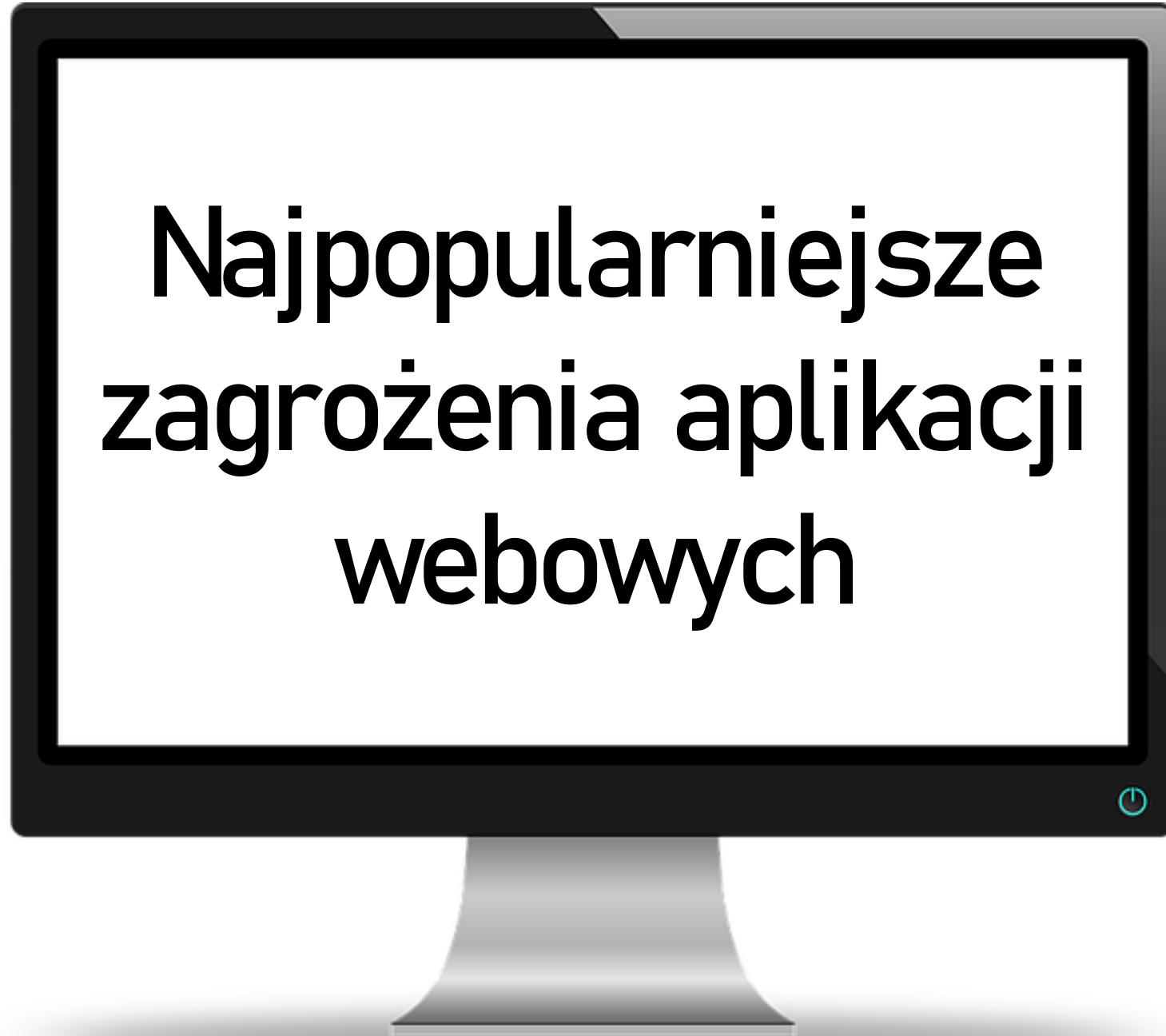




oze
ika
bo

Najpopularniejsze zagrożenia aplikacji webowych



Plan prezentacji

1. Dlaczego aplikacje webowe są częstym celem dla hakerów?
2. Opis popularnych ataków
3. Statystyki i trendy
4. Praktyczne przykłady
5. Strategie obronne



Dlaczego aplikacje webowe są częstym celem ataków hakerskich?



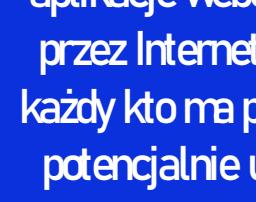
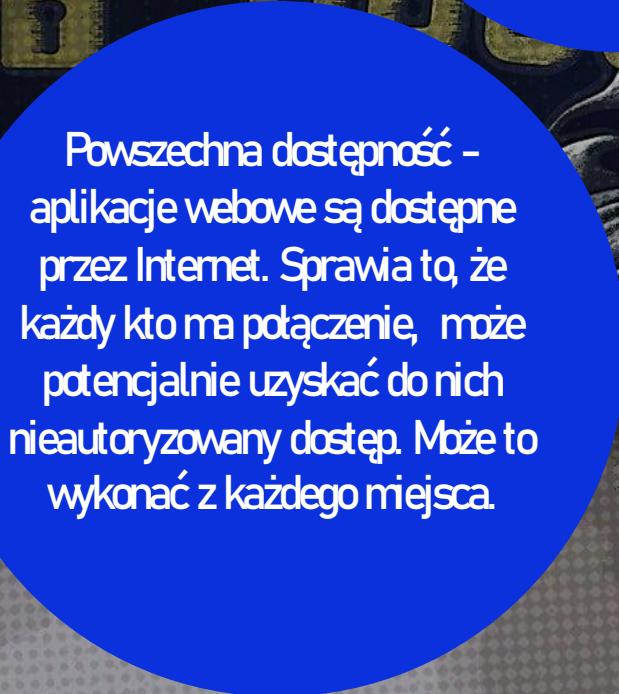
Powszechna dostępność - aplikacje webowe są dostępne przez Internet. Sprawia to, że każdy kto ma połączenie, może potencjalnie uzyskać do nich nieautoryzowany dostęp. Może to wykonać z każdego miejsca.

Złożoność technologiczna - współczesne aplikacje webowe są zbudowane z użyciem wielu różnych technologii i komponentów, co zwiększa ryzyko wystąpienia luk bezpieczeństwa.

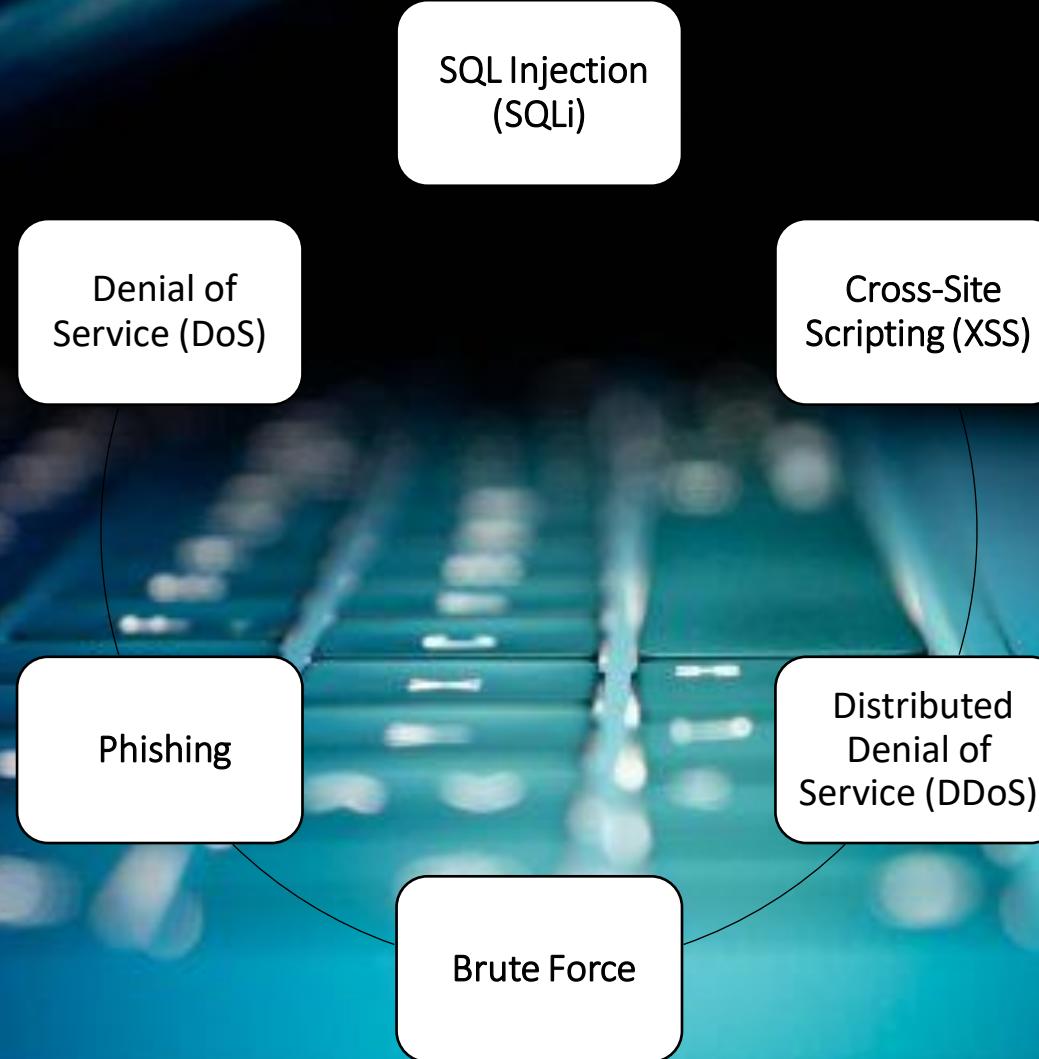


Duża ilość wrażliwych danych - aplikacje webowe często przechowują i przetwarzają duże ilości danych, tj. dane osobowe, dane logowania albo informacje finansowe. Są to wartościowe rzeczy dla cyberprzestępów.

Nedostateczna ochrona - często aplikacje nie są odpowiednio zabezpieczone. Wynika to z braku świadomości na temat zagrożeń, niewłaściwej konfiguracji serwerów, braku w regularnych aktualizacjach oprogramowania.



Przykładowe rodzaje ataków hakerskich



SQL Injection

SQLi - to technika ataku na aplikacje internetowe, która polega na wstrzyknięciu złośliwych poleceń SQL do zapytania do bazy danych, generowanego przez aplikację. Atak ten wykorzystuje luki w zabezpieczeniach, wynikające z niewłaściwej walidacji i filtrowania danych wprowadzanych przez użytkowników.

Denial Of Service

DoS - to rodzaj ataku hakerskiego mającego na celu uczynienie zasobów systemu, serwera, sieci lub usługi niedostępnymi dla użytkowników. Atak DoS polega na przeciążeniu zasobów docelowego systemu, co prowadzi do spowolnienia działania, awarii lub całkowitego wyłączenia usługi.

Cross-Site Scripting

XSS - to atak na aplikacje webowe, w którym atakujący wstrzykuje złośliwy kod (zazwyczaj JavaScript) do treści wyświetlanej przez stronę internetową. Kod ten jest następnie wykonywany w przeglądarkach użytkowników, co może prowadzić do kradzieży danych, przejęcia sesji, manipulacji zawartością strony i innych złośliwych działań.

Phishing

Phishing - to rodzaj ataku socjotechnicznego, w którym atakujący podszywają się pod wiarygodne instytucje lub osoby, aby oszukać ofiary i skłonić je do ujawnienia poufnych informacji, takich jak dane logowania, informacje o kartach kredytowych, numery ubezpieczenia społecznego czy inne dane osobowe

Distributed Denial Of Service

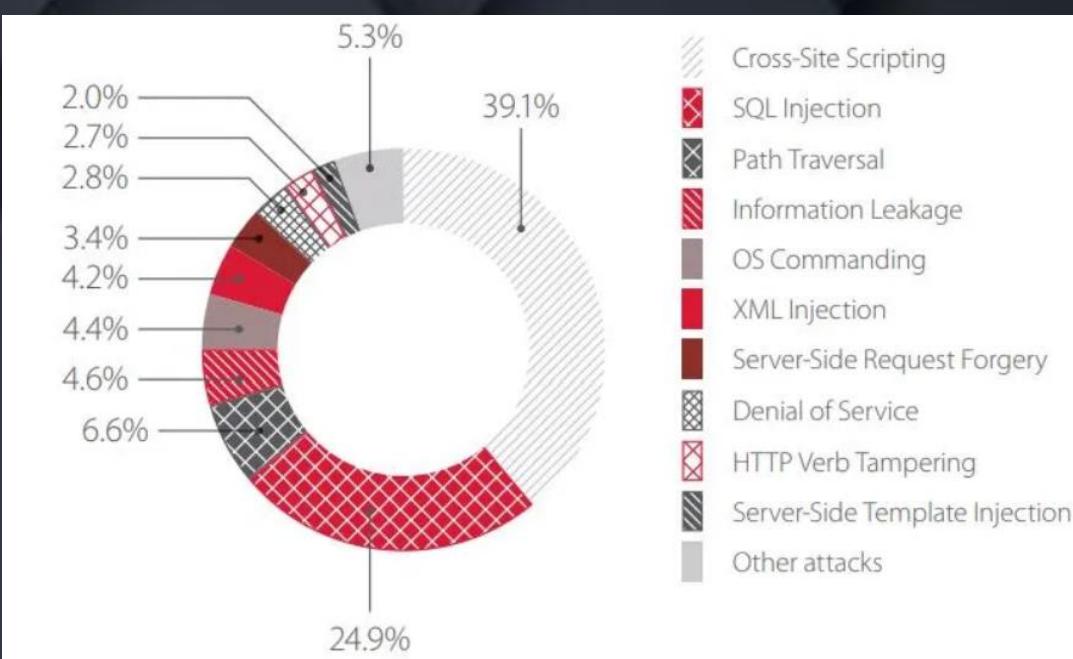
DDoS - to rodzaj ataku, w którym napastnik używa wielu zainfekowanych komputerów (zombie) do jednoczesnego wysyłania ogromnej liczby żądań do serwera, sieci lub usługi, co prowadzi do przeciążenia zasobów i uniemożliwia normalne działanie.

Brute Force

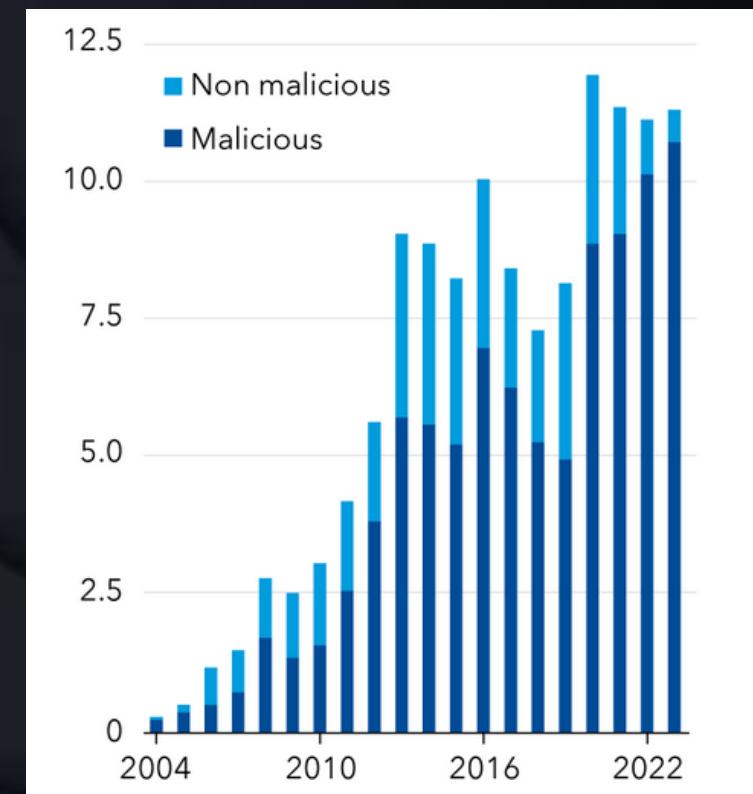
Brute Force - to metoda ataku polegająca na systematycznym sprawdzaniu wszystkich możliwych kombinacji haseł lub kluczy, aż do znalezienia poprawnego. Atak ten jest czasochłonny i wymaga dużej mocy obliczeniowej, ale może być skuteczny, zwłaszcza jeśli hasła są słabe lub krótkie.

Statystyki

Podział typów ataków

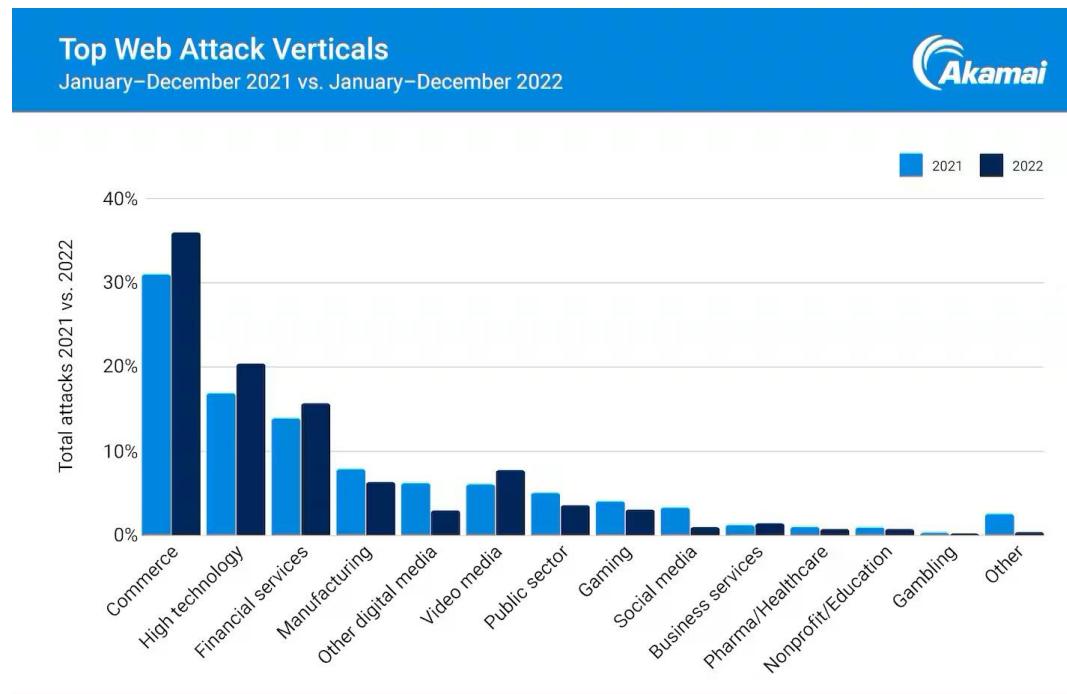


Liczba ataków w latach 2004 – 2023 w tysiącach

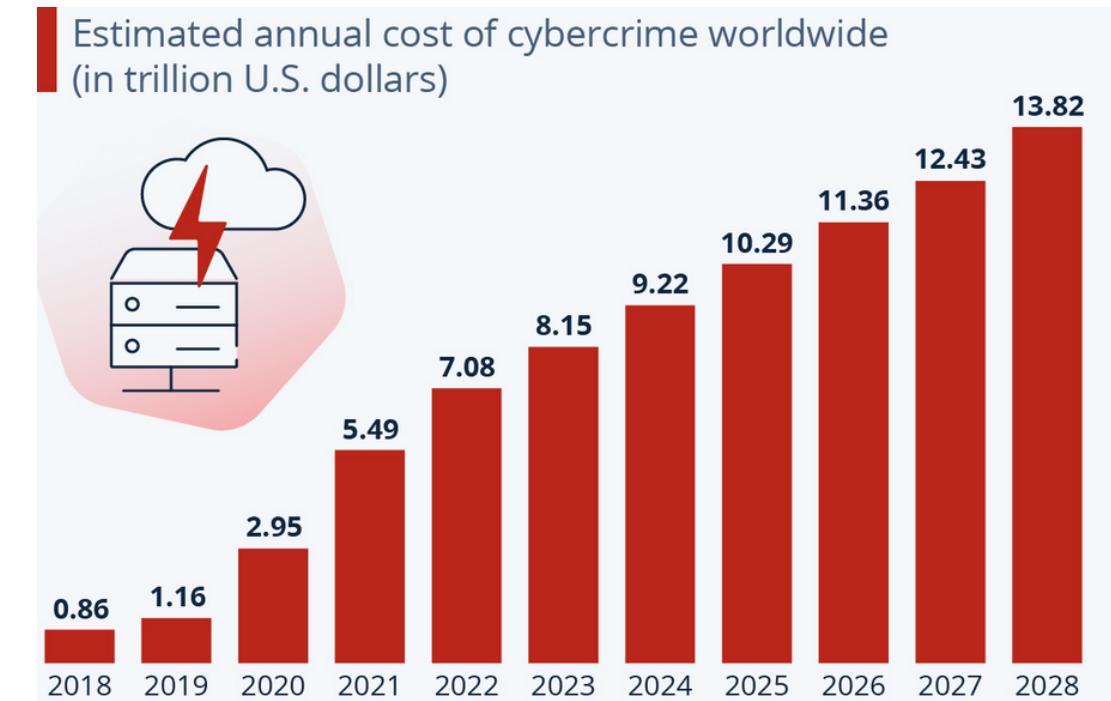


Analiza trendów i przewidywania na przyszłość

Typy sektorów narażone na ataki w latach 2021-2022r.



Szacunkowy roczny koszt cyberprzestępcości na świecie



Praktyczne przykłady ataków hakerskich, ich przyczyny oraz skutki



Atak na firmę
Sony
wykorzystujący
SQL Injection

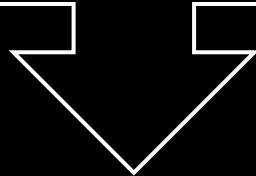
W 2011r. grupa hakerska „LulzSec” przeprowadziła atak na firmę Sony, wykorzystując SQL Injection. Znaleźli oni podatność na stronie SonyPictures.com, w której wstrzyknęli złośliwe zapytanie SQL do bazy danych. Uzyskali dzięki temu dostęp do wszystkich danych użytkowników tej firmy, co doprowadziło do ogromnych strat finansowych oraz utracenia zaufania klientów do firmy.



Atak na Twittera wykorzystujący Cross-Site Scripting

W 2009r. Twitter padł ofiarą ataku typu XSS. W tym przypadku hakerzy wykorzystali lukę na stronie Twittera, dzięki której mogli wstrzyknąć niepożądany kod JavaScript do tweetów. Wykonali również skrypt, który sprawiał, że każda osoba, która weszła na zainfekowany profil udostępniała mimowolnie ten sam wpis. Nie wykazano, że doszło do wykradnięcia danych osobowych, ale atak ten spowodował duży chaos na platformie. Przez tą sytuację wzrosła świadomość jak ważne w aplikacji jest zabezpieczenie przed nieautoryzowanym dostępem.

Wyciek danych z Pandabuy



Pod koniec marca 2024 dwójka hakerów o pseudonimach „Sanggiero” i „IntelBroker” wykorzystując liczne, krytyczne luki w API oraz wewnętrznych systemach serwisu wykradli dane 1,3 mln użytkowników, w tym ich adresy e-mail, dane osobowe, numery telefonów oraz adresy IP logowania. Sanggiero opisał, że ich atak polegał na manipulacji i wykorzystaniu błędów w kodzie API, który nie był wystarczająco zabezpieczony.



Przykłady skutecznych metod zabezpieczenia aplikacji webowych



- **Uwierzytelnianie JWT (JSON Web Token)** - to metoda uwierzytelniania, która pozwala aplikacji potwierdzić tożsamość użytkownika. Bezpiecznie przekazuje informacje o użytkowniku między klientem a serwerem.
- **Stosowanie protokołu HTTPS (Hypertext Transfer Protocol Secure)** - zapewnia bezpieczną komunikację między przeglądarką użytkownika a serwerem. Szyfruje dane, chroniąc je przed przechwyceniem przez osoby trzecie.
- **Używanie tokenów CSRF (Cross-Site Request Forgery)** - Ataki CSRF polegają na wykorzystaniu sesji użytkownika do wykonania niechcianych działań na innej stronie. Token CSRF pomaga zabezpieczyć przed tym rodzajem ataku.
- **Implementacja Captchy** - Captcha jest używana, aby odróżnić ludzi od botów. Pomaga w walce z automatycznymi atakami, takimi jak spamowanie formularzy.
- **Filtrowanie i walidacja danych wejściowych** - Nieprawidłowe dane wejściowe mogą prowadzić do ataków, takich jak SQL Injection. Filtrowanie i walidacja pomagają odfiltrować niebezpieczne dane.



rob
yde



Rodzaje incydentów

Krytyczny

To incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV;

Poważny

To incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej;

Istotny

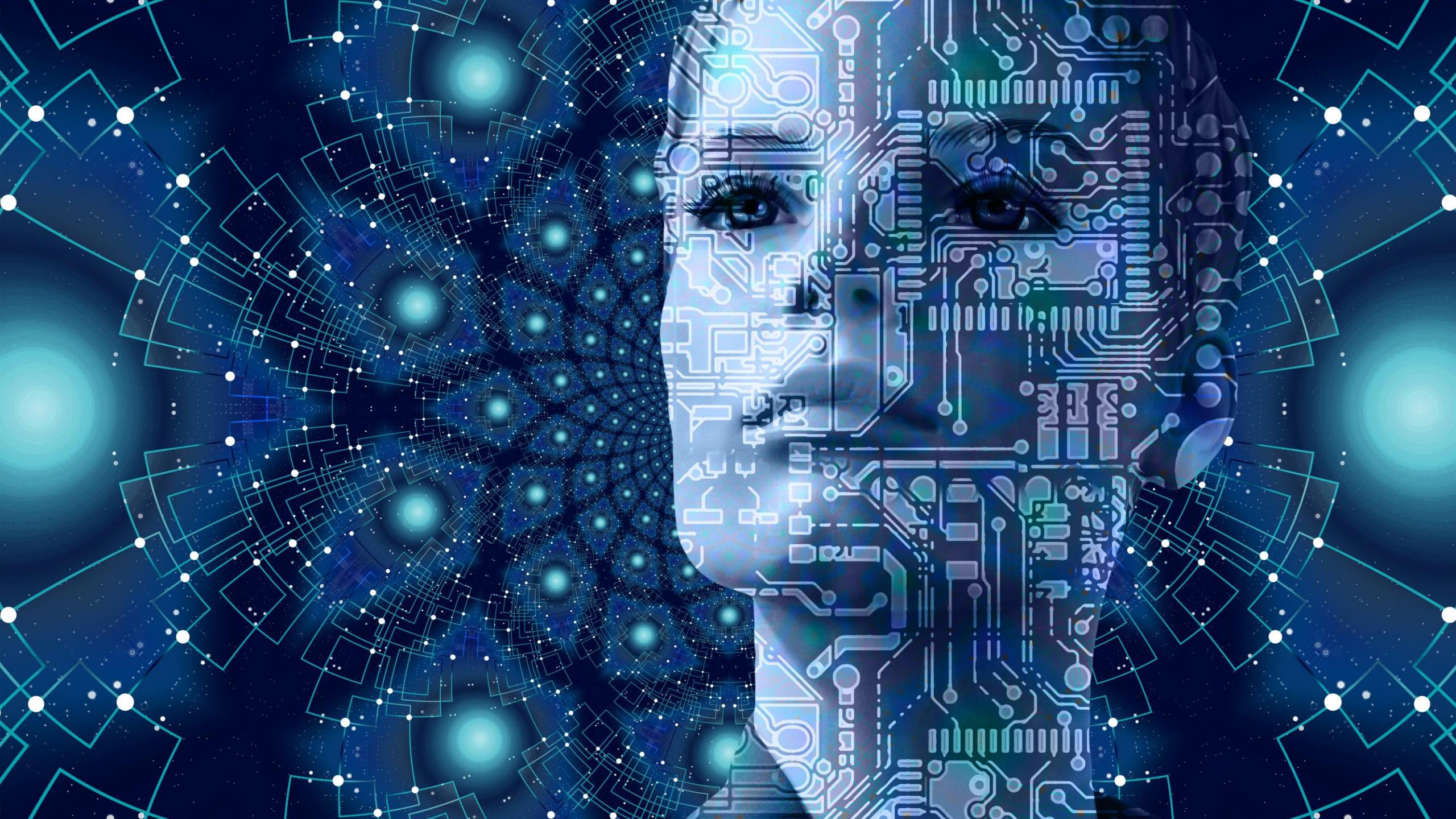
Dany incydent uznaje się za istotny jeżeli zaistniała co najmniej jedna z następujących sytuacji:

- a) usługa świadczona przez dostawcę usług cyfrowych była niedostępna przez ponad 5 000 000 użytkownikogodzin, przy czym pojęcie „użytkownikogodzin” odnosi się do liczby dotkniętych incydentem użytkowników w Unii przez okres sześćdziesięciu minut;
- b) incydent doprowadził do utraty integralności, autentyczności lub poufności przechowywanych lub przekazywanych bądź przetwarzanych danych lub powiązanych usług, oferowanych bądź dostępnych poprzez sieci i systemy informatyczne dostawcy usług cyfrowych, która dotknęła ponad 100 000 użytkowników w Unii;
- c) incydent spowodował ryzyko dla bezpieczeństwa publicznego lub ryzyko wystąpienia ofiar śmiertelnych;
- d) incydent wyrządził co najmniej jednemu użytkownikowi w Unii stratę materialną, której wysokość przekracza 1 000 000 EUR.

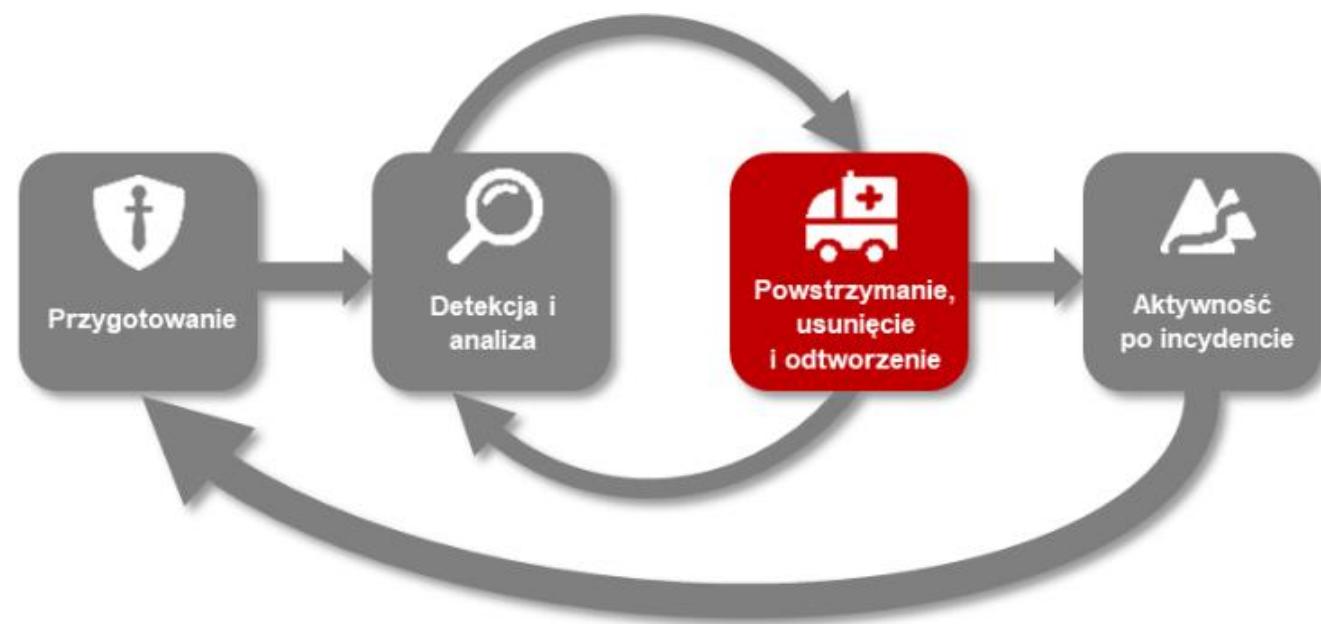
W podmiocie publicznym

To incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny, o którym mowa w art. 4 pkt 7–15;













CYBER SECURITY



<CERT.PL>
NASK



C:[SIRT]MON

Ochrona danych osobowych

Konstytucja RP

Jako najważniejszy dokument prawny zawiera zasady dotyczące ochrony danych osobowych, m.in Artykuł 47:

„Każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.”

RODO

Inaczej Ogólne rozporządzenie o ochronie danych osobowych, miało na celu ujednolicenie przepisów dotyczących ochrony danych osobowych we wszystkich krajach członkowskich Unii Europejskiej.

Ustawa o ochronie danych osobowych

Zapewnia stosowanie przepisów RODO oraz ustanawia nowy organ właściwy w sprawie ochrony danych osobowych- Prezesa Urzędu Ochrony Danych Osobowych(PUODO).

Definicja naruszenia ochrony danych osobowych



Art. 4 pkt 12 rozporządzenia RODO
„naruszenie ochrony danych
osobowych” oznacza naruszenie bezpieczeństwa
prowadzi do przypadkowego lub niezgodnego
z prawem zniszczenia, utraty,
zmodyfikowania, nieuprawnionego ujawnienia
lub nieuprawnionego dostępu do danych
osobowych przesyłanych, przechowywanych lub
w inny sposób przetwarzanych”

Procedury zgłaszania naruszeń

Administrator jak najszybciej zgłasza naruszenie do organów nadzorczych

Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi

Treść zgłoszenia do organu nadzorczego

Możliwość sukcesywnego udzielania informacji

Administrator dokumentuje wszelkie naruszenia



RANSOMWARE

Ransomware to rodzaj złośliwego oprogramowania, które szyfruje ważne pliki przechowywane na dysku lokalnym i sieciowym i żąda okupu za ich odszyfrowanie.



CZYM JEST RANSOMWARE?



MALWARE



ZASZYFROWANIE DANYCH



ŻĄDANIE OKUPU

Co należy zrobić po ataku ransomware?

Rekomendacje CERT Polska dotyczące postępowania po ataku:

- Izolacja zainfekowanej maszyny
- Identyfikacja oraz eliminacja źródła infekcji
- Identyfikacja rodziny ransomware
- Przywrócenie działania systemów
- Zgłoszenie incydentu



Kroki izolacji i dokumentacji incydentu

- **Izolacja:** Natychmiastowe odizolowanie zainfekowanych systemów, aby zapobiec dalszemu rozprzestrzenianiu się zagrożenia. Odłączenie urządzeń od sieci, wyłączenie zainfekowanych serwerów czy komputerów.
- **Dokumentacja:** Każdy krok podjęty podczas reakcji na incydent powinien być dokładnie dokumentowany. Dokumentacja powinna zawierać daty, godziny działań, osoby odpowiedzialne oraz użyte narzędzia.



Strony i narzędzia pomocowe

Korzystanie z aplikacji lub bazy danych, takiej jak system śledzenia problemów, pomaga zapewnić obsługę i rozwiązywanie incydentów w odpowiednim czasie. System śledzenia problemów powinien zawierać następujące informacje:

- Aktualny stan incydentu (nowy, w toku, przekazany do zbadania, rozwiązany itp.).
- Podsumowanie incydentu.
- Wskaźniki związane ze incydentem.
- Inne incydenty związane z tym incydentem.
- Działania podjęte w związku z tym incydentem przez wszystkie osoby obsługujące incydent.
- Łącuch dowodowy, jeśli dotyczy. Oceny skutków związanych z incydentem.
- Dane kontaktowe innych zaangażowanych stron (np. właścicieli systemu, administratorów systemu).
- Lista dowodów zebranych podczas badania incydentu.
- Komentarze osób obsługujących incydent.
- Kolejne kroki, które należy podjąć (np. przebudowa hosta, aktualizacja aplikacji).



Procedury zgłoszania incydentu

Identyfikacja i ocena incydentu

- Pierwszym krokiem jest stwierdzenie, że incydent miał miejsce. Może to wynikać z wykrycia anomalii w systemie, raportu od użytkownika lub zewnętrznego sygnału (np. ostrzeżenie od CERT Polska).

Zgłoszenie incydentu do administratora

Zgłoszenie incydentu do organu nadzorczego:

- Zgodnie z RODO, administrator ma obowiązek zgłosić incydent organowi nadzorcemu (w Polsce jest to Prezes Urzędu Ochrony Danych Osobowych, PUODO) bez zbędnej zwłoki, ale nie później niż w ciągu 72 godzin od stwierdzenia naruszenia.

Informowanie osób, których dane dotyczą:

Dokumentowanie naruszeń

- Administrator musi dokumentować wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia, jego skutki oraz podjęte działania zaradcze.

Działania zapobiegawcze

Aktywne monitorowanie zdarzeń w sieci- bieżące monitorowanie oraz bezpieczne przechowywanie logów z urządzeń w sieci, jest podstawą do sprawnej detekcji oraz skutecznego zablokowania ataku. Usprawni to również analizę powłamaniową w przypadku ewentualnego incydentu. Poniżej opisane zostały ważniejsze zagadnienia związane z logowaniem oraz monitorowaniem urządzeń:

- wysyłanie logów z urządzeń do centralnego serwera logów.,
- logi na serwerze powinny być przechowywane przez minimum 14 ostatnich dni.

Odpowiednie wykonywanie kopii zapasowych- w związku z kopiami zapasowymi, należy zbadać następujące zagadnienia:

- czy cyklicznie wykonywane są kopie zapasowe?
- czy treść kopii zapasowych jest aktualna?

Ważne jest również regularne testowanie kopii zapasowych, pod kątem późniejszego przywrócenia danych. Zapobiegnie to sytuacji, gdzie pomimo utworzonych backupów, nie udało się przywrócić stanu przed infekcją ze względu na błąd w kopii.

Dziękujemy za uwagę

Autorzy:

Tymoteusz Mróz

Michał Lekstan