CYBEREKSPRESS

Borys Braun-Walicki – SMYK

Kluczowe zdarzenia

Cyberatak na CISA (Cybersecurity and Infrastructure Security Agency) gdzie agencja została zhackowana w lutym 2024 i zmuszona do przejścia w offline 2 systemów odpowiadających za ocenę ryzyka cyberbezpieczeństwa oraz bezpieczeństwa fizycznego. Atakujący wykorzystali podatność w Ivanti Connect Secure VPN oraz Ivanti Policy Secure products.

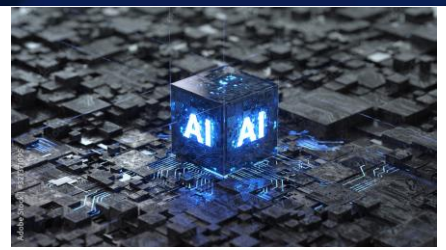
Cyberatak na BofA (Bank of America) gdzie bank został zaatakowany Ransomware i wyciekło 57000 rekordów danych osobowych. Co ciekawe atak nastąpił w listopadzie a sprawa ujrzała światło dzienne dopiero w styczniu 2024 kiedy informacje były przesyłane o ataku do klientów.

Największe wycieki danych w 2024 roku w Europie:

	Organisation name	Sector	Country	Known number of records breached	Month
1	Far Eastern Research Center for Space Hydrometeorology (Planeta)	Public	Russia	2 PB	January
2	IPL Consulting	IT services and software	Russia	>60 TB	January
3	Moscow International Higher Business School	Education	Russia	27,915,905	January
4	Vauxhall Motors Ltd	Manufacturing	UK	5,500,000	January
5	Cross Switch S.à.r.l.	Charity and non-profit	Luxembourg	3,600,000	January
6	Schneider Electric	Energy	France	“terabytes” of data	January
7	BeatBase ApS	IT services and software	Denmark	1,648,030	January
8	JD Sports Fashion	Retail	UK	1,493,344	January
9	Microbe&Lab	Healthcare	Netherlands	1,285,279	January
10	Stemcor Global Holdings Limited	Retail	UK	1.2 TB	January

Top 3 Trendy w IT Security na 2024

1. Large-scale Social Engineering Attacks
2. Insider Threats
3. Misconfiguration-based Threats



Ataki z wykorzystaniem AI w 2024

1. Przyspieszenie ataków: Średni czas od przełamania zabezpieczeń do przeniesienia się przez przeciwnika z początkowo skompromitowanego hosta na inny w obrębie organizacji wynosił zaledwie 62 minuty w 2023 roku, w porównaniu z 84 minutami w poprzednim roku. Najkrótszy zarejestrowany czas to zaledwie 2 minuty i 7 sekund
2. Interaktywne włamania: Wzrosła o 60% liczba interaktywnych włamań w 2023 roku, a 75% ataków wykorzystywanych do uzyskania początkowego dostępu nie korzystało z złośliwego oprogramowania. Przeciwnicy coraz częściej wykorzystują bardziej subtelne i skuteczne metody, takie jak phishing uwierzytelnieniowy, rozpylanie haseł i inżynieria społeczna.
3. Ataki w chmurze: W miarę jak organizacje przenoszą swoje operacje do chmury, przeciwnicy szybko rozwijają umiejętności wykorzystywania luk w ochronie. W 2023 roku odnotowano 75% wzrost w atakach w chmurze. Przeciwnicy wykorzystywali techniki oparte na tożsamości, aby uzyskać dostęp, utrzymać się i eskalować uprawnienia w środowiskach chmurowych.
4. Rozwój generatywnej sztucznej inteligencji: AI będzie prawdopodobnie wykorzystywane do działań cybernetycznych w 2024 roku, gdyż jej popularność nadal rośnie. Istnieje potencjał zakłócenia globalnych wyborów, ponieważ w 2024 roku zaplanowano ponad 40 demokratycznych wyborów, co daje przeciwnikom państwowym i eCrime wiele okazji do zakłócenia procesu wyborczego lub wpłynięcia na opinię wyborców.

Znaczące podatności Styczeń/Luty 2024

1. Wykryto krytyczne podatności w FortiOS.
2. Microsoft Patch Tuesday w lutym Microsoft wydał 73 łatki bezpieczeństwa, w tym dwie aktywnie wykorzystywane podatności zero-day (Outlook oraz Microsoft Dynamics Business Central).
3. Android Security Bulletin, w którym opisano podatności dotyczące urządzeń z systemem AndroidKrytyczna podatność w komponencie System mogła prowadzić do zdalnego wykonania kodu bez dodatkowych uprawnień.
4. Ivanti ujawniło podatności w swoich bramach Connect Secure i Policy Secure.
5. Atlassian zgłosiło wiele podatności w swoich produktach, w tym Confluence Data Center i Server, podatności Stored XSS oraz podatności DoS.

Dziękuję z uwagę ☺

Borys Braun-Walicki – SMYK