Wyciąg z mapy ryzyk dostępowych

Kto ma dostęp do Twoich systemów.

2	3	1
byłych współpracowników *zachowały aktywny dostęp do systemów firmy*	**podmioty zewnętrzne** *bez umowy powierzenia przetwarzania danych (DPA)*	**podmiot zewnętrzny** *z uprawnieniami administratora zamiast użytkownika*

Co to oznacza w praktyce:

→ Osoba po zakończeniu współpracy przez 47 dni miała dostęp do CRM, poczty firmowej, ofert, cenników, umów z możliwością ich kopiowania i pobrania;

→ Agencja zewnętrzna zarządza stroną i kampaniami reklamowymi bez podpisanej umowy powierzenia przetwarzania danych, brak kontroli dostępów do kont w SM (i brak 2FA) może prowadzić do ataków;

→ Trzy podmioty mają dostęp do danych klientów bez prawidłowo zawartej umowy powierzenia przetwarzania danych, co świadczy o braku kontroli nad przepływem danych.

Każda z powyższych sytuacji oznacza aktywne ryzyko naruszenia zasad bezpieczeństwa i rozliczalności RODO - niezależnie od tego, czy doszło do potwierdzonego wycieku danych.

Audyt obejmuje identyfikację krytycznych ryzyk dostępowych. Pełna techniczna inwentaryzacja wszystkich kont, ról i uprawnień może zostać wykonana jako osobny etap.

Wyciąg dodatkowy: optymalizacja kosztów IT

Audyt pokazuje,
za które systemy płacisz bez realnego wykorzystania.

49%	do 30%	58%
oprogramowania i aplikacji SaaS *pozostaje nieużywane przez pracowników* Nexthink, analiza ponad 6 mln urządzeń, 2023	**kosztów licencji można ograniczyć** *dzięki optymalizacji licencji i narzędzi* Gartner, Software Asset Management	**badanych firm przynajmniej raz** *kupiło oprogramowanie, które nie spełniło oczekiwań* CRN za Capterra, 2024

System	Co wykryto	Koszt / mies.	Rekomendacja
Microsoft 365 Business Premium	6 licencji nieużywanych od 90 dni	**ok. 596 zł**	**Redukcja planu**
System CRM	8 z 12 kont loguje się rzadziej niż raz w tygodniu	**ok. 1184 zł**	**Weryfikacja kont**
Platforma e-podpisu	Plan Enterprise. Użycie: 3 dokumenty w 6 miesięcy.	**ok. 245 zł**	**Zakup jednorazowy**
Narzędzie do zarządzania projektami	Dwa identyczne narzędzia opłacane równolegle przez różne działy	**ok. 794 zł**	**Konsolidacja**
Subskrypcja antywirusowa	EDR wdrożony 8 m-cy temu - stary antywirus wciąż aktywny i opłacany	**ok. 354 zł**	**Wyłączyć natychmiast**

Możliwe oszczędności z powyższych 5 pozycji (przykładowa organizacja):

3 173 zł miesięcznie · 38 076 zł rocznie

Wyciąg z analizy odpowiedzialności zarządu

NIS2 zwiększa osobistą odpowiedzialność zarządu.

Nie chodzi już tylko o karę dla spółki.

W określonych przypadkach brak nadzoru nad cyberbezpieczeństwem może prowadzić nie tylko do sankcji dla organizacji, ale również do osobistych konsekwencji dla osób zarządzających.

Kara RODO	+	Kara NIS2	Odpowiedzialność osobista zarządu
na organizację		na organizację	w określonych przypadkach
do 20 000 000 €		**do 10 000 000 €**	**do 300%**
lub 4% rocznego światowego obrotu		lub 2% obrotu (podmioty kluczowe)	wynagrodzenia
			w określonych przypadkach NIS2/UKSC

W jednym zdarzeniu mogą nakładać się różne reżimy odpowiedzialności: RODO, NIS2/UKSC oraz odpowiedzialność osób zarządzających - zależnie od statusu organizacji, charakteru naruszenia i ustaleń organu.
Standardowe OC spółki nie musi obejmować osobistych konsekwencji osób zarządzających; zakres ochrony zależy od warunków konkretnej polisy, w szczególności D&O/cyber.

Co zwiększa ryzyko	Co wspiera należytą staranność
✗ Brak procedury obsługi incydentów i terminów zgłoszeń	✓ Zatwierdzona procedura z terminami zgłoszeń do właściwych organów
✗ Brak niezależnego nadzoru zarządu nad IT	✓ Niezależny audyt zewnętrzny jako dowód aktywnego nadzoru
✗ Nieodebrane dostępy osób po zakończeniu współpracy	✓ Stosowana procedura offboardingu IT z dokumentacją
✗ Brak umów powierzenia przetwarzania danych (DPA)	✓ Podpisane DPA z każdym podmiotem przetwarzającym dane

Zlecenie niezależnego audytu, udokumentowanie wyników i realna realizacja planu naprawczego mogą stanowić istotny dowód należytej staranności zarządu.

Wyciąg z raportu zarządczego

Twój dział IT chroni systemy.

Ale kto kontroluje dział IT?

Poniższe pytania padają na każdym audycie. Zarząd zazwyczaj nie zna odpowiedzi.

Pytanie audytowe	Odpowiedź	Ryzyko
Kiedy ostatnio dostałeś niezależny raport o bezpieczeństwie IT — nie od własnego działu?	NIGDY	Krytyczne
Czy wiesz, kto ma dziś dostęp do bazy klientów — i czy każda z tych osób powinna?	NIE	Krytyczne
Czy Twoja agencja marketingowa ma podpisaną umowę powierzenia przetwarzania danych?	NIE WIEM	Krytyczne
Co się stanie w Twojej firmie w pierwszych 24h po ataku ransomware?	NIE WIEM	Wysokie
Czy zarząd formalnie zatwierdził ryzyka w rejestrze ryzyk cyberbezpieczeństwa?	NIE	Wysokie
Czy zakup ostatniego systemu IT był niezależnie zweryfikowany przed podpisaniem umowy?	NIE	Wysokie

NIS2 przenosi cyberbezpieczeństwo na poziom nadzoru zarządczego. Dział IT może realizować zadania techniczne, ale zarząd powinien rozumieć ryzyka, zatwierdzać kluczowe decyzje i sprawdzić faktyczny nadzór nad firmą oraz odpowiedzialność zarządu.

Wyciąg z analizy ryzyka regulacyjnego

Kary nakładane przez UODO.

Za sytuacje podobne do tych wykrytych w audycie.

2 178 894 zł

łączna wartość kar w przywołanych sprawach
żadna nie wymagała włamania ani wycieku danych

Kara	Za co	Sytuacja podobna w audycie
1 440 549 zł	Nieprawidłowa analiza ryzyka i niewdrożenie adekwatnych środków technicznych oraz organizacyjnych po wycieku danych	*Dostęp zewnętrzny do systemów z danymi klientów bez adekwatnych środków uwierzytelniania*
350 000 zł	Niewdrożenie odpowiednich środków bezpieczeństwa oraz braki w nadzorze nad podmiotem, któremu powierzono przetwarzanie danych	*Podmioty mają dostęp do danych klientów bez prawidłowo zawartej umowy powierzenia przetwarzania danych*
238 345 zł	Zgubienie nośnika z danymi osobowymi oraz brak adekwatnej analizy ryzyka i zabezpieczeń nośników	*Urządzenia przenośne bez szyfrowania nośników i adekwatnej analizy ryzyka*
100 000 zł	Brak weryfikacji i nadzoru nad poziomem uprawnień podmiotu przetwarzającego	*Podmiot zewnętrzny z uprawnieniami wykraczającymi poza niezbędne minimum*
40 000 zł	Brak udokumentowanej analizy ryzyka bezpieczeństwa i odpowiednich środków organizacyjnych	*Brak udokumentowanej i zatwierdzonej analizy ryzyka bezpieczeństwa informacji*
10 000 zł	Opóźnione lub niepełne zgłoszenie naruszenia do właściwych organów	*Brak procedury obsługi naruszeń z terminami zgłoszeń do właściwych organów*

Źródła: decyzje Prezesa UODO i publiczne komunikaty UODO. Każda ze spraw miała indywidualny stan faktyczny. Kwoty i opisy należy każdorazowo weryfikować z konkretną decyzją lub komunikatem UODO. Materiał ma charakter porównawczy, a nie predykcyjny. Szczegółowe odniesienia wskazywane są w pełnej wersji raportu.

Podsumowanie zakresu

Co otrzymuje zarząd po audycie.

Konkretne dokumenty. Konkretne decyzje.

Materiał ma charakter przykładowy. Zakres ustaleń zależy od wielkości organizacji, liczby systemów i uzgodnionego zakresu audytu.

01 — Raport zarządczy
Kluczowe ryzyka, priorytety i decyzje wymagane po stronie zarządu — w języku zarządczym, nie technicznym.

02 — Mapa ryzyk dostępowych
Krytyczne obszary dostępu: osoby po zakończeniu współpracy, podmioty zewnętrzne, konta administracyjne.

03 — Analiza odpowiedzialności zarządu
Co zwiększa ryzyko, a co wspiera wykazanie należytej staranności — według obszarów odpowiedzialności zarządczej.

04 — Plan naprawczy 30/60/90 dni
Lista działań z właścicielami, terminami i priorytetami. Zaprojektowany tak, by zarząd mógł monitorować realizację.

05 — Pakiet checklist operacyjnych
Offboarding IT, nadawanie dostępów, weryfikacja dostawców, obsługa incydentów — gotowe do wdrożenia od razu.

06 — Konsultacja wdrożeniowa
2 godziny konsultacji wdrożeniowej po przekazaniu raportu. Omówienie wyników, priorytetów i pierwszych decyzji zarządu. Opcjonalnie: prezentacja dla rady nadzorczej lub inwestorów.

Natalia Sołtowska
Adwokat · Audytor wiodący ISO 27001
RODO · NIS2 · DORA · Prawo IT

Marek Kliś
Radca prawny · Audytor wiodący ISO 27001
Cyberbezpieczeństwo · Infrastruktura IT · NIS2

Chcesz sprawdzić, czy podobne ryzyka występują w Twojej firmie?
Umów 30-minutową bezpłatną rozmowę diagnostyczną.
kontakt@legalcheckit.pl · +48 666 059 548 · +48 504 673 566