19. Zakłócenia w systemie telekomunikacyjnym/cyberatak

**19. Zakłócenia w systemie telekomunikacyjnym/cyberatak**

| **Lp.** | **Zagrożenie** | **Przyczyny/Typy** | **Ocena ryzyka** | **Mapa ryzyka** | **Mapa****zagrożenia** |
| --- | --- | --- | --- | --- | --- |
| **19** | **Zakłócenia w systemie telekomunikacyjnym** niepożądane przebiegi występujące razem z sygnałem (przebiegiem użytecznym) i pochodzące ze źródeł innych niż sygnał.**Ataki cybernetyczne** są jednymi z najbardziej skutecznych i jednocześnie uciążliwych (jeśli chodzi o szkody) działań uderzających we współczesne społeczeństwo. Cyberterroryzm staje się coraz bardziej powszechną metodą działania ponieważ:- do przeprowadzania działań związanych z cyberatakiem jedynym potrzebnym narzędziem jest komputer i podłączenie do sieci;- modus operandi tego typu działań to tworzenie wirusów, robaków komputerowych, tzw. „koni trojańskich” i przesyłanie ich docelowo w miejsce ataku, niszczenie serwerów, modyfikacja systemów IT oraz fałszowanie stron www. Cyberprzestrzeń nie posiada barier kontrolnych;- cele ataków są bardzo szerokie – zagrożone są sieci komputerowe, a także komputery rządowe i prywatnych przedsiębiorstw a prawdopodobieństwo znalezienia luk w zabezpieczeniach jest stosunkowo duże. | Ze względu na rodzaj źródła rozróżnia się m.in.: - **zakłócenia telekomunikacyjne atmosferyczne** powstające wskutek wyładowań elektrycznych w atmosferze, - **energetyczne** powodowane działaniem urządzeń energoelektrycznych,- **przenikowe** związane z częściowym przenikaniem energii do danej drogi przesyłowej sygnału z innych dróg przesyłowych.Zakłócenia telekomunikacyjne dzieli się na własne (m.in. szum cieplny, zakłócenia komutacyjne) i obce (m.in. przenikowe, atmosferyczne, energetyczne, szum otoczenia) oraz trwałe (m.in. energetyczne) i nietrwałe (m.in. atmosferyczne), a także — zależnie od lokalizacji miejsca dopływu zakłócenia — na aparatowe, stacyjne i międzystacyjne. Zakłócenia telekomunikacyjne pogarszają jakość transmisji.Na terenie powiatu, sieci telekomunikacyjne obsługuje kilku operatorów. Najgroźniejsze awarie, mogące dezorganizować funkcjonowanie regionu, występować będą w sieciach napowietrznych oraz w systemach sterujących. Głównymi czynnikamimogącymi spowodować awarie, mogą być: uszkodzenia mechaniczne sieci, uszkodzenia sieci i innychurządzeń instalacyjnych wywołane ekstremalnymi warunkami pogodowymi, głównie silnymi wiatrami,znacznymi spadkami temperatur oraz obfitymi opadami śniegu, awarie systemów informatycznychsterujących przepływem energii, zaniki w zasilaniu energetycznym, a także zamierzone bądź niezamierzone działanie człowieka. **PRZYCZYNY CYBERATAKU:**- Czynnik ludzki (nieznajomość/lekceważenie przepisów łapownictwo, frustracja, ideologia), modyfikacja systemów i danych, błąd organizacyjny, techniczny, sabotaż, uszkodzenie lub kradzież elementów przesyłowych.  | **MAŁE** | **LUDNOŚĆ:**- utrata zaufania do instytucji publicznych,- brak możliwości wykonywania zadań merytorycznych przez pracowników,- brak możliwości w komunikowaniu się oraz brak możliwości uzyskania i przekazywania informacji,- zagrożenia życia i zdrowia spowodowane zakłóceniami systemów energetycznych, sterowania ruchem.**GOSPODARKA/ MIENIE/ INFRASTRUKTURA:**- naruszenie bezpieczeństwa państwa i jego obywateli,- awaria systemu lub niesprawność urządzeń lub programowani,- możliwość wystąpienia zagrożeń dla obronności państwa,- zakłócenia w pracy infrastruktury przesyłowej,- obniżenie m.in. zaopatrzenia w energię i paliwa, teleinformatyczne, bankowe i finansowe, zaopatrzenia w żywność oraz wodę, opiekę zdrowotną, transport i komunikację, ratownicze, a także zapewnienie funkcjonowania organów władzy administracji publicznej,- znaczące straty finansowe, gospodarcze a także skutki społeczne,- zmiana lub zakłócenie wykonywanych procesów – naruszenie integralności.**ŚRODOWISKO:**Brak bezpośrednich skutków. | Obszar całego powiatu:- instytucje i urzędy państwowe oraz inne jednostki organizacyjne, w tym jednostki samorządu terytorialnego,- przedsiębiorcy w tym będący operatorem infrastruktury ważnej dla społeczności lokalnej |

**Cyberterroryzm –** politycznie umotywowany atak lub groźba ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych działań. W szerszym rozumieniu tego słowa jest to także użycie Internetu do komunikowania się, propagandy i dezinformacji przez organizacje terrorystyczne. Narzędziami cyberterrorystów są ataki cybernetyczne, włamania do ważnych z punktu widzenia bezpieczeństwa systemy (m.in. jednostki wojskowe, elektrownie), ataki typu DdoS na instytucje prywatne lub rządowe.

Wysoki poziom rozwoju technologicznego przyczynia się do poprawy zarządzania wieloma sferami życia politycznego, społecznego i gospodarczego, ale jednocześnie uzależnia państwo od sprawności i bezpieczeństwa infrastruktury krytycznej. Atak na jeden z elementów systemu może zakłócić funkcjonowanie pozostałych („efekt domina”), ponieważ są one ściśle ze sobą powiązane.

Uważa się, że w przyszłości podstawą wojen będą ataki sieciowe zamiast bezpośrednich działań zbrojnych, ponieważ Internet jest już podstawą działania wielu krajów, co w znaczący sposób upraszcza atak i sparaliżowanie atakowanego państwa.

Z uwagi na wzrost zagrożeń ze strony sieci publicznych, od których całkowita separacja jest niemożliwa, a także fakt rozproszonej odpowiedzialności za bezpieczeństwo teleinformatyczne, niezbędne jest skoordynowanie działań w zakresie zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni, które umożliwią szybkie i efektywne reagowanie na ataki wymierzone przeciwko systemom, sieciom teleinformatycznym i oferowanym przez nie usługom.

**1) Cyberterroryzm może przybierać trzy zasadnicze formy:**

a)Włamania – łącznie z nielegalnym pozyskaniem, usuwaniem lub zmianą danych) i blokady serwerów, które podlegają na zmianie lub uszkodzeniu systemów operacyjnych
i doprowadzeniu do wielokrotnych połączeń zarówno atakowanego serwera, jak i innych serwerów.

b) Wirusów – programów działających wbrew woli użytkownika systemu i na jego szkodę. Najczęściej przeznaczone są do uszkadzania baz danych i systemów operacyjnych.

c) Ataku konwencjonalnego – polega na fizycznym uszkodzeniu elementów systemu komputerowego, serwerów, infrastruktury telekomunikacyjnej (lotniska, koleje, m.in.).
W zależności od sposobu atak tego typu może prowadzić do czasowego paraliżu systemu lub nieodwracalnej utraty danych.

W każdej jednostce organizacyjnej, w ramach ochrony cyberprzestrzeni, kierownik jednostki musi ustanowić system zarządzania bezpieczeństwem informacji w cyberprzestrzeni, w oparciu o obowiązujące normy i najlepsze praktyki, z którego wynikać powinny m.in. role administratorów i inspektorów bezpieczeństwa informacji przetwarzanych w jawnych systemach i sieciach teleinformatycznych. Zgodnie z obowiązującymi przepisami podmioty publiczne realizujące zadania publiczne zobowiązane są do posiadania własnych polityk bezpieczeństwa. Podmiot publiczny opracowuje, modyfikuje w zależności od potrzeb oraz wdraża politykę bezpieczeństwa dla systemów teleinformatycznych używanych przez ten podmiot do realizacji zadań publicznych. Przy opracowywaniu polityki bezpieczeństwa, podmiot publiczny powinien uwzględnić postanowienia Polskich Norm z zakresu bezpieczeństwa informacji, a w szczególności grupy norm serii PN ISO/IEC 27000 i innych norm z nią powiązanych.

**2) Cel ataku cybernetycznego może być różny i skierowany na:**

a) zniszczenie systemu informatycznego;

b) kradzież danych;

c) szpiegostwo;

d) czasowe unieruchomienie systemu;

e) czasowe przejęcie kontroli nad systemem;

f) wprowadzanie fałszywych danych, m.in.

**3) Rodzaje zagrożenia:**

a) HAKING (nie jest zagrożeniem bezpieczeństwa państwa, traktowany w kategoriach kryminalnych)

motywacja: pozapolityczna i pozaekonomiczna

cel ataków: skuteczny atak, sam w sobie

szkody: brak lub bardzo małe

b) HAKTYWIZM (może być zagrożeniem bezpieczeństwa państwa lub działaniem kryminalnym)

motywacja: problem (konflikt) polityczny/społeczny;

cel ataków: zwrócenie uwagi społeczeństwa i rządu na określoną kwestię, przeniesienie konfliktu na nową płaszczyznę

szkody: ograniczone, mają charakter utrudnień, uciążliwości m.in.

Przestępstwa komputerowe leżą w zainteresowaniu zarówno zorganizowanych grup przestępczych, które wykorzystują Internet i systemy komputerowe jako nowy instrument prowadzenia nielegalnej działalności, jak i pojedynczych cyberprzestępców. Przestępstwa komputerowe obejmują przestępstwa, w których przetwarzanie danych jest przedmiotem czynności wykonawczych (przestępstwa komputerowe sensu stricto) oraz przestępstwa, w których komputer jest jedynie środkiem do jego popełnienia (przestępstwa komputerowe sensu largo). Do przestępstw komputerowych sensu stricto zaliczyć możemy m.in. hakerstwo, sabotaż komputerowy, a do przestępstw komputerowych sensu largo – oszustwo komputerowe, bądź piractwo komputerowe.

Mając na względzie prognozowany wzrost przestępczości popełnianej z wykorzystaniem Internetu i zaawansowanych technologii, a co za tym idzie, potrzebę bezpośredniej i szybkiej wymiany informacji pomiędzy organami ścigania, a społeczeństwem Wydział Wsparcia Zwalczania Cyberprzestępczości Biura Służby Kryminalnej Komendy Głównej Policji dostrzega konieczność funkcjonowania punktu kontaktowego drogą elektroniczną przeznaczonego do przekazywania informacji pomocnych w zwalczaniu cyberprzestępczości. Informacje, które mogą okazać się przydatne w zwalczaniu cyberprzestępczości należy przesyłać na adres poczty elektronicznej: cyber-kgp@policja.gov.pl Starosta Powiatu Mieleckiego, w ramach ochrony cyberprzestrzeni, ustanowił system zarządzania bezpieczeństwem informacji w cyberprzestrzeni, wdrażając własną politykę bezpieczeństwa, co stanowi Zarządzenie nr 82/2017 Starosty Powiatu Mieleckiego z dnia 6 listopada 2017 roku w sprawie ustalenia zasad bezpieczeństwa informacji w Starostwie Powiatowym w Mielcu, które określa tryb postępowania w sytuacji naruszenia zabezpieczeń sprzętu informatycznego oraz rolę administratorów i inspektorów bezpieczeństwa informacji przetwarzanych w jawnych oraz niejawnych systemach i sieciach teleinformatycznych.