzi do wydłużenia czasu wykrywania naruszeń. W wielu przypadkach oznacza to, że przedsiębiorstwa dowiadują się o tym, że zostały zaatakowane nawet po kilku miesiącach.

Zintegrowany system, który działa w chmurze, lokalnie i w punktach końcowych, ma zasadnicze znaczenie dla odporności cybernetycznej przedsiębiorstwa. Firmy muszą zrozumieć, że budowa zapory przed atakami już nie wystarcza, chociaż jest bardzo ważna. Wpływ cyberataku na brand, reputację i działalność przedsiębiorstwa może być bardzo dotkliwy. Dlatego też muszą planować z wyprzedzeniem i być przygotowane na najgorsze. Organizacje rozważają również, w jaki sposób naruszenie ochrony danych może wpłynąć na firmę z punktu widzenia przepisów oraz regulacji prawnych. Mając to wszystko na uwadze, przedsiębiorstwa muszą zagwarantować, że inwestują w technologie i procesy, które mogą im pomóc w zapobieganiu, ale także w szybkim wykrywaniu, reagowaniu, czy też samym naprawianiu skutków ataków.

Robert Arandjelovic
dyrektor ds. strategii bezpieczeństwa w regionie EMEA w firmie Symantec

O REDAKCJI

Redakcja

Tomasz Bonek
prezes zarządu i redaktor naczelny
+48 71 302 75 35
tb@interaktywnie.com

Paweł Musiał
redaktor Interaktywnie.com
redakcja@interaktywnie.com

Robert Cieszawski
redaktor Interaktywnie.com
redakcja@interaktywnie.com

Barbara Chabior
redaktor Interaktywnie.com
redakcja@interaktywnie.com

Kaja Grzybowska
redaktor Interaktywnie.com
+48 71 302 75 35
kg@interaktywnie.com

Reklama

Jakub Karczmarczyk
sales director
+48 693 710 118
jk@interaktywnie.com

Iwona Bodziony
+48 661 878 882
ib@interaktywnie.com

O INTERAKTYWNIE.COM

Adres i siedziba redakcji

interaktywnie.com

Interaktywnie.com sp. z o.o.
ul. Oławska 17 lok. 6 - III piętro
50-123 Wrocław
tel.: 71-302-75-35
redakcja@interaktywnie.com

NIP: 898-215-19-79
REGON: 020896541

Spółka zarejestrowana we Wrocławiu, kod pocztowy 50-302, przy ul. Jedności Narodowej 152/177, przez Sąd Rejonowy dla Wrocławia-Fabrycznej we Wrocławiu, VI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000322917

Kapitał zakładowy 6 000,00 zł

Interaktywnie.com to specjalistyczny magazyn dla wszystkich pracujących w branży internetowej oraz tych, którzy się nią pasjonują. Serwis zintegrował także społeczność, klika tysięcy osób, które wymieniają się tu doświadczeniami, doradzają sobie, piszą blogi, rozmawiają o najnowszych rozwiązaniach.

Interaktywnie.com istnieje od 2006 roku, na początku był branżowym blogiem. W ciągu trzech pierwszych lat znacząco poszerzył się zarówno zakres tematyczny jaki i liczba autorów, którzy w nim publikują. Zostało to docenione przez jury WebstarFestival i uhonorowane statuetką Webstara Akademii Internetu. Oprócz tego wortal jest laureatem Grand Webstara 2008 dla strony roku.

Dziś Interaktywnie.com to nowoczesne internetowe medium tematyczne z codziennie nowymi newsami z rynku polskiego i międzynarodowego, artykułami, wywiadami oraz omówieniami najciekawszych stron internetowych.

Jego redakcja przygotowuje też cykliczne, obszerne raporty branżowe, dystrybuowane do najlepszej grupy odbiorców. Wśród nich są specjaliści zarejestrowani w Interaktywnie.com. Są to szczegółowe opracowania dotyczące poszczególnych segmentów rynku internetowego i zmian, które na nim zachodzą.

Raporty promowane są także każdorazowo w największych polskich serwisach: wp.pl, gazeta.pl, interia.pl, oraz w mediach branżowych, takich jak Marketer+ czy Marketing w Praktyce.

Więcej raportów: www.interaktywnie.com/biznes/raporty

Wykorzystane do raportu zdjęcia pochodzą z banku zdjęć Fotolia.com. fotolia