**Co 10. pracownik używa tego samego hasła ponad 15 razy**

* **84% firm korzysta z menedżerów haseł, ale mimo to 54% pracowników zapisuje je również w plikach tekstowych na komputerze. Co więcej, prawie 90% używa tego samego hasła wielokrotnie.**
* **Hakerzy atakują nie tylko duże firmy. 58% ataków dotyka firmy zatrudniające mniej niż tysiąc pracowników.**
* **Ostatnią deską ratunku może być cyberpolisa, która zapewnia szerokie wsparcie finansowe dla walki ze skutkami ataków, np. na zatrudnienie dodatkowych specjalistów IT czy odzyskanie utraconych danych.**

Co kilka miesięcy dochodzi do masowego wycieku haseł, więc teoretycznie zdajemy sobie sprawę, jak poważne jest zagrożenie i powinniśmy dbać o ich bezpieczeństwo. Szczególnie jeśli chodzi o dane logowania do systemów firmowych, ponieważ ich złamanie może mieć poważne konsekwencje, np. w postaci ataku ransomware czy wyłudzenia pieniędzy. Jednak w praktyce działamy tylko połowicznie. Według raportu firmy Bitwarden (dostawca oprogramowania do zarządzania hasłami), choć 84% firm korzysta z menedżerów haseł, to nadal 54% pracowników zapisuje je w plikach tekstowych na komputerze. Co więcej, 41% specjalistów IT przekazuje dane logowania mailem, a prawie 90% pracowników wykorzystuje te same hasła wielokrotnie w różnych systemach (co dziesiąty pracownik nawet w ponad 15 serwisach). Te nawyki zdecydowanie zwiększają ryzyko skutecznego cyberataku.

– *Kwestia cyberbezpieczeństwa jest obecnie jednym z kluczowych zmartwień firm. Według analizy ryzyk dla biznesu przygotowanej przez Allianz, już drugi rok z rzędu cyberataki są na pierwszym miejscu. Nawet mimo trwającej recesji, niepewności na rynkach oraz kryzysu energetycznego, które odbijają się mocno na codziennej działalności firm. W tym kontekście bezpieczeństwo haseł jest więc szczególnie istotne, ponieważ ich złamanie prowadzi najczęściej do skutecznego ataku hakerskiego, który zawsze ma konsekwencje finansowe, czasem poważne. Gdy już dojdzie do najgorszego, ostatnią deską ratunku może być ubezpieczenie od zagrożeń cybernetycznych* – mówi Szymon Bąk, ekspert od cyberubezpieczeń, broker ubezpieczeniowy w EIB SA.

**Każda firma powinna zainteresować się cyberpolisą**

Warto zaznaczyć, że hakerzy nie skupiają się jedynie na światowych gigantach. Nie wszyscy cyberprzestępcy dążą do spektakularnych efektów – często wybierają za cel sektor MSP i stawiają na masowe ataki. Przede wszystkim dlatego, że mniejsze podmioty czasem nie dysponują tak rozbudowanymi systemami zabezpieczeń IT, więc są teoretycznie łatwiejszymi celami. Potwierdzają to dane Verizon z raportu 2023 Data Breach Investigations Report – 58% ataków dotyka firmy zatrudniające poniżej 1 tys. pracowników. Dlatego cyberubezpieczeniem powinny interesować się wszystkie firmy, niezależnie od wielkości i skali działalności. Hakerzy nie patrzą na to, czy firma działa lokalnie czy globalnie, ani ilu pracowników zatrudnia. Dla nich liczy się wyłącznie to, czy mogą złamać zabezpieczenia i wyrządzić szkody.

**Jak działa cyberpolisa?**

Zadaniem ubezpieczenia od zagrożeń cybernetycznych jest ochrona firmy przed skutkami finansowymi ataków oraz wsparcie w likwidacji szkód w wyniku ataku. Z polisy można pokryć wiele różnych kosztów związanych z reakcją na atak. Może uwzględniać zatrudnienie ekspertów od bezpieczeństwa IT czy informatyki śledczej, a także dodatkowej osoby odpowiedzialnej za zarządzanie incydentem. W przypadku wycieku danych osobowych polisa pomoże także pokryć koszty akcji informacyjnej wśród poszkodowanych. Z ubezpieczenia można również opłacić prawników oraz specjalistów ds. public relations. W końcu praktycznie każdy atak powoduje kryzys wizerunkowy. Dodatkowo, polisa może pokryć koszty usunięcia złośliwego oprogramowania, odzyskania dostępu do zainfekowanych urządzeń oraz zlikwidowania luk w zabezpieczeniach. W sytuacji, gdy firma poniesie straty finansowe w wyniku ataku, polisa może także zapewnić rekompensatę utraconego zysku.

- *Trzeba jednak zaznaczyć, że wraz z rosnącą skalą ataków, towarzystwa ubezpieczeń ostrożniej podchodzą do udzielania ochrony. Wielu ubezpieczycieli również znacznie ograniczyło swoją ofertę. Powstały jednak nowe propozycje, które zakładają wyższy próg wejścia i stawiają przed firmami dodatkowe wymagania. Przede wszystkim firmy muszą wykazać, że stosują odpowiednie środki bezpieczeństwa. W przypadku danych logowania, ubezpieczyciel może oczekiwać stosowania dwustopniowego procesu uwierzytelniania* – dodaje Szymon Bąk z EIB SA.