EKRAN SECURIVY

Zagrożenia wewnętrzne Statystyki na rok 2021

Fakty i liczby

Insiderzy są jednym z kluczowych zagrożeń dla cyberbezpieczeństwa organizacji. Zagrożenia wewnętrzne stale się zmieniają i rozwijają, stają się coraz bardziej powszechne, trudniejsze do wykrycia, istotniej szkodliwe i w konsekwencji znacząco bardziej kosztowne. Statystyki oraz raporty dotyczące tego zjawiska pomagają wykrywać te tendencje i ulepszać zabezpieczenia firm, w celu zwalczania ataków wewnętrznych.

Podsumowaliśmy kluczowe wnioski wyciągnięte na podstawie statystyk z 2020 roku i przeanalizowaliśmy w jaki sposób dane te, mogą pomóc w zrozumieniu zagrożeń wewnętrznych oraz dostosowaniu odpowiednich środków cyberbezpieczeństwa.

Badania statystyk zagrożeń wewnętrznych

Istnieją dziesiątki badań i ankiet zawierających szereg informacji oraz statystyk dotyczących zagrożeń wewnętrznych. Biorąc pod uwagę ten szeroki zakres, przeanalizowanie wszystkich dokumentów jest prawie niemożliwe, dlatego w tym artykule skupiliśmy się na najbardziej wiarygodnych raportach, które dostarczają najrzetelniejsze wiadomości.

Wykorzystane raporty i dokumentacje:

2020 Insider Threat Report
Cybersecurity Insiders

2019 Insider Threat Report
Verizon

2020 Cost of Insider Threats: Global Report
Ponemon Institute

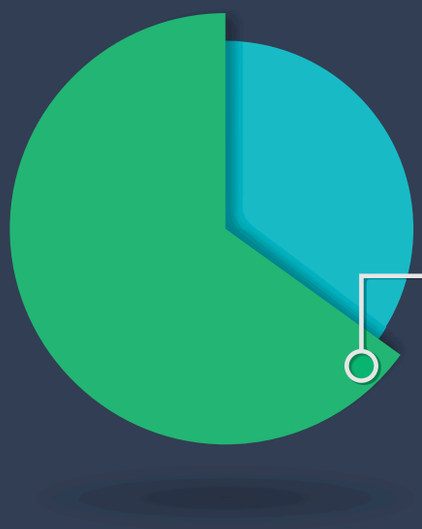
2018 Insider Threat Report
Crowd Research

2020 Insider Threat Report
bitglass

2018 Cost of Insider Threats: Global Report
Ponemon Institute

"Insiderzy mogą zagrozić każdej firmie, niezależnie od jej wielkości i poziomu zabezpieczeń."

5 zagrożeń wewnętrznych z 2020 roku



68% organizacji czuje się wyjątkowo podatnie na ataki i zagrożenia wewnętrzne.

*- według raportu **„2020 Insider Threat Report"** sporządzonego przez Cybersecurity Insiders*

Przykłady ostatnich ataków wewnętrznych

2020

shopify

Naruszenie danych w firmie Shopify

Incydent ten spowodował spadek ceny akcji Shopify o 1,27%

amazon

Wykorzystanie poufnych informacji

Starszy kierownik działu podatkowego organizacji został oskarżony o wykorzystanie poufnych danych i pozyskanie 1,4 miliona dolarów.

STRADIS HEALTHCARE

Atak na organizację Stradis Healthcare

Przywrócenie danych i wznowienie operacji kosztowało firmę 5000 dolarów.

Atak na platformę Twitter

Incydent ten spowodował spadek ceny akcji Twittera aż o 4%

TESLA

Próba ataku na firmę Tesla

Pracownik odrzucił łapówkę w wysokości 1 miliona dolarów, którą miał otrzymać za zainstalowanie w systemie złośliwego oprogramowani.

Najbardziej szkodliwi Insiderzy

Uprzywilejowani użytkownicy i administratorzy

Są oni szczególnie groźni, ponieważ posiadają klucze do całej infrastruktury IT organizacji, a także dostęp do poufnych danych i informacji.

Zwykli pracownicy

Nie są tak szkodliwi, jak użytkownicy uprzywilejowani. W praktyce jednak, nadal mogą oni świadomie nadużywać danych firmowych oraz instalować nieautoryzowane aplikacje.

Osoby trzecie i pracownicy tymczasowi

Dostawcy oraz partnerzy biznesowi często nie przestrzegają praktyk cyberbezpieczeństwa w infrastrukturze IT firmy, a także nieświadomie naruszają wdrożone zasady.

Uprzywilejowani użytkownicy biznesowi i kadra kierownicza

Ta kategoria użytkowników może nadużywać swoich praw i wykorzystywać poufne informacje w celu korzyści osobistych i finansowych lub możliwości zagrożenia korporacji.

Zagrożenia wewnętrzne stają się coraz częstsze

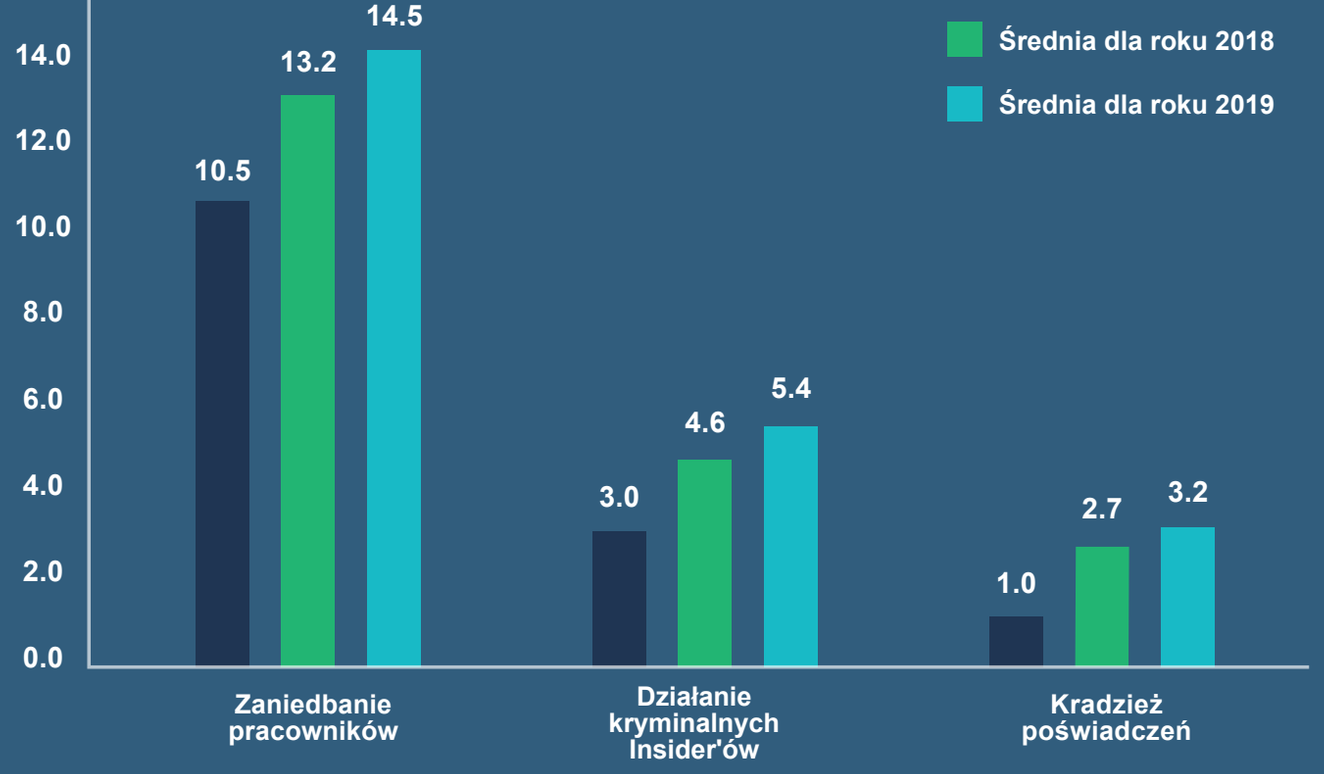
Mimo rosnącej świadomości w zakresie zagrożeń wewnętrznych i stale doskonalonych narzędzi pomagających zachować bezpieczeństwo IT infrastruktury firmy, odsetek tego typu ataków nieprzerwalnie rośnie.

Prognozy i przewidywania częstotliwości zagrożeń wewnętrznych w 2021 roku nie napawają optymizmem. Biorąc pod uwagę tendencje z lat 2016, 2018 i 2019, Forrester przewiduje, że liczba naruszeń bezpieczeństwa danych w obrębie firm, wzrośnie o nawet 8%.

Częstotliwość ataków w stosunku do 3 różnych powodów występowania zagrożeń wewnętrznych

16.0

Średnia dla roku 2016



Dane dostarczone przez 2020 Cost of Insider Threats: Global Report - Ponemon Institute

Wspomniane wyżej badanie Ponemon Insitute potwierdza, że stały wzrost zagrożeń jest konsekwencją trzech kluczowych czynników:

Zaniedbanie pracowników

Błąd ludzki związany z brakiem świadomości i odpowiedniej edukacji w zakresie potencjalnych ataków, jest najbardziej powszechnym powodem incydentów związanych z cyberbezpieczeństwem.

01

Działanie kryminalnych Insider'ów

Tacy pracownicy wyrządzają wiele szkód, ponieważ posiadają cenną wiedzę na temat środków cyberbezpieczeństwa wdrożonych i stosowanych przez organizację, w której pracują.

02

Kradzież poświadczeń

Dla hakerów wykradanie poświadczeń zaufanego pracownika jest jednym z najlepszych sposobów dostania się do chronionego obszaru organizacji.

03

▪ Koszt ataków wewnętrznych stale rośnie

Koszty bezpośrednie
Pieniądze niezbędne do wykrycia, zbadania i złagodzenia zagrożenia, a także naprawy naruszenia i luk w systemie

1

Koszty pośrednie
Wartość utraconych zasobów, a także czasu pracownika poświęconego na doprowadzenie systemu do stanu sprzed ataku

2

Przedsiębiorstwa z Ameryki Północnej najbardziej cierpią, właśnie z powodu ataków wewnętrznych i konsekwencji jakie one ze sobą niosą. Średni koszt naruszeń wewnętrznych w tym regionie wzrósł z 11,1 miliona do 13,3 miliona dolarów.

Całkowity średni koszt ataków wewnętrznych*

2017
8.76 milionów $

2019
11.45 milionów $

**Dane dostarczone przez The Ponemon Institute 2018 and 2020 Cost of Insider Threats: Global Reports*

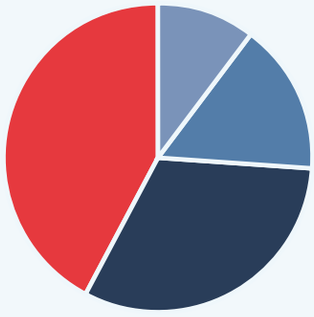
> *"Im dłużej zagrożenie pozostaje niewykryte, tym więcej szkód winfrastrukturze IT firmy może wyrządzić osoba atakująca."*

Czas potrzebny do wykrycia zagrożenia wewnętrznego wydłużył się

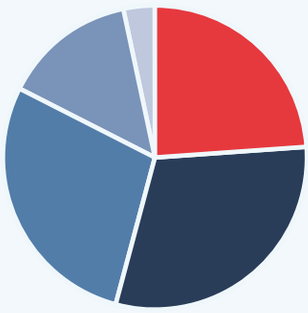
Według raportu Ponemon Institute, wykrycie ataku wewnętrznego zajmuje średnio 77 dni. Jednocześnie ankiety przeprowadzone wśród specjalistów ds. cyberbezpieczeństwa i administratorów działów IT pokazują, że wiele firm jest w stanie wykryć i powstrzymać nieautoryzowane włamanie do systemu w ciągu zaledwie kilku godzin.

Czas potrzebny do wykrycia zagrożenia wewnętrznego

16% — minuty
16% — 1 godzina
20% — 1 dzień



10% — kilka dni
15% — kilka tygodni
30% — kilka miesięcy



22% — kilka minut
28% — kilka godzin
26% — 1 dzień

20% — 1 tydzień
16% — 1 miesiąc
2% — 3 miesiące
4% — ponad 3 miesiące
7% — brak możliwości wykrycia

Dane dostarczone przez 2020 Insider Threat Report autorstwa bitglass

40% — lata

Dane dostarczone przez Verizon 2019 Insider Threat Report: Executive Summary

13% — 1 tydzień
3% — 1 miesiąc

Dane dostarczone przez Crowd Research Partners 2018 Insider Threat Report

Jaka jest najlepsza strategia ochrony?

Biorąc pod uwagę szeroki zakres narzędzi z obszaru cyberbezpieczeństwa dostępnych na rynku – trudno jest skoncentrować się na konkretnej, jednej linii obrony i wybrać oprogramowanie, które zapewni najlepsze wyniki, przy minimalnych zasobach. Jednym z możliwych sposobów, jest analiza statystyk dotyczących oszczędności kosztów związanych z wdrażaniem takich narzędzi i bezpiecznych praktyk pracy w cyberprzestrzeni.

Średni zysk po wdrożeniu narzędzi i praktyk z obszaru cyberbezpieczeństwa*

Narzędzie do analizy aktywności użytkowników (UBA)
3.4 millionów $

Zarządzanie dostępem uprzywilejowanym (PAM)
3.1 millionów $

Szkolenie i uświadamianie użytkowników
3 millionów $

Dokumentacja i wymiana informacji o zagrożeniach
2.8 millionów $

Skrupulatna weryfikacja pracowników trzecich
2.7 millionów $

Zarządzanie reakcjami na incydenty (IRM)
2.7 millionów $

Monitorowanie aktywności pracowników
2.6 millionów $

**Dane dostarczone przez 2020 Cost of Insider Threats: Global Report by the Ponemon Institute*

Jak możesz wdrożyć wyżej wymienione narzędzia i praktyki przy użyciu Ekran System – kompleksowej platformy do zarządzania aktywnością użytkowników i chroniącej sieć firmową przed zagrożeniami wewnętrznymi?

01

Narzędzie do analizy aktywności użytkowników (UBA) - funkcja ustala punkt odniesienia dla wszelkich zachowań pracowników, wykrywa nietypowe aktywności i powiadamia administratorów - na przykład o logowaniu się do systemu o nietypowych godzinach.

02

Zarządzanie dostępem uprzywilejowanym (PAM) – Ekran System oferuje solidny zestaw narzędzi PAM, który odpowiada za procedurę ręcznego zatwierdzania dostępu uprzywilejowanego, uwierzytelnianie wieloskładnikowe, bezpieczne zarządzanie hasłami oraz szereg innych funkcjonalności.

03 **Szkolenie i uświadamianie użytkowników** to czynność, która zwiększa świadomość pracowników w zakresie cyberzagrożeń. Ekran System może być częścią takiego szkolenia, ponieważ w czasie rzeczywistym, informuje - w postaci alertów - o działaniach, które naruszają korporacyjne zasady bezpieczeństwa

04 **Dokumentacja informacji o zagrożeniach –** ogólnobranżowa praktyka wymiany między organizacjami, informacji o wykrytych zagrożeniach i atakach. W celu zbierania danych możesz skorzystać z zestawu narzędzi do raportowania zawartych w programie Ekran System.

05 **Ocena poziomu cyberbezpieczeństwa dostawców zewnętrznych –** wskazane są rygorystyczne procedury weryfikacji osób i pracowników trzecich. Ekran System pozwala monitorować taki rodzaj pracownika równie łatwo i sprawnie jak w przypadku standardowych użytkowników firmowej sieci.

06 **Narzędzie do zarządzania aktywnością użytkowników –** pomaga natychmiast reagować na potencjalne zagrożenie wewnętrzne. Ekran System ostrzega administratorów bezpieczeństwa o podejrzanych działaniach wykrytych podczas monitoringu.

07 **Narzędzia do monitorowania i nadzoru pracowników –** rejestrują wszelkie działania użytkowników w obrębie firmowego systemu. Ekran System zapewnia stały monitoring poprzez rejestrowanie aktywności z ekranów podwładnych, a także przechwytywanie metadanych.

Administratorzy bezpieczeństwa mogą używać programu Ekran System do przeglądania sesji użytkowników w czasie rzeczywistym lub wyszukiwania zapisów dotyczących konkretnego zdarzenia czy incydentu.

Dzięki temu, mogą oni wykrywać zagrożenia wewnętrzne w błyskawicznym tempie i stosownie na nie reagować.

Ekran System® to rozwiązanie służące do kompleksowego zarządzania ryzykiem w obrębie firmowej sieci. Pomaga organizacjom przeciwdziałać zagrożeniom wewnętrznym poprzez wykrywanie potencjalnych ataków i podejrzanych aktywności w czasie rzeczywistym.

Czy chcesz trzymać Insiderów z dala od Twojej firmowej sieci?

Rozpocznij darmowy okres próbny:

www.ekransystem.com

Odwiedź nas na: **www.ekransystem.com**

EKRAN®

/securivy

/securivy

/Securivy - Bezpieczeństwo IT

SECURIVY

biuro@securivy.com
tel. +48 722-158-258

Copyright © 2021 Ekran System, All rights reserved.