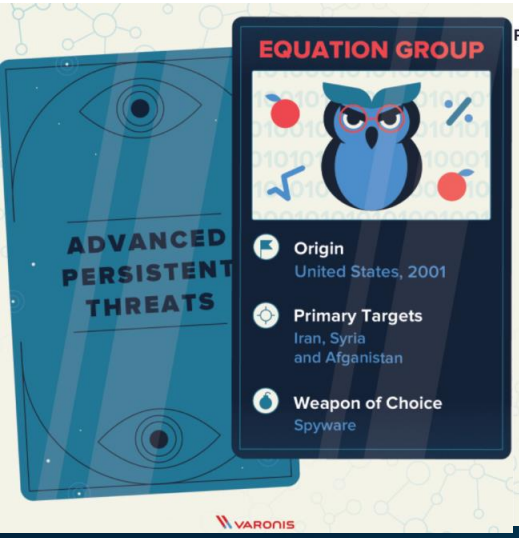
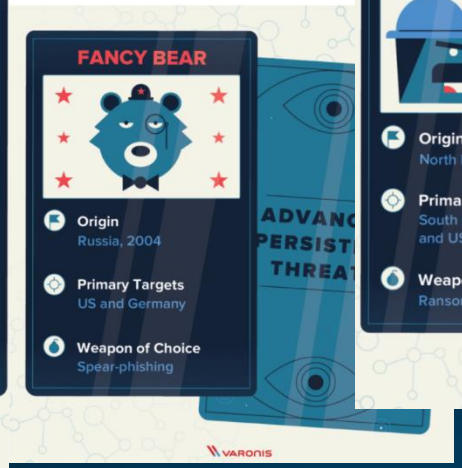
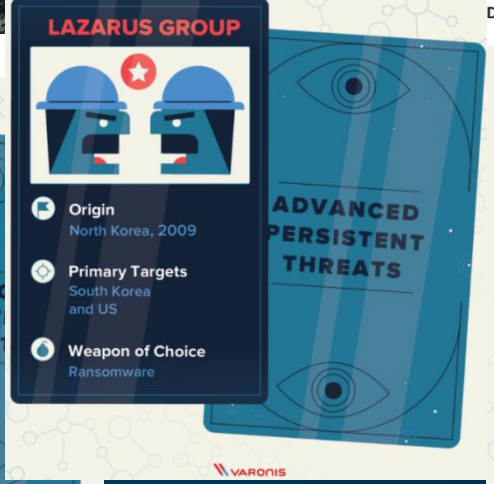


Fancy Bear (APT 28)



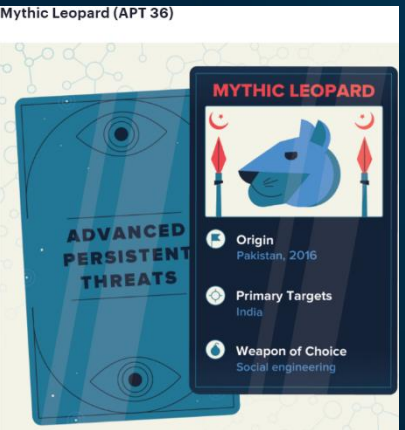


Dynamite Panda (APT 18)

Elfin (APT 33)

Machete

Mythic Leopard (APT 36)



CYBERBEZPIECZEŃSTWO W WYMIARZE WOJSKOWYM

Dr hab. inż. Stanisław Stanek, Prof. AWL

Stanislaw.Stanek@awl.edu.pl

OceanLotus (APT 32)

Charming Kitten

WYDZIAŁ ZARZĄDZANIA

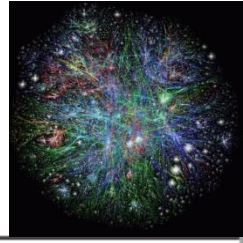
Plan spotkania

- Podstawowe pojęcia i modele.
- Wojna informacyjna.
- Charakterystyka wybranych cyberarmi.
- Zwięzły przegląd aktów prawnych regulujących funkcjonowanie cyberprzestrzeni
- Prawne aspekty bezpieczeństwa cyberprzestrzeni
- Zarys problematyki wyzwań i zagrożeń występujących w cyberprzestrzeni.
  - Klasyfikacja cyberataków.
  - Klasyfikacja programów złośliwych.
- Elementy problematyki ataków APT.

Słuchacz:

- zna istotę cyberbezpieczeństwa;
- zna zasady identyfikacji podstawowych zagrożeń cyberbezpieczeństwa;
- zna i rozumie wybrane definicje cyberbezpieczeństwa zawarte w ustawie z dnia 5 lipca 2018 r o krajowym systemie cyberbezpieczeństwa oraz dokumentach NATO;
- potrafi określić podział ról w czasie współdziałania układu militarnego podmiotami układu pozamilitarnego
- Potrafi odbierać ze zrozumieniem, tworzyć i przedstawiać umiarkowanie złożone wypowiedzi dotyczące roli i miejsca cyberbezpieczeństwa.

6. Cele wykładu.



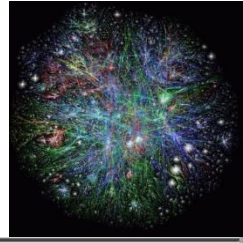
Pojęcie cyberprzestrzeni. Ujęcie literackie

(...) To jest cyberprzestrzeń. Konsensualna halucynacja doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach. Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność (...)

1984 rok publikacji *Neuromancera * Williama Gibsona - powieści, która w zgodnej opinii specjalistów zapoczątkowała nurt fantastyki cyberpunkowej (zob. cyberpunk), konstytuując jej główne założenia.

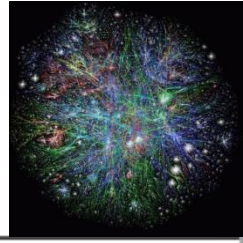
W wykreowanym w Neuromancerze świecie - w celu zwiększenia możliwości ludzkiego organizmu - stosowane są cybernetyczne rozszerzenia (tzw. deki, będące szczególnym rodzajem *wszczepów* biofeedback) zdolne m.in. wymieniać informacje ze światową siecią komputerową. Bohater, poruszający się w ten sposób w sieci, znajduje się w cyberprzestrzeni.

(…) To jest cyberprzestrzeń. Konsensualna halucynacja doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach. Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność (…)



Elementy wiwisekcji przemian kulturowych w literaturze cyberpunk

- Specyficzny bohater zna się na komputerach, włamuje się do ich systemów (hackers), systemów telefonicznych i teleinformatycznych (phreakers); łamie cyfrowe kody (cyphers), łamie zabezpieczenia programów (crackers). – nie jest to naganne bo działa w imię buntu przeciwko wszechwładzy ponowoczesnych korporacji.
- Powstaje ruch kontrkulturowy o nowym kształcie społecznym. Już nie hippisi głoszący „powrót do natury”, jeszcze bywalcy miejskiej przestrzeni wyposażeni w nowoczesne technologie, młodzi realizują archetyp wyobcowania oraz poszukiwania własnej drogi krytycznie kalkulując ryzyko cyberprzestrzeni głosząc dogmat „high tech & low life”.
- Wizja cyborga sieciowego – nowa SI powstająca w kontekście symbiozy człowieka i maszyny – z jednej strony „kiedy każdy »naturalny« organ może być bez końca zastępowany »sztuczną« protezą, a całość zawartości umysłu może być przechowywana dzięki załadowaniu w matriks, marzenie o nieśmiertelności staje się możliwe do zrealizowania”. Z drugiej strony sztuczny mózg Eugene Goostman może wydawać się atrakcyjnym rozmówcą.
- Dialektyczna tęsknota za Światem Otwartym wynurza się jako wyzwanie.



Trzy grupy definicji cyberprzestrzeni

zestawione na stronie Centrum Doskonalenia Cyberobrony NATO

1. Najliczniejszą grupą są definicje technokratyczne, sytuujące cyberprzestrzeń w obszarze połączonych infrastruktur informatycznych, jako przedłużenie oraz rozszerzenie globalnej intra Sieci Internet.

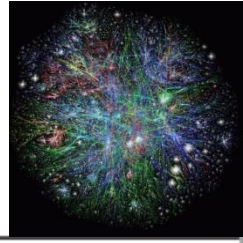
(Niemiecka) Wirtualna przestrzeń wszystkich systemów IT połączonych w skali globalnej na poziomie danych. Podstawą cyberprzestrzeni jest Internet będący powszechną i ogólnodostępną siecią połączeń i transportu, który może być uzupełniany oraz rozszerzany poprzez dowolną liczbę dodatkowych sieci danych. Systemy IT w izolowanej przestrzeni wirtualnej nie są częścią cyberprzestrzeni.

Trzy grupy definicji cyberprzestrzeni

zestawione na stronie Centrum Doskonalenia Cyberobrony NATO

2. Kilka definicji organizacyjnych plasuje pojęcie cyberprzestrzeni szerzej, w obszarze rozwoju społeczno-technicznego. To podejście jest dobrze osadzone w kontekście badań nad stykiem techniki i społeczeństwa (ultrastykiem), technopolią, odkrywaną w obliczu szybkich zmian technologii jej relacją z kulturą.

(Węgry) Cyberprzestrzeń oznacza powiązane zjawiska zarówno globalnie połączonych, zdecentralizowanych i ciągle rosnących elektronicznych systemów informacyjnych, jak również procesów społecznych i gospodarczych przejawiających się w tych systemach w postaci danych i informacji.



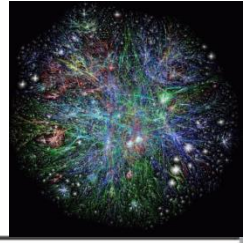
Trzy grupy definicji cyberprzestrzeni

zestawione na stronie Centrum Doskonalenia Cyberobrony NATO

3. Kilka innych definicji nowego świata eksponuje, że cyberprzestrzeń jest nową jakością (przestrzenią, środowiskiem, światem, domeną) wyodrębniającą się oraz manifestującą się w szczególny sugerowany w tych definicjach sposób.

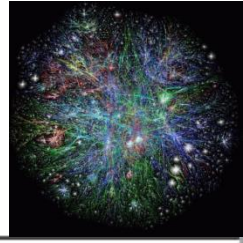
(Słownik Oxford) Hipotetyczne środowisko, w którym zachodzi komunikacja z wykorzystaniem sieci komputerowych.

(ISO/IEC 27032) Kompleksowe środowisko powstające w wyniku interakcji ludzi, oprogramowania oraz usług w Internecie z wykorzystaniem technologii, urządzeń oraz przyłączonych do nich sieci, które nie istnieje w żadnej formie fizycznej.



Definicja STRATEGICZNA

- W przyjętej w 2003 r. Narodowej Strategii dla Bezpiecznej Cyberprzestrzeni zapisano:
- Nasza Krajowa infrastruktura krytyczna jest budowana przez publiczne, jak i prywatne instytucje funkcjonujące w sektorach rolnym, żywieniowym, zaopatrzenia w wodę, służby zdrowia, usług ratunkowych, rządowym, obronnym, przemysłowym, informacyjnym oraz telekomunikacyjnym, energetycznym, transportowym, bankowym oraz finansowym, chemicznym oraz materiałów niebezpiecznych, a także pocztowym oraz dostawczym.
- Cyberprzestrzeń stanowi ich układ nerwowy – system kontrolny naszego kraju.
- **Cyberprzestrzeń jest zbudowana z setek tysięcy połączonych komputerów, serwerów, routerów, switchy oraz światłowodów, które umożliwiają pracę naszej infrastrukturze krytycznej**.
- Stąd też zdrowe funkcjonowanie cyberprzestrzeni jest kluczowe dla naszej ekonomii oraz bezpieczeństwa narodowego



Definicja USTAWOWA

ustawa z 30 sierpnia 2011 O zmianie ustawy o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw.

Wykorzystywane jest pojęcie **telekomunikacyjne urządzenie końcowe**, które w prawie telekomunikacyjnym jest definiowane, jako (…) **urządzenie telekomunikacyjne przeznaczone do podłączenia bezpośrednio lub pośrednio do zakończeń sieci**.

Z kolei zgodnie z określeniem w art. 3 pkt 3 ustawy z 17 lutego 2005 r. O informatyzacji działalności podmiotów realizujących zadania publiczne **system teleinformatyczny, to (…) zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego**".

Mając wyjaśnione te pojęcia możemy obecnie przytoczyć zmodyfikowaną po raz kolejny, funkcjonującą obecnie w systemie prawnym naszego kraju definicję cyberprzestrzeni:

(…) **Przez cyberprzestrzeń rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami.**

Przypomnienie podstawowych pojęć
Bezpieczeństwo

Pojecie bezpieczeństwa

- Według „Słownika nauk społecznych" **bezpieczeństwo** jest synonimem pewności (ang. *safety*) i oznacza **brak zagrożenia (ang. *danger*) fizycznego albo ochronę przed nim.**
- W najogólniejszym znaczeniu obejmuje ono zaspokojenie takich potrzeb, jak: istnienie, przetrwanie, całość, tożsamość, niezależność, spokój i pewność rozwoju.
- Można mówić o bezpieczeństwie konkretnego podmiotu, np. osoby, grupy ludzi, jednostki organizacyjnej, państwa, narodu, zakładu, miasta, regionu itp.
- Z pojęciem „**bezpieczeństwo**" **podmiotu** ściśle związane jest pojęcie „**zagrożenie**" **podmiotu**, które jest jego antonimem.
- **Zagrożenie** odnosi się do sfery świadomościowej danego podmiotu (człowieka, grupy społecznej, narodu) i oznacza pewien **stan psychiki lub świadomości wywołany postrzeganiem zjawisk ocenianych jako niekorzystne lub niebezpieczne**.

Jakie są uwarunkowania dostępu do informacji?

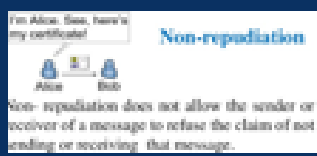
1. Nadanie identyfikatora (ciągu znaków lub wzorca) przypisanego do podmiotu oraz określającego jego tożsamość.
2. Uzgodnienie danych uwierzytelniających (np. hasło, certyfikat elektroniczny, token, kod jednorazowy, figura geometryczna, tożsamość z portalu społecznościowego, wspólna wiedza), które są przekazywane w celu ustalenia deklarowanej tożsamości podmiotu. Obecnie coraz częściej postuluje się, aby wykorzystywać jednocześnie różnego rodzaju dane uwierzytelniające (zwykle dwa rodzaje).
3. Identyfikowanie – proces rozpoznawania tożsamości podmiotu (poprzez przedstawienie identyfikatora). Wiadomo, za kogo podmiot się podaje, ale nie jest to jeszcze potwierdzone.
4. Uwierzytelnianie – weryfikowanie deklarowanej tożsamości podmiotu za pomocą danych uwierzytelniających. Zauważmy tutaj, że identyfikowanie i uwierzytelnianie może następować równolegle (np. gdy identyfikator stanowi jednocześnie hasło).
5. Z technicznego punktu widzenia możliwość dostępu do danego aktywu wymaga jeszcze autoryzacji tzn. przyznania dostępu na podstawie praw dostępu. Zezwolenie na dostęp do aktywu również określane jest terminem autoryzacji. Podmiot może mieć różne tożsamości, które umożliwiają mu dostęp do różnych konkretnych aktywów.

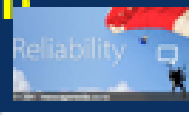
Cyberbezpieczeństwo

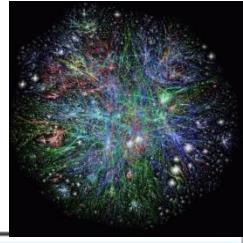
Cyberbezpieczeństwo - odporność systemów informacyjnych na działania naruszające poufności, integralności, dostępności i autentyczności przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

3. Cyberbezpieczeństwo

1. **Poufność** - zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom podmiotom lub procesom
2. **Integralność** - zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
3. **Dostępność** - zapewnienie bycia osiągalnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot.
4. **Uwierzytelnianie / Autentyczność** - zapewnienie, że tożsamość podmiotu lub zasobu jest taka. jak deklarowana (dotyczy użytkowników, procesów, systemów i informacji),
5. **Rozliczalność** - zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
6. **Niezaprzeczalność** - braku możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie
7. **Niezawodność** - zapewnieniu spójności oraz zamierzonych zachowań i skutków.





Cyberbezpieczeństwo

Środki odnoszące się do poufności, dostępności i integralności informacji, które są przetwarzane, przechowywane i przekazywane za pomocą technologii elektronicznych lub podobnych.

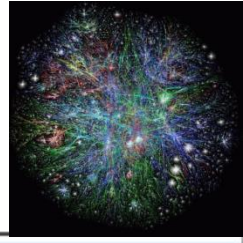
Cyberbezpieczeństwo jest pożądanym celem sytuacji, w której zagrożenia globalnej cyberprzestrzeni zostały zredukowane do akceptowalnego minimum.

Cyberbezpieczeństwo (w Niemczech) jest sumą odpowiednich i właściwych środków.

Cywilne cyberbezpieczeństwo skupia się na wszystkich systemach informatycznych do użytku cywilnego w niemieckiej cyberprzestrzeni.

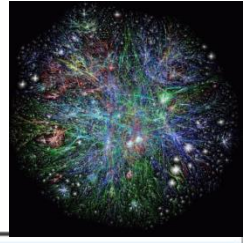
Wojskowe cyberbezpieczeństwo skupia się na wszystkich systemach informatycznych do użytku wojskowego w niemieckiej cyberprzestrzeni.

•White Paper 2006 on German Security Policy and the Future of the Bundeswehr



Cyberbezpieczeństwo - pożądany stan systemu informatycznego, w którym jest on w stanie oprzeć się zdarzeniom z cyberprzestrzeni mogącym zagrozić dostępności, integralności lub poufności przechowywanych, przetwarzanych lub przesyłanych danych oraz związanych z nimi usług, które te systemy oferują lub udostępniają.

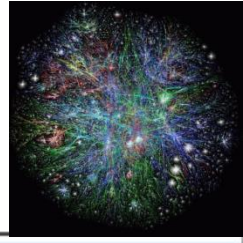
Cyberbezpieczeństwo wykorzystuje techniki bezpieczeństwa systemów informatycznych i opiera się na zwalczaniu cyberprzestępczości i tworzeniu cyberobrony.



Cyberbezpieczeństwo

Cyberbezpieczeństwo - działania podejmowane w celu zmniejszenia ryzyka i zabezpieczenia korzyści płynących z zaufanego środowiska cyfrowego dla przedsiębiorstw i osób fizycznych.

A Strong Britain in an Age ofUncertainty:The National Security Strategy, 2010

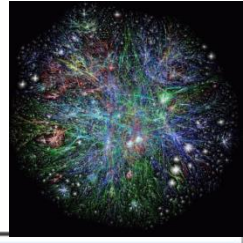


Cyberbezpieczeństwo

Cyberbezpieczeństwo to wolność od zagrożenia lub szkody wynikającej z zakłócenia, awarii lub niewłaściwego wykorzystania TIK.

Niebezpieczeństwo lub szkoda wynikające z zakłócenia, awarii lub niewłaściwego użycia może polegać na ograniczeniu dostępności lub niezawodności TIK, naruszeniu poufności informacji przechowywanych na nośnikach TIK lub uszkodzeniu integralności tych informacji.

NL: Strategie Nationale Veiligheid, 2007



Cyberbezpieczeństwo miltarne

Bezpieczeństwo wojskowe oznacza zdolność państwa narodowego do obrony i/lub powstrzymania agresji wojskowej.

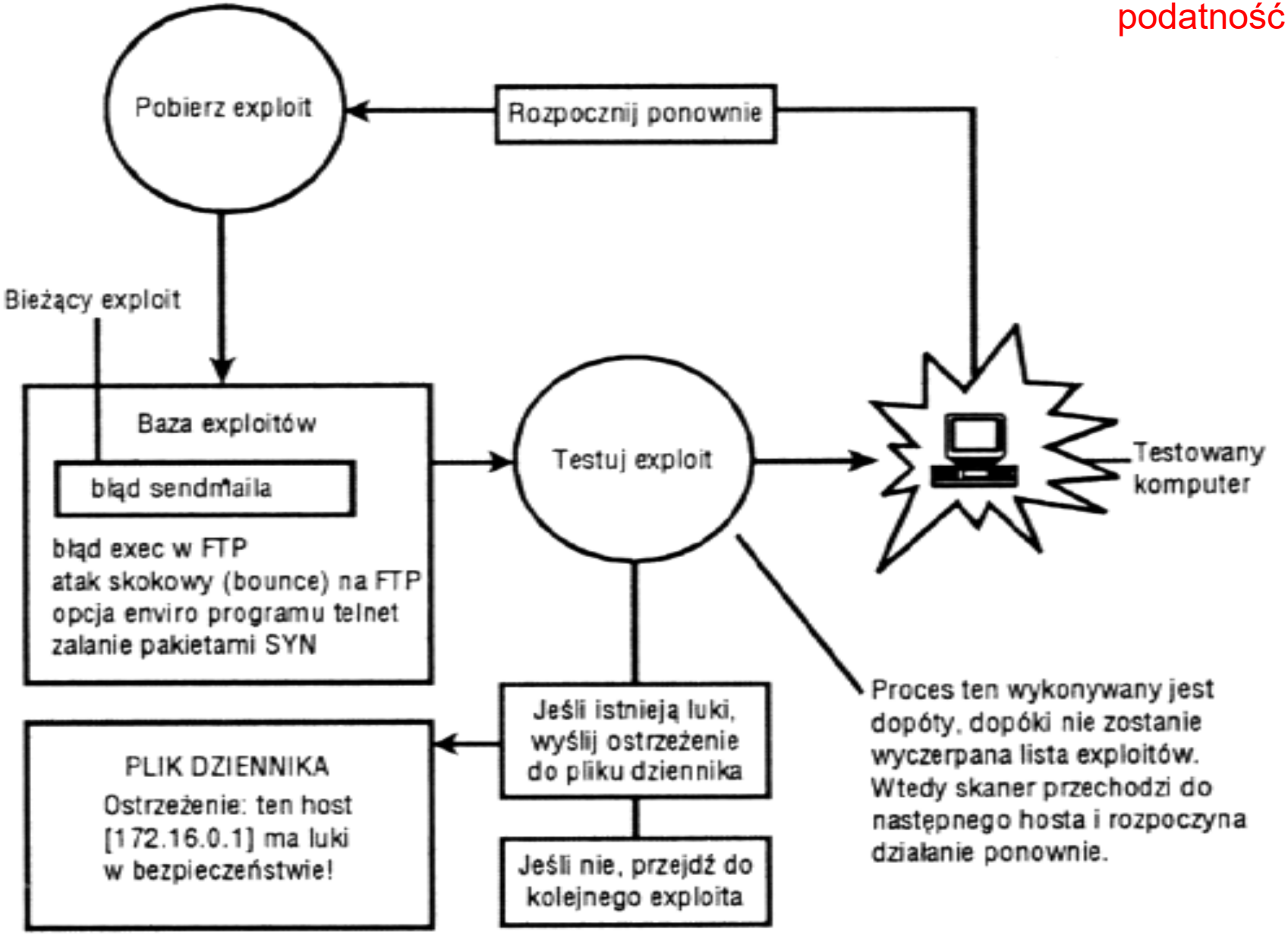
Alternatywnie, bezpieczeństwo militarne implikuje zdolność państwa narodowego do egzekwowania swoich wyborów politycznych poprzez użycie siły militarnej.

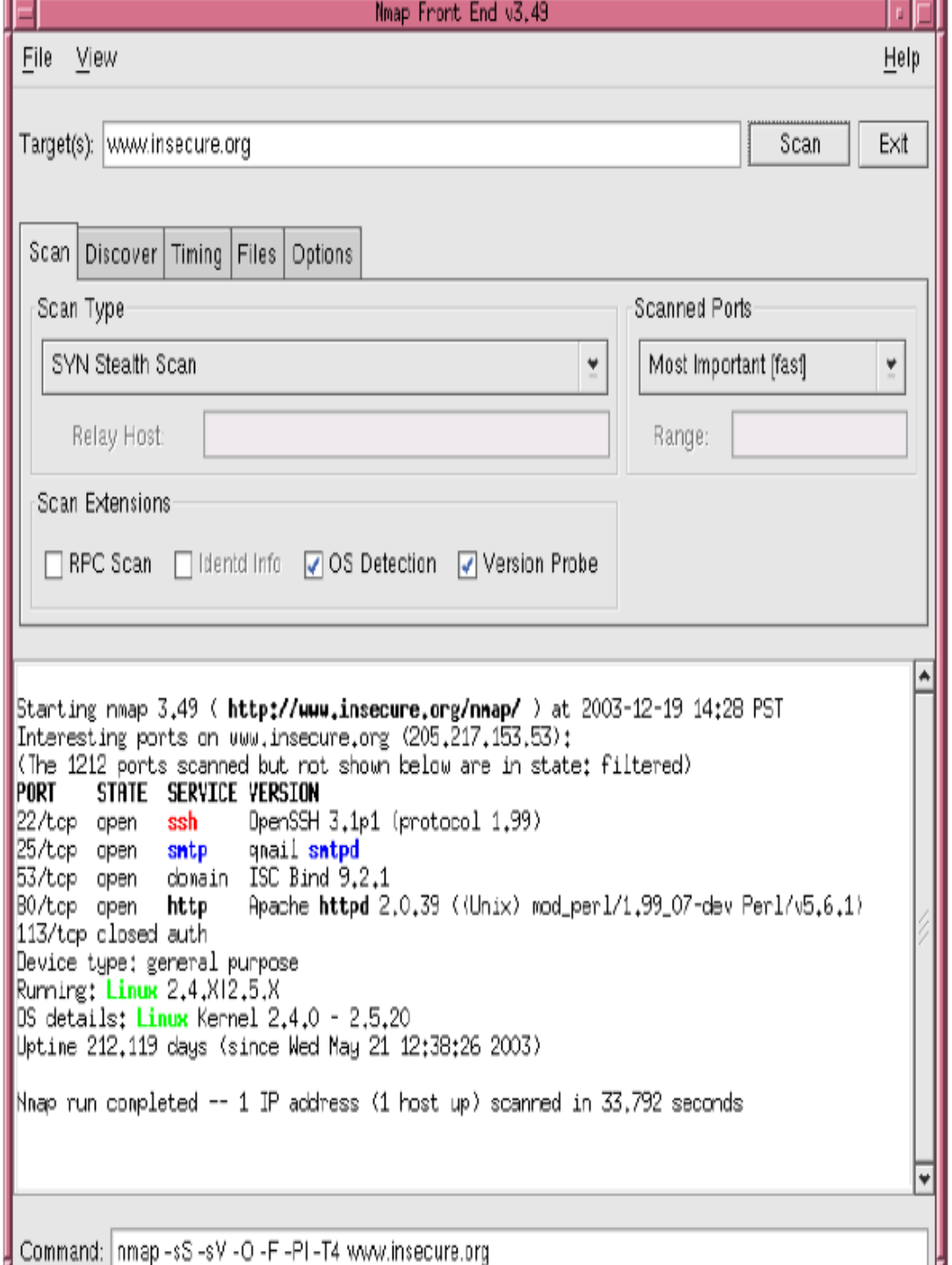
NL: Strategie Nationale Veiligheid, 2007

Jakie są podstawowe elementy modelu bezpieczeństwa informacji?

Skanery sieciowe opierają zazwyczaj swoje działanie na zasadzie przedstawionej na ilustracji:

Exploit – luka, podatność





Skanowanie nmapem

Co to jest incydent, gdzie zgłaszamy incydenty oraz analizujemy statystyki?

Incydent związane z bezpieczeństwem informacji to pojedyncze zdarzenie lub seria niepożądanych czy niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które **stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.**

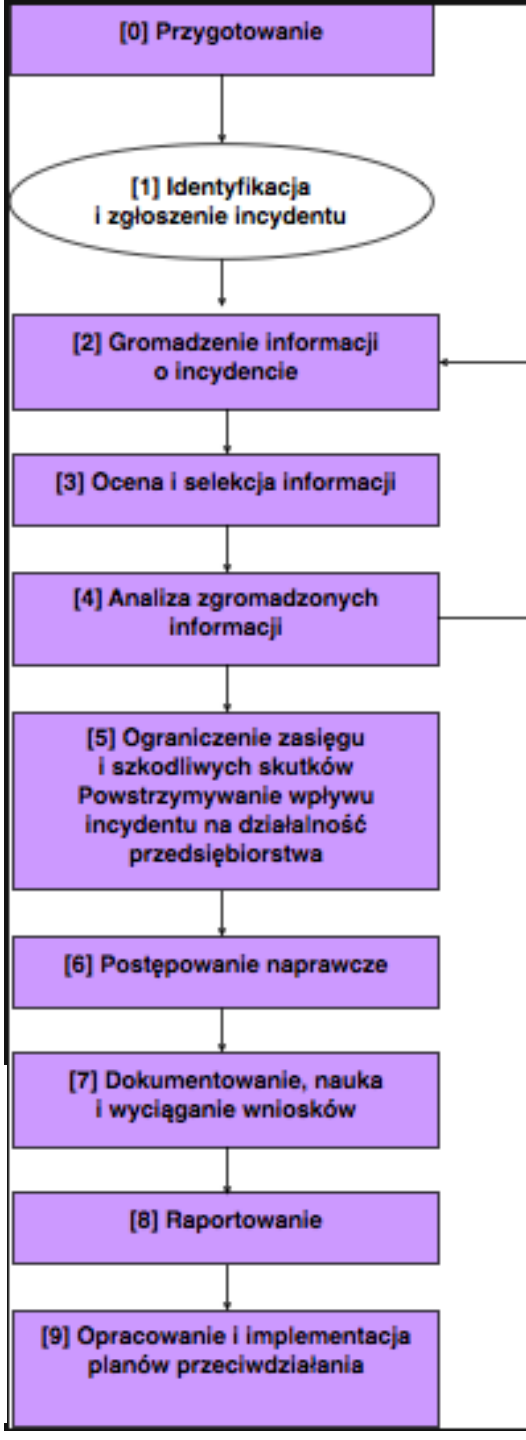
Łuczak Tyburski str. 28-29 SYSTEMOWE ZARZĄDZANIE BEZPIECZESTWEM INFORMACJI wg ISO/IEC **27001**

6. Reagowanie na incydenty

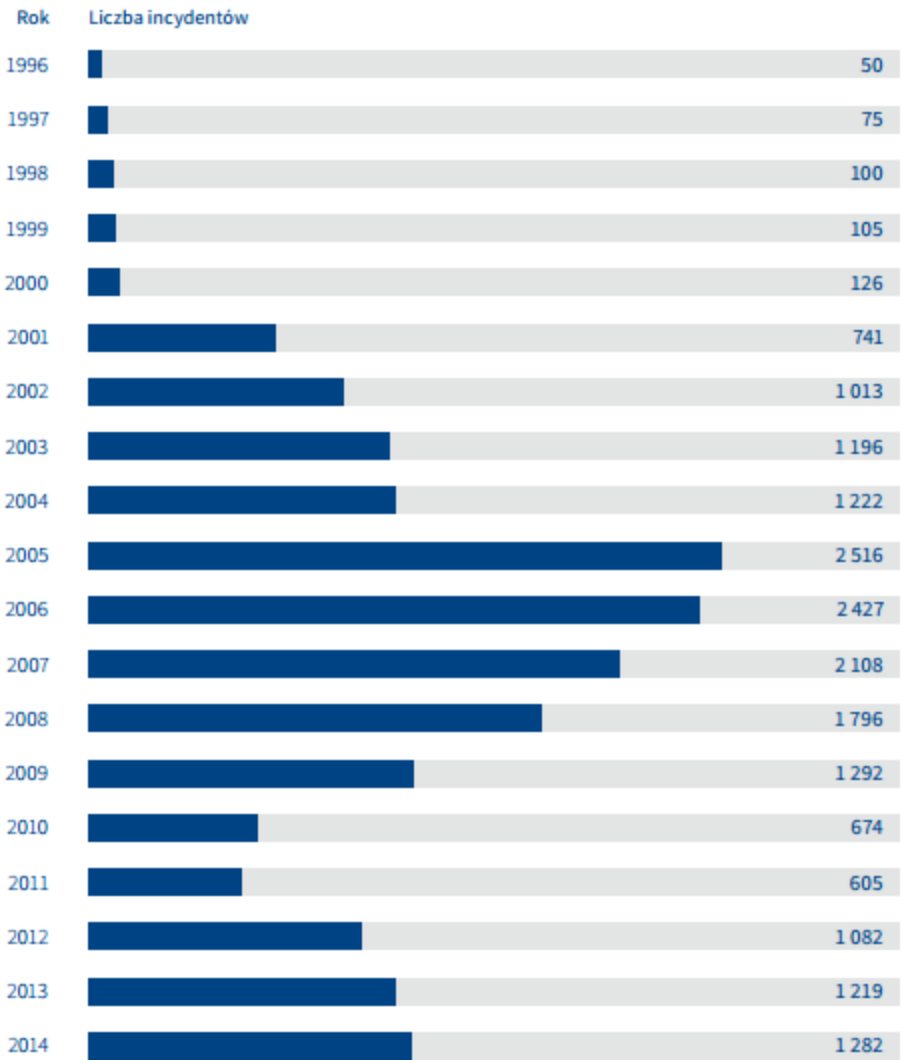
Tab. 1. Przykłady incydentów

Incydent
Mafiosi zdobyli kompletne dane klientów banku Millennium wraz ze wzorami podpisów. Prawdopodobnie sprzedał je jeden z pracowników banku. Dzięki temu gangsterzy wyczyścili kilka kont, kradnąc kilkaset tysięcy złotych.
Ściśle tajne materiały wojskowe, dotyczące m.in. nowoczesnych systemów bojowych Aegis w marynarce wojennej Japonii, przeciekły do wiadomości publicznej, ponieważ dołączone zostały do pornograficznych zdjęć, którymi wymieniali się marynarze.
Uwaga złe psy– pojawiło się na stronie WWW suwalskiej policji. Włamano się na serwer http://www.suwalki.policja.gov.pl/ i umieszczono złośliwe zdjęcie.
Przestępcy z grupy zwanej Warez City włamywali się do serwerów i zajmowali pamięć komputerów uczelni technicznych oraz banków, które mają największą pamięć i najszybsze łącza. Dyski, do których się dostali, służyły im jako magazyny na nielegalne oprogramowania, filmy, muzykę i skradzione bazy danych. Hakerzy mieli nieograniczony dostęp m.in. do baz osobowych takich instytucji, jak ZUS czy banki. Straty, jakie wyrządzili, szacuje się na setki milionów dolarów. (Jeden z nich pracował w banku jako administrator sieci komputerowej).
Na oficjalnej stronie Wielkiej Firmy Polska umieszczono prywatny numer telefonu (?) osoby do kontaktu z klientem, a taka osoba nie pracowała w tej firmie.
Sprawcą kradzieży ok 650 tys zł w firmie okazał się administrator sieci, z której łączono się z umieszczonym na zainfekowanym komputerze koniem trojańskim. Mógł on skutecznie zacierać ślady swojej działalności, udzielać błędnych informacji i tym samym utrudniać policyjne działania.
Gigantyczna burza spowodowała zakłócenia w sieci energetycznej – nagłe skoki napięcia uszkodziły system informatyczny banku, który jednak mimo to nie przerwał obsługi klientów, ale przeszedł na systemy awaryjne. Dla klientów oznaczało to jednak ograniczenia w obsłudze kart płatniczych. Usuwanie awarii trwało ponad tydzień!

- zainfekowanie systemu na dużą skalę przez wirusa lub robaka,
- przerwanie usługi,
- wykorzystanie systemu przez pracownika w niewłaściwych celach,
- próby włamania się do komputera (udane lub nieudane) w celu uzyskania nieautoryzowanego dostępu do systemu lub jego danych,
- atak typu „odmowa usługi" (Denial of Service),
- anonimowe niewłaściwe użycie protokołu FTP,
- wprowadzenie zmian w sprzęcie lub oprogramowaniu bez wiedzy, zgody czy odpowiednich wskazówek ze strony właściciela,
- występowanie w systemie aplikacji podatnych na atak.



CERT



Obraźliwe i nielegalne treści	**370**	**28,86**
Spam	365	28,47
Dyskredytacja, obrażanie	0	0
Pornografia dziecięca, przemoc	2	0,16
Niesklasyfikowane	3	1
Złośliwe oprogramowanie	**98**	**7,64**
Wirus	0	0
Robak sieciowy	0	0
Koń trojański	8	0,62
Oprogramowanie szpiegowskie	0	0
Dialer	0	0
Niesklasyfikowane	90	7,02
Gromadzenie informacji	**98**	**7,64**
Skanowanie	13	1,01
Podsłuch	0	0
Inżynieria społeczna	0	0
Niesklasyfikowane	5	0,39
Próby włamań	**36**	**2,81**
Wykorzystanie znanych luk systemowych	4	0,31
Próby nieuprawnionego logowania	5	0,39
Wykorzystanie nieznanych luk systemowych	1	0,08
Niesklasyfikowane	26	2,03
Włamania	**13**	**1,01**
Włamanie na konto uprzywilejowane	1	0,08
Włamanie na konto zwykłe	7	0,55
Włamanie do aplikacji	0	0
Niesklasyfikowane	5	0,39
Dostępność zasobów	**69**	**5,38**
Atak blokujący serwis (DoS)	6	0,47
Rozproszony atak blokujący serwis (DDoS)	63	4,91
Sabotaż komputerowy	0	0
Niesklasyfikowane	0	0
Atak na bezpieczeństwo informacji	**25**	**1,95**
Nieuprawniony dostęp do informacji	8	0,62
Nieuprawniona zmiana informacji	0	0
Niesklasyfikowane	17	1,95
Oszustwa komputerowe	**613**	**47,82**
Nieuprawnione wykorzystanie zasobów	5	0,39
Naruszenie praw autorskich	0	0
Kradzież tożsamości, podszycie się	383	29,88
Niesklasyfikowane	225	17,55
Inne	**40**	**3,12**

Tab. 1. Czynniki wpływające negatywnie na bezpieczeństwo teleinformatyczne

Zagrożenie	Przykładowe czynniki
1	2
Utrata poufności	- pokonanie zabezpieczeń fizycznych i programowych - niekontrolowana obecność w obszarze chronionym osób nieupoważnionych - nieroztropność osób uprawnionych - wynoszenie poza strefę ochronną wydruków, przenośnych komputerów oraz elektronicznych nośników danych - naprawy oraz konserwacje przez osoby nieuprawnione - podgląd i podsłuch - elektromagnetyczna emisja ujawniająca
Utrata integralności	- przypadkowe lub celowe spowodowanie awarii systemu operacyjnego lub urządzeń systemu sieciowego - przypadkowe lub celowe uszkodzenie, zniszczenie czy też nieautoryzowana zmiana danych - celowe bądź przypadkowe uszkodzenie oprogramowania aplikacyjnego i użytkowego - wirusy komputerowe - sytuacje kryzysowe: powódź, pożar, huragan itp. - ataki terrorystyczne
1	2
Utrata dostępności	- defektywnie działający sprzęt oraz programy - awaria zasilania - wirusy komputerowe - klęski żywiołowe - ataki terrorystyczne - błędy organizacyjne

Drogoń W., Mąka D., Skawina M., Jak chronić tajemnice? Ochrona informacji w instytucjach państwowych i przedsiębiorstwach prywatnych, Wydawnictwo Bellona, Warszawa 2004.

Jakie rodzaje zagrożeń dla bezpieczeństwa informacji możemy wyróżnić?

Zagrożenia dla bezpieczeństwa teleinformatycznego

Kategoria zagrożenia	**Przykłady**
Przypadkowe błędy i pomyłki	Wypadki, błędy pracowników
Naruszenie własności intelektualnej	Piractwo, naruszenie praw autorskich
Zamierzone działania o charakterze szpiegowskim lub wtargnięcia	Nieautoryzowany dostęp lub/i gromadzenie danych
Zamierzone działania w zakresie wyłudzania informacji	Szantaż lub ujawnienie informacji
Zamierzone działania o charakterze sabotażu lub wandalizmu	Zniszczenie systemów lub informacji
Kradzież	Nielegalne skonfiskowanie sprzętu lub informacji
Zamierzone ataki na oprogramowanie	Wirusy, robaki, makra, odmowa wykonania usługi, rootkity, trojany
Siły natury	Pożar, powódź, błyskawice, trzęsienie ziemi.
Odchylenie w jakości usług	ISP, zasilanie lub usługi WAN od dostawców usług
Techniczne błędy i awarie sprzętu	Awarie sprzętu
Techniczne błędy i awarie oprogramowania	Pluskwy, problemy kodowania, luki
Technologiczne starzenie	Przestarzałe technologie

Zagrożenia dla bezpieczeństwa teleinformatycznego

Przykłady zakłóceń z jakimi są związane powyższe zagrożenia

Zakłócenia	Kradzież i defraudacja	Utrata poufności	Utrata prywatności	Brak integralności	Uniemożliwienie dostępu
Używanie cudzych praw dostępu	✓	✓	✓		
Nieuprawnione zmienianie lub kopiowanie danych	✓			✓	
Zmiana programu	✓			✓	✓
Nieodpowiednie procedury pozwalające na mieszanie poufnych i jawnych wyników	✓	✓	✓		
Podsłuch na linii przesyłowej	✓	✓	✓		
Włamanie do systemu	✓	✓	✓		
Szantaż	✓	✓	✓		
Tworzenie „tajnych wejść" do systemu	✓	✓	✓		
Kradzież danych, programów i wyposażenia	✓	✓	✓		✓
Błędy w mechanizmach zabezpieczeń dające większy zakres dostępu, niż przewidywany		✓	✓	✓	
Niedostateczna liczba pracowników lub strajki				✓	✓
Złe przeszkolenie pracowników		✓	✓	✓	✓
Przeglądanie i ujawnianie danych bez prawa dostępu	✓	✓	✓		

Zagrożenia dla bezpieczeństwa teleinformatycznego

Przykłady zakłóceń

Zakłócenia	Kradzież i defraudacja	Utrata poufności	Utrata prywatności	Brak integralności	Uniemożliwienie dostępu
Wpływ innych urządzeń i napromieniowania na nośniki elektroniczne				✓	✓
Zniszczenie danych w efekcie skoku napięcia				✓	✓
Pożar (spięcie elektryczne, piorun, podpalacz), powódź, bomba				✓	✓
Fizyczne zniszczenie sprzętu				✓	✓
Przerwanie lub rozłączenie przewodów				✓	✓
Wprowadzenie wirusów				✓	✓

Instytucja musi określić rodzaje zagrożeń, które mogą jej dotyczyć, i uruchomić odpowiednie procedury i zabezpieczenia, mając świadomość kosztów ich wdrożenia. Oczywiście ponoszenie dużych nakładów pracy, czasu i kosztów może nie być opłacalne, gdy potencjalne zagrożenia mogą spowodować jedynie niewielkie niedogodności. Z drugiej strony działalność firmy może być podatna na pewne rodzaje zagrożeń, które należy wziąć pod uwagę, gdyż, choć bardzo rzadkie, mogą spowodować znaczne straty.

W klasyfikacji J. Kowalewskiego oraz M. Kowalewskiego zdefiniowano pięć klas podstawowych, z których każda zawiera kilka zagrożeń:

1. Siły wyższe (np. utrata personelu, pożar, woda, silne pole magnetyczne).
2. Uchybienia organizacyjne (np. brak uregulowań lub ich niestosowanie).
3. Błędy ludzkie (np. błędy popełniane przez użytkowników systemów).
4. Błędy techniczne (np. słaba jakość uwierzytelniania lub jej brak).
5. Działania rozmyślne (np. manipulowanie danymi lub oprogramowaniem).

Tabl. 2.1. Podstawowy zbiór zagrożeń kategorii „Siły wyższe"

Lp.	Nazwa zagrożenia	Rezultat zagrożenia
1.	Utrata personelu	Utrata dostępności, dezorganizowanie systemu, straty finansowe
2.	Wyładowania atmosferyczne	Utrata dostępności, integralności, straty finansowe
3.	Pożar	Utrata dostępności, utrata dokumentów i nośników informacji, straty finansowe
4.	Woda	Utrata dostępności i niezawodności, straty finansowe
5.	Zagrożenia środowiskowe	Utrata dostępności i niezawodności, utrata dokumentów i nośników informacji, straty finansowe
6.	Uszkodzenia systemów przetwarzania informacji	Utrata dostępności, utrata dokumentów i nośników informacji, straty finansowe
7.	Silne pola magnetyczne	Utrata dostępności, straty finansowe

Źródło: Kowalewski M. i in., *Zagrożenia dla infrastruktury telekomunikacyjnej i teleinformatycznej.* Praca zbiorowa [w:] *Modele zagrożeń aglomeracji miejskiej wraz z systemem zarządzania kryzysowego na przykładzie miasta stołecznego Warszawy*, red. A. Najgebauer, Warszawa 2009.

Tabl. 2.2. Podstawowy zbiór zagrożeń kategorii „Uchybienia organizacyjne"

Lp.	Nazwa zagrożenia	Rezultat zagrożenia
1.	Brak uregulowań organizacyjnych lub ich niestosowanie	Utrata poufności, dezorganizacja w pracy i systemie bezpieczeństwa, zły wizerunek organizacji, straty finansowe
2.	Zła organizacja pracy w procesie gromadzenia, przetwarzania, przesyłania i przechowywania informacji	Utrata poufności, wiarygodności, dezorganizacja w pracy i systemie bezpieczeństwa, zły wizerunek organizacji, straty finansowe
3.	Brak monitorowania i analizowania zagrożeń oraz zabezpieczeń	Dezorganizacja w pracy i systemie bezpieczeństwa, straty finansowe
4.	Niewłaściwie zorganizowane utrzymanie i eksploatowanie w systemie bezpieczeństwa informacji	Utrata poufności, integralności, wyciek informacji i danych, dezorganizacja w pracy, fałszywe alarmy, zły wizerunek organizacji, straty finansowe
5.	Dostęp do systemów bezpieczeństwa informacji osób nieuprawnionych	Utrata poufności, fałszywy alarm, straty finansowe
6.	Utrata bezpieczeństwa informacji jako rezultat utraty poufności, integralności i dostępności informacji	Utrata poufności, autentyczności, integralności danych, zły wizerunek organizacji, straty finansowe
7.	Niewłaściwe zarządzanie kluczami szyfrującymi	Utrata poufności, autentyczności, niezawodności, integralności danych, straty finansowe
8.	Niewłaściwe zarządzanie systemem bezpieczeństwa informacji i jego zasobami	Dezorganizacja, niezdolność do realizacji zadań, zły wizerunek organizacji, straty finansowe

Źródło: Kowalewski M. i in., *Zagrożenia dla infrastruktury...*

Tabl. 2.3. Podstawowy zbiór zagrożeń kategorii „Błędy ludzkie"

Lp.	Nazwa zagrożenia	Rezultat zagrożenia
1.	Błędy popełniane przez użytkowników systemów teleinformatycznych	Utrata wiarygodności, zły wizerunek organizacji, straty finansowe
2.	Niedbalstwo w wykonywaniu powierzonych obowiązków, niestosowanie podstawowych zasad zapewnienia bezpieczeństwa informacji	Utrata wiarygodności, zły wizerunek organizacji, straty finansowe
3.	Niewłaściwe administrowanie systemem teleinformatycznym	Utrata poufności, wiarygodności, straty finansowe
4.	Niewłaściwe użytkowanie systemu teleinformatycznego	Utrata poufności, wiarygodności, straty finansowe
5.	Nadużycia w zakresie ochrony kryptograficznej	Utrata poufności, wiarygodności, straty finansowe
6.	Niewłaściwe obchodzenie się z informacjami i danymi	Utrata poufności, wiarygodności, integralności, zły wizerunek organizacji, straty finansowe

Źródło: Kowalewski M. i in., *Zagrożenia dla infrastruktury...*

Tabl. 2.4. Podstawowy zbiór zagrożeń kategorii „Błędy techniczne"

Lp.	Nazwa zagrożenia	Rezultat zagrożenia
1.	Przerwy i zakłócenia w sieci energetycznej	Zakłócenia transmisji, straty finansowe
2.	Brak dyspozycyjności i zabezpieczeń w toku eksploatacji urządzeń i systemów teleinformatycznych	Utrata wiarygodności, chaos organizacyjny, straty finansowe
3.	Uszkodzenia systemów technicznych	Utrata integralności, dezorganizacja, straty finansowe
4.	Podatność oprogramowania	Utrata poufności, dostępności, integralności, niezawodności, rozliczalności, straty finansowe
5.	Złożoność dostępu w systemie	Dezorganizacja, straty finansowe
6.	Słaba jakość uwierzytelniania lub jej brak	Utrata dostępności, poufności i integralności

Źródło: Kowalewski M. i in., *Zagrożenia dla infrastruktury...*

Zagrożenia dla bezpieczeństwa teleinformatycznego

Tabl. 2.5. Podstawowe zagrożenia kategorii „Działania rozmyślne"

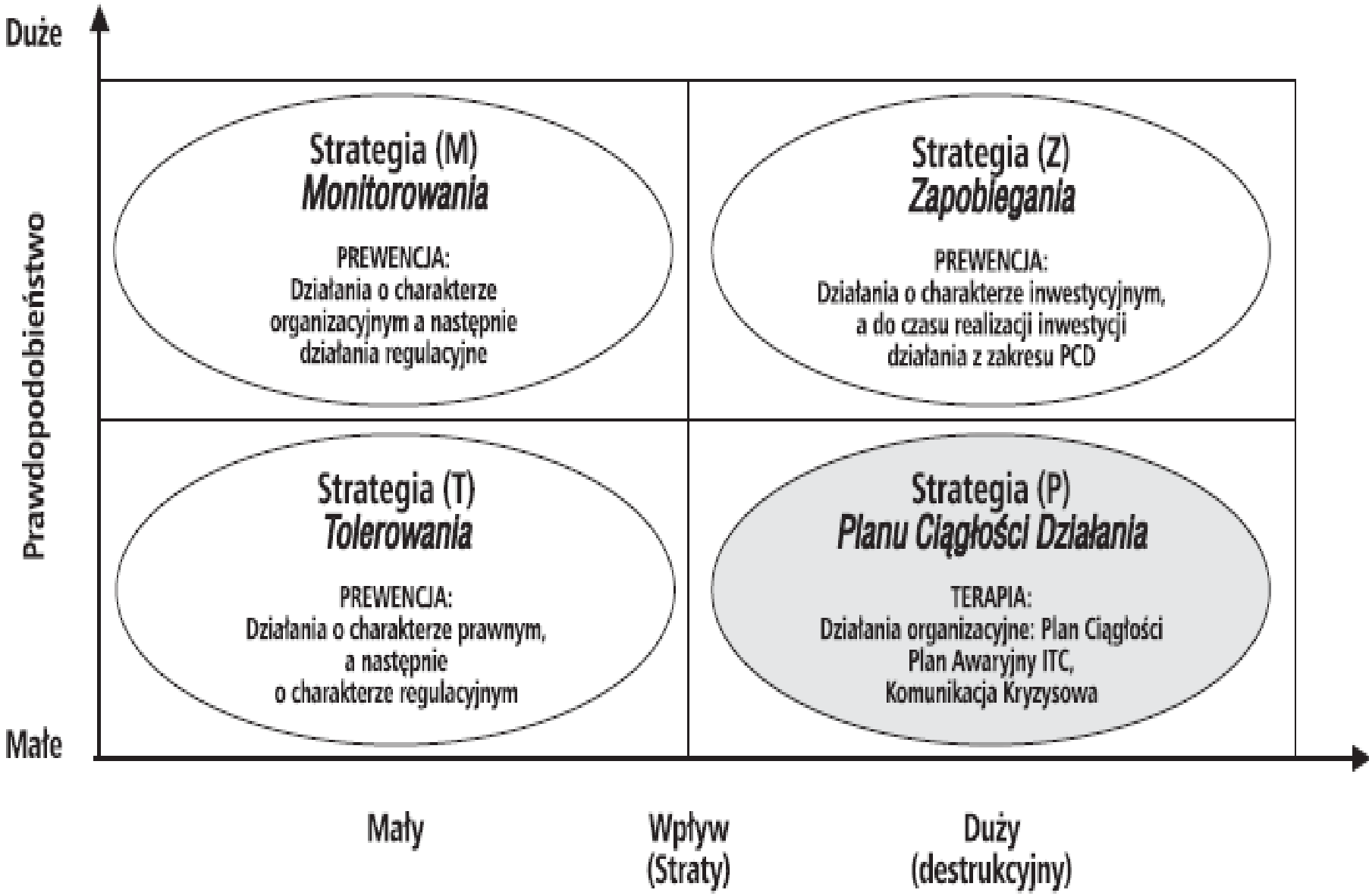
Lp.	Nazwa zagrożenia	Rezultat zagrożenia
1.	Manipulacja urządzeniami teleinformatycznymi lub ich uszkodzenie	Utrata integralności i dostępności, dezorganizacja, straty finansowe
2.	Manipulowanie danymi lub oprogramowaniem	Utrata dostępności, dezorganizacja, straty finansowe
3.	Oszustwa lub kradzieże przy użyciu komputera	Utrata integralności i dostępności, dezorganizacja, straty finansowe.

Źródło: Kowalewski M. i in., *Zagrożenia dla infrastruktury...*

Jak reagować na zakłócenia?

- **Strategia tolerowania (T)**: może być stosowana w przypadku zakłóceń zewnętrznych nieinwazyjnych i niedestrukcyjnych, rzadko występujących, mających mały wpływ na organizację, przemijających samoistnie i nie powodujących trwałych szkód.
- **Strategia monitorowania (M)**: dotyczy postępowania z zakłóceniami drobnymi, nie destrukcyjnymi, ale często występującymi, o dostatecznej informacji o zakłóceniach do uruchomienia mechanizmów kompensacji.
- **Strategia zapobiegania (Z)**: nazywana strategią prewencji jest stosowana w przypadkach dużego prawdopodobieństwa wystąpienia zakłóceń istotnych elementów działalności, a w szczególności wrażliwych elementów infrastruktury technicznej, których stopień destrukcji jest nieakceptowany.
- **Strategia Planów Ciągłości (P)**: dotyczy postępowania z zakłóceniami istotnymi, destrukcyjnymi o bardzo małym prawdopodobieństwie wystąpienia. Ze względu na niskie potencjalne prawdopodobieństwo wystąpienia katastrof mogących spowodować kryzys, ekonomicznie uzasadniona jest rezygnacja ze Strategii (Z) i uprzednie przygotowanie planu postępowania w sytuacjach kryzysowych.

's. 5. Strategie reagowania na zakłócenia



Cyberprzestrzeń jako środowisko walki informacyjnej

- Według Piotra Sienkiewicza *walka informacyjna* (*information warfare, infowar*) to nic innego jak *całokształt działań ofensywnych i defensywnych koniecznych do uzyskania przewagi informacyjnej nad przeciwnikiem i osiągnięcia zamierzonych celów militarnych czy politycznych*.
- Zgodnie z przyjętą w NATO definicją *walka informacyjna* to działania informacyjne prowadzone w okresie kryzysu lub konfliktu zbrojnego w celu osiągnięcia określonego celu politycznego lub wojskowego.
- Przebieg, charakter oraz wynik wojny w Zatoce Perskiej przyniósł międzynarodowe zainteresowanie się walką informacyjną jako formą rozwiązywania konfliktów. Wojna ta szybko została okrzyknięta jako pierwsza w historii wojskowości wojną informacyjną (1990).
- Cyberprzestrzeń charakteryzuje się wyjątkowo atrakcyjnymi z punktu widzenia prowadzenia działań militarnych cechami. Umożliwia bowiem oddziaływanie na przeciwnika znajdującego się w znacznej odległości w niewspółmiernie krótkim czasie, bez kontaktu fizycznego wojsk oraz narażania życia poszczególnych żołnierzy.
- Jednakże o jej wrażliwości na zniszczenie decyduje warstwa fizyczna cyberprzestrzeni, którą tworzą urządzenia teleinformatyczne istniejące już na ladzie, morzu czy w powietrzu i przestrzeni kosmicznej. Ta fizyczna warstwa cyberprzestrzeni będzie stanowiła pierwszy cel ewentualnego ataku konwencjonalnego.
- Cyberwojna jest przedłużeniem polityki poprzez działania podejmowane w cyberprzestrzeni przez państwowe lub niepaństwowe podmioty, które albo stanowią poważne zagrożenie dla bezpieczeństwa narodowego lub są prowadzone w odpowiedzi na postrzegane zagrożenie przeciwko bezpieczeństwu narodowemu.

Cyberprzestrzeń jako środowisko walki informacyjnej

- Aktywne formy operacji informacyjnych obejmują szereg działań z zakresu:
  - rozpoznania wojskowego;
  - bezpieczeństwa informacji;
  - działań psychologicznych;
  - dezinformacji;
  - walki radioelektronicznej;
  - fizycznego niszczenia wybranych elementów infrastruktury informatycznej przeciwnika
- Wojnę w Zatoce Perskiej często określa się również jako „pierwszą wojnę medialną”.
- „Wojna medialna” oznacza zwiększoną manipulację przekazem, inwigilację dziennikarzy oraz ograniczony obiektywizm.
- Etapy wojny informacyjnej:
  - Pierwszym z nich będzie budowanie przewagi informacyjnej poprzez kreowanie pozytywnego wizerunku własnego zarówno we własnym społeczeństwie, jak i społeczeństwie przeciwnika, a także na arenie międzynarodowej.
  - Drugim etapem będzie etap rozpoznania systemu informacyjnego przeciwnika ukierunkowany na jego elementy składowe; zasoby informacyjne, procedury postępowania oraz infrastrukturę krytyczną. Etapem równoległym do rozpoznania będą czynności ukierunkowane na mylenie i dezinformację przeciwnika oraz ochronę systemów własnych.
  - Ostatnim etapem takiego konfliktu będzie obezwładnienie systemu informacyjnego strony przeciwnej zarówno za pomocą technik informatycznych (hakerskich), jak i fizyczne niszczenie infrastruktury wykorzystując potencjał własnych sił zbrojnych

Amerykańskie podejście do walki informacyjnej

- Podejście techniczne uwzględniające:
  - walkę z systemami kierowania i dowodzenia przeciwnika (w tym niszczenie fizyczne sprzętu i infrastruktury);
  - walkę wywiadowczą i kontrwywiadowczą;
  - walkę elektroniczną, czyli rodzaj działań bojowych zmierzających do zakłócenia lub uniemożliwienia działania środkom technicznym przeciwnika za pomocą własnych środków emisji elektromagnetycznej;
  - operacje psychologiczne (oddziaływanie na percepcję elit rządzących oraz opinię publiczną społeczeństw);
  - operacje informatyczne (eksploatacja sieci informatycznych, ataki kompu-terowe na infrastrukturę informatyczną przeciwnika, obrona zasobów własnych, oprogramowanie złośliwe itd.);
  - ochronę informacji w kontekście uniemożliwienia zdemaskowania rozmieszczenia i możliwości bojowych wojsk własnych i sprzymierzonych oraz innych informacji związanych z tajemnicą państwową czy wojskową;
  - blokowanie dostępu do informacji ekonomicznych.
- Wojna informacyjna polega zatem na defensywnym i ofensywnym wykorzystaniu informacji i systemów informacyjnych w celu odcięcia przeciwnika od dopływu informacji, jak też wykorzystania, zniekształcania lub niszczenia informacji przeciwnika, przy jednoczesnym zachowaniu własnych zasobów i systemów informacyjnych w nietkniętym stanie.

Amerykańskie podejście do walki informacyjnej

- Z dokumentów wykradzionych przez Snowdena, świadczących o rozległej operacji hackingu, wynikało, że zasięg działań amerykańskiej agencji wywiadowczej NSA jest właściwie nieograniczony. Natomiast jaskrawym przykładem użycia cyberataku do celów militarnych było zainfekowanie w 2009 r. przez USA irańskich systemów informatycznych robakiem Stuxnet, w celu sabotażu irańskiego programu jądrowego.
- Rząd Stanów Zjednoczonych wraz z sztabem ekspertów w dziedzinie cyberprzestrzeni już w 2011 roku zaprezentował pierwszą wersją Międzynarodowej Strategii dla Cyberprzestrzeni pt. U.S. International Strategy for Cyberspace. Strategia nie zawierała gotowych rozwiązań lecz odnosiła się do wizji przyszłości i wyzwań jakie czekają Stany Zjednoczone. Celem strategii było stać się mapą postępowań dla amerykańskich instytucji, których głównym i wspólnym celem jest budowa otwartej, bezpiecznej i niezawodnej sieci globalnej.
- Nie można pominąć tak zwanego Patriot Act , czyli ustawy, która zapoczątkowała pierwsze ruchy w usprawnieniu cyberbezpieczeństwa. Uznany za przełomowy, akt prawny został wprowadzony w 2001 roku tuż po tragicznych wydarzeniach z World Trade Center. Ustawa swoim zakresem objęła wszelkie aspekty bezpieczeństwa wewnętrznego zaczynając od wzmocnienia bezpieczeństwa przeciwko działaniom terrorystycznym, po kwestie z omawianej dziedziny czyli, wzmocnienia procedur bezpieczeństwa, ochrony granic poprzez uruchomienie procedur polegających na wymianie informacji dotyczących ochrony newralgicznych budynków instytucji państwowych, aż po penalizację czynów terrorystycznych, których skutkiem jest upośledzenie systemów informatycznych.

Amerykańskie podejście do walki informacyjnej

- W związku z ingerencją do tajnych sieci wojskowych w 2008 roku na Bliskim Wschodzie hakerzy przejęli tysiące wojskowych danych.
- Odpowiedzią na to zdarzenie było utworzenie w 2010 roku United States Cyber Command (USCYBERCOM). Zadania jakie spłynęły na USCYBERCOM określały wszelką ochronę zasobów krytycznych systemów i zasobów sieci, znajdujących się na serwerach Departamentu Obrony USA, w celu zapobiegnięcia nieuprawnionemu wtargnięciu i przechwyceniu.
- Dodatkowo CYBERCOM rozszerzył swoje działania o możliwość prowadzenia pełnowymiarowych operacji w celu koordynacji działań jednostek przeznaczonych do walki w przestrzeni cybernetycznej, a także zapewnienia Stanom Zjednoczonym swobody działania natomiast jej pozbawienia – przeciwnikowi.

Podejście Chin do walki informacyjnej

- W Chińskiej Republice Ludowej tematyka dostępu do Internetu, wykorzystywania technologii informacyjnych oraz prowadzenia działań ofensywnych nabiera zupełnie innego kształtu niż w krajach europejskich czy USA.
- Według doniesień medialnych oraz dostępnych analiz publikowanych przez specjalistów sektora bezpieczeństwa teleinformatycznego jest to kraj, który obecnie najszerzej wykorzystuje zdolności inwigilacji cyfrowej, dopuszczając się ataków na najlepiej strzeżone bazy danych. Podejście do omawianej problematyki wywodzi się z uwarunkowań społeczno-historyczno-kulturowych, które kształtowały stosunek Chin do wojny, szeroko opisywany przez stratega Sun Tzu.
- Pomimo upływu wieków, jego główne myśli przewodnie są wykorzystywane w polityce i w działalności międzynarodowej, w tym przy używaniu technologii informacyjnych do osiągania przewagi ekonomicznej. W wielu obszarach życia gospodarczego i politycznego środki wykorzystywane w celu osiągnięcia przewagi znacznie odbiegają od norm przyjmowanych w krajach tzw. cywilizacji zachodniej.
- Z założenia neguje się działanie Chin jako kraju, który nie przestrzega określonych reguł. Przestrzega, ale stworzonych na własne potrzeby.

Podejście Chin do walki informacyjnej

- Jedną z zasad stosowanych przez chińskich strategów, od której się nie odchodzi, jest dokładna analiza przeciwnika. Chińczycy w kontekście cyberdziałań wskazują mocne i słabe strony Stanów Zjednoczonych jako głównego oponenta w działaniach w cyberprzestrzeni.
- Wysoko oceniają umiejętność gospodarowania budżetem w procesie rozwoju nowoczesnych technologii.
- Jako zdecydowaną wadę wskazują dużą zależność USA od technologii, które rozwijają, co może być przyczyną potencjalnych problemów natury technicznej w związku z możliwością zdalnego niszczenia niektórych z nich.
- Warto zauważyć, że w chińskiej literaturze wojskowej stwierdza się, iż: (…) *cyberatak w połączeniu z możliwościami unieszkodliwiania amerykańskich satelitów oraz zdalnych centrów dowodzenia stanowią specjalną broń, która może zahamować amerykańskie działania wojenne w rejonie Zachodniego Pacyfiku*.
- Chińczycy w wyścigu cyberzbrojeń uważają Amerykanów za największego przeciwnika i wiele doktryn oraz myśli przewodnich jest konstruowanych, mając właśnie ten kraj na uwadze.

Wielki Cyfrowy/CyberMur Chiński

- Chiny określają siebie mianem kraju, który zajmuje pierwsze miejsce w światowym rankingu państw najczęściej atakowanych w cyberprzestrzeni. Wskazuje się również wszelkiego rodzaju treści ogólnie dostępne w Internecie oraz portale społecznościowe jako podstawowe narzędzia dezinformacji, które należy kontrolować.
- Poza uregulowaniami prawnymi, które dokładnie wskazują, jakie treści są dozwolone, zastosowano wiele rozwiązań technologicznych.
- Stosuje się blokowanie witryn internetowych przez wykrywanie słów już na poziomie routerów, które są tak zaprogramowane, aby na połączeniu z serwerami proxy wykrywać istotne dla władz stwierdzenia, i jeżeli zostają wykryte – odsyłać użytkownikowi wiadomość blokującą dostęp.
- Te strony, które zostały w taki sposób skonstruowane, aby omijać zautomatyzowane formy filtrowania, są wyszukiwane przez „cyberpolicję”, czyli około zatrudnionych przez Ministerstwo Bezpieczeństwa Publicznego pracowników, którzy ręcznie przeszukują strony internetowe w poszukiwaniu nielegalnych treści.
- Próba dokonania pełnej kontroli Internetu w Chinach przechodziła trzy fazy rozwoju: automatycznego i ręcznego blokowania treści, filtrowania treści znajdujących się w sieciach Chin na podstawie międzynarodowych umów z operatorami i dostawcami Internetu oraz model, który zawiera w sobie oba powyższe w połączeniu z trzecim – samocenzurą obywateli, którzy są nagradzani za ujawnianie nielegalnych treści w Internecie.

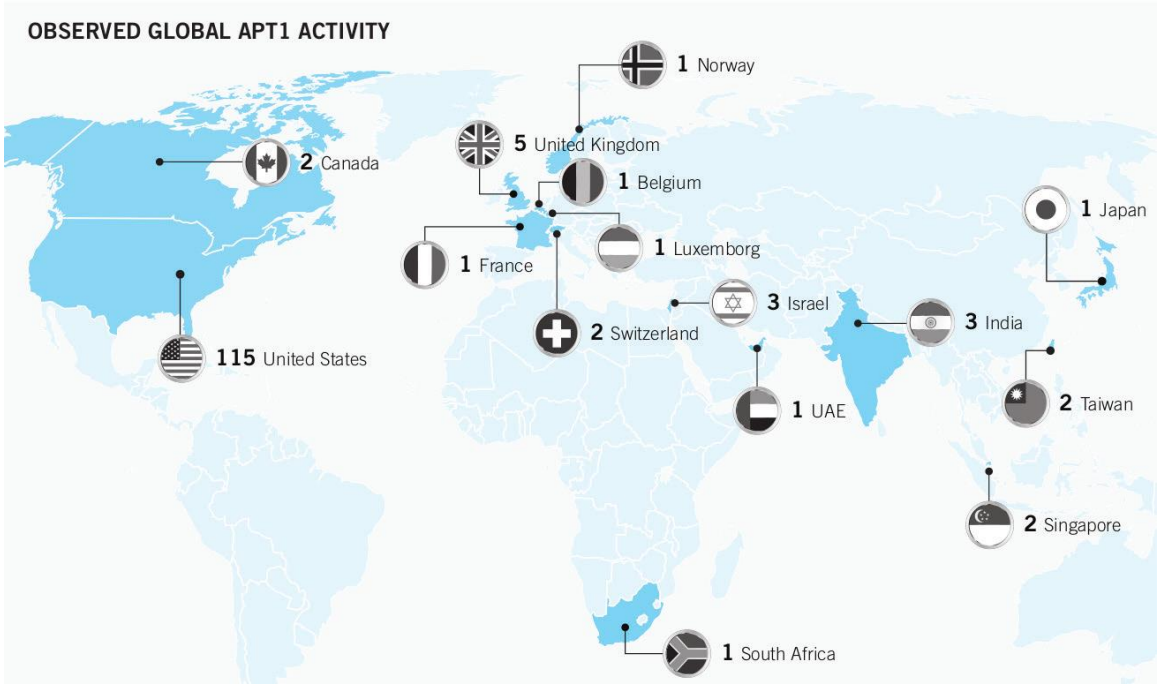
Podejście Chin do walki informacyjnej

- Ataki APT charakteryzują się następującymi fazami:

1. **wstępny rekonesans i wybór celu,**
2. **uzyskanie wstępnego dostępu do sieci**; na tym etapie najczęściej wykorzystywaną metodą jest phishing mailowy, w celu przekazania pracownikom złośliwego oprogramowania, które umożliwia dostęp do ich kont i uprawnień,
3. **stabilizacja dostępu**, która następuje po zainstalowaniu malware'u na komputerze ofiary. Wtedy w sposób zdalny napastnik formułuje komendy oraz programuje system w taki sposób, aby pozostać niezauważonym – może się to dziać przez implementację jakichś formuł tworzących napastnikowi nieistniejący do tej pory *backdoor*,
4. po stabilizacji następuje **etap główny**, na który składają się cztery procesy:
    1. zwiększanie uprawnień w sieci wewnętrznej,
    2. rekonesans wewnętrzny po sieci i pozyskiwanie danych,
    3. sprawdzanie bezpieczeństwa połączenia i maskowanie śladów obecności,
    4. utrzymywanie obecności przez jak najdłuższy czas,
5. **faza wyjścia** inicjowana albo przez napastnika, jeżeli uzyskał już wszelkie niezbędne informacje i wykonał misję, albo przez dyskredytację operacji i odnalezienie błędów przez dział bezpieczeństwa IT w danej instytucji

Podejście Chin do walki informacyjnej

- Do głównych obszarów inwigilowanych przez Chiny należą: systemy komputerowe Tybetu (GhostNet19), systemy obronne Ameryki oraz krajów europejskich, własność intelektualna znajdująca się w systemach amerykańskich oraz państw europejskich, szczegóły związane z pozycją negocjacyjną firm konkurujących z firmami chińskimi o wpływy w konkretnych sektorach.
- **Liczba ataków Comment Crew typu APT z podziałem na kraje, w których je przeprowadzono.**



Podejście Rosji do walki informacyjnej

- Strona rosyjska definiuje wojnę informacyjną jako oddziaływanie na masową świadomość w międzypaństwowej rywalizacji systemów cywilizacyjnych w przestrzeni informacyjnej, wykorzystujące szczególne sposoby kontroli nad zasobami informacyjnymi, które mogą być stosowane jako swoista broń informacyjna.
- Działania te skierowane są nie tylko przeciw siłom zbrojnym, ale przede wszystkim ukierunkowane są na całe społeczeństwo oraz jego świadomość, a także na aparat administracyjny, świat nauki i kultury oraz przemysł i ekonomikę danego państwa. Wojna informacyjna może mieć na celu przygotowanie, w założonej perspektywie czasowej, zbrojnej interwencji mogącej mieć charakter typowych działań wojennych między państwami, bądź też realizowanej jako wojna hybrydowa, wykorzystując własne oraz posiadane aktywa i zasoby na terenie przeciwnika, zbudowane i pozyskane podczas prowadzenia wojny informacyjnej.
- Ten drugi rodzaj aktywów jest szczególnie niebezpieczny, gdyż często trudno jest je zidentyfikować, a jeżeli już, to zwykle zabiera to dużo czasu. Wojna informacyjna, zorientowana na moralną, etyczną a także ekonomiczną degradację społeczeństwa i jego elit wcale nie musi się kończyć konfliktem zbrojnym.

Podejście Rosji do walki informacyjnej

- Na Ukrainie mieliśmy do czynienia z działaniami, które przybierają formę tzw. *wojny hybrydowej (Rosjanie nie używają pojęcia wojna hybrydowa np. Gierasimow używa terminu „nowoczesna wojna”)*.
- Wojnę hybrydową definiuje się jako połączenie działań militarnych i niemilitarnych, wymierzone najczęściej przeciw jakiemuś państwu, w których obok walki zbrojnej z użyciem konwencjonalnych sił zbrojnych zastosowano działania nieregularne, akty terrorystyczne i kryminalne, wspomagane szerokim atakiem informacyjnym oraz walką w obszarze cyberprzestrzeni. Prowadzona jest często bez oficjalnego wypowiedzenia.
- Rosja zajęła ośrodek łączności kosmicznej w Eupatorii na Krymie, pozbawiając Ukrainę całkowitej kontroli nad jej połączeniami satelitarnymi.
- Sabotaż ukraińskiego radia i telewizji polegający na dokonywaniu fizycznych zniszczeń infrastruktury nadającej.
- Żołnierzy wojsk specjalnych Sił Zbrojnych Federacji Rosyjskiej działający na Krymie występowali bez oznaczeń przynależności narodowej czy organizacyjnej. W rosyjskich mediach byli nazywani „krymskimi siłami samoobrony”

Powołanie wojsk cybernetycznych w Polsce

- 8 lutego 2022r. Szef MON powołał Wojska Obrony Cyberprzestrzeni. Minister obrony Mariusz Błaszczak, który poinformował o powołaniu Dowództwa Komponentu WOC we wtorek, zaznaczył, że "to regularne wojsko, posiada zdolności zarówno obronne, służące rozpoznaniu, jak i zdolności służące ofensywie". Dowódcą WOC został gen. Karol Molenda.
- Pierwsze sformułowania wskazujące na potrzebę utworzenia takich wojsk można doszukać się już w Strategii Bezpieczeństwa Narodowego RP z 2003 roku.
- W Strategii z 2014 mówi się w sposób ogólny o potrzebie budowy narodowego systemu obrony cybernetycznej, w tym o rozwijaniu Krajowego Systemu Reagowania na Incydenty Komputerowe w Cyberprzestrzeni Rzeczypospolitej Polskiej, kompatybilnego z systemami państw sojuszniczych.
- Wątek krajowego systemu ochrony cyberprzestrzeni był kontynuowany w Krajowych Ramach Polityki Cyberprzestrzeni Rzeczypospolitej na lata 2017-2024 w nawiązaniu do potrzeby konsolidacji działania wszystkich interesariuszy, również w kontekście operacyjnym umocowania kompetencyjnego na poziomie ustawy odpowiednich struktur w tym Narodowego Centrum Cyberbezpieczeństwa oraz zespołu reagowania CSIRT Narodowego.
- Pierwsze informacje nt. wojsk cybernetycznych w Polsce pochodzą z III Europejskiego Forum Cyberbezpieczeństwa CYBERSEC z 2017 roku, na którym informowano o planie utworzenia w Polsce wojsk cybernetycznych liczących przynajmniej 1 tys. żołnierzy zdolnych do walki w cyberprzestrzeni. Na ich utworzenie miano przeznaczyć 2 mld zł.

13:25
11/10/2017

- https://niebezpiecznik.pl/post/mon-stworzy-wojsko-cybernetyczne-z-komponentem-informacyjno-psychologicznym-infoops/

1. W jakim trybie tworzone są wspomniane przez ministra "wojska cybernetyczne" i jakie kroki formalne w tej sprawie już podjęto?
2. Czy utworzenie tego typu jednostki będzie wymagało zmian w prawie?
3. Na jakiego rodzaju zagrożenia mają reagować "wojska cybernetyczne". Czy będzie chodziło wyłącznie o ataki komputerowe (włamania, malware itd.), czy również o walkę z dezinformacją?
4. Czy opracowane koncepcję szkolenia żołnierzy, którzy będą tworzyli takie wojsko?
5. Czy wiadomo w ramach jakich struktur to wojsko będzie działać?
6. Czy na wspomniany cel zarezerwowano jakieś środki finansowe. Jeśli tak to jakie?

Szanowny Panie Redaktorze,

W odpowiedzi na pytania przesyłamy poniższe informacje. Ministerstwo Obrony Narodowej podjęło decyzję o zintensyfikowaniu prac nad rozwojem zdolności do obrony przed zagrożeniami w cyberprzestrzeni, zarówno pod względem obrony przez atakami na systemy teleinformatyczne, jak i obrony przed atakami informacyjnymi, z uwzględnieniem obrony przed manipulacją krajowym środowiskiem informacyjnym.

Wojska do działań w cyberprzestrzeni będą zawierały *komponent CYBEROPS* zdolny do obrony przed atakami teleinformatycznymi prowadzonymi w i przy użyciu cyberprzestrzeni oraz *komponent INFOOPS* zdolny do obrony przez operacjami informacyjnymi (w tym psychologicznymi) prowadzonymi w i z użyciem cyberprzestrzeni.

Wojska do działań w cyberprzestrzeni zachowają interoperacyjność z istniejącymi rodzajami wojsk Sil Zbrojnych RP. Wychodząc naprzeciw wyzwaniom środowiska bezpieczeństwa resort obrony narodowej opracowuje nowoczesne koncepcje szkoleń i rekrutacji personelu do nowo formowanych struktur. W tym i innych zadaniach planowana jest ścisła współpraca ze środowiskiem specjalistów i ekspertów spoza resortu obrony narodowej.

W chwili obecnej trwają intensywne prace mające na celu opracowanie dokumentów wykonawczo - decyzyjnych Po zakończeniu tego etapu, dokumenty decyzyjne (jawne) zostaną opublikowane w ogólnie dostępnym Dzienniku Urzędowym.

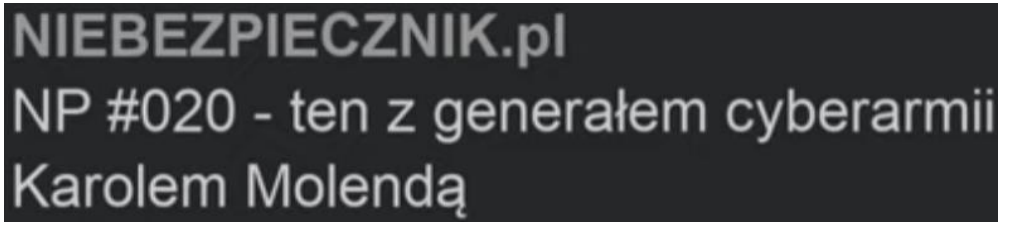
Z poważaniem
Oddział Mediów
Centrum Operacyjne
Ministra Obrony Narodowej

https/://niebezpiecznik.pl/post/mon-stworzy-wojsko-cybernetyczne-z-komponentem-informacyjno-psychologicznym-infoops

Wywiady z Dowódcą Wojsk Ochrony Cyberprzestrzeni Gen. Bryg. Karolem Molendą

2017 https://www.youtube.com/watch?v=mJ9TLaky8_c
2022 https://www.youtube.com/watch?v=q6Qy7RyKJyc

https://niebezpiecznik.pl/post/general-karol-molenda-na-podsluchu/?similarpost



Zapis przebiegu posiedzenia Sejmowej Komisji Obrony Narodowej /nr 17/ 17-11-2020

Sekretarz stanu w MON Wojciech Skurkiewicz

- … Sojusz Północnoatlantycki już w 2014 r. uznał atak w cyberprzestrzeni za jeden z rodzajów agresji, który może stanowić podstawę do wprowadzenia w życiemechanizmów obronnych opisanych w art. 5 Traktatu północnoatlantyckiego. … w 2016 r. podczas szczytu NATO w Warszawie oficjalnie uznano cyberprzestrzeń jako jedną z domen działań operacyjnych. To zrodziło konieczność opracowania przez NATO konkretnych struktur sojuszu, strategii ich funkcjonowania oraz realizacji przez nie działań o charakterze operacyjnym w wyżej wymienionej domenie cyfrowej.
- Każde państwo powinno samodzielnie rozwijać zdolności defensywne własnych sił zbrojnych w tym obszarze. Osiągnięcie wymaganego poziomu do działań w domenie cyberprzestrzeni stanowi CyberDefense Pledge, czyli jest obowiązkiem wszystkich członków Sojuszu Północnoatlantyckiego. W celu zwiększenia zdolności do realizacji zadań mających zapewnić odpowiedni poziom bezpieczeństwa narodowych systemów IT, w resorcie obrony narodowej w ostatnich latach podejmowane były i są liczne przedsięwzięcia natury informacyjnej, promocyjnej, organizacyjnej i szkoleniowej.

Dyrektor NCBC Dowódca WOC Gen. Bryg. Karol Molenda

Zapis przebiegu posiedzenia Sejmowej Komisji Obrony Narodowej /nr 17/ 17-11-2020

- Cała koncepcja utworzenia Wojsk Obrony Cyberprzestrzeni ma charakter niejawny.
- Na bazie Inspektoratu Informatyki i Narodowego Centrum Kryptologii powstało Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni jako jednostka, która konsoliduje te zasoby.
- W podporządkowaniu Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni jest sześć regionalnych centrów informatyki, czylijednostek, które odpowiadają za swój region, jeżeli chodzi o utrzymanie stacjonarnych systemów teleinformatycznych resortu obrony narodowej. Oprócz tego jest jednostkaCentrum Zasobów Cyberprzestrzeni Sił Zbrojnych, która jest naszą jednostką logistyczną.
- Został zwiększony nabór do dwóch kluczowych uczelni wojskowych, które kształcą w tym zakresie. Oczywiście jest to Wojskowa Akademia Techniczna, w której chociażby w latach 2015 i 2016 na elektronice było 84 i 97 osób. W chwili obecnej na rok 2020/2021 są to 222 osoby ... Na informatyce z 47 osób w 2015 r. liczba studentów wzrosła do 107 w 2021 r. Na kryptologii i cyberbezpieczeństwie z 15 osób w 2015 r. liczba studentów wzrosła do 116 osób w 2021 r. To jeżeli chodzi o Wojskową Akademię Techniczną.
- Równocześnie zwiększono limity przyjęć w Akademii Marynarki Wojennej do 22 podchorążych na kierunku informatyka. Jednocześnie w tym roku zostaje uruchomiony kierunek informatyka w Akademii Wojsk Lądowych we Wrocławiu.
- … należy zaadresować nasze potrzeby do młodszej młodzieży

Zapis przebiegu posiedzenia Sejmowej Komisji Obrony Narodowej /nr 17/ 17-11-2020

- z jednej strony powstało Wojskowe Ogólnokształcące Liceum Informatyczne przy WAT, które co roku przyjmuje 50 uczniów. … na pierwszy rok zgłosiło się ponad 500 kandydatów… Młodzież ma autorski kierunek związany z cyberbezpieczeństwem i informatyką. Część nauczycieli to wykładowcy z Wojskowej Akademii Technicznej.
- Kolejny program, …to „CYBER.MIL z klasą”. Program ma na celu, żeby w każdym województwie była jedna szkoła średnia, która będzie miała autorski program w zakresie cyberbezpieczeństwa. … szkoła średnia dostaje środki finansowe na infrastrukturę i na prowadzenie zajęć w tej klasie. Klasa nie może mieć więcej niż 15 uczniów. … regionalne centra informatyki podległe NCBC, mają za zadanie sprawowanie nadzoru merytorycznego nad tymi szkołami.
- Kolejną inicjatywą … Letnia Szkoła Cyberbezpieczeństwa i Zimowa Szkoła Cyberbezpieczeństwa .. konferencje, tygodniowe spotkania, które pomagają w wyrównywaniu wiedzy w zakresie cyberbezpieczeństwa.
- Kolejna inicjatywa to uruchomienie studiów MBA z zakresu cyberbezpieczeństwa w Wojskowej Akademii Technicznej.
- Mamy też Legię Akademicką, która cieszy się bardzo dużym zainteresowaniem. Jest to możliwość, żeby studenci z całej Polski w okresie wakacji mogli odbyć przeszkolenie wojskowe i uzyskać stopień kaprala rezerwy.
- Uruchomiliśmy infolinię przeznaczoną dla kandydatów do NCBC. W 2019 r. łącznie cywili, którzy do nas trafili, było 958. A w 2020 r. do chwili obecnej – 1330. W tej grupie odbyliśmy 726 rozmów kadrowych. Kandydaci dostają test do zrobienia. Dostają 30 pytań, na odpowiedź jest 30 minut, w sposób zdalny.

WYKAZ SZKÓŁ
ZAKWALIFIKOWANYCH DO "PROGRAMU CYBER.MIL. Z KLASĄ"

L.P.	WOJEWÓDZTWO	SIEDZIBA SZKOŁY	NAZWA I DANE ADRESOWE SZKOŁY
1	2	3	4
1.	PODLASKIE	Suwałki	I Liceum Ogólnokształcące z Oddziałami Dwujęzycznymi im. Marii Konopnickiej w Suwałkach, Pl. Mickiewicza 3, 16-400 Suwałki
2.	KUJAWSKO-POMORSKIE	Inowrocław	I Liceum Ogólnokształcące im. Jana Kasprowicza z Oddziałami Dwujęzycznymi w Inowrocławiu, ul. 3 Maja 11/13, 88-100 Inowrocław
3.	POMORSKIE	Lębork	I Liceum Ogólnokształcące im. Stefana Żeromskiego Zespołu Szkół Ogólnokształcących nr 1 w Lęborku, ul. Dygasińskiego 14, 84-300 Lębork
4.	ŚLĄSKIE	Jaworzno	Zespół Szkół Ogólnokształcących III Liceum Ogólnokształcące im. Orła Białego w Jaworznie, ul. Towarowa 61, 43-600 Jaworzno
5.	ŚWIĘTOKRZYSKIE	Ostrowiec Świętokrzyski	Liceum Ogólnokształcące Nr II im. Joachima Chreptowicza w Ostrowcu Świętokrzyskim, ul. Jana Rosłońskiego 1, 27-400 Ostrowiec Świętokrzyski
6.	MAŁOPOLSKIE	Bochnia	I Liceum Ogólnokształcące im. Króla Kazimierza Wielkiego w Bochni, Pl. Ks. A. Czaplińskiego 1, 32-700 Bochnia
7.	LUBELSKIE	Świdnik	I Liceum Ogólnokształcące im. Władysława Broniewskiego w Świdniku, ul. gen. Leopolda Okulickiego 13, 21-040 Świdnik
8.	ŁÓDZKIE	Ozorków	I Liceum Ogólnokształcące im. Stefana Żeromskiego w Zespole Szkół Ogólnokształcących w Ozorkowie, ul. Romualda Traugutta 1, 95-035 Ozorków
9.	WARMIŃSKO-MAZURSKIE	Nidzica	Zespół Szkół Ogólnokształcących-Liceum Ogólnokształcące im. St. Wyspiańskiego w Nidzicy, ul. Jagiełły 1, 13-100 Nidzica
10.	OPOLSKIE	Olesno	I Liceum Ogólnokształcące im. Lotników Polskich w Oleśnie, ul. Sądowa 2, 46-300 Olesno
11.	WIELKOPOLSKIE	Piła	Zespół Szkół Technicznych w Pile, ul. Ceglana 4, 64-920 Piła
12.	PODKARPACKIE	Leżajsk	Zespół Szkół Licealnych im. B. Chrobrego w Leżajsku, ul. M. Skłodowskiej - Curie 6, 37-300 Leżajsk
13.	ZACHODNIO-POMORSKIE	Stargard	I Liceum Ogólnokształcące im. Adama Mickiewicza w Stargardzie, ul. Staszica 2, 73-110 Stargard
14.	MAZOWIECKIE	Radom	Niepubliczne Technikum im. 72 Pułku Piechoty w Radomiu ZDZ, ul. Saska 4/6, 26-600 Radom
15.	DOLNOŚLĄSKIE	Bolesławiec	II Liceum Ogólnokształcące im. Janusza Korczaka w Bolesławcu, ul. Dolne Młyny 60, 59-700 Bolesławiec
16.	LUBUSKIE	Gorzów Wielkopolski	II Liceum Ogólnokształcące im. Marii Skłodowskiej-Curie w Gorzowie Wielkopolskim, ul. Przemysłowa 22, 66-400 Gorzów Wielkopolski

Zapis przebiegu posiedzenia Sejmowej Komisji Obrony Narodowej /nr 17/ 17-11-2020

- Opracowaliśmy witrynę zostanzołnierzem.pl, na której w sposób zdalny można zgłosić swój akces i otrzymać dokumenty do tego niezbędne. Jednocześnie te dane trafiają do właściwej wojskowej komendy uzupełnień. W chwili obecnej jesteśmy w przededniu uruchomienia aplikacji Zostań Żołnierzem na urządzenia mobilne – iOS i Android.
- I pewna wisienka na torcie … nasi żołnierze potrzebują mieć poligon, na którym mogą podnosić swoje kwalifikacje. Eksperckie Centrum Szkolenia Cyberbezpieczeństwa to właśnie takie miejsce (powstało 2XI2020 StSt). Już są określone ścieżki szkoleniowe … możliwości zgrywania zespołów. Jest taka możliwość w Fort Gordon w Stanach Zjednoczonych. W ramach takich ćwiczeń można wyszukiwać liderów … Jest eksperckie Centrum Doskonalenia Cyberobrony NATO w Tallinie. Natomiast przepustowość tego centrum, jeżeli chodzi o szkolenie, to dwie osoby na kraj. Polskie siły zbrojne potrzebują przeszkolić kilka tysięcy osób.
- … został przyznany dodatek o charakterze stałym dla żołnierzy wykonujących zadania w zakresie cyberbezpieczeństwa i informatyki. Oczywiście w zależności od ich wiedzy i umiejętności ten dodatek może wynosić od 450 zł do 2100 zł. Jako dodatek stały, czyli 10% za każdy rok, jest on dodawany do emerytury, co już spowodowało dość korzystne zainteresowanie nie tylko pracą, ale także służbą. Jednocześnie w zależności od zaangażowania żołnierzy w realizację zadań dyrektor NCBC ma możliwość przyznania od 100% do 620% jednorazowego dodatku raz w roku, w zależności od osiągnięć danego żołnierza i jego zaangażowania.
- … w ramach NCBC funkcjonuje też CSIRT MON, czyli zespół reagowania na incydenty komputerowe Ministerstwa Obrony Narodowej. Oczywiście żeby wyjaśniać incydenty i koordynować ich obsługę, niezbędna jest współpraca ze służbami w tym zakresie, również z CERT NASK, a także z uczelniami, które mogą zasilać nas kadrowo.

Zapis przebiegu posiedzenia Sejmowej Komisji Obrony Narodowej /nr 17/ 17-11-2020

- z jednej strony powstało Wojskowe Ogólnokształcące Liceum Informatyczne przy WAT, które co roku przyjmuje 50 uczniów. … na pierwszy rok zgłosiło się ponad 500 kandydatów… Młodzież ma autorski kierunek związany z cyberbezpieczeństwem i informatyką. Część nauczycieli to wykładowcy z Wojskowej Akademii Technicznej.
- Kolejny program, …to „CYBER.MIL z klasą”. Program ma na celu, żeby w każdym województwie była jedna szkoła średnia, która będzie miała autorski program w zakresie cyberbezpieczeństwa. … szkoła średnia dostaje środki finansowe na infrastrukturę i na prowadzenie zajęć w tej klasie. Klasa nie może mieć więcej niż 15 uczniów. … regionalne centra informatyki podległe NCBC, mają za zadanie sprawowanie nadzoru merytorycznego nad tymi szkołami.
- Kolejną inicjatywą … Letnia Szkoła Cyberbezpieczeństwa i Zimowa Szkoła Cyberbezpieczeństwa .. konferencje, tygodniowe spotkania, które pomagają w wyrównywaniu wiedzy w zakresie cyberbezpieczeństwa.
- Kolejna inicjatywa to uruchomienie studiów MBA z zakresu cyberbezpieczeństwa w Wojskowej Akademii Technicznej.
- Mamy też Legię Akademicką, która cieszy się bardzo dużym zainteresowaniem. Jest to możliwość, żeby studenci z całej Polski w okresie wakacji mogli odbyć przeszkolenie wojskowe i uzyskać stopień kaprala rezerwy.
- Uruchomiliśmy infolinię przeznaczoną dla kandydatów do NCBC. W 2019 r. łącznie cywili, którzy do nas trafili, było 958. A w 2020 r. do chwili obecnej – 1330. W tej grupie odbyliśmy 726 rozmów kadrowych. Kandydaci dostają test do zrobienia. Dostają 30 pytań, na odpowiedź jest 30 minut, w sposób zdalny.

Zapis przebiegu posiedzenia Sejmowej Komisji Obrony Narodowej /nr 17/ 17-11-2020

- Nowy autorski program to „Cyfrowi ambasadorzy NCBC”. … jesteśmy skorzy, żeby na tych uczelniach, na których nam zależy, znaleźć osoby – wyróżniających się studentów – które mogłyby być naszymi ambasadorami, naszymi przedstawicielami i budować obraz centrum, ale też wojska oraz zachęcać i informować o inicjatywach. Jest bardzo duże zainteresowanie.
- Podpisana jest współpraca z agencją NCI Agency z NATO, w ramach której funkcjonuje NATO Cyber Security Centre, czyli wcześniejszy NCSIRT – zespół reagowaniana incydenty komputerowe w sieciach NATO. Mamy ustalone zakresy wymiany informacji i funkcjonowanie punktów przez 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku. Nasze centra operacyjne NCBC także pracują w trybie 24 godziny na dobę.
- … bardzo ambitny plan, który określiliśmy, dotyczy zbudowania zdolności do działania w pełnym spektrum cyberprzestrzeni w ciągu 4–5 lat. Jest to o tyle ambitny plan, że chociażby Amerykanie budowali swoje zdolności przez 11 lat. Mam nadzieję, że fakt wymiany informacji z naszymi partnerami, w tym z Amerykanami, o czym wspominałem wcześniej, pozwoli nam na przyspieszenie
- … rotmapa dojścia do osiągnięcia zdolności do działania jest informacją niejawnąPierwszy etap już jest za nami. Natomiast jeżeli chodzi o czasowy rozkład, to 2025 r. jest rokiem, w którym będzie pełnedowództwo z pełnym FOK, full operations capability, jeżeli chodzi o cyberprzestrzeń, z certyfikowanym dowództwem i z certyfikowanymi zespołami.
- CSIRT MON działa w ramach NCBC, jest narodowym punktem kontaktowym pozostałych CSIRT-ów, czyli punktem do współpracy z NATO i z innymi zespołami reagowania na incydenty komputerowe i do współpracy z pozostałymi CSIRT-ami na poziomie krajowym, czyli z CSIRTGOV, który obecnie jest w ABW, i z CSIRT NASK.

Zapis przebiegu posiedzenia Sejmowej Komisji Obrony Narodowej /nr 17/ 17-11-2020

- … ustawa o krajowym systemie cyberbezpieczeństwa zakłada, że to wszystko jest na czas „P”, czyli na czas pokoju. Natomiast na czas „W” minister obrony narodowej jest zobowiązany do przejęcia koordynacji nad obsługą incydentów na poziomie krajowym. Dla nas jest to też i będzie pewnym wyzwaniem, bo musimy nie tylko zbudować kompetencje w ramach naszego CSIRT-u, ale również zapewnić element łącznikowy dla pozostałych zespołów reagowania i zrozumieć ich czasem odmienny tryb pracy przy wyjaśnianiu incydentów.
- Jest aspekt prawny, czyli to, w jakim zakresie żołnierze mogą realizować działania w domenie cyberprzestrzeni. W chwili obecnej jesteśmy trochę jak pięściarz w ringu – trzymamy gardę i dość dobrze się bronimy. Natomiast nasi partnerzy, chociażby Francuzi i Amerykanie, już dobrze to zdiagnozowali. Amerykanie bardzo dobrze to opisali w swojej strategii z 2018 r., definiując koncepcję pewnych działań w odpowiedzi na działania adwersarzy czy na złośliwe działania przeciwnika, którą nazwali „defending forward”. Tam żołnierze nie czekają na wypowiedzenie wojny.
- W 2022 r. nastąpi sformowanie podstawowych struktur dowodzenia dowództwa komponentu. Osiągnięcie częściowej zdolności nastąpi w 2023 r. Następnie będziemy prowadzili proces certyfikacji dowództwa, ale również zespołów, oceniający ich umiejętności. W 2025 r. nastąpi przeprowadzenie certyfikacji jednostek poziomu taktycznego z minimalną obsadą na poziomie 80% i osiągnięcie pełnej zdolności do prowadzenia pełnego spektrum działań w cyberprzestrzeni..

Dyrektor NCBC Dowódca WOC Gen. Bryg. Karol Molenda

Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni (NCBC)

- To jednostka ekspercka podległa Ministrowi Obrony Narodowej sformowana w oparciu o Narodowe Centrum Kryptologii i Inspektorat Informatyki.
- NCBC zapewnia bezpieczeństwo teleinformatyczne resortu obrony narodowej i pełni ważną funkcję w procesie informatyzacji państwa.
- Odpowiada za kluczowe obszary związane z konsolidacją kompetencji i zasobów resortu w zakresie: kryptologii, cyberbezpieczeństwa oraz budowy i eksploatacji systemów IT.
- Pełni także funkcję CSIRT-MON. Zadaniem NCBC jest również przygotowanie podwalin pod nowy rodzaj wojsk – Wojska Obrony Cyberprzestrzeni.
- Centrum realizuje też zadania w ramach działalności naukowo-edukacyjnej, wdrożeniowej, badawczo-rozwojowej i opiniodawczej. Prowadzi badania dotyczące metod wykrywania incydentów w cyberprzestrzeni, projektowania rozwiązań do ochrony i zabezpieczenia informacji, rozwija własne metody i urządzenia kryptograficzne.
- NCBC to też uczestnik największych ćwiczeń i konkursów programowania, w których zdobywa czołowe miejsca w kraju i za granicą m.in.: TIDE Hackathon, Locked Shields, Cyber Coalition. To dlatego możemy powiedzieć, że jesteśmy CYFROWYM SERCEM ARMII.

Cel strategiczny SBN[1] w obszarze cyberbezpieczeństwa

- Podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji.
- Cel określony w I Filarze – Bezpieczeństwo Państwa i Obywateli.
- ==========
- [1] STRATEGIA BEZPIECZEŃSTWA NARODOWEGO RZECZYPOSPOLITEJ POLSKIEJ, 2020

Spójność SBN z Ustawą o Krajowym Systemie Cyberbezpieczeństwa (KSC) z 5 lipca 2018.

- Ustawa definiuje zadania ośrodków reagowania na incydenty bezpieczeństwa komputerowego (CSIRT Computer Security Incident Response Team), które podzielono sektorowo na: CSIRT MON, CSIRT GOV i CSIRT NASK.
- Gen bryg. Karol Molenda dyrektor Narodowego Centrum Bezpieczeństwa Cybernetycnego podkreślił, że jego głównym celem jest inwestycja w ludzi. Najbardziej wrażliwymi systemami są te , które przetwarza ją informacje niejawne stąd musimy dbać w sposób szczególny o ich bezpieczeństwo. Współpraca z pozostałymi CSIRTami (a także współpraca międzynarodowa) jest kluczowa i pozwala nam wymieniać się informacjami o zagrożeniach)

Ustawa o krajowym systemie cyberbezpieczeństwa nałożyła na resort obrony narodowej szereg zadań związanych z zapewnieniem cyberbezpieczeństwa państwa. Zgodnie z Art. 51. Minister Obrony Narodowej odpowiedzialny jest za:

- − współpracę Sił Zbrojnych RP z właściwymi organami NATO, Unii Europejskiej i organizacji międzynarodowych w obszarze obrony narodowej w zakresie cyberbezpieczeństwa;
- − zapewnienie zdolności Siłom Zbrojnym RP w układzie krajowym, sojusz-niczym i koalicyjnym do prowadzenia działań militarnych w przypadku zagrożenia cyberbezpieczeństwa powodującego konieczność działań obronnych;
- − rozwijanie umiejętności Sił Zbrojnych RP w zakresie zapewnienia cyber-bezpieczeństwa przez organizację specjalistycznych przedsięwzięć szkoleniowych;
- − pozyskiwanie i rozwój narzędzi służących budowaniu zdolności zapewnienia cyberbezpieczeństwa w Siłach Zbrojnych RP;
- − kierowanie działaniami związanymi z obsługą incydentów w czasie stanu wojennego;
- − ocenę wpływu incydentów na system obrony państwa;
- − ocenę zagrożeń cyberbezpieczeństwa w czasie stanu wojennego oraz przed-stawianie właściwym organom propozycji dotyczących działań obronnych;
- − koordynację, we współpracy z ministrem właściwym do spraw wewnę-trznych i ministrem właściwym do spraw informatyzacji, realizacji zadań organów administracji rządowej i jednostek samorządu terytorialnego w czasie stanu wojennego dotyczących działań obronnych w przypadku zagrożenia cyberbezpieczeństwa.

Ponadto do zadań CSIRT MON należy koordynacja obsługi incydentów zgłaszanych przez podmioty podległe lub nadzorowane przez MON, w tym podmioty wchodzące w skład infrastruktury krytycznej, oraz przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym.

Spójność SBN z Strategią Cyberbezpieczeństwa RP na lata 2019-2024 (SCRP) z 22 października 2019.

SCRP definiuje następujące cele szczegółowe:

- Rozwój krajowego systemu cyberbezpieczeństwa
- Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty.
- Zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa
- Badanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa
- Zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa

Dokument normujący działania obywateli RP.

Ustawy.

Art. 1. Obrona Ojczyzny jest sprawą i obowiązkiem wszystkich obywateli Rzeczypospolitej Polskiej.`

Art. 3. 1. Na straży suwerenności i niepodległości Narodu Polskiego oraz jego bezpieczeństwa i pokoju stoją Siły Zbrojne Rzeczypospolitej Polskiej, zwane dalej „Siłami Zbrojnymi”.

…

3. W skład Sił Zbrojnych wchodzą jako ich rodzaje: 1) Wojska Lądowe; 2) Siły Powietrzne; 3) Marynarka Wojenna; 4) Wojska Specjalne; 5) Wojska Obrony Terytorialnej.

Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (ogłoszenie tekstu jednolitego 19 lipca 2019)

Art. 4. 1. Powszechnemu obowiązkowi obrony podlegają wszyscy obywatele polscy zdolni ze względu na wiek i stan zdrowia do wykonywania tego obowiązku…

2. W ramach powszechnego obowiązku obrony obywatele polscy są obowiązani do: 1) pełnienia służby wojskowej, 2) wykonywania obowiązków wynikających z nadanych przydziałów kryzysowych i przydziałów mobilizacyjnych, 3) świadczenia pracy w ramach pracowniczych przydziałów mobilizacyjnych, 4) pełnienia służby w obronie cywilnej, 5) odbywania edukacji dla bezpieczeństwa, 6) uczestniczenia w samoobronie ludności, 7) odbywania ćwiczeń w jednostkach przewidzianych do militaryzacji i pełnienia służby w jednostkach zmilitaryzowanych, 8) wykonywania świadczeń na rzecz obrony – na zasadach i w zakresie określonych w ustawie.

Dokumenty normujące działania w sieciach teleinformatycznych.

Ustawy.

WYDZIAŁ ZARZĄDZANIA

ACTA (ang. Anti-Counterfeiting Trade Agreement) to umowa handlowa dotycząca zwalczania obrotu towarami podrabianymi. Pomysł zawarcia międzynarodowego porozumienia powstał w USA w 2006 r. W styczniu 2012 r. Unia Europejska postanowiła podpisać umowę. Mimo to kilka miesięcy później się z tej deklaracji za pośrednictwem Parlamentu Europejskiego wycofała. To efekt ogromnych protestów pod hasłem „precz z cenzurą internetu". Uczestnikom wielotysięcznych manifestacji nie podobało się to, że umowa była negocjowana w sposób tajny. Zawarte w niej postanowienia zaś groziły ograniczeniami dla internautów. Regulacje były też wyraźnie korzystne dla największych sieciowych przedsiębiorców, niekorzystne zaś dla małych i średnich firm.

Tajne negocjacje
Do niedawna nie udostępniono wszystkich dokumentów związanych z procesem negocjacji ani nie przeprowadzono rzetelnych konsultacji społecznych.

Ryzyko naruszenia prawa do prywatności i ochrony danych osobowych
Posiadacze praw autorskich będą mogli żądać od dostawców internetu ujawniania im danych osobowych użytkowników.

Potencjalne podrożenie usług telekomunikacyjnych
Wynikać ono będzie z faktu doinwestowania przez dostawców usług internetowych swojej infrastruktury. Nowe prawo nałoży na dostawców zwiększenie monitorowania aktywności użytkowników w internecie. Każdy twój ruch będzie monitorowany co będzie generowało olbrzymie ilości danych, które trzeba będzie składować przez długi czas.

Ograniczenie wolności słowa
ACTA zobowiązuje dostawców internetu do monitorowania treści i działań, jakie podejmują użytkownicy, nadając im rolę „policji internetowej".

26 mar 2019. Parlament Europejski przyjął projekt dyrektywy o ochronie praw autorskich w Internecie. Przepisy miały być wymierzone w takich gigantów i monopolistów, jak Google, czy Facebook muszą płacić twórcom za powielane treści: artykuły prasowe, dzieła literackie, filmy czy muzykę..

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych

- Reguluje między innymi przedmiot, podmiot, oraz ochronę przedmiotu prawa autorskiego.
- Podstawowym założeniem jest rozróżnienie **autorskich praw osobistych** („ojcostwa utworu") oraz **autorskich praw majątkowych** (ang. *copyright*). Ustawa – zgodnie z nazwą reguluje także prawa pokrewne – związane z wykonaniami, produkcją i dystrybucją utworów.
- Od 19 lipca 2018 r. zasady działania organizacji zbiorowego zarządzania prawami autorskimi lub prawami pokrewnymi normuje odrębna ustawa.
- Zgodnie z polską ustawą, przedmiotem prawa autorskiego jest każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia.
- Prawo autorskie działa automatycznie – ochrona praw autorskich rozpoczyna się z chwilą ustalenia utworu, bez konieczności spełnienia jakichkolwiek formalności. Utwór nie musi przy tym być skończony.

WYDZIAŁ ZARZĄDZANIA

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (cd)

- Dla użytku osobistego wolno korzystać bez zgody twórcy utworu i nieodpłatnie z pojedynczych egzemplarzy utworu rozpowszechnionego, tzn. takiego, który za zezwoleniem twórcy został udostępniony publicznie
- Zakres podmiotowy prywatnego użytku obejmuje krąg osób pozostających w związku osobistym, w szczególności pokrewieństwa, powinowactwa lub stosunku towarzyskiego (art. 23 ust. 2 ustawy). Oznacza to na przykład, że można swoim krewnym i znajomym pożyczać, bądź wykonywać kopie książek, filmów, albumów muzycznych czy programów typu open source. Nie jest to jednak dozwolone w przypadku komercyjnych programów komputerowych bądź gier.
- Możliwe jest jednak podarowanie, bądź odsprzedaż również obcym osobom zakupionych wcześniej egzemplarzy utworów.
- **Można bez zgody autora przytaczać w utworach stanowiących samoistną całość urywki rozpowszechnionych utworów lub drobne utwory w całości, lecz trzeba podać autora i dzieło. Jest to tzw. prawo cytatu.**
- Twórca ma prawo do wynagrodzenia w przypadku, gdy rozpowszechnia się drobne utwory lub fragmenty większych utworów w podręcznikach, wypisach i antologiach w celu naukowym i dydaktycznym (art. 29 ust .2 i ust. 21ustawy).

Prawo autorskie [online]. Wikipedia : wolna encyklopedia, 2018-09-26 08:00Z [dostęp: 2018-09-30 14:16Z]. Dostępny w Internecie: //pl.wikipedia.org/w/index.php?title=Prawo_autorskie&oldid=54569285

WYDZIAŁ ZARZĄDZANIA

Plagiat.pl

1 Wartość **Współczynnika podobieństwa 1** określa, jaką część badanej pracy stanowią frazy o długości 5 wyrazów lub dłuższe, odnalezione w bazie uczelni macierzystej, bazach innych uczelni (uczestniczących w Międzyuczelnianym Programie Wymiany Baz), bazie RefBooks lub w zasobach Internetu (z wyłączeniem fragmentów aktów prawnych odnalezionych w Bazie Aktów Prawnych - BAP). Współczynnik podobieństwa 1 służy przede wszystkim do badania samodzielności językowej autora pracy.

2 Wartość **Współczynnika podobieństwa 2** określa, jaka część badanej pracy składa się z fraz odnalezionych w w/w bazach (z wyłączeniem BAP) o długości 25 wyrazów lub dłuższej. Ze względu na długość wykrywanych fraz Współczynnik podobieństwa 2 jest lepszym narzędziem do wykrywania nieuprawnionych zapożyczeń.

Regulamin wykorzystania Systemu Antyplagiatowego AWL

§ 7

1. Operator Systemu dokonuje przeglądu Raportu Podobieństwa pod kątem występowania w pracy nieuprawnionych zapożyczeń, w szczególności ustala czy:
a. współczynnik podobieństwa 1 nie przekracza 50%,
b. współczynnik podobieństwa 2 nie przekracza 5%,
c. próbowano ukryć obecność nieuprawnionych zapożyczeń („alert”).

Dokumenty normujące działania w sieciach teleinformatycznych.

WYDZIAŁ ZARZĄDZANIA

Geneza ustawy

- Obecność baz danych w prawie autorskim
- Specyfika ochrony baz danych prawem autorskim
  - Ograniczenie do „twórczych" elementów struktury, układu, zestawienia danych
- W dotychczasowym stanie prawnym - brak ochrony nakładu inwestycyjnego poniesionego na stworzenie bazy danych
- Potrzeba wzmocnienia ochrony w związku z rozwojem elektronicznych baz danych
  - Łatwość korzystania, przetwarzania i powielania elektronicznych baz danych

Art. 1. Bazy danych podlegają ochronie określonej w ustawie niezależnie od ochrony przyznanej na podstawie ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2006 r. Nr 90, poz. 631, Nr 94, poz. 658, Nr 121, poz. 843 oraz z 2007 r. Nr 99, poz. 662) bazom danych spełniającym cechy utworu.

Art. 2. 1. W rozumieniu ustawy:

1) baza danych oznacza zbiór danych lub jakichkolwiek innych materiałów i elementów zgromadzonych według określonej systematyki lub metody, indywidualnie dostępnych w jakikolwiek sposób, w tym środkami elektronicznymi, wymagający istotnego, co do jakości lub ilości, nakładu inwestycyjnego w celu sporządzenia, weryfikacji lub prezentacji jego zawartości,

Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych

Ustawy.

Producent, którego prawa do bazy danych zostały naruszone, może żądać od osoby, która naruszyła te prawa:

1) zaniechania naruszania;
2) usunięcia skutków naruszenia;
3) naprawienia wyrządzonej szkody:
   a) na zasadach ogólnych albo
   b) poprzez zapłatę sumy pieniężnej w wysokości odpowiadającej dwukrotności, a w przypadku gdy naruszenie jest zawinione - trzykrotności stosownego wynagrodzenia, które w chwili jego dochodzenia byłoby należne tytułem udzielenia przez uprawnionego zgody na korzystanie z bazy danych;
4) wydania uzyskanych korzyści.

Podstawowe dokumenty normujące politykę bezpieczeństwa teleinformatycznego. Ustawy.

WYDZIAŁ ZARZĄDZANIA

Ustawy uchylone

USTAWA

z dnia 29 sierpnia 1997 r.

o ochronie danych osobowych[1)]

Rozdział 1

Art. 1. 1. Każdy

2. Przetwarzanie dany

publiczne, dobro osoby, kt

i trybie określonym ust

Art. 2. 1. Ust

osobowych oraz prawa

przetwarzane w zbiorach d

uchylona 2018-05-25

USTAWA

z dnia 22 stycznia 1999 r.

o ochronie informacji niejawnych

Rozdział 1

1. Ustawa określa zasa

uprawnionym ujawnie

wą, niezależnie od form

wania, zwanych dalej

1) organizowania

2) klasyfikow

3) udostępn

4) postępowan

rękojmię zach

jącym";

uchylona 2011-01-02

USTAWA

z dnia 18 września 2001 r.

o podpisie elektronicznym[1)]

Rozdział I

Przepisy ogólne

Art. 1. Usta

prawne jego s

nadzoru nad podmio

Art. 2. Przepisy ust

certyfikacyjne, mających

Rzeczypospolitej Pol

Art. 3. U

1) podpis elek

danymi, do kt

służą do identyfikac

uchylona 2016-10-07

Podstawowe dokumenty normujące politykę bezpieczeństwa teleinformatycznego. Ustawy.

WYDZIAŁ ZARZĄDZANIA

Art. 1. Ustawa określa:

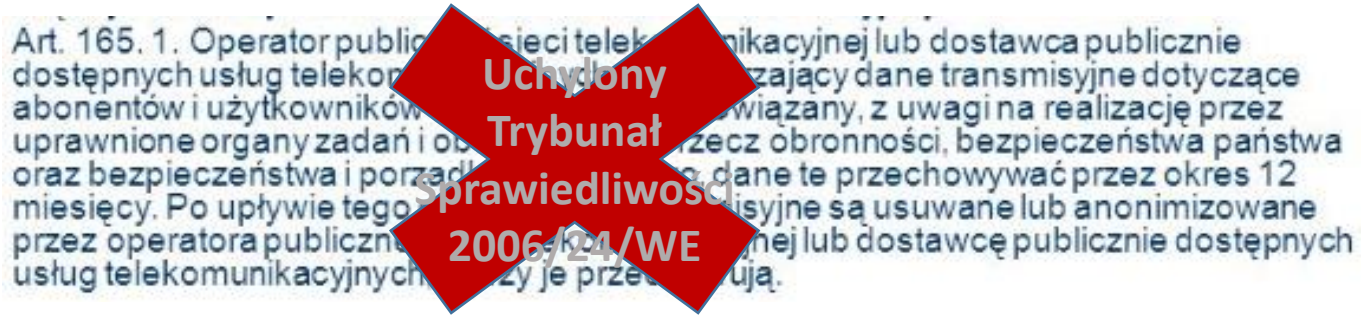
1) obowiązki usługodawcy związane ze świadczeniem usług drogą elektroniczną;
2) zasady wyłączania odpowiedzialności usługodawcy z tytułu świadczenia usług drogą elektroniczną;
3) zasady ochrony danych osobowych osób fizycznych korzystających z usług świadczonych drogą elektroniczną.

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (UŚDE)

- Ustawa dotyczy usług, których wykonanie następuje przez wysyłanie i odbieranie danych za pomocą systemów teleinformatycznych na indywidualne żądanie usługobiorcy (klienta), bez jednoczesnej obecności stron, przy czym dane te muszą zostać transmitowane **za pośrednictwem sieci publicznych**.
- W szczególności przykładem są usługi umożliwiające zawieranie w tym trybie umów sprzedaży, reklamy, informacji handlowej.
- Nie jest zaliczany zarówno **przekaz telewizyjny jak i radiowy** (nie są dostarczane na indywidualne żądanie usługobiorców), tradycyjne usługi telekomunikacyjne np. bankomatowe, sprzedaż biletów w automatach, gry losowe.

Podstawowe dokumenty normujące politykę bezpieczeństwa teleinformatycznego. Ustawy.

WYDZIAŁ ZARZĄDZANIA



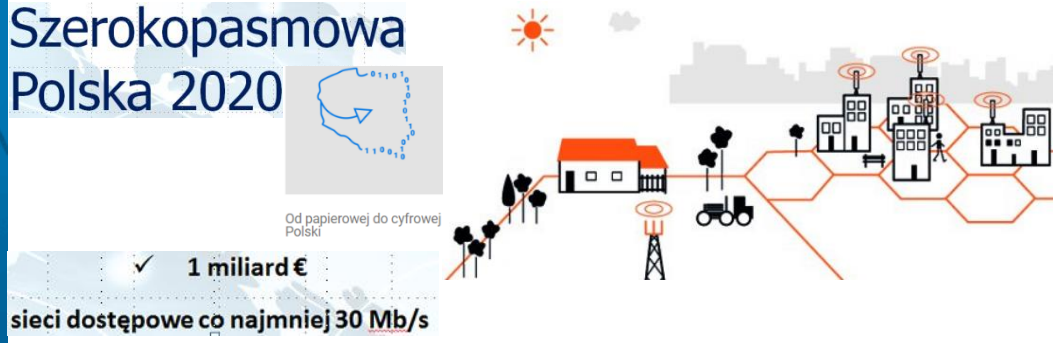
Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne

Cele:

- wspieranie równoprawnej i skutecznej konkurencji w zakresie świadczenia usług telekomunikacyjnych;
- rozwój i wykorzystanie nowoczesnej infrastruktury telekomunikacyjnej;
- zapewnienie ładu w gospodarce numeracją, częstotliwościami oraz zasobami orbitalnymi;
- zapewnienie użytkownikom maksymalnych korzyści w zakresie różnorodności, ceny i jakości usług telekomunikacyjnych
- zapewnienie neutralności technologicznej.

Dokumenty normujące działania w sieciach teleinformatycznych.

WYDZIAŁ ZARZĄDZANIA



Ustawa z 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (tzw. megaustawa)

Ustawy.

- formy i zasady wspierania inwestycji telekomunikacyjnych, w tym związanych z sieciami szerokopasmowymi;
- zasady działalności w zakresie telekomunikacji jednostek samorządu terytorialnego oraz podmiotów wykonujących zadania z zakresu użyteczności publicznej;
- zasady dostępu do infrastruktury telekomunikacyjnej, i innej infrastruktury technicznej, finansowanych ze środków publicznych;
- prawa i obowiązki inwestorów, właścicieli, użytkowników wieczystych nieruchomości, osób, którym przysługuje spółdzielcze prawo do lokalu, zarządców nieruchomości oraz lokatorów, w szczególności w zakresie dostępu do nieruchomości, w celu zapewnienia warunków świadczenia usług telekomunikacyjnych;
- zasady lokalizowania regionalnych sieci szerokopasmowych oraz innej infrastruktury telekomunikacyjnej.

Dokumenty normujące działania w sieciach teleinformatycznych.

Ustawy.

WYDZIAŁ ZARZĄDZANIA

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (UOIN)

- Wprowadzenie ustawy było związane z potrzebą dostosowania prawa do wymagań wiążących się z członkostwem Polski w NATO i w Unii Europejskiej, w szczególności z dokumentem regulującym politykę bezpieczeństwa **C-M(2002)49 z dnia 17 czerwca 2002 r. – "Bezpieczeństwo w ramach organizacji Traktatu Północnoatlantyckiego„**
- Wśród wyróżników informacji niejawnych wymienia się takie wartości jak **niepodległość, suwerenność, integralność terytorialna, bezpieczeństwo wewnętrzne, porządek konstytucyjny, sojusze, pozycja międzynarodowa, gotowość obronna, identyfikacja, życie lub zdrowie funkcjonariuszy, żołnierzy, pracowników służb, świadków koronnych.**

Dokumenty normujące działania w sieciach teleinformatycznych. Ustawy.

WYDZIAŁ ZARZĄDZANIA

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (cd)

- W zależności od tego, jaki skutek miałoby udostępnienie informacji wyróżniono
  - „wyjątkowo poważna szkoda” przy nadaniu klauzuli ŚCIŚLE TAJNE; NATO COSMIC TOP SECRET ; EU TOP SECRET ,
  - „poważna szkoda” przy nadaniu klauzuli TAJNE; NATO (EU) SECRET
  - „szkoda” przy nadaniu klauzuli POUFNE; NATO (EU) CONFIDENTIAL
  - „szkodliwy wpływ” przy nadaniu klauzuli ZASTRZEŻONE; NATO (EU) RESTRICTED
- Kontrolę ochrony informacji niejawnych prowadzą Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego w zakresie opisanym w ustawie o ochronie informacji niejawnych z 5 sierpnia 2010 roku.
- Za ujawnienie informacji o klauzuli *ściśle tajne* albo *tajne* polski Kodeks karny przewiduje karę pozbawienia wolności od 3 miesięcy do 5 lat.
- Za ujawnienie informacji o klauzuli *poufne* lub *zastrzeżone* przez funkcjonariusza publicznego grozi kara pozbawienia wolności do 3 lat

Dokumenty normujące działania w sieciach teleinformatycznych.

Ustawy.

WYDZIAŁ ZARZĄDZANIA

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (cd)

- ABW albo SKW udziela akredytacji dla systemu teleinformatycznego o klauzuli POUFNE lub wyższej, zaś o klauzuli ZASTRZEŻONE kierownik jednostki organizacyjnej. Podstawą dla akredytacji jest dokumentacja.
- Na dokumentację bezpieczeństwa systemu teleinformatycznego składają się dwa dokumenty: **szczególne wymagania bezpieczeństwa (SWB)** oraz **procedury bezpiecznej eksploatacji (PBE).**
- Jako wzór mogą posłużyć szczegółowe zalecenia opracowywania dokumentów SWB i PBE. Stanowią one dokumentację urzędową Agencji Bezpieczeństwa Wewnętrznego, a ich rozpowszechnianie odbywa się jedynie za pośrednictwem Departamentu Bezpieczeństwa Teleinformatycznego ABW.
- Więcej informacji można znaleźć w Rozporządzeniu Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego, na stronach:

- https://bip.abw.gov.pl/bip/informacje-niejawne-1/bezpieczenstwo-teleinf/154,BEZPIECZENSTWO-TELEINFORMATYCZNE.pdf
- https://www.bezpieczneit.com/dokumentacja-swb-pbe-systemu-niejawnego/
- **oraz w publikacji Metodyka opracowywania szczególnych wymagań bezpieczeństwa dla systemów lub sieci teleinformatycznych, SG WP, GZDiŁ, Warszawa 2000, Łączn. wew. 51/2000.**

Dokumenty normujące działania w sieciach teleinformatycznych.

Ustawy.

WYDZIAŁ ZARZĄDZANIA

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (cd)

- Dokument Procedur Bezpiecznej Eksploatacji powinien zawierać wykazy czynności (operacji), które realizować będą użytkownicy systemu TI wraz z dokładnym podaniem sposobu ich wykonania.
- Wymienione wykazy czynności powinny być pogrupowane w tematycznie wyodrębnione procedury bezpieczeństwa, opisujące sposób implementacji w systemie TI zasad bezpieczeństwa i środków ochrony określonych w dokumencie Szczególnych Wymagań Bezpieczeństwa.
- Oprócz „typowych” procedur bezpieczeństwa, w dokumencie PBE powinny również zostać przedstawione informacje, które są niezbędne dla użytkowników systemu TI w celu zapewnienia sprawnego i bezpiecznego funkcjonowania systemu TI.
- Wszystkie procedury bezpieczeństwa opracowane dla danego systemu TI powinny być ze sobą spójne, opracowane według określonego schematu i w określonej szacie graficznej.
- Treść procedur powinna być jasna i precyzyjna.

Dokumenty normujące działania w sieciach teleinformatycznych.

WYDZIAŁ ZARZĄDZANIA

DVB-T

Ustawy.

Ustawa z dnia 30 czerwca 2011 r. o wdrożeniu naziemnej telewizji cyfrowej (tekst jedn. z dnia 29 kwietnia 2016 r.)

Określa:

- sposób wdrożenia naziemnej telewizji cyfrowej,
- obowiązki operatorów,
- obowiązki nadawców.

Dokumenty normujące działania w sieciach teleinformatycznych.

Ustawy.

WYDZIAŁ ZARZĄDZANIA

Ustawa z 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej

- Wprowadza do polskiego prawa Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014, określane skrótem eIDAS (electronic IDentification, Authentication and trust Services)`
- Z dniem 1 lipca 2016 r. rozporządzenie to zastąpiło dyrektywę 1999/93/WE w sprawie wspólnotowych ram prawnych dla podpisów elektronicznych
- Obowiązuje bezpośrednio, bez konieczności transpozycji zawartych w nim przepisów na grunt prawa krajowego, dlatego została uchylona ustawa z 18 września 2001 r. o podpisie elektronicznym.
- Przepisy eIDAS mają duże znaczenie dla firm działających w Europie. Upraszczają one i standaryzują system identyfikatorów cyfrowych i podpisywania w całej Europie, przyczyniając się do powstania wspólnego rynku cyfrowego.

Dokumenty normujące działania w sieciach teleinformatycznych.

Ustawy.

WYDZIAŁ ZARZĄDZANIA

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych

- Ustawa jest uzupełnieniem i uszczegółowieniem RODO -unijnego rozporządzenia o ochronie danych osobowych, które obowiązuje od 25 maja 2018 roku.
- Nowy organ właściwy w sprawie ochrony danych osobowych - Prezesa Urzędu Ochrony Danych Osobowych. GIODO staje się Prezesem Urzędu, jego biuro staje się Urzędem Ochrony Danych Osobowych, a pracownicy zatrudnieni w biurze GIODO stają się pracownikami tego Urzędu.

Dokumenty normujące działania w sieciach teleinformatycznych.

Ustawy.

Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC)

- Efektem ma być podniesienie odporności usług kluczowych świadczonych z wykorzystaniem technologii informatycznych na ataki pochodzące z cyberprzestrzeni.
- Ustawa ma przyczynić się do zapewnienia ciągłości działania tych usług, tak aby zarówno obywatele, jak i przedsiębiorstwa miały do nich stały i niezakłócony dostęp.
- KSC obejmuje operatorów tzw. usług kluczowych z sektorów: energetyczny, zdrowotny, bankowy i transportowy, zaopatrzenia w wodę, infrastruktury cyfrowej (zał. 1), dostawców usług cyfrowych, określone podmioty publiczne (wymienione w art. 4 pkt 7-15 np. NBP), podmioty świadczące usługi z zakresu cyberbezpieczeństwa, organy właściwe (w randze ministra), Pełnomocnika Rządu, Kolegium ds. Cyberbezpieczeństwa (organ opiniodawczo doradczy przy Radzie Ministrów), niżej określone Zespołów Reagowania na Incydenty.
- Ustawa określa zadania trzech Zespołów Reagowania na Incydenty (Computer Security Incident Response Team): zespołu resort obrony narodowej (CSIRT MON), zespołu ABW (CSIRT GOV) oraz zespołu NASK (CSIRT NASK), a także zadania pozostałych członków KSC.

Dokumenty normujące działania w sieciach teleinformatycznych.

Ustawy.

Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC)

- Efektem ma być podniesienie odporności usług kluczowych świadczonych z wykorzystaniem technologii informatycznych na ataki pochodzące z cyberprzestrzeni.
- Ustawa ma przyczynić się do zapewnienia ciągłości działania tych usług, tak aby zarówno obywatele, jak i przedsiębiorstwa miały do nich stały i niezakłócony dostęp.
- KSC obejmuje operatorów tzw. usług kluczowych z sektorów: energetyczny, zdrowotny, bankowy i transportowy, zaopatrzenia w wodę, infrastruktury cyfrowej (zał. 1), dostawców usług cyfrowych, określone podmioty publiczne (wymienione w art. 4 pkt 7-15 np. NBP), podmioty świadczące usługi z zakresu cyberbezpieczeństwa, organy właściwe (w randze ministra), Pełnomocnika Rządu, Kolegium ds. Cyberbezpieczeństwa (organ opiniodawczo doradczy przy Radzie Ministrów), niżej określone Zespołów Reagowania na Incydenty.
- Ustawa określa zadania trzech Zespołów Reagowania na Incydenty (Computer Security Incident Response Team): zespołu resort obrony narodowej (CSIRT MON), zespołu ABW (CSIRT GOV) oraz zespołu NASK (CSIRT NASK), a także zadania pozostałych członków KSC.

Dokumenty normujące działania w sieciach teleinformatycznych.

Ustawy.

Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC)

- Ustawa wyznacza więc trzy CSIRT poziomu krajowego: CSIRT NASK w strukturach Państwowego Instytutu Badawczego NASK, CSIRT GOV w strukturach Agencji Bezpieczeństwa oraz CSIRT MON w strukturach Resortu Obrony Narodowej (RON)
- Każdy CSIRT poziomu krajowego ma jasno określone constituency – zakres podmiotów, które zobowiązane są raportować i którym świadczy on wsparcie. CSIRT MON koordynuje obsługę incydentów zgłaszanych przez podmioty podległe Ministrowi Obrony Narodowej i przedsiębiorstwa o szczególnym znaczeniu gospodarczo–obronnym.
- CSIRT GOV koordynuje incydenty zgłaszane przez administrację rządową, Narodowy Bank Polski, Bank Gospodarstwa Krajowego oraz operatorów infrastruktury krytycznej.
- CSIRT NASK koordynuje natomiast incydenty zgłaszane przez pozostałe podmioty, w tym m.in. operatorów usług kluczowych [13], dostawców usług cyfrowych, samorząd terytorialny. Do CSIRTNASK incydenty mogą także zgłaszać osoby fi yczne – zwykli obywatele. Można więcpowiedzieć, że CSIRT NASK stanowi tzw. cert ostatniej szansy (CERT of last resort)

Dokumenty normujące działania w sieciach teleinformatycznych.

Ustawy.

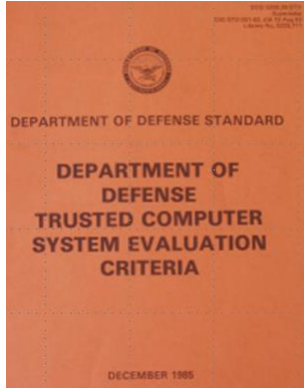
Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC)

- Wszystkie trzy CSIRT poziomu krajowego mają za zadanie współpracować z organamiwłaściwymi (więcej informacji na ten temat w rozdziale 3.1.), ministrem właściwym ds.informatyzacji oraz Pełnomocnikiem ds. Cyberbezpieczeństwa. Poza tym do ich zadań należy między innymi:
  - monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym;
  - szacowanie ryzyka w skali kraju;
  - przekazywanie informacji na temat incydentów i ryzyk innym podmiotom wchodzącym wskład krajowego systemu cyberbezpieczeństwa;
  - wydawanie komunikatów o zidentyfi kowanych zagrożeniach cyberbezpieczeństwa;
  - reagowanie na zgłoszone incydenty;
  - koordynowanie obsługi incydentów krytycznych (po wcześniejszym ich zakwalifikowaniujako incydenty krytyczne);
  - w uzasadnionych przypadkach badanie urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, której wykorzystanie może zagrozić integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwapaństwa;
  - …

Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (weszła w życie 6.02.19)

- Ustawa wdraża do polskiego porządku prawnego dyrektywę Parlamentu Europejskiego i Rady UE 2016/680 z 27 kwietnia 2016 regulującą sferę wyłączoną spod rozporządzenia o ochronie danych osobowych (RODO) tzw. „dyrektywa policyjna" (przetwarzanie danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, swobodnego przepływu takich danych).
- Określa zasady i warunki ochrony danych osobowych przetwarzanych w związku z działalnością organów (policja, prokuratura, sądy) powołanych do realizacji wskazanych w niej celów. Nie zawiera katalogu podmiotów. Reguluje zasady ochrony danych osobowych m.in. w odniesieniu do czynności operacyjno-rozpoznawczych, dochodzeniowo-śledczych i administracyjno-porządkowych, które są związane z zapobieganiem i zwalczaniem przestępczości.
- Osoba, której dane są przetwarzane ma m.in. prawo dostępu do nich, ich uzupełnienia, uaktualnienia lub sprostowania, usunięcia gdy są przetwarzane z naruszeniem przepisów.
- Spod działania ustawy ze względu na wykonywanie zadań dotyczących bezpieczeństwa narodowego wyłączone są służby specjalne: Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Służbę Kontrwywiadu Wojskowego, Służbę Wywiadu Wojskowego oraz Centralne Biuro Antykorupcyjne.

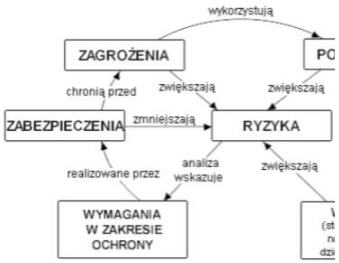
WYDZIAŁ ZARZĄDZANIA

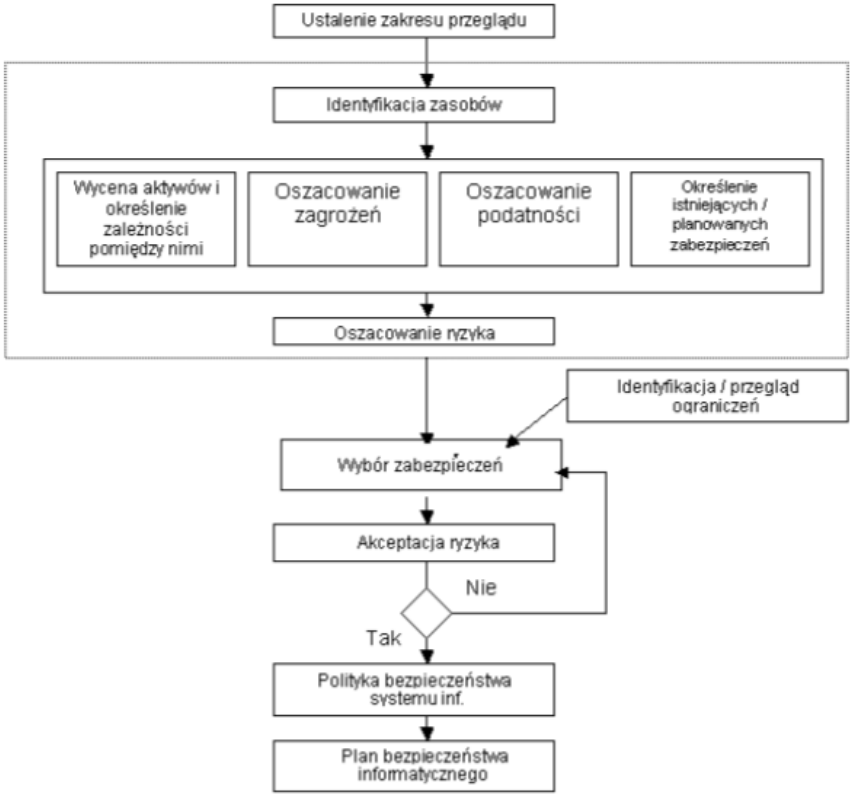


Standardy bezpieczeństwa teleinformatycznego o znaczeniu fundamentalnym.

- Wyłanianie się systemów wielodostępnych oraz sieciowych w latach sześćdziesiątych wywołało potrzebę w zakresie prac nad ich bezpieczeństwem.
- Jako jeden z pierwszych dojrzałych dokumentów uznaje się zwykle tak zwaną „Pomarańczową Księgę”(powstała w 1983, uaktualniona w 1985).
- Wśród organizacji standaryzacyjnych szerzej odniesiemy się do wyników:
  - ISO – International Standard Organization
  - IEC – Internationa Electrotechnical Commission
  - BSI – British Standard Institution
  - NIST – National Institute of Standards and Technology
- Do standardów o znaczeniu fundamentalnym trzeba niewątpliwie zaliczyć:
  - **Raporty techniczne ISO/IEC TR 13335** określane jako Wytyczne dla Zarządzania Bezpieczeństwem IT. Obecnie już nie rozwijane, ale wciąż stanowią wciąż podstawę dla zrozumienia stosowanych pojęć oraz rozwiązań.
  - **Publikacje NIST** dotyczące bezpieczeństwa teleinformatycznego (FIPS 199, FIPS 200, Publikacje Specjalne) prezentujące szczegółowe, amerykańskie spojrzenie
  - **Rodzinę standardów ISO/IEC 2700** ukształtowaną na ogólnym spojrzeniu BSI, obecnie najbardziej rozpowszechnioną oraz dynamicznie się rozwijającą.

WYDZIAŁ ZARZĄDZANIA





ISO/IEC TR 13335

- ISO/IEC 13335-1 / PN-I-13335-1 Wyt
do zarządzania bezpieczeństwem syster
  - Terminologia, związki między pojęc
  - Podstawowe modele
- ISO/IEC 13335-2 Technika informaty
bezpieczeństwem systemów inform
  - Różne podejścia do planowania an
  - Plany zabezpieczeń
  - Organizacja służb odpowiedzialnyc
  - Role i stanowiska pracy w instytucji związane z bezpieczeństwem
- ISO/IEC 13335-3 Techniki zarządzania bezpieczeństwem systemów informatycznych
  - Szczegółowe przedstawienie procesów zarządzania.
  - Formułowanie trójpoziomowej polityki bezpieczeństwa.
  - Rozwinięcie problematyki analizy ryzyka.
  - Rozwinięcie problematyki implementacji planu zabezpieczeń.
  - Czynności powdrożeniowe, w tym: utrzymanie, monitorowanie i reagowanie na incydenty

WYDZIAŁ ZARZĄDZANIA

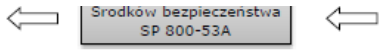
ISO/IEC TR 13335 (c.d.)

- ISO/IEC 13335-4 Wybór zabezpieczeń
  - Klasyfikacja i charakterystyka różnych form zabezpieczeń
  - Sposoby doboru zabezpieczeń ze względu na rodzaj zagrożenia albo specyfikę systemu
  - Prezentacja szczegółowych zaleceń wynikających z norm ISO/IEC i opracowanych przez różne organizacje
- ISO/IEC 13335-5 Zabezpieczenie dla połączeń z sieciami zewnętrznymi
  - Dobór zabezpieczeń stosowanych do ochrony styku systemów instytucji z siecią zewnętrzną

Źródło: Białas, A.: Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT, Warszawa, 2007

WYDZIAŁ ZARZĄDZANIA

1. SP 800-12 (DRAFT) Rev. 1: *An Introduction to Information Security*, january 2017.
2. SP-800-39: Managing Risk from Information Systems. *An Organizational Perspective*.
3. SP-800-50: *Building an Information Technology Security Awareness and Training Program*.
4. SP-800-53 Rev.4: *Recommended Security Controls for Federal Information System*, april 2013.



2353-1290, Nr 48/2016

Publikacje NIST

- Amerykańska agencja federalna opracowująca standardy i zalecenia techniczne dla administracji rządowej USA.
- W odpowiedzi na ogłoszony w Stanach Zjednoczonych w roku 2002 Akt Zarządzania Bezpieczeństwem Informacji (Federal Information Security Management Act FISMA), nakładający na organizacje państwowe obowiązek ochrony informacji NIST opracował dwa standardy (FIPS 199, FIPS 200) oraz szereg tzw. Publikacji Specjalnych (Special Publications SP), które są dostępne w PDF-ach na stronie
  - **http://csrc.nist.gov/publications/PubsSPs.html**.
- Przegląd przedsięwzięć związanych z postępowaniem w procesie budowy systemu bezpieczeństwa teleinformatycznego wraz z odesłaniem do publikacji szczegółowych zawiera **SP 800-12**. Zasadniczym dokumentem dotyczącym zarządzania bezpieczeństwem informacji jest **SP 800-53.** Dokument ten zawiera wytyczne do wybierania i specyfikowania mechanizmów bezpieczeństwa (security controls).

WYDZIAŁ ZARZĄDZANIA

Grupa zabezpieczenia	Lp.	Klasa zabezpieczenia	Symbol	Liczba zabezpieczeń w klasie
Zabezpieczenia organizacyjna Managment controls (29)	1	Oszacowanie ryzyka *(Risk Assessment)*	RA	5
	2	Planowanie (*Planning*)	PL	6
	3	Pozyskiwanie systemów i usług *(System and Services Acquisition)*	SA	11
	4	Certyfikacja, akredytacja i ocena bezpieczeństwa *(Certification, Accreditation, and Security Assessments)*	CA	7

National Institute of Standards and Technology (c.d.)

- Wyróżniono 168 zabezpieczeń w ramach trzech grup zabezpieczeń związanych z przedsięwzięciami: organizacyjnymi (ang. management controls), operacyjnymi (ang. operational controls) i technicznymi (ang. technical controls).
- Dodatkowo w każdej grupie wyróżniono klasy zabezpieczenia. W sumie jest 17 klas zabezpieczeń:
  - Grupa zabezpieczeń organizacyjnych klasy 1 – 4 (4 klasy, 29 zabezpieczeń)
  - Grupa zabezpieczeń operacyjnych klasy 5 – 13 (9 klasy, 80 zabezpieczeń)
  - Grupa zabezpieczeń organizacyjnych klasy 14 – 17 (4 klasy, 59 zabezpieczeń)
- W każdej klasie są podane zabezpieczenia niezbędne, zdaniem autorów rekomendacji, do osiągnięcia określonego poziomu ochrony (niski, średni, wysoki).

WYDZIAŁ ZARZĄDZANIA

Grupa zabezpieczenia	Lp.	Klasa zabezpieczenia	Symbol	Liczba zabezpieczeń w klasie
Zabezpieczenia operacyjne *Operational controls* (80)	5	Bezpieczeństwo osobowe *(Personnel Security)*	PS	8
	6	Ochrona fizyczna i środowiskowa *(Physical and Environmental Protection)*	PE	19
	7	Planowanie ciągłości działania *(Contingency Planning)*	CP	10
	8	Zarządzanie konfiguracją *(Configuration Management)*	CM	7
	9	Konserwacja *(Maintenance)*	MA	6
	10	Integralność systemu i informacji *(System and Information Integrity)*	SI	12
	11	Ochrona nosników *(Media Protection)*	MP	6
	12	Reakcja na incydenty *(Incident Response)*	IR	7
	13	Uświadamianie i trening *(Awareness and Training)*	AT	5

National Institute of Standards and Technology (c.d.)

WYDZIAŁ ZARZĄDZANIA

Grupa zabezpieczenia	Lp.	Klasa zabezpieczenia	Symbol	Liczba zabezpieczeń w klasie
Zabezpieczenia techniczne *Technical controls* (59)	14	Identyfikacja i autentykacja *(Identification and Authentication)*	IA	7
	15	Kontrola dostępu *(Access Control)*	AC	20
	16	Audyt i rozliczalność *(Audit and Accountability)*	AU	11
	17	Ochrona systemu i łączy *(System and Communications Protection)*	SC	21

National Institute of Standards and Technology (c.d.)

- W odróżnieniu od ogólnych norm ISO standardy NIST są bardziej techniczne i szczegółowe.
- To pewnie z tego powodu, pomimo że dedkowane były amerykańskim agencjom federalnym, znajdują uznanie na całym świecie.

Źródło: Liderman, K.: Bezpieczeństwo informacyjne, PWN, Warszawa, 2012, str. 51-52.

Dokumenty normujące działania w sieciach teleinformatycznych.

Standardy

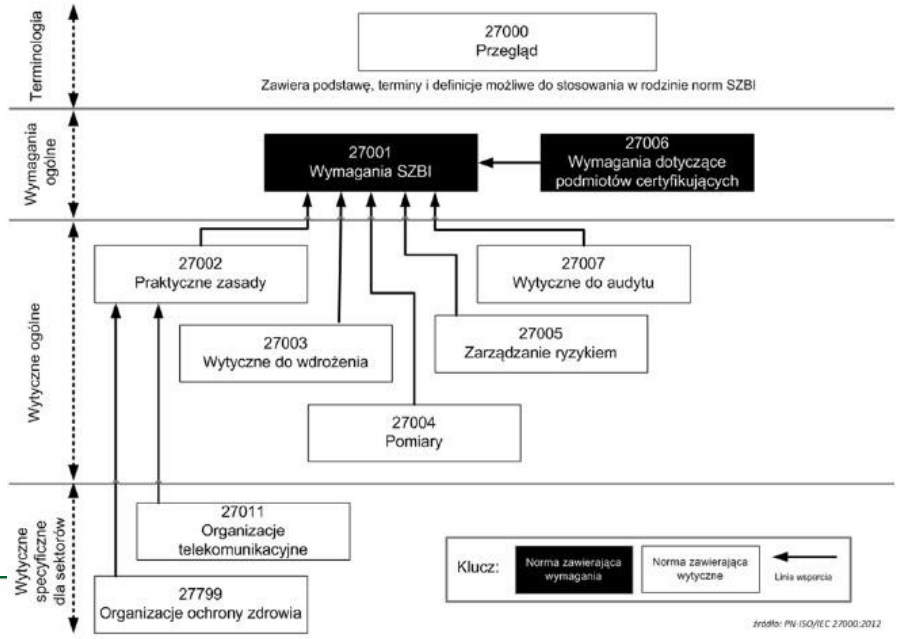
WYDZIAŁ ZARZĄDZANIA

Rodzina standardów ISO/IEC 27000: Geneza

- Angielski rodowód : Kodeks postępowania PD003 pod egidą Departamentu Handlu i Przemysłu
- Normy o charakterze wytycznych i wymagań
- Szybki rozwój. Poprawione wersje w 1999.
- Podejście procesowe w drugiej wersji z 2002 roku. Zgodność z ISO (PDCA, nacisk na zarządzanie ryzykiem.
- Wersje międzynarodowe tzw. „szybka ścieżka", wersje polskie wprowadzane ze zmniejszającym się opóźnieniem.
- Rozwój innych norm rodziny 2700
- Dostosowanie do Aneksu SL.

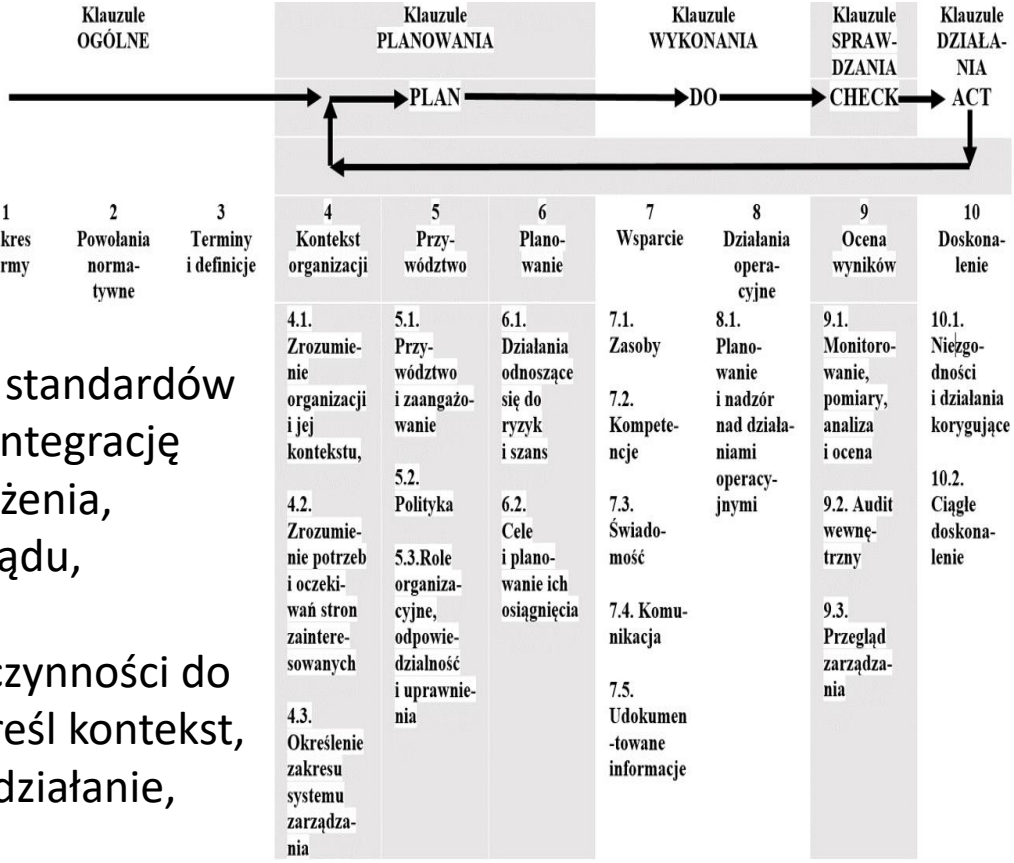
WYTYCZNE	ROK	WYMAGANIA
BS PD0003:1993	1993	
	1994	
BS 7799-1:1995	1995	
	1996	
	1997	
	1998	BS7799-2:1998
BS 7799-1:1995	1999	BS7799-2:1999
ISO/IEC 1799:2000	2000	
	2001	
BS 7799-1:2002	2002	BS7799-2:2002
PN-ISO/IEC 1799:2003	2003	
	2004	
ISO/IEC 1799:2005	2005	ISO/IEC 27001:2005; PN-I-07799-2:2005
	2006	
ISO/IEC 27002:2007	2007	ISO/IEC 27006:2007;PN-ISO/IEC 27001:2007
ISO/IEC 27005:2008; ISO/IEC 27779:2008	2008	
ISO/IEC27000:2009; ISO/IEC 27004:2009	2009	PN ISO/IEC 27006:2009
ISO/IEC27003:2010; PN-EN ISO 27799:2010	2010	
ISO/IEC 27005:2011; ISO/IEC 27007:2011	2011	
ISO/IEC 27013:2012; ISO/IEC 27032:2012	2012	
ISO/IEC 27002:2013	2013	ISO/IEC 27001:2013
ISO/IEC 2700:2014-11;PN-ISO/IEC 2700:2014-11; PN-ISO/IEC 27002:2014-12	2014	PN-ISO/IEC 27001:2014-12
PN ISO/IEC 2705:2014-01; PN ISO/IEC 2713:2014-01	2014	PN-ISO/IEC 27006:2014-01

Uchwała ISO TMB 12/2012 dotycząca zalecenia stosowania przez wszystkie Komitety ISO wymagań ISO Guide 8 HLS, które to wymagajnia zostają włączone do Załącznika SL (Annex XL) Dyrektywa ISO/IEC.



Relacje w ramach rodziny norm SZBI

WYDZIAŁ ZARZĄDZANIA



ISO/IEC 27001

- Struktura identyczna dla wszystkich standardów zarządzania ISO co ma wspomagać integrację
- Wymagania dla ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia SZBI.
- Podklauzule klauzul 4-10 wskazują czynności do wykonania i udokumentowania (określ kontekst, zorganizuj przywództwo, wsparcie, działanie, ocenianie oraz doskonalenie)
- Cykl doskonalenia PDCA wpisany już nie w standardzie, ale w strukturze klauzul.
- W procesie certyfikacji dokonywana jest ocena zgodności systemu zarządzania bezpieczeństwem informacji organizacji na zgodność z normą (ocena dokumentacji, wywiady dotyczące funkcjonowania system, testy zabezpieczeń, raporty z audytów ich ocena, ocena audytorów, podjęcie decyzji o przyznaniu certyfikatu.
- Certyfikat jest ważny trzy lata, po których audyt wznawiający (recertyfikacja).
- Certyfikacja zwiększa szanse pozyskania nowych rynków i klientów, dla wielu z nich spełnienie norm może być podstawowym warunkiem do rozpoczęcia współpracy.

Dokumenty normujące działania w sieciach teleinformatycznych.

Standardy

WYDZIAŁ ZARZĄDZANIA

ISO/IEC 27002

- 90-stronicowe wytyczne
- 14 klauzul (rozdziały 5-18) - obszarów bezpieczeństwa
- 35 kategorii bezpieczeństwa (podrozdziały)
- 114 zabezpieczeń
- Sposób wybierania zabezpieczeń oparty na analizie ryzyka
- Każda z 35 kategorii bezpieczeństwa zawiera:
  - Cele zabezpieczeń
  - Jedno lub więcej zabezpieczeń
- Każde zabezpieczenie zawiera
  - Nazwę i opis
  - Wskazówki implementacyjne
  - Dodatkowe informacje

Contents

Infrastruktura krytyczna i jej ochrona

- Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym definiuje infrastrukturę krytyczną jako systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi **kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców.**
- Zakres ochrony infrastruktury krytycznej został sprecyzowany w Narodowym Programie Ochrony Infrastruktury Krytycznej wydanym przez Rządowe Centrum Bezpieczeństwa (pierwsze wydanie 2013, aktualizacja 2015). Zgodnie z zapisami wymienionego dokumentu ochrona infrastruktury krytycznej obejmuje ochronę: fizyczną, techniczną, osobową, teleinformatyczną, prawną oraz plany odbudowy.
- Dokument nie zawiera kompletu zasad i informacji na temat ochrony infrastruktury krytycznej, może jednak posłużyć jako rozbudowana lista kontrolna tego, jak należy zorganizować system ochrony IK.

WYDZIAŁ ZARZĄDZANIA

11-systemów wchodzących w skład IK oraz ministrowie odpowiedzialni

WYKAZ MINISTRÓW ODPOWIEDZIALNYCH ZA POSZCZEGÓLNE SYSTEMY INFRASTRUKTURY KRYTYCZNEJ[2]

Systemy infrastruktury krytycznej	Minister odpowiedzialny za system infrastruktury krytycznej
System zaopatrzenia w energię, surowce energetyczne i paliwa	Minister Energii
System łączności	Minister Cyfryzacji Minister Infrastruktury i Budownictwa
System sieci teleinformatycznych	Minister Cyfryzacji
System finansowy	Minister Finansów
System zaopatrzenia w żywność	Minister Rolnictwa i Rozwoju Wsi
System zaopatrzenia w wodę	Minister Środowiska
System ochrony zdrowia	Minister Zdrowia
System transportowy	Minister Infrastruktury i Budownictwa Minister Gospodarki Morskiej i Żeglugi Śródlądowej
System ratowniczy	Minister Spraw Wewnętrznych i Administracji
System zapewniający ciągłość działania administracji publicznej	Minister Cyfryzacji
System produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych	Minister Środowiska

Infrastruktura krytyczna i jej ochrona

- W celu maksymalnej obiektywizacji Rządowe Centrum Bezpieczeństwa, we współpracy z ministrami i kierownikami urzędów centralnych oraz przy wsparciu przedsiębiorców prywatnych, opracowało kryteria identyfikacji IK. Kryteria te mają charakter niejawny
- Zgodnie z ustawą o zarządzaniu kryzysowym obowiązek ochrony obiektów, urządzeń, instalacji i usług infrastruktury krytycznej został powierzony operatorom infrastruktury krytycznej

WYDZIAŁ ZARZĄDZANIA

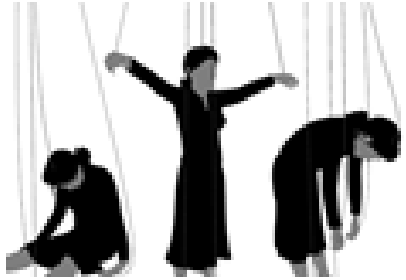
Zagrożenia dla bezpieczeństwa cyberprzestrzeni

- **Cyberprzestępczość** najczęściej definiuje się jako niezgodne z prawem działanie podmiotów niepaństwowych poprzez używanie IT, których celem jest zdobywanie zysków.
- **Cyberkonflikty**, czyli konflikty związane z działaniami w cyberprzestrzeni dzielimy na:
  - aktywizm – niedestrukcyjną działalność, w ramach której cyberprzestrzeń służy do wsparcia prowadzonej kampanii,
  - haktywizm – kombinację aktywizmu i działań przestępczych; wykorzystuje metody hackerskie przeciwko określonym celom w Internecie, by zakłócić ich funkcjonowanie, nie powodując przy tym poważnych strat; działalność ta ma na celu nie tyle zniszczenie zasobów przeciwnika, ale przede wszystkim zwrócenie uwagi na dany problem,
  - cyberterroryzm – politycznie motywowany atak lub groźba ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach realizacji daleko idących politycznych i społecznych działań w szerszym rozumieniu tego słowa; jest to także użycie cyberprzestrzeni do komunikowania się, propagandy i dezinformacji przez organizacje terrorystyczne.
- **Cyberszpiegostwo** to wykorzystanie cyberprzestrzeni do celów wywiadowczych. Również pozyskiwanie informacji poprzez ominięcie lub osłabienie sprzętowych i programowych mechanizmów kontroli dostępu a także włamanie się do systemu objętego ochroną.
- **Cyberinwigilacja** jest kontrolą społeczeństwa poprzez narzędzia teleinformatyczne. Najczęściej jest stosowana w państwach autorytarnych i totalitarnych. Jest to zjawisko bardzo podobne do cyberterroryzmu. Może również polegać na ograniczeniu dostępu obywateli do cyberprzestrzeni.

WYDZIAŁ ZARZĄDZANIA

Walka informacyjna w cyberprzestrzeni

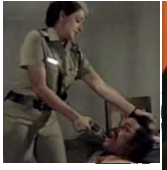
- Przestrzeń cybernetyczna jest dzisiaj uważana jako piąty wymiar pola walki.
- Rozgrywa się tu, nowy rodzaj wojny, czyli wojna informacyjna. Definiuje się ją jako działania (walka informacyjna) podjęte w celu osiągnięcia informacyjnej przewagi, wspierające narodową strategię militarną poprzez oddziaływania na informację i systemy informacyjne przeciwnika, przy jednoczesnej ochronie własnych informacji i systemów informacyjnych.
- W wyniku tych działań uzyskiwana jest kontrola nad treścią, przepływem i dostępnością istotnych informacji.
- Dwa rodzaje wojny informacyjnej w cyberprzestrzeni:
  - Netwar – wojna psychologiczna w cyberprzestrzeni, a więc propaganda mająca na celu formowanie morale żołnierzy oraz społeczeństwa, w szczególności osłabienie odporności psychicznej przeciwnika. Symbioza psychologii, w szczególności komunikacji społecznej oraz nowoczesnych technologii informacyjnych.
  - Cyberwar – penetracja infrastruktury przeciwnika w celu uzyskania nad nią kontroli lub jej zniszczenia w stosownym momencie, z jednoczesną ochroną własnej infrastruktury, z wykorzystaniem działań realizowanych w cyberprzestrzeni.
- Państwa narodowe często ukrywają swoją działalność pod przykrywką haktywistów, hakerów lub armii prywatnych, grup terrorystycznych i innych. Być może dlatego najczęściej posługujemy się terminem cyberatak.



Klasyfikacja cyberataków

I. **SOCJOTECHNIKA - ogół metod, środków i działań praktycznych zmierzających do wywołania pożądanych przemian w postawach lub zachowaniach społecznych, Mogą one, ale nie muszą leżeć w interesie osób podlegających socjotechnice. Wykorzystuje się szereg różnorodnych metod.**

- Miarą umiejętności socjotechnika jest jakość zgromadzonych przez niego informacji.
- Umiejętne **wywoływanie (elicitation)** pozwala na błyskawiczne uzyskiwanie informacji, do których dotarcie w inny sposób mogłoby wymagać dużego nakładu pracy, czasu oraz/lub umiejętności technicznych.
- **Wchodzenie w rolę (pretexting)** definiuje się jako kreowanie zmyślonego scenariusza w celu przekonania ofiary do ujawnienia określonych informacji lub podjęcia określonych działań.
- **Kotwiczenie –** proces wywoływania odruchowych, emocjonalnych powiązań przyczynowo-skutkowych z bodźcem.
- **Przeramowanie (reframing)** – taka zmiana kontekstu wypowiedzi, która nie zmieniając jej logicznej treści zmienia wypływające z niej wnioski.
- **Presupozycja** to wniosek wynikający zarówno ze zdania A, jak i z jego negacji np. presupozycją zarówno zdania "Obecny król Francji jest łysy" jak i zdania "Obecny król Francji nie jest łysy" jest: "Francja ma obecnie króla".



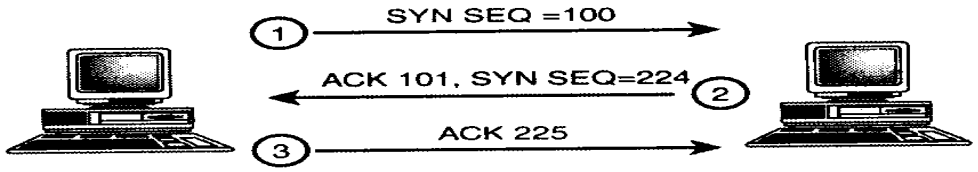


Klasyfikacja cyberataków.

I. **SOCJOTECHNIKA - ogół metod, środków i działań praktycznych zmierzających do wywołania pożądanych przemian w postawach lub zrachowaniach społecznych, Mogą one, ale nie muszą leżeć w interesie osób podlegających socjotechnice. Wykorzystuje się szereg różnorodnych metod.**

- **Rapport** – dostosowanie się do rozmówcy na poziomie pozycji ciała, tonacji głosu, sposobu wypowiadania się, a nawet oddechu.
- **Mikroekspresja (mowa ciała) –** bardzo krótko trwająca, rzędu 50 ms, pełna ekspresja mimiczna, charakterystyczna dla przeżywanej emocji.
- **Hipnoza** stan psychiczny (dokł. odmienny stan świadomości), pomiędzy snem a jawą, charakteryzujący się wzmożoną podatnością na sugestię.
- **Trash-diving (nurkowanie w śmieciach)** – przeszukiwanie wyrzuconych dokumentów.
- **Phishing** - oszukańcze pozyskanie poufnej informacji osobistej, jak hasła czy szczegóły karty kredytowej, przez udawanie osoby godnej zaufania, której te informacje są pilnie potrzebne.
- **Cyberstalking -** polega na ingerencji przestępcy w psychikę ofiary, na jej prześladowaniu i zastraszaniu.

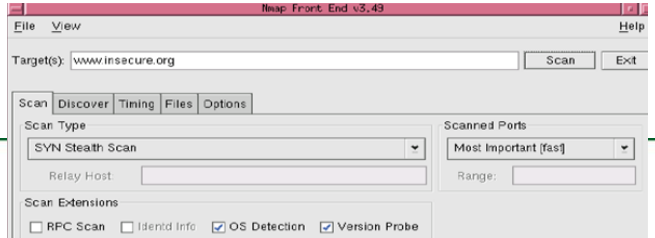
WYDZIAŁ ZARZĄDZANIA



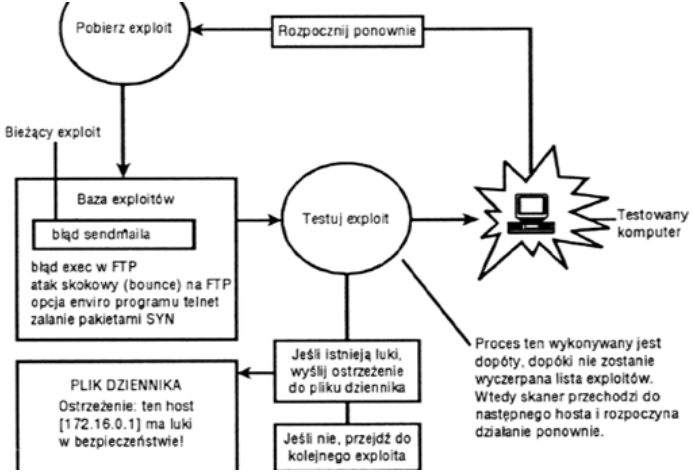
Klasyfikacja cyberataków (cd).

II. **SZPIEGOWANIE SIECI (NETWORK SNOOPING) - zaawansowana analiza sieci oraz hostów, której celem jest dobór metody ataku. Obejmuje między innymi**

- **Spacer po zaporze ogniowej (firewalking)** polegający na skanowaniu sieci chronionej zaporą ogniową oraz badaniu konfiguracji zapory ogniowej. Firewalking jest w pewnym sensie rozwinięciem traceroute.
- **Skanowanie hostów (network scanning)** atak aktywny polegający na przesyłaniu pakietów oraz analizowaniu odpowiedzi hostów z złożonego zakresu w celu wytypowania ofiary lub też poznania topologii atakowanej sieci. Uzyskujemy listę serwisów TCP/UDP uruchomionych na analizowanym hoście oraz wykaz podatności.
- **Zdejmowanie odcisku palca (fingerprinting) –** umożliwia uzyskanie informacji, jaki system operacyjny jest uruchomiony na badanym hoście, a nawet informację o wersji.
- **Podsłuchiwanie transmisji w sieci (sniffing) -** atak pasywny polega na monitorowaniu i rejestrowaniu ruchu sieciowego przepływającego przez dany host. Najprostsze sniffery przechwytują nazwy użytkowników i hasła, najbardziej złożone zapisują cały ruch sieciowy. Napisano wiele takich programów; wiele z nich dostępnych jest w Internecie za darmo.



WYDZIAŁ ZARZĄDZANIA

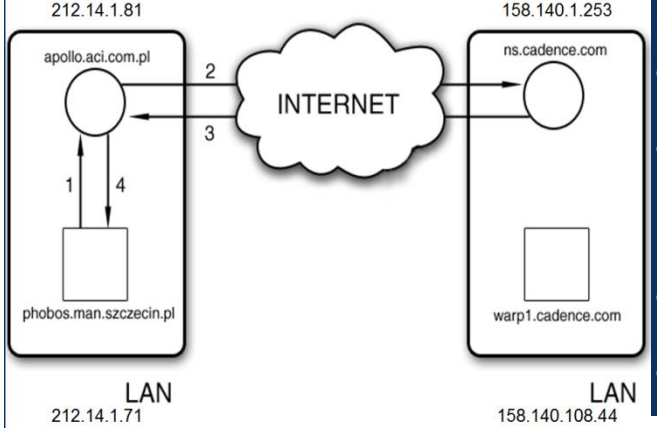


Klasyfikacja cyberataków (cd).

II. Szpiegowanie sieci (network snooping) - zaawansowana analiza sieci oraz hostów, której celem jest dobór metody ataku. Obejmuje między innymi

- **Tempest -** jest bardzo wyrafinowaną metodą przechwytywania haseł i innych informacji z komputera na podstawie emitowanych fal elektromagnetycznych, emitowanych w dużej ilości przez podzespoły komputera. Jedyną ochroną przed takim atakiem jest stworzenie osłony, która nie przepuszcza na zewnątrz żadnego promieniowania elektromagnetycznego.
- Wyrafinowane techniki szpiegowania elektronicznego wykorzystują specjalne oprogramowanie do zdalnego monitorowania aktywności na komputerze lub urządzeniu sieciowym.
- Na marginesie zauważmy, że większe firmy monitorują wykorzystanie komputerów przez swoich pracowników. Granica między dozwolonym, a nie dozwolonym monitoringiem pracowników nie została przez ustawodawcę sprecyzowana i jasno określona. Pracodawca chcąc zapewnić bezpieczeństwo prawne powinien uzyskać zgodę pracowników na zastosowanie środków kontroli, a także poinformować o celu, któremu środki mają służyć.

WYDZIAŁ ZARZĄDZANIA



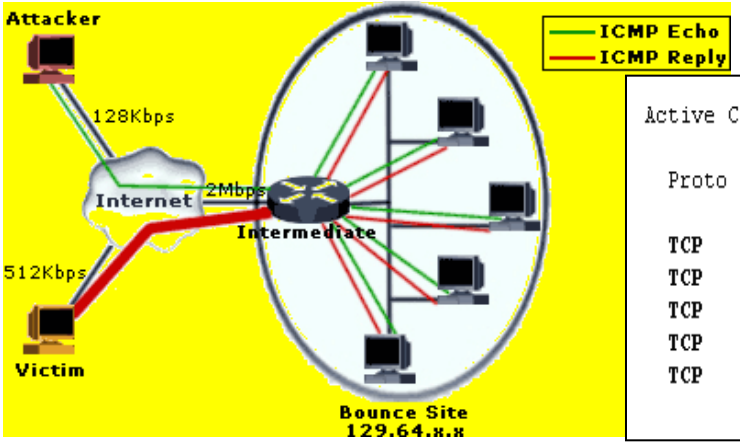
DNS spoofing, czyli podszywanie się pod serwer DNS (na podstawie artykułu T. Grabowskiego)

- Pole identyfikatora komunikatu jest dwubajtowej długości, a zatem istnieje możliwość wygenerowania maksymalnie 65535 różnych identyfikatorów.
- W najprostszym z możliwych przypadków intruz wyśle pakiety zawierające wszystkie możliwe identyfikatory komunikatu, czyli 65535 pakietów. Zakładając, że odpowiedź DNS, pod którą chce się podszyć intruz, zajmuje 183 bajty (tak jak w przykładzie przedstawionym wcześniej), musi on wysłać do atakowanego komputera około 11 MB danych.
- W nawiązaniu do przedstawionej podatności protokołu DNS powstało DNSSEC (ang. DNS Security Extensions) - rozszerzenie systemu DNS mające na celu zwiększenie jego bezpieczeństwa.
- DNSSEC zapewnia uwierzytelnianie źródeł danych (serwerów DNS) za pomocą kryptografii asymetrycznej oraz podpisów cyfrowych.

Klasyfikacja cyberataków (cd).

III. **PODSZYWANIE SIĘ (SPOOFING)** - w tradycyjnym ujęciu oznacza działanie atakującego, polegające na oszukaniu mechanizmu uwierzytelniania zachodzącego pomiędzy maszynami przekazującymi między sobą pakiety. Proces autoryzacji przeprowadzany jest poprzez sfałszowanie pakietów "zaufanego" hosta - należącego do atakowanej sieci.

- Istnieje wiele technik podszywania DNS spoofing, ARP spoofing, IP spoofing, …
- W sieciach lokalnych stosowany jest ARP spoofing, a więc podszycie się pod adres sprzętowy zaufanego komputera.
- Atak ten polega na wprowadzeniu zmian do bufora (cache) protokołu ARP (Address Resolution Protocol) , który zawiera informacje o odwzorowaniach adresów sprzętowych na sieciowy adres IP interfejsu, z którym nadawca pragnie się komunikować.
- ARP spoofing przeprowadzany jest głównie w sieciach lokalnych ze względu na fakt, iż protokół ARP nie jest protokołem internetowym.
- Obecnie mianem spoofingu określa się dowolną metodę łamania zabezpieczeń opartych na adresie lub nazwie hosta.

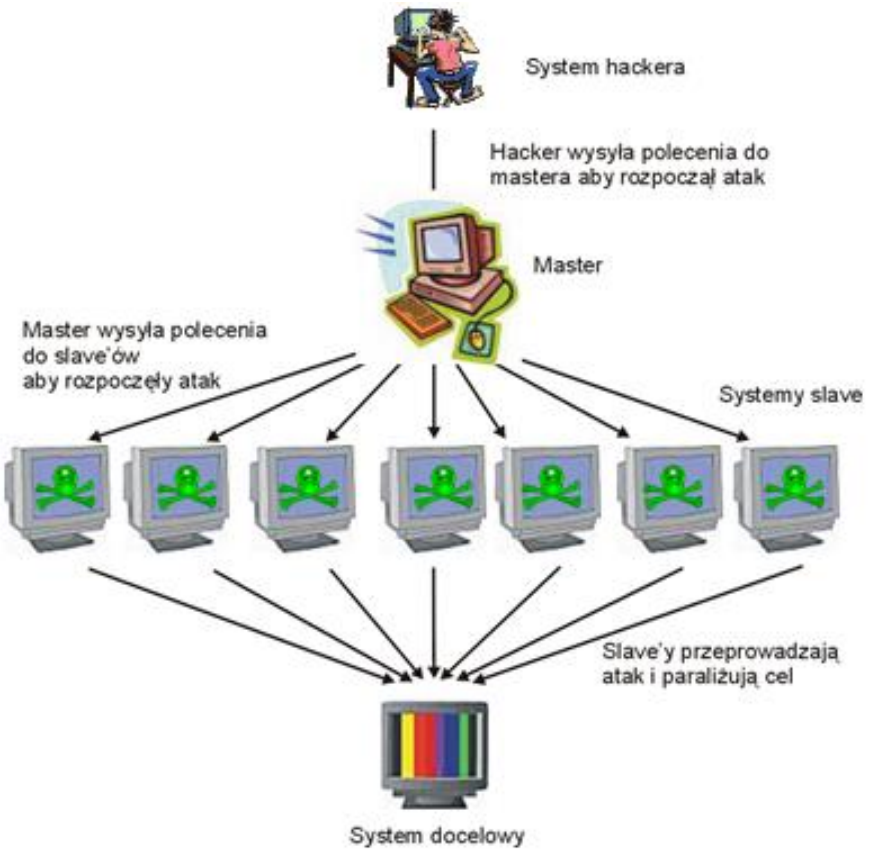



```
C:>netstat -n -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    172.29.44.16:80        172.29.27.254:1075     SYN_RECEIVED
  TCP    172.29.44.16:80        172.29.27.254:1076     SYN_RECEIVED
  TCP    172.29.44.16:80        172.29.27.254:1077     SYN_RECEIVED
  TCP    172.29.44.16:80        172.29.27.254:1078     SYN_RECEIVED
  TCP    172.29.44.16:80        172.29.27.254:1079     SYN_RECEIVED
```

Klasyfikacja cyberataków (cd).

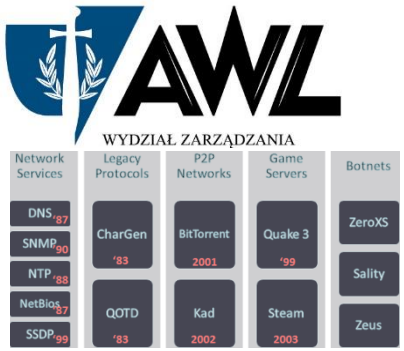
IV. **Blokowanie usług (Denial of service DoS) -** dowolne działanie unieruchamiające sprzęt lub oprogramowanie i powodujące zaprzestanie świadczenia usług przez system komputerowy.

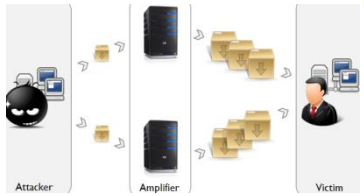
- **Ping flood** – popularny sposób ataku na serwer internetowy polegający na przeciążeniu łącza pakietami ICMP generowanymi na przykład przez program ping. Przeprowadza się go za pomocą komputera posiadającego łącze o przepustowości większej niż przepustowość łącza atakowanej maszyny, lub za pomocą wielu niezależnych komputerów (np. Smurf atack).
- Atakowany serwer otrzymuje bardzo dużą ilość zapytań ping ICMP Echo Request, odpowiadając na każde za pomocą ICMP Echo Reply, co może doprowadzić do przeciążenia jego łącza do internetu i w konsekwencji niedostępności oferowanych serwisów. Jednym ze sposobów obrony przed tego typu atakiem jest zapora sieciowa, która filtruje pakiety ICMP Echo Request.

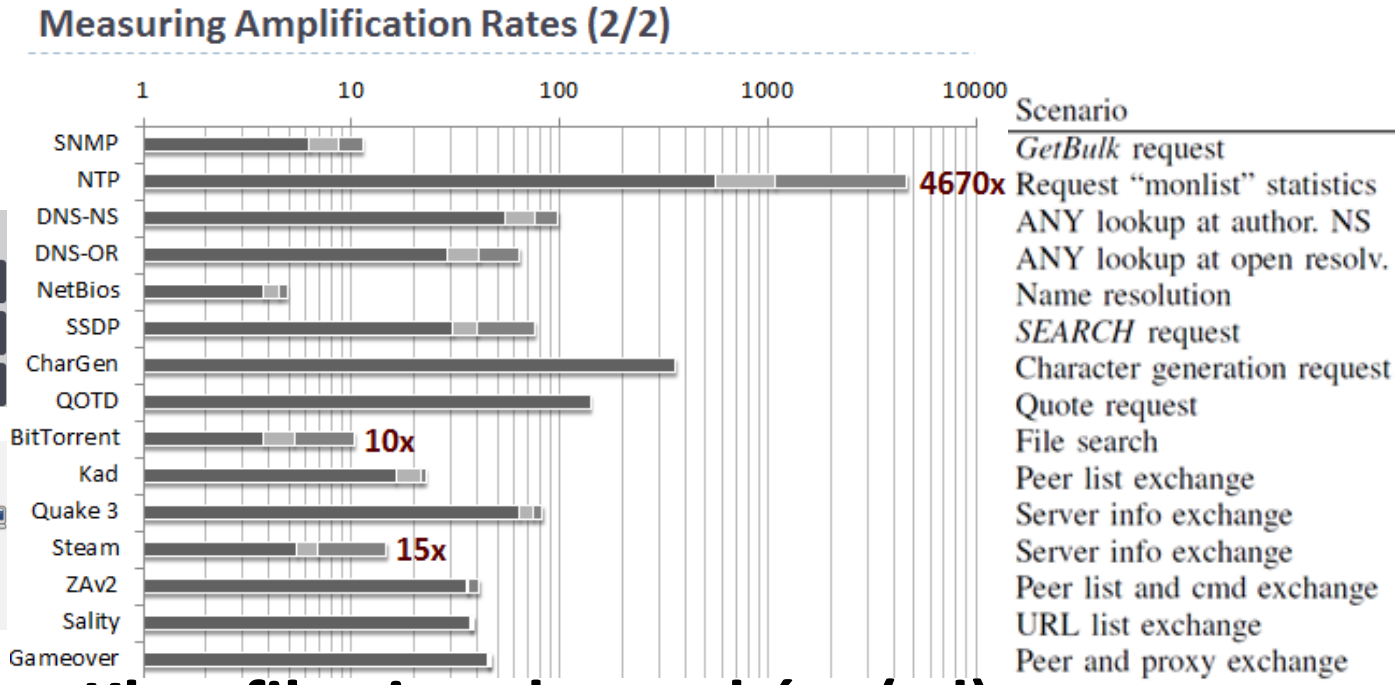


Klasyfikacja cyberataków (cd).

IV. **Blokowanie usług (Denial of service DoS) -** dowolne działanie unieruchamiające sprzęt lub oprogramowanie i powodujące zaprzestanie świadczenia usług przez system komputerowy.
   - **DDoS (Distributed Denial of Service)** to bardziej zaawansowana metoda DoS. Polega to na ataku rozproszonym - z wielu przejętych komputerów tzw. zombi jednocześnie. Zastosowanie wielu zombi zgrupowanych w ramach botnetu powoduje, że nawet wielkie i znane serwery padają po takim ataku.



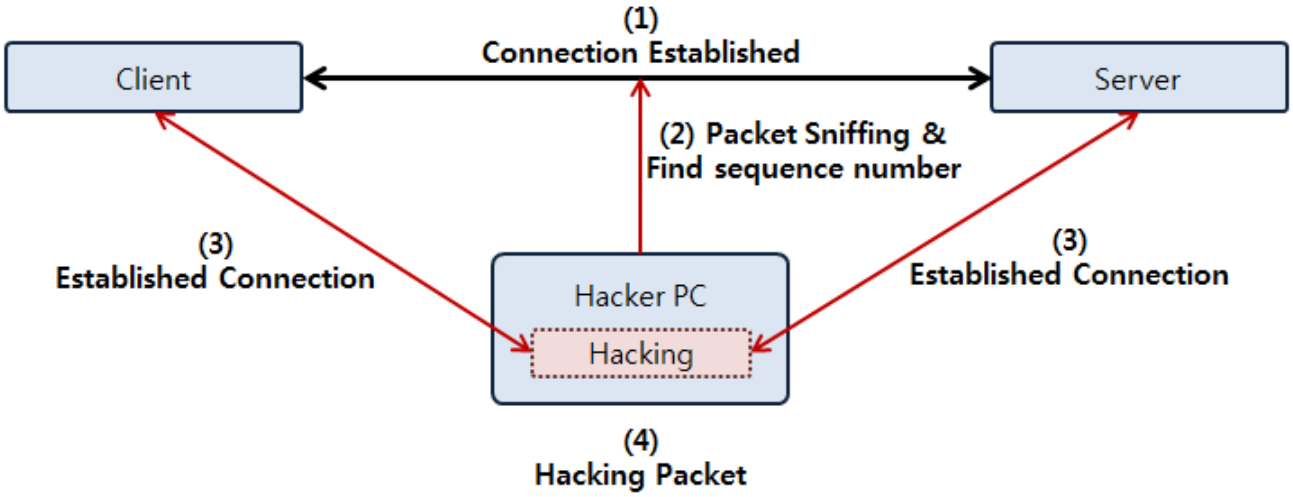




Klasyfikacja cyberataków (cd).

IV. **Blokowanie usług (Denial of service DoS) -** dowolne działanie unieruchamiające sprzęt lub oprogramowanie i powodujące zaprzestanie świadczenia usług przez system komputerowy.

- **Wzmocniony atak DDoS (Amplification DDoS)** – metoda jest …. bardzo efektywna. Wystarczy wysłać „zapytanie" do odpowiedniego serwisu internetowego (np. serwera czasu NTP), gdzie jako pytającego podaje się adres ofiary, a w efekcie serwis internetowy odpowiada ilością danych większą niż miało samo „zapytanie". Jeżeli te dane trafią na łącze ofiary to spowodują olbrzymi przyrost ruchu na łączu internetowym. Przy wykorzystaniu tej formy ataku bardzo łatwo można wysycić łącze internetowe dowolnego serwisu internetowego na świecie.



Klasyfikacja cyberataków (cd).

V. **PRZECHWYTYWANIE SESJI(HIJACKING) -** polega na przechwytywaniu transmisji odbywającej się między dwoma systemami. Dzięki temu wszystkie pakiety obu maszyn muszą przejść przez maszynę hakera, co stanowi poważne zagrożenie dla poufności przesyłanych danych. Ale jest to metoda specjalistyczna i stosowana tylko przez najlepszych.

- Następuje zerwanie połączenia TCP między dwoma systemami.
- Sesja TCP zostaje utrzymana tyle, że pakiety przepływają przez 3 komputer, który sprytnie zmienia numery sekwencyjne i potwierdzeń, aby pasowały klientowi oraz serwerowi.
- Użytkownik nie ma pojęcia, że jego sesja została przerwana, gdyż otrzymuje dane o które prosił.
- Modyfikując pakiety można nie tylko przesyłać żądania klienta, ale także dopisać własne np. z prośbą o wylistowanie zawartości danego katalogu lub inne.

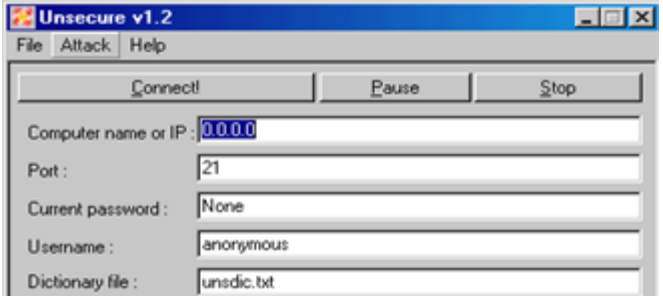
WYDZIAŁ ZARZĄDZANIA

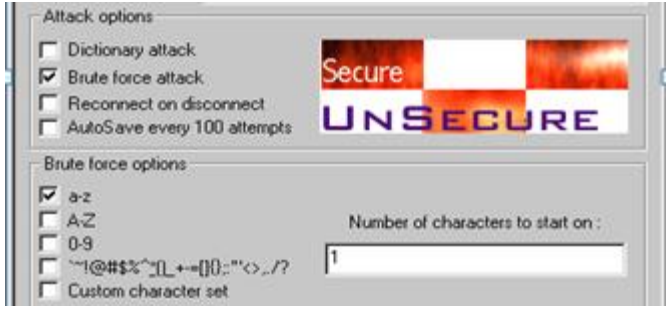
Klasyfikacja cyberataków (cd).

VI. **UZYSKANIE UPRAWNIEŃ SUPER UŻYTKOWNIKA(ROOT COMPROMISE)** to atak polegający na opracowaniu metody prowadzącej do opanowania systemu poprzez uzyskanie uprawnień administratora systemu inaczej nazywanego root'em. Atak ten wykorzystuje luki w systemie, tak aby uzyskać zmianę statusu atakującego, ze zwykłego użytkownika na administratora.

- Exploit - jest zautomatyzowaną metodą prowadzącą do opanowania systemu (także do zwiększenia uprawnień).
- Zero-day exploit jest publikowany tuż po ogłoszeniu istnienia określonej podatności w określonej aplikacji zanim producent wypuści "łatki" naprawiające ów błąd.
- Zero-class attack - jest to typowo indywidualny exploit typu non-public (niepublikowany oficjalnie), który to wykorzystuje także niepublikowaną oficjalnie lukę. Zarówno administrator, użytkownicy jak i autor podatnej aplikacji w ogóle nie wiedzą, iż w ich produkcie jest błąd, nie wiedzą także, że powstał już exploit wykorzystujący właśnie ten błąd (tak więc nie są świadomi tego, iż konkretny włamywacz jest w stanie ich zaatakować; fałszywe poczucie bezpieczeństwa). Exploity typu zero-class attack mogą działać "niezauważalnie" nawet przez okres kilku lat!

WYDZIAŁ ZARZĄDZANIA





Klasyfikacja cyberataków (cd).

VII. ŁAMANIE HASEŁ (PASSWORD CRACKING) jest ogólnym terminem opisującym różne czynności, których celem jest ominięcie mechanizmów ochrony systemu komputerowego opartych na systemie haseł, a więc wszelkie próby złamania, odszyfrowania lub skasowania haseł.

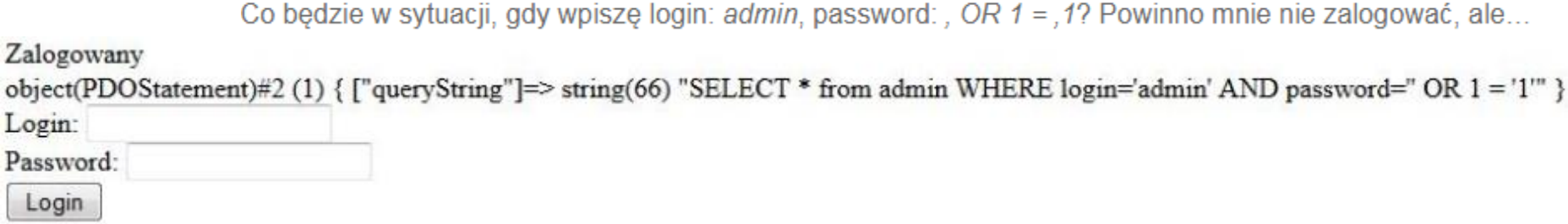
- Hasło po wprowadzeniu jest zamieniane na skrót (message digest) i porównywane z listą haseł. Odnalezienie dopasowania nazwy logowania oraz skrótu warunkuje dostęp do systemu.
- Atak siłowy (Brute force) - to najprostszy sposób wyszukiwania tajnych kluczy i haseł.
- Metoda słownikową - hasło łamie program, który do łamania wykorzystuje wcześniej spreparowany przez hackera słownik.
- Tęczowe tablice (rainbow tables) – zakładają wykorzystanie olbrzymich, wcześniej przygotowanych tablic z częściowo przeliczonymi danymi, które będą wykorzystywane wielokrotnie do odnajdywania różnych haseł.
- Znaleziona ostatnio metoda pozwala budować tablice, które przechowują ułamek wszystkich możliwych haszy, a mimo to gwarantują odtworzenie około 99% wszystkich haseł w ciągu kilku minut. Dobrym sposobem na zabezpieczenie się przed tego typu atakiem jest stosowanie tzw. soli (ang. salt).

WYDZIAŁ ZARZĄDZANIA

Klasyfikacja cyberataków (cd).

VIII. KRET (MOLE) wiadomość e-mail, którą nadawca wykorzystuje w celu otrzymania określonych informacji o jej odbiorcy - najczęściej jego adresu IP.

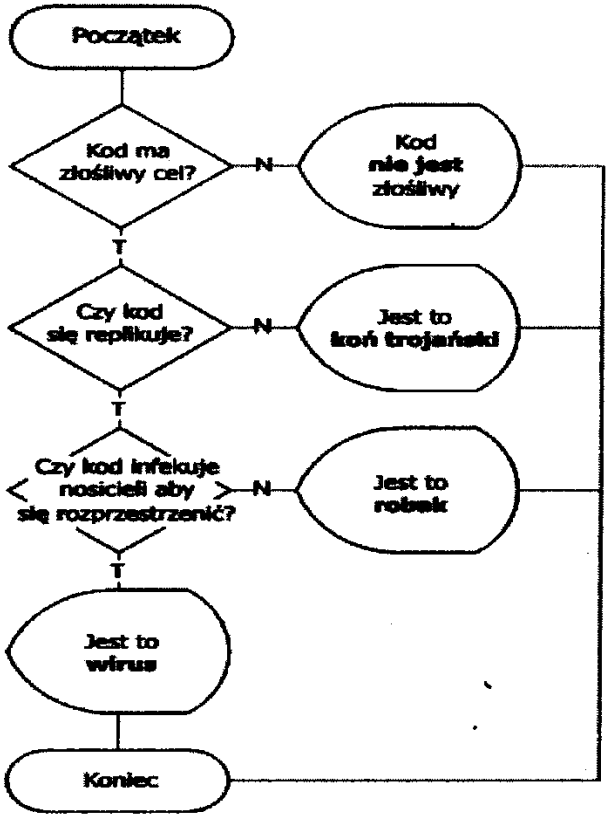
- Nadawca po odebraniu odpowiedzi na wiadomość może z nagłówka odczytać adres IP komputera oraz informacje na temat systemu operacyjnego danej osoby.
- Inna metoda polega na wysłaniu wiadomości w formacie HTML zawierającej odwołanie do pliku (np. grafiki) znajdującego się na serwerze nadawcy. Podczas otwierania takiej przesyłki, program automatycznie wysyła żądanie pobrania obrazka, pozostawiając w ten sposób ślad po sobie na serwerze, w tym własny adres IP.
- Metoda ta wykorzystywana jest zwłaszcza do przechwytywania dynamicznych adresów IP.
- Wejście w posiadanie adresu użytkownika oraz informacji na temat jego systemu operacyjnego pozwala następnie atakującemu wybrać odpowiednią metodę ataku oraz przeprowadzić ją na konkretny komputer.

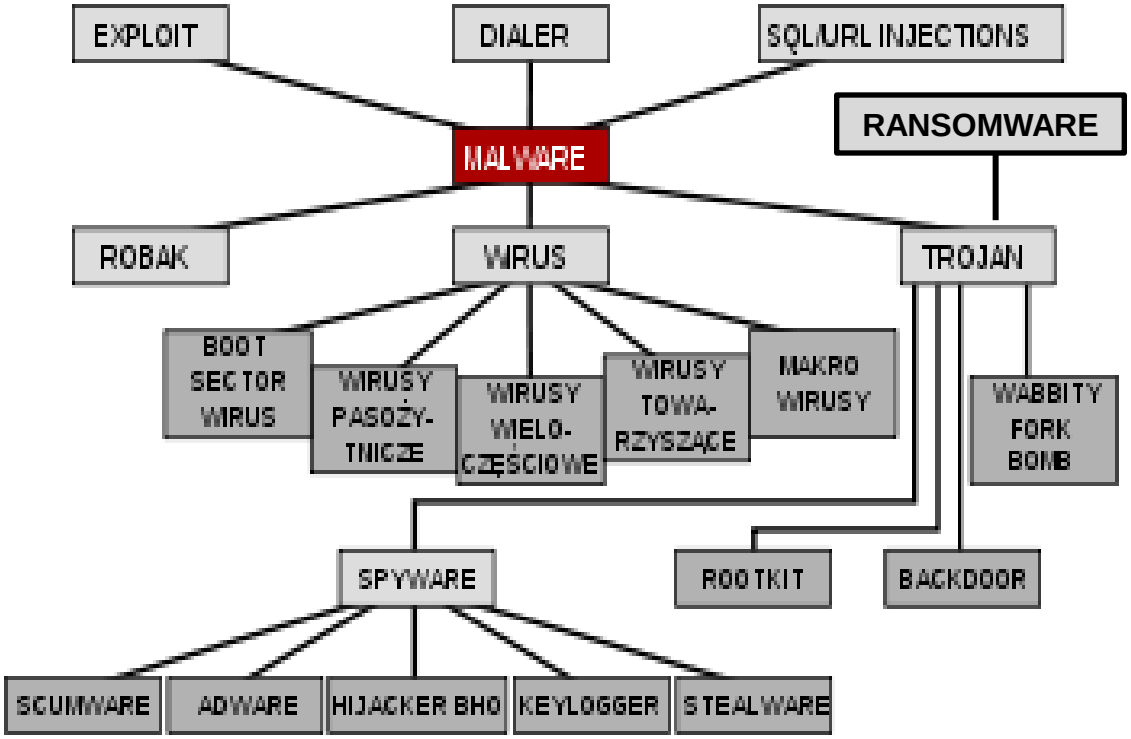


Klasyfikacja cyberataków (cd).

IX. **WEB-HACKING** - rodzina ataków internetowych wymierzonych w aplikacje web'owe, tzn. skrypty, formularze, itp. .

- Z reguły do skutecznego przeprowadzania takich ataków wymagana jest wyłącznie przeglądarka internetowa.
- Za pośrednictwem odpowiedniej manipulacji adresem w pasku URL lub poprzez manipulację przy wysyłaniu danych przez wszelakie "aktywne pola", atakujący jest w stanie przeprowadzić skuteczny atak na daną witrynę www lub użytkownika, który ją przegląda.
- Ostatnimi czasy terminem Web-hacking określa się także ataki wymierzone w użytkownika a wykorzystujące słabości samej przeglądarki internetowej (mowa tu głównie o plikach cookie).
- Code Injection - polega na spreparowaniu specjalnego ciągu i "wstrzyknięciu" go do aplikacji poprzez pasek URL, formularz on-line, itp. Spreparowanym ciągiem może być czyste wyrażenie HTML, SQL lub charakterystyczny dla danej platformy język komunikacji z nią. Podatna aplikacja pobiera dane od atakującego i wykonuje bez sprawdzenia, czy dane te są poprawnym czystym tekstem. Dzięki temu, włamywacz dostaje m.in możliwość generowania kodu wykonywanego w systemie, co może owocować nawet uzyskaniem uprawnień administratora.





Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).

WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).

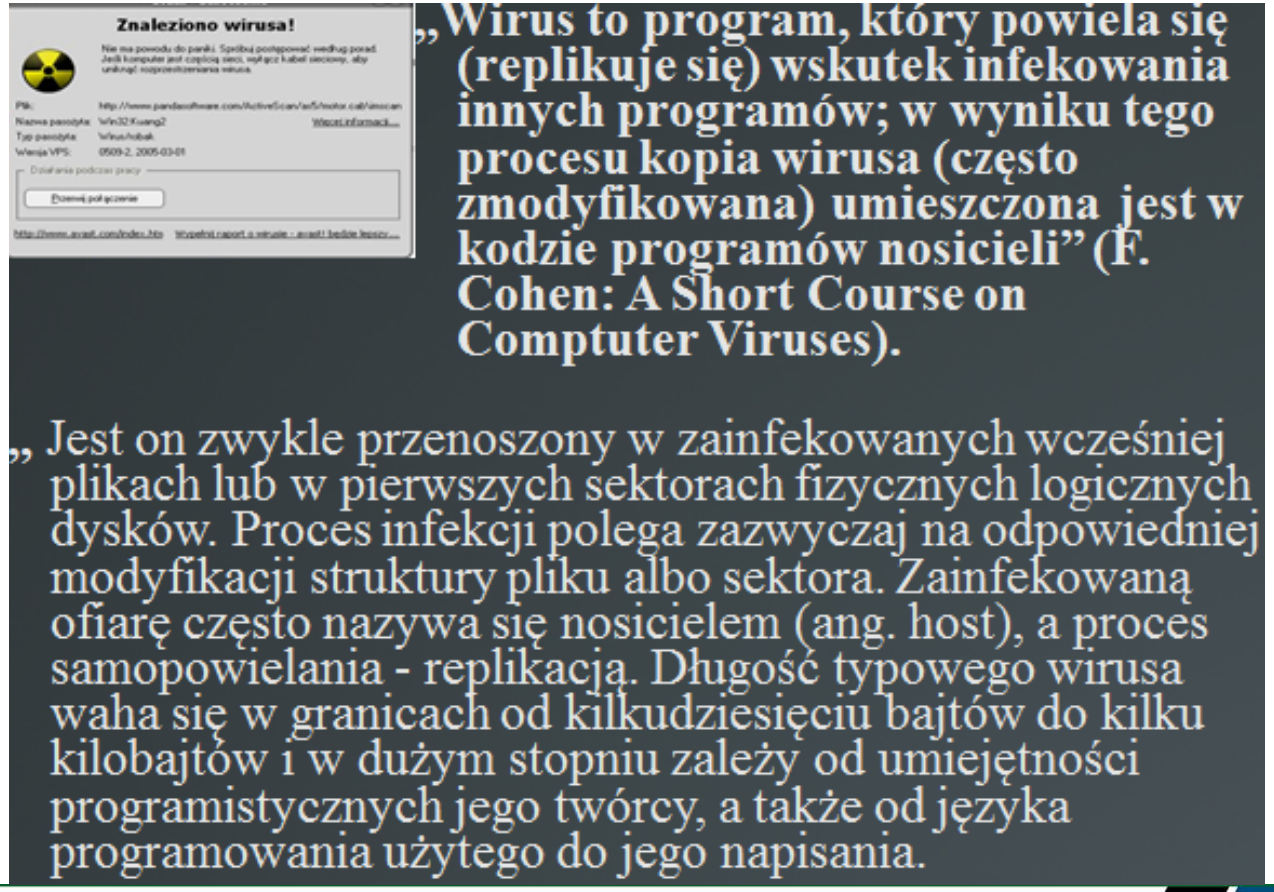
1. **Oprogramowanie szantażujące (ransomware)** - blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych (często poprzez techniki szyfrujące), a następnie żąda od ofiary okupu za przywrócenie stanu pierwotnego.
   - Obecnie znane są trzy różne rodzaje ransomware. "Najmilszy" z nich to "screen-locker", który blokuje użytkownikowi dostęp do urządzenia poprzez zablokowanie ekranu. Można się go pozbyć bez płacenia atakującemu, jeśli ofiara posiada wystarczającą wiedzę techniczną.
   - Kolejna wersja "crypto-ransomware" szyfruje lokalne pliki ofiary jak również pliki w chmurze. Następnie oferuje deszyfrator za uiszczeniem opłaty, przeważnie między $300-$900 dolarów. Ponieważ crypto-ransomware wykorzystuje ten sam typ szyfrowania co oprogramowanie chroniące transakcje bankowe lub wojskową komunikacje, zaszyfrowane pliki są praktycznie nie do odzyskania, bez opłacenia okupu. Rodzina oprogramowania crypto-ransomware jest odpowiedzialna za wyłudzenie ponad miliarda dolarów co roku od ofiar.
   - Ostatnio pojawił się trzeci rodzaj ransomware tzw.: "disk-encryptor" np. Petya. W odróżnieniu od crypto-ransomware disk-encryptor zaszyfrowuje cały dysk ofiary i nie pozwala na uruchomienie się systemu operacyjnego.


1989
AIDS Trojan
first "locker" ransomware
MAY
Archiveus
first to use RSA encryption
2006
JUNE
GPCode
first in an evolution of the "gpcode" family
HydraCrypt
2008
GPCode.ak
evolution of original GPCode with added RSA encryption
2010
Winlock
"locker" trojan
GPCode.ax
stronger encryption and more difficult file recovery
Browlock
"locker" ransomware
2013
Cryptolocker
one of the most successful early ransomware variants
2014
Linkup
Cryptolocker 2.0
CryptoDefense
TorrentLocker
CryptoWall
one of, if not THE most prolific ransomware
Simplelocker
Android ransomware
Citron
ZeroLocker
Coinvault
Virlock
spreads via cloud storage and collaboration apps
2015
TeslaCrypt
targeted video game data
CryptoLocker 2015
BandarChor
CryptoVault 2015
Tox
Ransomware-as-a-Service
PClock
Troldesh
Threat Finder
LockerPin
Android ransomware
Encryptor RaaS
Ransomware-as-a-Service
CryptoApp
2016
Petya
Master Boot Record encryption
Locky
one of the most prevalent ransomware attacks
UmbreCrypt
Samas
HydraCrypt
Cerber
Vipasana
Hi Buddy
RAA
pure JavaSCript ransomware
Mischa
evolution of Petya. RaaS
Crysis
Dogspectus
drive-by-download Android ransomware
zCrypt
Crypt XXX 3.0
Jigsaw
Satana
Cerber 2.0
Ranscam
"leaker" ransomware, blackmailing victims
HDDCrypto
Popcorn Time
decrypt files by infecting your friends
Cerber 3.0
Dharma
CryptoLuck
iRansom
Ransoc
"leaker" ransomware, blackmailing victims
2017
Satan
Ransomware-as-a-Service
SamSam 2017
Evil-JS
FirstRansomware
Sage 2.0
N-Splitter
variant of Hidden Tear Open-Source ransomware
Spora
Wcry
the parent of the infamous WannaCry 2.0 ransomware
Ranion (RaaS)
WannaCry
the first "Ransomworm
Goldeneye
potential nation-state attack, also called NotPetya or Petya 2.0
GX40
Cerberos
Cybercrooks
GX40 derivative
pyCL
Python-based ransomware
Cerber 6.0
Locky 2017
Fatboy
RaaS
ThunderCrypt
spreads using XSS
Gomasom
Chimera

WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

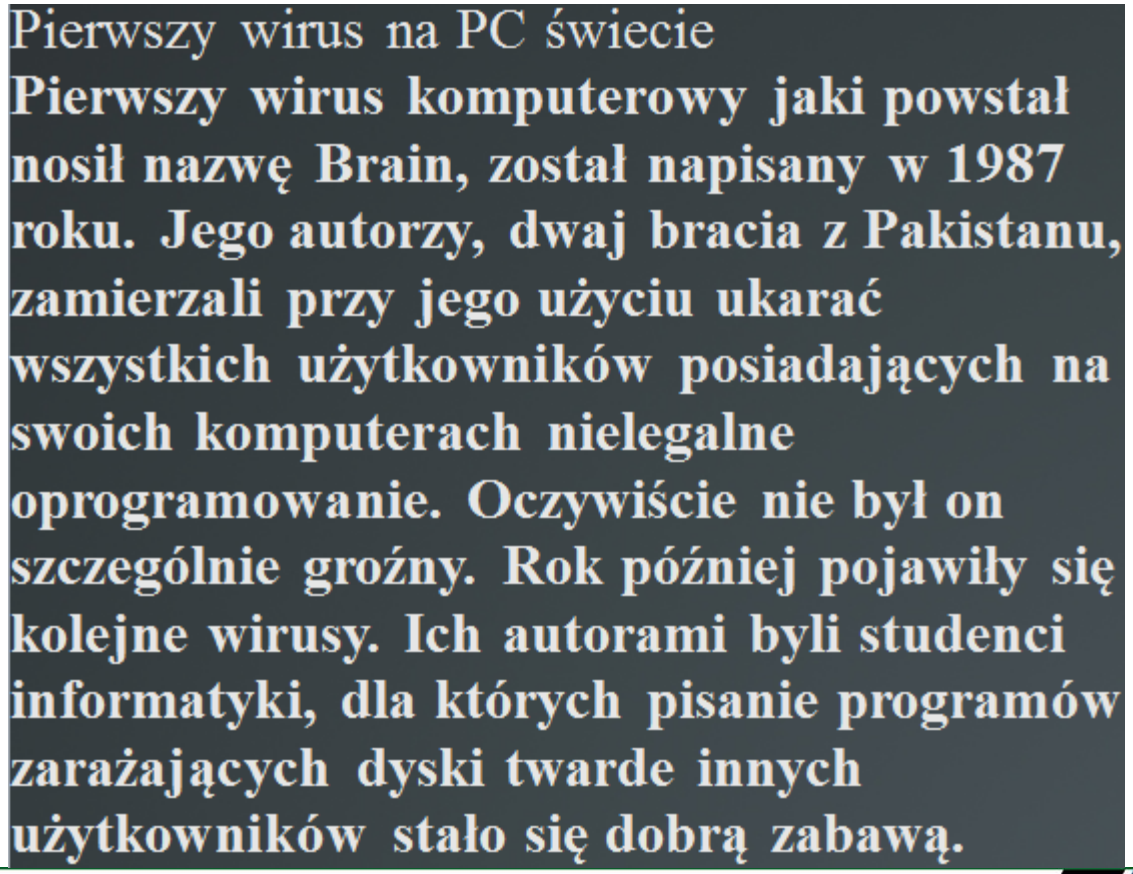
OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).



WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).



WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).

Generatory wirusów

Istnieje wiele programów umożliwiających stworzenie własnego wirusa, nawet bez znajomości systemu czy mechanizmów wykorzystywanych przez wirusy. Można je bez problemu znaleźć w Internecie. Korzystają one z gotowych modułów w asemblerze i umożliwiają stworzenie wirusa o zadanych parametrach wybieranych zwykle przy pomocy przyjaznego użytkownikowi menu. Można w nim określić zakres infekowanych obiektów oraz rodzaj efektów które ma on wywoływać. Oprócz kodu wynikowego wirusa, generatory tworzą także źródla w asemblerze, co umożliwia zainteresowanemu pisaniem wirusów użytkownikowi dokształcenie się w tej dziedzinie. Najbardziej znane generatory wirusów to: - IVP - Instant Virus Production Kit - VCL - Virus Construction Laboratory - PS-MPC - Phalcon-Skism Mass Produced Code Generator - G2 - G Squared - NRLG - Nuke Randomic Life Generator

WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).

Rodzaje wirusów komputerowych

Wirusy infekujące pliki – dołączają się do programów wykonywalnych.

Wirusy w boot sektorach

Wirusy typu Stealth – ukrywają się zacierając ślady swojej obecności w sektorze ładującym lub pamięci RAM

Wirusy polimorficzne – w czasie replikacji zmieniają własny kod

Makro wirusy (1995) – po otwarciu zainfekowanego dokumentu instalują się jako Makro, od tej chwili każdy otwierany dokument jest atakowany.

WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).

ROBAK – program który do swojego działania nie potrzebuje innych programów, zużywa na swoje potrzeby zasoby zainfekowanego komputera, w którym aktualnie rezyduje oraz potrafi przenosić się na inne komputery

Sober. Również znany jako: **Worm.Sober.I**
Niszczący:dyski–**nie,** pliki:**nie**
Efekty: wizualne:**nie,** dźwiękowe:**nie**

Działanie polega na rozsyłaniu własnych kopii za o pomocą poczty elektronicznej.

Pojawia się w komputerze ofiary w postaci załącznika do listu elektronicznego np.. o następujących parametrach:

Od: [fałszywy adres] **Temat:** hi

Załącznik z rozszerzeniem pif, zip, scr, bat, com

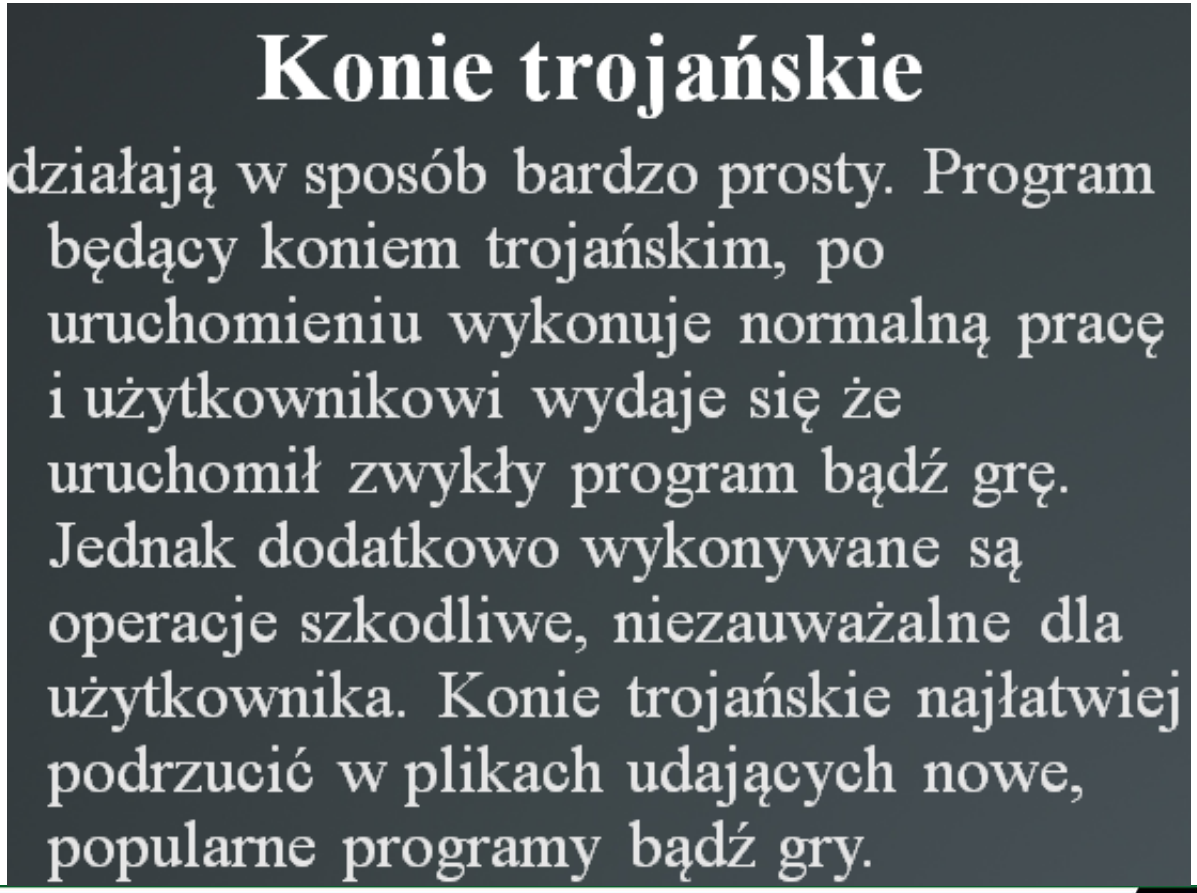
Po uruchomieniu przez użytkownika pliku załącznika robak tworzy na dysku swoją kopię w pliku o losowej nazwie oraz modyfikuje tak rejestr by jego kopia była automatycznie uruchamiana przy każdym starcie systemu Windows.

Następnie robak rozsyła własne kopie za pomocą poczty elektronicznej na wszystkie adresy odnalezione na zainfekowanym komputerze, wykorzystując do tego własny silnik SMTP.

WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).



WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).

Kon trojanski (trojan)

Udaje pożyteczny program, aby po zainstalowaniu uruchomić dodatkowe funkcje powodujące wykonanie określonych zadań - np. umożliwienie łączności z serwerem swego twórcy, lub przechwycenie haseł czy znaków wprowadzanych z klawiatury. Często również koń trojański udaje pożyteczną aplikacje internetowa, która do uzyskania pełni funkcjonalności wymaga od użytkownika podania określonych danych, które są wysyłane do hackera.

WYDZIAŁ ZARZĄDZANIA

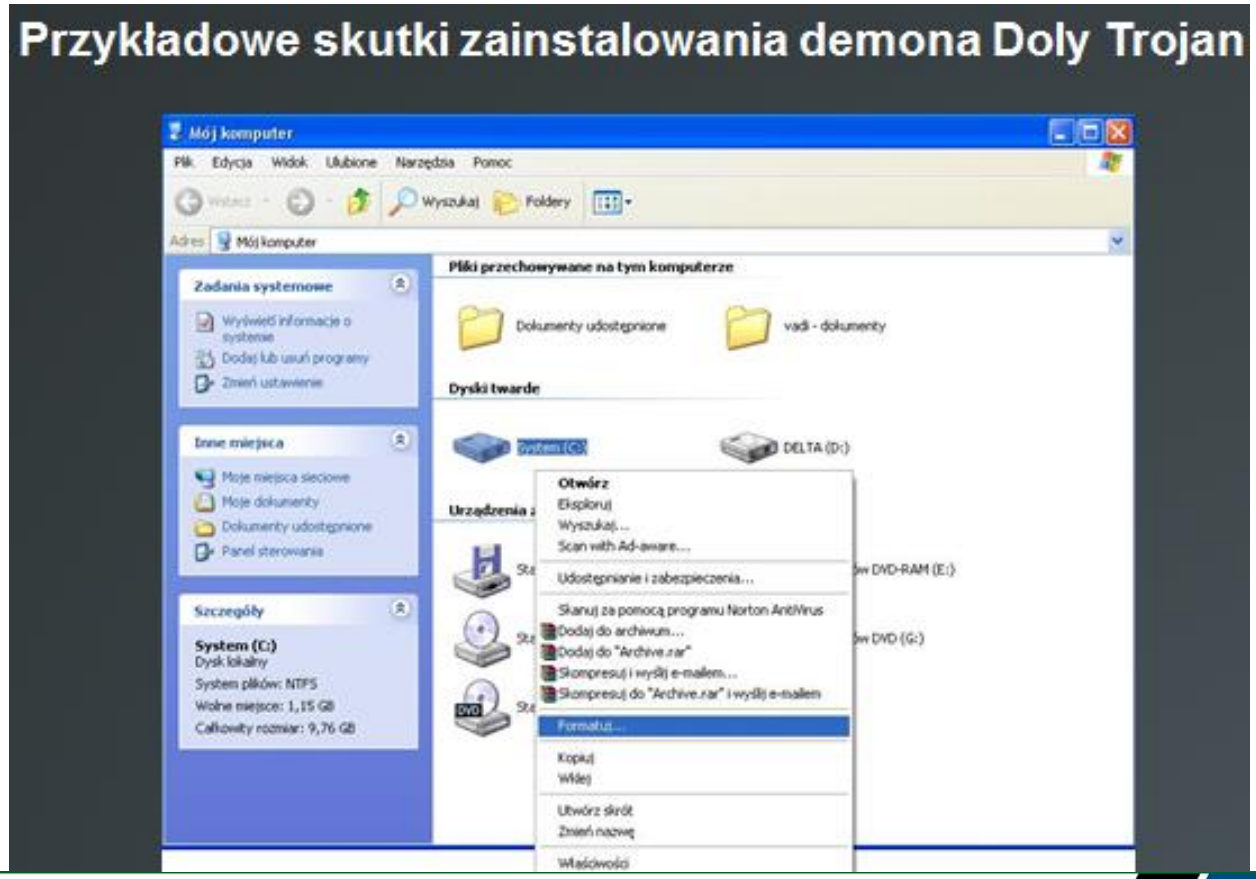
Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).

WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).



WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).

KOŃ TROJAŃSKI-nie ujawniona procedura zapisana w programie.

Trojan o nazwie LUZAK. Działanie programu polega na sterowaniu komputerem i oprogramowaniem osoby zaatakowanej przez osobę atakującą komputer.

Program zawiera dwa pliki- jeden do instalacji programu, drugi pozwala na sterowanie komputerem drugiej osoby.

Program wystarczy zainstalować na komputerze potencjalnej ofiary, aby móc stertować jego zasobami. Można tego dokonać wysyłając mailem plik, który po kliknięciu na niego automatycznie instaluje się na komputerze potencjalnej ofiary, która jest nieświadoma swojego czynu.

Drugi plik jest w komputerze atakującego. Po uruchomieniu programu pojawia się następujące okno:

WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).

WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).

Szkodliwość koni trojańskich polega na tym, ze otwierają własny port, czyli rodzaj logicznych wrot do systemu, i nasłuchują poleceń hackera. Tym samym umożliwia to hackerowi wykonywanie zdalnych poleceń na zainfekowanym komputerze.

WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).

Bomby logiczne

różnią się od konia trojańskiego tym, że ukryte operacje nie są wykonywane od razu po ich uruchomieniu, lecz dopiero w odpowiednim czasie. Może to być zajście określonego zdarzenia w systemie bądź wielokrotne uruchomienie danego programu. Często uruchomienie ukrytych operacji następuje automatycznie po upłynięciu określonej liczby dni od momentu uruchomienia bomby.

WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).

WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).

Maskowane zazwyczaj pod postacią żartów, ukryte w programach do pobrania lub załącznikach e-mail, programy „tylnego wejścia" stwarzają dla większości stacji ogromne zagrożenie.

Systemy pracujące w domu, biurze czy centrum przetwarzania danych w prosty sposób mogą zostać zarażone koniem trojańskim, który umożliwi swobodną wymianę plików, sterownie aplikacjami i procesami systemowymi, zarządzanie pulpitem, przeglądanie elektronicznej skrzynki pocztowej, a nawet kontrolę nad tym, co jest wyświetlane na monitorze.

WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).

ROOTKIT – „pojemnik", dostosowany do systemu operacyjnego ofiary, umożliwiający ukrycie modułu złośliwego

Ukrycie odbywa się najczęściej poprzez przejęcie wybranych funkcji systemu operacyjnego

Dostępnych jest kilka narzędzi do automatycznego wykrywania: Rootkit Reavealer, GMER

Przykłady rootkitów: HackDefender, Rootkit Sony, SVKP.SYS (?)

WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).

Rootkity

Rootkit infekuje jądro i usuwa ukrywane programy z listy procesów oraz plików zwracanych do programów. Może on np. ukryć siebie oraz konia trojańskiego
przed administratorem oraz oprogramowaniem antywirusowym. Ukrywanie odbywa się najczęściej przez przejęcie wybranych funkcji systemu operacyjnego, służących np. listowaniu procesów lub plików w katalogu, a następnie "cenzurowaniu" zwracanych przez te funkcje wyników tak. by ukrywane przez rootkit nazwy nie znajdowały się na liście wynikowej.

WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).

Keylogger

Programy te działają na zasadzie przejęcia kontroli nad procedurami systemu operacyjnego (głównie Microsoft Windows) służącymi do obsługi klawiatury. Każde wciśnięcie klawisza jest odnotowywane w specjalnym pliku. Opcjonalnie informacje o wciśniętych klawiszach poszerzone są o dodatkowe informacje, jak nazwa aktywnego programu lub okna.

Keyloggery zawierają funkcje chroniące je przed wykryciem przez niedoświadczonego użytkownika komputera, a plik w którym zapisywane są dane ukryty jest np. w katalogach systemowych. Dzięki temu długo mogą rezydować niewykryte na komputerze ofiary i przyczyniać się do ujawnienia wszystkich wykorzystywanych haseł. Większość keyloggerów ma specjalnie stworzoną funkcję, która pozwala na wysłanie pliku z hasłami na wyznaczony adres pocztowy.

Keyloggery sprzętowe mają postać małych przejściówek służących do wpięcia do portu klawiatury komputera. Klawiaturę wpina się następnie do gniazda w przejściówce. która potem zapisuje wszystkie wciskane klawisze we wbudowanej pamięci lub wysyła je drogą radiową. W przypadku keyloggerów pierwszego typu konieczny jest fizyczny dostęp do urządzenia dla odczytania danych. Można również spotkać keylogger sprzętowy wbudowany w klawiaturę lub przewód łączący klawiaturę z komputerem.

WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).

Moduły szpiegujące - to oprogramowanie potajemnie instalowane w systemie, które może monitorować i rejestrować różne aspekty działania systemu, a następnie przesyłać te informacje napastnikom

Najczęściej taki program (*Spyware)* monitoruje zachowania użytkowników korzystających z komputera: jak długo używają komputera każdego dnia, jakie uruchamiają programy, ile otrzymują listów elektronicznych i jakie strony WWW odwiedzili.

Do kategorii modułów szpiegujących należą też programy wyświetlające w czasie pracy pola reklamowe (adware). Aby reklama była skuteczniejsza, często analizują one dane zebrane w czasie pracy – narodowość użytkownika czy rodzaj odwiedzanych stron WWW – by personalizować wyświetlane ogłoszenia. Dane te muszą zostać wysłane do serwerów reklamodawców, by możliwe było pobranie stosownego zestawu reklam.

WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).

DIALER - Program przekierowujący zwykłe połączenie modemowe np.0202122 na nr.0-700 lub międzynarodowe.

Celem jest wyciągnięcie jak największej sumy pieniędzy poprzez realizowanie połączenia z Internetem za pomocą numerów z serii 0 700, za użycie których zapłacisz kilka złotych za minutę połączenia.

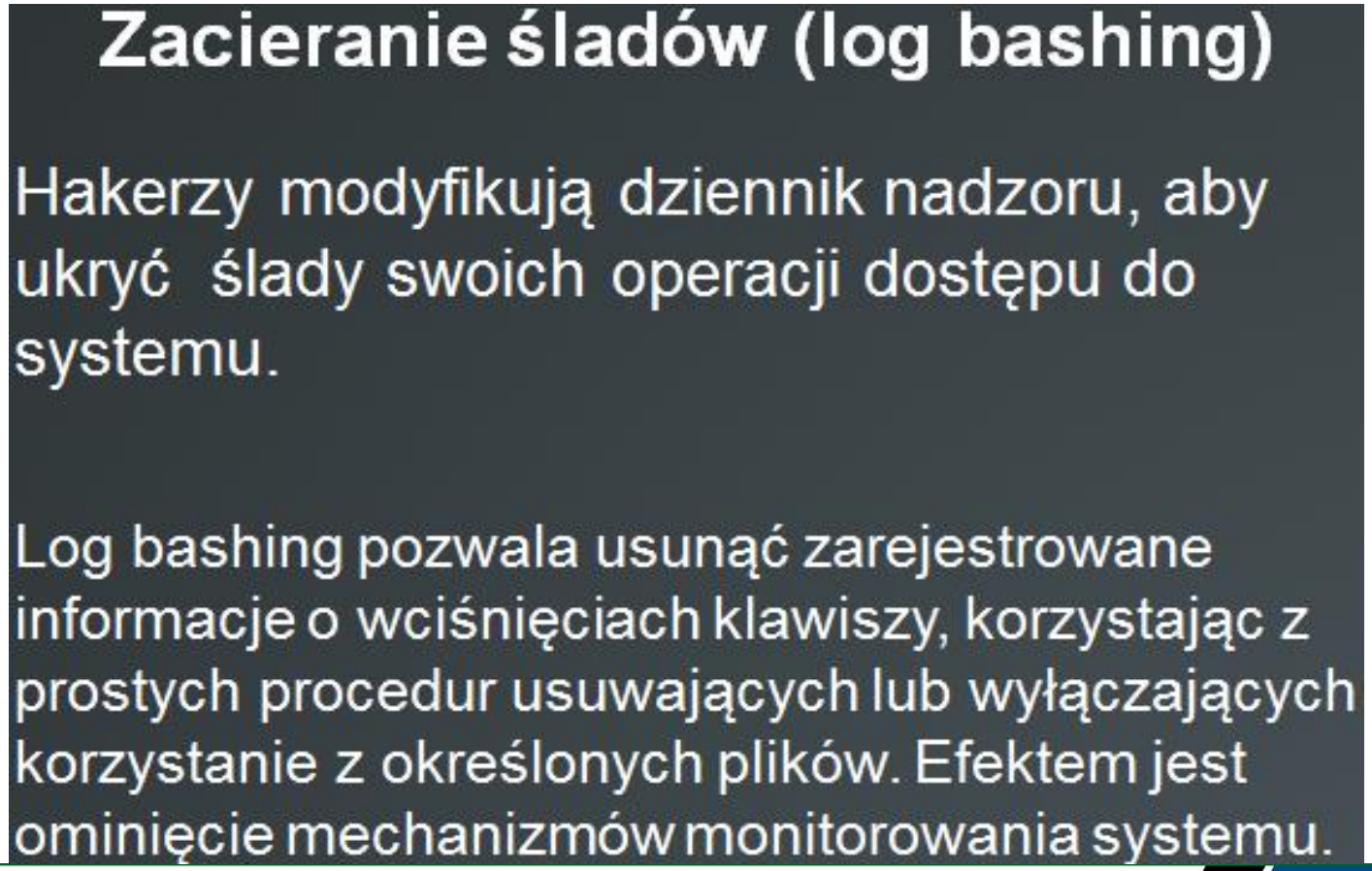
Niektóre z dialerów przypominają wirusy, instalują się podstępnie wykorzystując luki w zabezpieczeniach lub naiwność użytkownika klikającego OK. bez zrozumienia tekstu.

Innym dialerom bliżej jest do koni trojańskich: w zamian za ściągnięcie i zainstalowanie niewielkiego programu oferują dostęp do bezpłatnych archiwów oprogramowania lub stron pornograficznych.

WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).



WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).

Zacieranie śladów (log bashing)

Hakerzy modyfikują dziennik nadzoru, aby ukryć ślady swoich operacji dostępu do systemu.

Log bashing pozwala usunąć zarejestrowane informacje o wciśnięciach klawiszy, korzystając z prostych procedur usuwających lub wyłączających korzystanie z określonych plików. Efektem jest ominięcie mechanizmów monitorowania systemu.

WYDZIAŁ ZARZĄDZANIA

Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).

Zacieranie śladów aktywności online

Osoby skrycie włamujące się do innych komputerów usuwają zazwyczaj pliki, pozostawiane przez przeglądarkę (tymczasowe pliki internetowe, cookies, historia, plik wymiany).

Dla pełnego bezpieczeństwa hakerzy modyfikują również historię odwiedzonych stron w kluczu *Rejestru.*

Innym, ułatwiającym zachowanie prywatności przeglądania Internetu, sposobem jest całkowite wyłączenie bufora, listy historii i plików cookie.

WYDZIAŁ ZARZĄDZANIA

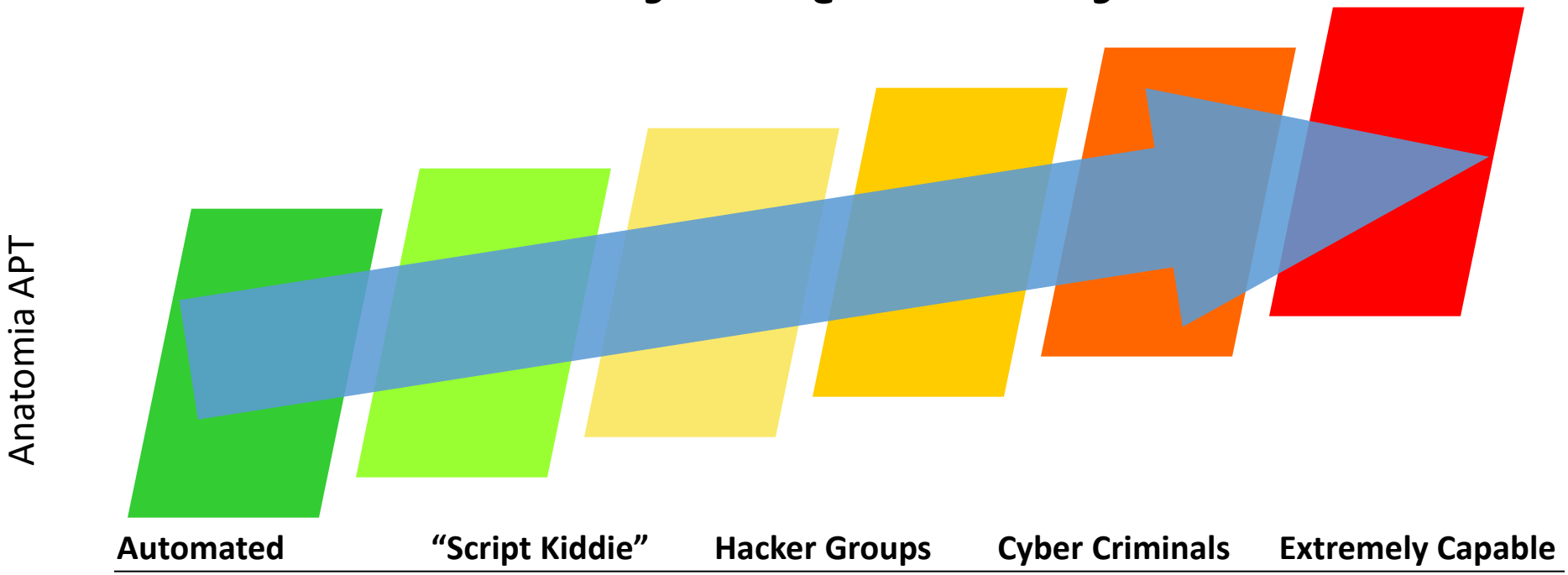
Klasyfikacja oprogramowania złośliwego

OPROGRAMOWANIE ZŁOŚLIWE (MALWARE)- rozległe i różnorodne oprogramowanie komputerowe zmniejszające bezpieczeństwo informacyjne użytkownika, zainstalowane w sposób jawny (za zgodą użytkownika) bądź też w sposób niejawny (bez uprzedniej akceptacji czy przyzwolenia).

Exploit:

Najbardziej znana metoda i zarazem najłatwiejszą. Exploit jest to program który wykorzystuje luki admina lub systemu i przydziela nam prawa roota. W większości przypadków aby uruchomić exploita w danym systemie potrzebujemy konto na tym systemie, ale są tez exploity zdalne (remote), do których uruchomienia nie potrzeba konta w atakowanym systemie !

Metodologia ataków hakerskich rozwija się. Co to jest APT?



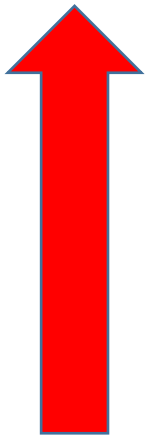
Ataki typu APT (z ang. Advanced Persistent Threat) są złożonymi, długotrwałymii wielostopniowymi działaniami kierowanymi przeciwko konkretnym osobom, organizacjom lub firmom. Nazywane są również atakami ukierunkowanymi. Stanowią zagrożenie, które wykorzystuje bardzo wyrafinowane metody i zaawansowane technologie do przeprowadzania sieciowych ataków na konkretne cele Za wzorcowy i najpopularniejszy przykład ataku typu APT uznaje się atak o nazwie Stuxnet.

Atak ATP jest innowacją, która wprowadza nową rzeczywistość w systemie informacyjnym ofiary

Wyjaśniamy nazwę: ADVANCED PERSISTENT THREAT?

Anatomia APT

Pojęcie *Advanced Persistent Threat* (APT; zaawansowane trwałe zagrożenie) zostało utworzone przez analityków z amerykańskich Sił Powietrznych w 2006 roku. Opisuje ono trzy aspekty ataków związane z profilem, zamiarami i strukturą grupy napastników:



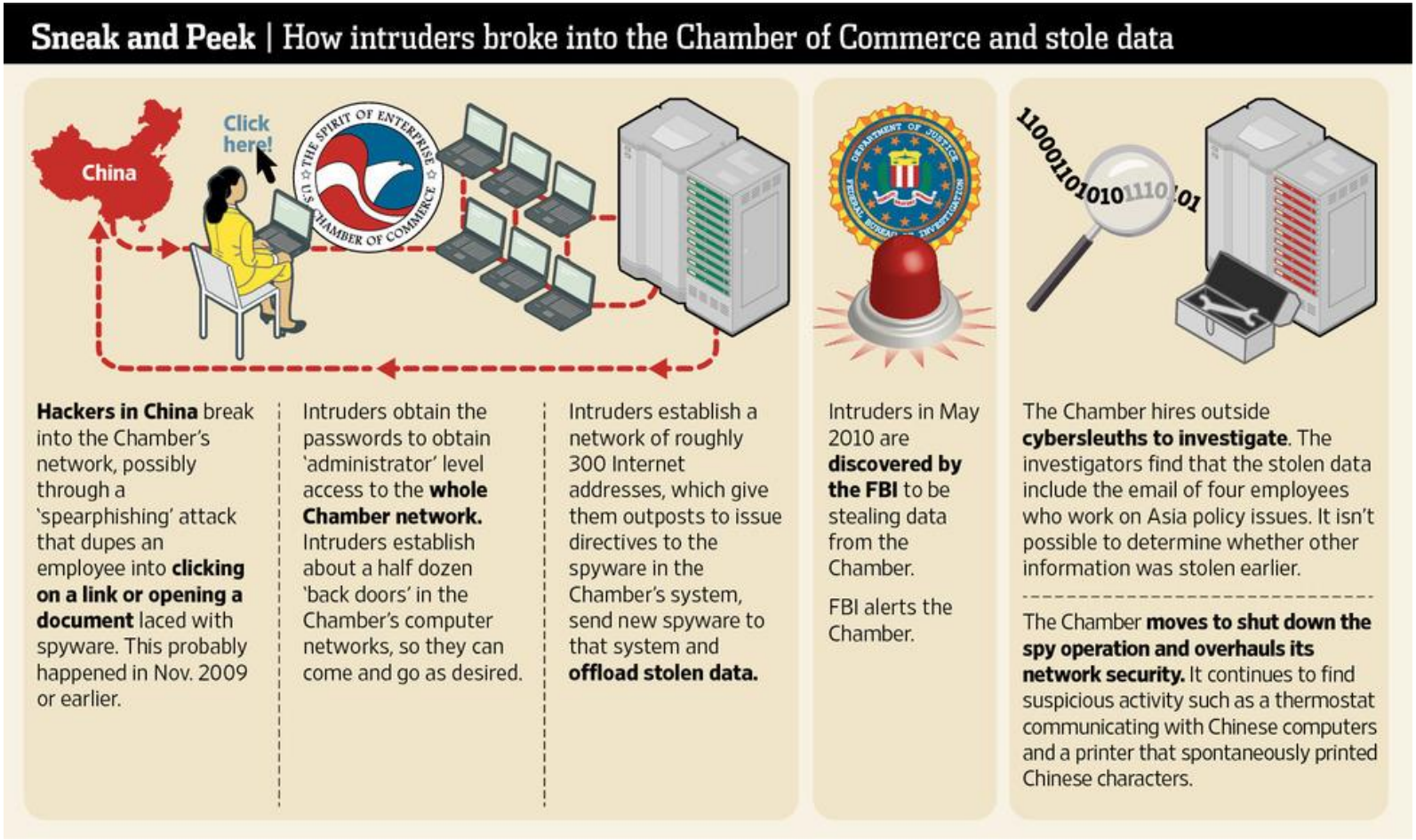
Zaawansowane. Napastnik jest biegły w metodach cyberataków i technikach administracyjnych. Potrafi rozwijać niestandardowe eksploity i narzędzia.

Trwałe. Napastnik ma długoterminowe cele i stara się je osiągnąć, unikając przy tym wykrycia.

Zagrożenie. Napastnicy są zorganizowani, mają duże środki, motywację
i możliwości.

Prosty przykład

The Wall Street Journal reported on an intrusion into the Chamber of Commerce that serves as a good example.



Proces APT (1)

Anatomia APT

W literaturze w procesie cyberataku wyróżnia się różne fazy np.:

1. Air Force Institute of Technology (5): rozpoznanie (rekonesans), skanowanie, dostęp do systemu, instalacja kodu złośliwego, eksploatacja kodu złośliwego
2. Lockheed Martin (7): rozpoznanie, uzbrojenie, dostarczenie, eksploracja, instalacja, kierowanie i dowodzenie, akcja, tzn. atak celu.
3. Hahn, Thomas, Lozano, Cardenas (6): rozpoznanie, uzbrojenie, dostarczenie, eksploracja, kierowanie i dowodzenie, osiągnięcie celu.

Hofman syntezuje te propozycje omawiając 7-faz:

Identyfikacja i definicja (S_1)	Identyfikacja i określenie potrzeb agresora/atakującego np.: „biznesowych", politycznych itp. Faza ta powinna wystąpić nawet, gdyby był to tylko pomysł przestępcy na przejęcie np. konta ofiary na twitterze. Na pewno występuje wówczas, gdy np. grupa przestępcza lub jakaś organizacja planuje swoje działania, wynika z przyjętej szerszej strategii państwa działań w cyberprzestrzeni itp.
Rozpoznanie (*reconnaissance*) (S_2)	Identyfikacja i dobór celów ataków (technicznych) poprzez rozpoznanie docelowego środowiska, np. skanowanie portów TCP, indeksowanie witryn internetowych, materiałów konferencyjnych, list adresów e-maili, sieci społecznościowych, informacji na temat stosowanych (specyficznych) technologii, socjotechniczne wyłudzenie informacji i danych itp.

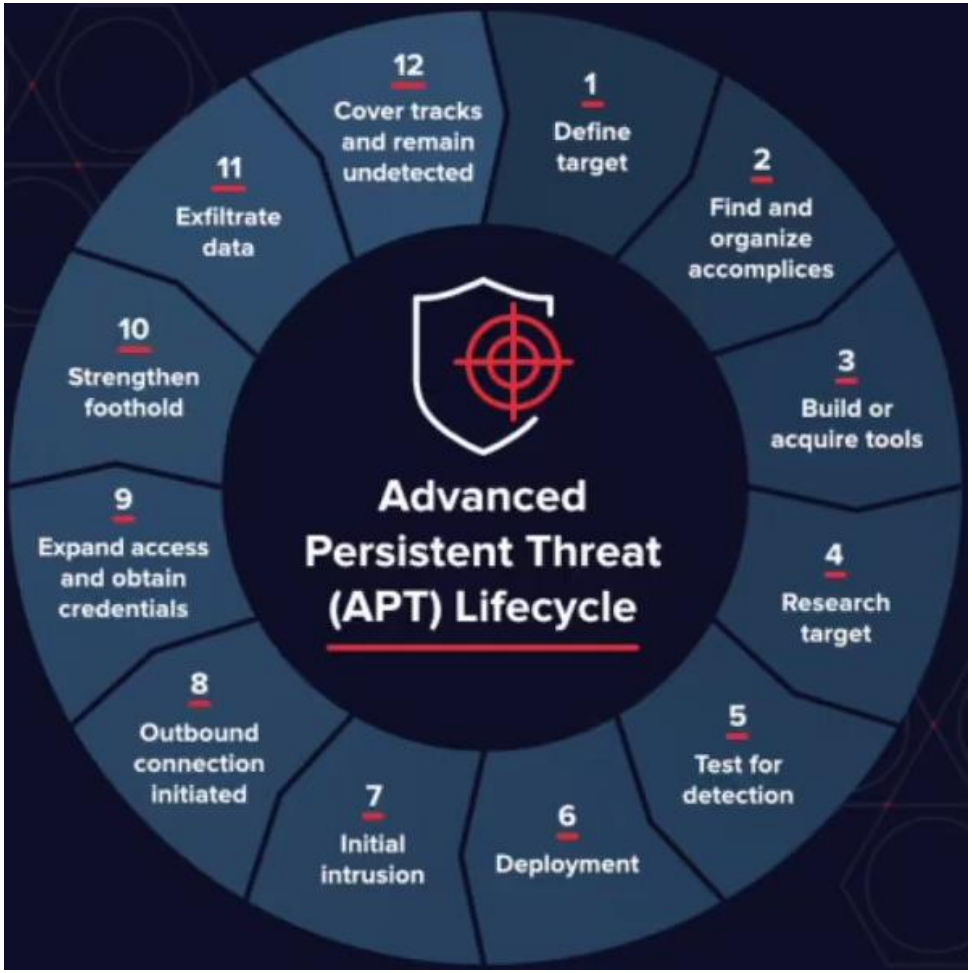
Proces APT (2)

Uzbrojenie (*weaponization*) (S_3)	Przygotowanie cyberbroni, tzn. specjalnego oprogramowania, np. zintegrowanie koni trojańskich z innym złośliwym kodem (*exploit*) w celu stworzenia możliwego do dostarczenia ładunku za pomocą automatycznego narzędzia (*weaponizer*). W przypadku, gdy nie zachodzi potrzeba budowy lub skonfigurowania pakietu oprogramowania, etap może zostać pominięty
Dostarczenie (*delivery*) (S_4)	Skopiowanie cyberbroni do docelowego środowiska, np. wykorzystanie najbardziej rozpowszechnionych sposobów dostawy (np. w ramach ataków APT), którymi przykładowo są: zainfekowane załączniki do e-maili, spreparowane lub złośliwie zmodyfikowane oprogramowanie strony internetowej (np. aplety, linki), wstrzyknięcie kodu SQL, zainfekowane nośniki danych podłączane do portów USB

Proces APT (3)

Uruchomienie i kontrola kodu złośliwego (*cyber execution*) (S_5)	Uruchomienie kodu złośliwego (po dostarczeniu cyberbroni do środowiska docelowego), np. w wyniku wykorzystania podatności/luki programowej w aplikacji lub systemie operacyjnym lub zmanipulowania użytkownika systemu docelowego. Instalacja dodatkowego kodu złośliwego, np. koni trojańskich (*Remote Access Trojan* – RAT), umieszczenie tylnych furtek (*backdoor*) w systemie docelowym w celu zestawienia stałego kanału komunikacji zainfekowanego środowiska wewnętrznego ofiary z centrum (zewnętrznym środowiskiem) dowodzenia i sterowania oprogramowaniem złośliwym. Kontrola i sterowanie zainfekowanego środowiska, np. eskalacja lub uzyskanie dodatkowych uprawnień, systemowych, doinstalowanie pozostałego lub dodatkowego kodu złośliwego (np. *backdoor/trojan/rootkit*), modyfikacja system plików, przeglądanie lub modyfikacja systemowych baz danych
Realizacja celów (Achieve Objectives) (S_6)	Podjęcie działań nakierowanych na osiągnięcie pierwotnych celów, np. skopiowanie danych, naruszanie integralności i/lub dostępności danych, uzyskanie dostępu do poczty elektronicznej ofiary w celu wykorzystania jej do głębszej penetracji zakatowanej infrastruktury lub wykorzystanie poczty elektronicznej do dalszego rozprzestrzenienia prowadzonego ataku. W tej fazie nie wyklucza się fizycznej destrukcji infrastruktury organizacji
Zakończenie ataku i zatarcie śladów (S_7)	Zakończenie ataku, może być połączone z usunięciem lub zamaskowaniem śladów ataku i aktywności kodu złośliwego. Etap opcjonalny, zależny od celów i stopnia zaawansowania technologicznego agresora

Cykl życia



Cykl życia APT

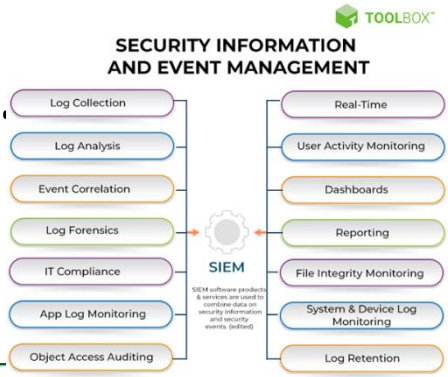
1. Zdefiniuj cel
2. Znajdź i zorganizuj wspólników
3. Buduj lub zdobywaj narzędzia
4. Zbadaj cel
5. Test na wykrywanie
6. Wdrożenie
7. Wstępne wtargnięcie
8. Zainicjowano połączenie wychodzące
9. Rozszerz dostęp i uzyskaj dane uwierzytelniające
10. Wzmocnij przyczółek
11. Eksfiltruj dane
12. Zakryj ślady i pozostań niewykryty

Ochrona przed APT- ZASADY

MON apeluje. Nie publikuj materiałów wojskowych w social mediach

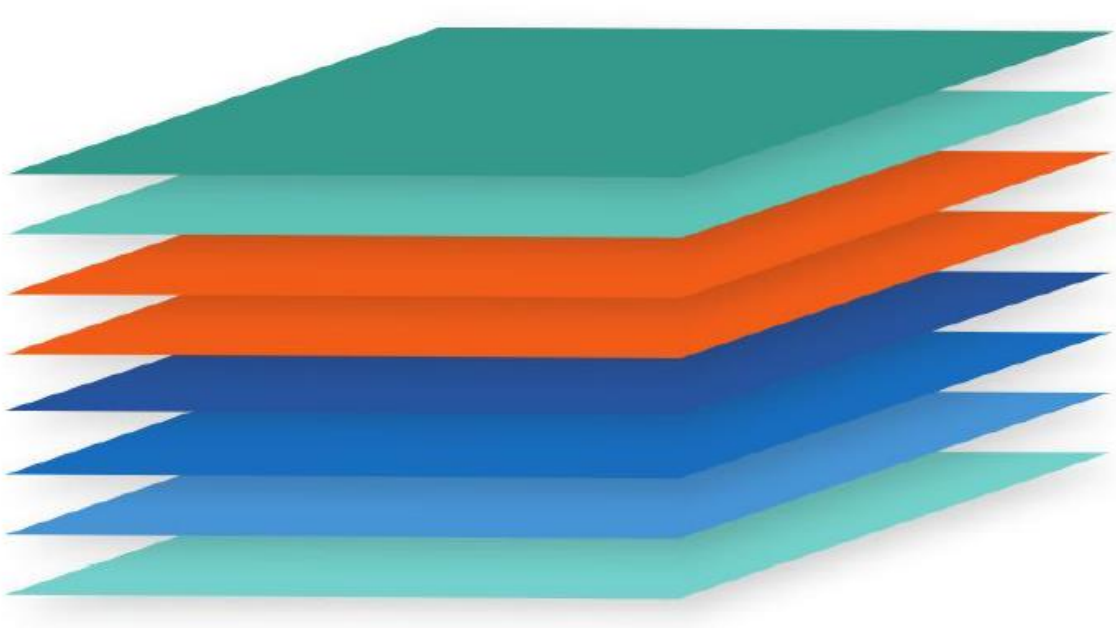
Anatomia APT

1. Zidentyfikuj krytyczne informacje dostępne publicznie i ogranicz je / usuń.
2. Monitoruj infrastrukturę sieci z dostępem do Internetu.
3. Edukacja użytkowników jest najważniejsza.
4. Wykorzystaj istniejącą technologię.
5. Użyj rozwiązania do zarządzania poprawkami dla przedsiębiorstw.
6. Zastosuj technologię anty-zero-day.
7. Zatrudnij informatykę śledczą i analizę włamań (reagowanie na incydenty).
8. Zrozum zagrożenie, korzystaj z raportów analizy złośliwego oprogramowania.
9. Ciągła analiza powinna zasilać twoje systemy obronne.
10. Wdrażaj i przeprowadzaj audyty bezpieczeństwa sieci.
11. Stosuj systemy wykrywania anomalii sieciowych.



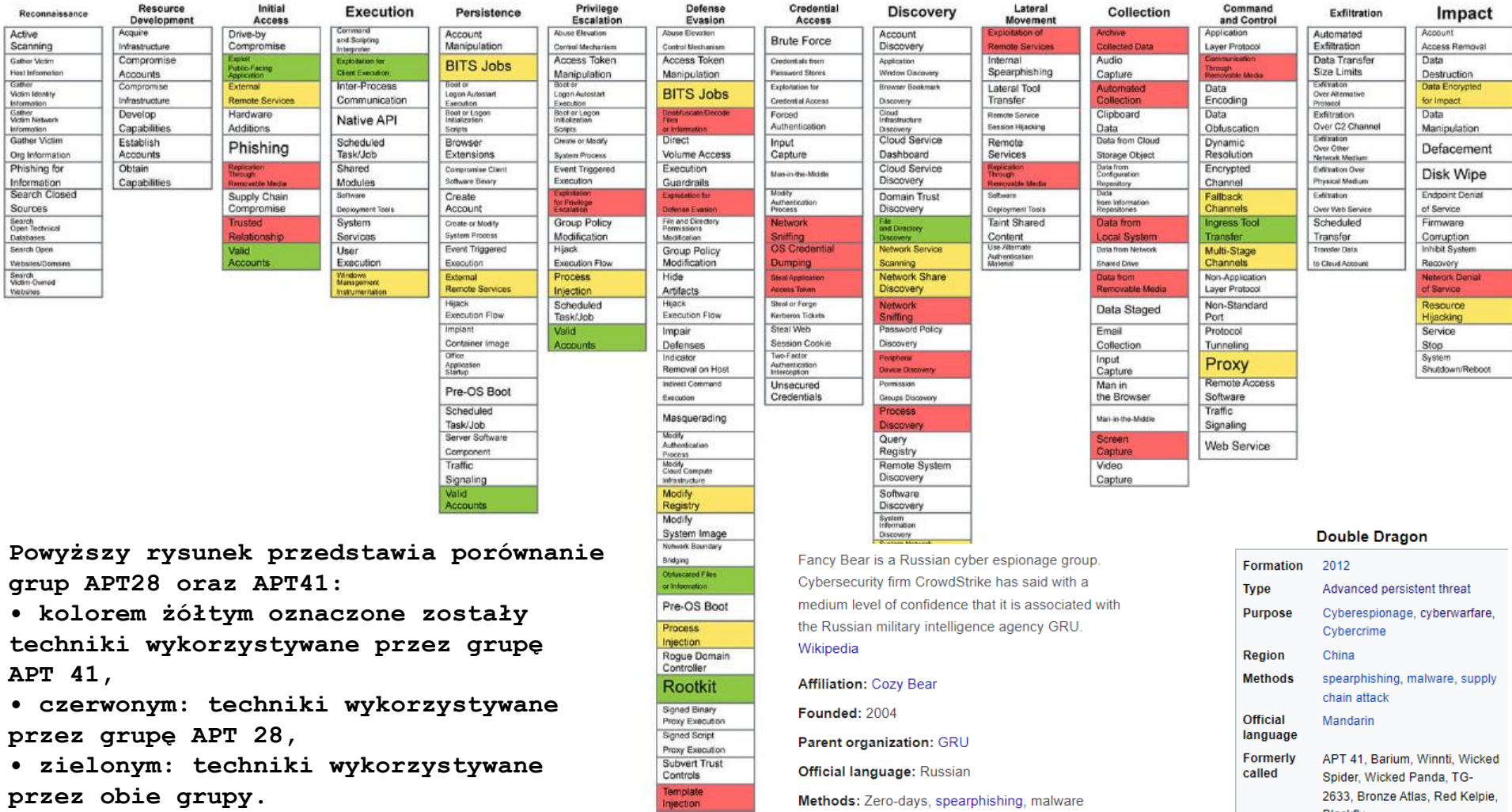
Ochrona przed APT - WARSTWY

WYDZIAŁ ZARZĄDZANIA



Firewall
Antivirus
Intrusion Prevention Systems (IPS)
Web Application Firewall
Web Protection
Email Protection
Botnet/Command and Control Detection
Sandboxing

Ochrona przed APT – DEPTANIE PO PIĘTACH



Powyższy rysunek przedstawia porównanie grup APT28 oraz APT41:

- **kolorem żółtym oznaczone zostały techniki wykorzystywane przez grupę APT 41,**
- **czerwonym: techniki wykorzystywane przez grupę APT 28,**
- **zielonym: techniki wykorzystywane przez obie grupy.**

Fancy Bear is a Russian cyber espionage group. Cybersecurity firm CrowdStrike has said with a medium level of confidence that it is associated with the Russian military intelligence agency GRU. Wikipedia

Affiliation: Cozy Bear

Founded: 2004

Parent organization: GRU

Official language: Russian

Methods: Zero-days, spearphishing, malware

Purpose: Cyberespionage, cyberwarfare

Double Dragon

Formation	2012
Type	Advanced persistent threat
Purpose	Cyberespionage, cyberwarfare, Cybercrime
Region	China
Methods	spearphishing, malware, supply chain attack
Official language	Mandarin
Formerly called	APT 41, Barium, Winnti, Wicked Spider, Wicked Panda, TG-2633, Bronze Atlas, Red Kelpie, Blackfly

Equation Group – grupa hakerska, sklasyfikowana jako APT, podejrzana o powiązania z Agencją Bezpieczeństwa Narodowego (NSA).
Kaspersky Lab opisuje ich jako jedną z najbardziej wyrafinowanych na świecie grup zajmujących się cyberatakami i "najbardziej zaawansowaną (...) jaką widzieliśmy".
Grupa działa razem z twórcami robaka Stuxnet i Flame, którzy wydają się być jej podporządkowani.
Większość jej celów znajdowała
się w Iranie, Rosji, Pakistanie, Afganistanie, Indiach, Syrii i Mali.
Nazwa Equation Group została nadana ze względu na szczególne upodobanie grupy do metod silnego szyfrowania.
Do 2015 roku Kaspersky udokumentował 500 infekcji szkodliwym oprogramowaniem grupy w co najmniej 42 krajach, uznając, że rzeczywista liczba może dochodzić do dziesiątek tysięcy.
W 2017 roku WikiLeaks opublikowała dyskusję przeprowadzoną w CIA odnośnie do możliwości zidentyfikowania grupy. Jeden z komentatorów napisał, że "Equation Group, jak określono ją w raporcie, nie odnosi się do konkretnej grupy, a raczej do zestawu narzędzi„
W badaniach Kaspersky'ego, przeprowadzonych nad grupą w 2015 roku, że jej oprogramowanie, "Grayfish", wykazywało podobieństwa do wcześniej wykrytego "Gaussa" znanego z innych serii ataków; ponadto, że Equation Group wykorzystała dwa ataki "zero-day" użyte później w "Stuxnet"

- APT28 (ang. Advanced Persistent Threat 28), STRONTIUM, Sofacy lub Fancy Bear, to nazwy nadawane przez analityków dla określenia nieznanych sprawców powiązanych z szeregiem głośnych włamań i ataków komputerowych.
- Specjaliści od bezpieczeństwa teleinformatycznego z takich firm jak Microsoft, CrowdStrike, Kaspersky Lab, FireEye i ThreatConnect określają ze stopniem pewności od średniego do wysokiego, że jest to rosyjskojęzyczna instytucja państwowa, prawdopodobnie część GRU – wywiadu wojskowego Federacji Rosyjskiej.
- Grupa ta została powiązana z włamaniami lub próbami włamań do systemów parlamentu Niemiec, Białego Domu, Komisji Europejskiej, Banku Światowego, NATO, amerykańskiej Partii Demokratycznej i innych instytucji, m.in. na Ukrainie, w Turcji, oraz w Gruzji w czasie konfliktów tych krajów z Rosją. Część incydentów dotyczyła też Polski. Celem działania APT28 wydaje się być prowadzenie ataków teleinformatycznych zgodnych z zadaniami politycznymi GRU.
- Grupa APT28 zdradza dysponowanie dużymi zasobami i możliwościami, przykładowo, w ciągu zaledwie czterech miesięcy w 2016 r. wykorzystała sześć nowych, nieznanych z innych źródeł exploitów typu zero-day na zamknięte oprogramowanie. Narzędzia jakimi posługuje się organizacja są złożone i programowane w metodycznym i profesjonalnym środowisku, w godzinach roboczych odpowiadających moskiewskiej strefie czasowej. Grupa korzysta też z VPN, płatności przy pomocy bitcoinów, oraz fałszywych tożsamości, takich jak Guccifer 2.0 lub Anonymous Poland w celu ukrycia swojego prawdziwego pochodzenia.

- Lazarus Group (znana również pod innymi nazwami, takimi jak Guardians of Peace czy Whois Team) to grupa cyberprzestępcza składająca się z nieznanej liczby osób, prowadzona przez rząd Korei Północnej. Chociaż niewiele wiadomo o Grupie Lazarus, badacze przypisali jej wiele cyberataków w latach 2010-2021. Pierwotnie grupa przestępcza, obecnie została określona jako APT ze względu na zamierzony charakter, zagrożenie i szeroki wachlarz metod wykorzystywanych podczas prowadzenia operacji. Nazwy nadane przez organizacje cyberbezpieczeństwa obejmują HIDDEN COBRA (używane przez Wspólnotę Wywiadowczą Stanów Zjednoczonych w odniesieniu do złośliwej aktywności cybernetycznej rządu północnokoreańskiego w ogóle) i Zinc (przez Microsoft).
- Grupa Lazarus ma silne powiązania z Koreą Północną.[9][10] Federalne Biuro Śledcze Stanów Zjednoczonych twierdzi, że Grupa Lazarus jest północnokoreańską "sponsorowaną przez państwo organizacją hakerską".
- Według północnokoreańskiego defetysty Kim Kuksonga, jednostka jest wewnętrznie znana w Korei Północnej jako 414 Liaison Office.
- Korea Północna czerpie korzyści z prowadzenia operacji cybernetycznych, ponieważ może przedstawić asymetryczne zagrożenie przy pomocy niewielkiej grupy operatorów, zwłaszcza dla Korei Południowej.

Operacje prowadzone przez chińskiego państwowego aktora zagrożeń APT18 są wspierane przez Marynarkę Wojenną Armii Ludowo-Wyzwoleńczej (PLA Navy) i są aktywne na całym świecie od 2009 roku.
APT18 działa od lat i celuje w sektory zdrowia, telekomunikacji, obrony, zaawansowanych technologii oraz grupy zajmujące się prawami człowieka. Wiadomo również, że grupa angażuje się w kradzież informacji i działania szpiegowskie z sektorów docelowych.
APT18 udało się wykraść informacje z podatnych na ataki systemów zdrowotnych, takie jak informacje o pacjentach, informacje o urządzeniach medycznych oraz prawa własności intelektualnej, które mogłyby zostać wykorzystane do osiągnięcia wysokich międzynarodowych standardów w różnych branżach oraz dla zysku Chin. Wśród informacji uzyskanych z systemów zdrowotnych ogłoszono, że atakujący przejęli informacje o tożsamości 4,5 mln pacjentów oraz o produkcji urządzeń medycznych.

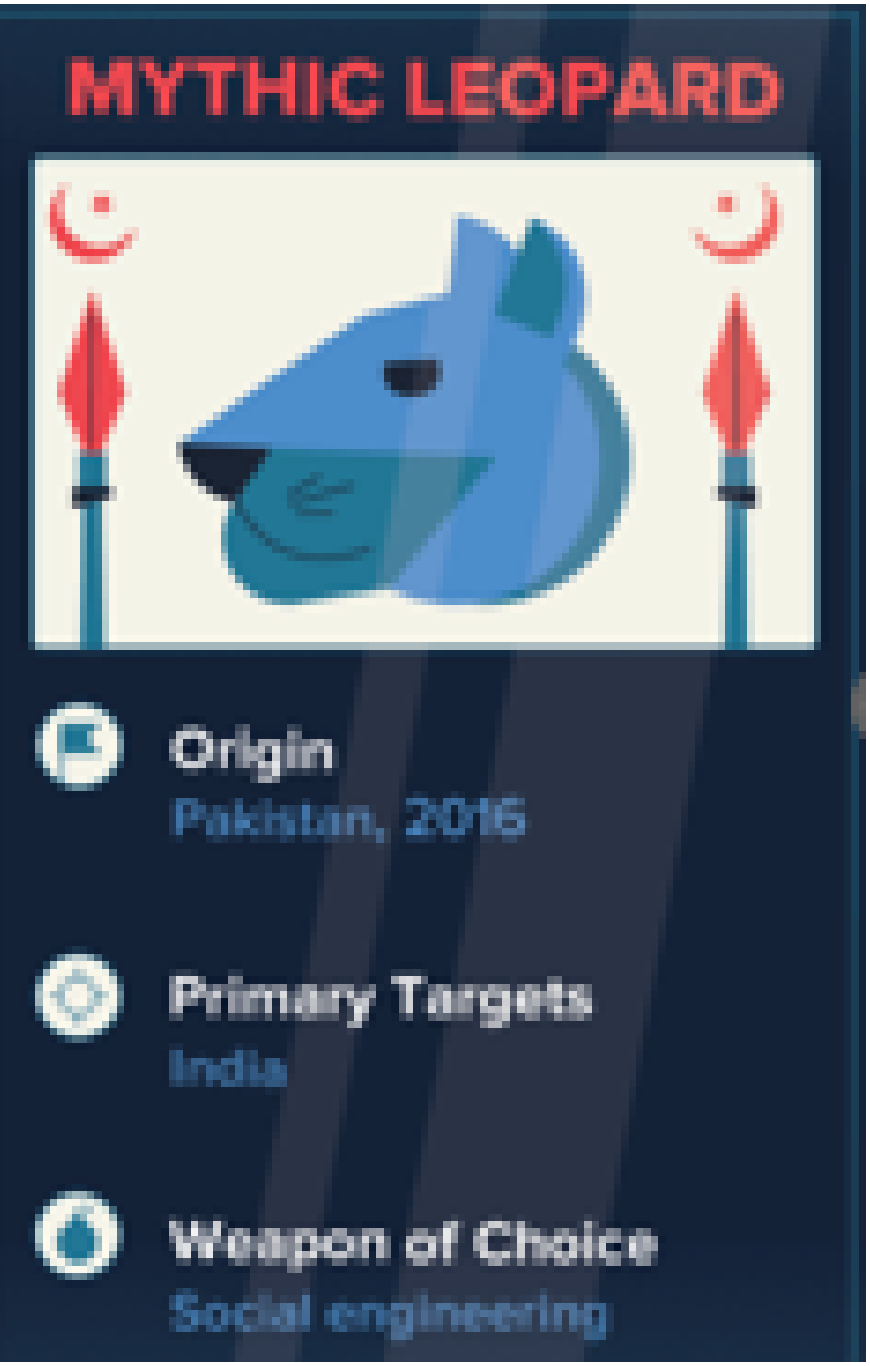
2015-16
Kampania phishingowa dla organizacji w Stanach Zjednoczonych APT18 przeprowadziło ataki na wiele organizacji z siedzibą w Stanach Zjednoczonych, w których złośliwe oprogramowanie Flash 0-day exploit, HTTPBrowser i Pisloader są dystrybuowane za pośrednictwem phishingowych wiadomości e-mail i adresów URL.

- **Advanced Persistent Threat 33 to grupa hakerska zidentyfikowana przez FireEye jako wspierana przez rząd Iranu. Grupa została również nazwana Refined Kitten (przez Crowdstrike), Magnallium (przez Dragos) i Holmium (przez Microsoft),**
- **APT33 podobno obrał za cel przemysł lotniczy, obronny i petrochemiczny w Stanach Zjednoczonych, Korei Południowej i Arabii Saudyjskiej.**
- **APT33 podobno używa programu droppera oznaczonego jako DropShot, który może wdrożyć wiper o nazwie ShapeShift lub zainstalować backdoora o nazwie TurnedUp. Grupa podobno używa narzędzia ALFASHELL do wysyłania e-maili spear-phishingowych załadowanych złośliwymi plikami HTML Application do swoich celów.**
- **APT33 zarejestrowało domeny podszywające się pod wiele podmiotów komercyjnych, w tym Boeing, Alsalam Aircraft Company, Northrop Grumman i Vinnell.**
- **FireEye i Kaspersky Lab zauważyły podobieństwa między ShapeShiftem a Shamoonem, innym wirusem powiązanym z Iranem. APT33 używał również języka Farsi w ShapeShifcie i DropShocie i był najbardziej aktywny podczas godzin pracy czasu standardowego Iranu, pozostając nieaktywnym w irański weekend.**
- **Jeden haker znany pod pseudonimem xman_1365_x był powiązany zarówno z kodem narzędzia TurnedUp, jak i z irańskim Instytutem Nasr, który został połączony z irańską cyberarmią. xman_1365_x ma konta na irańskich forach hakerskich, w tym Shabgard i Ashiyane.**

Cele: Sektor finansowy i rządowy

- **El Machete APT-C-43 hiszpańskojęzyczny aktor zagrożeń, który koncentruje się na celach w Ameryce Łacińskiej, w 2014 roku, przy czym aktywność grupy sięga 2010 roku. Działania grupy utrzymywały się przez lata, przyjmując praktykę wykorzystywania dokumentów o tematyce rządowej jako wabików, a także stosując przynęty związane z bieżącą sytuacją polityczną.**
- **W połowie marca El Machete została zauważona przy wysyłaniu spear-phishingowych e-maili do organizacji finansowych w Nikaragui, z załączonym dokumentem Word zatytułowanym "Mroczne plany neonazistowskiego reżimu na Ukrainie". Dokument zawierał artykuł napisany i opublikowany przez Aleksandra Chocholikowa, rosyjskiego ambasadora w Nikaragui, który omawiał konflikt rosyjsko-ukraiński z perspektywy Kremla.**

- **OceanLotus, znany również jako APT32, to grupa hakerska związana z rządem Wietnamu. Została oskarżona o cyberszpiegostwo wymierzone w dysydentów politycznych, urzędników państwowych i firmy mające powiązania z Wietnamem.**
- **W 2020 roku Bloomberg poinformował, że OceanLotus obrał za cel chińskie Ministerstwo Zarządzania Kryzysowego i rząd miejski Wuhan, aby uzyskać informacje o pandemii COVID-19. Wietnamskie Ministerstwo Spraw Zagranicznych nazwało oskarżenia bezpodstawnymi.**
- **W 2020 r. badacze firmy Kaspersky ujawnili, że OceanLotus wykorzystywał Sklep Google Play do dystrybucji szkodliwego oprogramowania. W listopadzie 2020 r. badacze Volexity ujawnili, że OceanLotus zakładał strony internetowe z fałszywymi wiadomościami i strony na Facebooku, aby zarówno angażować się w profilowanie sieci, jak i dystrybuować szkodliwe oprogramowanie. Według doniesień Facebook wyśledził działalność grupy do firmy informatycznej o nazwie CyberOne Group z Ho Chi Minh City.**
- **W lutym 2021 roku Amnesty International poinformowała, że OceanLotus przeprowadził szereg ataków spyware przeciwko wietnamskim działaczom praw człowieka, w tym Bui Thanh Hieu.**
- **W marcu 2021 roku poinformowano, że na działalność grupy wpłynął pożar w centrum danych OVH we Francji**



- Mythic Leopard to grupa zagrożeń z siedzibą w Pakistanie
- Głównie celuje w organizacje dyplomatyczne, obronne i badawcze w rządzie Indii oraz armię indyjską lub powiązane aktywa w Indiach i Afganistanie. Mythic Leopard wykorzystywał kilka zastrzeżonych rodzin malware dla systemów operacyjnych Windows i Android. Grupa jest zazwyczaj znana z działań szpiegowskich.
- Gdy śledzono adresy IP, o których sądzono, że należą do Mythic Leopard, ustalono, że pochodzą z Pakistanu. Ataki były częścią szerszej operacji wielowektorowej, takiej jak phishingowe kampanie e-mailowe i strony internetowe typu watering hole, dostarczające wyspecjalizowane RAT-y o nazwie Crimson i Peppy. Te RAT-y mogą wyprowadzać informacje, robić zrzuty ekranu i nagrywać strumienie z kamer internetowych.
- Mythic Leopard tworzy również fałszywe domeny, które naśladują legalne organizacje wojskowe i obronne jako główny element ich operacji. Stwierdzono, że aktor zagrożeń wykorzystał w kampanii kilka metod dostarczania. Są to pliki wykonywalne maskujące się jako instalatory legalnych aplikacji, pliki archiwalne i złośliwe dokumenty w celu wycelowania w indyjskie podmioty i osoby. Te łańcuchy infekcji były widoczne w umieszczaniu różnych typów implantów nie obserwowanych wcześniej.

Charming Kitten (inne pseudonimy to APT35 (przez Mandiant), Phosphorus (przez Microsoft), Ajax Security (przez FireEye), NewsBeef (przez Kaspersky), to irańska rządowa grupa cyberwojenna APT.
Badania przeprowadzone przez FireEye w 2018 roku sugerowały, że APT35 może rozszerzać swoje możliwości w zakresie złośliwego oprogramowania i kampanii włamań
Od tego czasu grupa znana jest z wykorzystywania phishingu do podszywania się pod strony internetowe firm, a także fałszywych kont i fałszywych domen DNS do wyłudzania haseł użytkowników.
W 2013 r. była sierżant techniczna Sił Powietrznych Stanów Zjednoczonych i kontrahent wywiadu wojskowego Monica Witt uciekła do Iranu, wiedząc, że może za to ponieść zarzuty karne ze strony Stanów Zjednoczonych. Jej przekazanie danych wywiadowczych rządowi Iranu spowodowało później Operację Szafranowa Róża, operację cyberwojny, która była wymierzona w amerykańskich kontrahentów wojskowych.

AWL
WYDZIAŁ ZARZĄDZANIA

Dziękuję za uwagę!