Cyberostrożności nigdy za wiele – czyli jak efektywnie chronić swoją firmę przed cyberzagrożeniami

W realiach gospodarki opartej na wiedzy i innowacjach to informacje – dane, kontakty biznesowe, *know-how* – są największym zasobem przedsiębiorstw. Niestety, również niezwykle podatnym na ataki czy kradzieże. Utrata danych, choćby w wyniku zwykłej awarii, może skutkować zakłóceniami i przestojami w funkcjonowaniu biznesu, nadwyrężeniem zaufania klientów, a wreszcie – konkretnymi stratami finansowymi. Cyberbezpieczeństwo z problemu uważanego za abstrakcyjny staje się więc palącą potrzebą przedsiębiorców.

Autorka: Ewa Piekart

„Cyberataki dotykają duże korporacje albo banki, nas to nie dotyczy" – to szkodliwe przekonanie cały czas pokutuje w społeczeństwie. Tymczasem na wyciek danych jesteśmy narażeni cały czas: i jako osoby prywatne, i jako przedsiębiorcy. Zjawisko to można już nazwać powszechnym. W 2017 roku 82 proc. spośród firm działających w Polsce odnotowało co najmniej jeden cyberincydent[1]. Globalne koszty związane z cyberprzestępczością idą w biliony dolarów rocznie. Co można zrobić, by uchronić swoją firmę przed cyberatakami?

Zwiększanie wydatków na bezpieczeństwo nie wystarczy

Świadomość skali zagrożeń, na które narażone są dane biznesowe, stale rośnie. Zresztą pewne działania związane z ich ochroną wymuszają nowe regulacje prawne, czyli słynne RODO. Coraz więcej przedsiębiorców wprowadza u siebie politykę bezpieczeństwa danych. Szacuje się też, że tylko w tym roku blisko połowa z nich zwiększy wydatki na ten cel. To oczywiście pozytywny trend. Jednak przekonanie, że bezpieczeństwo informacji są w stanie zapewnić jedynie zaawansowane technologicznie, kosztowne systemy, to mit. Często bowiem zdarza się, że wyciek danych następuje z winy pracownika. A w takim przypadku nie pomogą nawet najdroższe zabezpieczenia.

Aby skuteczniej chronić firmowe zasoby, nie potrzeba wcale gigantycznych budżetów. Należy jednak wystrzegać się pewnych błędów. Które z nich są popełniane najczęściej?

Błąd 1: brak szyfrowania danych na urządzeniach mobilnych

Kto choć raz nie zabrał ze sobą służbowego laptopa, żeby popracować z domu nad ważnym projektem? Nie ściągał plików lub korespondencji na służbowy smartfon? A przecież to urządzenia, które są wyjątkowo narażone na kradzież. Tak samo jak zewnętrzne nośniki danych, np. pendrive'y. Do ich notorycznego gubienia przyznaje się niemal połowa pracowników. Oznacza to, że dane, które na nich zapisujemy, bardzo łatwo mogą się dostać w niepowołane ręce.

Jedynym rozwiązaniem jest tu szyfrowanie. Szyfrując dane, uniemożliwia się uzyskanie do nich dostępu bez uprzedniego podania hasła lub szyfru. Stają się także niedostępne po wyjęciu dysku czy nośnika. Nie jest to skomplikowana czynność, wystarczy bowiem skorzystać z programów szyfrujących. Są one dostępne w ramach pakietu Windows (Windows 10 Professional i wyższe wersje). Można również kupić odpowiednią licencję.

Błąd 2: niewłaściwe tworzenie kopii zapasowych

Kopie zapasowe są jednym z filarów cyberbezpieczeństwa przedsiębiorstwa i polisą gwarancyjną na wypadek utraty danych, ale… tylko wtedy, gdy tworzy się je poprawnie. Podstawą dobrego backupu jest zasada „3-2-1", czyli: twórz trzy kopie zapasowe używając co najmniej dwóch różnych technologii przechowywania danych, a jedną z kopii zapasowych – koniecznie zaszyfrowaną! – trzymaj zawsze poza biurem. Tymczasem wielu przedsiębiorców zapomina o tym trzecim elemencie i przechowuje wszystkie kopie zapasowe w swojej siedzibie.

O co jeszcze należy zadbać? Przede wszystkim o właściwe zabezpieczenie kopii. Trzeba również sprawdzić poprawność ich odtwarzania. Kluczowe jest również, żeby wykonywać backup regularnie i cyklicznie. Tylko wtedy można mieć pewność, że w przypadku utraty danych, np. wskutek awarii, będzie można przywrócić je w aktualnej wersji. Dlatego najlepiej tworzyć kopie zapasowe online i w czasie rzeczywistym.

Błąd 3: niewłaściwa ochrona antywirusowa lub jej brak

Wraz z rozwojem technologii i zabezpieczeń rośnie również poziom złożoności zagrożeń. Źródłem znacznej części z nich jest tzw. złośliwe oprogramowanie, czyli prościej mówiąc – wiru-

[1] https://assets.kpmg/content/dam/kpmg/pl/pdf/2018/01/pl-Barometr-cyberbezpieczenstwa-cyberatak-zjawiskiem-powszechnym.pdf

sy komputerowe. Eksperci prognozują, że jeszcze w 2019 roku ataki typu ransomware („szantażujące" – czyli blokujące dostęp do danych do czasu wpłacenia okupu) będą występować średnio co 14 sekund! Dlatego dobra ochrona antywirusowa to podstawa.

Dobra, czyli jaka? Po pierwsze, nie należy używać w firmach programów antywirusowych na licencji darmowej lub typu „home". Często są one pozbawione typowo biznesowych funkcji, jak np. skanowanie poczty czy moduł ochrony bankowości elektronicznej. Po drugie, błędem jest instalacja dwóch różnych antywirusów (np. jednego biznesowego, drugiego darmowego). Wcale nie zyskuje się dzięki temu podwójnej ochrony. Wręcz przeciwnie – może to skutkować niestabilnością systemu i spadkiem poziomu zabezpieczeń.

Absolutną koniecznością są także jak najczęstsze aktualizacje – nie tylko antywirusów, lecz wszystkich programów i systemów. Często odkłada się je, bo wiążą się np. z restartem komputera. Tymczasem aktualizacje pozwalają załatać w oprogramowaniu luki, które mogłyby zostać wykorzystane przez wirusy czy hakerów.

Błąd 4: brak systemów typu IDS i IPS

IDS i IPS – te skróty mogą brzmieć obco i skomplikowanie, ale kryją się pod nimi systemy wykrywania (IDS) oraz zapobiegania (IPS) włamaniom. Analizują one ruch sieciowy i monitorują ruch pakietów danych, dzięki czemu są w stanie szybko namierzyć „intruzów". Wykrywają podejrzaną aktywność. Potrafią zablokować poczynania włamywacza czy też wysłać alert do administratora systemu. Dzięki temu znacząco poprawiają cyberbezpieczeństwo firmy, dlatego warto w nie zainwestować.

Błąd 5: niewłaściwa kontrola dostępu do systemu

Przedsiębiorstwa, które padły ofiarą cyberprzestępstw, najczęściej popełniały jeden z podstawowych błędów: niewłaściwie zarządzały dostępem do danych. Dostęp do danych i uprawnienia dla poszczególnych użytkowników powinny być limitowane, czyli nadawane z poziomu administratora tylko w takim zakresie, który rzeczywiście jest potrzebny do wykonywania zadań. Dobrą praktyką jest też jak najszybsze kasowanie nieaktywnych kont.

Dodatkowo należy zadbać o to, by hasła dostępu były unikalne dla każdego użytkownika. Należy zmieniać je cyklicznie i nie powinno się ich powtarzać. Nie należy również używać tego samego hasła w dwóch różnych systemach i serwisach, np. jako zabezpieczenia dostępu do komputera i do skrzynki pocztowej.

Błąd 6: brak odpowiedniego przeszkolenia pracowników

Wbrew obiegowym opiniom, za znaczną część przypadków wycieku danych nie odpowiadają wyrafinowane cyberataki, lecz… pracownicy. W branży IT mówi się, że najsłabszym ogniwem w systemie bezpieczeństwa jest człowiek. Kluczowe jest więc budowanie w pracownikach świadomości zagrożeń i zasad dotyczących bezpieczeństwa danych poprzez szkolenia.

Jeśli chodzi o błędy popełniane przez personel, najczęściej powtarzają się te same, niezależnie od miejsca zatrudnienia czy branży. Dlatego warto przypominać swoim pracownikom, by nie zostawiali w widocznym miejscu haseł zapisanych na samoprzylepnych karteczkach, nie udostępniali nikomu danych logowania czy stosowali hasła trudniejsze do złamania niż „QWERTY1234". Dobrze również ich przeszkolić, jak powinni się zachować w sytuacji zagrożenia bezpieczeństwa danych: tak, by wiedzieli, komu i w jakiej formie to zgłosić.

Konsekwencja przede wszystkim

Jak widać, wystarczy przestrzegać kilku prostych reguł, by w łatwy i niezbyt kosztowny sposób podnieść cyberbezpieczeństwo firmy. Kluczem do sukcesu jest jednak żelazna konsekwencja i egzekwowanie tych reguł od siebie i od swoich pracowników. Tylko wtedy przechowywane przez nas dane będą bezpieczniejsze, a my sami będziemy mogli spać spokojniej. ■