

Zagrożenia wewnętrzne (insider threat)

Jak je rozpoznać i ocenić ryzyko

Autor: Securivy sp. z o.o. — członek klastra Cyber Made in Poland



Spis treści

Streszczenie	3
1. Czym jest zagrożenie wewnętrzne	3
2. Dlaczego zagrożenia wewnętrzne są trudne do wykrycia	4
3. Ocena ryzyka zagrożeń wewnętrznych	5
4. Mechanizmy wykrywania	6
5. Model reagowania	7
6. Umocowanie normatywne i kwestia proporcjonalności	8
7. Dobre praktyki – lista kontrolna	8
8. Podsumowanie	9

Spis rysunków

Rysunek 1. Typologia zagrożeń wewnętrznych	4
Rysunek 2. Macierz oceny ryzyka zagrożeń wewnętrznych	5
Rysunek 3. Cykl wykrywania i reagowania na zagrożenia wewnętrzne	7

Streszczenie

Znaczna część incydentów bezpieczeństwa nie pochodzi z zewnątrz, lecz od osób, które mają legalny dostęp do systemów organizacji — pracowników, współpracowników, dostawców czy podwykonawców. Zagrożenia wewnętrzne (*ang. insider threat*) są trudniejsze do wykrycia niż ataki zewnętrzne, ponieważ działanie sprawcy mieści się formalnie w granicach nadanych mu uprawnień i nie generuje typowych sygnałów, na które reagują zabezpieczenia obwodowe.

Ten poradnik porządkuje typologię zagrożeń wewnętrznych, wyjaśnia, dlaczego są tak trudne do wykrycia oraz przedstawia praktyczne podejście do oceny ryzyka i budowy zdolności wykrywania. Omawiamy rolę monitorowania aktywności użytkowników (*ang. User Activity Monitoring - UAM*), analizy behawioralnej (*ang. User and Entity Behavior Analytics - UEBA*) oraz rejestrowania sesji jako mechanizmów wykrywania i reagowania.

1. Czym jest zagrożenie wewnętrzne

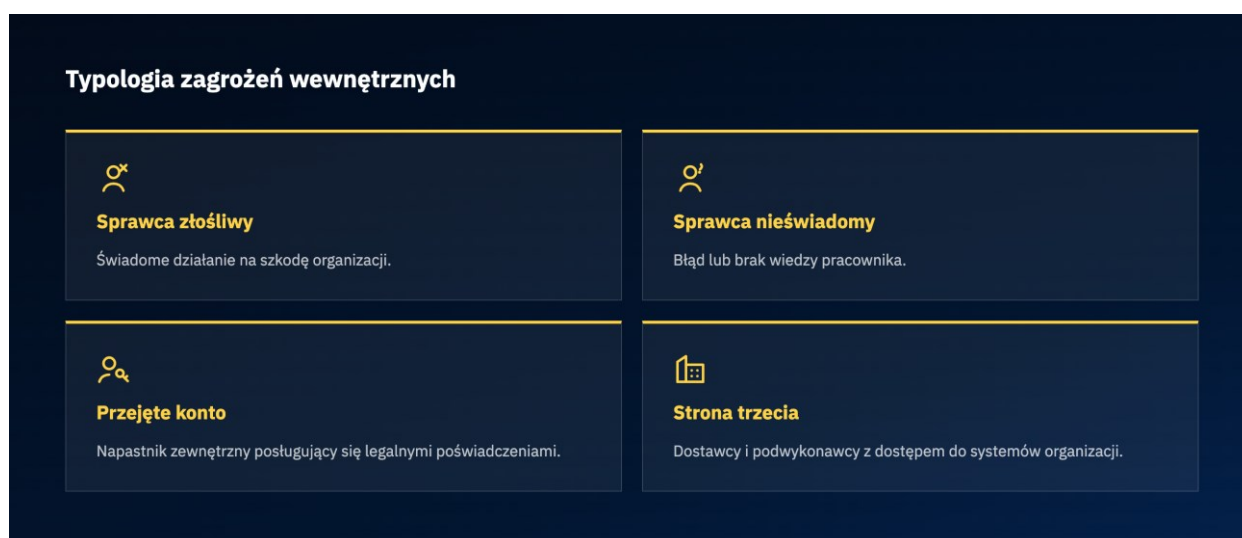
Zagrożenie wewnętrzne to ryzyko wynikające z działań osoby dysponującej autoryzowanym dostępem do zasobów organizacji. Nie jest to jedna kategoria, lecz co najmniej cztery różne profile, wymagające odmiennego podejścia.

Sprawca złośliwy. Osoba świadomie działająca na szkodę organizacji — z pobudek finansowych, z chęci zemsty lub w wyniku werbunku przez podmiot zewnętrzny. Typowe działania to kradzież danych, sabotaż lub nadużycie uprawnień.

Sprawca nieświadomy. Najczęstszy przypadek. Pracownik, który przez nieuwagę lub brak wiedzy doprowadza do incydentu — otwiera złośliwy załącznik, wynosi dane na nieszyfrowanym nośniku, konfiguruje usługę w sposób odsłaniający dane. Intencji szkodliwej nie ma, skutek bywa równie dotkliwy.

Przejęte konto. Napastnik zewnętrzny, który pozyskał poświadczenia legalnego użytkownika, z perspektywy systemów działa jak insider. To granica między zagrożeniem zewnętrznym a wewnętrznym — i jeden z powodów, dla których monitorowanie zachowań użytkowników ma sens niezależnie od źródła ataku.

Strona trzecia. Dostawcy, podwykonawcy, serwisanci i partnerzy z dostępem do systemów. Ich aktywność często wymyka się standardowym mechanizmom nadzoru, a odpowiedzialność za nią bywa rozmyta.



Rysunek 1. Typologia zagrożeń wewnętrznych

Opis alternatywny (WCAG 2): Cztery pola przedstawiające profile sprawców zagrożeń wewnętrznych: sprawca złośliwy (świadome działanie na szkodę), sprawca nieświadomy (błąd lub brak wiedzy), przejęte konto (napastnik zewnętrzny z legalnymi poświadczeniami) oraz strona trzecia (dostawcy i podwykonawcy z dostępem do systemów).

2. Dlaczego zagrożenia wewnętrzne są trudne do wykrycia

Klasyczne zabezpieczenia — zapory sieciowe, systemy antywirusowe, ochrona obwodowa — są projektowane pod kątem odróżniania ruchu i działań „obcych” od „swoich”. Insider z definicji jest „swoj”.

Działanie w granicach uprawnień. Sprawca korzysta z dostępu, który został mu nadany. Pojedyncza czynność — otwarcie pliku, skopiowanie danych, zalogowanie do systemu — sama w sobie nie jest anomalią. Sygnałem staje się dopiero kontekst: pora, skala, sekwencja, odstępstwo od zwykłego wzorca.

Brak sygnatur. W przeciwieństwie do znanego złośliwego oprogramowania, nadużycie wewnętrzne nie ma „sygnatury”. Nie da się go wykryć porównaniem z bazą znanych zagrożeń — trzeba analizować zachowanie.

Dłuższy horyzont czasowy. Działania insiderów, zwłaszcza złośliwych, bywają rozłożone w czasie i maskowane rutynową aktywnością. Wykrycie wymaga korelacji zdarzeń, a nie reakcji na pojedynczy alarm.

Czynnik zaufania. Organizacje z zasady ufają własnym pracownikom, co jest właściwe kulturowo, ale utrudnia obiektywną ocenę ryzyka. Celem nie jest zastąpienie zaufania podejrzliwością, lecz uzupełnienie go o rozliczalność.

3. Ocena ryzyka zagrożeń wewnętrznych

Zanim organizacja zacznie wykrywać, powinna zrozumieć, gdzie jej ryzyko jest największe. Ocena ryzyka insider threat opiera się na skrzyżowaniu dwóch wymiarów: **poziomu dostępu** danej roli oraz **wrażliwości zasobów**, do których ten dostęp prowadzi.

Czynniki podwyższające ryzyko:

- dostęp uprzywilejowany (konta administracyjne, techniczne, serwisowe);
- dostęp do danych wrażliwych (dane osobowe, tajemnica przedsiębiorstwa, dane finansowe);
- role z szerokim, niedostatecznie kontrolowanym zakresem uprawnień;
- dostęp stron trzecich i kont zdalnych;
- okresy podwyższonego ryzyka (np. proces rozstania z pracownikiem, restrukturyzacja).

Praktycznym narzędziem jest macierz, w której role klasyfikuje się według poziomu dostępu i wrażliwości danych, a następnie priorytetyzuje objęcie nadzorem te, które trafiają w obszar wysokiego ryzyka. Nie chodzi o monitorowanie wszystkich w jednakowym stopniu, lecz o proporcjonalność środków do ryzyka.



Rysunek 2. Macierz oceny ryzyka zagrożeń wewnętrznych

Opis alternatywny (WCAG 2): Macierz o dwóch osiach. Oś pozioma: poziom dostępu, od standardowego do uprzywilejowanego. Oś pionowa: wrażliwość danych, od niskiej do wysokiej. Cztery ćwiartki z przypisanym priorytetem nadzoru; najwyższy priorytet w ćwiartce łączącej dostęp uprzywilejowany z danymi o wysokiej wrażliwości.

4. Mechanizmy wykrywania

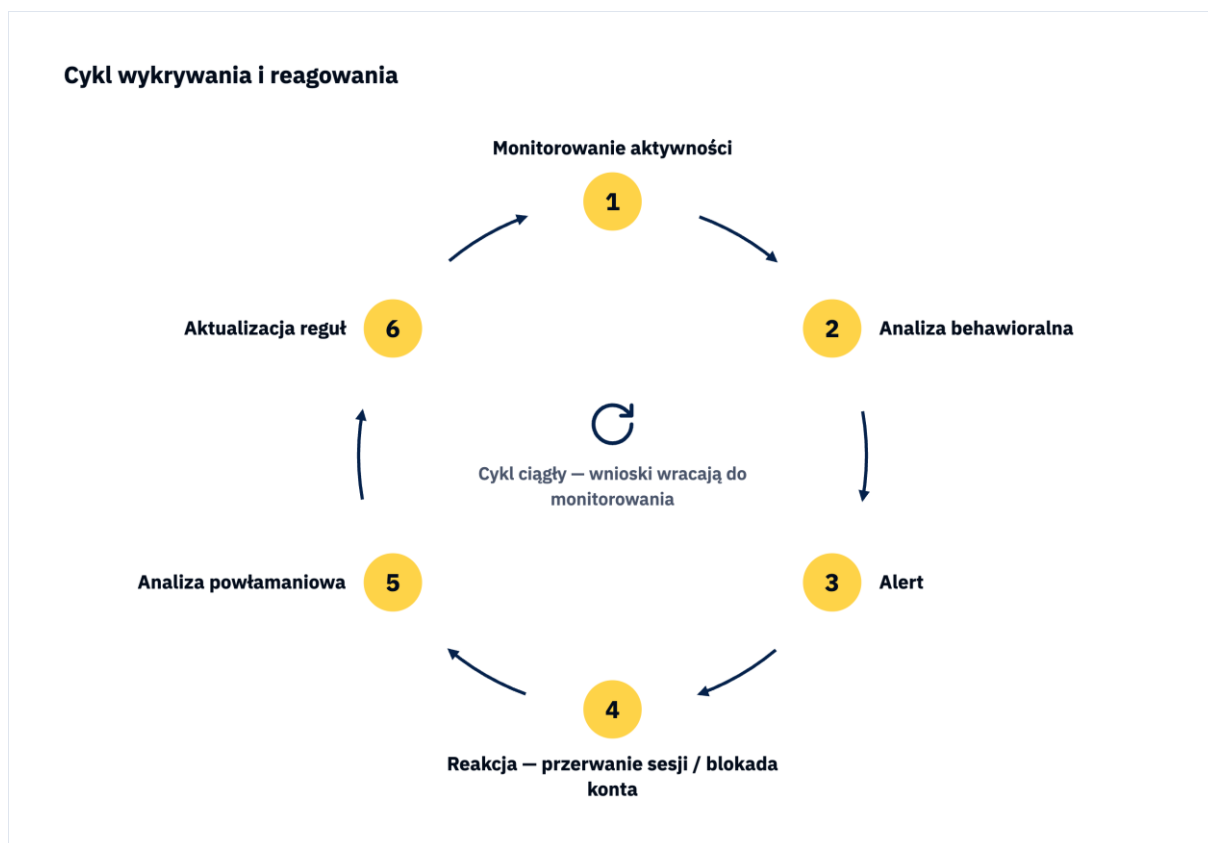
Wykrywanie zagrożeń wewnętrznych opiera się na obserwacji zachowań i kontekstu, a nie na sygnaturach. Trzy uzupełniające się warstwy:

Monitorowanie aktywności użytkowników (UAM). Rejestrowanie tego, co dzieje się w sesjach użytkowników – uruchamianie aplikacji, dostęp do plików i systemów, wykonywane operacje. W przypadku dostępu uprzywilejowanego i zdalnego szczególną wartość ma rejestrowanie sesji (nagranie ekranu wraz z metadanymi), które daje jednoznaczny materiał do analizy powłamaniowej.

Analiza behawioralna (UEBA). Budowanie profilu normalnego zachowania użytkownika i wykrywanie odstępstw – logowań o nietypowej porze, dostępu do zasobów spoza zwykłego zakresu, nagłego wzrostu wolumenu operacji. To warstwa, która pozwala dostrzec sygnał tam, gdzie pojedyncza czynność nie budzi podejrzeń.

Reguły i alerty w czasie rzeczywistym. Zdefiniowane wcześniej scenariusze wysokiego ryzyka (np. próba dostępu do określonych zasobów, użycie zabronionego narzędzia, podłączenie nośnika USB) mogą wyzwać alert lub automatyczną reakcję.

Dojrzałe platformy z tego obszaru łączą wszystkie trzy warstwy – monitorowanie aktywności, rejestrowanie sesji, analizę behawioralną oraz zarządzanie dostępem uprzywilejowanym. Umożliwiają nagrywanie sesji użytkowników i kont uprzywilejowanych, definiowanie reguł alertowania oraz reagowanie na zdarzenia, wspierając zarówno wykrywanie, jak i dokumentowanie incydentów. Dobór rozwiązania powinien uwzględniać zakres monitorowanych systemów, model przechowywania nagrań, zgodność z wymaganiami ochrony danych oraz możliwości integracji z posiadaną infrastrukturą bezpieczeństwa.



Rysunek 3. Cykl wykrywania i reagowania na zagrożenia wewnętrzne

Opis alternatywny (WCAG 2): Zamknięty cykl sześciu etapów: monitorowanie aktywności użytkowników, analiza behawioralna, wygenerowanie alertu, reakcja (przerwanie sesji lub blokada konta), analiza powtórzeniowa, aktualizacja reguł wykrywania. Cykl wraca do etapu monitorowania.

5. Model reagowania

Wykrycie bez zdolności reagowania ma ograniczoną wartość. Skuteczny model reagowania na zagrożenia wewnętrzne obejmuje:

Reakcję natychmiastową. Możliwość przerwania sesji, zablokowania konta lub ograniczenia dostępu w momencie wykrycia działania wysokiego ryzyka. Czas reakcji często decyduje o skali skutków.

Materiał dowodowy. Rejestracja sesji i dzienniki zdarzeń stanowią materiał do wyjaśnienia incydentu – zarówno wewnętrznego, jak i, w razie potrzeby, na potrzeby postępowań. Rozliczalność wymaga jednoznacznego przypisania działań do osób.

Proces, nie tylko technologia. Reagowanie musi być osadzone w procedurach organizacji: kto podejmuje decyzję, jak eskaluje się zdarzenie, jak angażowany jest dział prawny i HR w przypadku sprawcy wewnętrznego. Technologia dostarcza sygnał i dowód; decyzję podejmują ludzie.

6. Umocowanie normatywne i kwestia proporcjonalności

Monitorowanie aktywności użytkowników znajduje umocowanie w wymaganiach dotyczących rozliczalności i kontroli dostępu, między innymi w normie **PN-EN ISO/IEC 27001** oraz w obowiązkach zarządzania ryzykiem wynikających z dyrektywy **NIS2** i krajowego systemu cyberbezpieczeństwa.

Jednocześnie nadzór nad pracownikami podlega ograniczeniom wynikającym z **przepisów o ochronie danych osobowych (RODO)** oraz **prawa pracy**. Wdrożenie monitorowania wymaga:

- określenia i udokumentowania celu oraz podstawy prawnej przetwarzania;
- zachowania zasady proporcjonalności – zakres nadzoru adekwatny do ryzyka, nie szerszy;
- poinformowania pracowników o stosowanym monitorowaniu;
- ograniczenia dostępu do zebranych danych i ich retencji.

Ten poradnik nie stanowi porady prawnej. Konkretny model monitorowania należy skonsultować z osobą odpowiedzialną za ochronę danych i zgodność w organizacji.

7. Dobre praktyki – lista kontrolna

- Ryzyko zagrożeń wewnętrznych jest oceniane i priorytetyzowane według poziomu dostępu i wrażliwości danych.
- Nadzór jest proporcjonalny do ryzyka, a nie jednakowy dla wszystkich.
- Dostęp uprzywilejowany i zdalny objęty jest rejestrowaniem sesji.
- Analiza behawioralna uzupełnia reguły statyczne o wykrywanie odstępstw od wzorca.
- Zdefiniowane są scenariusze wysokiego ryzyka i reakcje na nie.
- Istnieje zdolność natychmiastowej reakcji (przerwanie sesji, blokada konta).
- Zebrane dane są chronione, a ich zakres i retencja – udokumentowane.
- Pracownicy są poinformowani o monitorowaniu; model jest zgodny z RODO i prawem pracy.
- Dostęp stron trzecich jest objęty odrębnym, wzmocnionym nadzorem.

8. Podsumowanie

Zagrożenia wewnętrzne wymykają się klasycznym zabezpieczeniom, ponieważ ich źródłem jest osoba działająca w granicach nadanego dostępu. Skuteczna obrona nie polega na nieufności wobec pracowników, lecz na rozliczalności: zrozumieniu, gdzie ryzyko jest największe, obserwacji zachowań tam, gdzie ma to uzasadnienie i zdolności do szybkiej, udokumentowanej reakcji.

Fundamentem są trzy uzupełniające się warstwy – monitorowanie aktywności, analiza behawioralna i rejestrowanie sesji – osadzone w procesie reagowania i w zgodzie z wymaganiami ochrony danych. Tak zbudowana zdolność chroni organizację nie tylko przed świadomym nadużyciem, ale również przed skutkami błędów i przejęcia poświadczeń.