

COMPLIANCE INSIGHTS

Vol.

102

Jeden klik może
kosztować miliony.
Jak zabezpieczyć
firmę przed
cyberatakami?



1. Częsty początek problemu: człowiek, mail i presja czasu

Atak rzadko wygląda jak filmowy „włam”. Często zaczyna się od fałszywej faktury, podmienionego numeru rachunku, linku do logowania albo telefonu od „kontrahenta”.

Co powinno wzbudzić czujność?

- zmiana numeru konta;
- prośba o pilny przelew;
- link do logowania;
- załącznik z makrem;
- literówki w adresie e-mail i treści wiadomości.



2. Często celem są MŚP. Dlaczego?

Najłatwiej atakować tam, gdzie nie ma rozbudowanego działu IT. Ryzyko rośnie też wtedy, gdy firma mocno opiera się na poczcie elektronicznej i danych w chmurze, podejmuje szybkie decyzje finansowe, nie ma rozwiniętego controllingu ani nawyku zgłaszania podejrzanych działań oraz nie ma zorganizowanych struktur odpowiedzialnych za bezpieczeństwo informacji.



3a. Minimalna ochrona:

7 obszarów, które powinny działać jednocześnie

ODPOWIEDZIALNOŚĆ. Zarząd lub właściciel powinien wskazać osobę odpowiedzialną za bezpieczeństwo informacji.

PROCEDURY. Reguły zrozumiałe dla pracowników, uwzględniające politykę haseł, zasady korzystania z nośników danych, umieszczania danych w chmurze, zabezpieczenia danych klientów, pracowników i kontrahentów.

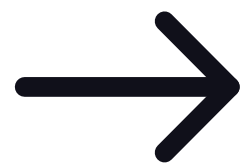


3b. Minimalna ochrona:

7 obszarów, które powinny działać jednocześnie

SZKOLENIA. Wiedza, która przekłada się na świadomość zagrożenia wśród pracowników. Ćwiczenia na przykładach: phishing, fałszywe faktury, presja czasu.

MFA i DOSTĘPY. Wdrożenie obowiązkowego uwierzytelnienia wieloskładnikowego (MFA), menedżera haseł, oddzielnych kont administracyjnych czy też wdrożenie zasady minimalizacji dostępu.



3c. Minimalna ochrona:

7 obszarów, które powinny działać jednocześnie

AKTUALIZACJE systemów, aplikacji, wtyczek i urządzeń powinny być automatyczne.

KOPIE ZAPASOWE muszą być wykonywane regularnie, odseparowane, szyfrowane i testowane odtworzeniowo.

PROCEDURA REAKCJI powinna zadziałać w przypadku incydentu. Procedura powinna zawierać listę osób decyzyjnych ze wskazaniem zakresu kompetencji oraz listę działań priorytetowych.



4. Dostawcy też są częścią bezpieczeństwa Twojej firmy

Hosting, księgowość, CRM, płatności, marketing automation, to punkty, przez które może dojść do naruszenia. Dlatego:

- w umowie opisz obowiązek niezwłocznego poinformowania o incydencie;
- wymagaj: MFA, szyfrowania, backupu, aktualizacji, logów i rozdziału uprawnień;
- sprawdź, gdzie i przez kogo są przetwarzane dane;
- ustal kontakt awaryjny, czas reakcji i sposób przekazywania informacji o incydencie;
- nie dawaj dostawcy dostępu szerszego niż konieczny.



5. Gdy dojdzie do ataku, działaj natychmiast

Odłącz zainfekowany sprzęt od sieci, zablokuj przejęte konta, wstrzymaj podejrzone płatności. Nie kasuj logów i wiadomości. Zapisz czas, zakres naruszenia, osoby, zainfekowane systemy, zrzuty ekranu i podejrzone wiadomości. Zdiagnozuj, czy doszło do naruszenia ochrony danych osobowych i jakie mogą być jego skutki dla osób. Jeśli ryzyko jest bardzo prawdopodobne, zgłoszenie do UODO powinno nastąpić w 72 h od wykrycia.



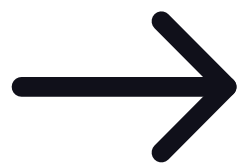
6a. **Działania po wycieku danych**

Zgłoś naruszenie do UODO, jeśli wyciek może powodować ryzyko naruszenia praw i wolności osób. Jeżeli istnieje wysokie ryzyko niekorzystnych skutków, poinformuj osoby bez zbędnej zwłoki prostym językiem. Zgłoś cyberincydent do CERT/CSIRT, przekaz dostępne informacje i uzupełniaj je w toku obsługi. Archiwizuj dokumentację, opisz przebieg i skutki, kryteria oceny ryzyka i przygotuj działania naprawcze.



6b. Działania po wycieku danych

- Zadbaj o komunikację.
- Przygotuj komunikat, co się stało, jakie dane wyciekły, jakie działania zostały podjęte i co powinien zrobić Twój klient lub kontrahent.
- Dopracuj procedury.
- Zweryfikuj, czy udzielone dostępy są zgodne z zasadą minimalizacji.
- Zadbaj o wiedzę pracowników i zorganizuj dodatkowe szkolenia z cyberbezpieczeństwa.
- Przetestuj backupy.
- Zweryfikuj umowy z dostawcami pod kątem bezpieczeństwa danych.



Compliance Insight



Mariusz Purgał

Partner

mariusz.purgal@kwkr.pl
+48 797 927 960



Joanna Bochaczyk

Associate

joanna.bochaczyk@kwkr.pl
+48 511 922 988

Zapraszamy do kontaktu
