**Czy można ubezpieczyć się od wycieku danych osobowych?**

* **Wobec rosnącego zagrożenia atakiem hakerskim, polisy od zdarzeń cybernetycznych stały się jednym z podstawowych elementów ochrony firmy.**
* **Polisa jest najczęściej ostatnią deską ratunku, która pozwala zminimalizować straty finansowe wynikające z ataku.**
* **W zakresie cyberpolis znajduje się również refundacja kosztów wynikających z RODO – przeprowadzenie akcji informacyjnej, wypłata odszkodowań czy zapłata kar administracyjnych.**

Wyciek danych, czy to firmowych czy osobowych klientów, zawsze jest dużym problemem dla firmy i wiąże się z poważnymi konsekwencjami. Jednak część skutków wycieku danych można zabezpieczyć ubezpieczeniem.

– *Coraz więcej przedsiębiorców zdaje sobie sprawę, że to nie kwestia „czy”, ale „kiedy” będę celem ataku. Dlatego rośnie popularność ubezpieczeń od zdarzeń cybernetycznych. Nie wolno jednak zapominać o modernizacji zabezpieczeń. Oba elementy, polisa i zabezpieczenia, są ze sobą ściśle związane. Wobec coraz większego zagrożenia możemy spodziewać się, że w procesie oceny ryzyka zyskają na znaczeniu wymagania techniczne i organizacyjne, które winny być spełnione przez wnioskujących o ubezpieczenie. Przykładowo, coraz częściej mówi się o posiadaniu systemu do analizy i wykrywania zagrożeń na urządzeniach końcowych, tzw. Endpoint Detection and Response, w skrócie EDR. Eksperci od oceny ryzyka zwracają też uwagę, czy firma prowadzi szkolenia dla pracowników z cyberbezpieczeństwa, wypracowała procedury reakcji, stosuje stopniowanie dostępu itd.* – zauważa Szymon Bąk, ekspert od cyberubezpieczeń, broker ubezpieczeniowy w EIB SA.

**Jak działają cyberpolisy?**

Zadaniem ubezpieczenia od zagrożeń cybernetycznych jest ochrona firmy przed skutkami skutecznego ataku, szczególnie finansowymi. Firmy mogą liczyć na wsparcie ubezpieczyciela m.in. w minimalizacji rozmiaru szkód oraz „obsłudze” formalno-prawnej incydentu. Z polisy można na przykład opłacić koszty związane z:

* zatrudnieniem dodatkowych, zewnętrznych ekspertów (specjalistów od bezpieczeństwa IT, osobę zarządzającą reakcją na zdarzenie, a także prawników i specjalistów public relations),
* usunięciem złośliwego oprogramowania,
* odzyskaniem dostępu do zainfekowanych urządzeń czy usunięciem luki w ochronie.

Polisa może też zapewnić rekompensatę strat finansowych, wynikających z ataku.

– *Ubezpieczenie zakłada także pokrycie kosztów działań wymaganych przez RODO w razie wycieku, czyli przeprowadzenia akcji informacyjnej wśród potencjalnych ofiar wycieku. Ponadto zapewnia zwrot kosztów związanych z postępowaniami administracyjnymi i sądowymi oraz wypłatę odszkodowań. Na ogół cyberpolisa może uwzględniać też zapłacenie kar nałożonych w myśl RODO* – mówi Szymon Bąk z EIB SA.

**Jak się bronić przed hakerami?**

Bezpieczeństwo IT jest obecnie tak samo ważne, jak np. BHP. Do żelaznych zasad, których należy przestrzegać, można zaliczyć:

* połączenia wyłącznie za pośrednictwem sprawdzonych i zabezpieczonych sieci,
* wykorzystanie maszyn wirtualnych, gdy nie ma możliwości skorzystania ze zweryfikowanego połączenia,
* sprawdzanie nadawców (adresów e-mail) wiadomości, które wydają się podejrzane,
* wielostopniowe logowanie do aplikacji i systemów firmowych,
* regularne testy szczelności zabezpieczeń.

– *Jak pokazuje jednak praktyka, jest jeden czynnik, nad którym żadna firma, żaden ekspert od cyberzagrożeń, nie ma kontroli – użytkownicy. O skuteczności większości ataków hakerskich decyduje właśnie nasza nieuwaga lub zlekceważenie procedur bezpieczeństwa. W przypadku phishingu są one podstawą sukcesu hakerów. A błąd może zdarzyć się każdemu z nas. Ostatnią deską ratunku jest najczęściej cyberubezpieczenie. Dlatego nie wolno go pomijać w programie ochrony ubezpieczeniowej firmy* – dodaje Szymon Bąk z EIB SA.

Źródło: EIB SA.