NET COMPLEX
Bezpieczeństwo IT

PROGNOZY CYBERBEZPIECZEŃSTWA 2024

33 816 04 11 | www.netcomplex.pl | Wita Stwosza 5 | Bielsko-Biała

NET COMPLEX
Bezpieczeństwo IT

SPIS TREŚCI

WSTĘP

W roku 2023, dynamiczny rozwój technologii przyniósł za sobą wyjątkowe wyzwania z zakresu cyberbezpieczeństwa. Zanotowano znaczący wzrost zarówno w **różnorodności**, jak i **intensywności** ataków cybernetycznych, co stanowiło poważne zagrożenie dla firm oraz instytucji na całym świecie.

Wpływ trwającej wojny na Ukrainie na krajobraz cyberbezpieczeństwa utrzymuje się, a nowe grupy pojawiające się na scenie przyczyniają się do rozprzestrzeniania się **haktywizmu**. W pierwszej połowie 2023 roku zaobserwowano także gwałtowny wzrost liczby incydentów związanych z ransomware, a tendencja ta wciaż się nasila.

Aby skutecznie przeciwdziałać ewoluującym zagrożeniom cybernetycznym, niezbędna jest wiedza. Dlatego, podobnie jak w ubiegłych latach, zgromadziliśmy kluczowe informacje od czołowych graczy w dziedzinie cybersecurity, takich jak WatchGuard, Proofpoint, Gartner czy Google.

Na tej podstawie przygotowaliśmy zestaw prognoz na rok 2024, by pomóc w pełni zrozumieć i skutecznie przeciwdziałać zagrożeniom cybernetycznym.

Miłej lektury!

Raport Cybersecurity Ventures wskazuje, że **globalny roczny koszt cyberprzestępczości** osiągnie w 2023 roku **8 bilionów dolarów.**

ROK 2023

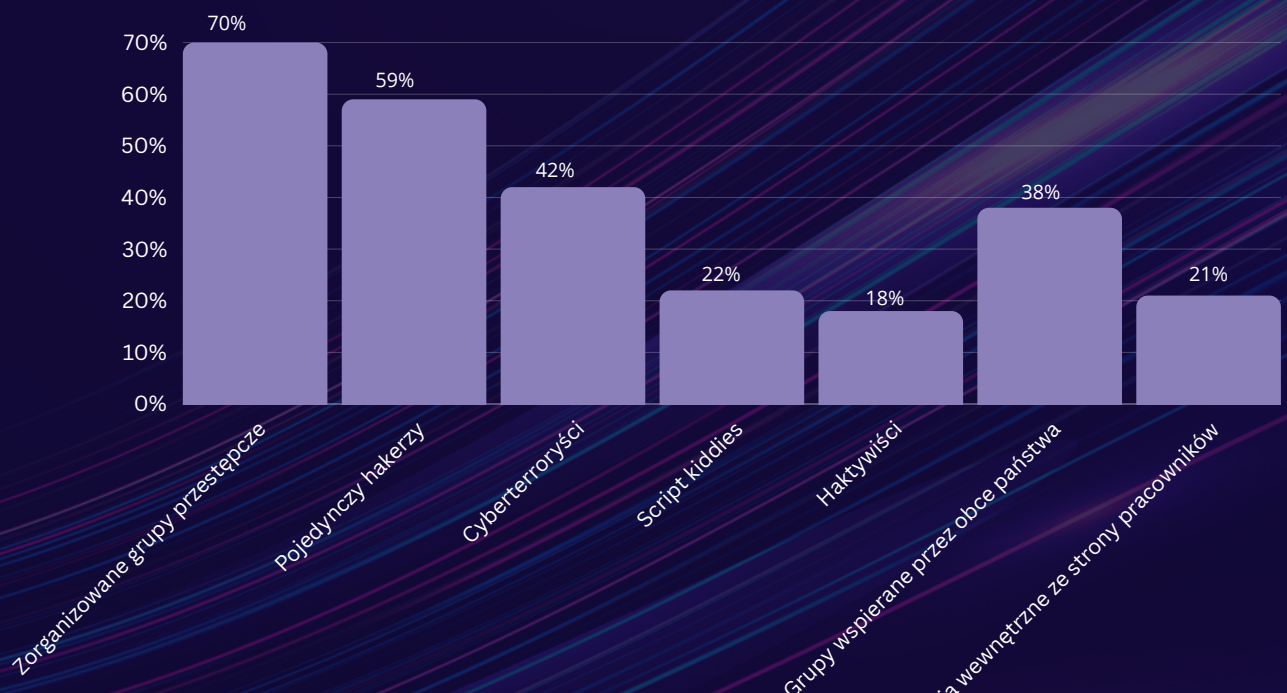
Wydarzenia w Ukrainie i związane z nimi zintensyfikowanie działań w cyberprzestrzeni mocno wpłynęły na percepcję zagrożeń wśród polskich przedsiębiorstw.

Jedna trzecia polskich firm zanotowała wzrost **intensywności ataków cybernetycznych**. Najbardziej niepokojącym źródłem zagrożeń cyfrowych pozostają zorganizowane grupy cyberprzestępcze, jednak rekordowy odsetek firm wykazuje obawy związane z grupami wspieranymi przez obce państwa.

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) wyróżniła osiem grup zagrożeń, które najmocniej wpłynęły na bezpieczeństwo firm w 2023 roku. Są to:

- Ransomware,
- Złośliwe oprogramowanie,
- Inżynieria społeczna,
- Naruszenia ochrony danych,
- Ataki DoS/DDoS,
- Zagrożenia mające wpływ na dostępność Internetu,
- Manipulacja i ingerencja w informacje,
- Ataki na łańcuch dostaw.

Jakie grupy stanowią realne zagrożenie dla organizacji?



Źródło: Barometr cyberbezpieczeństwa. Detekcja i reakcja na zagrożenia w czasie podwyższonego alertu

ROK 2023

Od początku 2023 roku zauważalnie wzrosła częstotliwość, z jaką cyberprzestępcy sięgają po technikę "***ad hijacking***". W ramach tego typu ataku, przestępcy zakupują reklamy w wyszukiwarce, np. Google, związane z określonymi słowami kluczowymi.

Dzięki wykorzystaniu Google Ads, fałszywe strony uzyskują pierwsze pozycje w wynikach wyszukiwania, co zwiększa ich atrakcyjność dla użytkowników.

CYBERPRZESTĘPCY PRZYCIĄGAJĄ UŻYTKOWNIKÓW FAŁSZYWYMI REKLAMAMI NA SPECJALNIE SPREPAROWANE STRONY.

FAŁSZYWE WITRYNY POSZYWAJĄ SIĘ POD RENOMOWANE MARKI, TAKIE JAK ADOBE READER, GIMP, MICROSOFT TEAMS, OBS, SLACK CZY THUNDERBIRD.

AD HIJACKING WYKORZYSTYWANY JEST DO ROZPOWSZECHNIANIA ZŁOŚLIWEGO OPROGRAMOWANIA TAKIEGO JAK AURORASTEALER, ICEDID, REDLINE STEALER CZY VIDAR.

Po kliknięciu w reklamę użytkownik jest przekierowywany na fałszywą stronę, udającą dostawcę wybranego oprogramowania. W witrynie znajduje się odnośnik do pobrania pliku zawierającego **szkodliwe oprogramowanie** w formatach .exe lub .zip.

Działania cyberprzestępców umożliwiają im uzyskanie pełnego dostępu do systemu użytkownika, co może skutkować chociażby **pozyskaniem danych uwierzytelniających** do serwisów, z których korzysta ofiara.

Ataki "ad hijacking" stanowiły jedną z najbardziej wyrafinowanych strategii wykorzystywanych przez hakerów w 2023 roku. Jakie wyzwania przyniesie zbliżający się rok 2024? Sprawdzamy!

PROGNOZY 2024

NET COMPLEX
Bezpieczeństwo IT

NA WSZYSTKO JEST SUBSKRYPCJA!

Płatności elektroniczne niezmiennie wypierają gotówkę. Jednak zamiast tradycyjnego modelu zakupów, coraz popularniejsze staje się korzystanie z subskrypcji i licencjonowania usług. Trend ten obejmie różne sektory, w tym również rynek cyberbezpieczeństwa.

W kontekście cybersecurity, przedsiębiorstwa coraz częściej preferują **subskrypcje usług bezpieczeństwa**, które zapewniają stałe wsparcie, monitorowanie i aktualizacje w zamian za okresowe opłaty.

Model taki umożliwia łatwy dostęp do najnowszych rozwiązań i technologii bez konieczności ponoszenia dużych kosztów. W efekcie, organizacje są w stanie skupiać się na utrzymaniu wysokiego poziomu ochrony przed zagrożeniami cybernetycznymi poprzez elastyczne i aktualizowane na bieżąco usługi subskrypcyjne.

Sztuczna inteligencja i LLM jako usługa... służąca do ataków

Duże modele językowe (*large language model*, LLM) i inne narzędzia sztucznej inteligencji również będą coraz częściej opracowywane i oferowane jako płatna usługa, a następnie wykorzystywane do różnych celów, takich jak **kampanie phishingowe** czy **rozpowszechnianie dezinformacji**.

Na podobnej zasadzie działają usługi ransomware-as-a-service, lub też szerzej crime-as-a-service, które już teraz cieszą się sporą popularnością na podziemnych forach.

Raport CyberMadeInPoland "Polski rynek cyberbezpieczeństwa 2023 – 2028" wskazuje, że wśród przebadanych przedsiębiorstw z sektora prywatnego 10,5% korzysta ze wsparcia **Managed Security Services Providers (MSSP)**, czyli integratorów oferujących produkty i usługi w modelu abonamentowym.

Przyszłość usług Managed Security Service Providers (MSSP) w Polsce jest obiecująca. Spodziewa się, że wraz ze wzrostem świadomości korzyści wynikających z outsourcingu IT, popyt na tego typu usługi będzie nadal wzrastał.

2 MNIEJ NIŻ ZERO (TRUST)

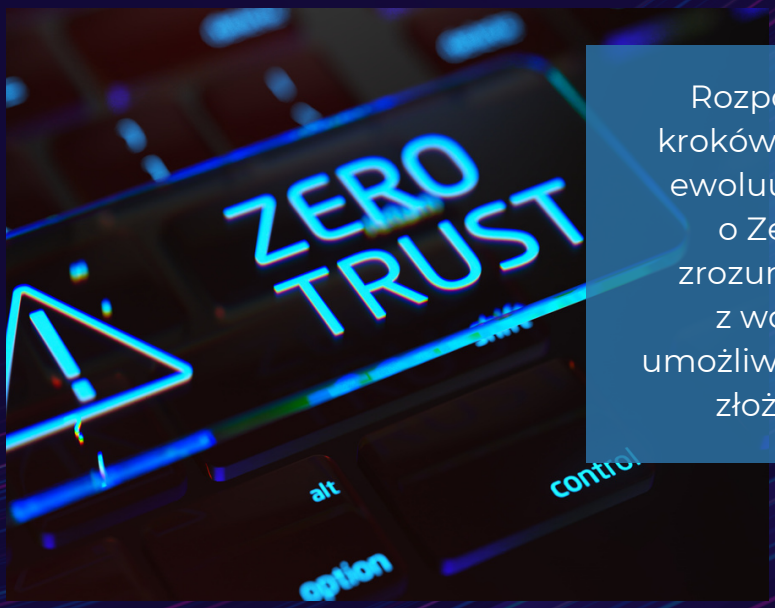
Podstawowe założenie modelu Zero Trust, czyli zasada "zawsze weryfikuj", rozwija się w miarę wzrostu złożoności systemów oraz połączenia bezpieczeństwa ze strategią biznesową.

W roku 2024 koncepcja bezpieczeństwa Zero Trust nadal będzie zyskiwać na popularności. To proaktywne podejście ma na celu ochronę przed zagrożeniami zarówno zewnętrznymi, jak i wewnętrznymi, a także bocznymi ruchami w sieci.

Poprzez wdrożenie zasad bezpieczeństwa opartych na zerowym zaufaniu, organizacje mogą **wzmocnić swoją pozycję** w kwestiach bezpieczeństwa, **minimalizując ryzyko** nieautoryzowanego dostępu.

W miarę ewolucji krajobrazu zagrożeń zasada ta rozciąga się poza infrastrukturę korporacyjną, obejmując ekosystem pracowników zdalnych, partnerów i urządzeń IoT.

Można spodziewać się, że paradygmat Zero Trust przestanie być jedynie technicznym modelem bezpieczeństwa sieci, a stanie się **adaptacyjną i kompleksową strategią**. Będzie ona możliwa dzięki ciągłemu **uwierzytelnianiu w czasie rzeczywistym** oraz **monitorowaniu aktywności** przy wykorzystaniu sztucznej inteligencji.



Rozpoczynanie od niewielkich kroków i stopniowe przyjmowanie ewoluującego sposobu myślenia o Zero Trust ułatwia lepsze zrozumienie korzyści płynących z wdrożenia koncepcji oraz umożliwia skuteczne zarządzanie jej złożonością etap po etapie.

3 CYBERBEZPIECZEŃSTWO W BIURZE ZARZĄDU

W 2024 r. cyberbezpieczeństwo stanie się strategicznym priorytetem dla każdego przedsiębiorstwa. Nowe regulacje prawne i rosnące ryzyko ataków zmuszają firmy do skoncentrowanego działania w tym obszarze.

Prognozy Gartnera wskazują, że do 2026 roku aż **70% zarządów** będzie miało co najmniej jednego członka z odpowiednim doświadczeniem w obszarze cyberbezpieczeństwa. Umożliwi to przedsiębiorstwom wyjście poza reaktywną obronę i skoncentrowanie się na nowych biznesowych możliwościach, wynikających z **proaktywności**.

Wejście w życie regulacji **DORA** (Digital Operational Resilience Act) oraz **NIS 2** (Directive on Security of Network and Information Systems 2) stawia przed przedsiębiorstwami nowe wyzwania. **Zarządy organizacji** są teraz odpowiedzialne za skrupulatne przestrzeganie nowych przepisów, co wymaga skoncentrowanych wysiłków w zakresie odporności cyfrowej oraz bezpieczeństwa sieci i informacji.

Niestety, na decyzje organizacji w obszarze cyberbezpieczeństwa najmocniej wpływa konfrontacja z atakami:

83%

Taki odsetek przedsiębiorstw zgłasza, że po cyberataku zanotowano **wzrost świadomości zarządu** w zakresie bezpieczeństwa.

60%

Blisko 2/3 przedsiebiorstw jednocześnie **zwiększyło budżet** na rozwiązania z zakresu cybersec.

4 CYBERWOJNA SPONSOROWANA PRZEZ PAŃSTWA

Cyberwojna to nie tylko pole działań hakerów; także państwa aktywnie uczestniczą w tym konflikcie. W 2024 roku prognozowany jest wzrost liczby cyberataków sponsorowanych przez państwa i działań szpiegowskich. Wszystko to wywołać może istotne skutki geopolityczne i zakłócić funkcjonowanie infrastruktury krytycznej.

38% firm wskazuje na realne zagrożenie płynące ze strony grup wspieranych przez obce państwa. Dla porównania w ubiegłym roku było to 27%

Aby skutecznie przeciwdziałać zagrożeniom, poszczególne państwa będą zobligowane do wzmacniania swoich zdolności obronnych w obszarze cybernetyki oraz do współpracy w ramach międzynarodowych inicjatyw dotyczących cyberbezpieczeństwa.

5 KRYZYS UMIEJĘTNOŚCI

Utrzymujący się problem braku personelu posiadającego niezbędną wiedzę specjalistyczną do skutecznej ochrony przedsiębiorstw przed cyberzagrożeniami pozostaje jednym z głównych wyzwań w 2024 roku.

Aż 47% przedsiębiorstw wskazuje, że trudności w zatrudnieniu i utrzymaniu specjalistów jest największą przeszkodą w budowaniu cyberbezpieczeństwa.

Prognozy na nadchodzący rok wskazują, że działania mające na celu rozwiązanie tego problemu obejmą podwyżki wynagrodzeń, a także zwiększone inwestycje w programy skoncentrowane na szkoleniach, rozwoju i podnoszeniu kwalifikacji.

Możemy oczekiwać także wzrastającego znaczenia **umiejętności miękkich,** zwłaszcza w obszarze komunikacji interpersonalnej, budowania relacji oraz rozwiązywania problemów, szczególnie w kontekście konieczności obrony przed zagrożeniami cybernetycznymi.

6 ATAKI NA USŁUGI W CHMURZE

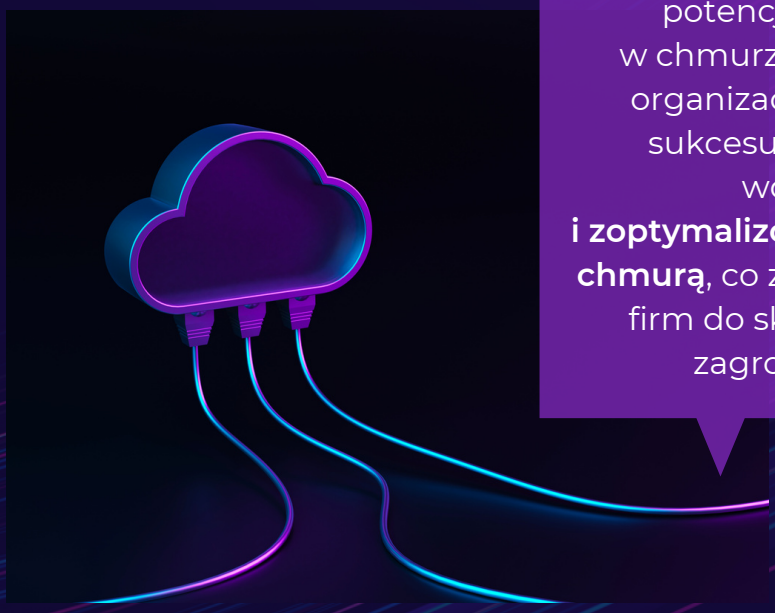
W ciągu kilku ostatnich lat nastąpiła znacząca migracja firmowych danych, procesów i infrastruktury do chmury obliczeniowej.

Prognozy Gartnera wskazują, że w 2024 roku globalne wydatki użytkowników końcowych na **usługi w chmurze publicznej** osiągną 679 miliardów dolarów, a prognozy na rok 2027 przewidują przekroczenie 1 biliona dolarów.

Tendencja ta wskazuje na rosnące zaufanie firm i użytkowników do korzystania z usług chmurowych, co wynika z korzyści związanych z elastycznością, skalowalnością i efektywnością oferowaną przez chmurę obliczeniową.

Mimo licznych korzyści wynikających z migracji do chmury, pojawiają się także wyzwania.

Zagrożenia takie jak ograniczona widoczność i kontrola, błędnie skonfigurowane pamięci masowe i ustawienia, podatne na ataki aplikacje w chmurze, niekompletne usuwanie danych, czy kwestie zgodności będą nadal stanowiły wyzwanie dla firm.



Ochrona krytycznych danych w obliczu potencjalnych ataków na usługi w chmurze stanie się priorytetem dla organizacji. Kluczowym elementem sukcesu w tym kontekście będzie wdrożenie **dojrzałego i zoptymalizowanego modelu zarządzania chmurą**, co znacząco przyspieszy zdolność firm do skutecznego reagowania na zagrożenia bezpieczeństwa.

7 KONIEC ERY MALWARE?

Z uwagi na rosnącą powszechność aplikacji chmurowych i modelu SaaS, ataki na tożsamość stają się coraz częstszą techniką naruszeń. Wyprze ona tym samym ataki wykorzystujące luki zero-day czy malware.

Wykorzystywanie malware do przeprowadzania ataków staje się ryzykowne z powodu coraz bardziej zaawansowanych narzędzi detekcji. W związku z tym napastnicy skoncentrują się uzyskiwaniu dostępu do sieci korporacyjnych za pomocą **skradzionych tożsamości**.

Co czwarta firma w Polsce planuje większe inwestycje w zakresie **zarządzania tożsamością i dostępem** w ciągu najbliższych dwunastu miesięcy.

Dla porównania w ubiegłym roku odsetek ten wynosił 16%.

“Identity is the new vulnerability.”

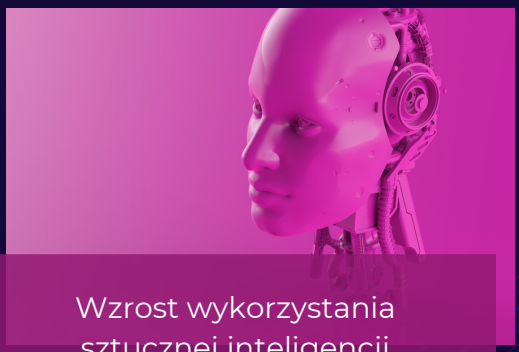
Organizacje powinny skoncentrować się nie tylko na wzmacnianiu infrastruktury, lecz także na zabezpieczaniu przechowywanych danych uwierzytelniających, plików cookie sesji, kluczy dostępu oraz rozwiązywaniu problemów związanym z błędnymi konfiguracjami, szczególnie dotyczącymi kont uprzywilejowanych.

Kluczowe stanie się wprowadzenie zarządzania dostępem do danych za pomocą rozwiązań **IAM** oraz **PAM**.

8 AI JAKO MIECZ OBOSIECZNY

Gwałtowny rozwój narzędzi generatywnej sztucznej inteligencji niesie ze sobą zarówno nadzieje, jak i zagrożenia.

Nowym trendem w sferze działań cyberprzestępczych jest zastosowanie algorytmów sztucznej inteligencji do **doskonalenia i optymalizowania działań przestępczych**.
Działania te obejmują przede wszystkim automatyzację procesów oraz generowanie przekonujących treści tekstowych, głosowych i wizualnych, celem **wzmacniania przekazów phishingowych**, a także w ramach innych działań z zakresu inżynierii społecznej.

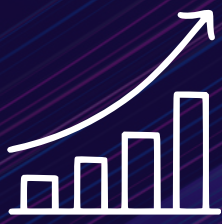


Wzrost wykorzystania sztucznej inteligencji w działaniach przestępczych wymaga stosowania rozwiązań opartych na AI w celu ochrony danych oraz przeciwdziałania nadużyciom i przestępstwom.

Z kolei możliwości AI w kontekście analizy złośliwego oprogramowania już na chwilę obecną wyglądają imponująco.

70%

AI identyfikuje aż o 70% więcej złośliwych skryptów niż tradycyjne metody.



300%

AI wykazuje 300% większą dokładność w wykrywaniu prób ataków poprzez powszechne luki w zabezpieczeniach za pomocą złośliwych skryptów lub exploitów.

500 tys.

Nawet tylu specjalistów brakuje na rynku europejskim.
Zdolność AI do szybszej oraz dokładniejszej analizy złośliwego oprogramowania może mieć realny wpływ na ten deficyt.

9 DEEPFAKE JAKO BROŃ

Prawdziwy przełom w technologii *deepfake* nastąpił wraz z rozwojem narzędzi służących do manipulacji treściami.

W obecnej chwili, jednym z najpoważniejszych wyzwań dla sił zbrojnych na całym globie jest wojna informacyjna.
Najbardziej zaawansowane armie na świecie mogą wykorzystywać technologię deepfake w celu szerzenia **dezinformacji oraz wprowadzenia zamętu** zarówno w szeregach przeciwnika, jak i wrogo nastawionych społeczeństwach.
Taka strategia może prowadzić do **zakłócenia stabilności politycznej** oraz **wywołania chaosu społecznego**.

Deepfake kwestionuje rzetelność wszelkich treści i informacji, co w efekcie może doprowadzić do **destabilizacji fundamentów państwa**.

10 INTERNET OF THINGS NA CELOWNIKU

Liczba urządzeń Internetu Rzeczy (IoT) rośnie wykładniczo, a urządzenia te stają się coraz bardziej zintegrowane z naszym życiem.

Według prognoz IDC, liczba ataków na krytyczną infrastrukturę miejską, przeprowadzanych poprzez słabo zabezpieczone urządzenia brzegowe i IoT, ma podwoić się do 2025 roku.

Często już projekt urządzeń IoT przedkłada łatwość obsługi i wygodę nad solidne środki bezpieczeństwa, czyniąc je **podatnymi na potencjalne zagrożenia** wynikające z nieodpowiednich protokołów bezpieczeństwa i słabych haseł. W 2024 roku nacisk zostanie położony na poprawę bezpieczeństwa urządzeń IoT i sieci, do których się łączą.

PODSUMOWANIE

W nadchodzącym roku należy spodziewać się coraz bardziej złożonych metod działania cyberprzestępców, którzy dążą do uzyskania nielegalnego dostępu do zasobów firm i instytucji na światową skalę.
Specjaliści zaznaczają, że poziom zagrożenia wzrośnie szczególnie w przypadku **ataków na łańcuchy dostaw** oraz wykorzystania **złośliwych serwerów proxy**.

ROSNĄCY WPŁYW NA ŻYCIE SPOŁECZEŃSTWA

W nadchodzącym czasie działalność hakerów będzie miała coraz większy wpływ na **codzienne życie społeczeństwa**, obejmując aspekty takie jak prywatność, bezpieczeństwo finansowe i komunikację.

Jak wobec tego kształtować [illegible]

WZROST WYDATKÓW NA OCHRONĘ PRYWATNOŚCI DANYCH I ZABEZPIECZANIE CHMURY

W segmencie bezpieczeństwa chmury przewiduje się, że łączne wydatki na oprogramowanie **CASB** (*Cloud Access Security Broker*) i platformy **CWPP** (*Cloud Workload Protection Platform*) osiągną w 2024 roku **7 miliardów dolarów**. Prognozowany jest także wzrost zapotrzebowania na rozwiązania dedykowane wykrywaniu i reagowaniu na podejrzane aktywności, takie jak **EDR** (*Endpoint Detection and Response*) oraz **MDR** (*Managed Detection and Response*).

OCHRONA POPRZEZ ŁATANIE LUK I UWIERZYTELNIANIE WIELOSKŁADNIKOWE

Decydującym aspektem efektywnej strategii obronnej jest **wykrywanie i eliminacja luk w zabezpieczeniach**, które stanowią główny punkt ataków. Równie ważne pozostaje **stosowanie uwierzytelniania wieloskładnikowego**, które zmusza cyberprzestępców do poszukiwania innych metod ataku, co tworzy dodatkową przeszkodę dla niepożądanych działań.

ŹRÓDŁA

1. CEI America -Top 11 Trends in Cybersecurity For 2024
   https://www.ceiamerica.com/blog/top-11-trends-in-cyber-security-for-2024/
2. Cisco Talos - Incident Response Quarterly Report (Q2 2023)
3. CyberMadeInPoland - Polski rynek cyberbezpieczeństwa 2023-2028
4. Cyberpolicy NASK - Cyberbezpieczeństwo AI. AI w cyberbezpieczeństwie.
5. Cybersecurity Ventures - 2022 Official Cybercrime Report
6. Cybertalk.org - Five Dangerous Cyberattacks you should expect in 2023
7. Fortinet Cyberthreat Predictions for 2024
8. Gartner Unveils Top Eight Cybersecurity Predictions for 2023-2024
   https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-unveils-top-8-cybersecurity-predictions-for-2023-2024
9. Google Cloud Cybersecurity Forecast 2024
10. KPMG - Barometr cyberbezpieczeństwa. Detekcja i reakcja na zagrożenia w czasie podwyższonego alertu
11. KPMG - Monitor Transformacji Cyfrowej Biznesu 2023
12. Marr Bernard, The 10 Biggest Cyber Security Trends In 2024 Everyone Must Be Ready For Now, Forbes
    https://www.forbes.com/sites/bernardmarr/2023/10/11/the-10-biggest-cyber-security-trends-in-2024-everyone-must-be-ready-for-now/?sh=73f43dd85f13
13. Microsoft Digital Defense Report 2023
14. Polska Agencja Rozwoju Przedsiębiorczości - Raport o stanie sektora małych i średnich przedsiębiorstw w Polsce
15. Polska Izba Informatyki i Telekomunikacji - Trendy w branży teleinformatycznej
16. Proofpoints 2024 Predictions
    https://www.proofpoint.com/us/blog/ciso-perspectives/proofpoints-2024-predictions-brace-impact
17. Top Cybersecurity Trend Predictions for 2024: BeyondTrust Edition
18. VirusTotal Empowering Defenders: How AI is shaping malware analysis

DANE KONTAKTOWE

Net Complex sp. z o.o.

ul. Wita Stwosza 5
43-300 Bielsko-Biała

(33) 816-04-11

www.netcomplex.pl
biuro@netcomplex.pl