Grant Thornton

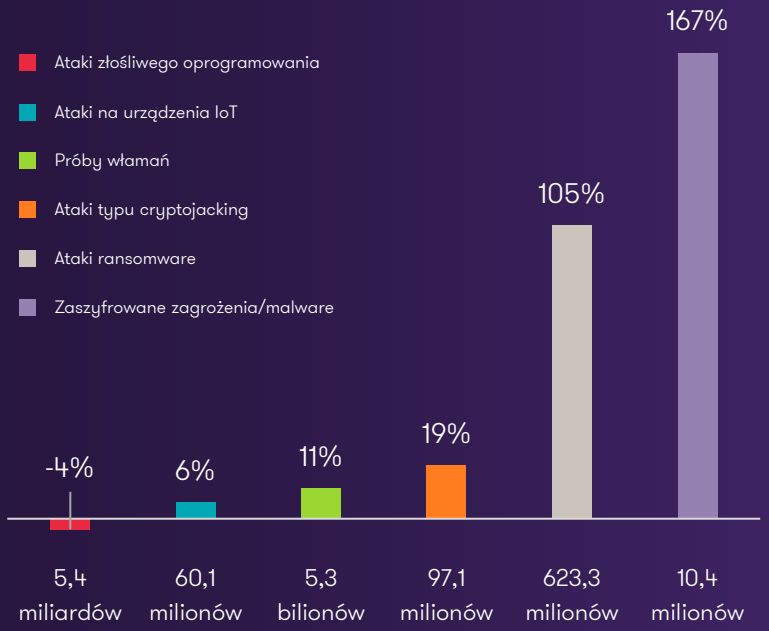
Podsumowanie cyberzagrożeń 2022 i prognozy na 2023

Cyberzagrożenia

w 2022 r.

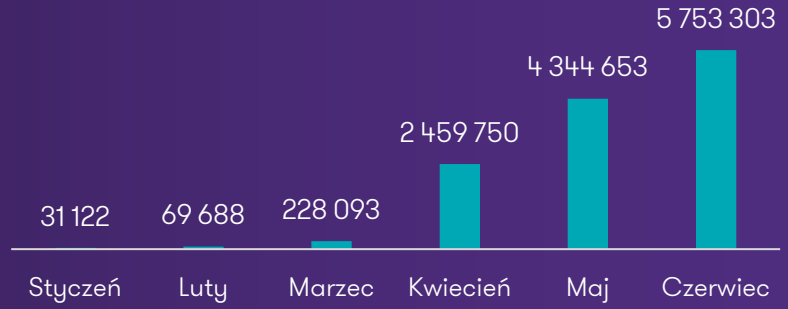
Cyberzagrożenia 2022 – trendy, świat

Wykres 1. Światowe trendy dot. cyberataków w roku 2022 r.



- Ogólny wzrost liczby cyberataków o 38% w 2022/2021
- Wzrost ataków ukrytych przez szyfrowanie o 167%
- Ransomware pozostaje zagrożeniem numer jeden dla dużych i średnich firm.
- Spadek liczby ataków malware na świecie (wolumen to 5,4 biliona) vs Ukraina.

Wykres 2. Ilość złośliwego oprogramowania w 2022 r. | Ukraina



Źródło: 2022 SonicWall Cyber Threat Report

Cyberzagrożenia 2022 – trendy, świat

- 30,6% wszystkich otrzymanych e-maili było spamem, a 1,6% zawierało złośliwe oprogramowanie lub linki phishingowe.
- Średnia tygodniowa liczba ataków na organizację na całym świecie osiągnęła ponad 1130.
- Około 40 milionów adresów URL zostało zablokowanych tylko w okresie od lipca do listopada 2022 r. (wg. danych od Acronis).
- Hasła które wyciekły lub zostały skradzione były przyczyną prawie połowy zgłoszonych naruszeń w pierwszej połowie 2022 r.

Cyberzagrożenia 2022 – trendy, świat

Region	Liczba tygodniowych ataków na organizację	Zmiana YoY
Afryka	1,758	+3%
Azja	1,684	+25%
Ameryka Łacińska	1,602	+29%
Europa	963	+26%
ANZ	937	+82%
Ameryka Północna	854	+54%

Źródło: Check Point 2022 Security Report

Wzrost liczby cyberataków w 2022 r. w porównaniu z 2021 r.

ANZ (+82%), Ameryka Północna (+54%), Ameryka Łacińska (+29%) i Europa (+26%)
Afryka doświadczyła największej liczby ataków - 1758 ataków tygodniowo na organizację, region APAC - 1684 ataków na organizację tygodniowo

Wzrost ogólnej liczby cyberataków w 2022 r.

Wielka Brytania (77%), USA (57%), Singapur (26%).

Najczęściej atakowanymi krajami (pod względem złośliwego oprogramowania na użytkownika) w III kwartale 2022 r. były Korea Południowa, Jordania i Chiny.

Cyberzagrożenia 2022 – trendy, świat

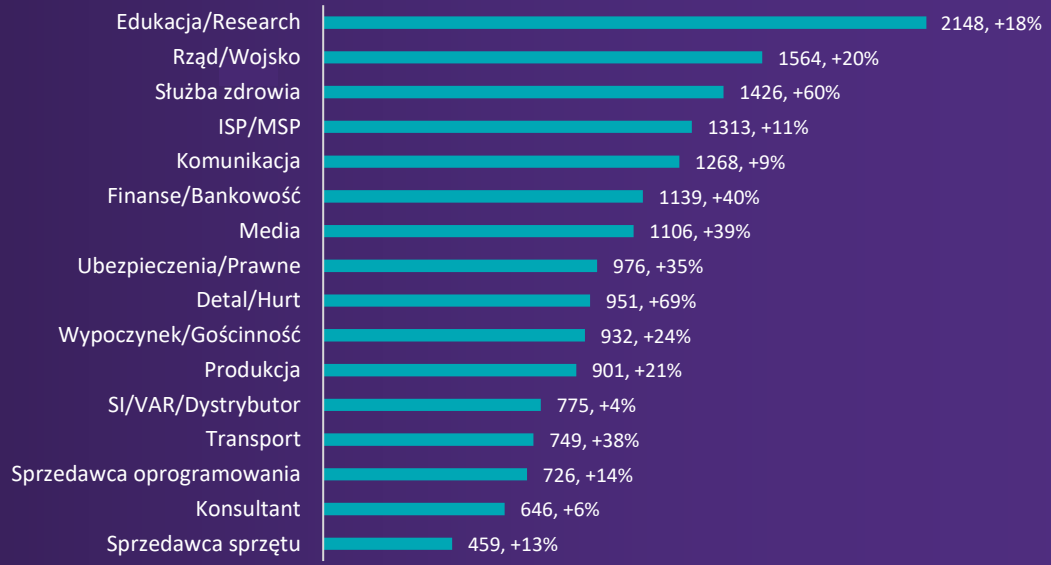
Trzy najczęściej atakowane branże na świecie w 2022 roku to edukacja i badania, agencje rządowe oraz branża zbrojeniowa i opieka zdrowotna.

Najczęściej atakowaną branżą w trzecim kwartale roku był sektor edukacji/badań, ze średnią liczbą 2 148 ataków na organizację tygodniowo, co stanowi wzrost o 18% w porównaniu z trzecim kwartałem 2021 r.

Sektor opieki zdrowotnej był branżą najczęściej atakowaną przez oprogramowanie ransomware w trzecim kwartale 2022 r.

34% firm z branży naftowej i gazowniczej na świecie w ciągu ostatnich dwóch lat napotkało problem przejęcia stacji roboczych i serwerów przez hakerów.

Wykres 3. Średnia tygodniowa ilość ataków na organizację ze względu na branżę – Globalnie 2022 Q3 i YoY



Źródło: Check Point 2022 Security Report

Cyberzagrożenia 2022 – trendy, Polska

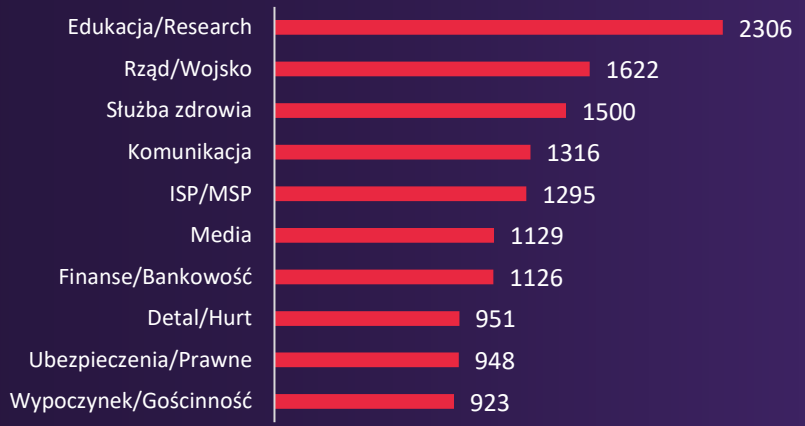
Polska. Tylko w październiku 2022 nastąpił wzrost ilości ataków na sektor użyteczności publicznej o blisko 100 proc. z 1214 do 2316 (tygodniowo) na koniec grudnia.

W 2021 roku prawie 14% wszystkich cyberataków w naszym kraju dotyczyło sektora energetycznego.

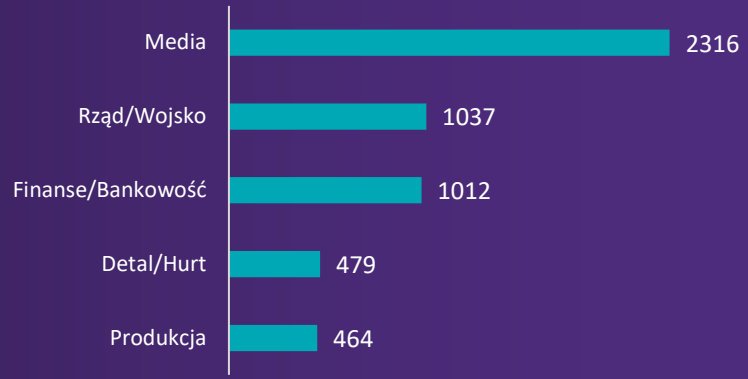
W 2022 roku najczęściej atakowano agencje rządowe oraz firmy obsługujące infrastrukturę krytyczną, która jest kluczowa dla ciągłości funkcjonowania państwa.

Firmy logistyczne są atakowane głównie atakami typu DDOS oraz wiperware, w celu zakłócenia zagranicznej pomocy wojskowej i innej, napływającej na Ukrainę.

Wykres 4. Tygodniowa liczba ataków na organizację - Globalnie



Wykres 5. Tygodniowa ilość ataków na organizację - Polska



Źródło: Check Point 2022 Security Report

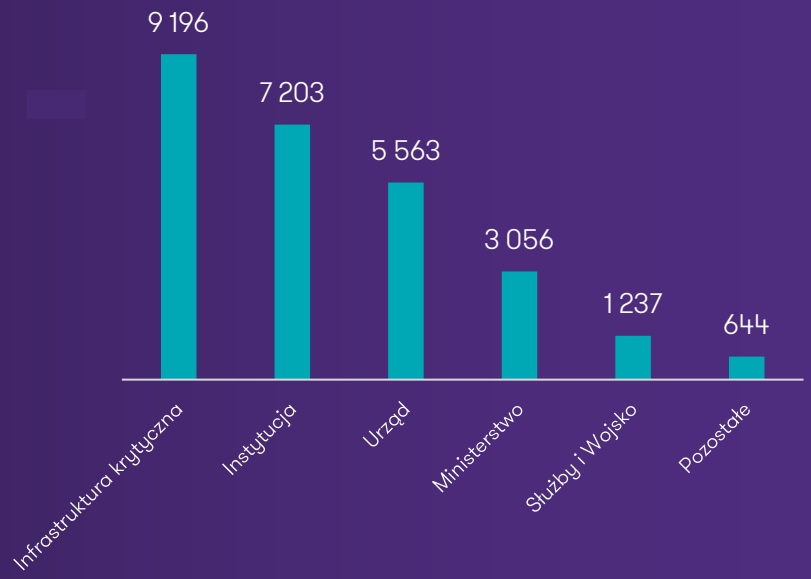
Cyberzagrożenia 2022 – trendy, Polska

9196 zarejestrowanych incydentów dotyczących operatorów infrastruktury krytycznej vs 2626 w 2020 roku

W 2022 roku Komisja Europejska opublikowała pięciopunktowy plan na rzecz ochrony infrastruktury krytycznej w priorytetowych obszarach: gotowości, reagowania i współpracy międzynarodowej.

Plan priorytetowo traktuje kluczowe sektory **energii, infrastruktury cyfrowej, transportu i przestrzeni kosmicznej.**

Wykres 3. Liczba incydentów wg sektorów



Źródło: Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku

Cyberzagrożenia

Prognozy w 2023 r.

Cyberzagrożenia 2023 – prognozy

- Przewiduje się, że średni koszt udanego ataku w 2023 roku osiągnie **5 milionów dolarów**.
- Liczba cyberataków na infrastrukturę użyteczności publicznej, taką jak przedsiębiorstwa **gazowe czy energetyczne, transport publiczny, służba zdrowia, przedsiębiorstwa zaopatrzenia w wodę** drastycznie wzrośnie.
- Niespodziewane i niekontrolowane wyłączenia infrastruktury krytycznej mogą spowodować zakłócenia na dużą skalę.
- Rządy będą nadawały priorytety ochrony cybernetycznej infrastrukturze krytycznej, nastąpi zacieśnianie współpracy rządów i przemysłu.

Cyberzagrożenia 2023 – prognozy

- Współpraca sektora publicznego i prywatnego w zakresie ochrony cyberprzestrzeni ulegnie wzmocnieniu.
- Ubezpieczenia cybernetyczne staną się bardzo ważnym elementem niwelowania skutków finansowych ataków.
- Regulacje prawne dotyczące cyberprzestrzeni będą znacząco wpływać na ubezpieczenia cybernetyczne.
- Wzrost liczby celowanych ataków typu ransomware.

Cyberzagrożenia 2023 – prognozy

- Wzrost ataków z obszaru inżynierii społecznej na media społecznościowe - BEC i deepfakes w tym deepfake voice cloning.

- Wzrośnie znaczenie zabezpieczania pracowników zdalnych i hybrydowych.

- Zwiększanie znaczenia **SASE**.

Secure Access Service Edge to składnik architektury zero trust, który chroni elementy sieci w jej tradycyjnych granicach i poza nimi. Wraz z digitalizacją firm, popularyzacją telepracy i coraz silniejszym powiązaniem aplikacji z usługami w chmurze, rośnie znaczenie bezpieczeństwa chmury, którego strzeże SASE.

- Dalszy wzrost wykorzystania chmury i przyspieszanie transformacji cyfrowych spowoduje wzrost ataków.

Wyzwania związane z zapewnianiem cyfrowej ochrony w polskich firmach

- wysokie koszty rozwiązań ochronnych
- niska świadomość zagrożeń wśród pracowników
- brak zainteresowania kwestiami dotyczącymi bezpieczeństwa

- **35%** managerów wskazuje na zbyt niski budżet na bezpieczeństwo
- **30%** pracowników nie jest świadomych cyberzagrożeń
- **32%** brak zainteresowania ochroną danych i systemów

*wg badania SW Research dla Sophos

Wyzwania związane z zapewnianiem cyberbezpieczeństwa w polskich firmach

- **28%** - zbyt długi czas wdrażania zabezpieczeń
- **26%** - przestarzała infrastruktura IT
- **20%** - niechęć pracowników do wdrażania zabezpieczeń przed cyberatakami

40 proc. menedżerów jest świadoma, że dotkliwym skutkiem cyberataku mogą być problemy z płynnością finansową firmy.

*wg SW Research „Sposób postrzegania cyberbezpieczeństwa wśród menedżerów polskich firm"

Rozwiązania

1. Poznaj wroga - zidentyfikuj zagrożenia, które mogą wpłynąć na firmę.
2. Zdefiniuj priorytety ochrony.
3. Poznaj siebie - przeprowadź **analizę ryzyka**.
4. Określ mocne i słabe strony.
5. Określ strategię postępowania z ryzykiem.
6. Uwzględnij w zakresie działań Procesy, Ludzi i Systemy.
7. **Wdrażaj zabezpieczenia detekcyjne**, prewencyjne i korekcyjne.
8. **Monitoruj poziom ryzyka.**
9. **Buduj świadomość w zakresie cyfrowych zagrożeń.**
10. **Wykorzystaj specjalistyczne usługi outsourcingu.**

Kalendarz cyberbezpieczeństwa - 2023

Styczeń

- **Plan działania na Q1**
- **Testy podatności systemów**
- Plan szkoleń dla IT

Luty

- **Testy socjotechniczne**
- **Przegląd dostawców**

Marzec

- **Przegląd uprawnień**
- **Szkolenia dla pracowników**

Kwiecień

- **Testy kopii zapasowych**
- Podsumowanie Q1
- Plan działania na Q2

Maj

- **Przegląd stacji roboczych**
- **Przegląd ochrony antywirusowej**
- Testy podatności systemów

Czerwiec

- **Przegląd ochrony sieci**
- Testy socjotechniczne

Lipiec

- **Przegląd infrastruktury**
- Szkolenia dla pracowników

Sierpień

- **Przegląd kont uprzywilejowanych**
- Podsumowanie Q2
- Plan działania na Q3

Wrzesień

- **Testy penetracyjne**
- Szkolenia dla IT
- Udział w konferencjach

Październik

- **Testy procedur awaryjnych**
- Testy socjotechniczne

Listopad

- **Przegląd polityk i procedur**
- Aktualizacja dokumentacji
- Analiza ryzyka
- Szkolenia dla pracowników

Grudzień

- **Podsumowanie 2023**
- **Plan działania na 2024**
- **Nowy Rok z Grant Thornton**

Grant Thornton

Zapraszamy do kontaktu

Tomasz Janas
Doradca, Digital Drive
M +48 531 700 531
E tomasz.janas@pl.gt.com