INFORMACJA, al. Niepodległości 34, 61-714 Poznań, hol główny, tel.: 61 626 66 66; fax 61 626 67 44, e-mail: kancelaria@umww.pl

Cyberbezpieczeństwo

Czym jest cyberatak?

Cyberatak jest to próba naruszenia systemu teleinformatycznego w celu uzyskania korzyści z zakłócenia pracy tego systemu jak i również kradzieży danych.

Rodzaje cyberataków:

Malware – Oprogramowanie typu malware przedostaje się do systemu teleinformatycznego poprzez lukę w oprogramowaniu, najczęściej poprzez kliknięcie niebezpiecznego linku lub załącznika wiadomości email. W momencie, gdy użytkownik kliknie w link lub uruchomi załącznik, spowoduje to instalację złośliwego oprogramowania, które w następstwie może spowodować: zablokowanie dostępu do komputera, sieci, zaszyfrowanie danych, uzyskanie dostępu do informacji przechowywanych na dysku twardym, a następnie przesłanie ich atakującemu.

Ransomware - atak, którego skutkiem jest zaszyfrowanie danych na komputerze, serwerze w celu wymuszenia okupu. Jest to bardzo popularny rodzaj ataku, który może spowodować bezpowrotną utratę danych.

Phishing – polega na wysyłaniu fałszywych wiadomości, które podszywają się pod wiadomości pochodzące ze sprawdzonego źródła. Zazwyczaj tego typu cyberatak ma na celu pozyskanie danych poufnych takich jak dane kart kredytowych, danych logowania.

Man in the Middle – atak polegający na podsłuchiwaniu przez atakującego ruchu sieciowego pomiędzy np. klientem i serwerem. W trakcie podsłuchu może dojść do przejęcia loginów, haseł i wrażliwych danych użytkownika. Zdarza się często w niezabezpieczonych sieciach Wi-Fi. Atak może być wykonany również poprzez zainstalowanie na komputerze ofiary oprogramowania nasłuchującego cały ruch sieciowy komputera.

DOS – atak, którego skutkiem jest wyczerpanie zasobów systemu teleinformatycznego (np. serwera WWW). Atak ten polega na nadmiarowym zalaniu systemu teleinformatycznego ruchem sieciowym, co w rezultacie powoduje niedostępność systemu. Atakujący często wykonują rozproszony atak (Distributed DOS - **DDOS**), w takiej sytuacji blokujący ruch sieciowy przychodzący do systemu teleinformatycznego pochodzi z wielu zainfekowanych urządzeń.

SQL Injection – atakujący z użyciem odpowiednio zmodyfikowanego zapytania SQL, zmusza serwer SQL do ujawnienia danych z bazy danych, których normalnie by nie ujawnił. Tego typu atak wykonywany jest często poprzez użycie pól wyszukiwania w nieprawidłowo zabezpieczonej witrynie internetowej.

Exploit typu Zero – day – tego typu exploity pojawiają się w tym samym dniu, w którym doszło do ujawnienia luki w zabezpieczeniach systemu teleinformatycznego, jeszcze przed stworzeniem poprawki do tego systemu.

Aby zminimalizować ryzyko wystąpienia ataku lub ograniczenia jego skutków, należy stosować następujące zabezpieczenia:

- wykonuj regularne kopie zapasowe danych,
- zwracaj uwagę, czy komunikacja między komputerem a serwerem jest szyfrowana,
- używaj oprogramowania antywirusowego z aktualną bazą sygnatur wirusów,
- aktualizuj system operacyjny komputera oraz serwera,
- nie otwieraj załączników w mailach niewiadomego pochodzenia,
- ostrożnie korzystaj z publicznych, ogólnodostępnych sieci WIFI,
- nie uruchamiaj aplikacji niewiadomego pochodzenia,
- nie podawaj nikomu loginu i hasła do systemów, nikt nie powinien prosić o takie dane,
- weryfikuj adres nadawcy wiadomości email, w szczególności zwróć uwagę na literówki w adresie email wiadomości przychodzących,
- edukuj siebie oraz swoich pracowników w kwestii zagrożeń - najsłabszym ogniwem systemu zabezpieczeń jest zawsze człowiek,
- używaj prawidłowo skonfigurowanych systemów firewall, IPS w organizacji,
- wykonuj regularne audyty bezpieczeństwa posiadanych stron WWW i innych usług zewnętrznych.

Poniżej linki do popularnych serwisów, które mogą stanowić dodatkowe wsparcie w uzyskaniu stosownych informacji w kwestii cyberbezpieczeństwa:

- **Aktualności oraz Baza wiedzy dostępne pod adresem** https://www.gov.pl/web/baza-wiedzy/aktualnosci
- **OUCH!** Aktualizowany cyklicznie zestaw porad bezpieczeństwa dla użytkowników komputerów dostępny pod adresem: https://cert.pl/ouch/

Poniżej linki do stron podmiotów zajmujących się cyberbezpieczeństwem (w ramach Ministerstwa Cyfryzacji):

- CERT Polska, https://cert.pl/
- CSIRT GOV, https://csirt.gov.pl/
- CSIRT NASK, https://www.nask.pl/pl/dzialalnosc/csirt-nask/3424,CSIRT-NASK.html

Dziękujemy za odwiedziny i zapraszamy ponownie