**Czy polskie firmy i instytucje są bezpieczne?**

**Nie ma tygodnia, aby media nie donosiły o przypadkach wycieku danych. Z jednej strony – firmy i instytucje mają zazwyczaj zaufanie do własnych zabezpieczeń. Z drugiej – hackerzy i oszuści wciąż są aktywni, nie tylko wymuszając haracze, ale też narażając ofiary na wysokie kary finansowe, nakładane z kolei przez odpowiednie instytucje.**

Powiedzenie „mądry Polak po szkodzie” doskonale pasuje do tematyki cyberbezpieczeństwa. Firmy i instytucje zazwyczaj wykazują zainteresowanie przeprowadzaniem audytów czy też szkoleniami dla pracowników dopiero wtedy, gdy dojdzie do tzw. incydentu bezpieczeństwa. Mowa tu o włamaniach do systemów informatycznych, ich zainfekowaniu, czy też o uzyskiwaniu nieuprawnionego dostępu do danych pracowników, a często i klientów.

**Haracz albo kara**

Bardzo często wirtualni włamywacze pobierają dane osobowe lub blokują dostępy do systemów firmy z myślą o wymuszeniu od ofiary gigantycznego haraczu. Skoro ten proceder trwa, można sądzić, że wiele przedsiębiorstw takiemu szantażowi ulega.

Dlaczego się na to godzą? Ponieważ alternatywa bywa jeszcze bardziej kosztowna. Gdy haracz nie zostanie zapłacony, dane klientów trafiają na czarny rynek, a to oznacza ujawnienie ich danych osobowych, w tym adresów e-mail, numerów telefonów, a w skrajnych sytuacjach, nawet numerów kart kredytowych. To z kolei oznaczać będzie nie tylko kłopoty dla klientów, ale także bolesne konsekwencje dla okradzionej firmy. Za naruszenie Rozporządzenia o Ochronie Danych Osobowych przewidziane są ogromne kary w wysokości aż do 4% całkowitego rocznego obrotu z poprzedniego roku.

O ile firmy komercyjne mogą obawiać się ataków motywowanych głównie chęcią zysku, o tyle instytucjom grożą ataki również ze względów politycznych. Na przykład wywiad obcego państwa może chcieć w ten sposób zdestabilizować pracę urzędów na szczeblu krajowym lub samorządowym. Dlatego instytucje powinny przykładać do zabezpieczeń nie mniejszą wagę niż przedsiębiorstwa prywatne.

- Problemem jest również to, że wiele firm i instytucji nigdy nie testowało swoich zabezpieczeń. Także tych ludzkich. Dlatego poza zapewnieniem „pana informatyka”, że „u nas jest wszystko OK”, organizacje nie wiedzą tak naprawdę jak i czy wystarczająco są zabezpieczone – mówi Arkadiusz Stawczyk – trener i audytor, który w firmie Empemedia prowadzi szkolenia z cyberbezpieczeństwa.

**Zarząd – najsłabsze ogniwo**

Kiedy firmy i instytucje stają przed możliwością przeszkolenia pracowników w zakresie bezpieczeństwa cyfrowego, często pada stwierdzenia, że to temat dla działów IT. Tyle że osoby dbające o techniczne bezpieczeństwo organizacji mają zazwyczaj wysoką świadomość w tym zakresie. Nie mają jej natomiast pozostali pracownicy, a nawet zarząd.

 - Statystyki bezlitośnie wskazują, że większość udanych ataków to wina człowieka. Jego braku świadomości, pośpiechu lub ignorowania wewnętrznych polityk bezpieczeństwa, a często wszystkiego naraz – wyjaśnia ekspert.

To zaś oznacza, że samo wprowadzenie zabezpieczeń i nawet najlepszy dział IT nie wystarczą, jeśli firma nie będzie prowadziła polityki bezpieczeństwa obejmującej wszystkich pracowników mających do czynienia z danymi osobowymi i dokumentacją elektroniczną.

- Paradoksalnie, najgorzej jest z tymi, którzy ponoszą największą odpowiedzialność. Mowa o kadrze zarządzającej, która bardzo rzadko uczestniczy w szkoleniach z cyberbezpieczeństwa – zauważa trener.

To jednak ma się już niedługo zmienić. W ramach implementacji unijnej dyrektywy dotyczącej cyberbezpieczeństwa „NIS2” już wkrótce wejdzie w życie formalny obowiązek, aby kadra zarządzająca przechodziła odpowiednie szkolenia minimum raz w roku. W ocenie trenera z firmy Empemedia, jest to duża i potrzebna zmiana.

**Bezpieczeństwo w rękach pracowników**

Skoro prezesi i menedżerowie nie palą się do szkoleń w zakresie cyberbezpieczeństwa cyfrowego, to tym bardziej temat muszą wziąć na swoje barki pracownicy. To oni powinni pilnować, by do danych firmy czy instytucji nie uzyskały dostępu nieodpowiednie osoby. Niestety, do tego trzeba mieć odpowiednią wiedzę.

- Pracownicy nie wiedzą jak łatwo jest ich oszukać, wzbudzić zaufanie, podszyć się pod znany im numer telefonu, adres e-mail czy stronę internetową – mówi Arkadiusz Stawczyk. – Dopiero na szkoleniach zderzają się z przykładami ataków na inne firmy lub instytucje. Wtedy oczy mocno się otwierają – dodaje.

Dodatkowo, na brak wiedzy nakłada się ogólny brak zaufania Polaków do przestrzegania zasad i regulaminów, które często są traktowane „pro forma”. A gdy dowiadują się o atakach w innych firmach, zakładają, że „to inni są głupi, skoro dali się oszukać”.

- Cyberprzestępcy nie są idiotami i cały czas korygują swoje scenariusze, aby zwiększać swoją skuteczność. Rozwój sztucznej inteligencji, coraz większa rola dezinformacji a także zwykły pośpiech w codziennych obowiązkach powodują, że nawet osoby z „branży” dają się oszukać – zauważa trener.

Obecnie wciąż popularne są rozmaite warianty scenariuszów „*na wnuczka*”, „*na kod Blik*”, „*na OLX*”, „na super inwestycje”. Ich rozmaite „mutacje” pokazują, że ludzie nadal dają się nabrać nawet na stosunkowo proste do wykrycia metody. Wśród ofiar zdarzają się także osoby dobrze wykształcone, ale niewystarczająco jednak czujne w momencie zagrożenia.

**Praca zdalna – realny problem**

Praca zdalna zyskuje na popularności od wielu lat, a po okresie pandemii jej znaczenie jeszcze radykalnie wzrosło. Obecnie praca w trybie całkowicie zdalnym lub hybrydowym to standard w bardzo wielu firmach. Czy jednak praca na odległość nie wiąże się z większym ryzykiem?

- Najczęściej, tak. Przeważnie ryzyko jest większe, ponieważ zmieniają się zabezpieczenia z „*firmowych”* na „*domowe*”, ale tak być wcale nie musi. Aby uniknąć ryzyka, również w domu trzeba przestrzegać tych samych zasad, np. stosować „politykę czystego biurka i ekranu”, a także nie dopuszczać do służbowych informacji żony, dzieci, czy też kota (tak, tak – kot także może przez przypadek wysłać maila) – mówi ekspert.

Jeśli dodatkowo mamy szyfrowane nośniki w urządzeniach, chronimy fizycznie sprzęt i dane firmowe oraz łączymy się z systemami firmowymi w bezpieczny, zaakceptowany przez dział IT sposób np. korzystając z VPN i dwuskładnikowego uwierzytelnienia, to ryzyko nie będzie większe.

Pytanie tylko, czy naprawdę wszystkich tych zasad przestrzegamy podczas pracy z domu? Praktyka pokazuje, że poza murami firmy pewne zasady traktujemy wybiórczo. Ma być łatwo i szybko, a to już prosta droga do problemów.

**Jak uchronić firmę przed incydentami?**

Na pocieszenie warto dodać, że przed incydentami bezpieczeństwa zazwyczaj można się obronić. Przestępcy rzadko kiedy są tak zdeterminowani, aby włamywać się do systemów, które są wzorcowo strzeżone. Zazwyczaj „idą na łatwiznę” wyszukując popularnych luk w systemach informatycznych lub też licząc na naiwność pracowników. A nuż się uda! Niestety, często ten łut szczęścia im się przytrafia.

- Jeśli firma dba o świadomość pracowników i kadry zarządzającej np. poprzez szkolenia, to większość zagrożeń uda się rozpoznać i zapobiec im, zanim dojdzie do nieszczęścia – twierdzi Arkadiusz Stawczyk.

Poprosiliśmy eksperta, aby wskazał także kilka konkretnych zasad cyberhigieny, których przestrzegać powinni pracownicy biurowi. Oto 5 najważniejszych wskazówek.

1.

Stosuj silne hasła i zarządzaj nimi przy pomocy menedżera haseł (a na pewno nie zapisuj na żółtych karteczkach przyklejanych nad monitorem).

2.

Archiwizuj dane nie tylko w chmurze, ale także na fizycznych nośnikach. Serwer w chmurze również może spłonąć, ktoś lub coś go może wyłączyć albo uszkodzić.

3.

Używaj skutecznych programów antywirusowych (skuteczne, to zazwyczaj te płatne), zarówno w komputerze, jak i w telefonie.

4.

Na bieżąco aktualizuj oprogramowanie w komputerze i telefonie, ponieważ aktualizacje zazwyczaj „łatają” luki bezpieczeństwa.

5.

Weryfikuj każdą otrzymaną informację. Zanim klikniesz w link, otworzysz załącznik, a nawet uwierzysz, że na pewno rozmawiasz przez telefon z właściwą osobą, upewnij się.

Szczególnie istotny jest ten ostatni punkt. Obecnie powinniśmy weryfikować każdą informację, jeśli na jej podstawie mamy podjąć jakąkolwiek decyzję. Każdy e-mail, sms, telefon, strona www, wiadomość na portalu społecznościowym, obrazek, materiał audio itd. musi podlegać sprawdzeniu. Nawet doświadczeni menedżerowie są często zaskoczeni jak łatwo można się podszyć pod prawie każdy numer telefonu. To, że na wyświetlaczu widzimy nazwę banku lub czyjeś nazwisko nie musi oznaczać, że dzwoni do nas właśnie ten nadawca. Podobną ostrożność należy zachować wobec korespondencji e-mail. Zawsze należy sprawdzać adresy nadawców, ale te rzeczywiste a nie ustawione jako „nazwa wyświetlana”.

- To może być nieco uciążliwe, ale warto. Chodzi w końcu o nasze bezpieczeństwo – podsumowuje trener z firmy Empemedia.

Naprawdę skuteczne zabezpieczenie może wydać się banalne – jest nim ciągłe zwiększanie świadomości i wiedzy pracowników różnych szczebli poprzez szkolenia, a do tego przeprowadzanie w firmie regularnych testów i audytów bezpieczeństwa.