Bezpieczeństwo w sieci - o czym musi pamiętać przedsiębiorca

Nieważne, czy prowadzisz jednoosobową działalność gospodarczą, czy Twoja firma to kilka osób, musisz pamiętać o cyberbezpieczeństwie. Niezależnie od profesji i sektora – wdrażacie i stosujecie nowe technologie. Ministerstwo Cyfryzacji podpowiada, jak to robić bezpiecznie.

Zacznijmy od wydawałoby się najprostszej sprawy – strony internetowej. W dzisiejszych czasach każdy chce ją mieć. Często to najlepsza wizytówka i jeden z najskuteczniejszych sposobów na zdobycie klientów. Ważne, żebyś Ty się nie dał złapać. Przestępcom.

przedewszystkimbezpieczenstwo.pl

Jeśli „trzymasz" stronę na swoim serwerze, pamiętaj o aktualizacjach bezpieczeństwa i ważnym oprogramowaniu. Jeśli do firmowej witryny logują się Twoi współpracownicy, wymagaj od nich, aby robiąc to stosowali bezpieczne hasła. Kolejna sprawa – ogranicz możliwość przesyłania plików bezpośrednio na serwer i rozważ możliwość przeprowadzenia testów bezpieczeństwa witryny. Dobrym pomysłem jest także zarejestrowanie nazw domenowych brzmiących podobnie do adresu Twojej strony WWW. Chodzi m.in. o to, aby nikt nie podszywał się pod Twoją firmę.

Następna sprawa – poczta e-mail. Na pewno z niej korzystasz. Pamiętaj, aby usuwać wiadomości, które wydają Ci się podejrzane. Zachęć współpracowników do tego, aby Cię informowali, jeśli też dostali takie maile. Dlaczego to ważne?

– *Nawet przypadkowe zachowania każdego pracownika w przedsiębiorstwie mogą się stać przyczyną ataku na system informatyczny firmy. Dlaczego? Klikając umieszczone w mailach spreparowane linki lub uruchamiając załączniki przygotowane przez cyberprzestępców, otwieramy szeroko drzwi do naszych systemów* – tłumaczy Krzysztof Silicki, dyrektor ds. cyberbezpieczeństwo i innowacji w NASK. – *To dlatego stworzenie cyberbezpiecznej firmy wymaga odpowiedzialności i zaangażowania wszystkich pracowników* – dodaje.

Generalna zasada: dbaj o stosowanie bezpiecznych i niepowtarzalnych haseł, aktywuj dwuskładnikowe uwierzytelnianie. Używaj menedżera haseł. Tego typu oprogramowanie pozwala tworzyć bardzo długie, losowe hasła do serwisów internetowych. Pamięta je i – w trakcie logowania – wpisuje za Ciebie.

Drukarka to komputer?

Tak. Drukarki, kopiarki i faksy to też komputery. Wniosek? W ich przypadku także musimy dbać o bezpieczeństwo. Jak to zrobić? Po pierwsze – korzystaj z oferowanych przez te urządzenia funkcjonalności w zakresie bezpieczeństwa. Zmień też domyślne hasło i wyłącz możliwość bezpośredniego logowania do urządzeń z zewnętrznych sieci.

Inna kwestia – wybieraj urządzenia, które posiadają możliwości szyfrowania i bezpiecznego usuwania danych. A jeśli chcesz pozbyć się jakiś sprzętów (nie tylko drukarki, ale i komputerów, czy telefonów) – zabezpiecz lub zniszcz przechowywane na nich dane.

Jednym z najważniejszych zasobów firmy są właśnie informacje – finansowe, dane klientów, itp. Ich utrata to wielki problem. Dlatego powinny być szczególnie chronione.

– *Zapewnianie bezpieczeństwa w sieci to stały proces. Pierwszym krokiem jest przede wszystkim podnoszenie świadomości pracowników, by ograniczyć ryzyko utraty wrażliwych danych firmy na skutek prostego błędu ludzkiego* – mówi Krzysztof Silicki z NASK. – *Dlatego w codziennej działalności nie zapominajmy o zagrożeniach dla bezpieczeństwa IT, bo one mogą mieć istotny wpływ na stabilność i wiarygodność przedsiębiorstwa* – podkreśla.

Źródło: Ministerstwo Cyfryzacji