Bezpieczeństwo przede wszystkim!

Cyberbezpieczeństwo – to słowo brzmi groźnie i onieśmiela. Kojarzy się ze skomplikowanym oprogramowaniem i rozbudowanymi, kosztownymi systemami, na które pozwolić mogą sobie nieliczni. Tymczasem, jak przekonuje Ewa Piekart, szefowa Data Point i CKZ.pl, czasami wystarczy zacząć od wdrożenia bardzo prostych reguł, by uchronić nasze dane przed kradzieżą, wyciekiem czy bezpowrotną utratą.

Rozmawia ALEKSANDRA BOROWIEC

W dzisiejszych czasach – w dobie RODO – słowo „dane" odmieniane jest przez wszystkie przypadki. Składujemy je, przetwarzamy, analizujemy, archiwizujemy. Zwykłym ludziom, konsumentom, kojarzą się głównie z dziesiątkami zgód i oświadczeń, które podpisujemy czy odklikujemy każdego dnia. Ale przecież szeroko pojęte dane to we współczesnym świecie podstawa funkcjonowania przedsiębiorstw.

– Powiedziałabym więcej: to często ich największy kapitał! A liczba danych cały czas rośnie. Eksperci szacują, że w przeciętnej firmie liczba przechowywanych danych może wzrastać nawet o 65 proc. rocznie. Odpowiednio je zabezpieczyć – to dopiero wyzwanie. Śmieję się, że bezpieczeństwo danych jest moim i mojej firmy oczkiem w głowie, ale… tak jest. Proszę sobie wyobrazić, że przedsiębiorca w jednej chwili traci na przykład korespondencję z kluczowymi klientami lub listę kontaktów. Albo, co gorsza, wycieka ona z firmy i trafia w ręce konkurencji. Katastrofa! Oczywiście, przykład tego typu wrażliwych danych, w tym danych osobowych, jest bardzo przejaskrawiony, jednak dobrze obrazuje skalę potencjalnych zagrożeń.

Ale czy rzeczywiście niebezpieczeństwo jest tak realne? Cyberataki, poważne awarie systemów i inne tego typu sytuacje kryzysowe wydają się raczej abstrakcyjne. I powszechnie uważa się, że narażone są na nie duże firmy.

– To błędne myślenie, które może drogo kosztować. To właśnie małe, świeżo powstałe firmy bardziej odczują paraliż związany z utratą danych. Wszystko przez to, że bardzo często nie zdążyły one jeszcze wypracować kompleksowej polityki bezpieczeństwa informacji – zbioru zasad i procedur, które pozwalają minimalizować ryzyko utraty danych, ale także np. instrukcji postępowania w sytuacjach kryzysowych. Oczywiście, trudno mówić o uniwersalnej polityce bezpieczeństwa, która pasowałaby wszystkim. Rozwiązania powinny być skrojone do potrzeb konkretnego przedsiębiorcy. Zawsze należy zacząć od pytania: „po co?", a dopiero potem: „jak?". Inaczej przecież zabezpieczać będziemy dane w banku, a inaczej – w hurtowni.

A jak wygląda poziom świadomości problemu w społeczeństwie i w firmach?

– Na szczęście systematycznie rośnie. Na początku padło już hasło „RODO". To właśnie zmiany w przepisach dotyczących przetwarzania danych osobowych coraz częściej skłaniają przedsiębiorców do opracowania polityki bezpieczeństwa danych. Posiadają ją już cztery na pięć polskich firm. Kolejnym bodźcem jest coraz większe zagrożenie. Tutaj liczby mówią same za siebie. Szacuje się, że w 2017 roku aż 80 proc. polskich firm odnotowało przynajmniej jeden cyberincydent. Prawie jedna czwarta z nich deklaruje, że w wyniku ataku straciła klientów. Proszę zatem zobaczyć, jaka jest skala problemu.

To wszystko brzmi dość groźnie i… dość skomplikowanie. Polityka bezpieczeństwa informatycznego to nie dokument, który można przygotować z dnia na dzień.

– Oczywiście, że nie. Nie chodzi o to, żeby tworzyć pewną fikcję, ale żeby uzyskać skuteczne i efektywne narzędzie.

Nie mogę nie zapytać o koszty. Nie sądzi pani, że dla części przedsiębiorców to one mogą być barierą w odpowiednim zabezpieczeniu danych? Co innego wielka korporacja z własnym działem IT i dużym budżetem, a co innego – rodzinna firma, która nie dysponuje takimi pieniędzmi. Czy i tu da się znaleźć jakieś rozwiązanie?

– Przekonanie o tym, że zabezpieczanie danych musi pochłonąć ogromne koszty, to kolejny szkodliwy mit. Poza tym, wbrew temu, co pokazuje nam Hollywood, wyciek danych w wyniku ataków hakerskich to nie mozolne łamanie kodu, lecz bardzo często efekt błędów, zaniedbań czy zwykłej nieświadomości pracowników. Zawsze znajdzie się przecież ktoś, kto hasło do komputera czy skrzynki pocztowej zapisze na tej nieszczęsnej żółtej karteczce, a taką łatwo jest wykraść. Dlatego też sam zakup najbardziej zaawansowanych technologicznie, choćby nie wiem jak kosztownych zabezpieczeń, nie wystarczy. Kluczowe jest czynnik ludzki i uświadamianie pracowników. Na tym poziomie możemy podjąć bardzo dużo działań, które nie wymagają dużego budżetu, a i tak znacząco poprawią cyberbezpieczeństwo naszej firmy.

Zawsze doradzam zabezpieczanie hasłami również zewnętrznych nośników danych. Coraz częściej podróżujemy np. z pendrive'ami czy zewnętrznymi dyskami, na których mogą znajdować się wrażliwe, istotne dla naszej firmy informacje

Na przykład?

– Pierwszy z brzegu – zabezpieczenie wejścia do komputera hasłem. Brzmi ba-

nalnie, prawda? Większość z nas stosuje to rozwiązanie także w życiu prywatnym. A jednak kluczowy jest tu dobór odpowiedniego hasła. Powinniśmy wybierać tylko te, które są dostatecznie silne.

Silne, czyli jakie?

– Takie, które mają minimum osiem znaków, w tym wielkie i małe litery, cyfry oraz znaki specjalne. Czyli nie popularne „1234", „password" czy własne imię. Takie hasło powinno być także cyklicznie zmieniane i nie powinno się powtarzać. Używajmy różnych haseł, czyli: jeśli hasłem A blokujemy dostęp do komputera, to do poczty zastosujmy hasło B. Nie udostępniajmy naszych haseł nikomu i dbajmy o to, by po skończonej pracy – czy w czasie przerwy, gdy wychodzimy z pokoju – wylogować się. Nie używajmy opcji zapamiętywania hasła. To elementarne zasady, ale w rzeczywistości, zapewniam, ich przestrzeganie sprawia problemy. Aha, i błagam – żadnych żółtych karteczek!

Czyli bezwzględnie hasła do komputera. Co jeszcze możemy zrobić?

– Zawsze doradzam zabezpieczanie hasłami również zewnętrznych nośników danych. Coraz częściej podróżujemy np. z pendrive'ami czy zewnętrznymi dyskami, na których mogą znajdować się wrażliwe, istotne dla naszej firmy informacje. Tymczasem często widuje się takie nośniki beztrosko porzucone na stole konferencyjnym po skończonej prezentacji, prawda? Coraz mniejsze pendrive'y łatwo też zgubić. Dlatego powinniśmy zabezpieczyć je hasłem, by uniemożliwić kradzież danych. Tu wspomniałabym też o jeszcze jednej ważnej sprawie, która łączy się z kwestią zabezpieczenia dostępu do komputera. Pamiętajmy o jednym: tablety i smartfony, będące dzisiaj w powszechnym użyciu, to też komputery! Powinniśmy także i w nich używać odpowiednich zabezpieczeń, o czym wielu zapomina. Szacuje się, że prawie trzy czwarte cyberzagrożeń w polskich firmach w 2017 roku dotyczyło właśnie urządzeń mobilnych!

Zatem: hasła i jeszcze raz hasła. Ale załóżmy, że stało się. W wyniku, dajmy na to, awarii, straciliśmy dane. Co robić? Jak sprawić, żeby taka sytuacja nie sparaliżowała działalności naszej firmy i jak ograniczyć straty?

– Odpowiedź jest jedna: kopie zapasowe, czyli inaczej mówiąc, backup danych. To podstawa. Żelazną regułą jest zasada „3-2-1", czyli: miej trzy kopie zapasowe, używaj dwóch technologii przechowywania danych i jedną z kopii przechowuj zawsze poza biurem. Najlepiej, by jedna była wykonywana online, czyli w czasie rzeczywistym, i właśnie to rozwiązanie rekomenduję swoim klientom. Tym zaś, którzy z różnych powodów z niego nie korzystają, sugerowałabym regularne monitorowanie swoich backupów, by były one możliwie najbardziej aktualne. Zresztą zachęcam również do takiego postępowania w życiu prywatnym. Róbmy kopie zdjęć z wakacji czy fotografii naszych bliskich. To przecież ich najbardziej szkoda, gdy zalejemy kawą smartfon czy laptop.


Fot. Stasiuk

Wniosek jest jeden: zawsze należy zaczynać od prostych rozwiązań.

– Dokładnie. Oraz przekonać pracowników, że przestrzeganie zasad bezpieczeństwa ma znaczenie, a cyberbezpieczeństwo to nie abstrakcyjny wymysł kolegów z działu IT czy namolnego szefa. A tym spośród przedsiębiorców, którzy do tej pory raczej bagatelizowali tę kwestię, przypominam: cyberincydenty oznaczają często realne straty, które mogą iść nawet w setki tysięcy euro rocznie. ■