„Aktualne zagrożenia w cyberprzestrzeni”

Dariusz Deptała

Dyrektor Regionalny KSOIN

Serock 29-31 maja 2017 r.

Agenda prezentacji

1. Czego się boimy, jako przedsiębiorcy i jako obywatele?
2. Gdzie w cyberprzestrzeni można umieścić cyberprzestępczość i cyberwojnę?
3. Jaka jest motywacja sprawców cyberzagrożeń?
4. Jaka jest przestępczość internetowa wg iOCTA Europolu z 2016 r. ?
5. Jakie są Cyberzagrożenia wg „Norton Cybercrime Report z 2016”?
6. W jaki sposób możemy podzielić cyberprzestępczość, a w jaki zagrożenia z nią związane?
7. Czy obecny system w Polsce skutecznie chroni cyberprzestrzeń i pozwala na efektywne ściganie cyberprzestępców?
8. Podsumowanie

Co posiadamy w firmie/organizacji/przedsiębiorstwie ?

- Aktywa finansowe
- Informacje stanowiące tajemnicę przedsiębiorstwa
- Dane osobowe (klienci, kontrahenci, współpracownicy, pracownicy)
- Informacje niejawne
- Wyposażenie materialne/trwałe

Czego się boi przedsiębiorca?

Czego się boi zwykły użytkownik?

Czego się boi przedsiębiorca?

- utarty reputacji
- wykradnięcia własności intelektualnej i danych klientów
- kradzieży i włamań pospolitych

Czego się boi zwykły użytkownik?

- kradzieży pieniędzy z rachunków bankowych
- utraty swoich danych, jednocześnie nie dbając o nie
- innych kradzieży (np. kradzież pojazdu, włamanie do domu)
- innych przestępstw pospolitych

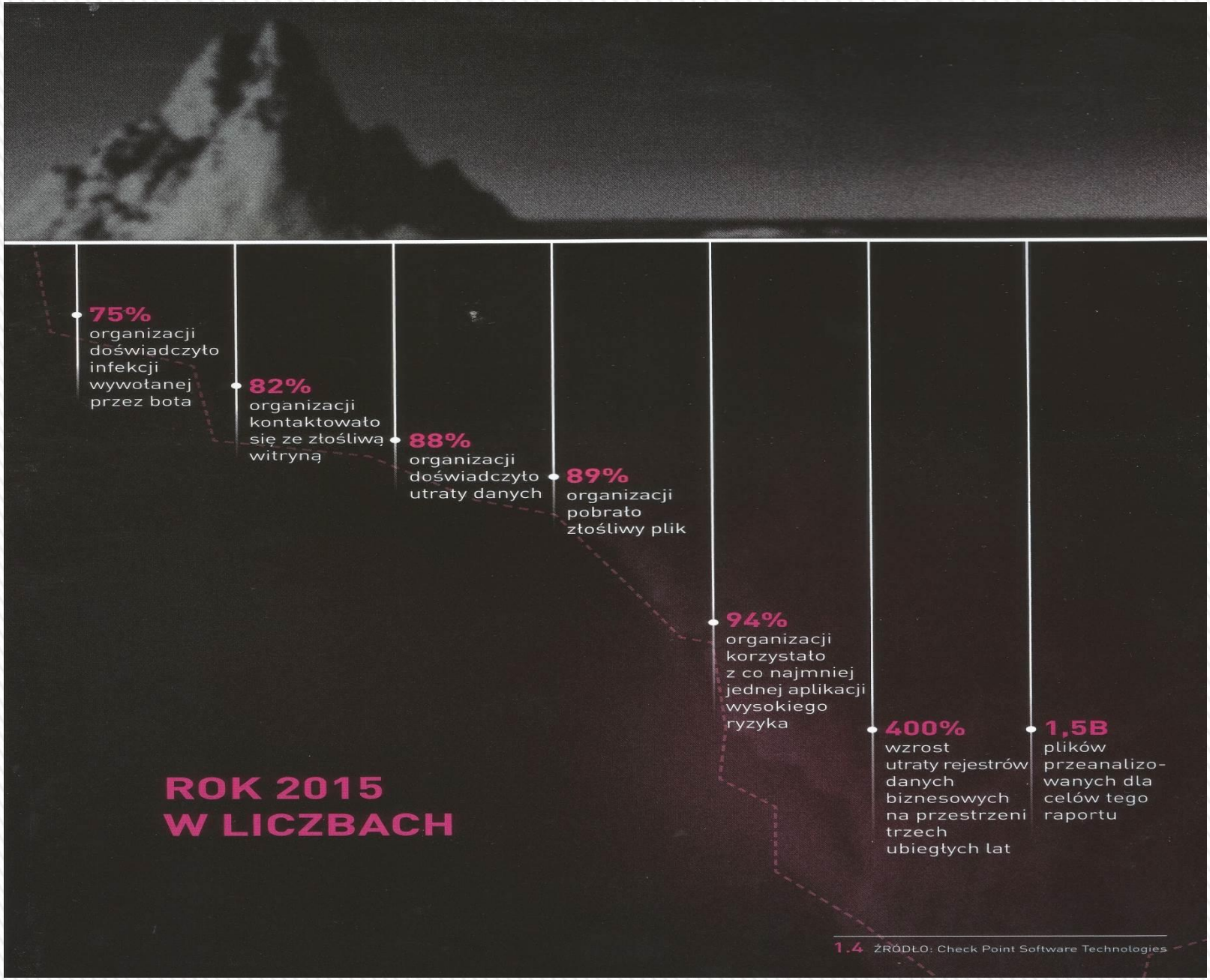
Co myślimy ?

- **77%** organizacji zdaje sobie sprawę z dużej wartości informacji
- **31%** deklaruje realne straty finansowe i wizerunkowe spowodowane utarta informacji
- **97%** badanych uważa że warta inwestować w środki zapobiegające utracie danych
- wyciek danych to w 25% nośniki papierowe a **75%** nośniki elektroniczne
- **21 %** to pracownicy powodujący wyciek danych z przyczyn niedbalstwa i braku znajomości podstawowych norm bezpieczeństwa
- **53%** uważa że systemy bezpieczeństwa w ich organizacji są na średnim poziomie
- **70%** przedsiębiorców uważa, że wyciek danych może skutkować dużymi stratami finansowymi w firmie

(Źródło: Global Data Leakage Report, raport Efektywne Zarządzanie System Informacji)

Co się dzieje ?

- Co 5 sekund użytkownik uzyskuje dostęp do złośliwej witryny
- 75 % badanych organizacji doświadczyło infekcji z wykorzystaniem botów
- 971 nieznanych złośliwych programów uderza w organizację co godzinę
- Wystarczy jedna infekcja na urządzeniu aby zaatakować prywatne oraz domowe dane i sieci
- 88% organizacji doświadczyło utraty danych


75%
organizacji doświadczyło infekcji wywołanej przez bota
82%
organizacji kontaktowało się ze złośliwą witryną
88%
organizacji doświadczyło utraty danych
89%
organizacji pobrało złośliwy plik
94%
organizacji korzystało z co najmniej jednej aplikacji wysokiego ryzyka
400%
wzrost utraty rejestrów danych biznesowych na przestrzeni trzech ubiegłych lat
1,5B
plików przeanalizowanych dla celów tego raportu
ROK 2015
W LICZBACH
1.4 ŹRÓDŁO: Check Point Software Technologies

CELE

ORGANIZACJE WEDŁUG BRANŻY

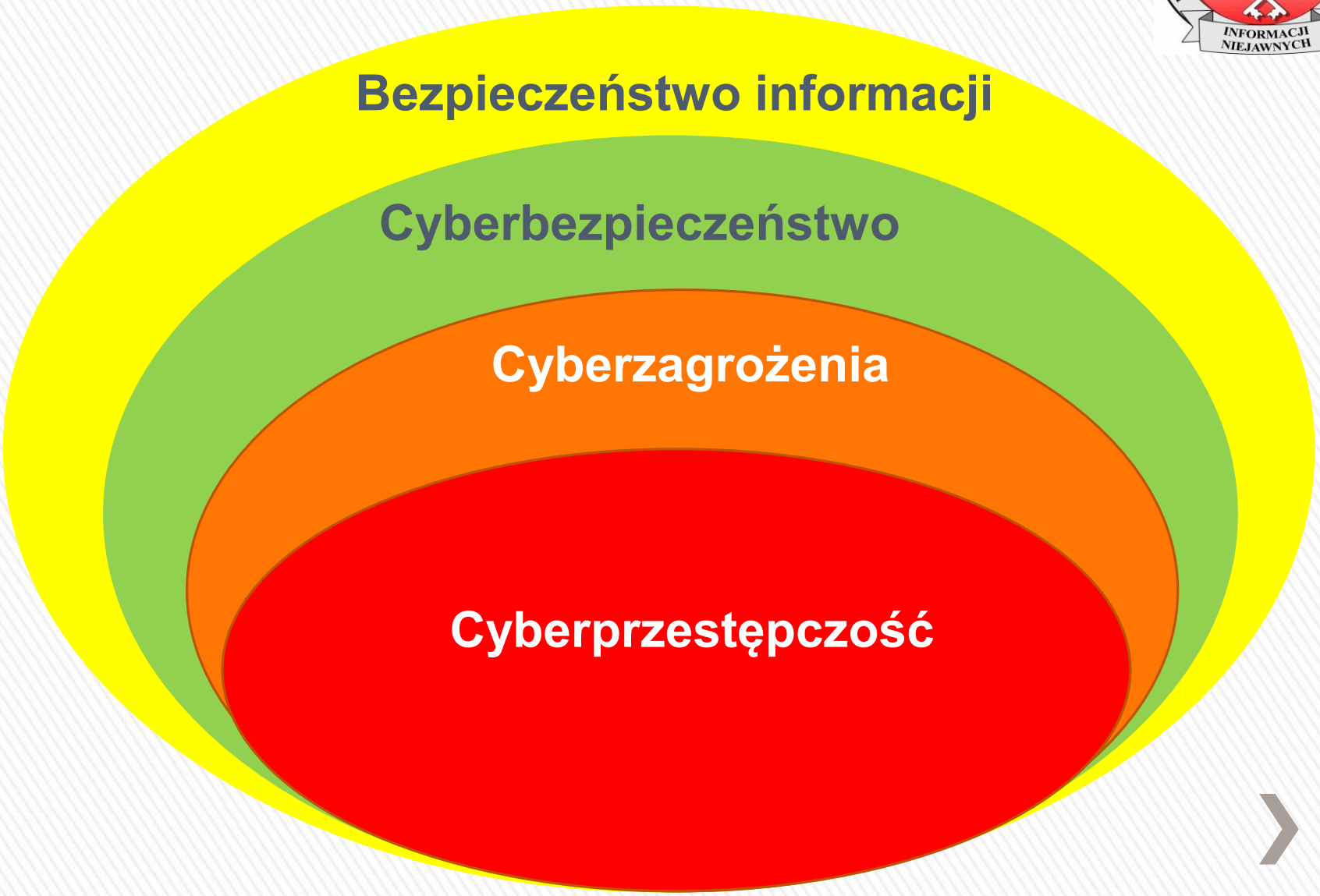
*Sektor prawny, rozrywkowy / Sektor hotelowo-gastronomiczny, handel detaliczny i hurtowy, reklama/media, papiery wartościowe, inne

1.3 ŹRÓDŁO: Check Point Software Technologies

Cyberprzestrzeń

przestrzeń przetwarzania i wymiany informacji tworzona prze
systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy
nimi oraz relacjami z użytkownikami

CYBERPRZESTRZEŃ



Źródło: J. Kosiński „Paradygmaty cyberprzestępczości

Malware - złośliwe oprogramowanie - szkodliwe, przestępcze lub złośliwe działanie w stosunku do użytkownika komputera, które może uzyskiwać zdolny dostęp do systemu, zapisywać i wysyłać dane z tego systemu osobom trzecim bez wiedzy i zgody użytkownika, wyłączać środki bezpieczeństwa (wirusy, robaki, konie trojańskie, backdoory, rookity, keyloggery, spyware

- Exploit – przyjmuje kontrolę nad działaniem procesu poprzez wykonanie spreparowanego kodu
- Rogues – udaje program antywirusowy
- Ransomware – ogranicza użytkownikowi prowadzenie aktywności w systemie
- Rootkit – ukryty program który maskuje swoją obecność w komputerze

Sposoby dostania się:

- Wykorzystanie zainfekowanych stron internetowych do kierowania na nie odwiedzających witryny
- Wykorzystanie zainfekowanych stron www lub e-maili do oszukania użytkowników
- Wykorzystanie wymiennych nośników
- Wykorzystanie portali społecznościowych

Botnet - sieć komputerów zarażonych złośliwym oprogramowaniem, przyjętych i zarządzanych przez cyberprzestępców (tzw, zombie). Można nimi zarządzać zwykle bez wiedzy użytkownika - z innego komputera. Działanie sprawcy składa się z 2 faz:

- Zainfekowanie jak największej liczby komputerów (wykorzystanie słabych haseł, programy crackujące, błędy w oprogramowaniu, wykorzystanie metod socjotechnicznych do uzyskania haseł)
- Zarządzanie utworzoną armią botów pozwalającą głownie na:
  - kradzieże (danych, haseł, identyfikatorów, dostepów)
  - zysk (handel *malwerem, botnetami*, z zarobku za spam)
  - *pihishing* (fałszywe strony przesyłane z jednego zombie na drugi)
  - spam
  - rozprzestrzenianie *malware*
  - piractwo intelektualne
  - wymuszenia

Phishing - metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję, w celu wyłudzenia określonych informacji - np. danych logowania, szczegółów karty kredytowej lub nakłonienia ofiary do określonych działań

Skimming **-** obejmuje wszelkiego rodzaju czyny dotyczące fałszowania kart płatniczych, tj. podrabiania, przerabiania, kopiowania np. poprzez instalowanie na bankomatach urządzeń do pozyskiwania danych z pasków magnetycznych kart płatniczych. ***Skimming bis”*** **-** polega na skanowaniu kart pre-paidowych za pomocą aplikacji smartphonowych

DDoS (rozproszona odmowa usługi) – polega na wysłaniu do ofiary dużej ilości pakietów, które wyczerpują możliwości zasoby komputerów. Pakiety mają zwykle sfałszowane adresy źródłowe

Spam – wiadomość rozsyłana do osób, które jej nie zamawiały i nie oczekują. Polega zwykle na rozsyłanie informacji komercyjnych o jednakowej treści do nieznanych sobie osób.
Spamy dzielą się na komercyjne i niekomercyjne
Cechy spamu:

- Treść wiadomości jest niezależna od tożsamości odbiorcy
- Odbiorca nie wyraził zgody na otrzymanie tej wiadomości
- Treść wiadomości daje podstawę do przypuszczeń, że nadawca może odnieść zyski nieproporcjonalne do korzyści odbiorcy

Spam nigeryjski - wyłudzenie pieniędzy na koszty manipulacyjne związane z transferem mln USD

Fałszywa reklama – metoda bazuje na cenie i jest osiągana przez przez ukrycie opłaty i dopłaty

Spam na portalach społecznościowych

Zagrożenia w 2016 r.

- infiltracja i wyciek danych
- unieruchomienie usług (np.. atak DDos)
- proliferacja (rozprzestrzenienie się, pozostanie w ukryciu)
- wykorzystanie działań szkodliwych
- inżyniera społeczna (*pihishing*)
- *botne*t, w tym na urządzenia sieciowe np. rutery, punkty dostępu (w PL ponad 20.000 ataków dziennie)
- wymuszenia (szyfrowanie, ujawnianie danych)
- sabotaż (modyfikacja informacji np. kadrowych w firmie)
- legalny podsłuch
- kompromitacja i dysfunkcja *IoT* np. atak na samochód
- ataki na urządzenia mobline
- *ransomware*

Atak ransomware

- atak 12 maja 2017 r. od 7.00
- 200 tys. zaatakowanych komputerów w 150 krajach
- wykorzystanie błędu w portalu SMB dzięki pewnej aplikacji
- infekcja i skanowanie sieci w poszukiwaniu ofiar
- szyfrowanie plików ofiary i żądanie okupu 300 USD
- po 3 dniach kwota okupu wzrosła do 600 USD
- ofiary m. in: szpitale, koncerny samochodowe, koncerny RTV itp.

Sprawcy

Główny cel ataku, to zdobycie kasy, a więc banki, instytucje finansowe + oszustwa finansowe

Sprawcy (pojedyncze osoby lub zorganizowane grupy):

- Cyberprzestępcy
- Wrogie państwa
- Konkurencja

ATAKUJACY	ZAMIERZENIE
Uczeń	Testowanie możliwości (zamiast czytania instrukcji)
Student	Odczytywanie cudzych listów dla zabawy
Kraker	Przełamanie zabezpieczeń systemu komputerowego np. dziekanatu
Haker	Testowanie bezpieczeństwa obcych systemów
Przedst. handlowy	Chęć poprawy własnego wizerunku i prestiżu
Biznesmen	Poznanie strategicznych tajemnic konkurentów
Pracownik	Nieświadome zawirusowanie komputera firmowego
Były pracownik	Zemsta za zwolnienie z pracy
Księgowy	Defraudacja pieniędzy firmowych
Makler giełdowy	Wycofanie się z obietnicy złożonej klientowi drogą elektroniczną
Oszust	Przechwycenie numerów karty kredytowej, fikcyjna sprzedaż
Szpieg	Zapoznanie się z wojskowymi i przemysłowymi tajemnicami
Terrorysta	Dokonanie zniszczeń i zabicie jak największej liczy osób
Pedofil	Podszywanie się pod dziecko przy korzystaniu z komunikatora

Źródło: J. Kosiński „Paradygmaty cyberprzestępczości”

- ✓ Strukturalne rozwinięcie *Malware*, w tym mobilnego, w bankowości internetowej oraz samrtphonach
- ✓ Kluczowy rodzaj *Malware* *Ransoware*
- ✓Wykorzystywanie seksualne dzieci
- ✓Oszustwa przy płaceniu
- ✓ Naruszanie danych i ataki sieciowe (APTs)
- ✓ Ataki na Infrastrukturę Krytyczną
- ✓ Oszustwa finansowe on-line i pihishing (konta bankowe, karty kredytowe, czeki, ser. aukcyjne)
- ✓ Nielegalny handel stronami w *Darknecie*
- ✓ Wykorzystywanie „mułów” i pranie pieniędzy
- ✓ Niekontrolowana komunikacja przestępców (fora Internetowe przestępców)
- ✓ Cyberterroryzm
- ✓ *Big data* i *Cloud* (w ogromnych zbiorach danych łatwiej ukryć informacje o przestępstwie

1. Wzrost przestępczości w cyberprzestrzeni, która nie wymaga umiejętności technicznych
2. *Malware* jest kluczowym zagrożeniem dla osób prywatnych i biznesu
3. Obserwuje się wycofywanie starych programów wykorzystywanych przez cyberprzestępców i zastępowanie ich programami nowej generacji
4. Przestępcy wykorzystują bardzo często inżynierię społeczną jako efektywne narzędzie przy kompleksowych cyberatakach w celach oszustw
5. Zmniejsza się liczba oszustw wymagająca obecności kart płatniczych a zwiększa się liczba oszustw bez obecności kart płatniczych (bankowość mobilna, e-handel)
6. Potencjalne ofiary nie stosują „higieny cyfrowe” (nie zmieniane hasła, narzędzia, produkty cyfrowe)
7. TOR jest w dalszym ciągu ulubioną platformą dla „podziemnych” forów i handlu
8. Rozwój Internetu w krajach rozwijających się i wysoki stopień anonimowości jedną z przyczyn wzrostu liczby seksualnego wykorzystania dzieci
9. Posiadanie *smartphonów* przez dzieci i nastolatki powoduję zwiększenie podatności na wymuszenia seksualne.
10. Rozszerzenie anonimowości i szyfrowania danych wykorzystywana jest przez przestępców do własnej ochrony


GLOBALNE KOSZTY SPOWODOWANE CYBERPRZESTĘPCZOŚCIĄ
$110 MLD
85% KOSZTÓW BEZPOŚREDNICH TO EFEKT OSZUSTW, KRADZIEŻY I STRAT ORAZ NIEZBĘDNYCH NAPRAW
INNE; 15%
OSZUSTWA; 42%
NAPRAWY; 26%
KRADZIEŻ LUB UTRATA; 17%
ŚREDNI KOSZT W PRZELICZENIU NA 1 OFIARĘ 197 USD
STRATY W POLSCE SPOWODOWANE CYBERPRZESTĘPCZOŚCIĄ
4,8 MLD ZŁ
ŚREDNI KOSZT W PRZELICZENIU NA 1 OFIARĘ
672 ZŁ

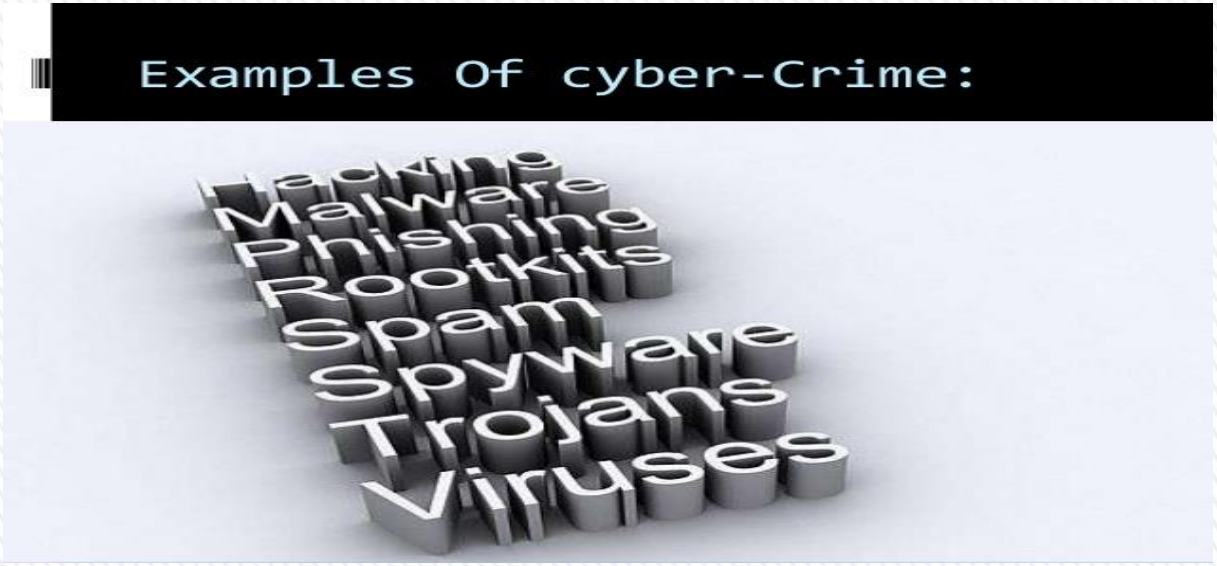
2016 SYMANTEC Norton Raport c.d

Obszary najbardziej narażone na ataki to:

- smartphone
- Internet rzeczy
- Web 3,0 (ataki sieciowe)
- Media społecznościowe
- Komunikatory i e-maile(blogi, fora, serwis MySpace, YouTube, Twitter)

2016 SYMANTEC Norton Raport

- 430 milionów nowych ataków *malware* w 2015 r. – wzrost 0 36 % do roku 2014, (złośliwy program New Zero-Day wzrost o 125%)
- Ukradziono 429 milinów danych osobowych – wzrost o 23 %
- O 55% wzrosła liczba ataków na organizacje rządowe i instytucje finansowe
- O 35 % wzrosła liczba ataków *ransomware* na PC, smartphone
- Wzrost o 43 % liczby ataków na małe firmy (od 1 do 261 pracowników)
- Do sukcesu cyberprzestępczości przyczynia duża liczba nowych usług internetowych z których chętnie korzystają użytkownicy.



Zagrożenia w sieci

Cechy wspólne przestępstw popełnianych w cyberprzestrzeni

Lekcjoważone kwestie na poziomie kraju i firm:

- bezpieczeństwa i brak systemowej ochrony cyberprzestrzeni RP
- obstrukcyjne przepisy
- wybór technologii – nieprzemyślane decyzje zakupowe
- brak edukacji
- podejście „szefów” – kupiliśmy, mamy, wystarczy i nie ma co inwestować
- podejście „szefów” – szkoda pieniędzy na nowe wdrożenia – nic się przecież nie dzieje.

Zabezpieczenia systemowe:

- budowa systemów rozwiązań dla ochrony cyberprzestrzeni RP
- identyfikacja i analiza podatności
- wdrożenie polityki zabezpieczeń w kluczowych obszarach
- tworzenie regionalnych centrów bezpieczeństwa
- pomoc w planowaniu ochrony przed atakami i usuwaniu ich skutków
- przygotowanie i pomoc we wdrożeniu plany zabezpieczeń
- Edukacja
- szkolenia dla „VIP”

Podnoszenie poziomu bezpieczeństwa
EDUKACJA

Nadal wielu Polaków nie zna podstawowych mechanizmów ochrony swoich komputerów oraz zawartych w nich danych, a także ochrony swojej tożsamości w sieci internetowej.

Bezpieczeństwo teleinformatyczne Państwa nie leży jedynie w gestii instytucji rządowych oraz zespołów reagowania na incydenty, ale spoczywa ono na każdym użytkowniku komputera.

Podstawowym elementem dbania o bezpieczeństwo cyberprzestrzeni jest kształtowanie świadomości istnienia zagrożeń w sieci internetowej oraz wskazywanie konieczność przeciwdziałania cyberzagrożeniom.


CYBER CRIME SCENE

Podstawowym aktem prawnym, na którym opiera się walka z cyberprzestępczością w Polsce jest Kodeks karny

- Art. 190a § 2 – podszywanie się pod inną osobę, fałszywe profile
- Art. 202 kk – dot. treści pedofilskich,
- Art. 256 kk – ekstremizm polityczny – treści faszystowskie
- Art. 267 § 1 kk – nieuprawnione uzyskanie informacji (hacking),
- Art. 267 § 2 kk – podsłuch komputerowy (sniffing),
- Art. 268 § 2 kk – udaremnienie uzyskania informacji,
- Art. 268a kk – udaremnienie dostępu do danych informatycznych,
- Art. 269 § 1 i 2 kk – sabotaż komputerowy,
- Art. 269a kk – rozpowszechnianie złośliwych programów oraz cracking,
- Art. 269b kk – tzw. „narzędzia hacker'skie",
- Art. 271 kk – handel fikcyjnymi kosztami,
- Art. 286 kk – oszustwo popełniane za pośrednictwem Internetu
- Art. 287 kk – oszustwo komputerowe.

- ✓ Prawo karne nie posiada tzw. legalnej tj. jednolitej definicji dowodu elektronicznego.
- ✓ Dowód elektroniczny jest to informacją zapisaną na nośniku elektronicznym. Może on przybierać postać dokumentów komputerowych (e-maile, smsy, zdjęcia, teksty tworzone w Wordzie) jak i danych cyfrowych (tzw. logów komputerowych)
- ✓ W procesie karnym dowody elektroniczne są dopuszczalne i podlegają ocenie Sądu tak jak każdy inny dowód
- ✓ Niewątpliwie jednak, aby dowód elektroniczny był procesowo "użyteczny" musi on być najpierw prawidłowo zabezpieczony dla potrzeb procesu karnego.
- ✓ Metodyka zabezpieczania dowodów elektronicznych (co może poważnie zadziwiać) nie została przez ustawodawcę uregulowana w żadnym powszechnie obowiązującym normatywnym akcie prawnym.
- ✓ Jedynym dokumentem poruszającym wskazaną kwestię jest zarządzenie komendanta głównego policji nr 1426 z dnia 23 grudnia 2004 r. w sprawie metodyki wykonywania czynności dochodzeniowo-śledczych przez służby policyjne Wskazane tam zalecenia obejmują m.in.: nakaz udziału biegłego w przeszukaniu systemów informatycznych, czy też obowiązek sporządzania protokołu z przebiegu zatrzymania oraz przeszukania systemu informatycznego.
- ✓ **Metodyka zabezpieczania dowodów elektronicznych** została przez ustawodawcę pozostawiona praktyce, czyli pewnym zwyczajom oraz procedurom przyjętym przez organy ścigania w drodze zwyczajowej.

Podnoszenie poziomu bezpieczeństwa - przeciwdziałanie

Działalność państw i organizacji międzynarodowych w ochronie cyberprzestrzeni

- CERT-y czyli Computer Emergency Response Team
- Centrum Dowodzenia Cyberprzestrzennego

Działania państwa polskiego w zakresie ochrony cyberprzestrzeni

- ✓ NCC
- ✓ CERT-y
- ✓ Narodowe Centrum Kryptologii

PODSUMOWANIE

- Komputer, sieć komputerowa, urządzenie teleinformatyczne jest przedmiotem, środkiem lub celem przestępstwa
- Przestępcy wykorzystują zwykle łatwe w obsłudze ale zaawanasowane technologie
- Mamy do czynienia z anonimowością sprawcy
- Przestępcy komputerowi traktowani są przez społeczeństwa jako ludzie nieszkodliwi
- Ofiara jest zwykle nieświadoma, że jej system został zaatakowany
- Bardzo rzadko są składane doniesienia o cyberprzestępstwach, chyba, ze doszło do znacznych strat finansowych
- Krótki czas potrzebny do popełnienia przestępstwa
- Niskie koszty, duże korzyści
- Cyberprzestępczość to międzynarodowy zasięg i transgraniczność
- Asymetryczność zagrożeń
- **….. i jak zawsze myślenie, że to na pewno nas nie dotyczy**

Bibliografia (wybrana)

- ✓ Kosiński J. „Paradygmaty cyberprzestępczości”, wyd. Difin, W-wa 2015
- ✓ „The Internet Organised Crime Threat Assessment” , wyd. Europol, Haga 2016 (www.europol.eu)
- ✓ „Nortom Cybercrime Report 2016”, wyd. Norton (www.norton.com)
- ✓ Ustawa z dnia 6 czerwca 1997 r. Kodeks karny
- ✓ 2016 Raport bezpieczeństwa Check Point

Dziękuję za uwagę!

Dariusz Deptała

E-mail: ddeptala@ksoin.pl

tel.: +48-601-284-209

- **KONSULTACJE**
- **DORADZTWO**
- **SZKOLENIA**
- **AUDYT**

KRAJOWE STOWARZYSZENIE OCHRONY INFORMACJI NIEJAWNYCH

- **PROFESJONALIZM**
- **DOŚWIADCZENIE**
- **KOMPETENCJE**