ANTYWIRUS TO ZA MAŁO. JAK DBAĆ, BY DANE NIE WYCIEKŁY Z FIRMY?

Autor tekstu:
Redakcja magazynu MŚP Biznes

Firmy, które doświadczają ataku hakerskiego, wycieku danych lub innego cyberprzestępczego działania i nie są na taką katastrofę przygotowane w większości upadają. Zabezpieczenia, które byłyby w stu procentach pewne nie istnieją. Dlatego każda firma stale powinna zwiększać świadomość w zakresie cyberbezpieczeństwa wśród swoich pracowników. Tylko w ten sposób można zminimalizować ryzyko wycieku, włamania czy wykradzenia danych, a co za tym idzie utraty ciągłości pracy, szkód wizerunkowych i strat finansowych.

Dla wielu osób pojęcie „bezpieczeństwo informacji" kojarzy z przede wszystkim z zabezpieczaniem systemów komputerowych lub ochroną danych osobowych w firmie. Temat bezpieczeństwa informacji jest jednak bardzo rozbudowanym procesem i dotyczy właściwie każdej informacji, która jest cenna dla użytkownika. Firmy, bez względu na branżę i ilość przetwarzanych danych, powinny zadbać o wdrożenie profesjonalnych zabezpieczeń, dzięki którym infrastruktura będzie chroniona przed potencjalnymi atakami - mówi Adam Wojak z Virtline, firmy specjalizującej się we wdrożeniach i audytach związanych z bezpieczeństwem informatycznym.

Według eksperta najważniejszymi funkcjami bezpieczeństwa są:

- **poufność** – dokładne sprecyzowanie, jakie osoby będą miały dostęp do zasobów firmowych,
- **dostępność** – zapewnienie upoważnionym osobom swobodnego dostępu do informacji w każdej chwili, bez występowania o specjalne zgody,
- **integralność** – doprowadzenie do sytuacji, w której wszystkie dane będą ze sobą spójne.

Wykaz strat poniesionych przez firmy na skutek ataków sieciowych:

33% - utrata klientów
33% - poniesienie wysokich strat finansowych
31% - ujawnienie lub modyfikacja danych
16% - spadek zaufania rynkowego i zachwianie reputacji firmy

Źródło: PwC

Coraz częściej do niestabilności systemów doprowadzają błędy popełnione przez użytkowników. Wynikają one głównie z braku dostatecznej wiedzy na temat bezpieczeństwa informacji oraz zasad prawidłowego używania sprzętu firmowego.

Najpierw szkolenia, audyt i monitoring

Wielokrotnie udowodniliśmy, że firmy przechodzą negatywnie testy socjotechniczne. Przykładowo: zdołaliśmy zalogować się do kont służbowych na skrzynkach pocztowych oraz uzyskaliśmy dostęp do serwerowni bez żadnego nadzoru ze strony personelu - mówi ekspert Virtline i dodaje, że to czynnik ludzki okazuje się najsłabszym ogniwem. Dlatego warto pamiętać, że nawet jeśli systemy informatyczne wydają się pozornie bezpiecznie, mogą nie spełniać swojej roli, jeśli personel nie będzie świadomy istniejących zagrożeń. Najlepszą metodą na zminimalizowanie ryzyka jest przeprowadzanie cyklicznych szkoleń przez profesjonalistów ds. bezpieczeństwa.

Podczas spotkań z klientami często spotykamy się z negatywnym nastawieniem do wprowadzania środków ochronnych. Słyszymy: „jesteśmy zbyt małym przedsiębiorstwem, aby zabezpieczać dane, ataki nas nie dotyczą". Tymczasem realia pokazują, że jest zupełnie odwrotnie - mówi Adam Wojak. Małe firmy nie inwestują w systemy bezpieczeństwa, dlatego zdecydowanie bardziej są podatne na ataki sieciowe i zagrożenia płynące z Internetu - ostrzega. Podobnego zdania jest to Piotr Kupczyk z Kaspersky Lab Polska. Jego zdaniem nawet najlepszy system bezpieczeństwa może zawieść, jeżeli personel

firmy będzie popełniał podstawowe błędy i ignorował higienę komputerową. Dlatego niezbędnym elementem firmowego bezpieczeństwa powinny być szkolenia, podczas których pracownicy nauczą się postępować tak, by nie zagrażać sobie i pracodawcy.

Niewiedza i niedbałość pracowników, zgodnie ze statystykami, są główną przyczyną powstałych incydentów bezpieczeństwa IT, ale zdarza się również, że jest to celowe działanie pracowników. Dotyczy to zazwyczaj najcenniejszych danych firmy, gdyż nikt inny tylko pracownicy mają dostęp do takich informacji. Przed tego typu incydentami chronią rozwiązania monitorujące.

Dostępne są dwa podejścia DLP (Data Leakage Prevention) oraz UEBA (User and Entity Behavior Analytics). Narzędzia DLP zabezpieczają przed wyciekiem informacje krytyczne, skupiając się na samych informacjach. Natomiast narzędzia UEBA analizują zachowania użytkowników i zasobów do których mają dostęp. Innymi słowy DLP koncentruje się na samych danych, a UEBA na użytkownikach obsługującym te dane - wyjaśnia Paulina Świątek, konsultant rozwiązań ICT w Comarch. Naturalnym wydaje się być łączenie tych rozwiązań celem usprawnienia analizy interakcji między użytkownikami i wrażliwymi danymi – dodaje.

Zdaniem Adama Wojaka z Virtline, metodologią, pozwalającą na weryfikację faktycznego stanu bezpieczeństwa w firmie, jest cykliczne przeprowadzenie audytów sieci, serwerów i bezpieczeństwa informacji. Celem audytu jest weryfikacja stanu faktycznego infrastruktury teleinformatycznej. Po jego zakończeniu następuje przekazanie raportu, który zawiera opis wszystkich luk, niezgodności oraz potencjalnych zagrożeń. Rekomendacje rozwiązań dotyczą zarówno sprzętu, jak i cyklicznych prac, które mają za zadanie podnieść poziom bezpieczeństwa.

Narzędziem usprawniającym zarządzanie infrastrukturą IT w firmie jest z kolei wdrożenie monitoringu informatycznego. Obserwacja sieci, serwerów i oprogramowania w czasie rzeczywistym pozwala przewidzieć wystąpienie potencjalnych awarii. Dzięki szybkiej reakcji na pojawiające się alerty, informatycy są w stanie zapobiec atakom sieciowym czy niestabilności działania urządzeń. W przypadku napotkania potencjalnego zagrożenia, system powiadamia o tym fakcie odpowiednią osobę drogą e-mailową lub przez wysłanie SMS. Dzięki bieżącej obserwacji usług sieciowych i sprzętu firmy mogą uniknąć awarii lub zminimalizować jej negatywne konsekwencje – podkreśla Adam Wojak. Często monitoring informatyczny jest sprzężony z systemami, takimi jak IDS/IPS czy SIEM, dzięki którym jest w stanie ostrzec administratorów danych przed anomaliami sieciowymi oraz atakami – dodaje.

Zagrożenia wewnętrzne

Najbardziej niszczycielskie i najbardziej ukryte ataki na nowoczesne systemy cyberbezpieczeństwa pochodzą od osób wewnątrz firmy, mających uprawniony dostęp, znających tajniki korporacyjnej infrastruktury i codziennie wykonujących tysiące operacji na danych i konfiguracjach – twierdzi Paweł Chudziński, CEO firmy Ekran System, dostarczającej narzędzia do monitorowania zagrożeń związanych z bezpieczeństwem wewnętrznym.

Zdaniem eksperta, wystarczy spojrzeć na statystyki:

- 53% organizacji doświadczyło ataków wewnętrznych w ciągu ostatnich 12 miesięcy – wynika z Threat Report by Crowd Research Partners 2018.
- Koszt naruszenia danych przez pracowników rośnie z każdym rokiem. Całkowity średni koszt incydentów związanych z informacjami poufnymi w okresie 12 miesięcy = 8,76 mln USD (11,1 mln USD w USA).
- Roczny koszt z powodu: Zaniedbania = 3,81 mln USD, Osoby odpowiedzialnej za przestępstwo = 2,99 mln USD, Kradzieży poświadczeń = 1,96 mln USD - według raportu 2018 Cost of Insider Threats: Global Organizations by the Ponemon Institute.
- 19% wszystkich przypadków naruszenia danych w sektorze finansowym spowodowanych jest przez użytkownika wewnętrznego. 56% wszystkich przypadków naruszenia danych w służbie zdrowia spowodowanych jest przez użytkownika wewnętrznego. 34% wszystkich przypadków naruszenia danych w administracji publicznej spowodowanych jest przez użytkownika wewnętrznego - według Verizon 2018 Data Breach Investigation Report.

Aplikacje kontrolujące

Osoby odpowiedzialne za bezpieczeństwo informatyczne w firmach i bezpieczeństwo danych coraz częściej interesują się specjalistycznymi rozwiązaniami kategorii Data Loss Prevention (DLP). Wynika to jednak nie tyle z braku zaufania do pracowników, ile ze zmian prawa dotyczących unijnego rozporządzenia o ochronie danych osobowych (RODO).

Są to aplikacje ściśle kontrolujące to, co każdy z pracowników robi na swoim komputerze z poufnymi danymi. Mogą to być dane osobowe, ale nie tylko. Mogą to również być poufne projekty, technologie – wszystko co stanowi ścisłą tajemnicę firmy – wyjaśnia Paweł Jurek, wicedyrektor ds. rozwoju w firmie DAGMA. Oprogramowanie tego typu może ściśle monitorować jakie czynności każdy z pracowników wykonuje na zbiorach tych danych – czy i kiedy je otwiera, kopiuje, czy też w jakie miejsca wysyła. Aplikacje DLP mogą również zablokować możliwość wysłania pewnych kategorii danych poza firmę – tym samym zapobiegając wyciekowi danych.

Oprogramowanie tego typu, samo w sobie – jest już znane od kilku lat. Nowością jest rosnące zainteresowanie firm z kategorii średnich i małych przedsiębiorstw. Dlatego też na przykład firma DAGMA wprowadziła niedawno do oferty rozwiązania firmy SAFETICA.

Wcześniej systemy tego typu stosowane były jedynie w dużych korporacjach, a ich wdrożenie było nierozłącznie związane z bardzo dużym nakładem pracy – pracodawca musiał bardzo ściśle kategoryzować dane i ustalać uprawnienia każdego z pracowników, bo bez tego aplikacje nie mogły skutecznie działać - mówi Paweł Jurek. Dla skutecznego wdrożenia tego typu ochrony w firmach małych i średnich potrzeba rozwiązania elastycznego, które może dostosować się do specyfiki działania takich firm.

Zdaniem eksperta, barierą jest nadal niska wiedza klientów na temat tego typu rozwiązań. Ci, którzy wcześniej oglądali trudniejsze we wdrożeniu rozwiązania wciąż mają wysokie obawy przed tym, czy będą w stanie skutecznie system DLP wdrożyć. Jednak rosnąca troska klientów o ochronę poufnych danych firmy, w tym przede wszystkim danych osobowych, sprawia, że z czasem te obawy będą odgrywać coraz mniejszą rolę.

Zaawansowane rozwiązania

Typowy antywirus już nie wystarcza do skutecznej walki z zagrożeniami biznesowymi - twierdzi Piotr Kupczyk z Kaspersky Lab Polska. Dlatego, jego zdaniem, oprócz niezbędnej ochrony punktów końcowych warto stosować rozwiązania zabezpieczające klasy enterprise, takie jak Kaspersky Anti Targeted Attack Platform, które wykrywa zaawansowane zagrożenia i wszelkie anomalie na poziomie sieci już na wczesnym etapie. W celu zapewnienia wykrywania na poziomie punktu końcowego, badania i niezwłocznego naprawiania szkód można rozważyć wdrożenie rozwiązania EDR, takiego jak Kaspersky Endpoint Detection and Response, lub korzystać z usług profesjonalnego zespołu ds. reagowania na incydenty.

Kolejnym krokiem, zdaniem eksperta z Kaspersky Lab Polska, jest zastosowanie źródeł danych o cyberzagrożeniach i zintegrowanie ich z działającymi w firmie systemami bezpieczeństwa. Daje to możliwość zauważenia potencjalnego ataku na bardzo wczesnym etapie, zanim cyberprzestępcy zdążą wyrządzić konkretne szkody.

Niezbędnym elementem nowoczesnej ochrony jest także system wykrywania luk w zabezpieczeniach, najlepiej wyposażony w możliwość automatycznego usuwania takich podatności. Biorąc pod uwagę niesłabnące zagrożenie ze strony oprogramowania szyfrującego dane dla okupu (tzw. ransomware), warto zwrócić uwagę, by wdrażane rozwiązanie bezpieczeństwa posiadało dodatkowe funkcje, przygotowane z myślą o odpieraniu ataków tego typu.

Ochronę należy traktować całościowo i z tego względu najlepszym rozwiązaniem jest zdecydowanie się na dostawcę, który jest w stanie zaoferować spójną platformę bezpieczeństwa, która jest łatwa w zarządzaniu, a jej moduły płynnie ze sobą współgrają.

Działania w chmurze

Przyzwyczailiśmy się do składowania danych w usługach chmurowych, nie zawsze jednak zdajemy sobie sprawę z konsekwencji na jakie naraża nas tzw. shadow IT. Administrator musi dbać o tę sferę środowiska IT, kontrolować kanały komunikacyjne, a tam, gdzie to jest uzasadnione - zabezpieczać dane w poprawny sposób – mówi Grzegorz Szmigiel, dyrektor techniczny w firmie Veracomp, dystrybutora rozwiązań teleinformatycznych. Jego zdaniem muszą temu towarzyszyć również szkolenia pracowników, aby świadomie korzystali z narzędzi zewnętrznych, mieli świadomość ryzyk i tym samym chętniej stosowali zasady ochrony danych. Z pomocą mogą tutaj przyjść rozwiązania producentów Symantec, Fortinet, Watchguard, Proofpoint.

A czy aplikacje w chmurze są bezpieczne oraz czy możemy je kontrolować? Producenci systemów bezpieczeństwa pracują nad tym obszarem od dłuższego już czasu dostarczając rozwiązania typu CASB (Cloud Access Security Broker). W ramach tej grupy systemów oferują mechanizmy, które zabezpieczają, ale przede wszystkim kontrolują informacje w komunikacji naszych aplikacji do świata zewnętrznego. W tym zakresie, Grzegorz Szmigiel, wymienia produkty firm: Fortinet oraz Symantec.

Zabezpieczenie danych

Nie tylko technologia idzie do przodu, ale również hakerzy robią wszystko, by być o krok przed użytkownikiem. Dlatego zdaniem Marcina Bręczewskiego, dyrektora działu wsparcia IT w IT Company warto pomyśleć nie tylko o ochronie przed atakami, ale też prawidłowym i przede wszystkim skutecznym zabezpieczeniu danych.

Firma IT Company opracowała dla klientów tzw. plan disaster recovery. Jest to zbiór procedur reaktywacji funkcjonowania środowiska IT po wystąpieniu krytycznego dla organizacji zdarzenia, jak np. zniszczenie środowiska serwerowego, czy właśnie atak hakerski. Plan disaster recovery ma na celu zapewnienie ciągłości działania procesów biznesowych oraz efektywne przywrócenie pełnej sprawności systemu IT w ściśle określonym czasie. W skrócie, określa kto, gdzie, kiedy i w jaki sposób ma zareagować na konkretne zdarzenie. Disaster recovery chroni firmę przed nieplanowanymi przestojami w pracy i innymi kosztownymi komplikacjami – wyjaśnia Marcin Bręczewski.

Jeżeli mówimy o przywracaniu i ochronie danych, to warto również wspomnieć o szerokiej gamie usług backupu w chmurze (cloud backup). Sama ochrona danych to jeszcze za mało. Bardzo istotne jest to, jak szybko i łatwo można te dane odzyskać. Małe i średnie firmy często nie tworzyły planów disaster recovery z powodu wysokich kosztów budowy środowiska odtworzeniowego. Możliwości, które oferuje chmura i różne modele współpracy całkowicie zmieniły dostępność nowoczesnych systemów backupowych.

Ubezpieczenie cybernetyczne

Pamiętać powinniśmy, że zdarzenia wywołane przez hakerów mogą zaszkodzić firmie pod kątem prawnym i finansowym, a także negatywnie wpłynąć na jej reputację. Dodatkowo rygorystyczne wymagania w związku z RODO i rosnąca świadomość zagrożeń, które czekają w cyberprzestrzeni, sprawiają, że warto zwrócić uwagę na ubezpieczenia cybernetyczne. Co dzięki takiej polisie możemy zyskać?

Przede wszystkim ubezpieczona firma ma możliwość skorzystania z oferowanej przez ubezpieczyciela i dostępnej 24/7 infolinii. Za jej pomocą zgłasza problem, jaki wystąpił w organizacji, a specjalistyczny podmiot koordynujący wszelkie działania (opłacany przez ubezpieczyciela), podejmuje decyzje o dalszych krokach - mówi Marcin Czyszka, dyrektor biura ds. informatyki brokera ubezpieczeniowego Mentor, oferującego specjalistyczne ubezpieczenia dla firm. Po zgłoszeniu incydentu uruchamiana jest pomoc informatyków śledczych, którzy badają źródło ataku i pomagają usunąć zagrożenie. Ubezpieczyciel pokrywa przy tym także odzyskanie utraconych danych i postawienie systemów do stanu sprzed szkody.

Zdaniem eksperta powinniśmy pamiętać, że pierwsze godziny po wykryciu cyberataku są niezwykle ważne. Szybkie zatrzymanie np. dalszego wycieku danych może zaowocować mniejszymi kosztami całego zdarzenia. Może zdarzyć się, że osoby niepowołane uzyskają dostęp do danych osobowych np. naszych klientów czy kontrahentów. Warto pamiętać, że przepisy RODO nakładają na administratora danych obowiązek powiadomienia zarówno organu nadzoru oraz osób, których dane zostały naruszone. Jest on aktualizowany w przypadku wysokiego ryzyka naruszenia praw i wolności takich osób. Ubezpieczyciel w takim przypadku pokryje koszty notyfikacji, czyli na przykład koszty sporządzenia pisma do urzędu czy wysyłki oświadczeń do osób fizycznych.

Tak samo jak w przypadku szkody majątkowej, istnieje duże prawdopodobieństwo, że cyberatak przed dłuższy czas negatywnie będzie wpływał na wyniki finansowe firmy. Ubezpieczenie oferuje pokrycie szkody wynikającej z utraty dochodów netto. Jest to kwota, która odpowiada wysokości, jaką podmiot uzyskałby w sytuacji, gdyby nie doszło do zdarzenia. Niezwykle ważnym elementem ochrony są również koszty wynajęcia specjalistów ds. ochrony wizerunku - przypomina Marcin Czyszka. Praktycznie codziennie spotykamy się z informacjami medialnymi o wyciekach danych czy cyberatakach, co może powodować spadek zaufania do podmiotu dotkniętego takim zdarzeniem. Wynajęta firma będzie odpowiadać za poprawę wizerunku wśród opinii publicznej.

Ubezpieczenia tego rodzaju ma w swoje ofercie kilka firm. Przykładowo PZU w ramach ubezpieczenia od ryzyk cybernetycznych zapewnia pomoc ekspertów w razie sytuacji kryzysowej m.in. informatyków śledczych, kancelarii prawnej, agencji PR oraz rekompensuje utratę zysku przedsiębiorstwa. Pokrywa koszty roszczeń np. odszkodowań, zadośćuczynień, kar administracyjnych oraz, co ważne, zapewnia pomoc prawną w zakresie zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych.

W ofercie STU ERGO Hestia również znajdziemy ubezpieczenie Cyber. Zawiera ono w sobie elementy wielu znanych produktów ubezpieczeniowych: majątkowych, odpowiedzialności cywilnej, BI, ochrony prawnej. Jak deklaruje Tomasz Dolata z Biura Ubezpieczeń Korporacyjnych STU ERGO Hestia, ubezpieczyciel zapewnia ochronę ubezpieczeniową w czterech różnych obszarach:

1. **Ochrona danych elektronicznych** – ubezpieczony otrzymuje zwrot kosztów za przywrócenie danych, ich odtworzenie, zakupu nowego oprogramowania, odblokowania dostępu do danych, a także serwis asystorski w postaci informatyki śledczej. Ochroną mogą być objęte także błędnie wykonane przelewy bankowe w wyniku działania wirusa komputerowego.

2. **Pozostałe koszty ataku** – ubezpieczyciel pokrywa koszty wsparcia prawniczego, ekspertów public relations, notyfikacji klientów w przypadku wycieku danych, poszukiwania sprawcy ataku, kary administracyjne, koszty okupu, a także koszty zakupu nowego sprzętu elektronicznego uszkodzonego w wyniku działania wirusa lub ataku komputerowego.

3. **Ochrona osób trzecich** – przewiduje pokrycie kosztów zadośćuczynienia w sytuacji, gdy w efekcie wycieku danych z firmy pokrzywdzone osoby zgłoszą się do niej z roszczeniami. Ubezpieczenie w tej sekcji zadziała również wtedy, gdy np. zainfekujemy sieć kontrahenta lub spowodujemy wyciek danych u klienta.

4. **Zapewnienie ciągłości działalności** – ubezpieczyciel pokrywa utracony zysk oraz zwiększone koszty działalności poniesione przez ubezpieczonego w okresie, kiedy usuwał skutki ataku.

Możliwość zawarcia ubezpieczenia warunkowana jest przede wszystkim stanem zabezpieczeń informatycznych firmy oraz stosowaniem procedur przetwarzania danych osobowych, a także posiadaniem planu kontynuacji na wypadek wystąpienia zagrożenia. Od spełnienia wspomnianych wymagań, a także od wysokości sumy ubezpieczenia i wielkości firmy uzależniona jest wysokość składki. Dla dobrze zabezpieczonych organizacji składki przy sumie ubezpieczenia 1.000.000 zł oscylują w granicach 8-10 tys. zł.

Czy to dużo? Na to musi odpowiedzieć sobie już każda firma sama. Warto zdawać sobie jednak sprawę z tego, że 90% firm, które doświadczyły katastrofy, a nie mają wdrożonego planu disaster recovery o którym mówił Marcin Bręczewski z IT Company, upada. Każda firma powinna być zatem przygotowana na najbardziej prawdopodobne ryzyko i pewna, że ciągłość pracy zostanie przywrócona w oczekiwanym terminie. ■