

# ZROZUMIEĆ

C

Y

B

E

R

B

E

Z

P

I

E

C

Z

E

Ń

S

T

W

O



DANE, RAPORTY I ANALIZY

ADAM TROJAŃCZYK

© Copyright by Adam Trojańczyk  
Wszelkie prawa zastrzeżone  
All rights reserved  
Wydanie I  
Łódź 2022

---

Zespół redakcyjny: Maciej Sielecki  
Korekta: Marta Trywiańska  
Zdjęcia w książce pochodzą z serwisu Unsplash.com

#### Zdjęcia:

Marek Piwnicki – <https://unsplash.com/@marekpiwnicki>  
Niclas Illg – <https://unsplash.com/@nicklbaert>  
Behnam Norouzi – [https://unsplash.com/@behy\\_studio](https://unsplash.com/@behy_studio)  
Anne Nygård – <https://unsplash.com/@polarmermaid>  
Luba Ertel – <https://unsplash.com/@ertelier>  
Clint Patterson – <https://unsplash.com/@cbpsc1>  
Maximalfocus – <https://unsplash.com/@maximalfocus>  
Lorenzo Herrera – <https://unsplash.com/@lorenzoherrera>  
Lennon Cheng – <https://unsplash.com/@lennonzf>

#### Kontakt z autorem:

e-mail: [adam@trojanczyk.pl](mailto:adam@trojanczyk.pl)  
[www.trojanczyk.pl](http://www.trojanczyk.pl)

---

Autor i eksperci dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor i eksperci nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce. Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

# Spis treści

Zrozumieć cyberbezpieczeństwo Dane, raporty i analizy.....	1
O autorze.....	5
Wstęp.....	6
Cyberataki na porządku dziennym.....	7
Czym jest cyberatak.....	8
Jak często dochodzi do ataków.....	8
Jak sytuacja wygląda w Polsce.....	9
Najpopularniejsze rodzaje cyberataków.....	10
Malware.....	11
DoS i DDoS.....	12
MITM (Man-in-the-middle).....	13
Phishing.....	15
Ransomware.....	16
Wybrane cyberataki w latach 2020-2022.....	19
Jaką cenę przychodzi nam płacić za ataki w cyberprzestrzeni.....	20
Rok 2020.....	21
Microsoft.....	22
Marriott International.....	22
Estée Lauder.....	23
MGM Resorts.....	24
Zoom.....	24
EasyJet.....	25
Uniwersytet Kalifornijski w San Francisco.....	25
Twitter.....	26
Garmin.....	27
CWT.....	28
Software AG.....	28
SolarWinds.....	29
Rok 2021.....	31
CD Projekt.....	32
Microsoft Exchange.....	32
CNA Insurance.....	33
Facebook.....	34
Drużyna NBA – Houston Rockets.....	34
Colonial Pipeline.....	35
JBS.....	36

AXA .....	36
Kaseya.....	37
Log4j .....	38
Rok 2022.....	39
Crypto.com .....	40
Bernalillo County, Nowy Meksyk .....	40
NVIDIA.....	41
Kojima, Denso i Bridgestone .....	42
Microsoft .....	43
Shields Health Care Group .....	43
Rząd Kostaryki.....	44
Centrum Medyczne Baptistów.....	45
Trendy związane z cyberbezpieczeństwem .....	46
Trendy na najbliższe lata nie są takie oczywiste .....	47
Zwiększona świadomość.....	48
Geotargetowane zagrożenia phishingowe .....	49
Uczenie maszynowe .....	49
Podatność Internetu rzeczy (IoT).....	50
Eksploity w łańcuchu dostaw.....	51
Ataki na oprogramowania low-code, no-code .....	51
Wzrost znaczenia usług chmurowych.....	52
Konieczność wprowadzenia regulacji .....	53
Zakończenie.....	54
Słowo końcowe.....	55
Źródła.....	56

## O autorze



Z branżą IT jestem związany od 2004 roku. Przez ten czas pracowałem z dziesiątkami firm z USA, Europy, z największymi agencjami interaktywnymi w Polsce, a także przedsiębiorstwami z różnych zakątków świata takich jak: Japonia, Australia czy Meksyk. W międzyczasie zarządzałem także swoim software house’em oraz miałem przyjemność współtworzyć wiele startupów i angażować się w ich rozwój.

Gdybym miał określić się jednym zdaniem, powiedziałbym, że jestem inżynierem i humanistą wierzącym, że technologia oraz startupy mogą pomóc zmienić świat na lepsze.

Obecnie pełnię funkcję członka zarządu i COO w Inwedo – software house’ie specjalizującym się w tworzeniu indywidualnych rozwiązań informatycznych dla firm. Byłem mentorem i ekspertem w programach akcelerycyjnych Startup Spark i S5 (jeden z pierwszych akceleratorów technologii 5G w Polsce) oraz miasta Łodzi, uczelni wyższych i fundacji AIP. Pełniłem także funkcję członka rady naukowej Technikum Automatyki i Robotyki, byłem doradcą ds. startupów dla Central European Startup Awards, finalistą jednego z konkursów tej organizacji oraz zdobywcą wyróżnienia Ecosystem Hero of The Year. Moje firmy zdobyły prawie dwadzieścia nagród i nominacji, w tym nagrodę Mocni w Biznesie.

Jestem także członkiem zarządu głównego i sekretarzem Polskiego Stowarzyszenia Chorych na Hemofilię.

Pisząc ten e-book, dołożyłem wszelkich starań, by treść zawarta w nim, była odpowiednia dla każdego, kto pragnie zrozumieć, jak ważne jest cyberbezpieczeństwo w biznesie. Poprzez przykłady, dane i analizy pokazuję, jak drobne zaniedbania mogą prowadzić do ogromnych problemów z funkcjonowaniem naszych biznesów, ale także uderzyć w nasze życie prywatne. Nie jestem ekspertem z zakresu cyberbezpieczeństwa. Jestem praktykiem biznesowym, który zdaje sobie sprawę, jak ważne jest położenie odpowiedniego nacisku na kwestie bezpieczeństwa organizacji.

Gdybyście po zakończonej lekturze mieli jakieś pytania – zapraszam Was do kontaktu. Zazwyczaj odpowiadam następnego dnia.

# Wstęp

Przedsiębiorstwa, organizacje, rządy, a także sektor publiczny coraz bardziej się ucyfrawiają. Zespoły stają się rozproszone, a praca zdalna sprawia, że wiele naszych zasobów znajduje się poza tradycyjnymi (fizycznymi) granicami. Możemy z poziomu laptopa zarządzać firmą, kontaktować się z ludźmi z całego świata, a nasze komputery domowe stały się centrami dowodzenia, z których porozmawiamy np. z lekarzem, ubezpieczycielem, nauczycielem czy załatwimy sprawę w urzędzie bez wychodzenia z domu.

Dzięki nowoczesnym rozwiązaniom cyfrowym nasza praca oraz życie prywatne stają się coraz lepsze i łatwiejsze. Możemy dziś snuć opowieści o tym, jak technologia pomaga ludziom rozwijać się. Niestety, jak na większość dobrych historii przystało, również w tej pojawić się muszą czarne charaktery, które będą starały się wykorzystać rzeczy dobre, by obrócić je przeciwko ludzkości.

Mowa o przestępcach i terrorystach, którzy wykorzystują nowoczesną technologię, aby bezlitośnie atakować firmy, organizacje, instytucje rządowe, wojsko czy osoby prywatne. Robią to głównie w celu pozyskania danych i użycia ich przeciwko ich właścicielom, atakowania ważnych systemów czy infrastruktur, kradzieży pieniędzy, niszczenia sprzętów, a w skrajnych przypadkach pozbawiania życia. Dzieje się tak, gdy ataki dotyczą np. systemów opieki zdrowotnej, służb pierwszej pomocy czy oprogramowania wykorzystywanego w środkach transportu.

Zagrożenia, które jeszcze kilkanaście lat temu wydawały się istnieć jedynie w sferze rozważań teoretycznych, teraz stały się jak najbardziej realne.

Do napisania tej publikacji natchnęła mnie książka pt. Cyberbroń i wyścig zbrojeń. Mówią mi, że tak kończy się świat. Pozycja ta znacząco wpłynęła na moje postrzeganie technologicznej rzeczywistości, mimo że przecież i tak w pełni rozumiałem, jak wielkie zagrożenie niesie za sobą technologia. Książka *Cyberbroń i wyścig zbrojeń* to efekt siedmiu lat dziennikarskiego śledztwa. Jej treść stanowi sygnał ostrzegawczy, że zarówno nasze życie, jak i obecna cywilizacja mogą zależeć od jakości mechanizmów obronnych w cyberprzestrzeni.

Dziękuję Maciejowi Sieleckiemu, który pomógł mi usystematyzować wiedzę i przygotował m.in. listę ataków z lat 2020-2022.



# Cyberataki na porządku dziennym

*„Pięciu najbardziej skutecznych cyberobrońców to: przewidywanie, edukacja, wykrywanie, reagowanie i odporność”*

*Stéphane Nappo*

# Czym jest cyberatak

Cisco definiuje cyberatak jako złośliwą i celową próbę naruszenia przez osobę lub grupę osób systemu informatycznego innej osoby lub organizacji. Zazwyczaj atakujący szuka jakiegoś rodzaju korzyści z zakłócenia pracy (sieci) ofiary. Inna organizacja, Checkpoint, określa cyberatak jako atak przeprowadzony przez przestępców wykorzystujący jeden lub więcej komputerów przeciwko jednemu lub wielu komputerom lub sieciom. Poprzez cyberatak oszust może w złośliwy sposób wyłączyć komputery, wykraść dane lub wykorzystać zaatakowany komputer jako punkt, który posłuży do kolejnych ataków. Cyberprzestępcy stosują różne metody przeprowadzania cyberataków, między innymi poprzez złośliwe oprogramowanie, phishing, ransomware czy ataki kryptologiczne.

## Jak często dochodzi do ataków

Z badania przeprowadzonego przez adiunkta wydziału Clark School Uniwersytetu Maryland Michaela Cukiera wynika, że komputery są hakowane średnio dwa tysiące dwieście czterdzieści cztery razy dziennie. Do przestępstwa w cyberprzestrzeni dochodzi co trzydzieści dziewięć sekund. Inne dane dotyczące cyberataków również nie napawają optymizmem. Okazują się, że:

- ponad trzydzieści trzy miliardy rekordów zostanie skradzionych przez cyberprzestępców do 2023 roku, co stanowić będzie wzrost o 175% w stosunku do roku 2018,
- według IBM / Ponemon Institute średni całkowity koszt naruszeń danych w 2021 roku w Stanach wyniósł 4,24 mln dolarów,
- koszty naruszenia danych w branży opieki zdrowotnej w USA wyniosły średnio 9,23 mln dolarów,
- 43% ataków, wedle raportu Accenture, jest skierowanych w stronę małych i średnich przedsiębiorstw, z których tylko 14% jest przygotowanych do obrony,
- 82% organizacji przebadanych przez VMware obawia się, że jest podatnych na cyberatak, ponadto raport wykazał, że 49% organizacji nie ma wiedzy i narzędzi do odpowiedniego reagowania na tego typu incydenty.



Gdy czytamy o ogromnej ilości włamań i naruszeń, może się wydawać, że zagrożenia wykrywane są w krótkim czasie. Jednak badanie przeprowadzone przez IBM i Ponemon Institute pokazuje, że jest zupełnie inaczej.

*Zidentyfikowanie, że doszło do jakiegokolwiek zagrożenia, zajmuje średnio dwieście sześć dni, a średni czas potrzebny do opanowania sytuacji wynosi siedemdziesiąt trzy dni.*

Długi czas reakcji to dopiero początek problemów, ponieważ cyberprzestępczość ma wpływ na organizację przez wiele lat po ataku. Koszty z nim powiązane – sprawy sądowe, większe ubezpieczenie, dochodzenia w sprawach karnych czy zła prasa – mogą szybko wyeliminować firmę z rynku. Wedle danych zgromadzonych przez Hiscox, pojedynczy cyberatak kosztuje firmę średnio 200 000 dolarów, a wiele przedsiębiorstw nim dotkniętych wypada z rynku w ciągu sześciu miesięcy od incydentu.

## **Jak sytuacja wygląda w Polsce**

Spoglądając w polski „Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku” z lipca 2022 roku, który został wydany przez Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, możemy zauważyć, że w 2021 roku zarejestrowano siedemset sześćdziesiąt dwa tysiące sto siedemdziesiąt pięć zgłoszeń związanych z cyberbezpieczeństwem. Daje to ponad trzykrotnie więcej naruszeń niż w roku poprzednim. Spośród wszystkich zgłoszeń zarejestrowano 26809 incydentów, które podzielono na kategorie. Najwięcej z nich przydzielono do kategorii „zagrożenie spowodowane wirusem komputerowym”, na drugim miejscu znalazły się przestępstwa z kategorii „podatności w systemach”, a na trzecim z kategorii „ataki socjotechniczne”, tj. phishing. Warto także wspomnieć, że najwięcej incydentów, w liczbie 9096, dotyczyło operatorów infrastruktury krytycznej RP.



# Najpopularniejsze rodzaje cyberataków

*„Gdyby liczyło się tylko bezpieczeństwo, komputery nigdy nie byłyby włączane, a co dopiero podłączane do sieci z dostównie milionami potencjalnych intruzów”*

*Dan Farmer*

Istnieje wiele odmian cyberataków, które zdarzają się w dzisiejszym świecie. Część z nich są jeszcze w fazie projektowania. Takim cyberatakiem może być np. przekształcenie złośliwego oprogramowania w dane przechowywane w fizycznych niciach syntetycznego DNA (Tak! Ktoś modyfikuje DNA, by zhakować maszynę, która je czyta). Inne bardzo niebezpieczne, ale występujące z niewielką częstotliwością, zagrożenie to np. deepfake, a także bardziej popularny phishing. Znając możliwości i rodzaje cyberataków, łatwiej będzie nam się przed nimi chronić. Rzućmy okiem, jak kształtują się najpopularniejsze z nich.

## Malware

Malware to oprogramowanie, którego zadaniem w głównej mierze jest wykorzystanie lub uszkodzenie usług, aplikacji, elementów sieci lub urządzenia. Dzieli się na kilka rodzajów:

- Wirus – najstarszy rodzaj złośliwego oprogramowania, które może kasować lub uszkadzać wszelakie dane. Wirus potrzebuje nosiciela lub nośnika, aby się rozprzestrzeniać. Najczęściej jest nim zainfekowany plik lub skrypt (np. w pliku tekstowym).
- Robak (Worm) – najczęściej występujący typ szkodliwego oprogramowania. Często mylone jest ono z wirusem, różni się od niego jednak tym, że jest w stanie rozprzestrzenić się samemu (nie potrzebuje innego pliku jako nosiciela).
- Koń Trojański (Trojan horse, Trojan) – program nazwany na cześć swojego legendarnego odpowiednika z czasów wojny trojańskiej. Jest to najczęściej plik lub program, który wydaje się / udaje, że jest godny zaufania, jednak w środku zawiera ukryty kod umożliwiający hakerowi przejęcie kontroli nad komputerem i przedostanie się za jego pośrednictwem do zabezpieczonej sieci.
- Adware – oprogramowanie, które zarzuca nas niechcianymi reklamami. Zwykle jest mniej groźne niż ww. zagrożenia i spowalnia działanie komputera. Może też poprzez reklamę zachęcać do pobrania i zainstalowania innego zainfekowanego oprogramowania.
- Spyware – oprogramowanie szpiegujące. Potajemnie zbiera informacje na temat działań użytkownika. Rejestruje dane logowania, hasła i jego aktywność w sieci. Może

wykorzystywać wbudowane albo podłączone do urządzenia akcesorium, np. kamerę lub mikrofon. Wykorzystywane jest m.in. do kradzieży tożsamości, a także oszustw bankowych czy finansowych.

- Keylogger – przechwytyje wszelkie informacje wprowadzane za pomocą klawiatury, np. hasła czy loginy.
- Ransomware – oprogramowanie, które blokuje dostęp do komputera lub uniemożliwia odczyt danych (np. poprzez techniki szyfrujące). Zdarza się, że cyberprzestępca żąda od użytkownika okupu za przywrócenie jego maszyny do stanu pierwotnego. Ataki tego typu wykorzystywała Rosja, infekując oprogramowanie do księgowości podatkowej używane przez ukraińskie firmy. Spowodowało to szkody o wartości 10 mld dolarów poprzez trwałe zaszyfrowanie komputerów.

Jak pokazują dane, malware najczęściej rozpowszechniany jest poprzez załączniki do wiadomości przychodzących pocztą elektroniczną.

*Verizon w raporcie Data Breach Investigations ujawnił, że poczta elektroniczna jest głównym narzędziem wykorzystywanym do ataków z użyciem złośliwego oprogramowania. Ponad 90% ataków zostało przeprowadzonych za pośrednictwem wiadomości e-mail.*

## DoS i DDoS

Ataki DoS (Denial of Service) i DDoS (Distributed Denial of Service) wykorzystywane są, aby aplikacja, urządzenie czy sieć zostały odcięte od użytkowników. Różnią się od siebie głównie tym, że przeprowadzane są z jednego lub wielu urządzeń jednocześnie. Celem oszusta jest doprowadzenie do przeciążenia atakowanego obiektu poprzez wysłanie dużej ilości żądań/zapytań, co skutkuje blokadą usługi.

*Kiedy kolektyw hakerów Anonymous wypowiedział Rosji cyberwojnę, wykorzystał w głównej mierze właśnie ataki DoS i DDoS. Wedle dostępnych danych pochodziły one z około 100 mln urządzeń. W ten sposób Anonymous wyłączał oficjalne strony rządowe czy uniemożliwiał korzystanie z bankowości.*

70% organizacji badanych przez Corero zgłosiło, że doświadcza od 20 do 50 ataków DDoS miesięcznie. Większość z nich kończy się całe szczęście niepowodzeniem. Mimo to, dzięki potężnym maszynom, zhakowanym i przejętym wcześniej komputerom „zwykłych” ludzi oraz specjalistycznym narzędziom, cyberprzestępcy mogą obecnie przeprowadzać ataki DDoS znacznie szybciej, ponosząc przy tym mniejsze koszty.

Raport „Threat Intelligence Report” firmy Netscout wskazuje, że częstotliwość ataków DDoS w całym Internecie w 2021 roku wzrosła o 11% w porównaniu z rokiem 2020. Jeśli chodzi natomiast o podział na części świata, to liczba ataków wzrosła o 7% w przypadku USA i aż o 479% w przypadku Ameryki Łacińskiej. Można także zaobserwować rosnący trend wykorzystywania ataków DDoS do wymuszenia okupu za zaprzestanie kolejnych ataków. W czwartym kwartale 2021 roku firma Cloudflare odnotowała 175% wzrost wolumenu ataków tego typu, w porównaniu z trzecim kwartałem. Nie ma jeszcze pełnych danych pokazujących, jak zmienił się świat w perspektywie 2022 roku.

## **MITM (Man-in-the-middle)**

Kolejną ciekawą i popularną formą cyberataku jest Man-in-the-middle (MITM). Ma on miejsce, gdy ktoś przechwytuje komunikację między dwiema stronami, do której nikt, poza zainteresowanymi, nie powinien mieć dostępu. Stosuje się go najczęściej w celu kradzieży lub uszkodzenia danych, pozyskania informacji osobistych, szpiegowania czy sabotowania komunikacji. Ataki MITM są jedną z najstarszych form cyberataku i sięgają wczesnych lat 80. ubiegłego wieku. Już wtedy informatycy szukali sposobów, aby nas przed nimi uchronić.

Głównym sposobem zabezpieczeń w Internecie stało się szyfrowanie, jednakże skuteczni napastnicy omijają je, przekierowując ruch na strony phishingowe zaprojektowane tak, aby

wyglądały na ich prawdziwe odpowiedniki (np. stronę udającą witrynę naszego banku) albo po prostu do innego miejsca, co sprawia, że wykrycie takich ataków jest niezwykle trudne. Do przekierowania ruchu mogą służyć sieci wi-fi lub fałszywe wieże telefonii komórkowej.

*Do przekierowania czy nasłuchu ruchu wykorzystuje się przede wszystkim sieci wi-fi lub ich fizyczne odpowiedniki, jednak możliwe jest również przeprowadzenie ataków MITM za pomocą fałszywych wież telefonii komórkowej.*

Ataki MITM zanotowano już w Stanach Zjednoczonych, Kanadzie i Wielkiej Brytanii. I to nie tylko ze strony przestępców, ponieważ w większości przypadków to służby tych krajów wykorzystywały fałszywe maszty do podsłuchiwania swoich obywateli. Urządzenia tego typu można łatwo znaleźć i kupić w dark necie.

Fakt, że naukowcy z Uniwersytetu Technicznego w Berlinie, ETH z Zurichu i SINTEF Digital w Norwegii odkryli błędy w protokołach sieci 3G i 4G, które umożliwiają nasłuch, także nie napawa optymizmem. Te same protokoły mają być stosowane we wdrożeniach technologii bezprzewodowych 5G.

Oprócz ataków, które wymagają od hakera, by znalazł się on blisko źródła, które chce podsłuchać, możliwe są również ataki zdalne. Cyberprzestępcy mogą łatwo poznać nasz adres IP, gdyż ten wyświetla im się, gdy np. odwiedzimy stworzoną przez nich stronę WWW lub klikamy w zaprojektowaną przez nich reklamę. Następnie, znając adres, hakerzy uzyskują dostęp do naszej sieci poprzez otwarty lub słabo zabezpieczony router. W dalszej kolejności przeskanują urządzenia w poszukiwaniu luk i możliwych punktów wejścia. Przechwycą dane, zbiorą informacje i zaczną manipulować naszymi doświadczeniami w sieci. Cały ten proces da się w pełni zautomatyzować, co oznacza, że ofiara takiego ataku nie musi być specjalnie wybranym celem – wystarczy, że sama wejdzie w nieodpowiednie miejsce w Internecie.

Atakujący mogą również zmienić ustawienia DNS dla domeny – dzięki DNS możemy wpisywać w adresie przeglądarki proste adresy WWW, a nie numery IP komputerów czy serwerów. Wówczas wchodząc na stronę WWW, w rzeczywistości połączymy się z niewłaściwym adresem IP, który dostarczył nam atakujący.

*Trudno jest znaleźć twarde dane mówiące o tym, jak wiele odbywa się ataków typu MITM. Wydany cztery lata temu raport „IBM X-Force Threat Intelligence Index” wspomina, że 35% aktywności Exploitów (programów mających na celu wykorzystanie istniejących błędów w oprogramowaniu) skupionych było na przeprowadzeniu ataków MITM.*

## Phishing

Phishing to próba zdobycia poufnych informacji, takich jak nazwy użytkownika, hasła, dane kart kredytowych lub numery ubezpieczenia społecznego (SSN) poprzez podszywanie się pod kogoś innego. Najczęściej spotykaną formą takiego ataku są wiadomości e-mail, w których oprawcy podszywają się pod firmy, np. sieci społecznościowe, banki, dostawców prądu czy kurierów i informują nas, że doszło do jakiejś nieprawidłowości. Aby ją naprawić, wystarczy wykonać jakąś czynność – najczęściej jest nią kliknięcie w przycisk (np. „Zweryfikuj swoje konto”) lub wypełnienie formularza.

*Każdego dnia w Internecie wysyłanych jest trzy miliardy czterysta mln maili phishingowych. Google i Threat Analysis Group blokuje każdego dnia około 100 mln takich wiadomości. Cała reszta (w większości) dociera do adresatów.*

Statystyki dotyczące phishingu opracowane przez Verizon mówią, że 93% udanych cyberataków rozpoczyna się od tzw. spear phishingu. Jest to działanie ukierunkowane na konkretną osobę, które wymaga odpowiedniego przygotowania, poznania ofiary i użycia wiedzy o niej przeciwko niej. Tego procesu nie da się łatwo zautomatyzować, chyba że

wykorzysta się do tego dane pochodzące z Internetu zachowań. Szerzej o IoB – pisałem w swoim artykule, który można znaleźć [tutaj](#).

Phishing należy także do najczęstszych typów ataków na mikro-, małe i średnie firmy. Cyberprzestępcy wykorzystują fałszywe wiadomości e-mail, atakując pracowników organizacji w celu uzyskania danych autoryzacyjnych, które następnie umożliwią im wniknięcie w głąb przedsiębiorstwa.

Według raportu „Cybersecurity Threat Trends” firmy Cisco około 90% naruszeń danych następuje w wyniku phishingu. 80% wszystkich zgłoszonych w 2021 roku incydentów dotyczących cyberbezpieczeństwa to także tego typu ataki.

Inne badanie przygotowane przez firmę Tessian pokazało, że pracownicy z całego świata w 2021 roku otrzymywali średnio czternaście złośliwych e-maili rocznie, a według badań firmy ESET przeprowadzonych w 2021 roku tylko między majem a sierpniem częstotliwość ataków z użyciem poczty elektronicznej wzrosła o 7,3%. Raport IBM „Cost of a Data Breach Report 2022” wykazał, że naruszenia spowodowane przez phishing kosztują organizacje średnio 4,65 mln dolarów, a według FBI z roku na rok odnotowuje się 400% wzrost tego typu ataków.

W dodatku, jak informuje Infosec, około 97% osób na świecie nie potrafi rozpoznać fałszywej wiadomości phishingowej, a jedna na dwadzieścia pięć osób klika w takie wiadomości, padając tym samym ofiarą cyberataku.

## Ransomware

Ransomware to oprogramowanie, które blokuje dostęp do komputera i plików, by umożliwić hakerowi wyłudzenie okupu za przywrócenie maszyny do stanu pierwotnego. Po włączeniu komputera jedyne, co jesteśmy w stanie zobaczyć, to ekran informujący o blokadzie oraz informacje o tym, w jaki sposób wpłacić okup. Atak polega na wykorzystaniu technik kryptograficznych, więc jeżeli staniemy się jego ofiarą, nasze pliki zostaną zakodowane i niemożliwy będzie ich odczyt bez podania odpowiedniego klucza.

Od 2000 roku cyberataki przy użyciu tej metody koncentrowały się na komputerach osobistych. Cyberprzestępcy jednak w szybkim tempie za cel wzięli również firmy, organizacje, a także



instytucje rządowe, które są w stanie zapłacić o wiele więcej za odblokowanie krytycznych systemów niż osoby prywatne.

Rok 2021 był przełomowy dla oprogramowania ransomware. Po przejściu przedsiębiorstw na pracę zdalną, a także w związku z szybką cyfryzacją i transformacją cyfrową rozpoczętą w 2020 roku za sprawą pandemii, szybko przekonaliśmy się, że organizacje nie są dobrze zabezpieczone przed zagrożeniami ze strony cyberprzestępców. Ataki cybernetyczne z użyciem ransomware spowodowały spustoszenie wśród osób i organizacji na całym świecie. Wpłynęły na zdolność ludzi do korzystania z opieki zdrowotnej, zatankowania samochodów czy nawet zrobienia zakupów. Trend użycia tego rodzaju złośliwego oprogramowania będzie rósł w nadchodzących latach. Ransomware-as-a-service (RaaS) staje się już codziennością. Minęły czasy, kiedy atakujący musiał napisać własny kod. Obecnie taki rodzaj oprogramowania można z powodzeniem kupić „na rynku” i wdrożyć za pomocą prostych instrukcji.

*Według publikacji „2021 Ransomware Study: Where You Are Matters!” firmy IDC, około 37% organizacji na całym świecie padło ofiarą ataku ransomware w 2021 roku.*

W minionym roku FBI odnotowało 62% wzrost skarg dotyczących tego typu ataków. Z kolei w lutym 2022 roku Agencja Bezpieczeństwa Cybernetycznego i Infrastruktury raportowała, że wie o incydentach ransomware w czternastu z szesnastu amerykańskich sektorów infrastruktury krytycznej. Średni czas przestoju, jakiego doświadcza firma po ataku za pomocą oprogramowania blokującego, wynosi 22 dni.

Ponieważ ataki ransomware coraz bardziej dotyczą także sektory publiczne, firma Gartner przewiduje, że państwa prawdopodobnie uchwalą przepisy dotyczące płatności okupów w przypadku zablokowania systemów.

*Gartner oszacował, że obecnie tylko 1% rządów na całym świecie posiada przepisy dotyczące ransomware. Prognozuje się, że do 2025 roku odsetek ten wzrośnie do około 30%.*

Kiedy zdamy sobie sprawę, że, jak podaje Business Insider, rekordowa wypłata dokonana przez firmę ubezpieczeniową z tytułu okupu za atak za pomocą oprogramowania blokującego wynosi 40 mln dolarów, zrozumiemy, jak poważne i realne jest to zagrożenie. Dodatkowo, jak podaje National Security Institute, średnia żądana opłata za okup wzrosła z 500 dolarów w 2018 roku do około 200 000 dolarów.

Ważne jest także określenie przepisów prawa i procedur, które mają zarówno przeciwdziałać takim próbom okupu, jak i dać obywatelom jasny sygnał, jak postępować, gdy dojdzie do incydentu tego typu. Zapłata okupu nie jest gwarancją odzyskania danych, ponieważ, jak podaje Cybereason, 80% ofiar, które zapłaciło przestępcom, wkrótce potem zostało ponownie zaatakowanych, a chociaż 46% z nich uzyskało dostęp do swoich danych, to większość była uszkodzona.



# Wybrane cyberataki w latach 2020-2022

*„Hasła są jak bielizna: nie pozwól, aby ludzie je widzieli, zmieniaj je bardzo często i nie dziel się nimi z nieznajomymi”*

Chris Pirillo

# Jaką cenę przychodzi nam płacić za ataki w cyberprzestrzeni

Zaprezentowane wcześniej dane rysują krajobraz zagrożeń oraz pokazują, jak dramatycznie zmienił się on w ciągu ostatnich lat. Praktycznie każdy sektor publiczny i prywatny jest pod ciągłym atakiem hakerów, którzy za cel wybrali sobie kradzież danych, okupy lub zakłócanie działalności organizacji czy rządów. Nie wszystkie oczywiście okazują się skuteczne. Nowoczesne technologie pozwalają coraz lepiej zabezpieczać się przed włamaniami, jednak słabym ogniwem pozostanie podatność organizacji na działania socjotechniczne i luki w projektowanym oprogramowaniu.

*Do 2025 roku cyberprzestępczość będzie kosztować świat 10,5 bln dolarów.*

Według badania „Cost of Cybercrime Study” firmy Accenture 43% cyberataków jest skierowanych na małe przedsiębiorstwa, ale tylko 14% zaatakowanych organizacji jest przygotowanych do obrony. W dodatku, jak podaje Checkpoint, średnia ilość ataków na firmy w tygodniu na całym świecie w 2022 roku wynosi 1200. Jest to wzrost o 32% w stosunku do roku poprzedniego. Sektor rządowy i wojskowy może „pochwalić się” wynikiem 1600 ataków tygodniowo (wzrost o 44%), sektor edukacji zaś 2315 (ze wzrostem 53%).

Tego, że nigdy nie możemy być pewni zabezpieczeń, spróbuję dowieść, przytaczając przykłady ataków z lat 2020-2022. Przykłady te pokazują, że najczęstszym celem cyberprzestępców są podmioty będące ogniwem w łańcuchu dostaw dla większych firm, a także sektor medyczny, z którego hakerzy wykradają nasze dane dotyczące zdrowia.

# Rok 2020

„Jak już zdążyliśmy się zorientować, pogląd, że bezpieczeństwo zaczyna się i kończy na zakupie gotowego firewalla, jest po prostu błędny”

Art Wittmann

# Microsoft

**Data:** styczeń 2020.

**Typ ataku:** wyciek danych spowodowany błędną konfiguracją serwera (data leak – server misconfiguration).

**Skutek:** wyciek 250 mln rekordów z danymi klientów.

W 2020 roku na blogu firmy Microsoft pojawiła się informacja o tym, że wewnętrzna baza danych związana z obsługą klientów wyciekła przypadkowo do sieci. Miały być to zanonimizowane dane użytkowników, które docelowo służyły ich analizie. Okazało się jednak, że treść wpisu była bardziej optymistyczna niż rzeczywistość. Baza danych (która jak się okazało, nie była nawet zabezpieczona hasłem) zawierała ponad 250 mln rekordów z danymi klientów firmy z okresu czternastu lat jej działalności.

Microsoft winą za to zdarzenie obarczył błędną konfigurację reguł bezpieczeństwa Azure z 5 grudnia 2019 roku. Wyciek ujawnił adresy e-mail, adresy IP i inne dane dotyczące klientów. Microsoft twierdzi, że w bazie nie były przechowywane żadne inne dane osobowe.

# Marriott International

**Data:** styczeń 2020 (odkryty pod koniec lutego 2020).

**Typ ataku:** kradzież danych (data breach).

**Skutek:** w wyniku ataku wyciekły dane ok. 5,2 mln hotelowych gości.

Marriott International w połowie stycznia 2020 roku został zaatakowany przez hakerów. W wyniku tego incydentu doszło do naruszenia danych, które dotknęło około 5,2 mln gości hotelowych korzystających z programu lojalnościowego Marriott Bonvoy. Marriott w odpowiedzi na atak wymusił zmianę danych logowania do kont użytkowników dotkniętych naruszeniem i zasugerował im włączenie wieloskładnikowego uwierzytelniania.

W marcu 2020 roku ogłoszono, że dostęp do bazy klientów został uzyskany poprzez użycie danych dostępowych pracowników sieci franczyzowej.

To niejedyny incydent, z jakim musiał poradzić sobie Marriott. Wycieki odnotowano także w roku 2018 (tu według źródeł mówimy o danych nawet 500 mln gości) i 2022, kiedy to hakerzy uzyskali dostęp do poufnych dokumentów biznesowych, informacji o płatnościach klientów hoteli i numerów ich kart kredytowych.

## Estée Lauder

**Data:** luty 2020.

**Typ ataku:** wyciek danych (data leak).

**Skutek:** ujawniono poufne informacje o klientach przechowywane w ponad 440 milionach rekordów.

Jeremiah Fowler, badacz bezpieczeństwa i współzałożyciel Security Discovery, natrafił w sieci na olbrzymią bazę danych należącą do firmy Estée Lauder, giganta branży kosmetycznej. Według Fowlera niezabezpieczone archiwum ujawniało poufne informacje o klientach przechowywane w ponad 440 milionach rekordów. Nie stwierdzono, aby informacje o płatnościach lub inne wrażliwe dane były niezabezpieczone, ale adresy e-mail, adresy IP i inne informacje stały się dostępne dla każdego.

Rzecznik prasowy Estée Lauder tłumaczył później, że za udostępnienie danych odpowiedzialne były błędy w zabezpieczeniach oprogramowania pośredniczącego (middleware). Mogły one umożliwić złośliwemu oprogramowaniu uzyskanie dostępu do aplikacji, danych i systemów firmy. Najprawdopodobniej baza danych była częścią platformy edukacyjnej, która nie zawierała żadnych danych konsumentów. Firma utrzymuje, że nie było żadnych dowodów na nieautoryzowane wykorzystanie danych.

## MGM Resorts

**Data:** luty 2020.

**Typ ataku:** wyciek danych (data leak).

**Skutek:** dane ponad 10,5 miliona gości hotelowych MGM Resort trafiają na forum hakerskie.

W lutym 2020 roku dane ponad 10,5 miliona gości hotelowych, którzy zatrzymali się w MGM Resorts, pojawiły się na jednym z forów hakerskich. Dane obejmowały ich nazwiska, adresy zamieszkania, numery telefonów, e-maile i daty urodzenia.

W lipcu 2020 roku osoby badające temat odnalazły sto czterdzieści dwa miliony rekordów klientów tej samej sieci wystawione na sprzedaż w dark webie. Sugeruje to, że wyciek danych był zdecydowanie większy, niż pierwotnie ogłoszono.

## Zoom

**Data:** kwiecień 2020.

**Typ ataku:** kradzież danych (data breach).

**Skutek:** w dark webie pojawiła się oferta sprzedaży danych 500 mln loginów i haseł użytkowników aplikacji Zoom.

W kwietniu 2020 roku wiele firm zmuszonych sytuacją pandemiczną na świecie przeszło na system pracy zdalnej. Przedsiębiorstwa i organizacje instalowały w związku z tym różnorakie narzędzia do komunikacji, aby pracownicy mogli pozostać ze sobą w kontakcie. Jedną z najbardziej popularnych platform do wideokonferencji był wówczas Zoom, który szybko trafił na celownik hakerów. W tym samym miesiącu w dark webie odkryto ofertę sprzedaży bazy zawierającej 500 mln loginów i haseł do aplikacji Zoom.

Ze względu na niski stopień zabezpieczeń w szybkim tempie rozpowszechniło się zjawisko włamań i zakłóceń przebiegu (teoretycznie) prywatnych konferencji. Od nazwy aplikacji zjawisko to zostało nazwane: zoombombing.



Oprócz samego ataku badacze ds. bezpieczeństwa odkryli również, że firma udostępniała dane osób korzystających z Zoomu (oczywiście bez ich zgody) Facebookowi. Wywołało to niezadowolenie użytkowników, które było podsycane również faktem, że w związku ze znaczącym wzrostem popytu na aplikację i rosnącymi kosztami jej utrzymania, ich dane zaczęły być przechowywane na serwerach w Chinach (bez wcześniejszego informowania o tym).

Zoom podjął wysiłki w celu rozwiązania wspomnianych problemów, a dyrektor generalny organizacji publicznie wziął za nie winę na siebie. W odpowiedzi na te kwestie Federalna Komisja Handlu Stanów Zjednoczonych nakazała firmie Zoom wdrożenie konkretnych i kompleksowych środków związanych ze zwiększeniem bezpieczeństwa danych.

Wskutek ataku reputacja Zoomu ucierpiała tak mocno, że niektóre organizacje zakazały swoim podwładnym używania aplikacji.

## EasyJet

**Data:** maj 2020.

**Typ ataku:** kradzież danych (data breach).

**Skutek:** wyciek danych 9 mln klientów i pozew na 18 mld funtów.

Brytyjskie linie lotnicze EasyJet w 2020 roku ogłosiły, iż padły ofiarą „wysoce zaawansowanego” cyberataku. W jego wyniku ujawnione zostały adresy e-mail i dane związane z podróżami około 9 mln klientów. Brytyjskie linie lotnicze stanęły w obliczu zbiorowego pozwu złożonego przez klientów dotkniętych ujawnionym naruszeniem danych. Jego wartość oszacowano na 18 mld funtów.

## Uniwersytet Kalifornijski w San Francisco

**Data:** czerwiec 2020.

**Typ ataku:** ransomware.

**Skutek:** okup w wysokości 3 mln dolarów.

3 czerwca 2020 roku Uniwersytet Kalifornijski w San Francisco poinformował o udanym ataku na systemy IT UCSF School of Medicine. Dwa dni wcześniej napastnicy użyli oprogramowania typu ransomware, szyfrując pliki na serwerach i uniemożliwiając do nich dostęp. Zaszifrowane pliki były danymi prac naukowych, które miały służyć dobru publicznemu. Instytucja w tym czasie pracowała m.in. nad lekiem na COVID-19. Hakerzy, powołując się na miliardowe przychody UCSF (co wiedzieli z uzyskanego wcześniej dostępu do danych finansowych), zażądali okupu w wysokości 3 mln dolarów. Uniwersytet podjął negocjacje z atakującymi, co pozwoliło na obniżenie kwoty do 1,14 mln dolarów, która ostatecznie została wypłacona w bitcoinach. Grupa NetWalker odpowiedzialna za atak została także zidentyfikowana jako sprawca ataków na co najmniej dwa inne uniwersytety w tym samym roku.

## Twitter

**Data:** lipiec 2020.

**Typ ataku:** kradzież kont (account hijacking).

**Skutek:** w wyniku „skoordynowanego ataku socjotechnicznego” na pracowników Twittera atakujący uzyskali dostęp do wewnętrznych narzędzi organizacji.

W lipcu 2020 roku hakerzy przejęli ponad 130 twitterowych kont o milionowych zasięgach. Należały one do znanych i wysoko postawionych osób, m.in. Baracka Obamy, Joe Bidena, Jeffa Bezosa, Billa Gatesa, Elona Muska, a także firm takich jak Uber czy Apple. Następnie opublikowali, podszywając się pod ofiary, tweety zawierające prośbę o wysłanie bitcoinów do określonego portfela kryptowalutowego. W zamian za wysłanie pieniędzy darczyńca miał zostać obdarowany prezentem w postaci podwojenia wpłaconej kwoty. Na ten rodzaj oszustwa nabrały się tysiące osób, które nie wiedziały, że wiadomości te nie pochodzą od znanych osobistości ani nie są akcją marketingową żadnej organizacji.

Do przejęcia kont doszło podobno w wyniku „skoordynowanego ataku socjotechnicznego” na pracowników Twittera. Atakujący uzyskali dostęp do wewnętrznych narzędzi giganta, dzięki czemu mogli samodzielnie zmienić i przejąć wybrane konta.

Trzy godziny po incydencie, Twitter poinformował, że rozwiązał problem, jednak w wyniku ataku wyłudzonych zostało ponad 100 000 dolarów. Coinbase (jedna z giełd kryptowalut) poinformowała, że dzięki umieszczeniu na czarnej liście adresów portfeli, które widniały

w fałszywych tweetach, udało zablokować się ponad tysiąc transakcji na łączną kwotę ponad 280 000 dolarów.

Dwa tygodnie po incydencie Departament Sprawiedliwości Stanów Zjednoczonych ogłosił aresztowanie trzech osób, w wieku od 16 do 22 lat, związanych z oszustwem i postawił im zarzuty.

## Garmin

**Data:** lipiec 2020.

**Typ ataku:** ransomware.

**Skutek:** żądanie 10 mln dolarów okupu.

Kilka dni po problemach, z jakimi musiał zmierzyć się Twitter, atakiem ransomware został zaskoczony producent smartwatchy Garmin. Firma musiała zablokować dostęp do kilku swoich usług, ponieważ hakerzy skierowali działania w stronę sieci firmowej, centrów telefonicznych oraz części systemów produkcyjnych. W wyniku ataku Garmin doświadczył m.in. przerwy w działaniu swojej strony internetowej oraz, co ważne, systemu odpowiedzialnego za synchronizację danych pomiędzy sprzedawanymi przez firmę akcesoriami a jej serwerami. Uniemożliwiło to klientom korzystanie z większości funkcji urządzeń oraz aplikacji. Nie mogli oni m.in. dokonać rejestracji treningów ani uzyskać dostępu do danych zdrowotnych na swoich smartwatchach lub telefonach. Piloci samolotów nie mogli zaś pobrać planów lotu, aby nawigować samolotami zgodnie z wymogami FAA.

Początkowo Garmin nie ujawnił żadnych szczegółów dotyczących incydentu, ale kilku pracowników podzieliło się informacjami na temat rzekomego ataku ransomware w mediach społecznościowych.

Według nieoficjalnych danych, za przywrócenie działania sieci i systemu żądano okupu w wysokości 10 mln dolarów, i podobno żądania te zostały spełnione, czego jednak Garmin nigdy nie potwierdził.

# CWT

**Data:** lipiec 2020.

**Typ ataku:** ransomware.

**Skutek:** 4.5 mln dolarów okupu i 30 000 zablokowanych komputerów.

Carlson Wagonlit Travel (CWT) to firma, która pomaga zarządzać podróżami służbowymi, spotkaniami, konferencjami oraz wystawami. Zajmuje piąte miejsce na liście najlepiej zarabiających firm turystycznych opublikowanej przez „Travel Weekly”.

Pod koniec lipca 2020 roku, organizacja ujawniła, że stała się celem ataku ransomware Ragnar Locker. To nowy typ ataku, który zaobserwowano po raz pierwszy pod koniec 2019 roku. Wdraża on w atakowanej sieci wirtualną maszynę z systemem operacyjnym w celu uwolnienia złośliwego oprogramowania. Jako ofiary wybiera również kopie zapasowe, powiązane z nimi narzędzia i podłączone dyski pamięci masowej i usuwa je. Typowe wektory ataku obejmują m.in. źle skonfigurowane usługi zdalnego pulpitu.

Napastnicy w trakcie ataku na CWT wykradli poufne dane, zablokowali 30 000 komputerów firmowych i zażądali około 4,5 mln dolarów okupu. Ponieważ CWT jest dostawcą usług dla 1/3 firm z listy S&P 500 (indeks giełdowy, w skład, którego wchodzi pięćset największych przedsiębiorstw notowanych na New York Stock Exchange i NASDAQ) i ujawnienie wykradzonych danych mogłoby mieć katastrofalne skutki, ostatecznie firma zdecydowała się na zapłacenie okupu.

# Software AG

**Data:** październik 2020.

**Typ ataku:** ransomware.

**Skutek:** wyciek danych i żądania okupu w wysokości 20 mln dolarów.

Software AG, niemiecka firma związana z produkcją oprogramowania (w branży – druga co do wielkości w Niemczech i siódma w Europie), padł ofiarą ataku ransomware (Clop ransomware), w wyniku którego doszło do wycieku danych. Firma ujawniła, że incydent zakłócił pracę części

jej wewnętrznej sieci, jednak nie miał wpływu na usługi świadczone klientom. Atakujący domagali się okupu w wysokości 20 mln dolarów. Firma próbowała negocjować z hakerami, ale nie przyniosło to efektów. Ostatecznie Software AG odmówił zapłaty, a w rezultacie przestępcy dotrzyмали obietnicy i opublikowali poufne dane pracowników, wewnętrzne e-maile i informacje finansowe.

## SolarWinds

**Data:** grudzień 2020.

**Typ ataku:** atak na łańcuch dostaw (supply chain attack).

**Skutek:** wpływ na międzynarodowe firmy, organizacje i agencje rządowe.

SolarWinds to firma programistyczna, która dostarcza m.in. narzędzia do zarządzania systemami oraz monitorowania sieci i infrastruktury dla tysięcy organizacji na całym świecie. By pozyskiwać dane z logów oraz informacje o wydajności, narzędzia monitorujące SolarWinds mają szeroki dostęp do systemów IT. Ze względu na uprzywilejowaną pozycję i ogromną bazę klientów SolarWinds stał się atrakcyjnym celem dla cyberprzestępców. Przez zhakowanie oprogramowania produkowanego przez firmę, które następnie trafiło do jej klientów, hakerzy w szybkim tempie otrzymali dostęp do tysięcy organizacji.

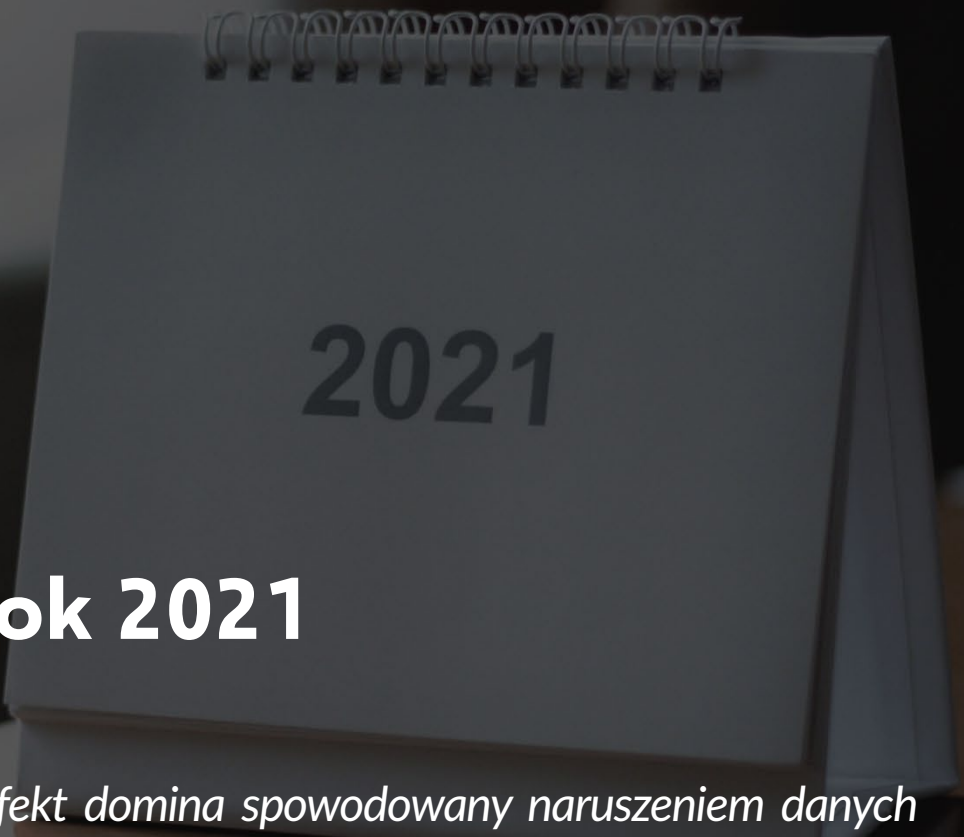
Według raportów złośliwe oprogramowanie dotknęło m.in. amerykańskie departamenty rządowe, w tym Departamenty Handlu, Skarbu, Stanu czy Bezpieczeństwa Krajowego, a także prywatne firmy takie jak Microsoft, Intel, Cisco czy Deloitte.

Atak został wykryty w grudniu 2020 roku, gdy firma FireEye zajmująca się cyberbezpieczeństwem potwierdziła, że została zainfekowana złośliwym oprogramowaniem. Taki sam rodzaj infekcji odkryła w systemach swoich klientów. Microsoft również potwierdził, że znalazł oznaki złośliwego oprogramowania w własnych systemach.

Atakującym oprogramowanie SolarWinds była grupa UNC2452 sponsorowana przez rząd rosyjski (nation-state actor). Mimo że jej poczynania zostały odkryte w grudniu 2020 roku, wewnątrz śledztwo wykazało, że pierwsze włamanie do sieci dostawcy oprogramowania miało miejsce jeszcze w styczniu 2019 roku. Szacuje się, że od początku marca 2019 roku, wadliwe aktualizacje zostały pobrane przez 18 000 klientów.

Zakres ataku, jego złożoność i długi czas, który upłynął do momentu wykrycia sprawiają, że jest on uważany za największy atak roku 2020 (niektórzy twierdzą, że jest to największy atak tej dekady), a zdarzenie pokazuje, jak niebezpieczne mogą być ataki na łańcuchy dostaw.

Cel włamania pozostaje nadal nieznany. Można domniemywać, że hakerzy chcieli dostać się do systemu organizacji, w tym otrzymać dostęp do planów rozwojowych, informacji o pracownikach czy klientach. Nie jest też jeszcze jasne, jakie informacje, jeśli w ogóle, hakerzy wykradli z agencji rządowych. Tego pewnie nigdy się nie dowiemy.

A desk calendar for the year 2021. The calendar is white with a silver spiral binding at the top. The year '2021' is printed in a large, bold, black font in the center of the calendar page. The calendar is standing on a dark surface, and the background is dark and out of focus.

2021

## Rok 2021

*„Efekt domina spowodowany naruszeniem danych może być dla firmy niszczący. Kiedy klienci zaczynają przenosić swoje interesy – i swoje pieniądze – gdzie indziej, może to być prawdziwy cios”*

*Christopher Graham*

## CD Projekt

**Data:** luty 2021.

**Typ ataku:** ransomware.

**Skutek:** kradzież kodów źródłowych gier wideo.

W lutym 2021 roku CD Projekt Red, znany polski wydawca oraz producent gier komputerowych padł ofiarą grupy hakerskiej o nazwie HelloKitty. Hakerzy podczas ataku uzyskali dostęp i wykradli kody źródłowe gier, zarówno ukończonych (tj. Cyberpunk 2077, Wiedźmin 3: Dziki Gon, Gwint: Wiedźmińska gra karciana), jak i tych będących w fazie rozwoju, a także dokumentów księgowych, danych administracyjnych i wielu innych. Dodatkowo przestępcy zaszyfrowali dane na serwerach za pomocą ransomware. CD Projekt posiadał kopie zapasowe, które nie zostały naruszone, dzięki czemu koderom udało się zabezpieczyć infrastrukturę IT. CD Projekt nie zapłacił szantażystom.

## Microsoft Exchange

**Data:** marzec 2021.

**Typ ataku:** wykorzystanie podatności (vulnerabilities exploitation).

**Skutek:** ogromne wycieki danych i ujawnianie ostępów do kont użytkowników.

W marcu 2021 roku świat obiegła informacja, że jedna z największych korporacji na świecie, Microsoft, została zaatakowana przez grupę Hafnium sponsorowaną przez chiński rząd (nation-state actor).

Microsoft poinformował o znalezionych w swoim oprogramowaniu lukach, które rzutowały na systemy pocztowe i kalendarzowe Exchange Server dla korporacyjnych oraz rządowych centrów danych. Braki w zabezpieczeniach dały napastnikom pełny dostęp do wiadomości e-mail oraz haseł użytkowników, uprawnienia administratora na zaatakowanym serwerze oraz dostęp do podłączonych urządzeń w tej samej sieci. Okazało się, że odkryte wady sięgały dziesięciu lat wstecz i według oficjalnych danych były wykorzystywane przez chińskich hakerów co najmniej od stycznia 2021 roku.



Microsoft bardzo szybko wydał aktualizację swojego oprogramowania w celu załatwienia znalezionych dziur, jednak niestety nie udało się za jego pomocą cofnąć szkód ani usunąć backdoorów zainstalowanych przez atakujących.

Hakerzy obrali za cel zdobycie informacji od kontrahentów obronnych, szkół i innych podmiotów w Stanach Zjednoczonych i na świecie. Po powiadomieniu opinii publicznej o błędach i w czasie prac nad naprawą luk co najmniej dziesięć innych grup advanced persistent threat zaczęło wykorzystywać poznane braki w zabezpieczeniach w celach szpiegowskich.

Wkrótce parlament Norwegii, zgłosił, że padł ofiarą włamania. Europejski Urząd Nadzoru Bankowego również poinformował, że był celem takiego ataku. Kilka dni później Microsoft Security Intelligence ogłosiło, że zaatakowane wcześniej serwery zostały ponownie zainfekowane: „nową rodziną ransomware” o nazwie DearCry. Zawartość przejętych urządzeń została zaszyfrowana, czyniąc serwery bezużytecznymi. Następnie z wykorzystaniem tych samych luk zaatakowano firmę Acer, której wykradziono dane i zażądano okupu w wysokości 50 mln dolarów.

## CNA Insurance

**Data:** marzec 2021.

**Typ ataku:** ransomware.

**Skutek:** wyciek danych siedemdziesięciu 5000 pracowników, zaszyfrowane dane i okup w wysokości 40 mln dolarów.

CNA Insurance to jedno z największych towarzystw ubezpieczeniowych w Stanach Zjednoczonych. Atakujący włamali się do firmowej sieci i zaszyfrowali dane znajdujące się na piętnastu tysiącach urządzeniach, w tym także używanych podczas pracy zdalnej. W wyniku ataku wyciekły dane osobowe siedemdziesięciu 5000 pracowników (byłych i aktualnych) i numery ich ubezpieczeń społecznych.

Media ujawniły, że firma zgodziła się zapłacić okup w wysokości 40 mln dolarów.

# Facebook

**Data:** kwiecień i wrzesień 2021.

**Typ ataku:** wyciek danych (data leak).

**Skutek:** hakerzy uzyskali dostęp do danych ponad 533 mln użytkowników portalu.

W 2021 roku doszło do jedno z największych ataków typu data leak. W sieci znalazły się dane ponad 533 mln użytkowników portalu Facebook ze 106 krajów, w tym także Polski. Mimo upływu czasu nadal można je znaleźć i pobrać z GitHuba lub grup w serwisie Telegram.

Wyciek danych dotyczył informacji takich jak: imiona i nazwiska, daty urodzenia, aktualne miejsca zamieszkania, posty i zdjęcia zamieszczane w serwisie, zainteresowania, reakcje i wielu innych informacji, które umożliwiają sprofilowanie osoby.

W trakcie dochodzenia okazało się, że użyta przez przestępców luka bezpieczeństwa istniała od 2019 roku i to wtedy najpewniej doszło do pierwszego wycieku, o którym to firma nikogo nie poinformowała.

W połowie września 2021 roku doszło do kolejnego wycieku danych organizacji. Tym razem były to dokumenty obejmujące wewnętrzne badania wpływu Instagrama na zdrowie psychiczne nastolatków. Z akt wynikało, że Instagram jest szkodliwy dla dużej części młodych użytkowników, szczególnie nastolatków.

# Drużyna NBA – Houston Rockets

**Data:** kwiecień 2021.

**Typ ataku:** ransomware.

**Skutek:** wyciek 500 GB poufnych danych.

W połowie kwietnia grupa hakerska o nazwie Babuk poinformowała o wykradzeniu 500 GB poufnych danych drużyny NBA Huston Rockets. Hakerzy odpowiedzialni za atak reklamują siebie jako zewnętrzną firmę audytorską, która wykrada dane z korporacji. Jeśli te zostaną ocenione jako kompromitujące, żąda pieniędzy za utrzymanie ich w tajemnicy.

Ujawnione miały zostać dane o kontraktach zawodników, personalia, umowy o zachowaniu poufności oraz informacje finansowe. Notka pozostawiona przez hakerów informowała, że upublicznienie danych: „mogłyby doprowadzić firmę do problemów prawnych i wywołać niepokój u klientów”. Klub Houston Rockets postanowił rozwiązać sprawę, współpracując z FBI, a końcowe szkody okazały się nie tak poważne, jak początkowo się obawiano.

## Colonial Pipeline

**Data:** kwiecień/maj 2021.

**Typ ataku:** ransomware.

**Skutek:** zatrzymanie dostaw paliwa na Wschodnim Wybrzeżu Stanów Zjednoczonych.

Firma Colonial Pipeline, która dostarcza około 45% paliwa na Wschodnim Wybrzeżu Stanów Zjednoczonych, odkryła, że padła ofiarą ransomware. Grupa DarkSide włamała się do systemów firmy, wykradła 100 GB danych i zainfekowała komputery. Udało się to dzięki wcześniejszemu wyciekowi danych dostępowych do VPN organizacji (najprawdopodobniej poprzez osobiste hasło jednego z pracowników firmy znalezione w dark webie).

W wyniku ataku ucierpiała korporacyjna sieć IT Colonial Pipeline, natomiast sprzęt i oprogramowanie, które sterują fizycznymi urządzeniami dostawcy, procesami i zdarzeniami pozostały nienaruszone. Mimo to z ostrożności firma zdecydowała jednak się na tymczasowe wyłączenie systemów zarządzających rurociągami, aby mieć pewność, że infekcja nie rozprzestrzeni się na kolejne środowiska. Poskutkowało to zatrzymaniem dostaw paliwa na całym Wschodnim Wybrzeżu Stanów Zjednoczonych (w sumie 12 stanów).

Hakerzy zażądali okupu, a CEO Colonial Pipeline ostatecznie autoryzował zapłatę w wysokości 4,4 mln dolarów w bitcoinach w celu przywrócenia systemów. Dzięki staraniom Departamentu Sprawiedliwości, odzyskano około 2,3 mln dolarów.

## JBS

**Data:** maj 2021.

**Typ ataku:** ransomware.

**Skutek:** 11 mln dolarów okupu.

JBS to brazylijska firma zajmująca się przetwórstwem mięsnym. Jest trzecim co do wielkości przedsiębiorstwem tego typu na świecie.

JBS odkrył włamanie, gdy zespół IT znalazł nieprawidłowości w części wewnętrznych systemów. Po skontaktowaniu się z FBI i ekspertami ds. bezpieczeństwa, firma zaczęła wyłączać systemy, aby spowolnić atak. W wyniku działań hakerów unieruchomione zostały ubojnie, a skutki dotknęły obiekty w Stanach Zjednoczonych, Kanadzie i Australii. W obliczu ryzyka utraty danych JBS zapłacił hakerom z rosyjskiej grupy REvil okup w wysokości 11 mln dolarów (co jest jednym z najwyższych opłaconych okupów za ransomware w historii).

## AXA

**Data:** maj 2021.

**Typ ataku:** ransomware.

**Skutki:** kradzież danych i wpływ na działania firmy na Filipinach, w Hong Kongu, Malesji i Tajlandii.

Europejski ubezpieczyciel AXA został zaatakowany po opublikowaniu zmian w polisie ubezpieczeniowej dotyczącej cyberprzestrzeni. Zmiany dotyczyły zaprzestania wypłat dla klientów AXA za szkody związane z cyberatakami. Grupa Avaddon, której ewidentnie taka decyzja nie była na rękę, wykradła 3 TB wrażliwych danych, co wpłynęło na działania firmy AXA na Filipinach, w Hong Kongu, Malesji i Tajlandii. Dodatkowo zaobserwowano zmasowany atak DDoS przeciwko globalnym stronom internetowym AXA.

Według hakerów kompromitujące dane uzyskane przez Avaddon dotyczyły raportów medycznych klientów (ujawniały diagnozy związane ze zdrowiem seksualnym), kopii dowodów osobistych, wyciągów z kont bankowych, formularzy roszczeń, umów i innych dokumentów.

AXA ogłosiła, że specjalny zespół z zewnętrznymi ekspertami kryminalistycznymi zbadał atak, a partnerzy biznesowi i regulatorzy zostali o nim poinformowani. Oficjalnie AXA nie ujawniła żadnych innych skutków i rodzaju cyberataku.

## Kaseya

**Data:** czerwiec 2021.

**Typ ataku:** ransomware / supply chain attack.

**Skutek:** żądanie okupu w wysokości 70 mln dolarów.

Po atakach na JBS i Colonial Pipeline ta sama grupa hakerów, używając tego samego narzędzia, zaatakowała dostawcę oprogramowania do zdalnego monitorowania i zarządzania rozbudowaną infrastrukturą IT Kaseyę.

Atak na firmę składał się z dwóch części. W pierwszej kolejności przestępcy wykorzystali lukę w oprogramowaniu Kaseya VSA, co dało im dostęp do serwerów organizacji. Serwery te zostały użyte w drugiej fazie operacji do rozpowszechnienia złośliwego oprogramowania wśród klientów tejże firmy (dane mówią o 1500 zaatakowanych).

Udany atak stał się dla oszustów podstawą, by skierować wobec firmy żądanie 70 mln dolarów – najwyższej w historii kwoty ogłoszonej za okup. Kaseya poinformowała wszystkich klientów o problemie i wyłączyła centra danych na czas prowadzenia dochodzenia.

Był to już kolejny głośny atak tego typu, co zmusiło prezydenta USA Joe Bidena do ostrzeżenia prezydenta Rosji, że Stany Zjednoczone będą działać na własną rękę przeciwko najgorszym gangom hakerskim operującym na rosyjskiej ziemi. Kaseya w niedługim okresie opracowała uniwersalny klucz deszyfrujący i uniknęła płacenia przestępcom. Wywołało to spekulacje, że amerykańskie agencje zhakowały rosyjską grupę REvil.

# Log4j

**Data:** czerwiec 2021.

**Typ ataku:** atak zero-day, remote code execution vulnerability.

**Skutek:** możliwość całkowitego przejścia kontroli nad systemami.

Log4j to popularne narzędzie open source, które zbiera dane diagnostyczne z aplikacji napisanych w języku Java. W czerwcu 2021 roku okazało się, że w jego zabezpieczeniach znajduje się krytyczna luka, która może być wykorzystana przez hakerów do atakowania systemów. Luka pozwalała na zdalne wykonanie kodu i całkowite przejście kontroli nad systemem. Biblioteka Log4j wykorzystywana była w zatrważającej ilości aplikacji czy usług wykorzystywanych przez takie firmy, jak Microsoft, Twitter, VMware, Amazon czy Apple.

Wkrótce po ujawnieniu luki w zabezpieczeniach odnotowano masowe skanowania Internetu w celu jej wykorzystania. Firma Check Point Software Technologies będąca notowanym na giełdzie dostawcą usług cyberbezpieczeństwa ujawniła, że zablokowała ponad 800 000 prób ataków związanych z wykorzystaniem luki w bibliotece. Określiła także występującą lukę jako jedną z najpoważniejszych w ostatnich latach. Apache Software Foundation, która odpowiada za rozwój Log4j, bardzo szybko wydała łatkę usuwającą lukę.



20  
22

# Rok 2022

*„Internet rzeczy (IoT) pozbawiony kompleksowego zarządzania bezpieczeństwem jest równoznaczny z Internetem zagrożeń”*

*Stephane Nappo*

# Crypto.com

**Data:** styczeń 2022.

**Typ ataku:** kradzież danych (data breach).

**Skutek:** poszkodowani stracili łącznie ok. 34 mln dolarów.

W środę 19 stycznia 2022 roku CEO Crypto.com Kris Marszalek potwierdził naruszenie bezpieczeństwa kont serwisu. 483 użytkowników aplikacji związanej z giełdą kryptowalut stało się ofiarami włamania. Jak możemy przeczytać w oficjalnym komunikacie firmy, nieautoryzowane wypłaty wyniosły 4836,26 eterów (11,14 mln funtów), 443,93 bitcoinów (13,7 mln funtów) oraz około 66,2 tys. dolarów (48 638,45 tys. funtów). Część okupu wypłat dokonano w innych walutach.

CEO firmy potraktował ten błąd jako bardzo ważną lekcję, która w niedalekiej przyszłości przyniosła zmiany w infrastrukturze, a także wzmocnienie dwustopniowej autentykacji użytkowników.

Rynki kryptowalut stają się coraz bardziej kuszące, szczególnie w efekcie rosnącej inflacji część osób szuka tam wybawienia dla swoich finansów. Mimo to inwestycja w kryptowaluty nadal budzi obawy ankietowanych co jakiś czas konsumentów, szczególnie ze względu na niezrozumiałe i ogromne wahania notowań. Dodatkowo, jeżeli spojrzymy na Raport Crystal Blockchain, możemy zauważyć, że w 2021 roku skradziono kryptowaluty o wartości ponad 4 mld dolarów, co stanowi prawie trzykrotnie więcej niż w 2020 roku.

# Bernalillo County, Nowy Meksyk

**Data:** styczeń 2022.

**Typ ataku:** ransomware.

**Skutek:** odcięcie pracowników hrabstwa od baz rządowych oraz przejęcie kontroli nad systemami bezpieczeństwa więzienia.

Na początku roku 2022 największe hrabstwo w Nowym Meksyku odkryło, że padło ofiarą ataku złośliwego oprogramowania ransomware. Hakerzy uniemożliwi pracę kilku wydziałom



hrabstwa oraz biuram rządowym, odcinając ich pracowników od dostępu do rządowych baz danych. Nie ucierpiała cała szczęście infrastruktura krytyczna.

Wydarzenie to wzbudziło niepokój społeczny, co dodatkowo spotęgował fakt, że w lokalnym MDC, czyli metropolitalnym areszcie śledczym ransomware wyłączył kamery bezpieczeństwa i automatyczne drzwi. Więźniowie musieli zostać zamknięci w swoich celach. Brak kontroli nad systemem elektronicznego zarządzania więzieniem zmusił placówkę do ograniczenia przemieszczania się skazanych, co stanowiło potencjalne naruszenie warunków przetrzymywania więźniów.

## NVIDIA

**Data:** luty 2022.

**Typ ataku:** ransomware.

**Skutek:** wyciek 1 TB danych.

Jeden z największych na świecie producentów procesorów graficznych i innych układów scalonych przeznaczonych na rynek komputerowy został zaatakowany przez oprogramowanie ransomware w lutym 2022 roku. Dane z zainfekowanych maszyn, które zawierały w sobie zastrzeżone informacje, a także te uwierzytelniające pracowników, zaczęły pojawiać się w Internecie. Do ataku przyznała się grupa Lapsus\$, która publicznie potwierdziła, że uzyskała dostęp do 1 TB danych.

W zamian za odblokowanie komputerów hakerzy żądali, aby NVIDIA usunęła wprowadzoną funkcję uniemożliwiającą wydobywanie kryptowalut (Lite Hash Rate) ze swoich nowych kart graficznych, a także udostępniła kod źródłowy swoich sterowników na licencji open source.

NVIDIA szybko zareagowała na ransomware, wzmacniając swoje zabezpieczenia i natychmiast angażując ekspertów, aby opanować sytuację. Niektóre serwisy informacyjne sugerują nawet, że NVIDIA rzekomo: „zhakowała hakera”, namierzając członków grupy Lapsus\$ i infekując ich systemy. Ta informacja nie została oficjalnie potwierdzona. NVIDIA nie potwierdziła tych domysłów i nie odniosła się do nich w swoim oświadczeniu. Zgodnie z obecnym prawem USA hakowanie hakerów jest nielegalne.

Sprawcy ataku poinformowali, że wykradli ponad 70 000 adresów e-mail pracowników i haseł, a także informacje o jeszcze nieogłoszonych procesorach, SDK i kodzie źródłowym GPU.

## Kojima, Denso i Bridgestone

**Data:** luty/marzec 2022.

**Typ ataku:** ransomware.

**Skutek:** wpływ ataku na możliwości produkcyjne firmy.

Na przełomie lutego i marca zaatakowanych zostało trzech dostawców z branży motoryzacyjnej. Gdy pierwszy z nich, Kojima Industries, dostarczający elementy karoserii i wnętrza samochodów, został dotknięty cyberatakiem, musiał wstrzymać pracę w swoich 14 japońskich zakładach. Serwisy internetowe poinformowały, że atak spowodował spadek miesięcznych możliwości produkcyjnych firmy o 5%. Jedenaście dni później dwóch kolejnych dostawców, Denso i Bridgestone, również padło ofiarą ataków ransomware.

Denso jest firmą z listy Fortune 500, która dostarcza komponenty samochodowe dla Toyoty, Forda, Hondy, Mercedes-Benz, Volvo, Fiata i General Motors. Posiada ponad 200 filii na całym świecie i zatrudnia ponad 168 000 pracowników. Do ataku przyznała się grupa Pandora, która zagroziła wyciekiem tajemnic dostawcy motoryzacyjnego, informacji o transakcjach, zamówieniach, schematów technicznych części samochodowych oraz e-maili.

Bridgestone, największy producent wyrobów gumowych i opon na świecie, doświadczył zaś ataku powodującego wyłączenie sieci komputerowych i zakładów produkcyjnych w Ameryce Środkowej i Północnej. Odpowiedzialność za ten atak wzięt na siebie LockBit.

# Microsoft

**Data:** marzec 2022.

**Typ ataku:** ransomware.

**Skutek:** ograniczony dostęp do Cortany, Binga i kilku innych produktów.

Hakerzy skompromitowali serwery usługi DevOps Microsoftu i eksfiltrowali z nich kody źródłowe kilku produktów korporacji. Wyciek nie dotyczył jednak oprogramowania na komputery osobiste, takiego jak Microsoft Windows czy Microsoft Office. Dotknął jedynie infrastruktury sieciowej, stron internetowych i aplikacji mobilnych.

Atakującym okazała się grupa Lapsus\$, która to pochwaliła się, że otrzymała dostępy do Cortany, Binga i Bing Maps. Microsoft stwierdził, że posiadanie kodu nie przyniosłoby hakerom korzyści, nawet gdyby udało im się do niego dostać. Wedle firmy bezpieczeństwo organizacji nie polega na zapewnieniu, aby kod źródłowy był tajny, a jego przeglądanie nie prowadzi do podniesienia ryzyka wycieku danych.

Kilka dni po incydencie Microsoft ogłosił, że problem włamania szybko udało się rozwiązać i że żadne dane klientów nie zostały skradzione. Firma, śledząc wcześniejsze przypadki ataków Lapsus\$, np. na NVIDIĘ, była przygotowana na próbę złamania zabezpieczeń serwerów.

# Shields Health Care Group

**Data:** marzec 2022.

**Typ ataku:** kradzież danych (data breach).

**Skutek:** wykradzione dane medyczne dwóch mln pacjentów.

Shields Health Care Group, niezależny dostawca usług medycznych, padł na początku roku ofiarą włamania. W jego wyniku wykradzione zostały dane 2 mln pacjentów, a naruszenie bezpieczeństwa miało wpływ na 56 placówek opieki zdrowotnej i ich leczących się tam osób.

W oświadczeniu, firma poinformowała, że dowiedziała się o ataku 28 marca i zaraz po tym incydencie zatrudniła specjalistów z dziedziny cyberbezpieczeństwa w celu określenia jego zakresu.

Okazało się, że hakerzy posiadali dostęp do systemów organizacji od 7 do 21 marca, co pozwoliło im na potencjalny wgląd do danych pacjentów, które obejmowały: imiona i nazwiska, numery ubezpieczenia społecznego, daty urodzin, adresy zamieszkania, informacje o świadczeniach, informacje o ubezpieczeniach zdrowotnych, a także dostęp do dokumentacji medycznej. Sprawa skończyła się pozwem zbiorowym ze strony osób poszkodowanych.

## Rząd Kostaryki

**Data:** kwiecień i maj 2022.

**Typ ataku:** ransomware.

**Skutek:** wydarzenia te pokazały, w jaki sposób możliwe jest sparaliżowanie całego kraju za pomocą stosunkowo prostego ataku. Oprócz tego atakujący zażądali od rządu okupu w wysokości 20 mln dolarów.

17 kwietnia 2022 roku rozpoczął się atak ransomware przeciwko prawie 30 instytucjom rządu Kostaryki. Dotknięte przestępstwem zostały m.in.: Ministerstwo Finansów, Ministerstwo Nauki, Ministerstwo Innowacji, Ministerstwo Technologii, Ministerstwo Telekomunikacji, Ministerstwo Pracy i Ubezpieczeń Społecznych, a także Narodowy Instytut Meteorologiczny, państwowy dostawca usług internetowych, Fundusz Ubezpieczeń Społecznych, Fundusz Rozwoju Społecznego i Zasiłków Rodziny oraz Zarząd Administracyjny Miejskiej Służby Elektrycznej.

O wydarzeniu stało się bardzo głośno, gdyż był to pierwszy przypadek w historii, kiedy kraj ogłosił stan wyjątkowy w odpowiedzi na cyberatak. W wyniku ataku sparaliżowane zostały usługi rządowe, ale także sektor prywatny zajmujący się importem/eksportem.

Do ataku przyznała się grupa Conti, jednocześnie żądając zapłaty okupu w wysokości 10 mln dolarów. Z czasem kwota została podwojona. Atak odbił się rykoszetem także na systemach podatkowych i budżecie kraju, przez co około 16 000 pracowników sektora publicznego nie dostało wynagrodzenia lub ich pensję źle naliczono. Dziesiątki osób wyszły na ulice w ramach protestów.

Kolejny atak przypadł na końcówkę maja i tym razem pogrzyżył w chaosie system opieki zdrowotnej kraju oraz fundusz ubezpieczeń społecznych. Niestety tym razem dotknął on

bezpośrednio zwykłych Kostarykańczyków, ponieważ spowodował zablokowanie systemów opieki zdrowotnej w kraju. Departament Stanu USA zaoferował nagrodę w wysokości 10 mln dolarów dla każdego, kto dostarczy informacje, które doprowadzą do identyfikacji liderów grupy hakerskiej odpowiedzialnej za atak.

## Centrum Medyczne Baptistów

**Data:** kwiecień 2022.

**Typ ataku:** malware.

**Skutek:** dostęp do wrażliwych danych 1,24 mln pacjentów.

Cyberataki nie omijają szpitali. W kwietniu bieżącego roku, w wyniku ataku z użyciem złośliwego oprogramowania, uzyskano nieautoryzowany dostęp do wrażliwych danych 1,24 mln pacjentów dwóch teksańskich szpitali – Baptist Medical Center w San Antonio i Resolute Health Hospital w New Braunfels. Wykradzione pliki zawierały wyczerpujące informacje, takie jak: imiona i nazwiska, daty urodzenia, adresy zamieszkania, numery i szczegóły ubezpieczenia społecznego pacjentów i inne dane medyczne – numery kartotek, daty i nazwy dostawców usług i placówek, gdzie je wykonywano, główne dolegliwości lub powody wizyt pacjentów, a także inne informacje dotyczące określonych procedur i diagnoz. Wykradzono również dane o rozliczeniach czy roszczeniach i wiele innych.

Ataki na placówki medyczne stają się coraz bardziej niebezpieczne. Kiedy spojrzymy na statystyki [Departamentu Zdrowia i Usług Społecznych w Stanach Zjednoczonych](#) możemy zobaczyć, że praktycznie nie ma dnia bez wycieku danych osobowych pacjentów. Zebrane informacje wskazują, że tego typu regularne wycieki dotyczą od 500 do 3 500 000 osób tylko w Stanach Zjednoczonych (stan na koniec października 2022 roku). Skala zjawiska jest więc bardzo niepokojąca.



# Trendy związane z cyberbezpieczeństwem

*„Zaufanie do technologii to dobra rzecz, ale jej kontrola jest lepsza”*

*Stéphane Nappo*

# Trendy na najbliższe lata nie są takie oczywiste

Cyberprzestępczość rośnie na całym świecie. Można wręcz odnieść wrażenie, że złoczyńcy w większości przypadków pozostają bezkarni. Państwa tworzą własne grupy uderzeniowe lub zatrudniają hakerów, by atakować infrastruktury krytyczne innych krajów lub wyciągać dane od największych potentatów technologicznych. Wykradane dane medyczne także służą wywiadowi do definiowania zagrożenia.

Napięcia geopolityczne będą miały coraz większy wpływ na cyberprzestrzeń. Coraz częściej będą pojawiać się konflikty pomiędzy hakerami różnych państw. Nawet jeśli liczba ataków wydaje się nieznacząca, w rzeczywistości może mieć ogromny wpływ na ważne dla wydarzenia, takie jak np. wybory. Wraz z trwającymi konfliktami możemy spodziewać się głośnych naruszeń danych i ujawniania tajemnic politycznych i przemysłowych, przeciwdziałanie którym znajdzie się na szczycie listy trendów związanych z cyberbezpieczeństwem w nadchodzących miesiącach.

Oprócz tego należy mieć na uwadze, że przyspieszona cyfryzacja organizacji, a także coraz większa liczba urządzeń IoT będą jednymi z najważniejszych aspektów wpływających na trendy w cyberbezpieczeństwie w najbliższych latach. Rosnąca ilość ataków zmusi firmy do wdrażania systemów wykrywania zagrożeń opartych na sztucznej inteligencji, które będą mogłyby przewidywać nowe zagrożenia i natychmiast powiadamiać administratorów o naruszeniach danych. To pewnie z kolei wymusi ataki hakerów na te właśnie systemy.

Spróbujmy głębiej zanurzyć się w ciekawą przyszłość i rzucić okiem na trendy nadchodzących lat.

# Zwiększona świadomość

Według raportu Cyber Observer 80% naruszeń danych mogłoby nie mieć miejsca, gdyby firmy i organizacje zachowały i praktykowały higienę cybernetyczną. Świadomość konieczności zabezpieczania naszych urządzeń i systemów jest niezbędna, aby zapobiec kosztownej kradzieży danych i tożsamości, włamaniom do sieci czy naruszeniom łańcuchów dostaw.

Tradycyjne podejście do szkoleń z zakresu świadomości bezpieczeństwa w sieci jest nieskuteczne. Dane mówią same za siebie – 95% incydentów związanych cyberbezpieczeństwem jest spowodowanych przez błąd ludzki. Organizacje na całym świecie muszą więc przemyśleć swoje strategie dotyczące tej kwestii. Firma Gartner w swoich materiałach wskazuje, że wystarczą trzy działania, aby zwiększyć skuteczność programów podnoszących świadomość, jak ważne jest cyberbezpieczeństwo. Te trzy kroki to:

1. ustalenie wizji – za pomocą wielofunkcyjnej grupy roboczej składającej się z przedstawicieli całej organizacji,
2. zdefiniowanie mierzalnych, pożądaných zachowań – najlepiej za pomocą metryk opartych na wynikach (outcome-driven metrics),
3. powiązanie pożądaných zachowań z wymiernymi korzyściami biznesowymi – zaczynając od mierzenia podstawowych przyczyn zagrożeń cybernetycznych generowanych przez człowieka, których eliminacja przyniesie natychmiastową korzyść.

Gartner zachęca także do tego, aby organizacje nieustannie rozmawiały o możliwych niebezpieczeństwach, a także modyfikowały wykorzystywane przez siebie technologie, aby zawsze były one dostosowane do nowych, nadchodzących zagrożeń. Namawia także do pozostawiania decyzji dotyczących zagrożeń cybernetycznych jednostkom biznesowym, bo to one mają największą wiedzę, która może pomóc poprawić stan bezpieczeństwa organizacji.



# Geotargetowane zagrożenia phishingowe

Ataki typu geo-targeted phishing stały się bardzo popularne w 2022 roku. Mimo regularnych prób przeciwdziałania temu zjawisku, jakich podejmują się dostawcy poczty i systemów zabezpieczeń, skala ataków za pomocą tej metody nie maleje. Przewiduje się, że w najbliższych latach jeszcze bardziej zyskają one na popularności.

Hakerzy uderzać będą w organizacje czy osoby prywatne za pomocą dobrze ukierunkowanych działań. Będą wykorzystywać geolokalizację użytkowników, która posłuży im do automatycznego tworzenia niestandardowych wiadomości (e-mail, SMS) czy stron internetowych. Następnie będą mogli wyłudzać informacje lub zainfekować urządzenia za pomocą oprogramowania ransomware zaprojektowanego specjalnie na dany region.

## Uczenie maszynowe

Uczenie maszynowe jest podzbiorem sztucznej inteligencji. Wykorzystuje do działania stosunkowo proste algorytmy powstałe dzięki analizie istniejących już zbiorów danych. W przypadku cyberbezpieczeństwa takim zbiorem mogą być np. dane informujące o zachowaniach maszyny/komputera podczas ataku. Poprzez ich analizę algorytmy nauczą się wychwytywać potencjalne ataki, rozpoznawać ich typ, a także na nie reagować. Każde kolejne możliwe źródło niebezpieczeństwa będzie z kolei uzbrajać algorytmy w kolejne funkcje, do których wcześniej nie zostały zaprogramowane i będą one mogły adaptować się do zmian na bieżąco.

Podobnie będzie z potencjalnie niebezpiecznymi plikami – tymi, których zwykły antywirus nie uzna za zagrożenie, a które mogą być np. plikami programów ransomware. Dzięki uczeniu maszynowemu algorytm wykryje taki plik, a system zajmie się nim, zanim zdąży dokonać spustoszenia.

Uczenie maszynowe jest już wykorzystywane do skanowania podatności sieci i automatyzacji reakcji na ataki. Uczenie maszynowe jest wybawieniem, jeżeli chodzi o cyberbezpieczeństwo

i w kolejnych latach będzie wykorzystywane coraz częściej. Należy jednak pamiętać, że nie wystarczy patrzeć na dane historyczne, by przewidzieć to, co przyniesie nam przyszłość. Nie można nauczyć się wszystkiego tylko z suchych danych.

## **Podatność Internetu rzeczy (IoT)**

Internet rzeczy odnosi się do obiektów fizycznych, które są (lub mogą być) podłączone do Internetu i komunikują się wzajemnie ze sobą. Urządzenia te wykonują określone akcje, zbierają informacje, a następnie analizują je lokalnie lub wysyłają na zewnątrz, np. do chmury obliczeniowej. Firmy będące producentami tych urządzeń prowadzą za pomocą danych zebranych przez urządzenia szeroko pojętą analitykę. Dzięki temu, że nasza pralka jest podłączona do Internetu, firma, która ją zaprojektowała, może określić, z których programów korzystamy najczęściej i na tej podstawie tworzyć coraz bardziej dopasowane do naszych potrzeb modele kolejnych pralek. W ten sposób powstają także lodówki, które analizują, czego w nich brakuje i podpowiadają, co powinniśmy zamówić czy opaski na nadgarstek ze wskazówkami treningowymi. IoT stale się rozwija, a gromadzone i udostępniane przez urządzenia dane (BI, big data, CDP itp.) dostarczają np. cennych informacji o zachowaniach, zainteresowaniach i preferencjach ich użytkowników. Szacuje się, że do 2025 roku wartość branży IoT wyniesie 6,2 mld dolarów.

Rosnąca popularność urządzeń działających w IoT, stosunkowo krótki czas zapewniania wsparcia w postaci aktualizacji ich oprogramowania, a także ogromna ilość pieniędzy na rynku w tym sektorze stały się niektórymi z przyczyn ataków na IoT. W następnych latach możemy spodziewać się wzmożonych prób włamań, szukania podatności na ataki w oprogramowaniu lub protokołach komunikacyjnych właśnie takich urządzeń.

Atak na Internet rzeczy daje także możliwość całkowitego przejęcia urządzenia, które w nim działa. Może to skutkować podsłuchiowaniem wszystkiego, co dzieje się w otoczeniu posiadacza sprzętu będącego w sieci lub służyć do wykradania za jego pomocą informacji z sieci lokalnej. Zhakowane urządzenia (np. kamery) mogą służyć następnie jako punkty startowe kolejnych ataków, w tym ataków na systemy bezpieczeństwa organizacji. Przez wiele lat temat ten był pomijany w debatach publicznych. Dopiero w 2022 roku Unia Europejska przedstawiła

koncepcję Cyber Resilience Act – mającą na celu ustanowienie wspólnych standardów cyberbezpieczeństwa dla urządzeń podłączonych do sieci.

## **Eksploity w łańcuchu dostaw**

Opisany przeze mnie wcześniej atak na SolarWinds z 2020 roku był jednym z pierwszych ataków na łańcuchy dostaw, które przeprowadzono, wykorzystując zbudowane pomiędzy organizacjami relacje. Firmy bazujące na ogromnym wzajemnym zaufaniu wypracowały między sobą symbiozę, co zostało wykorzystane przez hakerów. Zaatakowali oni mniejszą organizację, zainfekowali ją i w ten sposób dostali się do niczego nieświadomej większej.

W najbliższych latach możemy spodziewać się ataków na zaufanych kontrahentów, kontraktorów, sprzedawców czy klientów, poprzez których dojdzie do kolejnych cyberprzestępstw w sieci partnerskiej. Będą to najprawdopodobniej ataki na istniejące oprogramowanie, wstrzykiwanie złośliwego oprogramowania do tego, które jest aktualnie tworzone albo przejęcia kont użytkowników i poprzez wiadomości phishingowe uderzenia w inne firmy.

Także biblioteki oparte na otwartym kodzie i wykorzystywane w systemach IT staną się jeszcze atrakcyjniejszym celem ataków hakerów. Dzięki infekcji biblioteki, przy próbie aktualizacji oprogramowania korporacyjnego, atakujący uzyskają dostęp do jej środowiska.

## **Ataki na oprogramowania low-code, no-code**

Platformy oferujące rozwiązania low-code i no-code mają symbolizować wizualne podejście do tworzenia oprogramowania i umożliwiać automatyzację niemal każdego etapu życia aplikacji poprzez szybkie dostarczanie użytkownikom różnorodnych rozwiązań. Platformy te zapewniają nie tylko kod czy skrypty, ale także systemy integracyjne. Dzięki temu firmy mogą prototypować, budować i skalować aplikacje bez opracowywania skomplikowanych infrastruktur.

Wyobraźmy sobie, że ww. platforma jest swego rodzaju integratorem. Loguje się do jednego systemu, wyciąga z niego dane, umieszcza je w innym, wykonuje operacje, a następnie informuje o swoich działaniach członka działu.

Brak wykwalifikowanych programistów w połączeniu ze wzmożonymi potrzebami ze strony biznesu dotyczącymi transformacji cyfrowej spowodował, że tego typu platformy programistyczne mocno zyskały na popularności. Obecnie wykorzystywane są głównie do projektowania i wdrażania baz, interfejsów użytkownika, projektowania procesów oraz automatyzacji. Ich głównym zadaniem jest skracanie czasu potrzebnego na ręczne wykonywanie działań. Niektóre dane mówią o tym, że do 2024 roku aplikacje low-code będą odpowiadać za ponad 65% działań związanych z tworzeniem oprogramowania.

61% organizacji wprowadziło lub planuje wprowadzić aktywne inicjatywy na rzecz low-code, by w szybki sposób użytkownicy biznesowi mogli tworzyć swoje aplikacje. Istotą no-code i low-code jest zmniejszenie zapotrzebowania na tradycyjnych programistów. Dzięki temu przy minimalnym lub zerowym przeszkoleniu z zakresu kodowania błyskotliwa osoba będzie mogła tworzyć nowe funkcje w oprogramowaniu.

Przez takie oprogramowanie przebiegają miliardy różnorodnych danych, ponieważ korzystają z niego setki tysięcy firm na całym świecie. Ataki na oprogramowanie low-code mogą dać hakerom potencjalny dostęp do przechowywanych przez te organizacje zasobów informacji. Jeśli zostanie ono zainfekowane, może wstrzyknąć złośliwy kod do innego oprogramowania, z którym użytkownicy będą próbowali się zintegrować.

## **Wzrost znaczenia usług chmurowych**

Chmury obliczeniowe od lat cieszą się ogromną popularnością. Dzięki swojej uniwersalności i stosunkowo niskiemu progowi wejścia, mają coraz więcej zwolenników. Chmury to w rzeczywistości fizyczna sieć połączonych ze sobą serwerów. Przechowują one dane, służą do wykonywania obliczeń, oferują wiele usług, do których użytkownik ma do dostęp za pomocą połączenia internetowego. Szacuje się, że do 2025 roku w chmurze będzie przechowywanych ponad 100 zettabajtów danych (jeden zettabajt to miliard terabajtów).

Coraz więcej organizacji wybierać będzie technologie chmurowe ze względu na zaawansowane rozwiązania dotyczące bezpieczeństwa i mechanizmów obronnych. Rozwiązania chmurowe nie są tak podatne na ataki z użyciem ransomware jak standardowe maszyny, głównie ze względu na specyfikę tworzenia kopii zapasowych.

## Konieczność wprowadzenia regulacji

Firma Gartner przewiduje, że do końca 2025 roku 30% państw na całym świecie przyjmie ustawy i przepisy, które będą regulowały kwestie płacenia okupów żądanych przez hakerów. Chodzi szczególnie o ataki ransomware, w przypadku których łączne kwoty sięgają już kilkunastu milionów dolarów. Firmy ubezpieczeniowe coraz częściej odmawiają wypłacania odszkodowań, które miałyby zostać przekazane jako zapłata w celu odblokowania zainfekowanych maszyn. Jest to o tyle istotne, że firmy i organizacje powinny jak najszybciej podjąć decyzje związane ze zwiększeniem odporności używanych przez siebie systemów komputerowych na ataki z zewnątrz oraz wprowadzić politykę zwiększania świadomości w kwestii cyberbezpieczeństwa wśród swoich pracowników. To szczególnie ważne, ponieważ badanie przeprowadzone przez HP wskazuje, że siedmiu na dziesięciu pracowników używa komputerów służbowych do celów prywatnych. Prawie tyle samo używa swoich prywatnych komputerów do celów biznesowych podczas pracy zdalnej. Dodatkowo trzech na dziesięciu pracowników pozwala innym osobom korzystać z ich urządzenia służbowego.

Na koniec warto zauważyć, że coraz więcej menadżerów wysokiego szczebla patrzy na cyberbezpieczeństwo jako kwestię związaną z zarządzaniem ryzykiem. Przewiduje się, że w ciągu najbliższych trzech lat 70% prezesów będzie wdrażać w swoich organizacjach kulturę odporności organizacyjnej. Będzie ona wspierać firmy głównie w dążeniu do przetrwania zagrożeń pochodzących z sieci, ale także niepokojów społecznych czy niestabilności politycznej.

A vibrant, futuristic city street at night. The scene is dominated by a cool blue and purple color palette. In the foreground, tram tracks run down the center of a wet, reflective pavement. A tram with glowing red lights is visible in the distance. The street is lined with tall buildings, some with digital billboards and advertisements. One billboard on the right features a woman's face and the text 'L'ÉRO' and 'MORBA'. Another on the left says 'CAP' and 'WINTER IS IN THE CITY'. The sky is dark, punctuated by numerous small, colorful lights (red, purple, blue) that create a sense of depth and atmosphere. The overall mood is one of a high-tech, cybernetic urban environment.

# Zakończenie

*„W świecie cyberbezpieczeństwa ostatnią rzeczą, jakiej pragniesz, jest posiadanie namalowanego na sobie celu”*

*Tim Cook*

# Słowo końcowe

Siadając do tej publikacji, postawiłem przed sobą cel, aby w prosty sposób przedstawić dane, raporty i założenia związane z cyberbezpieczeństwem. Chciałem, aby pozycja ta przyczyniła się do realnej zmiany naszego nastawienia do cyberzagrożeń.

Wraz z rozwojem urządzeń mobilnych, IoT, mediów społecznościowych, chmury obliczeniowej i analityki big data cyberbezpieczeństwo zyskuje coraz większą uwagę – zarówno naszą, jak i przestępców.

Zaprezentowane przykłady włamań i wycieków danych z ostatnich lat pokazują, że do ataku może dojść nawet tam, gdzie zupełnie się tego nie spodziewamy. Chwila nieuwagi może prowadzić do nieodwracalnych zmian, utraty pieniędzy, reputacji, pracy czy skutkować nawet wielomilionowymi pozwami.

Przedsiębiorstwa, organizacje, startupy, instytucje publiczne i osoby prywatne muszą opracować kompleksowe strategie bezpieczeństwa i skutecznie je wdrożyć, aby nie ponosić druzgocących strat w wyniku cyberataków. Zwiększanie świadomości zagrożeń jest jedną z dróg, jakie powinniśmy obrać.

Jeżeli spodobały Ci się treści w tej publikacji oraz widzisz w nich wartość, możesz wspomóc to, co robię, wpłacając dowolną sumę pieniędzy na konto Polskiego Stowarzyszenia Chorych na Hemofilię lub przekazując 1% podatku. Wszystkie fundusze zostaną przeznaczone na działalność statutową stowarzyszenia, m.in: pomoc osobom chorym na hemofilię, organizowanie obozów i wyjazdów rehabilitacyjnych, zakup sprzętu rehabilitacyjnego do szpitali, organizowanie warsztatów dla chorych, wydawanie publikacji na temat hemofilii i innych skaz krwotocznych. Dane znajdziesz poniżej. Dziękuję.

Polskie Stowarzyszenie Chorych na Hemofilię

KRS: 0000169422

ul. I. Gandhi 14

02-776 Warszawa

Numer konta: 06 2030 0045 1110 0000 0245 3030

# Źródła

<https://www.helpnetsecurity.com/2020/04/01/marriott-data-breach-2020/>  
<https://www.forbes.com/sites/thomasbrewster/2018/11/30/marriott-admits-hackers-stole-data-on-500-million-guests/>  
<https://www.theverge.com/2022/7/6/23196805/marriott-hotels-maryland-data-breach-credit-cards>  
<https://www.theguardian.com/business/2020/may/19/easyjet-cyber-attack-customers-details-credit-card>  
<https://www.zdnet.com/article/easyjet-faces-18-billion-class-action-lawsuit-over-data-breach/>  
<https://cloudsecurityalliance.org/blog/2022/03/13/an-analysis-of-the-2020-zoom-breach/>  
<https://www.forbes.com/sites/daveywinder/2020/06/29/the-university-of-california-pays-1-million-ransom-following-cyber-attack/>  
<https://blocksandfiles.com/2020/08/18/ucsf-ransomware-attack-data-protection/>  
<https://www.mitnicksecurity.com/blog/2020-garmin-ransomware-attack>  
<https://www.globesign.com/en/blog/cyber-autopsy-series-great-twitter-attack-2020>  
[https://en.wikipedia.org/wiki/2020\\_Twitter\\_account\\_hijacking](https://en.wikipedia.org/wiki/2020_Twitter_account_hijacking)  
[https://en.wikipedia.org/wiki/CWT\\_\(company\)](https://en.wikipedia.org/wiki/CWT_(company))  
<https://www.securitymagazine.com/articles/92986-us-carlson-wagonlit-travel-pays-a-45m-ransom-to-get-its-data-back>  
<https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020>  
<https://www.embroker.com/blog/cyber-attack-statistics/>  
<https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/>  
<https://www.varonis.com/blog/cybersecurity-statistics>  
<https://www.unisys.com/glossary/cyber-attack/>  
<https://legaljobs.io/blog/cybersecurity-statistics/>  
<https://www.phonexia.com/blog/most-common-cybercrime-types-to-be-aware-of-in-2022/>  
<https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks>  
<https://www.csoonline.com/article/3340117/man-in-the-middle-attack-definition-and-examples.html>  
<https://www.crowdstrike.com/cybersecurity-101/man-in-the-middle-mitm-attacks/>  
<https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/>  
<https://purplesec.us/resources/cyber-security-statistics/>  
<https://easydmarc.com/blog/phishing-statistics-easydmarc-report-january-june-2022/>  
<https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts>  
<https://dataprot.net/statistics/ransomware-statistics/>  
<https://www.varonis.com/blog/ransomware-statistics>  
<https://www.pandasecurity.com/en/mediacenter/security/ransomware-statistics/>  
<https://www.sophos.com/en-us/press-office/press-releases/2022/04/ransomware-hit-66-percent-of-organizations-surveyed-for-sophos-annual-state-of-ransomware-2022>  
<https://www.cisecurity.org/solarwinds>  
<https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know>  
<https://www.bleepingcomputer.com/news/security/cd-projekt-red-gaming-studio-hit-by-ransomware-attack/>  
<https://resources.infosecinstitute.com/topic/hellokitty-the-ransomware-affecting-cd-projekt-red-and-cyberpunk-2077/>  
<https://www.bleepingcomputer.com/news/security/cd-projekts-stolen-source-code-allegedly-sold-by-ransomware-gang/>  
<https://www.cnn.com/2021/03/09/microsoft-exchange-hack-explained.html>  
[https://en.wikipedia.org/wiki/2021\\_Microsoft\\_Exchange\\_Server\\_data\\_breach](https://en.wikipedia.org/wiki/2021_Microsoft_Exchange_Server_data_breach)  
<https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack>  
<https://nypost.com/2021/05/21/cna-financial-reportedly-paid-hackers-40m-in-ransom/>  
<https://hacked.com/cna-falls-victim-to-sophisticated-hack/>  
<https://www.bloomberg.com/news/articles/2021-04-14/nba-s-houston-rockets-face-cyber-attack-by-ransomware-group>  
<https://abc13.com/houston-rockets-cyberattack-nba-ransomware-who-cyber-attacked-attack-against-team/10517049/>  
<https://www.trtworld.com/sport/houston-rockets-works-with-fbi-after-being-hit-by-major-cyberattack-45918>  
<https://www.forbes.com/sites/leemathews/2021/04/15/ransomware-gang-strikes-the-houston-rockets/>  
[https://en.wikipedia.org/wiki/Colonial\\_Pipeline\\_ransomware\\_attack](https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack)  
<https://www.energy.gov/ceser/colonial-pipeline-cyber-incident>  
[https://www.cyber.nj.gov/garden\\_state\\_cyber\\_threat\\_highlight/colonial-pipeline-incident-ransomware-impacts-and-mitigation-strategies](https://www.cyber.nj.gov/garden_state_cyber_threat_highlight/colonial-pipeline-incident-ransomware-impacts-and-mitigation-strategies)  
<https://edition.cnn.com/2021/06/02/business/beef-hack-jbs/index.html>  
[https://en.wikipedia.org/wiki/JBS\\_S.A.\\_ransomware\\_attack](https://en.wikipedia.org/wiki/JBS_S.A._ransomware_attack)  
<https://www.techradar.com/news/axa-suffers-major-ransomware-attack>  
<https://www.reuters.com/article/us-axa-cyber-idUSKCN2CX0B0>  
<https://www.bleepingcomputer.com/news/security/insurer-axa-hit-by-ransomware-after-dropping-support-for-ransom-payments/>  
<https://www.reuters.com/technology/kaseya-ransomware-attack-sets-off-race-hack-service-providers-researchers-2021-08-03/>



<https://edition.cnn.com/2021/07/06/tech/kaseya-ransomware-what-we-know/index.html>  
<https://techcrunch.com/2021/07/05/kaseya-hack-flood-ransomware>  
<https://www.zdnet.com/article/report-increased-log4j-exploit-attempts-leads-to-all-time-peak-in-weekly-cyberattacks-per-org/>  
<https://www.f5.com/company/blog/protection-against-apache-log4j2-vulnerability>  
<https://www.cisa.gov/uscirt/apache-log4j-vulnerability-guidance>  
<https://siliconangle.com/2021/12/13/researchers-detect-hundreds-thousands-log4j-cyberattack-attempts/>  
<https://edition.cnn.com/2021/04/04/tech/facebook-user-info-leaked/index.html>  
[https://en.wikipedia.org/wiki/2021\\_Facebook\\_leak](https://en.wikipedia.org/wiki/2021_Facebook_leak)  
<https://heimdalsecurity.com/blog/everything-you-need-to-know-about-the-2021-facebook-data-breach/>  
<https://github.com/attakercyber/Facebook-Data-Leak>  
<https://www.theguardian.com/technology/2021/apr/03/500-million-facebook-users-website-hackers>  
<https://www.wired.com/story/facebook-data-leak-500-million-users-phone-numbers/>  
<https://www.cbsnews.com/news/crypto-com-hack-bitcoin-ethereum-30-million/>  
<https://netlibsecurity.com/blog/crypto-com-and-rising-data-breach-numbers/>  
<https://www.exchangewire.com/blog/2022/01/20/crypto-com-data-breach-confirmed-marfeel-violate-privacy-policies/>  
<https://www.techtarget.com/searchsecurity/news/252512445/Bernalillo-County-ransomware-attack-still-felt-weeks-later>  
<https://www.usnews.com/news/best-states/new-mexico/articles/2022-01-05/bernalillo-county-reports-suspected-ransomware-attack>  
<https://www.govtech.com/security/bernalillo-county-n-m-systems-disrupted-by-cyber-attack>  
<https://therecord.media/albuquerque-impacted-by-ransomware-attack-on-bernalillo-county-government/>  
<https://www.cpomagazine.com/cyber-security/nvidia-data-leak-exposed-proprietary-information-but-wasnt-a-russian-ransomware-attack-company-says/>  
<https://www.malwarebytes.com/blog/news/2022/03/nvidia-the-ransomware-breach-with-some-plot-twists>  
<https://www.reuters.com/business/autos-transportation/toyota-suspends-all-domestic-factory-operations-after-suspected-cyber-attack-2022-02-28/>  
<https://www.euronews.com/next/2022/02/28/toyota-cyberattack>  
<https://edition.cnn.com/2022/03/01/business/toyota-japan-cyberattack-production-restarts-intl-hnk/index.html>  
<https://www.cpomagazine.com/cyber-security/japanese-automotive-suppliers-targeted-as-denso-suffers-pandora-ransomware-attack-and-bridgestone-compromised-by-lockbit/>  
<https://siliconangle.com/2022/03/14/data-stolen-cyberattack-targeting-another-toyota-supplier/>  
<https://www.techcircle.in/2022/03/22/ransomware-group-claims-breach-at-microsoft-leaks-sources-codes-of-cortana-and-bing>  
<https://gurukul.com/news/hackers-accessed-published-source-code-for-microsoft-bing-cortana-and-maps>  
<https://www.classaction.org/news/shields-health-care-group-hit-with-class-action-over-march-2022-data-breach>  
<https://www.forbin.com/blog/post/monthly-breach-deets-shields-health-group-data-breach>  
[https://en.wikipedia.org/wiki/2022\\_Costa\\_Rican\\_ransomware\\_attack](https://en.wikipedia.org/wiki/2022_Costa_Rican_ransomware_attack)  
<https://www.nytimes.com/2022/05/17/us/politics/russia-hacking-costa-rica.html>  
<https://hacknotice.com/2022/06/16/baptist-medical-center-resolute-health-hospital-report-cybersecurity-hack-involving-patient-information-ksat-san-antonio/>  
[https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)  
<https://us.norton.com/blog/emerging-threats/cybersecurity-statistics>  
<https://interestingengineering.com/innovation/cyber-attacks-more-likely-to-bring-down-f-35-jets-than-missiles>  
<https://www.roundrobin.tech.com/email-protection>  
<https://us.norton.com/blog/online-scams/how-to-recognize-and-avoid-tech-support-scams>  
[https://www.ic3.gov/Media/PDF/AnnualReport/2020\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf)  
<https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>  
[https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021\\_NortonLifeLock\\_Cyber\\_Safety\\_Insights\\_Report\\_Global\\_Results.pdf](https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf)  
<https://cybersecurityventures.com/healthcare-industry-to-spend-125-billion-on-cybersecurity-from-2020-to-2025/>  
<https://blog.checkpoint.com/2021/05/12/the-new-ransomware-threat-triple-extortion/>  
<https://blog.checkpoint.com/2022/07/26/check-point-research-weekly-cyber-attacks-increased-by-32-year-over-year-1-out-of-40-organizations-impacted-by-ransomware-2/>  
<https://www.cloudwards.net/cyber-security-statistics/>  
<https://www.gartner.com/smarterwithgartner/3-actions-help-you-train-more-cybersecurity-savvy-employees>  
<https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022>  
<https://owasp.org/www-project-top-10-low-code-no-code-security-risks/>  
<https://trojanczyk.pl/trendy-w-technologii-na-2021/>  
<https://www.cloudwards.net/cloud-computing-statistics/>  
<https://venturebeat.com/security/what-gartners-top-cybersecurity-predictions-for-2022-23-reveal/>  
<https://www.purdueglobal.edu/blog/information-technology/cybersecurity-trends/>