GRUDZIEŃ 2022

Cyberterroryzm

jako zagrożenie dla bezpieczeństwa wewnętrznego państwa.

fundacja instytut CYBERBEZPIECZEŃSTWA

AUTOR

Mikołaj Rogalewicz

MINISTERSTWO SPRAWIEDLIWOŚCI

www.ms.gov.pl

FUNDUSZ SPRAWIEDLIWOŚCI

SFINANSOWANO ZE ŚRODKÓW FUNDUSZU SPRAWIEDLIWOŚCI, KTÓREGO DYSPONENTEM JEST MINISTER SPRAWIEDLIWOŚCI

Intensywny rozwój nowoczesnych technologii w XXI wieku sprawił, że codzienne funkcjonowanie nieodłącznie związane jest z cyberprzestrzenią. Technologie informacyjne odgrywają kluczową rolę w funkcjonowani państwa, a także w działalności przedsiębiorstw. Nowe technologie dają wiele korzyści, ale jednocześnie wiążą się z szeregiem zagrożeń. Jednym z nich jest cyberterroryzm, który stanowi zagrożenie dla bezpieczeństwa państwa.

Czym jest cyberterroryzm?

Cyberterroryzm to jedno z największych zagrożeń w XXI wieku. Powstał na gruncie terroryzmu i bazuje na wykorzystaniu cyberprzestrzeni. Możemy go zdefiniować jako bezprawny atak na system informatyczny, w celu zastraszenia albo wymuszenia na przedstawicielach atakowanego podmiotu określonych ustępstw albo zachowań. Jest rodzajem przestępstwa skierowanego przeciwko państwu oraz jego obywatelom. Jego cechą charakterystyczną, tak jak w przypadku terroryzmu, jest stosowanie przemocy w celu wywołania zamierzonych skutków, w szczególności lęku, niepewności i zastraszenia. Z cyberterroryzmem wiążą się trzy główne obszary zagrożeń, które przedstawia grafika. Pierwszym obszarem, który narażony jest na działania cyberterrorystów są systemy wojskowe. Przechowują one kluczowe informacje dotyczące systemów łączności, położenia satelitów czy rozmieszczenia wojsk i broni. Utrata tych informacji stanowi bezpośrednie zagrożenie dla bezpieczeństwa państwa. Drugi obszar związany jest z działalnością przedsiębiorstw. Systemy przedsiębiorstw przechowują informacje związane z ich działalnością, w tym informacje o klientach, umowach, planowanych działaniach, czy też wykorzystywanych technologiach. Przedsiębiorstwo narażone jest na utratę tych danych w wyniku cyberataku. Trzecim obszarem zagrożeń są systemy infrastruktury krytycznej, których zniszczenie albo uszkodzenie może doprowadzić do osłabienia zdolności obronnych państwa. Jednym z kluczowych systemów infrastruktury krytycznej państwa są systemy energetyczne, związane z produkcją, przesyłem oraz dystrybucją energii. Ich uszkodzenie może doprowadzić do braku prądu, wody lub gazu. Istotne znaczenie mają także systemy transportowe, obejmujące transport lotniczy, morski, kolejowy i drogowy. Ich uszkodzenie może wprowadzić chaos i wpłynąć na funkcjonowanie państwa. Do systemów infrastruktury krytycznej można zaliczyć także systemy bankowo-finansowe, związane z przechowywaniem i transferem pieniędzy, a także systemy telekomunikacyjne obejmujące linie telefoniczne oraz sieci komputerowe. Cyberterroryzm może być wymierzony także w systemy komunikacji pomiędzy służbami ratunkowymi.

Metody Cyberataków

Istnieją różne metody cyberataków. Poniżej przedstawione zostaną najpopularniejsze z nich:

- DoS (Denial of Service) – atak na system komputerowy mający na celu uniemożliwienie dostępu do usługi. Strona internetowa zaatakowana w ten sposób nie będzie się po prostu wyświetlać. Atak DoS może mieć różny czas trwania i może być wymierzony w więcej niż jedną stronę lub system w tym samym czasie. Jednym z rodzajów ataku DoS jest DDoS (Distributed Denial of Service), który oznacza, że atak jest realizowany w sposób rozproszony, czyli atakujący wysyła ruch równolegle z wielu różnych lokalizacji.
- Hijacking – atak, w którym haker przejmuje kontrolę nad komputerem lub urządzeniem mobilnym ofiary, aby uzyskać dostęp do danych lub je ukraść.
- Sniffing – technika polegająca na monitorowaniu ruchu internetowego w czasie rzeczywistym i pozwalająca na przechwytywanie wiadomości płynących z i do danego urządzenia
- Phishing – próba wyłudzenia informacji za pomocą różnego rodzaju metod socjotechnicznych. Polega na podstępnym nakłanianiu ludzi do podania poufnych informacji, takich jak hasła lub numery kart kredytowych, poprzez podszywanie się pod godne zaufania źródło. Może się odbywać poprzez pocztę elektroniczną, media społecznościowe, złośliwe strony internetowe, czy wiadomości SMS. Metoda ta bazuje na wysyłaniu wiadomości wyglądających na rzetelne, które zawierają zazwyczaj link, przenoszący na fałszywą stronę internetową. Użytkownik proszony jest na niej o podanie danych osobowych, które zostają wykradzione.
- Ransomware – forma złośliwego oprogramowania, które szyfruje pliki, po czym atakujący żąda od ofiary okupu, aby po zapłaceniu przywrócić dostęp do danych. Użytkownicy uzyskują instrukcję, w jaki sposób powinni uiścić opłatę, aby pliki zostały odszyfrowane.

Przykłady cyberataków

W ciągu ostatnich lat przeprowadzono wiele cyberataków. Jeden z najpopularniejszych miał miejsce w 2007 roku przeciwko Estonii, kiedy grupa rosyjskich hakerów zablokowała strony internetowe banków, mediów i niektórych służb rządowych. Był to atak typu DDoS. Rosja wykorzystuje także cyberataki w obecnej wojnie w Ukrainie. Zgodnie z danymi Ukraińskiej Państwowej Służby Łączności Specjalnej i Ochrony Informacji (SSSCIP), od początku wojny odnotowano ponad 1000 cyberataków ze strony Rosji. Ciekawym przykładem cyberataku było wykorzystanie ukradzionego oprogramowania przez jednego z byłych pracowników australijskiej firmy zajmującej się zarządzaniem urządzeniami kanalizacyjnymi, za pomocą którego wypuścił on do rzeki miliony litrów ścieków w Queesland w Australii. Jego działania miały negatywne skutki biologiczne dla całego rejonu.

Cyberataki stanowią także aktualnie coraz większe zagrożenie w Polsce. Jak wynika z badania „Barometr Cyberbezpieczeństwa", przeprowadzonego przez KPMG, w 2021 roku 69 proc. przedsiębiorstw w Polsce odnotowało co najmniej jeden incydent, związany z naruszeniem bezpieczeństwa. Ponadto, w przypadku ponad 20 proc. przedsiębiorstw nastąpił wzrost liczby cyberataków.

Największym zagrożeniem dla polskich firm są wycieki danych za pomocą złośliwego oprogramowania (malware) oraz phishing. Jako źródło największego zagrożenia polscy przedsiębiorcy wskazują zaś zorganizowane grupy przestępcze.

Podsumowanie

Cyberterroryzm to jedno z największych zagrożeń XXI wieku. Obecnie państwa uzależnione są od technologii informacyjnych, których zaatakowanie może wyrządzić poważne szkody i zakłócić funkcjonowanie danego kraju. Na akty cyberterroryzmu narażone są w szczególności systemy infrastruktury krytycznej, systemy wojskowe oraz systemy przedsiębiorstw. Problem związany z cyberatakami wzrasta także w Polsce, a w 2021 roku większość przedsiębiorstw odnotowała incydenty z naruszeniem ich cyberbezpieczeństwa.

Mikołaj Rogalewicz

MINISTERSTWO SPRAWIEDLIWOŚCI
www.ms.gov.pl

FUNDUSZ SPRAWIEDLIWOŚCI

SFINANSOWANO ZE ŚRODKÓW FUNDUSZU SPRAWIEDLIWOŚCI, KTÓREGO DYSPONENTEM JEST MINISTER SPRAWIEDLIWOŚCI

fundacja@instytutcyber.pl
www.instytutcyber.pl