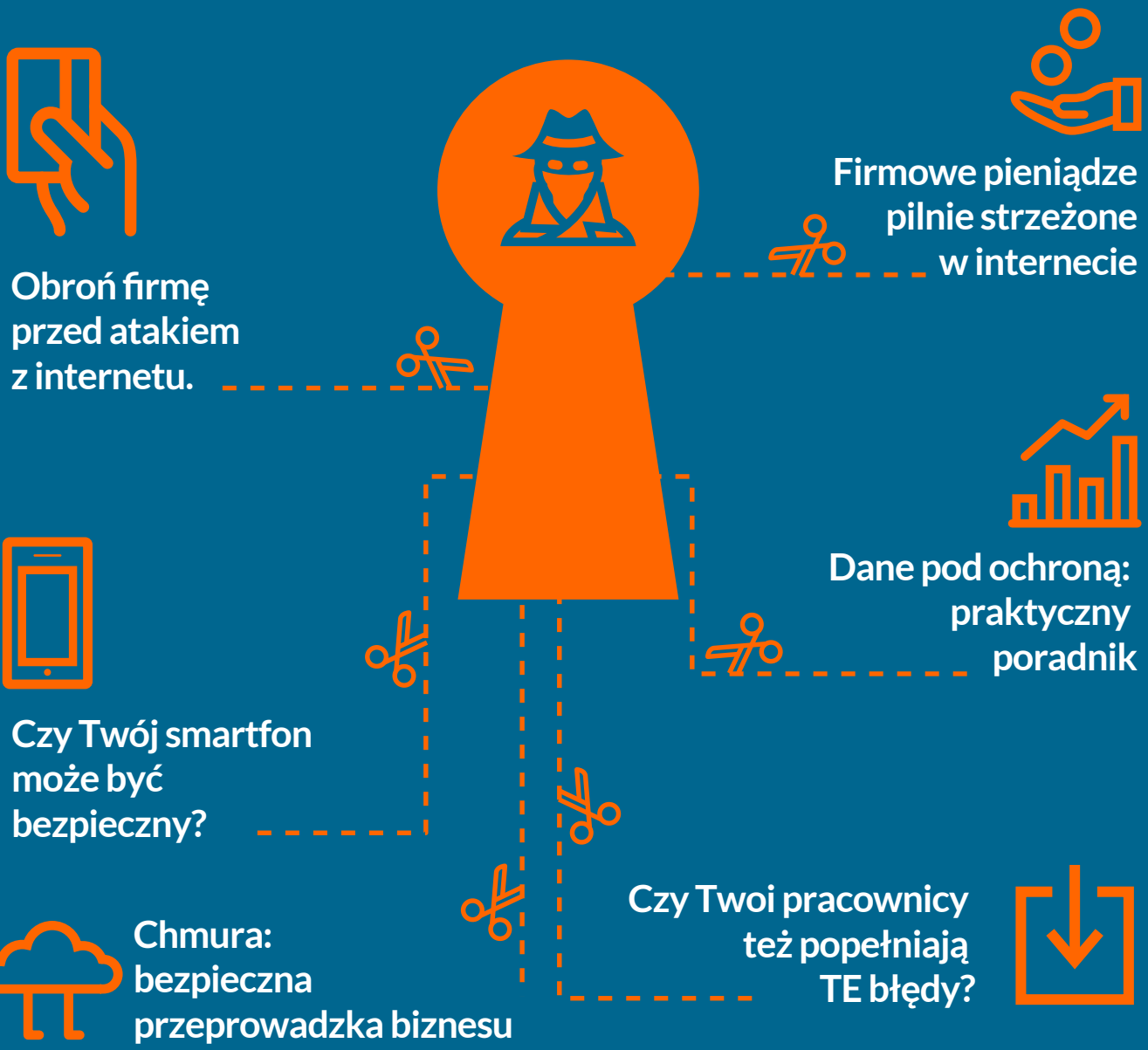
NIEZBĘDNIK DI

cyberbezpieczeństwo

#1/2016

FIRMA BEZPIECZNA W INTERNECIE



Patroni Honorowi Niezbędnika:

GIODO Generalny Inspektor Ochrony Danych Osobowych

KRAJOWA IZBA GOSPODARCZA

Ministerstwo Cyfryzacji

do lektury zaprasza Partner Merytoryczny Niezbędnika: Microsoft

OD AUTORÓW

DROGI CZYTELNIKU,

jeśli czytasz te słowa, z pewnością poszukujesz konkretnej, uporządkowanej wiedzy o bezpiecznym korzystaniu z nowych technologii. **Niezbędnik Dziennika Internautów/Cyberbezpieczeństwo** to fachowa, podręczna pomoc w razie pytań, wątpliwości czy konkretnego problemu z zakresu bezpieczeństwa IT.

Pierwsze wydanie Niezbędnika, *Firma bezpieczna w sieci*, kierujemy do małych i średnich przedsiębiorstw. Chcemy uczulić je na ryzyka i zagrożenia czyhające na nie w cyfrowej erze. Jednak przede wszystkim pokazujemy **środki skutecznej ochrony** zarówno przed przypadkową utratą czy wyciekiem danych, jak i przed celowym działaniem przestępców.

Jeden z naszych ekspertów zauważył, że przestępcy chętniej zaatakują dużo małych firm niż jedną dużą, a to dlatego, że mniejsze firmy są łatwiejszym celem. W *Niezbędniku* pokazujemy, że wcale tak nie musi być.

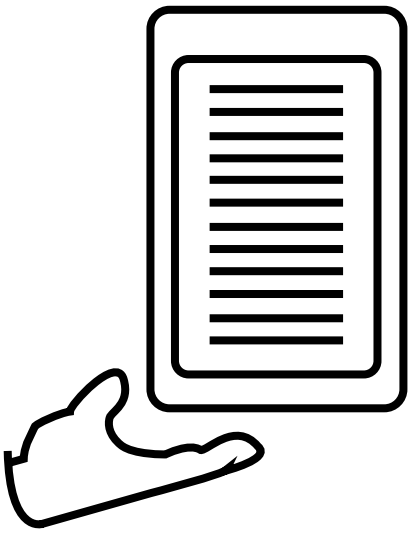
Dziś każda mała i średnia firma, łącząc świadomość, zdrowy rozsądek i odpowiednie rozwiązania techniczne, może bezpiecznie funkcjonować w cyfrowym świecie i bez obaw korzystać z nowoczesnych technologii.

Wraz z Partnerem Merytorycznym wydania, firmą Microsoft, życzymy wszystkim odbiorcom *Niezbędnika*, by pomógł im w prowadzeniu bezpiecznego i efektywnego biznesu.

w imieniu zespołu redakcyjnego
Joanna Ryńska
Krzysztof Gontarek

PS. *Niezbędnik* przygotowaliśmy, by był realną pomocą dla MŚP. Z wdzięcznością przyjmiemy wszelkie uwagi, które pomogą nam jeszcze lepiej zrealizować ten cel w kolejnych wydaniach. Nasz adres: redakcja@di24.pl.

SPIS TREŚCI



FIRMA BEZPIECZNA W SIECI

Dziś niemal każda firma korzysta z rozwiązań cyfrowych, które ułatwiają pracę w biurze i umożliwiają pracę zdalną. Jednak wraz z rozwojem technologii przybywa też zagrożeń. Ryzyko utraty lub wycieku danych, utrudnienie działalności, kradzież pieniędzy dotyczą nie tylko dużych, rozpoznawalnych korporacji. Blisko połowa cyberataków wymierzona jest w małe i średnie firmy.

W ostatnich latach coraz częściej słyszy się o atakach na duże firmy, np. Sony (upublicznienie e-maili zarządu, wyciek danych) czy Ryanair (kradzież niemal 5 mln euro). Skoro tak nieprzyjemne przygody mogły spotkać duże i dobrze zabezpieczone korporacje, mogą przydarzyć się także i mniejszej firmie. W internecie lawinowo przybywa złośliwych programów (według G Data w pierwszej połowie 2015 roku pojawiły się 3 mln nowych szkodników), a za atakami stoją zorganizowane, coraz lepiej przygotowane grupy przestępcze. Wykorzystują one bez skrupułów niewiedzę lub niedostateczne zabezpieczenia. Wiedzą, jakich sztuczek socjotechnicznych użyć, aby nakłonić pracowników do nieświadomego zadziałania na szkodę własnej firmy.

65%

W 2015 roku blisko tyle małych firm było przedmiotem cyberataku (badania Vipre Security)

CZY TO MNIE DOTYCZY?

Jak wynika z badania firmy Microsoft oraz EY *Security Trends. Bezpieczeństwo w cyfrowej erze* (*listopad 2015 r.*), 83% szefów działów IT w dużych firmach i instytucjach uważa, że wiedza działów biznesowych na temat ▸

PIOTR BRALSKI

Dyrektor Działu IT Microsoft

Ci źli są bystrzy, zdeterminowani i używają najlepszych dostępnych narzędzi. Nie ma powodu, aby ci dobrzy nie mogli robić tego samego.

cyberzagrożeń wyraźnie wzrosła w ciągu ostatniego roku, jednak wobec skali problemu nadal jest na zbyt niskim poziomie.

W małych i średnich firmach świadomość cyberzagrożeń zwykle jest niska, a częstym powodem beztroski przedsiębiorców jest przekonanie, że ich firma nie robi niczego, co mogłoby zainteresować przestępców. Tymczasem badania firmy Symantec (2013 r.) pokazują, że 40% wszystkich ataków wymierzonych jest właśnie w MŚP. Stanowią bowiem łatwy cel dla przestępców, którzy mogą m.in. wykraść dane i wykorzystać je do innych celów, przejąć przelewane z firmowego konta pieniądze czy zaszyfrować dane na urządzeniach i żądać okupu za ich odszyfrowanie (jak podano w Kaspersky Security Bulletin 2015, przedmiotem tego rodzaju ataku było w 2015 r. 58% firm). Co gorsza, często zdarza się, że tak zaszyfrowane dane są dla właścicieli na tyle ważne, że decydują się zapłacić. Jak łatwo się domyślić, mimo to danych nie odzyskują.

NARZĘDZIA I TECHNOLOGIE

Przestępcy mogą skutecznie zagrozić każdej firmie, ale też każda firma może skutecznie zabezpieczyć się przed atakami. Nadal jednak wielu przedsiębiorców traktuje kwestię bezpieczeństwa IT jako wydatek, który można odłożyć na później, lekceważąc zagrożenia i sądząc, że są czymś, co przydarza się innym.

Bagatelizowanie tematu to pozorne oszczędności, tym bardziej, że dziś na technologie poprawiające bezpieczeństwo stać każdą małą i średnią firmę. Inwestycje w te rozwiązania są nieporównywanie niższe od strat, na które naraża firmę każdy cyberatak.

25 tys. zł

tyle wyniósł średni koszt naprawy skutków cyberataku dla MŚP (badania firmy Kaspersky Lab).

Dostawcy rozwiązań informatycznych uwzględniają bezpieczeństwo podczas projektowania swoich produktów. Ulepszane są nie tylko programy wspomagające bezpieczeństwo (np. inteligentne programy antywirusowe), ale też narzędzia, z których korzystamy na co dzień. „Bezpieczna technologia" w firmie rozpoczyna się od uwzględniania aspektu bezpieczeństwa podczas wyboru rozwiązań potrzebnych ▸

w codziennej pracy. O bezpieczeństwo pomagają dbać m.in. systemy operacyjne, rozwiązania umożliwiające pracę zdalną (np. technologia *cloud computing*), przeglądarki, programy biurowe czy księgowe.

– Staramy się uprzykrzyć życie atakującym. Każdy nowy element bezpieczeństwa, który firma Microsoft tworzy, obniża opłacalność ataku. Przykładowo, w złamanie hasła trzeba obecnie włożyć tak dużo pracy, że przestępcom przestaje się to opłacać. Z Windows 10 nie chcemy już tylko budować wyższych murów przed atakiem, a po prostu uniemożliwić go osobom atakującym – podkreśla Piotr Bralski, Dyrektor Działu IT w firmie Microsoft.

WIELE ZALEŻY OD PRACOWNIKÓW

Każdy może być słabym ogniwem w łańcuchu bezpieczeństwa informatycznego – zarówno 67-letni pan Janusz, który uważa internet za zło konieczne, jak i 21-letnia Maja, która nie wyobraża sobie życia bez smartfona i aplikacji mobilnych. Pan Janusz może zapisywać hasła do ważnych zasobów na karteczkach przyklejanych do monitora, a Maja – korzystać na komputerze lub w telefonie z przydatnych jej, ale pobranych bez uzgodnienia z firmą, aplikacji.

Aż 67% pytanych przez Microsoft i EY informatyków mówi, że niefrasobliwość użytkowników jest jednym z największych zagrożeń dla bezpieczeństwa IT w firmie.

– Brak wiedzy personelu na temat zagrożeń jest niewspółmierny z postępem technologicznym, który odbywa się na tym polu – czytamy w komentarzu do badań ***Security Trends***. Tak uważa aż 81% informatyków, którzy najczęściej wskazują następujące problemy:

- korzystanie z firmowych zasobów przez nieautoryzowany sprzęt,
- przekazywanie niezabezpieczonych danych między programami używanymi do celów firmowych i do celów prywatnych,
- wykorzystanie serwisów społecznościowych do służbowej komunikacji pomiędzy członkami zespołów.

EKSPERT PODPOWIADA

MICHAŁ SAJDAK

Ekspert bezpieczeństwa Securitum.pl

Typowe zagrożenie w MŚP to brak higieny w codziennym korzystaniu z komputera, np. otwieranie nieznanych maili i załączników, klikanie w podstawione linki. Ochrona? Podnoszenie świadomości pracowników, monitorowanie poczty przychodzącej.

Jeśli wciąż zadajesz sobie pytanie: „Czy moja firma może być celem ataku?", stoisz na straconej pozycji. Aby wygrać grę, pytaj: „Jak moja firma jest przygotowana do ataku?".

Jeśli Twoja firma ma być bezpieczna w sieci:

- uświadom sobie, że dla zagrożeń IT nie ma granic, łatwo się rozprzestrzeniają i dotyczą wszystkich, także Twojej firmy,
- wybieraj rozwiązania IT pochodzące z pewnych źródeł i zwracaj uwagę na to, jak są przygotowane pod względem bezpieczeństwa,
- stosuj specjalistyczne technologie obrony przed zewnętrznymi atakami i wewnętrznymi zagrożeniami, ale nie przyjmuj z entuzjazmem każdego nowego rozwiązania. Z pomocą specjalisty stwórz spójny pakiet, najlepszy dla Twojej firmy,
- opracuj politykę bezpieczeństwa dla swojej firmy, spisz ją w przystępnej formie, przekaż swoim pracownikom, przedyskutuj ją z nimi i upewnij się, że ją rozumieją – po czym „ufaj i sprawdzaj",
- pamiętaj, że żadne rozwiązanie bezpieczeństwa nie jest dobre raz na zawsze. Bądź na bieżąco – aktualizuj programy oraz korzystaj ze szkoleń dla siebie i organizuj je dla pracowników.

1 mln zł

straciło 4% polskich firm z powodu cyberataków (Raport PwC *W obronie cyfrowych granic*, 2016)

Wskazówki eksperta na 2016 rok

Maciej Ziarek
ekspert ds. bezpieczeństwa IT
Kaspersky Lab Polska

Gdybym kierował małą firmą, w 2016 roku skupiłbym się przede wszystkim na zagrożeniach przesyłanych drogą mailową. Coraz częściej słyszymy o fałszywych fakturach czy wiadomościach wysyłanych rzekomo przez np. banki. Niektóre z tych wiadomości mają na celu wyłudzenie danych, inne zachęcenie do instalacji oprogramowania, które może być szkodliwe. Skutki infekcji zazwyczaj są bardzo poważne. Szkodliwe oprogramowanie może np. zmienić numer konta w trakcie dokonywania przelewu lub zaszyfrować cały dysk i żądać opłaty za klucz deszyfrujący.

Istotne zagrożenia – prognozy na rok 2016

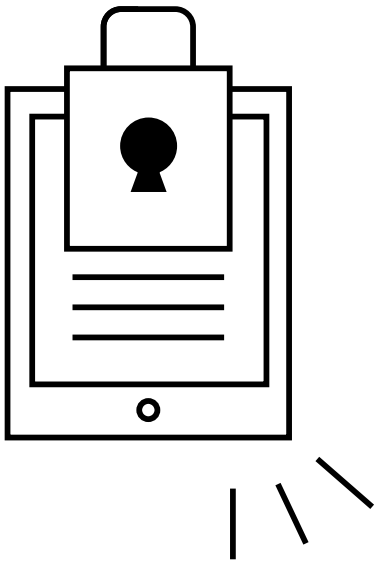
CERT Orange Polska

- Więcej ataków na sieci firmowe z wykorzystaniem prywatnych profili pracowników na portalach społecznościowych, słabości połączeń domowych (z których pracownicy coraz częściej łączą się z firmową siecią) oraz oprogramowania szpiegowskiego,
- ataki phisingowe (wyłudzające poufne dane bezpośrednio od użytkowników),
- ataki DDoS (odmowa dostępu do usługi). Już w 2015 roku najczęściej kierowane były tak, by zablokować dostęp do serwisów transakcyjnych.

Wyzwania dla MŚP w ciągu najbliższych 5 lat

István Szabó, Product Manager w firmie Balabit

Poza atakami z zewnątrz, najgroźniejsze dla bezpieczeństwa IT organizacji są ataki wewnętrzne, dokonywane przez osoby podszywające się pod pracowników firmy. Nowym czynnikiem wpływającym na bezpieczeństwo IT są więc użytkownicy systemu. Szkodliwi użytkownicy wykorzystują słabe punkty podstawowych narzędzi bezpieczeństwa stosowanych w firmach (np. firewall), ponieważ są one zaprojektowane tak, by chronić przed zagrożeniem zewnętrznym, a nie przed zaufanymi pracownikami. Ponadto tradycyjne mechanizmy obronne nie są w stanie poradzić sobie z ogromną liczbą alarmów czy identyfikacją nieznanych zagrożeń, które mogą czaić się w systemie. Najlepszym rozwiązaniem jest zastosowanie narzędzi do analizy zachowań użytkowników, które identyfikują zewnętrzne zagrożenia i szkodliwych użytkowników wewnętrznych (nie zakłócając przy tym codziennego funkcjonowania firmy) oraz optymalizują alarmy bezpieczeństwa.



BEZPIECZNE URZĄDZENIA FIRMOWE. OD CZEGO ZACZĄĆ?

Przeczytaj, jeśli:

- **korzystasz z wielu programów łączących się z internetem**
- **uważasz, że bezpieczeństwo firmy w sieci wymaga dużych nakładów**
- **chcesz mieć pewność, że dobrze zabezpieczasz swój komputer, smartfon czy tablet**
- **tworzysz politykę bezpieczeństwa dla swojej firmy**

Złośliwe programy są wpuszczane na urządzenia przez samych użytkowników albo korzystają z niedoskonałości programów używanych na co dzień. Dlatego bezpieczeństwo IT zaczyna się od korzystania z legalnych i aktualnych programów.

Żadne, nawet najbardziej zaawansowane oprogramowanie, nie jest wolne od luk i błędów. Trzeba je na bieżąco aktualizować, aby uniemożliwić przestępcom wykorzystanie tych „dziur" do zainfekowania komputera.

Dostawcy programów regularnie opracowują do nich łatki i aktualizacje. Zainstalowane na komputerach programy same je wykrywają i proponują ich wprowadzenie. Można także pobierać aktualizacje i nowe wersje ze strony producenta.

EKSPERT PODPOWIADA

MARCIN KLIMOWSKI

Windows Product Marketing Manager

Korzystasz ze specjalistycznego oprogramowania (np. grafika inżynierska, modelowanie, symulacje etc.) i boisz się, że automatyczna aktualizacja systemu Windows 10 sprawi, że Twoje podstawowe narzędzie pracy przestanie działać? Możesz w kontrolowany sposób opóźnić aktualizacje, korzystając z Windows Update for Business. Zyskujesz czas na dostarczenie aktualizacji poza godzinami pracy lub ich przetestowanie na wybranych grupach komputerów.

Dobre praktyki

- **Używaj tylko aktualnych narzędzi:** systemu operacyjnego, przeglądarek i innego oprogramowania.
- **Aktualizacje wprowadzaj natychmiast po informacji o ich dostępności.** Każdy dzień opóźnienia to większe ryzyko, że przestępca skorzysta z niezałatanej dziury. Programy często same przypominają o aktualizacjach – reaguj na wyświetlane przypomnienia.
- **Ustaw aktualizacje automatyczne**, jeśli tylko jest to możliwe w danym programie (np. programy antywirusowe, Adobe Acrobat, Office 365 czy przeglądarki: Chrome, Edge, Firefox).
- **Unikaj przypadkowych źródeł.** Łatki, aktualizacje czy nowe wersje programów pobieraj tylko z oficjalnej strony producenta lub – w przypadku urządzeń przenośnych – z oficjalnych sklepów z aplikacjami mobilnymi.

- **Uważaj na nietypowe komunikaty.** Jeśli na Twoim urządzeniu (komputerze czy smartfonie) znienacka pojawi się baner czy pop-up „Masz 4 wirusy" (lub podobny) – nawet w niego nie klikaj. Podobnie potraktuj zachętę do aktualizacji jakiegokolwiek programu, wyświetlającą się jako reklama na (np. baner) na stronie, którą odwiedzasz. To zwykle złośliwy program w przebraniu. Jeśli masz wątpliwości, czy to jednak nie jest ważna aktualizacja – sprawdź to na stronie producenta.

Przykład znaczenia aktualizacji

Na początku grudnia 2015 roku Microsoft usunął podatność Outlooka na zagrożenie pod nazwą BadWinmail. Do infekcji komputera wystarczyło... odebranie poczty, zawierającej załącznik z obiektem Flash. Aktualizowałeś/aś Outlooka od tamtego czasu?

UWAŻAJ NA PRZEGLĄDARKI!

Aktualizuj regularnie także przeglądarki. Bramą dla złośliwego oprogramowania są też dodatki (wtyczki) do przeglądarek – odtwarzacze Flash i Java. Stopniowo są one eliminowane – przeglądarki już dziś ograniczają korzystanie z tych dodatków, np. Firefox traktuje Flash jako element niebezpieczny i automatycznie go blokuje. W Edge – nowej przeglądarce w Windows 10 – dodatki będą wprowadzone w sposób bezpieczny, a w najbliższym czasie wszystkie nieistotne elementy flashowe będą zatrzymywane lub wyłączane.

Przeglądarki mogą też pełnić funkcję ochrony przed zagrożeniami internetowymi – głównie przed stronami wyłudzającymi dane (ochrona antyphishingowa), np. SmartScreen – filtr wbudowany w przeglądarki Internet Explorer (od wersji 9) oraz Edge – ostrzega przed fałszywymi (wyłudzającymi dane), ocenia „reputację" pobieranych plików i pomaga uniknąć pobrania złośliwego oprogramowania.

Bezpieczne hasło: 7 prostych zasad

1. Hasło musi być silne: długie (co najmniej 12 znaków) i trudne do odgadnięcia (np. długie i wymyślne zdanie pisane slangiem). Hasło powinno też zawierać zarówno małe jak i wielkie litery, cyfry i znaki specjalne.
2. Do każdej strony ustaw osobne hasło. Jeśli łupem przestępcy padnie jedno hasło, spróbuje go użyć do logowania w innych miejscach.
3. Nie podawaj nikomu hasła ani sposobu, w jaki je tworzysz.
4. Unikaj zapamiętywania haseł w przeglądarce, nie zapisuj hasła w widocznym miejscu.
5. Stosuj menedżer haseł – program służący do bezpiecznego przechowywania licznych haseł, trzeba pamiętać tylko jedno hasło główne.
6. Regularnie (np. co 2–3 miesiące) zmieniaj hasła do kluczowych usług.
7. Jeśli to możliwe, stosuj podwójne uwierzytelnianie (weryfikację dwuskładnikową) – oprócz hasła musisz mieć "coś jeszcze", np. jednorazowy kod SMS.

MOJA ZŁOTA ZASADA BEZPIECZEŃSTWA

MICHAŁ SAJDAK

Ekspert bezpieczeństwa Securitum.pl

1. Odpowiednie sprawdzenie przed instalacją pliku ściągniętego z internetu (np. weryfikacja podpisu cyfrowego).

2. Zadbanie o dostępność wszystkich istotnych aktualizacji.

3. Wyłączenie niepotrzebnych i notorycznie niebezpiecznych elementów w przeglądarkach internetowych (np. Flash).

OCHRONA PRZED ZŁOŚLIWYM OPROGRAMOWANIEM

Komputery i urządzenia przenośne należy dodatkowo zabezpieczyć przed złośliwym oprogramowaniem. Podstawą i najbardziej popularnym środkiem jest program antywirusowy – to jednak za mało. Komputer powinien być wyposażony w pełny pakiet bezpieczeństwa:

- program antywirusowy – chroni komputer przed złośliwymi programami zakłócającymi pracę właściwego oprogramowania,
- zapora sieciowa (*firewall*) – zabezpiecza przed próbami włamania do komputera podczas połączenia z internetem,
- narzędzie antyszpiegowskie (*antispyware*) – chroni przed programami szpiegowskimi, czyli takimi, które zbierają z komputera dane bez wiedzy i zgody właściciela,
- narzędzie antyphisingowe – zabezpiecza przed fałszywymi stronami, wyłudzającymi poufne dane (to narzędzie często jest już wbudowane w przeglądarkę).

Jakie pakiety są do wyboru?

- systemowy – wbudowany w system operacyjny, zatem nie wymaga kupowania dodatkowych licencji,
- komercyjny – oferowany przez firmy specjalizujące się w zabezpieczeniach,
- bezpłatny – należy uważać, bo nie brakuje fałszywych rozwiązań: programów udających zabezpieczenie antywirusowe, a będących wirusami (mniej zaawansowani użytkownicy internetu dają się skusić tym, że „rozwiązanie" jest bezpłatne).

BEZPIECZEŃSTWO OPARTE O ZŁUDZENIA?

Lepiej korzystać z antywirusów systemowych – niż z żadnych. Lepiej korzystać z antywirusów systemowych niż z programów nieaktualnych – programy nieaktualne są nawet gorsze niż żadne, gdyż dają użytkownikowi fałszywe poczucie bezpieczeństwa.

Przykłady programów antywirusowych dla MŚP

Bitdefender Endpoint Security, F-Secure Client Security, G Data AntiVirus Business, Intel Security, McAfee Endpoint Security, Kaspersky Lab: Endpoint Security i Small Office Security, Seqrite Endpoint Security, Sophos Endpoint Security and Control, Symantec Endpoint Protection, Trend Micro Office Scan.

PRZYKŁADY PROGRAMÓW ANTYWIRUSOWYCH

Rozwiązanie wbudowane w Windows 10 to Windows Defender. Uruchamia się domyślnie, dopóki na komputerze nie ma innego programu antywirusowego. Windows 10 zapewnia też, że zainstalowany na komputerze program antywirusowy uruchamia się w początkowej fazie startu systemu. Windows Defender aktywizuje się także, jeśli wykryje nieaktualny program antywirusowy – informuje o tym użytkownika i proponuje, że się włączy.

Rozwiązania komercyjne, dostosowane do potrzeb użytkownika firmowego (np. licencje wielostanowiskowe). Wybierając taki pakiet, można uwzględniać niezależne badania skuteczności oprogramowania (popularne testy dostępne są na AV-Test.org).

Baza wirusów sprzed doby jest za stara!

Marcin Klimowski,
Windows Product Marketing Manager

Program antywirusowy powinien aktualizować się codziennie do najnowszej bazy wirusów (tak robi np. Windows Defender). To bardzo ważne, bo każdego dnia pojawiają się nowe szkodniki, np. ostatnio odnotowujemy wysyp złośliwych programów typu ransomware. Dlatego po prostu trzeba mieć program antywirusowy absolutnie aktualny, z dzisiejszymi bazami. Jeśli mamy bazy sprzed dnia czy półtora dnia, wystawiamy się na atak!

Do bazy wirusów nie można oczywiście dodać szkodnika nieznanego specjalistom bezpieczeństwa (tzw. szkodnika dnia zerowego - zero day exploit). Z pomocą przychodzą programy uczące się (heurystyczne). Uczą się tego, co dzieje się na komputerze i reagują na odstępstwa od tych wzorców.

BEZPIECZNY LAPTOP – WYBÓR I UŻYTKOWANIE

Przeczytaj, jeśli:

- **wybierasz nowy laptop firmowy**
- **chcesz bezpiecznie korzystać ze swojego urządzenia**
- **chcesz poprawić bezpieczeństwo firmy „od podstaw”**

Dostawcy zarówno oprogramowania, jak i samych urządzeń nie ustają w wysiłkach, by przekonać Cię do zakupu swojego najlepszego i najnowocześniejszego rozwiązania. W jednym mają rację – najnowsze urządzenia pozwalają najpełniej korzystać z istniejących rozwiązań technologicznych i są najlepiej przygotowane na radzenie sobie z zagrożeniami.

Jeśli zamierzasz kupić laptopy do firmy i chcesz dobrze ulokować pieniądze, przed Tobą dwie opcje: laptopy ze spełniającym różnorodne oczekiwania systemem Windows 10 (najlepiej w wersji Pro, przeznaczonej dla firm), a dla fanów nadgryzionego jabłka – rozwiązania z systemem OS X (np. MacBook Air). Najpopularniejszym rozwiązaniem, które sprawdzi się w większości małych i średnich firm, jest Windows (w nowych laptopach Windows 10).

BEZPIECZNY LAPTOP DLA MOBILNEGO PRZEDSIĘBIORSTWA

Wybierając urządzenie, które najlepiej sprawdzi się w firmie stawiającej na mobilność (ultralekkie, trwałe i o długo działającej baterii), należy postawić też na bezpieczeństwo. W praktyce będą to następujące rozwiązania:

Rosnąca popularność Windows 10

Amerykański instytut badawczy Gartner prognozuje, że pilotażowe wdrożenia Windows 10, rozpoczęte w przedsiębiorstwach w 2016 r., osiągną apogeum w latach 2017–2018 ze względu na:

- wspieranie mobilności,
- fabryczne wyposażenie w system urządzeń 2w1 (tablet+laptop),
- planowanie zakończenie wsparcia dla Windows 7.

- system Windows Pro, rekomendowany dla firm (umożliwia np. zarządzanie bezpieczeństwem floty firmowych urządzeń),
- system 64-bitowy,
- oprogramowanie układowe (*firmware*) – UEFI zamiast BIOS. Zapewnia ono tzw. bezpieczny rozruch – rozwiązanie, które znacznie utrudnia złośliwym programom zagnieżdżenie się w oprogramowaniu układowym,
- TPM (*Trusted Platform Module* – wyspecjalizowany układ wspierający funkcje bezpieczeństwa i szyfrowania). Jest wymagany do prawidłowego działania niektórych technologii, np. chroniących przed kradzieżą danych,
- rozwiązania wspierające biometrię – skaner odcisku palca lub specjalna kamera umożliwiająca wykonanie kompleksowego skanu twarzy. Nawet jeśli rozwiązanie to wydaje się futurystyczne, będzie spotykane coraz częściej. Już dziś skan twarzy to podstawa biometrycznego logowania na komputery wyposażone w Windows 10.

ZANIM FACHOWO ZABEZPIECZYSZ LAPTOP

Laptop i jego zawartość należy chronić, korzystając przede wszystkim ze zdrowego rozsądku:

- blokuj dostęp do komputera – uruchomienie go musi wymagać identyfikacji (np. hasła),
- pracując, ustawiaj blokowanie ekranu po danym czasie nieaktywności (np. po minucie), zaś odblokowanie umożliwiaj za pomocą hasła – nigdy nie wiesz, kiedy będzie trzeba oderwać się od urządzenia otwartego na ważnych danych,
- pracując poza firmą, upewnij się, czy nikt nie zagląda Ci w ekran, w kawiarni usiądź pod ścianą, w pociągu możesz użyć tzw. filtra prywatyzującego, czyli nakładki na ekran, dzięki której Ty widzisz wszystko, a osoba patrząca z boku – ciemny ekran,
- nie używaj pamięci USB z nieznanego źródła, uważaj m.in. na darmowe reklamówki. To jeden z najprostszych sposobów, by zainfekować komputer. Zawsze skanuj pendrive'y (także swoje, jeśli były komuś pożyczane lub udostępniane) programem antywirusowym.

Kierunek: brak hasła

FIDO (*Fast IDentity Online*) Alliance – stowarzyszenie firm (wśród założycieli m.in. Lenovo i PayPal), działające (od 2013 r.) na rzecz poprawy bezpieczeństwa i jednoczesnego uproszczenia sposobu identyfikacji użytkownika – dąży do „świata bez haseł". Przyszłością jest m.in. logowanie za pomocą wskaźnika biometrycznego + kodu PIN przechowywanego lokalnie na urządzeniu.

Zdrowy rozsądek warto wspomagać rozwiązaniami technologicznymi.

KONTROLA DOSTĘPU FIZYCZNEGO

Komputer należy przede wszystkim zabezpieczyć przed dostępem niepowołanych osób. Zwykle do blokowania urządzeń używa się prostego hasła. Alternatywą jest korzystanie z funkcji biometrycznych (komputer identyfikuje konkretną osobę, a nie wpisane hasło) – odcisku palca, skanu twarzy lub skanu tęczówki.

Rozpoznawanie odcisku palca dostępne jest już od kilku lat, m.in. w niektórych laptopach Della, HP czy Lenovo, natomiast rozpoznawanie zaawansowanego skanu twarzy to nowe rozwiązanie. Obecnie jest ono dostępne jako **Windows Hello** w systemie Windows 10, pod warunkiem stosowania komputera z odpowiednią kamerą (np. Intel RealSense lub własne rozwiązanie Microsoft).

Kamera do skanowania twarzy na potrzeby biometrii tworzy dokładną mapę twarzy użytkownika, rozpoznając jej specyficzne punkty i dokładne odległości między nimi (w tym głębokość obrazu) oraz delikatne ruchy skóry. Nie nabierze się więc na bliźniaków, zdjęcie twarzy czy jej model 3D. Działa też w złych warunkach oświetleniowych.

Kamera jest też dostępna jako urządzenie przenośne, ale działa tylko we współpracy z systemem Windows 10.

Przykłady urządzeń z kamerą do skanu twarzy

- Acer: Aspire V 17 Nitro
- Asus: N551JQ, ROG G771JM, X751LD
- Dell: Inspiron 15 5548, Inspiron 23 7000
- HP: Envy 15t Touch RealSense Laptop, Sprout
- Lenovo: ThinkPad Yoga 15, ThinkPad E550, B5030
- Microsoft: Surface Pro 4 (urządzenie typu 2w1 – tzw. tablet biznesowy, przekątna 12,3")

EKSPERT PODPOWIADA

KAMIL SADKOWSKI

analityk zagrożeń ESET

Pomiar biometryczny (np. odcisk palca) nie powinien być używany jako hasło lub kod dostępu. Powinien być traktowany jako dodatkowy dowód tożsamości, połączony z numerem PIN.

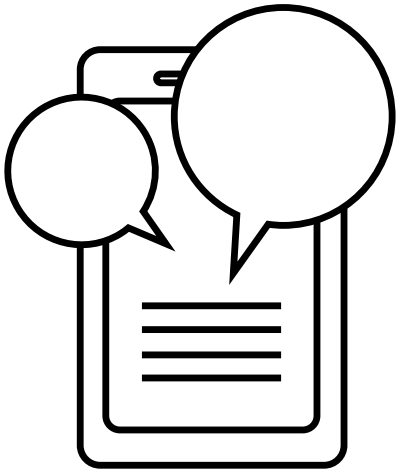
Szyfrowanie urządzeń

Nawet jeśli zabezpieczysz komputer, istotnym ryzykiem w pracy mobilnej pozostaje utrata (zgubienie, kradzież) urządzenia, a wraz z nim danych firmowych. Zapewne pamiętasz o kopiach zapasowych, ale dane należy zabezpieczyć także przed przejściem w niepowołane ręce. Stąd warto szyfrować tablety, karty w smartfonach oraz dyski w laptopach. Wówczas ten, kto przejmie utracone urządzenie, nie będzie mógł skorzystać z dysku lub karty, nawet jeśli przełoży je do innego urządzenia.

Do szyfrowania (całych urządzeń, poszczególnych partycji czy dysków) używa się programów szyfrujących. Dla urządzeń z systemem Windows w edycjach biznesowych dostępne jest szyfrowanie dysku za pomocą rozwiązania BitLocker. Istnieją rozwiązania konsumenckie (np. nieodpłatne rozwiązanie TrueCrypt) lub biznesowe (w tym przeznaczone specjalnie dla MŚP).

Korzystanie z tego typu rozwiązania jest proste – należy stworzyć tzw. klucz zabezpieczeń (może to być silne hasło lub odpowiedni plik zapisany poza komputerem, np. na karcie), który trzeba wprowadzić przed rozpoczęciem pracy (czyli wpisać hasło lub otworzyć plik z zewnętrznego urządzenia).

Przedsiębiorca powinien być szczególnie wyczulony na to, jak i gdzie przechowywane są klucze do szyfrowania danych komputerów pracowników. Należy stosować zasadę ograniczonego zaufania i ustalić w firmie jeden sposób szyfrowania zawartości dysków. Klucz zabezpieczeń powinien być przekazany pracodawcy. Kłopotów z pracownikiem, który skopiował samodzielnie zaszyfrowane dane i żąda gratyfikacji za ich zwrot, nie należy życzyć nikomu.



SMARTFONY I TABLETY W FIRMIE – MOBILNIE I BEZPIECZNIE

Przeczytaj, jeśli:

- **Twoi pracownicy korzystają ze smartfonów i/lub tabletów**
- **wybierasz lub konfigurujesz urządzenia przenośne dla firmy**
- **Twoi pracownicy mogą korzystać w pracy z własnych urządzeń**

BOGDAN DUMITRU

Dyrektor Techniczny, Bitdefender

Z zagrożeniami muszą liczyć się użytkownicy wszystkich smartfonów. Cyberprzestępcy będą wykorzystywać to, co sprawdzało się w 2015 roku. Coraz większe znaczenie będzie miało oprogramowanie adware.

Smartfony czy tablety firmowe są używane do pracy poza biurem, ale też stosowane do celów pozasłużbowych, co bardziej naraża je na szereg niebezpieczeństw: włamanie, próby przejęcia danych czy utratę informacji przez zgubienie urządzenia. Wielu z tych zagrożeń można łatwo uniknąć, wdrażając proste zasady bezpieczeństwa.

Niedopilnowany smartfon może stać się źródłem wycieku danych firmowych – tym bardziej, że coraz częściej pracujemy na tych urządzeniach, np. korzystając z firmowej poczty czy współdzieląc bazę Excel (dokumenty) online. Jak podkreśla Piotr Bralski, Dyrektor Działu IT w firmie Microsoft, skoro każdy pracownik może mieć dostęp do danych firmowych na swoich urządzeniach mobilnych, dopiero na tych urządzeniach kończy się zakres odpowiedzialności szefów działów IT! ▸

EKSPERT PODPOWIADA

ALICJA RDZANEK

Senior Product Marketing Manager, Microsoft

Jeśli wszystkie urządzenia w firmie, tj. komputery, tablety i smartfony, pracują na jednym systemie operacyjnym, zarządzenie flotą jest dużo prostsze. Takim rozwiązaniem jest Windows 10.

PODSTAWOWE ZASADY BEZPIECZEŃSTWA

Urządzenia firmowe i prywatne używane do pracy trzeba chronić w czasie rzeczywistym. Większość producentów oprogramowania antywirusowego na komputery posiada również aplikacje ochronne dla smartfonów i tabletów. Tak jak w przypadku komputerów, jest to podstawowe zabezpieczenie przed intruzami i szkodliwym oprogramowaniem. Można także znaleźć szereg wyspecjalizowanych aplikacji zabezpieczających przed podsłuchiwaniem przesyłanych danych lub przed atakami przestępców (np. Kaspersky Internet Security dla Androida, Avira Mobile Security dla iOS czy Avast Mobile Security dla Windows).

ZASADY BEZPIECZEŃSTWA DLA PRACODAWCY:

- zainstaluj na urządzeniach firmowych oprogramowanie pozwalające na jego lokalizację – dzięki temu skradzione/zgubione będzie można łatwo odzyskać, oprogramowanie to może być rozwiązaniem systemowym (mają je np. telefony z systemem iOS lub Windows 10 Mobile) lub stanowić część komercyjnego pakietu zabezpieczeń internetowych,
- zaszyfruj dyski, co pozwoli na zabezpieczenie danych w pamięciach urządzeń,
- wprowadź system MDM (*Mobile Device Management* – zarządzanie urządzeniami mobilnymi). Oprogramowanie to pozwala instalować, monitorować i usuwać oprogramowanie na wszystkich urządzeniach przenośnych w firmie. Przydaje się np. do zdalnej konfiguracji tabletów, kupionych dla oddziałów firmy lub kontrolowanie, czy zabezpieczenia IT są aktualizowane,
- jeżeli pracownicy używają urządzeń firmowych także poza siecią firmową lub do celów prywatnych albo korzystają do celów firmowych z własnych urządzeń, warto rozważyć skorzystanie z oprogramowania do zarządzania modelem BYOD (*Bring Your Own Device* – przynieś własne urządzenie).

EKSPERT PODPOWIADA

ALICJA RDZANEK

Senior Product Marketing Manager, Microsoft

W przypadku smartfonów Lumia osoba zarządzająca flotą telefonów w firmie może określić, które aplikacje są traktowane jako firmowe, a które – jako prywatne. Zapobiega to wymianie danych między aplikacjami firmowymi a osobistymi. Przykładowo, nie można skopiować danych z poczty firmowej i przenieść ich (choćby przypadkowo) do aplikacji prywatnej, np. Facebooka.

Oprogramowanie, które umożliwia bezpieczną pracę w modelu **BYOD**, to bardzo dobre rozwiązanie dla konsultantów, pracowników marketingu, działów IT, ale też przedstawicieli handlowych i innych pracowników terenowych. Ciekawe funkcje, które można zrealizować:

- rejestracja urządzeń i użytkowników w specjalnym systemie. Użytkownik, korzystając ze swojego urządzenia, musi uwierzytelnić się hasłem, by uzyskać bezpieczny dostęp do zasobów firmowych;
- nadanie użytkownikom uprawnień (np. do jakich danych mają dostęp z konkretnego urządzenia);
- monitorowanie zgodności zainstalowanych aplikacji z wytycznymi firmowymi;
- rozdzielenie danych prywatnych od osobistych;
- możliwość zdalnego usunięcia zawartości firmowej, np. po wyrejestrowaniu urządzenia lub zakończeniu współpracy z użytkownikiem urządzenia.

Rozwiązania komercyjne przeznaczone dla tego modelu pracy to m. in. FortiOS 5, Cisco BYOD Smart Solution, Air-Watch. Dla firm mało zinformatyzowanych dobrym rozwiązaniem jest Microsoft Intune. Jest to usługa, która umożliwia zarządzanie wszystkimi urządzeniami poprzez intuicyjny panel, dostępny przez stronę www. Umożliwia on m.in. inwentaryzację zainstalowanych programów, w tym sprawdzanie zgodności i aktualności programów antywirusowych.

ZASADY BEZPIECZEŃSTWA DLA KAŻDEGO PRACOWNIKA

- nigdy nie pobieraj plików z niezaufanych źródeł. Zaufane źródła aplikacji to Google Play (dla systemu Android), Sklep Windows (dla Windows 10 Mobile) oraz App Store (dla iOS). Aplikacje przed umieszczeniem w sklepie są weryfikowane przez korporację firmującą sklep, ale zawsze może zdarzyć się przeoczenie (uważa się, że najmniej restrykcyjne są procedury Google). **Firmowe sklepy z aplikacjami to pewne źródło zaufanych aplikacji. Jednak – uwaga!** Czasami przestępcy umieszczają podrobione programy, podszy-

MOJA ZŁOTA ZASADA BEZPIECZEŃSTWA

MACIEJ ZIAREK

ekspert ds. bezpieczeństwa IT Kaspersky Lab Polska

Korzystając z urządzenia mobilnego, zawsze staram się instalować oprogramowanie z oficjalnego sklepu. Przed instalacją sprawdzam, do jakich zasobów aplikacja chce mieć dostęp i czy powinienem go udzielać (sprawdzam, czy program nie chce mieć dostępu do usług systemowych, których nie powinien wymagać do działania).

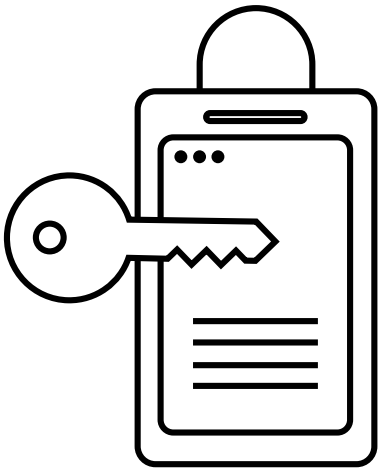
wając się pod znanych producentów. Przed pobraniem należy zatem sprawdzić na stronie danego producenta, czy faktycznie opublikował on aplikację mobilną. Przygoda z podrobionym antywirusem dla urządzeń z systemem Android spotkała np. firmę Kaspersky,

- stosuj blokadę ekranu - kod, hasło, sekwencję pociągnięć lub rozwiązania biometryczne. Jeśli urządzenie zostanie skradzione lub zgubione, nie będzie można w prosty sposób dostać się do danych,
- w zabezpieczeniu urządzeń z systemem Windows 10 pomaga funkcja Windows Hello, zastosowana m.in. w smartfonie Lumia 950 czy tablecie biznesowym Surface Pro 4. Polega na odblokowaniu urządzenia tabletu za pomocą skanu twarzy lub czytnika linii papilarnych, a w przypadku Lumii 950 lub 950 XL – przez skan tęczówki oka,
- skonfiguruj opcje prywatności. Ogranicz liczbę aplikacji, które korzystają z prywatnych danych czy umożliwiają geolokalizację (stwierdzają, gdzie znajduje się smartfon). To utrudni potencjalnemu włamywaczowi dostęp do poufnych danych,
- aktualizuj na bieżąco system operacyjny smartfona i oprogramowanie, zwłaszcza antywirusowe. Szczególnie beztroscy są pod tym względem użytkownicy urządzeń z systemem Android. Tylko ok. 20% korzysta z aktualnej wersji systemu (**raport G Data** za 3. kwartał 2015 r.). Ułatwione zadanie mają np. użytkownicy telefonów z Windows 10 Mobile, których aktualizacje (automatyczne) planowane są w czasie, kiedy użytkownik zwykle najmniej korzysta z urządzenia.

Szyfruj urządzenia!

Alicja Rdzanek,
Senior Product Marketing Manager, Microsoft
W Windows 10 Mobile możliwe jest szyfrowanie plików w smartfonie. W przypadku utraty urządzenia nie można odczytać przechowywanych danych.

Robert Dziemianko, Marketing Manager, G DATA
Pełne szyfrowanie treści zapobiega nieuprawnionemu dostępowi do zawartości smartfona. Wiadomości są dostępne tylko dla odbiorcy, bo tylko jego smartfon może odszyfrować wysłane wiadomości.



BEZPIECZNE ŁĄCZENIE Z SIECIĄ

Przeczytaj, jeśli:

- masz w firmie sieć Wi-Fi
- Twoi pracownicy korzystają z Wi-Fi w podróży
- udostępniasz swoją sieć Wi-Fi gościom w firmie

NEIL MCDONALD

Instytut Gartnera

Niezależnie od tego, jakie środki bezpieczeństwa zastosuje firma, i tak zostanie zaatakowana. Należy więc nie tylko uniemożliwiać ataki, ale i umieć wykryć obecność intruza w sieci firmowej!

Dostęp do internetu: niezbędny dla funkcjonowania większości firm. Dzisiejsze standardy pracy: szybka i wydajna firmowa sieć bezprzewodowa czy łączenie z internetem w sprawach firmowych poza biurem.

W połowie 2015 roku firma Fortinet opublikowała raport *Security Census* 2015 poświęcony bezpieczeństwu sieci bezprzewodowych w firmach – co prawda, dużych (od 250 pracowników), ale ich nastawienie brzmi znajomo. Choć firmy obawiają się utraty poufnych danych (własnych i klienta), szpiegostwa przemysłowego czy zakłócenia w działaniu, podchodzą dość beztrosko do zabezpieczenia swoich sieci.

Zobacz, jak powinno być – sprawdź wraz ze swoim działem IT, czy stosujecie w firmie choćby podstawowe zasady bezpieczeństwa.

PODSTAWA – BEZPIECZNY ROUTER

Sieć firmowa powinna być skutecznie zabezpieczona zarówno przed nieuprawnionym dostępem z zewnątrz, jak i nieprawidłowościami w sieci wewnętrznej. Pierwszą linią obrony jest prawidłowe zabezpieczenie wejścia do sieci – routera.

Dobre praktyki

Etap wyboru urządzenia:

- kieruj się w mniejszym stopniu ceną, a bardziej reputacją dostawcy (sprawdzeni dostawcy routerów to m.in. Asus, Cisco, D-Link, Linksys, Neatgear),
- sprawdź, czy urządzenie ma domyślną blokadę zdalnego dostępu z internetu—to istotne tu odstęp wygląda jak podwójny (zgłoszenie klienta) atakami z zewnątrz na router.

Etap konfiguracji:

- ustawienie prawidłowych DNS-ów (o wartościach należących do dostawcy internetu)

  Uwaga! Podmiana DNS-ów na takie, które kierują ruch na podstawione strony (służące zazwyczaj do wyłudzania danych lub infekcji niezaktualizowanych systemów czy przeglądarek), to jeden z typowych ataków na routery.
- zmiana wszystkich domyślnie ustawionych haseł: sieciowego, administracyjnego etc. na własne, silne hasła

  Uwaga! Hasła domyślne mogą być łatwe do odgadnięcia, bo są np. powiązane z nazwą dostawcy lub z numerem seryjnym sprzętu.
- zmiana nazwy sieci (SSID) na taką, która nie będzie zawierała nazwy producenta routera ani nazw domyślnych (np. „wireless" lub „default").
- włączenie szyfrowania WPA2 z wykorzystaniem silnego hasła (od 8 do 63 znaków—zaleca się co najmniej 30 znaków). Przy szyfrowaniu wszystkie dane przesyłane w firmie są szyfrowane.

  Przykładowo, Apple zaleca stosowanie trybu WPA-AES, jako najsilniejszą formę zabezpieczeń, w drugiej kolejności WPA/WPA2 (tryb mieszany uwzględniający obecność zarówno nowszych, jak i starszych urządzeń) i dopiero jako ostateczne, kompromisowe rozwiązanie tryb WPA-TKIP (tylko jeśli nie jest obsługiwany tryb WPA/WPA2). Nie zaleca się stosowania trybu WEP, jako niebezpiecznego, ani tym bardziej trybu niezabezpieczonego.
- przypisywanie stałego adresu IP do adresów sprzętowych oraz kart sieciowych.

Jeśli udostępniasz połączenie internetowe ze swojego smartfona, zabezpiecz je hasłem!

Etap korzystania

- bieżąca aktualizacja oprogramowania routera
- włączone dodatkowe zabezpieczenia: firewall i systemy kontroli włamań.

DODATKOWE ZABEZPIECZENIE RUCHU SIECIOWEGO

Sieć można dodatkowo zabezpieczyć za pomocą systemu wykrywania włamań (IDS – *Intrusion Detection System*) lub systemu zapobiegania włamaniom (IPS – *Intrusion Prevention System*). Zadaniem systemów wykrywania włamań jest np. wykrywanie nietypowych zjawisk w sieci firmowej i alarmowanie administratora, która ma wtedy szansę sprawnie zareagować. Może go w tym wesprzeć system zapobiegania włamaniom, który pozwala np. na:

- zablokowanie dostępu do sieci dla komputera firmowego, który zachowuje się podejrzanie;
- zablokowanie podejrzanych plików przed dotarciem do komputera;
- kontrolę korzystania z aplikacji sieciowych, co umożliwia m.in. odcięcie dostępu do wybranych programów (np. komunikatory, odtwarzacze, starsze wersje przeglądarek).

Rozwiązania z tego zakresu są w ofercie takich firm jak Corero, Fortinet, HP, Net Optics, NETGEAR, Radware czy Sourcefire.

IDS i IPS nie są cudownym remedium na wszelkie zagrożenia ruchu sieciowego – jeśli są źle dostrojone, mogą powodować fałszywe alarmy. To może nie tylko utrudnić pracę, ale też uśpić czujność administratora, który po licznych takich doświadczeniach może zlekceważyć prawdziwe zagrożenie.

ZABEZPIECZONY DOSTĘP DLA GOŚCI

Jeśli Twoja działalność wymaga udostępniania sieci gościom (np. prowadzisz szkolenia wymagające dostępu do internetu), warto wydzielić dla nich sieć izolowaną (bez dostępu do sieci wewnętrznej). Dostęp do ▸

EKSPERT PODPOWIADA

ROBERT DZIEMIANKO

Marketing Manager,
G DATA

Korzystanie z darmowego połączenia WLAN może być przyczyną kłopotów. Wysyłane oraz otrzymywane dane mogą być przechwycone przez przestępców. Co zrobić, aby nie stać się ofiarą tego typu ataków? Najlepiej używać szyfrowanych połączeń, a poza postępować z wyjątkową ostrożnością.

tej sieci warto zabezpieczyć, albo podając gościom tymczasową nazwę użytkownika i hasło, albo ustawiając specjalny portal, gdzie wpisuje się odpowiednie dane (rozwiązanie często stosowane np. w hotelach, kawiarniach czy na lotniskach).

JAK ŁĄCZYĆ SIĘ Z DANYMI I APLIKACJAMI FIRMOWYMI Z ZEWNĄTRZ

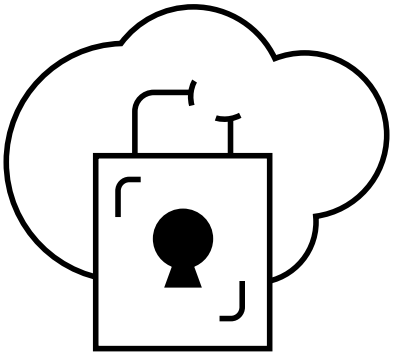
Jeśli sprawy firmowe wymagają od Ciebie lub pracowników łączenia się z zasobami firmowymi (np. poczta czy dyski sieciowe) z różnych miejsc poza firmą, zadbaj o bezpieczne połączenie internetowe. Jeśli nie stosujesz rozwiązań wspierających BYOD, dobrym rozwiązaniem jest VPN (Virtual Private Network – Wirtualna Sieć Prywatna). W takim rozwiązaniu dane przesyłane podczas sesji są zaszyfrowane, co zapewnia im „bezpieczną podróż".

Uwaga! Zasady bezpiecznego łączenia z sieciami bezprzewodowymi dotyczą **wszystkich** urządzeń – od smartfonu przez tablet po laptopy!

Warto korzystać z VPN prywatnego (tj. ustawionego w firmie na urządzeniu zwanym koncentratorem). Odpowiednie ustawienia na komputerze, tablecie czy smartfonie dają możliwość bezpiecznego łączenia się z internetem z dowolnego miejsca na świecie.

Na prostą konfigurację VPN pozwalają m.in. systemy operacyjne (np. w przypadku Windows 10 przy odpowiednich ustawieniach kanał VPN sam uruchamia się w tle). Dobierając rozwiązanie, należy zwracać uwagę na wiarygodność (w tym referencje) dostawcy oraz posiadane przez niego zasoby (sieci, globalne serwery).

VPN jest rozwiązaniem bardziej godnym polecenia niż korzystanie z publicznych sieci Wi-Fi, które nigdy nie dają gwarancji bezpieczeństwa. Nie wiesz, jaki rodzaj zabezpieczeń ma dana sieć ani czy w ogóle jest prawdziwa – oszuści udostępniają sieci pod nazwami podobnymi do wiarygodnych dostawców (np. nazwa hotelu). Podłączenie do takiej sieci zwykle skutkuje zainfekowaniem komputera złośliwym oprogramowaniem, które może choćby modyfikować treści przesyłanych stron, np. zmieniać numery kont lub wyświetlać fałszywe formularze logowania.



BEZPIECZNA CHMURA

Przeczytaj, jeśli:

- **chcesz bezpiecznie i wygodnie pracować także poza biurem**
- **myślisz o przejściu do chmury i nie wiesz, jak wybrać dostawcę**
- **obawiasz się, czy dane na Twoim firmowym serwerze są odpowiednio zabezpieczone**
- **masz za mało miejsca na serwerze albo musisz wymienić stare urządzenia**

Każdej firmie przybywa danych, plików, narzędzi i aplikacji. Przynajmniej do części z nich pracownicy – np. handlowcy w podróżach służbowych – powinni mieć dostęp także spoza biura. Jeśli widzisz, że potrzebujesz takiego rozwiązania, a do tego kończy Ci się miejsce na firmowym serwerze, sprawdź, jak bezpiecznie przechowywać firmowe dane i uruchamiać aplikacje.

Tradycyjnie w siedzibie firmy znajduje się serwer. Mieszczą się na nim dane oraz wszystkie systemy informatyczne, np. program księgowy z bazą klientów. Dziś, kiedy przybywa i danych, i narzędzi do ich przetwarzania, można przechowywać je także poza firmą – wykorzystując zasoby dostawcy usług chmurowych, umieszczone w odpowiednio zabezpieczonych centrach danych. Takie usługi dostarczają m.in. Microsoft (Azure) czy Amazon (Amazon Web Services). Nie brakuje też krajowych dostawców – są to m.in. Beyond, Exea czy Oktawave.

W zależności od miejsca przechowywania danych, można mówić o kilku rodzajach chmur. Jeśli wynajmujesz przestrzeń na serwerze należą- ▸

EKSPERT PODPOWIADA

ŁUKASZ PIĄTKOWSKI

Product Manager
Microsoft Azure

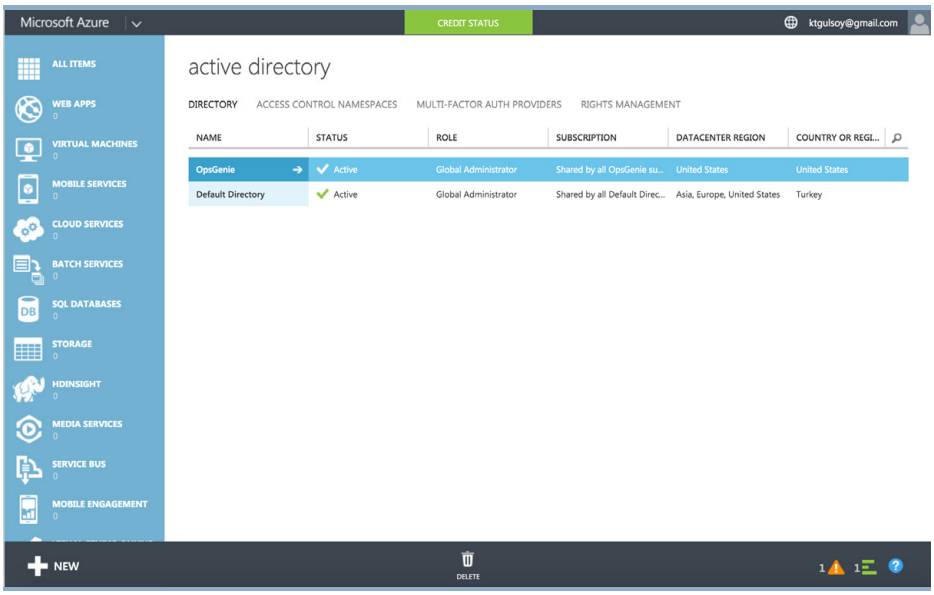
Usługa backupu całego serwera (np. Azure Site Recovery) to mechanizm, który umożliwia ciągłość pracy aplikacji i usług. Chmura monitoruje serwer objęty tą usługą – „patrzy", czy działa i cały czas tworzy w drugim środowisku (często oddalonym) urządzeniu kopię zawartości chronionego serwera. Jeśli serwer przestaje działać, usługa zapewnia automatyczne przełączenie się na zapasowe środowisko drugiego serwera.

cym do usługodawcy, korzystasz z chmury publicznej. Jeśli Twój serwer znajduje się we własnym centrum przetwarzania, mówimy o chmurze prywatnej. Możliwe jest też rozwiązanie hybrydowe, kiedy część zasobów mieści się na Twoich serwerach, a część – w wynajętej infrastrukturze.

Gdyby usługi przetwarzania w chmurze ograniczały się tylko do wynajmu bezpiecznego magazynu na Twoje dane, byłaby to skromna oferta. Korzystanie z chmury umożliwia m.in.:

- **bezpieczne łączenie z dowolnego miejsca z firmowymi aplikacjami działającymi w chmurze** – ważne i potrzebne, jeśli Twoi pracownicy często pracują poza biurem. Warto skorzystać z usługi bezpiecznego łączenia się z zasobami informatycznymi, która nosi nazwę wirtualnej sieci prywatnej (VPN). Jeśli trzeba przesyłać dane przez internet, połączenie musi być stabilne i bezpieczne. Można wybrać połączenie sieciowe, przeznaczone wyłącznie dla Twojej firmy (np. rozwiązanie ExpressRoute z oferty Microsoft).
- **backup, czyli pierwszy krok do bezpieczeństwa danych oraz mechanizm zapewniający ciągłość pracy serwerów** – zaawansowane tworzenie kopii zapasowych (plików i konfiguracji całych serwerów). W przypadku awarii podstawowego serwera zaczyna pracować drugi, na którym mieści się kopia zapasowa. Tworzenie kopii zapasowych oraz przełączanie środowisk odbywa się automatycznie.
- **łatwe zarządzanie pracownikami** korzystającymi z plików i aplikacji. – *To dobre rozwiązanie dla firm, które chętnie i dużo pracują zdalnie i są przekonane do rozwiązań chmurowych* – wyjaśnia Marcin Klimowski (Windows Product Marketing Manager) – *W odpowiednim panelu można dodać użytkowników i zarządzać ich tożsamościami – przypisać hasła do aplikacji i nadać uprawnienia do korzystania z nich. Łatwo jest również odebrać uprawnienia osobie, która przestaje pracować w firmie. To proste rozwiązanie także z punktu widzenia pracowników. Jednorazowo logując się na specjalnej stronie, użytkownik może korzystać ze wszystkich aplikacji, które są z nim powiązane, bez konieczności wielokrotnego logowania do każdej z nich (rozwiązanie takie nosi nazwę Single Sign-On,*

SSO—jednokrotne logowanie). Bezpieczeństwo takiego rozwiązania można wzmocnić dodatkowym uwierzytelnianiem (tzw. uwierzytelnienie wieloskładnikowe, multi-factor authentication).



Panel zarządzania pracownikami – Azure Active Directory

DLA KOGO SAAS?

BARBARA MICHALSKA

Product Manager
Office 365

Model SaaS często wybierają firmy korzystające tylko z wybranych funkcji danego programu albo używające go okresowo (np. firmy zatrudniające pracowników sezonowych). Dobrym przykładem jest Excel, używany np. przez handlowców w innej wersji niż przez pracowników magazynu. Miesięczny abonament pozwala go równie łatwo włączyć, jak i wyłączyć.

CHMURA CZY WŁASNA SERWEROWNIA?

Rozważając korzystanie z chmury, szefowie firm najczęściej obawiają się wyprowadzania danych na zewnątrz. Mają poczucie, że na własnym serwerze dane te są bardziej bezpieczne. Zbyt często jest to jednak bezpieczeństwo pozorne. Wcale nierzadko zdarza się, że firmy zaniedbują odpowiednią konfigurację serwera czy narażają go na fizyczne uszkodzenia, np. trzymając urządzenia w źle zabezpieczonych pomieszczeniach. Klasycznym przykładem jest źle dobrana klimatyzacja – jeśli zastosujesz zwykły klimatyzator, w trudnych warunkach (np. środek upalnego lata), może on nie poradzić sobie ze skutecznym obniżeniem temperatury w serwerowni. Łatwo wtedy o przegrzanie i awarię urządzeń. Dodajmy do tego, że mniejsze firmy często nie mają na miejscu administratora serwera albo serwerem opiekuje się informatyk „do wszystkiego". Problem z serwerem może więc oznaczać dłuższe przestoje.

— *Prawidłowy poziom bezpieczeństwa, bariery fizyczne (zapory czy odpowiednia ilość kamer), zabezpieczenie ciągłej pracy urządzeń (klimatyzacja precyzyjna, ochrona przeciwpożarowa, agregaty prądotwórcze na wypadek przerw w dostawie prądu), odpowiednie zabezpieczenie danych – to wszystko oznacza duże inwestycje, na które małe i średnie firmy często po prostu nie stać. Profesjonalny dostawca usług chmurowych, który się w tym specjalizuje i obsługuje tysiące klientów w swoim centrum przetwarzania danych, dzięki efektowi skali, może sobie pozwolić na taką inwestycję* – wyjaśnia Łukasz Piątkowski (Product Manager, Microsoft Azure).

33%

Tyle firm w Polsce korzysta z chmury obliczeniowej (według raportu PwC, *W obronie cyfrowych granic* 2016).

CHMURA TO PRZYSZŁOŚĆ PRODUKTÓW

Z przetwarzania w chmurze korzystasz również, sięgając po nowe wersje znanych produktów czy usług (np. Office 365). W takim rozwiązaniu, zamiast kupić pudełko i instalować program na komputerach firmowych, płacisz abonament za licencję do korzystania z usługi.

Takie rozwiązanie nosi nazwę SaaS (Software as a Service – oprogramowanie jako usługa) i jest coraz częściej spotykane. Zaletą takiego rozwiązania jest m.in. brak długotrwałych wdrożeń oraz uniknięcie jednorazowej dużej inwestycji. W modelu SaaS dostępne są np. programy graficzne, których jednorazowy zakup bywa barierą, a miesięczne opłaty abonamentowe mieszczą się w granicach ich możliwości.

Główną zaletą programów dostępnych jako SaaS jest łatwość ciągłego z nich korzystania. Aplikacje SaaS są dostępne zarówno przez przeglądarkę na dowolnym komputerze, jak i na urządzeniach przenośnych. W przypadku ***Office 365*** *dotyczy to także systemów iOS czy Android. Model ten umożliwia zespołom łatwą i nieograniczoną pracę na jednym dokumencie oraz bardzo ułatwia dostęp do firmowych plików, np. daje handlowcowi możliwość łatwego zerknięcia do cennika w czasie spotkania* – mówi Barbara Michalska (Product Manager Office 365).

Krótko o przejściu z rozwiązań pudełkowych na chmurowe („tradycyjny" Office na Office 365)

Mariusz Pleban, Prezes agencji PR Multi Communications:
Koszty licencji obniżyliśmy o 20%. Skróciliśmy też czas zarządzania serwerami do 60%. Przy poprzednim rozwiązaniu prace administracyjne zajmowały nam 4 godziny każdego dnia, a teraz wystarczy kilka godzin tygodniowo.

EKSPERT PODPOWIADA

BARBARA MICHALSKA

Product Manager, Office 365

Zwróć uwagę, jaki poziom niezawodności działania usługi gwarantuje dostawca oprogramowania w modelu SaaS oraz czy zapewnia backup danych.

ZANIM POWIESZ „TAK" DOSTAWCY CHMURY

Jeśli zdecydujesz się przejść na rozwiązania chmurowe, rozsądnie wybierz ich dostawcę. Przedsiębiorcy powinni zwrócić uwagę na następujące aspekty:

- **czy dostawca ma certyfikat bezpieczeństwa Tier III** czy **Tier IV**. Certyfikat ten mówi o tym, że zewnętrzny audytor sprawdził, jak bezpieczne jest centrum przetwarzania danych. Przykładowo, Tier III mówi o stopniu bezpieczeństwa n+1: wszystkie urządzenia (nie tylko serwery, ale też m.in. klimatyzatory) są w nadmiarze. Ewentualna awaria jednego oznacza więc, że jego pracę może przejąć ten nadmiarowy.
- **jak dostawca usług dba o powierzone mu dane** (czy zapewnia bezpieczeństwo, poufność i integralność danych). Dostawca powinien mieć ważny (zwróć uwagę na datę!) certyfikat zgodności z normą ISO:27001:2013 lub ISO:27018:2014. Certyfikat ten potwierdza, że firma pozytywnie przeszła zewnętrzny audyt, sprawdzający zgodność działania firmy z procedurami podanymi w normie.
- **gdzie są przechowywane Twoje dane**. Sprawdź, czy możesz decydować, gdzie uruchamiane są Twoje usługi i przechowywane dane – szczególnie upewnij się, czy choć jedno centrum przetwarzania znajduje się na terenie Unii Europejskiej. Usługi chmurowe pozwalają dodatkowo na tworzenie kopii zapasowych Twoich systemów i danych w dowolnie wybranym centrum na świecie.

- **czy Twoje zasoby mogą być umieszczone w różnych strefach dostępności.**
- **czy dostawca ma usługi dla małych i średnich firm**, które będą rzeczywiście zgodne z Twoimi potrzebami, np. pozwolą Ci opłacać abonament za przestrzeń dopasowaną do Twoich potrzeb (nie za dużą ani nie za małą). Dobry dostawca powinien, niezależnie od wielkości Twojej firmy, zaproponować Ci najlepsze dla Ciebie rozwiązanie, składające się z odpowiednio dobranych usług chmurowych.

Łukasz Piątkowski,
Product Manager Microsoft Azure

W centrum przetwarzania, bez dodatkowych opłat, przechowujemy nie tylko oryginał, ale i dwie kopie danych. Oczywiście, są one fizycznie trzymane w innych miejscach serwerowni niż oryginał. Szczególnie cenne dane można dodatkowo zabezpieczyć poprzez umieszczenie kolejnego zestawu kopii w innej, wybranej lokalizacji geograficznej. Zabezpieczenia te można ustawić dosłownie kilkoma kliknięciami.

PRZYKŁAD WDROŻENIA

Biuro podróży Neckermann Polska (130 pracowników) stanęło przed kilkoma problemami informatycznymi, m.in. dział IT notorycznie zmagał się z ograniczoną powierzchnią dyskową.

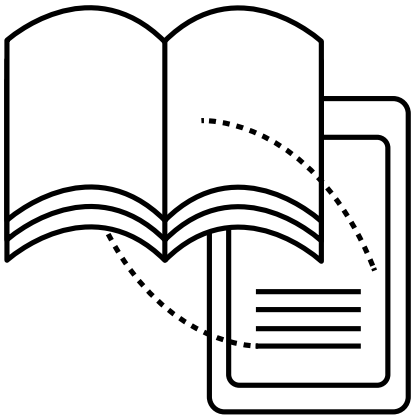
– *Wraz z dynamicznym rozwojem firmy liczba jej danych zwiększyła swoją objętość, co wymusiło na nas konieczność rozbudowy posiadanych urządzeń. Wiedzieliśmy, że to jedynie doraźne rozwiązanie na kolejny rok ograniczające nasze plany, ale i mające wpływ również na bezpieczeństwo chociażby poprzez ograniczenie możliwości backupu danych* – mówi Dariusz Wronikowski, kierownik działu IT w Neckermann.

Skorzystanie z usług w chmurze pozwoliło firmie ograniczyć koszty związane z zakupem lub rozbudową serwerów. Wybierając dostawcę, Neckermann zwrócił uwagę m.in. na stabilność usługi, możliwość jej rozwoju i rozbudowy, odporność na awarie, bezpieczeństwo oraz możliwość integracji z innymi usługami. Do tego doszła dostępna przestrzeń i cena. Firma wybrała **usługę Microsoft Office 365**. Wśród podstawowych korzyści firma wymienia m.in. automatyczny backup oraz nieograniczone wersjonowanie, dostęp do zasobów z dowolnego urządzenia oraz miejsca czy brak infrastruktury serwerowej.

– Kiedyś nasi administratorzy wykonywali prace związane z monitorowaniem oraz sprawdzeniem backupu, miejsca dostępnego na dyskach, aktualności oprogramowania i czytaniem logów bezpieczeństwa. Obecnie wszystkie funkcje zostały przeniesione na usługę Microsoft – teraz tylko jeden administrator zarządza całością usług poprzez konsolę web – mówi Dariusz Wronikowski, kierownik działu IT w Neckermann.

► Do zapamiętania

1. Wybieraj sprawdzonego dostawcę zarówno usług chmurowych, jak i programów działających w chmurze. Zwróć uwagę na posiadane certyfikaty, gwarantowany poziom niezawodności działania usługi oraz usługę backupu.
2. Wybierz dostawcę usług chmurowych, którego centra przetwarzania danych mieszczą się w Europie (najlepiej w UE).
3. Zadbaj o bezpieczne i stabilne połączenie internetowe z firmowymi zasobami przechowywanymi w chmurze.
4. Zabezpiecz zasoby przechowywane w chmurze – oprócz silnego hasła zastosuj uwierzytelnienie dwuskładnikowe (np. konieczność podania poza hasłem także kodu otrzymanego SMS-em).



BEZPIECZNA STRONA WWW

Przeczytaj, jeśli:

- **masz sklep internetowy**
- **masz na stronie firmowej formularz zapisu do newslettera**
- **prowadzisz system zamówień B2B lub chcesz go stworzyć**
- **strona www jest (lub ma być) kluczową częścią Twego biznesu**
- **dbasz o bezpieczeństwo w sieci nie tylko swojej firmy, ale i swoich klientów**

Twoi klienci wiedzą coraz więcej. Znają swoje prawa i Twoje obowiązki jako przedsiębiorcy, interesują się ochroną przed zagrożeniami w internecie. Będą więc zwracać coraz większą uwagę na to, czy mogą bezpiecznie kupować na Twoich stronach i korzystać z Twoich usług w sieci.

3 GŁÓWNE ASPEKTY BEZPIECZEŃSTWA STRONY WWW

1. Ma działać w sposób ciągły, nie powinno być możliwości zablokowania jej z zewnątrz.
2. Ma być szczelna, nie mogą wyciec z niej dane (np. nazwy użytkowników i hasła klientów).
3. Nawet w przypadku zwiększenia ruchu, powinna działać wydajnie. ▸

EKSPERT PODPOWIADA

ŁUKASZ PIĄTKOWSKI

Product Manager
Microsoft Azure

Microsoft Azure oferuje – niezależnie od tego, czy system działa w serwerowni klienta, w środowisku zwirtualizowanym czy w chmurze publicznej – usługę odpowiedzialną za automatyczne uruchomienie środowiska zapasowego, gdy nastąpi awaria. Po odzyskaniu stabilności systemu lub usługi podstawowej, Azure samoczynnie przywróci przetwarzanie do pierwotnej lokalizacji.

ZADBAJ O CIĄGŁOŚĆ DZIAŁANIA STRONY

Przerwa w działaniu takich stron jak e-sklep czy platforma zamówień to katastrofa – wizerunkowa i finansowa, bo wraz ze straconymi zamówieniami tracisz pieniądze. Może być wynikiem awarii lub ataku DDoS (Distributed Denial of Service – dosł. rozproszona odmowa usługi).

Przestępcy mogą zablokować Twoją stronę, np. „zapychając" ją milionami udawanych prób logowania. Przeciążona strona przestaje działać. Taka przygoda w w 2014 r. spotkała wiele polskich firm, np. Allegro. Według CERT Polska (Computer Emergency Response Team, w Polsce część NASK), właśnie w 2014 r. liczba ostrzeżeń o atakach DDoS na polskie firmy (w tym małe i średnie!) przekroczyła 100 tys.

JAK ZACHOWAĆ CIĄGŁOŚĆ PRACY STRONY

Zapobieganie awariom

Możesz np. skorzystać z rozwiązania chmurowego, mieć kilka kopii swojej strony i trzymać ją w kilku miejscach. W przypadku awarii następuje automatyczne przełączenie na usługę zapasową.

Obrona przed atakami

W pewnym uproszczeniu za odporność na ataki DDoS odpowiada serwer. Trzeba więc zwrócić uwagę na jego zabezpieczenie:

- zapytaj informatyków, czy stosowane są zabezpieczenia przed DDoS (np. czy firmowe serwery są wyposażone w filtr „złego" ruchu internetowego).
- ochrona przed DDoS nie jest tania. Rozważ całkowitą lub częściową rezygnację z serwerów firmowych na rzecz skorzystania z serwerów zewnętrznych (tzw. chmura publiczna). Dostawca takich usług zabezpiecza serwery przed atakami bardziej skutecznie, niż może to zrobić we własnym zakresie Twoja firma.

JAK POKAZAĆ KLIENTOM, ŻE DBASZ O ICH DANE

Klienci coraz częściej zwracają uwagę na to, jak usługodawcy dbają o poufność ich danych (np. loginów i haseł w sklepie internetowym). Możesz poprawić swoją wiarygodność, jeśli Twoja strona www będzie stroną z „bezpiecznym połączeniem".

Strony z bezpiecznym połączeniem można poznać po zielonej kłódce, https:// na początku adresu i komunikacie przeglądarki (po kliknięciu w kłódkę) o zabezpieczonym połączeniu.
„Bezpieczne połączenie" oznacza, że dane (np. loginy i hasła) wpisane na tej stronie zostaną zaszyfrowane, zanim powędrują z przeglądarki lub aplikacji klienta do Twojego serwera. Do szyfrowania najczęściej stosuje się technologię zwaną SSL (Secure Socket Layer).

Dlaczego to ważne? Przestępcy próbują „podsłuchiwać" wędrujące w internecie dane – jeśli przechwycą dane niezaszyfrowane, to tak, jakby ktoś im je po prostu podał. A jeśli trafią na dane zaszyfrowane, nie będą mogli ich wykorzystać.

„BEZPIECZNE POŁĄCZENIE" – JAK TO ZROBIĆ?

Przyjęło się, że z bezpiecznego połączenia korzystają np. banki czy instytucje publiczne. Ale mała i średnia firma też może mieć „bezpieczne połączenie", nie poświęcając na to dużo czasu ani pieniędzy. Musisz uzyskać certyfikat, zwany certyfikatem SSL. Jest to po prostu plik, który należy wstawić na serwer, na którym znajduje się Twoja strona firmowa. Kiedy klient otworzy stronę, przeglądarka „zobaczy" ten plik i będzie wiedzieć, że dane mają wędrować jako zaszyfrowane, a strona ma się wyświetlać jako bezpieczna.

SKĄD WZIĄĆ CERTYFIKAT?

- Certyfikat zamawiasz w zewnętrznej instytucji

Jak wybrać wystawcę certyfikatu.
Certyfikat należy zamówić w firmie, która ma uprawnienia od instytucji rządowej (w Polsce od Narodowego Centrum Certyfikacji) i spełnia standardy międzynarodowej organizacji WebTrust.

Polskie uprawnione firmy: EuroCert, Krajowa Izba Rozliczeniowa, Polska Wytwórnia Papierów Wartościowych, Unizeto.

Certyfikaty WebTrust
Tylko certyfikat wystawiony przez firmę z uprawnieniami i spełniającą standardy sprawi, że przeglądarka rozpozna Twoją stronę jako bezpieczną.

- Certyfikat to potwierdzenie, że nie podszywasz się pod właściciela strony, tylko naprawdę nim jesteś. Jest kilka poziomów certyfikatów. Certyfikat na poziomie najniższym (najtańszy i chętnie wykorzystywany przez mniejsze firmy) potwierdza, że domena jest Twoja.

Masz do wyboru kilka opcji cenowych. Za dość niską cenę możesz uzyskać certyfikat dla jednej wybranej strony.

Uzyskiwanie certyfikatu krok po kroku:

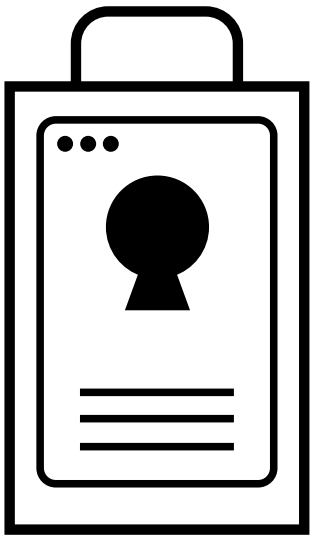
- zamówienie przez stronę instytucji,
- opłacenie usługi,
- weryfikacja danych przez instytucję,
- przesłanie mailem pliku certyfikatu,
- wstawienie otrzymanego pliku na serwer.

Co jeszcze warto wiedzieć o certyfikatach:

- Certyfikat wydawany jest na określony czas – zwykle 1, 2 lub 5 lat. Kiedy minie okres ważności, klienci wchodzący na Twoją stronę widzą komunikat, że certyfikat jest nieważny.
- Ostrożnie z pozornymi oszczędnościami. Możesz spotkać się z bardzo tanimi certyfikatami od firm, które nie są zaufanymi dostawcami. Możesz także znaleźć program, który pozwala na samodzielne wystawienie certyfikatu. Szczerze odradzamy. Przeglądarka uzna certyfikat od niezaufanego dostawcy za nieprawidłowy i wyświetli klientowi ostrzeżenie o zagrożeniu.
- Jeśli usłyszysz od swojego informatyka: „A może lepiej szyfrowanie TLS?", zgódź się. TLS (Transport Layer Security – protokół bezpiecznej transmisji) to następca technologii SSL, uważany za jeszcze bardziej bezpieczny.
- Strony z bezpiecznym połączeniem są wyżej pozycjonowane w wyszukiwarkach.

► Do zapamiętania

1. Właściciela każdej małej i średniej firmy stać na bezpieczną stronę www.
2. O bezpieczeństwie strony decydują:
   a. sposób jej wykonania;
   b. bezpieczeństwo serwera, na którym jest umieszczona,
   c. trzymanie się prostych zasad (np. aktualizacja oprogramowania).



POLITYKA BEZPIECZEŃSTWA W FIRMIE

Przeczytaj, jeśli:

- **chcesz, żeby pracownicy przestrzegali zasad bezpieczeństwa IT w firmie**
- **chcesz widzieć , jak szybko i łatwo stworzyć politykę bezpieczeństwa w firmie**

Technologie zapewniające bezpieczeństwo nie na wiele się zdadzą, jeśli wszyscy pracownicy nie będą znali, rozumieli i stosowali się do obowiązujących zasad bezpieczeństwa. Dopiero wtedy można powiedzieć, że firma jest zabezpieczona przed zagrożeniami ery cyfrowej.

– Często spotykałem się z tym, że firma była świetnie zabezpieczona od strony infrastruktury, natomiast kwestie „czynnika ludzkiego" były całkowicie pominięte, co narażało właściciela na poważne konsekwencje (od zawirusowania po kompromitujący wyciek danych) – mówi Arkadiusz Zakrzewski, dyrektor pomocy technicznej CORE, dystrybutora programu antywirusowego AVG w Polsce. *– Przedsiębiorcy nie mogą zapominać, że pracownik jest ważnym ogniwem zabezpieczeń, a duża część infekcji wynika właśnie z błędu ludzkiego i ignorowania (nieraz podstawowych) zasad bezpieczeństwa.*

Rozmowę o tym, by Twoi pracownicy przestrzegali zasad bezpieczeństwa, trzeba zacząć od ich ustanowienia. Dlatego w każdej firmie, nie ▸

EKSPERT PODPOWIADA

BARTOSZ PUDO

Kancelaria Adwokatów i Radców Prawnych Ślązak, Zapiór i Wspólnicy

Obowiązek opracowania polityki bezpieczeństwa dotyczy wszystkich administratorów danych osobowych. W praktyce więc każdy przedsiębiorca zatrudniający przynajmniej jednego pracownika lub przetwarzający w jakikolwiek sposób dane swoich klientów – osób fizycznych – musi posiadać politykę bezpieczeństwa (podstawa prawna: **Rozporządzenie MSWiA z dn. 29 kwietnia 2004 r.)**

zależnie od wielkości, powinna powstać **polityka bezpieczeństwa**, czyli zbiór zasad, obowiązujący wszystkich, spisany w czytelnej i zwięzłej formie oraz udostępniony tak, aby każdy mógł się z nim zapoznać.

Czy wiesz, że blisko 80% małych firm (dane firmy Vipre Security) uważa, że mogą się obyć bez polityki bezpieczeństwa? Ich szefowie często są przekonani, że opracowanie polityki bezpieczeństwa jest czasochłonne i skomplikowane. Tymczasem zwykle wystarczy prosta, zrozumiała dla wszystkich lista obowiązujących zasad.

Polityka bezpieczeństwa będzie stosowana, jeśli pracownicy będą ją znać i rozumieć. Dlatego warto nie tylko rozdać pracownikom oficjalny dokument, ale i proste wyciągi z obowiązujących zasad (przykłady takich wyciągów znajdziesz w Niezbędniku).

PODSTAWY POLITYKI BEZPIECZEŃSTWA

Polityka bezpieczeństwa dla każdej firmy będzie inna. Oto, jakie elementy mogą się w niej znaleźć.

1. **Odpowiednie stosowanie haseł.** Hasła na wszystkie urządzenia – ze smartfonami włącznie – muszą być silne, czyli długie (min. 13 znaków) i możliwie skomplikowane. Janek Kowalski nie powinien więc logować się z hasłem „Kowalski" – hasło nie powinno kojarzyć się z jego danymi, musi też (to absolutne minimum) zawierać jedną dużą literę i znak specjalny. Takie hasło należy regularnie zmieniać. **Dbanie o bezpieczeństwo haseł to absolutnie podstawowy warunek bezpieczeństwa.** Dlatego w Niezbędniku zamieszczamy szczegółowe wyjaśnienia dotyczące bezpieczeństwa haseł.
2. **Rodzaje danych.** W polityce bezpieczeństwa należy jasno podzielić dane na kategorie (np. według wpływu na biznes lub według wrażliwości) i określić, jak postępować z każdą z nich. Przykładowo, dane osobowe albo tajemnice handlowe zaliczymy do „danych o dużym wpływie na biznes" lub do „danych o dużej wrażliwości", które powinny być traktowane ze szczególną ostrożnością.

3. **Nadawanie dostępu.** Nie wszyscy pracownicy muszą mieć dostęp do wszystkich danych. W pewnych przypadkach administrator powinien nadać dostęp tylko dla wybranych osób – co powinno być jasno określone i wymagane. Nie może dochodzić do sytuacji, gdy jeden pracownik pracuje na koncie drugiego kolegi, bo „nie chciało się przełączyć".
4. **Instalowanie oprogramowania.** Czasami pracownicy instalują na firmowych komputerach programy do celów prywatnych, dla rozrywki lub dla ułatwienia sobie zadań – bez wcześniejszego uzgodnienia. Może się to skończyć zainfekowaniem komputera, szczególnie jeśli oprogramowanie zostało pobrane z niepewnego źródła. Konsekwencje takiego ataku mogą wykraczać poza jeden komputer. Przestępcy posługują się sprytnym chwytem. Zwykle po zauważeniu problemów z komputerem loguje się na niego użytkownik z większymi uprawnieniami (np. informatyk), co może ułatwić przejęcie kontroli nad kolejnymi maszynami.
5. **Zabezpieczenia komputerów.** Każdy komputer powinien mieć zaktualizowany system operacyjny i zabezpieczenia takie jak oprogramowanie antywirusowe czy firewall (sporo na ten temat w poradniku). Najlepiej, jeśli na komputerze są wydzielone konta dla pracowników z logowaniem na hasło.
6. **Transport danych, urządzenia zewnętrzne, korzystanie z własnych urządzeń (BYOD).** Powinno być jasne, na jakich zasadach pracownikom wolno używać nośników takich jak pendrive'y oraz czy w pracy można używać swoich prywatnych urządzeń. Jeśli tak, zasady korzystania z tych urządzeń powinny być jasno określone.
7. **Korzystanie z usług online.** Nierzadko zdarza się, że pracownicy ułatwiają sobie pracę przy pomocy usług online, z których korzystają prywatnie. Coraz bardziej powszechnym przykładem jest korzystanie z usług chmurowych do przechowywania plików, co rodzi ryzyko celowego lub przypadkowego udostępnienia danych osobom niepowołanym. Często pojawiają się też komunikatory (np. stosowane między biurami lub do kontaktów z niektórymi klientami), takie jak Skype, Google Hangouts czy Facebook Messenger. Po- ▸

lityka bezpieczeństwa powinna określać, na jakich zasadach można korzystać z „prywatnych" usług online, w tym – w jakim zakresie można korzystać z popularnych komunikatorów na urządzeniach firmowych lub na urządzeniach prywatnych do celów służbowych.

8. **Oddzielenie danych firmowych od prywatnych.** Wszelkie dane firmowe powinny pozostać w firmie. Najbardziej podstawowy przykład to poczta elektroniczna. Przykładowo, pracownicy mogą używać prywatnych kont e-mail – to się zdarza, kiedy pracownik zapomni hasła do służbowego konta i musi coś szybko wysłać albo konto firmowe jest chwilowo niedostępne, a trzeba szybko przesłać informację. Należy jasno wskazać, że bezwarunkowo nie wolno podawać firmowego adresu e-mail na forach, na listach adresowych czy w mediach społecznościowych. Nie należy też korzystać ze służbowego adresu do spraw prywatnych (ani na odwrót).
9. **Kopie zapasowe.** Jasno określ zasady ich tworzenia, odpowiadając na następujące pytania: Jak często robimy kopie zapasowe? Gdzie robimy kopie zapasowe? Jakie dane są kopiowane? Czy tworzymy kopie w dwóch miejscach? Jeśli tak, to których danych?
10. **Proste procedury bezpieczeństwa.** Pracownicy muszą być po prostu uważni – ale też warto ich w tym wspomóc odpowiednimi technologiami. W marcu 2015 roku dane dotyczące Obamy, Putina, Merkel i innych ważnych polityków zostały przypadkowo ujawnione przez urzędnika, który zagapił się przy wysyłaniu e-maila. Po prostu wysłał wrażliwe dane pod niewłaściwy adres. Nie doszłoby do tego, gdyby używał technologii RMS (Rights Management Server), która zabezpiecza m.in. przed wysłaniem e-maila pod adres spoza domeny firmowej.
11. **Aktualizowanie wiedzy o bezpieczeństwie.** Żadne rozwiązanie z zakresu bezpieczeństwa nie wystarczy raz na zawsze, gdyż wraz z nowymi zagrożeniami pojawiają się nowe możliwości zapobiegania im. W firmie powinien istnieć system szkoleń – i to nie tylko wprowadzenie dla nowych pracowników. Ważne są też szkolenia okresowe, pozwalające nie tylko zapoznać pracowników z nowymi zasadami, ale i upewnić się, że znają i przestrzegają tych już obowiązujących. ▸

EKSPERT PODPOWIADA

MICHAŁ SAJDAK

Ekspert bezpieczeństwa Securitum.pl

Gdybym układał politykę bezpieczeństwa, na pewno zapisałbym w niej stałe podnoszenie edukacji pracowników z obszaru bezpieczeństwa IT.

ODDZIELIĆ SPRAWY FIRMOWE OD PRYWATNYCH

W wielu współczesnych przedsiębiorstwach ważnym elementem będą zasady korzystania z urządzeń przenośnych (polityka BYOD, *Bring Your Own Device*). Należy wskazać, na ile pracownicy mogą korzystać ze swoich firmowych urządzeń do celów prywatnych lub odwrotnie – jakie są zasady korzystania do celów firmowych z prywatnych telefonów, tabletów czy laptopów.

Ustal zasady korzystania z poczty firmowej do celów prywatnych. Jeśli chcesz monitorować korespondencję pracowników, zwróć uwagę na ważne zasady.

– Efektywna i zgodna z prawem kontrola korespondencji służbowej może być realizowana wyłącznie w przypadku, gdy monitoringiem objęte zostają ***służbowe*** *skrzynki poczty elektronicznej pracowników, a pracownicy zostają pouczeni o zakazie wykorzystywania tego narzędzia w celu prowadzenia korespondencji prywatnej* – wyjaśnia Bartosz Pudo.

– Istotnym jest, iż każda z osób, których korespondencja podlegać ma tego rodzaju kontroli, musi zostać o tym fakcie uprzednio poinformowana. Nie jest natomiast konieczne wyrażenie przez pracownika zgody na takie działania pracodawcy – dodaje Bartosz Pudo.

EKSPERT PODPOWIADA

BARTOSZ PUDO

Kancelaria Adwokatów i Radców Prawnych Ślązak, Zapiór i Wspólnicy

Na gruncie przepisu art. 23 Kodeksu cywilnego, a przede wszystkim art. 49 Konstytucji RP, każdemu zapewnia się ochronę tajemnicy korespondencji. Ochrona ta nie ma charakteru absolutnego i nie rozciąga się w szczególności na przypadki monitorowania treści korespondencji służbowej przez pracodawcę.

CO JESZCZE WARTO WIEDZIEĆ

W polityce bezpieczeństwa należy też ująć warunki odpowiedzialności pracowników za naruszenia zasad.

Polityka bezpieczeństwa może (i musi) być wspierana specjalistycznym oprogramowaniem. Przykłady zamieściliśmy w tym Niezbędniku.

Nie istnieje jeden przepis na idealną politykę bezpieczeństwa. Czy można ją napisać samemu, we współpracy z działem IT? To zależy od stopnia informatyzacji przedsiębiorstwa. Jeśli internet stanowi wspar- ▸

cie pracy biurowej, zwykle własny dokument wystarczy. Przy bardziej złożonych systemach, szczególnie kiedy przechowujesz online dane osobowe klientów (np. w przypadku sklepów internetowych), warto skorzystać ze wsparcia specjalisty. Dobrym pomysłem może się okazać audyt bezpieczeństwa, w ramach którego specjalista sprawdzi zasady i narzędzia bezpieczeństwa w firmie i podpowie, czy czegoś nie brakuje.

Jedno jest pewne: zasady powinny być ustalone i konsekwentnie egzekwowane. Pozwoli to uniknąć szeregu problemów.

Środki bezpieczeństwa IT w firmie są trochę jak zabezpieczenia przeciwpożarowe – tak samo muszą w firmie być, wymagają regularnego testowania i przypominania procedur w sytuacji zagrożenia, a każdy życzyłby sobie, by nigdy nie były naprawdę używane. Muszą być tak samo niezawodne. Początkowo procedury bezpieczeństwa wydają się uciążliwe, ale z czasem wejdą w nawyk, a nawet zostaną docenione.

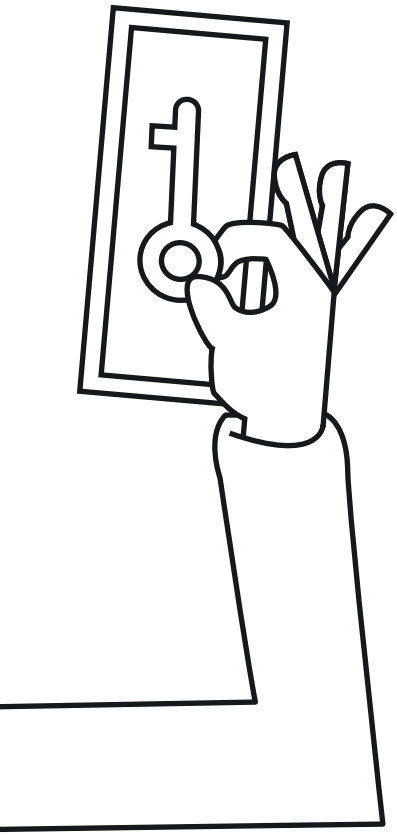
Tworząc politykę bezpieczeństwa uwzględnij, że rosną wymagania UE wobec firm w zakresie bezpieczeństwa IT i ochrony danych osobowych!

Od 25 maja 2018 roku wzrośnie odpowiedzialność firm za przetwarzane przez nie dane osobowe osób fizycznych. W zakresie bezpieczeństwa będą miały m.in. obowiązek:

- skutecznego zabezpieczenia przetwarzanych danych,
- zgłaszania naruszenia ochrony danych organowi nadzorczemu,
- zawiadamiania (w niektórych sytuacjach) osoby, której dane dotyczą, o naruszeniu ochrony danych.

Kwestie te reguluje tzw. pakiet w sprawie ochrony osób fizycznych: Rozporządzenie (UE) 2016/679 oraz Dyrektywa (UE) 2016/680.

Szereg obowiązków (ocena ryzyka zagrożeń IT, wdrożenie środków ochrony, zgłaszanie poważnych incydentów) będą miały od 2017 roku firmy z „sektorów krytycznych": m.in. energetycznego, finansowego, transportowego, ochrony zdrowia, telekomunikacyjnego (np. e-sklepy, wyszukiwarki, usługi w chmurze). Wymusi to dyrektywa NIS (Network and Information Security).



UWAGA NA DANE OSOBOWE!

Przeczytaj, jeśli:

- **chcesz, by dane osobowe na komputerach firmowych były zabezpieczone zgodnie z prawem**
- **użytkownicy lub klienci podają na Twoich stronach adresy e-mail (np. do logowania)**

Na pewno zbierasz i przetwarzasz dane osobowe. Dotyczy to zarówno danych pracowników i klientów, które znajdują się w Twoich zasobach jak I danych użytkowników, którzy logują się na Twojej stronie, zamawiają newsletter czy składają zamówienia.

Twoim prawnym obowiązkiem jest dbanie o bezpieczne przechowywanie danych osobowych.

Obok danych takich jak imię i nazwisko czy adres zamieszkania, wśród danych pozyskiwanych za pośrednictwem stron internetowych, jako chronione przepisami prawa wskazać należy w szczególności adresy poczty elektronicznej (e-mail)—wyjaśnia Bartosz Pudo, prawnik związany z Kancelarią Adwokatów i Radców Prawnych Ślązak, Zapiór i Wspólnicy, specjalizujący się zagadnieniach ochrony danych osobowych.—*Co istotne, ochronie podlegają niezależnie od tego, czy są powszechnie dostępne, np. w internecie. Pogląd ten został wyrażony przez Generalnego Inspektora Ochrony Danych Osobowych. Wobec powyższego, ochronie na podstawie ustawy o ochronie danych osobowych podlegać będzie zbiór adresów e-mail, zebranych na potrzeby mailingu.* ▸

Podstawa Prawna

- Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. 2002 Nr 144 poz. 1204).
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (najnowszy tekst jednolity: Dz. U. 2014 r. poz. 1182).
- Ustawa z dnia 30 maja 2014 r. o prawach konsumenta (Dz.U. 2014 poz. 827).

Zlecając wykonanie czy modernizację strony (np. sklepu internetowego czy platformy obsługi zamówień B2B), zawsze pytaj wykonawcę o to, jak będzie zapewnione bezpieczeństwo Twoich serwisów.

WSZYSTKO POD KONTROLĄ!

– *Zabezpieczenie danych osobowych przetwarzanych przez firmę podlega kontroli Generalnego Inspektora Danych Osobowych* – wyjaśnia dr Edyta Bielak-Jomaa, GIODO. – *Inspektor podczas kontroli sprawdza także bezpieczeństwo fizyczne, czyli zabezpieczenie obszaru, w którym dane osobowe są przetwarzane (m.in. organizacja ochrony, drzwi, zamki, miejsce, gdzie znajduje się serwer etc.).*

DANE OSOBOWE W CHMURZE

Jeśli do przetwarzania danych osobowych korzystasz z zewnętrznego centrum przetwarzania danych, zwróć uwagę na jego lokalizację.

- W przypadku podstawowych usług online Microsoft, centra danych, w których są przechowywane dane klienta tzw. magazynowane (data at rest), znajdują się w Europejskim Obszarze Gospodarczym – wyjaśnia Renata Zalewska, Radca Prawny Microsoft Sp. z o.o. – *Z uwagi na przyjęte w Polsce rozwiązania prawne, przekazywanie danych osobowych do państw Europejskiego Obszaru Gospodarczego podlega ogólnym zasadom przetwarzania danych osobowych wynikającym z polskiej ustawy o ochronie danych osobowych (z wyłączeniem przepisów o przekazywaniu danych do państw trzecich), a więc jest traktowane analogicznie jak transfer danych na terytorium Polski.*
Więcej informacji na ten temat znajduje się na **stronach GIODO**

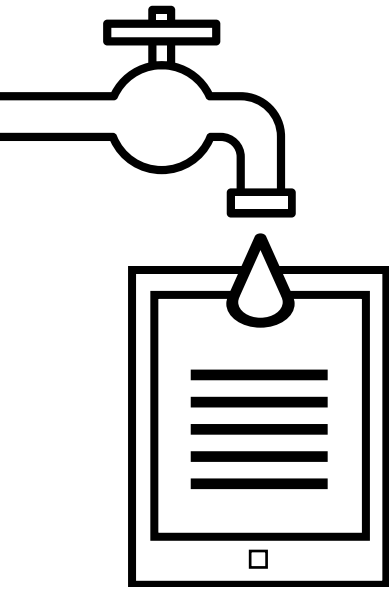
GIODO
Generalny Inspektor
Ochrony Danych Osobowych

ZAPEWNIENIE OCHRONY DANYCH OSOBOWYCH

Dr Edyta Bielak-Jomaa, Generalny Inspektor Ochrony Danych Osobowych, zwraca uwagę na kilka aspektów ochrony danych osobowych:

- Dane osobowe chronimy zgodnie z Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz odpowiednim rozporządzeniem MSWiA.
- Administrator danych osobowych ma obowiązek zapewnić ochronę przetwarzanych danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utrata, uszkodzeniem lub zniszczeniem. Środki zabezpieczające wybiera według własnego doświadczenia.
- Administrator musi prowadzić dokumentację opisującą sposób przetwarzania danych oraz zastosowane środki techniczne i organizacyjne zapewniające ochronę danych osobowych.
- Wymogi dotyczące zabezpieczenia danych przetwarzanych w systemach informatycznych obejmują także bezpieczeństwo fizyczne danych.
- Istnieje kilka poziomów ochrony danych, zależnie od ich kategorii (podstawowy, podwyższony, wysoki). Poziom wysoki dotyczy przetwarzania w systemie informatycznym podłączonym do sieci danych szczególnie chronionych (np. o stanie zdrowia).
- Administrator danych opracowuje instrukcję zarządzania systemem informatycznym, która określa m.in. zasady nadawania uprawnień do przetwarzania danych, procedury uwierzytelniania użytkowników, tworzenie i przechowywanie kopii zapasowych, zabezpieczenia przed działalnością oprogramowania szkodliwego etc.

Na **stronie internetowej GIODO** znajduje się wiele materiałów dotyczących ochrony danych osobowych przetwarzanych w systemach informatycznych. Więcej szczegółów: w specjalnym **PORADNIKU GIODO DLA ADMINISTRATORÓWDANYCH OSOBOWYCH!**



OCHRONA PRZED UTRATĄ I WYCIEKIEM DANYCH

Przeczytaj, jeśli:

- **Twoja firma przechowuje dane w formie elektronicznej**
- **wymieniacie poufne dane firmowe przez internet, np. jako załączniki do e-maili**
- **kilku pracowników pracuje na jednym dokumencie**

Firmy, niezależnie od wielkości, są coraz bardziej narażone na utratę lub wyciek cennych danych firmowych. Dlatego należy wprowadzać procedury, które ograniczą ryzyko utraty kontroli nad danymi, łącząc rozsądek i rozwiązania technologiczne. Zabezpieczenia poufnych danych są dziś dostępne dla każdej firmy.

Dane zabezpieczone przed utratą – kopie zapasowe

Małe i średnie firmy uważają tworzenie kopii zapasowych (backup) danych za podstawową metodę ich zabezpieczenia. Rzeczywiście, przywrócenie ostatniej kopii zapasowej utraconych plików pozwala kontynuować pracę bez większych kosztów w sytuacjach, kiedy:

- komputer firmowy zostanie zniszczony lub zgubiony,

EKSPERT PODPOWIADA

BARTŁOMIEJ MACHNIK

Windows Server Product Manager

Ogromna ilość naruszeń to nie ataki z zewnątrz, a działania wewnątrz organizacji – błędy, niedociągnięcia czy nawet celowe działania. Pracownik – źle przygotowany lub po prostu nieuważny – może się okazać większym zagrożeniem!

- pracownik, celowo lub przez niedopatrzenie, zmodyfikuje zawartość ważnych plików,
- zbuntowany pracownik wykradnie i usunie dane,
- dane na komputerze firmowym zostaną zaszyfrowane przez złośliwe oprogramowanie (tzw. ransomware), a przestępcy będą żądać okupu za ich przywrócenie.

Ponad 25% pracowników zabiera ze sobą dane, opuszczając firmę. Są do tego bardziej skłonni, jeśli to firma rozstanie się z nimi. 85% takich pracowników zabiera własne dokumenty, zaś 25% - dane, które nie są ich dziełem. 95% uważa, że mogli zabrać dane, bo w firmie nie ma polityki bezpieczeństwa lub jej zasady są przez pracowników ignorowane (badania własne firmy Biscom, grudzień 2015).

ZASADY EFEKTYWNEGO TWORZENIA KOPII ZAPASOWYCH:

- twórz kopie zapasowe odpowiednio często – najlepiej automatycznie. Umożliwią Ci to specjalistyczne programy pracujące w tle (np. Data Protection Manager Microsoft), usługi chmury publicznej (np. Azure Backup). Są też programy darmowe i komercyjne,
- kopie zapasowe najważniejszych danych przechowuj w co najmniej dwóch miejscach, w tym przynajmniej jedną poza firmą (w chmurze). Zabezpieczy Cię to przed sytuacją krytyczną, czyli awarią miejsca przechowywania kopii zapasowych,
- ustal z działem IT zasady konfigurowania kopii zapasowych, np. ile czasu ma być przechowywana kopia danego pliku.

Tworzenie kopii zapasowych zabezpieczy Cię przed utratą danych. Pamiętaj jednocześnie, by chronić dane także przed wyciekiem. Czy wiesz, że aż 69% osób odpowiedzialnych za bezpieczeństwo informatyczne w firmach właśnie wyciek danych uważa za najpoważniejsze zagrożenie (badanie Microsoft oraz EY *Security Trends. Bezpieczeństwo w cyfrowej erze*)?

DR EDYTA BIELAK-JOMAA

GIODO

W przypadku teletransmisji danych osobowych podstawowym wymogiem jest zabezpieczenie przesyłanych informacji przed udostępnieniem osobom nieuprawnionym oraz przed utratą, uszkodzeniem lub zniszczeniem. Jeśli administrator danych wykorzystuje przenośne urządzenia zawierające dane osobowe (np. laptop, pendrive), jest zobowiązany do szyfrowania tych danych.

BEZPIECZEŃSTWO INFORMACJI W E-MAILU

Informatycy w firmach czy urzędach uważają, że największe zagrożenie dla danych firmowych stanowi korzystanie z e-maila (tak wynika m.in. z badań firmy Fortinet). Pracownikom zdarzają się niedopatrzenia lub nieuwaga, która może doprowadzić do niekontrolowanego wycieku ważnych danych poza firmę. Poufne dane wysyłane przez e-mail można zaszyfrować, wykorzystując m.in. następujące mechanizmy:

- szyfrowanie danych dla konkretnych odbiorców (tak że mogą je odczytać tylko oni i nikt inny);
- podpisywanie danych (podpis elektroniczny) – odbiorcy mogą weryfikować, że dokument w tej postaci rzeczywiście pochodzi od nadawcy i nie został „po drodze" zmodyfikowany w żaden sposób.

Szyfrowanie e-maili wymaga stworzenia tzw. kluczy, czyli odpowiednich plików, które potrzebne są zarówno do zaszyfrowania („zamknięcia") wiadomości, jak i ich odczytania („otwarcia"). Stworzenie takich kluczy i przeszkolenie pracowników to łatwe zadanie dla pracowników IT. Klucze muszą mieć i nadawca, i odbiorca. Muszą też korzystać z tego samego narzędzia szyfrującego. Do wyboru jest kilka narzędzi, m.in.:

- ogólnie dostępny program PGP (ang. Pretty Good Privacy),
- rozwiązanie S/MIME dostępne w wielu programach pocztowych (np. Outlook),
- łatwe do wdrożenia i obsługiwania rozwiązania komercyjne,
- opcja szyfrowania wbudowana w system operacyjny, np. CMS (ang. Cryptographic Message Syntax) w obrębie Windows 10.

NIEPOWOŁANY ODBIORCA?

Wysyłając komuś załącznik, musisz ufać, że nie zostanie on rozpowszechniony dalej bez Twojej zgody czy wiedzy. Nie jest to komfortowa sytuacja, a jeszcze gorzej jest, gdy wiadomość z ważnym załącznikiem trafi do niewłaściwego odbiorcy. RMS (ang. Rights Management Service) umożliwia zaawansowane śledzenie dokumentów i rozwiązuje pro-

ARKADIUSZ ZAKRZEWSKI

dyrektor pomocy technicznej CORE

Największym problemem przedsiębiorców jest bagatelizowanie odpowiedniego przeszkolenia pracowników. Właściciele firm lekceważą takie kwestie jak np. blokowanie komputerów, wylogowywanie czy wynoszenie firmowych plików na zewnętrznych nośnikach.

blem załączników. Pozwala ograniczyć grono uprawnionych odbiorców oraz umożliwić śledzenie wiadomości.

– **RMS** *to funkcja, która pozwala zabezpieczyć dokumenty przed niepowołanym użyciem na komputerach i urządzeniach przenośnych z systemem Windows 8 lub wyższym* – wyjaśnia Bartłomiej Machnik, Windows Server Product Manager. - *Na innych w ogóle nie uda się go otworzyć. Przykładowo, pracując nad dokumentem w Wordzie, ustalam atrybuty dostępności pliku – np. „tylko dla mnie" – wówczas nikt nie może go zmienić, wydrukować, zrobić zrzutu ekranu czy wysłać poza firmę, a nawet pokazać na zewnątrz. Rozwiązanie to zapobiega wyciekowi poza firmę informacji, np. zawartych w dokumencie dotyczącym nowych rozwiązań produktowych.*

Platformy wymiany danych

Szyfrowanie, choć nietrudne, może okazać się uciążliwe, szczególnie dla pracowników „nietechnicznych". Dlatego np. do bezpiecznej pracy na jednym dokumencie warto rozważyć rezygnację z e-maila na rzecz platformy wymiany danych (np. OneDrive dla Firm z oferty Microsoft czy Google Drive). Na takiej platformie łatwo umieszczać pliki, korzystać z nich podobnie jak przez znane edytory oraz określać, komu udostępniony jest dokument (wskazujemy adres e-mail osoby, która może ten plik zobaczyć i zmieniać).

Jeśli zdecydujesz się na pracę w takiej platformie, jasno określ i zapisz w polityce bezpieczeństwa zasady udostępniania plików – przy plikach do użytku wewnętrznego (firmowego) korzystamy z opcji dawania dostępu konkretnej osobie, zamiast opcji podawania linku do pliku. Taki link może, często przypadkiem, trafić w niepowołane ręce i dać nieuprawnionej osobie łatwy wgląd do ważnych danych.

EKSPERT PODPOWIADA

BARBARA MICHALSKA

Office 365 Product Manager

W przypadku Office 365 informacje wymienione przez komunikator zapisywane są w historii korespondencji (w Outlooku), co ułatwia ich późniejsze przeglądanie i ocenę, czy komunikator był stosowany zgodnie z firmowymi zasadami.

BEZPIECZNE KORZYSTANIE Z KOMUNIKATORÓW

Komunikatory pozwalają na szybką i bezpośrednią wymianę informacji, np. wideokonferencje między pracownikami czy z klientami to spora oszczędność czasu. Można sprawdzić, czy ktoś jest przy biurku, czy też nawiązywać połączenia głosowe (korzystać jak z telefonu), a odpowiednie kamery pozwalają na efektywne połączenia konferencyjne.

Jednak pracownicy przez komunikatory przesyłają wszystko—od plotek firmowych po kluczowe raporty. Wiedzą o tym też oszuści, którzy mogą podsłuchiwać wymieniane informacje. Dlatego wybieraj dla swojej firmy bezpieczne komunikatory i dbaj o rozsądne korzystanie z nich:

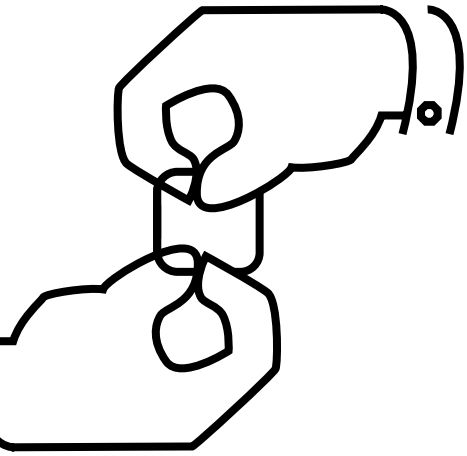
- do pracy w firmie wybierz komunikator biznesowy (np. Skype dla Firm, dostępny m.in. w usłudze Office 365). Rozwiązania takie mają szereg zabezpieczeń, w tym funkcję szyfrowania, co chroni m.in. przed wyciekiem danych,
- wymagaj od wszystkich w firmie stosowania jednego komunikatora,
- jasno określ i zapisz w polityce bezpieczeństwa zasady przesyłania informacji przez komunikatory (np. nie można przesyłać haseł).

Jeśli pracownicy korzystają na komputerach firmowych także z komunikatorów konsumenckich (np. specyfika Twojej firmy wymaga tej formy kontaktów z niektórymi klientami), przestrzegaj kilku zasad bezpieczeństwa:

- komunikator nie służy do przesyłania loginów i haseł,
- unikamy korzystania z kamerki,
- przyjmujemy połączenia głosowe tylko od znanych sobie osób,
- po zakończeniu pracy zamykamy komunikator.

► 3 sposoby na bezpieczne dane

1. Ważne pliki=kopie zapasowe w 2 miejscach (1 w chmurze).
2. Poufny plik udostępnij przez platformę wymiany plików lub zaszyfruj e-mail, którym go przesyłasz.
3. Stosuj jeden komunikator (biznesowy!) dla całej firmy.



BEZPIECZNE KORZYSTANIE Z POCZTY

Przeczytaj, jeśli:

- **Twoja firma korzysta z poczty elektronicznej**
- **dostajesz e-faktury**
- **tworzysz politykę bezpieczeństwa dla swojej firmy.**

Każdego dnia na firmowy adres e-mail przychodzi po kilkadziesiąt e-maili – nic dziwnego, że czasem ich lektura jest pobieżna. Jednak nierozważne korzystanie z poczty elektronicznej – np. otwieranie załączników z nieznanego źródła – może skończyć się zainfekowaniem komputera złośliwym oprogramowaniem albo wyłudzeniem poufnych danych. Uważaj szczególnie na spreparowane wiadomości od przestępców!

Pierwszą linią obrony jest filtr antyspamowy. Dzięki jego stosowaniu wiele niebezpiecznych wiadomości w ogóle nie trafia do skrzynki. Pozostałe są przez program pocztowy odpowiednio opisywane i porządkowane (np. trafiają do folderu „Spam"/„Niechciane"/„Wiadomości-śmieci" lub są oznaczane w temacie jako spam).

Część wiadomości prześlizguje się jednak bez żadnego przyporządkowania. Jeśli trafisz na taką wiadomość, możesz poprawić skuteczność narzędzia antyspamowego:

- przed skasowaniem niepożądanej wiadomości oznacz ją jako spam lub skorzystaj z opcji „zgłoś spam",

- wskaż programowi pocztowemu, że nadawca jest niepożądany – zależnie od używanego programu dodaj nadawcę do czarnej listy lub ustaw filtr na konkretny adres.

Spam kojarzy się zwykle z wiadomościami, które są po prostu uciążliwe. Co gorsza, coraz częściej są one narzędziem dla przestępców, którzy używają e-maili, by rozprowadzać wirusy zaszyte w wiadomości czy podsuwać odbiorcom linki prowadzące na strony spreparowane w celu wyłudzenia danych.

WIADOMOŚCI E-MAIL MOGĄ BYĆ NIEBEZPIECZNE!

Żeby uświadomić sobie skalę zjawiska, wyobraź sobie newsletter, który trafia do bazy odbiorców z milionami adresów. Przy tak dużej liczbie „odbiorców" cyberprzestępcy łatwo trafią na sporą grupę osób, których niewiedzę, nieuwagę, niefrasobliwość czy obawy będą mogli wykorzystać. Skąd mają adresy? Te firmowe łatwo gromadzić, m.in. dzięki informacjom kontaktowym na stronach firmowych. Ale nie tylko...

Wielu pracodawców zdziwiłoby się, wiedząc, jak często pracownicy podają służbowe maile w różnych miejscach miejscach, takich jak fora, media społecznościowe, listy adresowe etc. Należy ich uczulać, by tego nie robili (powinno to zostać zapisane w polityce bezpieczeństwa)!

Wszystkie wiadomości, które zdecydujesz się otworzyć, zawsze czytaj z uwagą i pomyśl dwa razy przed podjęciem jakiejkolwiek akcji.

Najpoważniejsze zagrożenia przychodzące (dosłownie) z e-mailem to te związane z nierozsądnym postępowaniem użytkownika, który:

- **uruchamia złośliwe oprogramowanie**, otrzymane w postaci załączników do e-maili lub pobierane po kliknięciu w zawarty w wiadomości odnośnik,
- **podaje poufne dane na podstawionych stronach www**.

MICHAŁ SAJDAK

Ekspert bezpieczeństwa Securitum.pl

Przerażające jest to, że do ataku często wystarczają techniki dość brutalne i grubymi nićmi szyte. Na przykład w mailu, który otrzymują pracownicy, nic się nie zgadza (dziwna domena źródłowa/nadawca, błędy literowe, linki prowadzące do absurdalnych domen), a użytkownicy i tak będą otwierać takiego maila i klikać!

ROZSĄDEK PRZY ODBIERANIU POCZTY

Zabezpieczenia systemowe nie wyłapią wszystkich zagrożeń, dlatego użytkownicy poczty elektronicznej powinni wyrobić sobie dobre nawyki:

1. Jeśli e-mail wydaje Ci się podejrzany, najlepiej skasuj go bez otwierania i czytania. Nadawca, któremu zależy na kontakcie, dotrze do Ciebie w inny sposób.
2. Skanuj wiadomości i załączniki programem antywirusowym. Zawsze. Nawet jeśli są to maile od znanych nadawców – może się zdarzyć, że otrzymasz wiadomość z zainfekowanego systemu.
3. Kiedy trafia do Ciebie e-mail, odpowiedz na poniższe pytania, opracowane przez ekspertów ds. bezpieczeństwa z organizacji CERT (Computer Emergency Response Team - zespół reagowania na incydenty, w Polsce część NASK):

- Czy znasz nadawcę wiadomości?
- Czy otrzymywałeś już inne wiadomości od tego nadawcy?
- Czy spodziewałeś się otrzymać tę wiadomość?
- Czy tytuł wiadomości i nazwa załącznika mają sens?
- Czy wiadomość nie zawiera złośliwego oprogramowania (jaki jest wynik skanowania)?

Jeśli odpowiadasz twierdząco na powyższe pytania, wiadomość prawdopodobnie jest bezpieczna.

4. Na adres firmowy przychodzą wiadomości, dla których na pierwsze trzy pytania odpowiadasz „nie". Wówczas:

- Oceń, czy wiadomość jest poprawna językowo, czy wydaje się przetłumaczona translatorem.
- Zanim odpowiesz, otworzysz załącznik lub klikniesz w link – zweryfikuj nadawcę (np. telefonicznie).

5. Jeśli weryfikacja wypadnie negatywnie:

- nie odpowiadaj na wiadomość,
- nie klikaj w odnośniki,
- nie pobieraj i nie otwieraj załączników,
- zgłoś przyjście wiadomości administratorowi IT.

O LINKACH I ZAŁĄCZNIKACH

Załączniki i linki są szczególnie niebezpieczne, każdy powinien wzbudzić Twoją czujność.

- skanuj programem antywirusowym **każdy** załącznik
- **nigdy** nie otwieraj załączników o rozszerzeniach *.exe, *.com, *.pif, *.scr, *.bat (co ciekawe, Office 365 z definicji blokuje przekazywanie i pobieranie tych plików). Najczęściej są to wirusy. Uwaga! Wirusy mogą być też „zaszyte"w arkuszach kalkulacyjnych, plikach tekstowych czy plikach .pdf. Ostrożnie!
- nie klikaj w linki, nawet od znajomych, szczególnie jeśli wiadomość wygląda dziwnie (np. jest w obcym języku).

SPRAWDZAJ ZAUFANEGO KONTRAHENTA

Twoja firma coraz częściej korespondencję od banków czy dostawców usług otrzymuje w formie elektronicznej i nikogo to już nie dziwi. Z tego faktu korzystają również cyberprzestępcy! Traktuj wiadomości od dostawców usług z dużą uwagą i uczul na to wszystkich pracowników – także i tych, którzy zwykle nie otrzymują takich wiadomości na firmowe adresy e-mail.

JAK POZNAĆ PODEJRZANĄ (RZEKOMĄ) KORESPONDENCJĘ OD BANKU LUB DOSTAWCY KLUCZOWYCH USŁUG:

- nie oczekujesz takiej wiadomości,
- wiadomość przyszła na adres firmowy, ale inny niż zwykle używany do korespondencji z daną instytucją (np. otrzymał ją inny niż zwykle pracownik),
- adres nadawcy jest dziwny, inny niż zwykle, nie z domeny nadawcy,
- wiadomość jest niezręczna językowo lub wręcz zawiera błędy językowe,

- wiadomość jest inna niż zwykle – np. zwykle otrzymujesz tylko powiadomienia o nowym rachunku/fakturze, a w podejrzanej wiadomości jest załącznik,
- wiadomość zawiera rzekome dane firmowe (np. numer klienta), które są niepoprawne,
- wiadomość zawiera odnośnik, np. do „weryfikacji konta", „potwierdzenia hasła", „potwierdzenia transakcji",
- wiadomość zawiera prośbę o zalogowanie się (np. na stronie banku).

Uwaga! Banki NIGDY nie wysyłają odnośników służących do potwierdzania haseł/transakcji lub do weryfikacji danych konta ani próśb o zalogowanie się.

JOANNA FOTEK

Bank PKO BP

Apelujemy o ostrożność wobec e-maili lub SMS-ów, w których znajduje się prośba o podanie poufnych danych lub skorzystanie z linku. Są to fałszywe wiadomości, działające na szkodę użytkownika! Nie należy odpowiadać na podejrzane wiadomości, korzystać z podanego linku i udostępniać żadnych poufnych informacji.

Jeśli otrzymasz taką wiadomość, zapewne jesteś na liście potencjalnych ofiar phishingu, czyli podszywania się pod wiarygodnego nadawcę w celu wyłudzenia poufnej informacji. Dla firm usługowych jest to niemal taki sam problem jak dla producentów znanych marek pojawiające się na rynku podróbki ich produktów. Nie daj się zwieść rozpoznawalnemu nadawcy – o taki właśnie efekt chodzi przestępcy!

- medialnie głośne były przypadki podszywania się pod takie firmy jak UPC, Vectra, PKO BP, Netia, Orange, Apple, mBank, Allegro etc.,
- w czasie, kiedy rośnie liczba przesyłek (np. przed świętami) nasila się fala korespondencji, której nadawcy podszywają się pod firmy kurierskie (np. DHL), Pocztę Polską lub InPost i informują o nieodebranej przesyłce,
- w ostatnim kwartale roku nasilają się e-maile od „kancelarii prawnych", które wzywają np. do uregulowania zaległych faktur.

CO ROBIĆ Z PODEJRZANYM E-MAILEM?

- nie otwieraj załącznika (to zwykle złośliwe oprogramowanie, które pobrane na dysk i otwarte wyrządzi szkody na Twoim komputerze)!
- nie klikaj w odnośnik (to zwykle przekierowanie na spreparowaną stronę, wyłudzającą dane)!
- nie odpowiadaj na wiadomość (tylko potwierdzisz swój adres)!
- zadzwoń do usługodawcy, pod którego podszywa się nadawca (ale nie pod telefon podany w podejrzanym e-mailu). Unikniesz problemów i pomożesz ostrzec innych odbiorców!

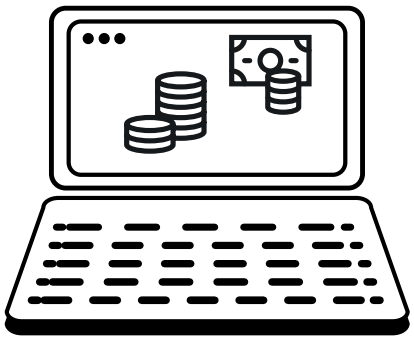
W PRZYPADKU NIEOSTROŻNEGO DZIAŁANIA...

Jeśli w Twojej firmie zdarzy się kliknięcie w wyłudzający link lub otwarcie i zainstalowanie złośliwego oprogramowania z załącznika, wówczas:

- zainfekowany komputer należy odłączyć od sieci,
- nie należy korzystać z zainfekowanego komputera do czasu oczyszczenia go z niechcianego oprogramowania przez specjalistę,
- jeśli jednak użytkownik tego komputera logował się z niego do serwisu z usługami, należy zmienić hasło (korzystając z innego urządzenia) oraz poinformować administratora tej usługi o incydencie.

► 3 główne zasady bezpiecznego korzystania z poczty

1. Nie klikaj na załączniki w mailach od podejrzanych nadawców – programy szpiegowskie (spyware), często dostarczane są użytkownikom w spreparowanych mailach jako niewinne załączniki, np. udające rachunki w formacie PDF.
2. Nie uruchamiaj plików pobranych z sieci bez uprzedniego przeskanowania ich programem antywirusowym – zamiast zawartości, która jest obiecywana, może być w nim wirus!
3. Nie klikaj na podejrzanie wyglądające linki – mogą przekierować na spreparowaną przez oszustów witrynę.



FIRMOWE PIENIĄDZE BEZPIECZNE W SIECI

Przeczytaj, jeśli:

- korzystasz z płatności internetowych
- płacisz przez urządzenia mobilne
- wybierasz nowego dostawcę usług

Spieszysz się. Doskonale to rozumiemy. Ale kiedy w grę wchodzą firmowe pieniądze, trzy dodatkowe minuty (bo zwykle tyle wystarcza) poświęcone na sprawdzenie, czy przelew rzeczywiście wędruje zgodnie z Twoimi oczekiwaniami – to niezbyt wiele.

Zacznij od podstaw – chcąc dokonać płatności przez witrynę banku, upewnij się, czy nie znajdujesz się na podstawionej stronie. Banki stosują bezpieczne połączenie, ale i tak należy zastosować zasadę ograniczonego zaufania. Tym bardziej, że nie musisz robić niczego specjalnego – przeglądarka zaalarmuje Cię, jeśli:

- certyfikat bezpieczeństwa jest nieważny,
- certyfikat nie został wystawiony przez zaufanego dostawcę,
- certyfikat jest wystawiony dla tej właśnie witryny (zdarzają się ataki z użyciem autentycznych certyfikatów na podrobionych stronach).

Zanim ze zniecierpliwieniem przejdziesz dalej, upewnij się, jaka jest przyczyna ostrzeżenia i czy nie znajdujesz się na podstawionej stronie. ▸

SPRAWDŹ, NA JAKI RACHUNEK PRZESYŁASZ PIENIĄDZE

Jeśli chcesz połączyć się z bankiem, ostrożnie z klikaniem w linki – lepiej wpisać adres banku w przeglądarkę ręcznie. Kiedy już jesteś na stronie, przed logowaniem przeczytaj uważnie adres witryny.

To tylko pozorne dziwactwo. Cyberprzestępcy to świetni socjotechnicy – w przypadku płatności internetowych wykorzystają np. zaufanie do instytucji, rutynę w działaniu czy wszechobecny pośpiech. Wizualne podrobienie witryny banku jest łatwe, a na niewielki błąd w adresie (np. bnak zamiast bank) użytkownik może nie zwrócić uwagi. Dlatego sprawdzaj, czy w adresie nie ma np. literówki, cyfry udającej literę etc.

Równie poważna jest sprawa z możliwością zmiany numeru konta, na które chcesz dokonać przelewu. Szkodliwe oprogramowanie, takie jak VBKlip czy Banatrix, wykrywa kopiowanie numeru rachunku bankowego (np. z maila lub ze strony kontrahenta) i przy wklejaniu podmienia cyfry – na numer konta przestępców. Po wklejeniu numeru konta przeczytaj więc go uważnie. Najnowsze wersje Banatrixa potrafią pokazać w przeglądarce właściwy numer konta, a do banku wysłać sfałszowany. Dlatego sprawdź numer jeszcze raz – przed wpisaniem jednorazowego kodu potwierdzającego transakcję!

Pamiętaj też o złośliwych aplikacjach, które podmieniają przychodzące z banku SMS-y. Zawsze więc sprawdzaj poprawność numeru konta podanego w wiadomości SMS. Możesz też sprawdzić numer tuż po potwierdzeniu operacji na stronie banku (w większości banków operację można cofnąć).

Warto stosować też zabezpieczenia związane z przeglądarkami, np.:

- funkcja „bezpiecznej przeglądarki", która często jest zintegrowana z programami antywirusowymi.
- przeglądarka z wbudowanym systemem zabezpieczającym przed wyłudzeniem poufnych danych (mechanizm antyphishingowy) – obecne np. w Internet Explorer 11 czy Edge.

TELEFON I ODROBINA ZDROWEGO ROZSĄDKU

Stosuj także dwie pozornie oczywiste, ale wcale nierzadko lekceważone rady w zakresie wykorzystywania telefonu do kontaktów z bankiem:

- Zachowaj wszelkie informacje o firmowym koncie bankowym dla siebie. Jeśli załatwiasz jakąś sprawę w banku przez telefon i musisz podać informacje uwierzytelniające – pilnuj, by nikt nie słuchał Twoich rozmów.
- Ostrożnie z podawaniem danych uwierzytelniających, jeśli żąda ich od Ciebie dzwoniący do Ciebie przedstawiciel banku. Zwróć uwagę, że:
  - telefon z banku następuje w dni robocze, w godzinach pracy;
  - nie każda rozmowa wymaga uwierzytelniania (konsultant nie powinien zaczynać od tego rozmowy). Bank nie pyta o hasła czy loginy, także te używane w innych kanałach;
  - jeśli masz wątpliwości, czy rzeczywiście rozmawiasz z bankiem, zadzwoń pod sprawdzony (!) numer i spytaj, czy osoba, która się z Tobą kontaktowała, rzeczywiście pracuje w banku.

Niektóre banki proponują ustanowienie dodatkowego hasła, którym będą się posługiwać osoby dzwoniące w imieniu banku.

ZAGROŻENIA DOTYCZĄCE TRANSAKCJI MOBILNYCH

Smartfon jest coraz popularniejszym urządzeniem stosowanym w bankowości mobilnej. Coraz częściej służy nie tylko do rozmów z bankiem czy odbierania SMS-ów weryfikujących płatności, ale też do przeprowadzania transakcji mobilnych. Zalecamy szczególną ostrożność - płatności z użyciem smartfona często wykonywane są w dużym pośpiechu. Może się to wiązać ze zwykłą nieuwagą, np. użytkownik bez namysłu kliknie w komunikat (pojawiający się w mailu lub wyświetlany jako baner), rzekomo przygotowany przez bank. Tego typu rutynowe „grzeszki" skrupulatnie wykorzystują oszuści.

Bezpieczeństwu przelewów mobilnych sprzyjają wszystkie znane zasady korzystania z urządzeń mobilnych. Warto jednak zwrócić uwagę na kilka charakterystycznych zagrożeń, jakie niesie złośliwe oprogramowanie „dedykowane" bankowości mobilnej:

- załączniki do wiadomości e-mail, zawierające szkodliwe oprogramowanie, które po otwarciu (czyli kliknięciu w załącznik) pozwala przestępcom przechwytywać dane przekazywane między zainfekowanym telefonem a bankiem (np. dane logowania);
- zmodyfikowana strona banku, wyświetlająca zachętę do pobrania z legalnego sklepu aplikacji, która umożliwia przestępcy dostęp do konta użytkownika i przechwytywanie haseł jednorazowych z urządzenia mobilnego;
- podstawienie fałszywej aplikacji, udającej aplikację mobilną banku i wyświetlenie fałszywej strony logowania, co pozwala przestępcy na przechwycenie wpisywanych tam danych.

Warto zauważyć, że funkcja szybkich przelewów internetowych (bez wpisywania numeru konta) jest stosunkowo bezpiecznym rozwiązaniem.

MŚP a bankowość mobilna (według działu cyberbezpieczeństwa w Deloitte)

- Z bankowości mobilnej aktywnie korzysta 1,3 mln MŚP (dane Związku Banków Polskich), a średnia wartość dokonywanych transakcji wynosi ponad 85 tys. zł miesięcznie.
- Przestępcy często atakują małe i średnie firmy, ze względu na wartość transakcji oraz niespójne zasady bezpieczeństwa w firmie.
- Celem przestępców jest kradzież pieniędzy, ale także kradzież tożsamości umożliwiająca podszycie się pod ofiarę i np. zaciąganie kredytów oraz pranie pieniędzy.
- Przy korzystaniu z bankowości mobilnej należy kierować się zasadą ograniczonego zaufania i uważać na to, jakie aplikacje są ściągane na telefon.

ZAUFANE INSTYTUCJE PŁATNICZE

Do kanonów bezpieczeństwa płatności internetowych należy też zaliczyć korzystanie z usług sprawdzonych dostawców—zarówno samego systemu płatności, jak i opłacanych towarów czy usług.

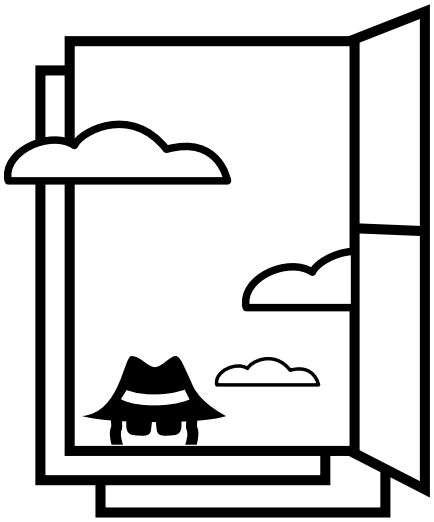
Chcesz korzystać z usług innej instytucji płatniczej niż banki? Sprawdź rejestr Komisji Nadzoru Finansowego, która weryfikuje, czy akredytowana firma spełnia wszystkie wymagania dotyczące bezpieczeństwa. W każdej chwili na stronie **https://erup.knf.gov.pl/View/** możesz sprawdzić, czy wybrany przez Ciebie podmiot znajduje się w rejestrze dostawców usług płatniczych. Dodatkowo możesz prześledzić rejestr licencjonowanych Agentów Rozliczeniowych prowadzony przez Narodowy Bank Polski. Zwróć uwagę, czy dana firma posiada certyfikat PCI DSS świadczący o zgodności z popularnymi systemami płatności kartami kredytowymi.

ZAUFANY KONTRAHENT

Szukasz nowego dostawcy dla swojej firmy? Na pewno sprawdzisz oferentów pod wieloma względami. Weź też pod uwagę, jak działa w internecie, szczególnie jeśli chcesz korzystać z sieci do kontaktów, zamówień i płatności:

- rozszerzenie .pl nie wskazuje jednoznacznie, że masz do czynienia z polskim przedsiębiorcą. Pamiętaj, że z punktu widzenia prawa liczy się geograficzna siedziba przedsiębiorcy, nie położenie serwerów.
- sprawdź, czy sprzedawca korzysta z usług agregatora płatności internetowych (dającego możliwość wykonania bezpiecznej transakcji za pomocą wszystkich dostępnych metod).

Uwaga! Zanim zapłacisz w internecie, sprawdź swojego kontrahenta!



PORADNIK ZAGROŻEŃ W INTERNECIE

Skoro już wiadomo, że incydenty włamań, kradzieży pieniędzy, przejęć czy wycieków danych mogą przydarzyć się każdej firmie, warto też mieć świadomość zagrożeń i tego, jak łatwo wpuścić na komputer, telefon czy tablet szkodnika.

Wbrew częstemu przekonaniu firm, że na firmowych komputerach, tabletach czy smartfonach „nie ma niczego cennego", zawsze są tam rozliczne dane, dla przestępców bezcenne. Urządzenie może też stać się celem ataku w wyniku m.in. „kampanii" e-mailowej czy pobrania darmowego programu z ukrytym szkodnikiem.

– *Każdy komputer ma wartość dla napastników, którzy mogą wykorzystać jego zawartość na wiele sposobów, np. zainfekowane komputery mogą być włączone do sieci botnetów i wykorzystane jako źródło spamu lub do ataków DDoS*– dodaje Robert Dziemianko, Marketing Manager w firmie G DATA. Przed tymi nieprzyjemnymi incydentami można w dużej mierze bronić się dzięki... zdrowemu rozsądkowi, znając sposoby, w jaki szkodniki mogą się dostać na urządzenia.

PODSTAWY SŁOWNICZKA MALWARE

Pod ogólną i częstą spotykaną nazwą **malware** (od *malicious software*) kryją się wszelkie złośliwe i szkodliwe programy pojawiające się na naszych urządzeniach.

Wirus to program (zwykle krótki) lub wręcz fragment kodu, który mnoży się na zaatakowanym urządzeniu, zmieniając sposób działania właściwych programów na komputerze. Na komputer najczęściej trafia jako beztrosko pobrany przez użytkownika plik – z niepewnego źródła lub z załącznika w zawirusowanym mailu.

Trojan – szkodliwy program działający w tle, mający konkretne zadanie. Najczęściej wpuszczamy go na urządzenia w atrakcyjnym opakowaniu użytecznego programu (podobnie jak w mitologii greckiej Trojanie słynnego konia – stąd nazwa). Przykładem są trojany bankowe, opisane poniżej.

NAJCZĘŚCIEJ SPOTYKANE MALWARE

Spyware (oprogramowanie szpiegujące) – umożliwia przestępcy śledzenie wszystkich poczynań użytkownika systemu – od uruchamianych aplikacji po odwiedzane strony. Zwykle szkodniki z tej rodziny używane są w celu wykradania poufnych danych, jak hasła i PIN-y do kont.

Keylogger – specjalistyczna aplikacja *spyware*, używana do zapamiętywania znaków wprowadzanych za pośrednictwem klawiatury. Pozwala to na poznanie haseł, loginów oraz innych poufnych informacji.

Adware (oprogramowanie reklamowe) – uporczywy szkodnik, który często występuje w połączeniu ze spyware. Jego zadanie to wyświetlanie reklam, przekierowanie użytkownika na wybrane strony internetowe oraz takie czynności, jak zmiana strony startowej przeglądarki czy umieszczenie w niej dodatkowego paska narzędzi, który oczywiście ciężko usunąć.

Jednym z najbardziej znanych adware okazał się... oficjalny program instalowany fabrycznie przez Lenovo na laptopach. **Superfish** miał za zadanie polecać użytkownikom produkty z sieci na podstawie przeglądanych przez nich grafik. Korzystał w tym celu z techniki „man-in-the--middle", przechwytując połączenia między użytkownikiem a serwerem, a następnie „wstrzykując" własną treść. Po wykryciu tych metod działania Lenovo wypuściło program do deinstalacji Superfish, jednak reputacja producenta została mocno nadszarpnięta.

Ransomware (oprogramowanie do wymuszania okupu) – wyjątkowo niebezpieczny szkodnik, który szyfruje dane na urządzeniu, a w zamian za ich odblokowanie żąda wpłacenia konkretnej sumy na wskazane konto. Ofiary często płacą – i przekonują się, że przestępca nie dotrzymał słowa. Uwaga! Według badań firmy Kaspersky Lab, w 2015 roku głównym celem ataków były komputery biurowe (zaatakowano 58% takich urządzeń).

W sierpniu 2015 roku przestępcy wykorzystali zainteresowanie systemem Windows 10. Odbiorcy na całym świecie otrzymywali maile zachęcające do darmowego przejścia z aktualnie używanego systemu operacyjnego na Windows 10. Do maila dołączony był niewielki plik mający zaktualizować Windows. Po kliknięciu uruchamiał się szkodnik ransomware, który natychmiast blokował cały system operacyjny i żądał równowartości 4 bitcoinów za podanie hasła dostępu.

Ataki ransomware dotyczą wszystkich systemów operacyjnych – według przewidywań firm zajmujących się bezpieczeństwem IT zagrożeń tych będzie przybywać w 2016 roku. Przykładowo, w marcu 2016 roku stwierdzono ataki ransomware KeRanger na komputery Mac. Według informacji firmy Kaspersky Lab, w 2015 roku 17% prób ataków ransomware dotyczyło urządzeń z Androidem (a pierwszy ransomware atakujący ten system został wykryty w 2014 roku).

Rootkit – szkodnik, pozwalający przestępcy na zdalny dostęp do komputera oraz mogący instalować ukryte oprogramowanie, mające negatywny wpływ na system operacyjny. Napastnik może uzyskać wręcz całkowitą kontrolę nad zainfekowaną maszyną i wykonywać w zasadzie dowolne działania.

Mebroot to jeden z najbardziej znanych rootkitów w historii. Był aktywny w latach 2007 – 2009, a dostawał się na komputery użytkowników poprzez tysiące specjalnie spreparowanych stron. Umożliwiał przestępcy uzyskanie całkowitej kontroli nad zainfekowanym komputerem, a maskował się tak sprytnie, że wiele programów antywirusowych nie widziało go jako zagrożenia.

Przykładem rootkita jest na szczęście rzadki, ale bardzo niebezpieczny **bootkit**, przeznaczony do modyfikacji programu ładującego komputera – oprogramowania, które uruchamia się przed załadowaniem systemu operacyjnego. W ostatnich latach ukształtowała się grupa rootkitów mobilnych, które atakują urządzenia mobilne (zwłaszcza z systemem Android).

Scareware (oprogramowanie „straszące") – szkodnik, który wykorzystuje niewiedzę użytkownika, aby skłonić go do wykonania danej akcji. Na przykład, po wejściu na stronę internetową pojawia się informacja, że na komputerze wykryto wirusa i należy kliknąć na podany na niej link, aby go usunąć. Równie popularnym rodzajem tego typu „ogłoszenia" jest zachęta do kliknięcia w odsyłacz, aby komputer szybciej pracował. Instalacja oprogramowania „pomagającego" to oczywiście wpuszczenie do systemu któregoś z opisanych powyżej szkodników.

Trojan bankowy – odmiana szkodnika typu „trojan" (działającego „cicho" w tle). Działanie trojanów bankowych mogą polegać na przechwytywaniu SMS-ów na smartfonach, śledzeniu działań użytkownika czy też przejmowaniu listy kontaktów. Zagrożenia te istnieją w wersji dla komputerów i urządzeń przenośnych.

GROŹNE FORMY ATAKÓW

Metody socjotechniczne (wykorzystanie inżynierii społecznej) – w uproszczeniu, umiejętności skłonienia ludzi, by postąpili w oczekiwany sposób, działając na swoją szkodę. Przestępcy internetowi bazują często na:

- ciekawości np. zachęty do obejrzenia „niezwykłych" materiałów dotyczących gwiazd (skrywające oczywiście złośliwe oprogramowanie) czy maile, do których rzekomo załączono arkusz z płacami pracowników w firmie),
- niepewności i niedostatecznej wiedzy – przewrotną formą są np. zachęty do pobierania fałszywych programów antywirusowych,
- zaufaniu do instytucji, np. spreparowane maile, udające m.in. korespondencję od znanego nadawcy (chociażby banku), faktury od dużego usługodawcy (np. dostawcy usług telekomunikacyjnych), pisma z sądu czy kancelarii prawnych lub powiadomienia od firm kurierskich/pocztowych.

Phishing–wyłudzanie poufnych danych, najczęściej za pośrednictwem fałszywej strony internetowej. Wszystkie wpisywane na niej informacje wędrują do przestępcy. Najczęściej przejście na tę stronę następuje po kliknięciu w link zamieszczony w spreparowanej przez przestępcę wiadomości e-mail.

DDoS – (Distributed Denial of Service, rozproszona odmowa usługi) – atak prowadzony z wielu komputerów naraz, skierowany na konkretny system komputerowy lub usługę sieciową (często stronę www), aby zablokować ich działanie. Atak następuje z wielu miejsc jednocześnie i prowadzi do zajęcia wszystkich wolnych zasobów (w ten sposób np. przestaje działać przeładowany serwis transakcyjny). Do tego celu wykorzystuje się często sieć komputerów „zombie", czyli takich, które dzięki zainstalowanemu wcześniej szkodliwemu oprogramowaniu wykonują polecenie wydane zdalnie przez komputer „zarządzający" (bot master).

Do przemyślenia...

Michał Sajdak
Ekspert bezpieczeństwa, Securitum.pl

Gdybym miał zaatakować małą firmę, wybrałbym sprytny atak socjotechniczny. Przy minimalnych kosztach atakujący może osiągnąć naprawdę porażające efekty.

Brian Andersen
Consulting System Engineer,
specjalista w zakresie Wi-Fi, Fortinet

Gdybym był przestępcą internetowym, zaatakowałbym raczej 100 małych firm niż jedną dużą, ponieważ to właśnie małe firmy są bardzo łatwym celem!

CO ROBIĆ W PRZYPADKU WYKRYCIA INCYDENTU?

W Niezbędniku podpowiadamy przede wszystkim, jak skutecznie zabezpieczyć się przed zagrożeniami pochodzącymi z internetu. Jeśli jednak taki incydent już się wydarzył, przede wszystkim zachowaj rozsądek!

Uwaga! Nie ma „cybeprzestępców". Są przestępcy.

W polskim prawie nie istnieje używane potocznie pojęcie „cyberprzestępczości". Przestępstwa, o których piszemy w Niezbędniku, są karane na mocy następujących zapisów kodeksu karnego:

- **Art. 286 k.k. § 1**. Kto, w celu osiągnięcia korzyści majątkowej, doprowadza inną osobę do niekorzystnego rozporządzenia własnym lub cudzym mieniem za pomocą wprowadzenia jej w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.
- **Art. 287 k.k. §1.** Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

JEŚLI PADNIESZ OFIARĄ TAKIEGO PRZESTĘPSTWA:

Uwaga! Możesz także zgłosić incydent do CERT.

- odłącz zainfekowany komputer od sieci, bez logowania się użytkowników z wyższymi uprawnieniami,
- pracownik działu IT powinien zabezpieczyć wszelkie dokumenty i dowody elektroniczne, w tym tzw. rejestr logów, który pozwoli prześledzić, co działo się na zainfekowanym komputerze,
- jeśli mowa o wyłudzeniu bankowym, przygotuj wydruki i potwierdzenia przelewów,
- jeśli przestępca podszył się pod usługodawcę czy instytucję, powiadom o incydencie także ten podmiot,
- jeśli przestępca żąda okupu za odszyfrowanie zawartości komputera, nie płać! Skonsultuj się z działem IT lub odpowiednim specjalistą,
- zgłoś się do komendy Policji lub ewentualnie złóż zawiadomienie o popełnieniu przestępstwa do prokuratury rejonowej.

Możesz, podobnie jak 8% polskich firm, wykupić polisę ubezpieczeniową od cyberzagrożeń. Najwięcej odszkodowań wypłacanych jest z tytułu utraty danych identyfikacyjnych czy z kart płatniczych, kradzieży własności intelektualnej i szkód dla reputacji marki (dane za Raportem PwC).

NIEZBĘDNIK DI

cyberbezpieczeństwo

Niezbędnik przygotował zespół redakcyjny Dziennika Internautów.

redaktor serii: **KRZYSZTOF GONTAREK**
redaktor prowadząca wydania: **JOANNA RYŃSKA**
redaktorzy wydania:
MARCIN MAJ, ALEKSANDER PAWLAK, HENRYK TUR, TOMASZ SMYKOWSKI, ANNA WASILEWSKA-ŚPIOCH
kontakt z redakcją Niezbędnika: redakcja@di24.pl

Wsparcie merytoryczne zapewnili eksperci firmy Microsoft Polska: BARBARA MICHALSKA, ALICJA RDZANEK, RENATA ZALEWSKA, PIOTR BRALSKI, MARCIN KLIMOWSKI, BARTŁOMIEJ MACHNIK, ŁUKASZ PIĄTKOWSKI

Dziękujemy za udział w opracowaniu Niezbędnika ekspertom z firm oferujących rozwiązania i usługi, wspomagajace bezpieczeństwo IT małych i średnich przedsiębiorstw.

WYDAWCA:
Dziennik Internautów Sp. z o.o.
ul. Okopowa 58/72
01-042 Warszawa
www. di24.pl

PARTNER MERYTORYCZNY WYDANIA: Microsoft