UNIWERSYTET OPOLSKI

Problematyka bezpieczeństwa i zagrożeń w cyberprzestrzeni dla systemów i sieci teleinformatycznych

w aspekcie pozamilitarnych przygotowań obronnych

w działach administracji rządowej nauka i szkolnictwo wyższe, funkcjonowanie Uniwersytetu Opolskiego w czasie możliwego zagrożenia dla systemów i sieci teleinformatycznych Uczelni powstałego w cyberprzestrzeni RP

Opole 12.12.2018 r

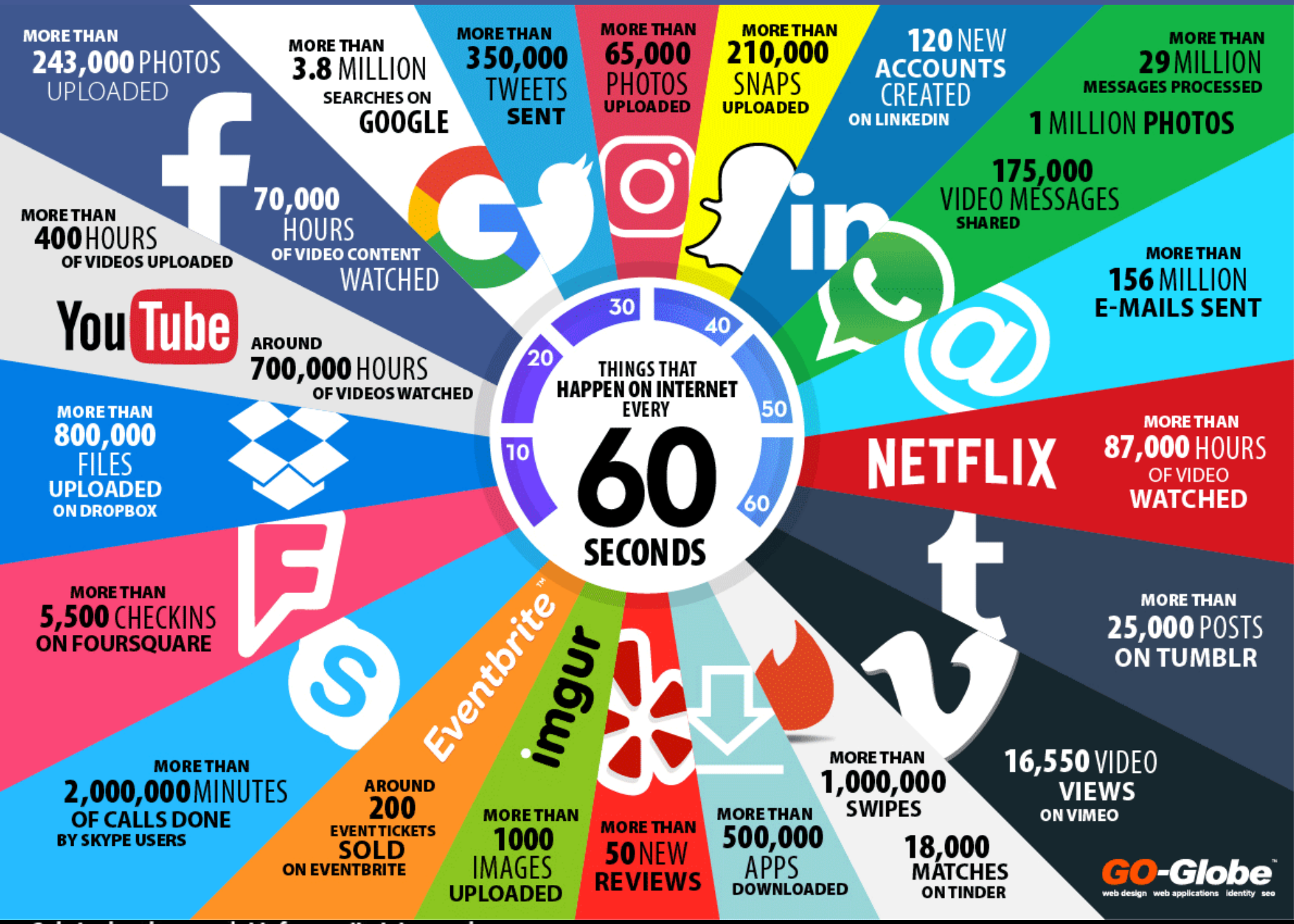
Najgebauer Jacek

UNIWERSYTET OPOLSKI

Słownik

Cyberprzestrzeń - przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami.

Cyberprzestrzeń RP – cyberprzestrzeń w obrębie terytorium państwa polskiego oraz w miejscach, gdzie funkcjonują przedstawicielstwa RP (placówki dyplomatyczne, kontyngenty wojskowe, jednostki pływające oraz statki powietrzne poza przestrzenią RP, podlegające polskiej jurysdykcji).



Sekcja ds. obronnych i informacji niejawnych

Słownik

Cyberatak - celowe zakłócenie prawidłowego funkcjonowania cyberprzestrzeni.

Cyberprzestępstwo - czyn zabroniony popełniony w obszarze cyberprzestrzeni.

Cyberterroryzm - przestępstwo o charakterze terrorystycznym popełnione w cyberprzestrzeni.

Wojna cybernetyczna - (ang. cyberwarfare) to każdego rodzaju spektrum działań w cyberprzestrzeni związane z atakami na systemy informatyczne przeciwnika.

UNIWERSYTET OPOLSKI

Cyberwojna

Pojęcie wojny cybernetycznej stworzył ***William Gibson*** *w powieści* ***„Neuromancer”*** *w roku 1984 r.,* ***z początkiem lat 90. określenie to weszło do powszechnego obiegu.***

Pierwsze działania w cyberprzestrzeni oraz kampanie (dez)informacyjne miały miejsce w pierwszej połowie lat 90. **Za początek współczesnych działań wojennych w cyberprzestrzeni przyjmuje się atak Rosji na Estonię 17 maja 2007 r.**

Współczesne spektrum zagrożeń dla bezpieczeństwa narodowego może dotyczyć wszelkiego rodzaju **działań w cyberprzestrzeni**, mających na celu **zmianę wizerunku** oraz możliwości kształtowania samodzielnych **działań państw oraz organizacji i ludzi.**

Państwami posiadającymi realne zdolności do przyjęcia oraz odpowiedzi na działania w cyberprzestrzeni są m.in. Chiny, Izrael, Korea Północna, Rosja i Stany Zjednoczone.

Bezpieczeństwo cyberprzestrzeni RP

część cyberbezpieczeństwa państwa, obejmująca zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych, mających na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni RP, wraz ze stanowiącą jej komponent publiczną i prywatną teleinformatyczną infrastrukturą krytyczną oraz bezpieczeństwa przetwarzanych w niej zasobów informacyjnych.

Cyberbezpieczeństwo – odporność systemów informacyjnych na działania naruszające **poufność, integralność, dostępność i autentyczność** przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy

Słownik

CERT (ang. Computer Emergency Response Team) - zespół powołany do reakcji na zdarzenia naruszające bezpieczeństwo w sieci Internet.

W Polsce powstały zespoły reagowania na incydenty bezpieczeństwa komputerowego działających w:

- Ministerstwie Obrony Narodowej,
- Agencji Bezpieczeństwa Wewnętrznego,
- oraz przy Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym

Zespół CERT.GOV w Agencji Bezpieczeństwa Wewnętrznego funkcjonujący od 1 lutego 2008 roku pełni rolę głównego zespołu CERT odpowiadającego za koordynację procesu reagowania na incydenty komputerowe w obszarze administracji rządowej.

UNIWERSYTET OPOLSKI

Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej

przyjęta przez rząd w 2013 mająca na celu podniesienie poziomu bezpieczeństwa w cyberprzestrzeni RP.

Główne kierunki działań określone w Polityce:

1. Szacowanie ryzyka.
2. Bezpieczeństwo portali administracji rządowej.
3. Założenia działań legislacyjnych.
4. Założenia działań proceduralno-organizacyjnych.
5. Założenia dotyczące kształcenia, szkoleń i uświadamiania w dziedzinie bezpieczeństwa.
6. Założenia działań technicznych.

UNIWERSYTET OPOLSKI

Polityka Ochrony Cyberprzestrzeni RP - bezpieczeństwo portali administracji rządowej

Polityka wskazwała na znaczenie cyberprzestrzeni w komunikacji jednostek administracji publicznej a obywatelami. W związku z tym należy przestrzegać wymagań bezpieczeństwa, do których należą odpowiednia dostępność, integralność oraz poufność danych. Podkreślona jest również zasadność wdrożenia dobrych praktyk, za których przygotowanie odpowiedzialny jest Zespół zadaniowy do spraw ochrony portali rządowych we współpracy z Rządowym Zespołem Reagowania na Incydenty Komputerowe CERT.GOV.PL.

UNIWERSYTET OPOLSKI

Cyberbezpieczeństwo w Strategii Bezpieczeństwa Narodowego RP

(5 lipiec 2014 r.)

„Rzeczpospolita Polska zapewnia bezpieczeństwo państwa i obywateli poprzez stwarzanie warunków do realizacji interesów narodowych i osiągania celów strategicznych. Interesy narodowe określa art. 5 Konstytucji Rzeczypospolitej Polskiej. Z nich wynikają interesy narodowe w dziedzinie bezpieczeństwa, do których należą:

- *[…]*
- ***zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni;”***

UNIWERSYTET OPOLSKI

Doktryna cyberbezpieczeństwa RP

W opublikowanej przez Biuro Bezpieczeństwa Narodowego w 2015 r. Doktrynie cyberbezpieczeństwa RP, która jest dokumentem koncepcyjnym oraz wykonawczym w stosunku do Strategii Bezpieczeństwa Narodowego RP określono m.in. cele operacyjne RP w dziedzinie cyberbezpieczeństwa, a także zdefiniowano szanse, wyzwania, ryzyka oraz zagrożenia dla cyberprzestrzeni RP.

UNIWERSYTET OPOLSKI

Doktryna cyberbezpieczeństwa RP - zagrożenia wewnętrzne cyberbezpieczeństwa

- **zagrożenia cyberbezpieczeństwa** – pośrednie lub bezpośrednie zakłócające lub destrukcyjne oddziaływania na podmiot w cyberprzestrzeni.

Wobec zagrożeń cyberprzestrzeni RP w wymiarze wewnętrznym Doktryna cyberbezpieczeństwa RP wskazuje na znaczenie ochrony infrastruktury krytycznej, na którą cyberprzestępcy mogą wpływać uderzając w systemy komunikacji zapewniające sprawne funkcjonowanie podsystemu kierowania bezpieczeństwem narodowym, podsystemu obronnego i podsystemów ochronnych, a także podsystemów wsparcia.

UNIWERSYTET OPOLSKI

Doktryna cyberbezpieczeństwa RP

- zagrożenia zewnętrzne cyberbezpieczeństwa

Dynamiczny rozwój technologii informatycznych zwiększa znaczenie zagrożeń o wymiarze zewnętrznym takich jak cyberkryzysy czy cyberkonflikty, istnieje także groźba cyberwojny.

Doktryna zwraca również uwagę na zagrożenie w cyberprzestrzeni ze strony cyberszpiegostwa, prowadzonego przez służby obcych państw. Ponadto zewnętrznymi źródłami zagrożeń w cyberprzestrzeni są także organizacje ekstremistyczne, terrorystyczne oraz zorganizowane transnarodowe grupy przestępcze.

UNIWERSYTET OPOLSKI

Dyrektywa NIS
(Network and Information Systems Directive)

6 lipca 2016 r. Parlament Europejski przyjął dyrektywę 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, str. 1), tzw. Dyrektywę NIS, dotyczącą bezpieczeństwa sieci i informacji.

Dyrektywa nakłada obowiązki związane z zapewnieniem bezpieczeństwa cybernetycznego na objęte nią podmioty.

UNIWERSYTET OPOLSKI

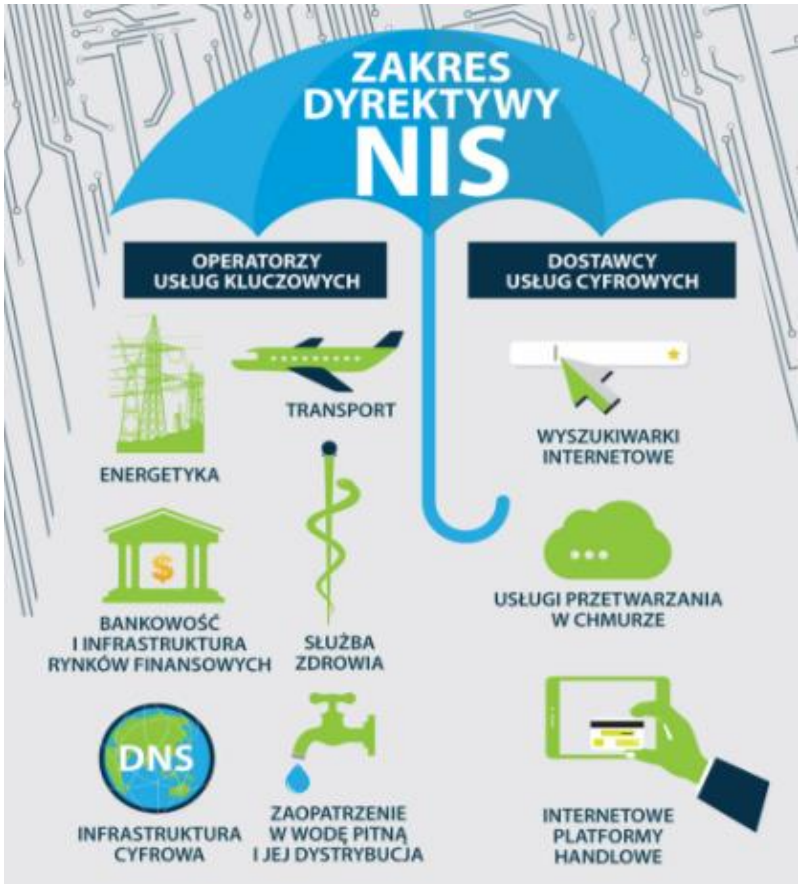
Założenia Dyrektywy NIS

- Dyrektywa nakłada obowiązki na operatorów usług kluczowych (przedsiębiorców z sektorów energetyki, transportu, bankowości i infrastruktury rynków finansowych, służby zdrowia, zaopatrzenia w wodę pitną, infrastruktury cyfrowej), **których zidentyfikować mają państwa członkowskie.**
- Państwa członkowskie miały 21 miesięcy na transpozycję przepisów dyrektywy do krajowych porządków prawnych oraz dodatkowe 6 miesięcy na identyfikację wspomnianych operatorów usług kluczowych.

UNIWERSYTET OPOLSKI

Założenia Dyrektywy NIS - obowiązki operatorów

- Operatorzy usług kluczowych zobowiązani będą do wprowadzenia środków ochrony (technicznych i organizacyjnych) zależnych od poziomu ryzyka.
- Na zidentyfikowanych operatorów nałożona zostanie także konieczność raportowania o incydentach.



Źródło: https://www.cybsecurity.org/

UNIWERSYTET OPOLSKI

Założenia Dyrektywy NIS

- Wyznaczeni przez Unię Europejską dostawcy usług cyfrowych, (operatorzy platform handlowych, wyszukiwarek i usług w chmurze) również będą zobowiązani, choć w mniejszym stopniu, do zapewnienia bezpieczeństwa swojej infrastruktury i zgłaszania poważnych incydentów organom krajowym.
- Państwa członkowskie będą musiały także utworzyć Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT). CERT Polska (przy Naukowej i Akademickiej Sieci Komputerowej) otrzymał od Ministerstwa Cyfryzacji mandat do reprezentowania Polski w sieci CSIRT, którą stworzono w 2017 roku na mocy dyrektywy NIS.

(Decyzją obowiązywała do lipca 2018 r.).

UNIWERSYTET OPOLSKI

Założenia Dyrektywy NIS

Na mocy nowych przepisów państwa zostały zobowiązane do przyjęcia krajowych strategii NIS.

Efektem tego założenia dyrektywy jest przyjęta 9 maja 2017 r. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022. stanowi kontynuację działań, podejmowanych w przeszłości przez administrację rządową

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 - 2022

UNIWERSYTET OPOLSKI

Strategia Cyberbezpieczeństwa RP - cel główny

Strategia przedstawia wizję cyberprzestrzeni RP w 2022 r., a także definiuje cel główny oraz cele szczegółowe związane z realizacją założonej wizji.

Cel główny Strategii Cyberbezpieczeństwa RP: *„zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych*.”

Pełnomocnik Rządu do spraw Cyberbezpieczeństwa

Rozporządzenie Rady Ministrów z dnia 16 marca 2018 r. w sprawie ustanowienia Pełnomocnika Rządu do spraw Cyberbezpieczeństwa

Na podstawie art. 10 ust. 1 i 4 ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz. U. z 2012 r. poz. 392 oraz z 2015 r. poz. 1064) zarządza się, co następuje:

§ 1. 1. Ustanawia się Pełnomocnika Rządu do spraw Cyberbezpieczeństwa, zwanego dalej „Pełnomocnikiem”.

2. Pełnomocnikiem jest **sekretarz stanu albo podsekretarz stanu w Ministerstwie Obrony Narodowej**.

§ 2. 1. Do zadań Pełnomocnika należy zapewnienie koordynacji działań oraz realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa.

Premier Mateusz Morawiecki w dn. 7.12.2018 r. powołał Karola Okońskiego, sekretarza stanu w Ministerstwie Cyfryzacji, na stanowisko Pełnomocnika Rządu do spraw Cyberbezpieczeństwa

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

Ustawa w zakresie swojej regulacji wdraża dyrektywę NIS

określa:

1) **organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu;**
2) **sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy;**
3) **zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.**

UNIWERSYTET OPOLSKI

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

Krajowy system cyberbezpieczeństwa obejmuje instytucje i podmioty wymienione w 20 punktach art. 4 ustawy, między innymi **operatorów usług kluczowych, dostawców usług cyfrowych,** Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego: **CSIRT GOV** – działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego, **CSIRT MON** –poziomie krajowym, prowadzony przez Ministra Obrony Narodowej, **CSIRT NASK** – działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – **Uczelnie wyższe** (np. zapisów pkt. 7 art. 4).

Obowiązki **operatorów usług kluczowych i dostawców usług kluczowych precyzują** odpowiednio rozdziały 3 i 4 ustawy.

Organem właściwe do spraw cyberbezpieczeństwa dla uczelni wyższych jest minister cyfryzacji (n.p. zapisów art. 41 ustawy).

UNIWERSYTET OPOLSKI

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa – obowiązki Uczelni

Obowiązki **podmiotów publicznych** **/Uczelni wyższych/** precyzuje rozdział 5 ustawy, obejmują one :

Art. 21. 1. Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, realizujący zadanie publiczne zależne od systemu informacyjnego **jest obowiązany do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa**.

Art. 22. 1. Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, realizujący zadanie publiczne zależne od systemu informacyjnego:

1) **zapewnia zarządzanie incydentem** w podmiocie publicznym;
2) **zgłasza incydent** w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, **CSIRT NASK** lub CSIRT GOV;

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa – obowiazki Uczelni

3) zapewnia obsługę incydentu w podmiocie publicznym i **incydentu krytycznego we współpracy z właściwym** CSIRT MON, **CSIRT NASK** lub CSIRT GOV, **przekazując niezbędne dane, w tym dane osobowe**;

4) zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, **dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami**, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej;

5) przekazuje do właściwego CSIRT MON, **CSIRT NASK** lub CSIRT GOV dane osoby, o której mowa w art. 21, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, **w terminie 14 dni od dnia jej wyznaczenia**, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.

UNIWERSYTET OPOLSKI

Zagrożenia w polskiej cyberprzestrzeni – Raporty Roczne 2017

- 1. CERT Polska obsłużył w 2017 roku rekordową liczbę **21 711**, **198 proc**. więcej przesłanych zgłoszeń w stosunku do roku 2016, w ich wyniku zarejestrowano łącznie **3 182** incydenty bezpieczeństwa (czasami kilka zgłoszeń z różnych źródeł dotyczyło tego samego incydentu) – wzrost o 68 %.
  2. Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL odnotował **28 281** zgłoszeń stanowi to znaczący wzrost (147%) względem 2016 roku, w którym zarejestrowano 19 954 zgłoszenia. Faktyczne naruszenie bezpieczeństwa teleinformatycznego instytucji miało miejsce w **5 819** przypadkach, co stanowi spadek (o 38%) względem 2016 roku, w którym faktycznych incydentów odnotowano 9 288.
  3. W 2017 roku w sieciach teleinformatycznych podmiotów uczestniczących w projekcie ARAKIS 2.0 GOV zanotowano **347 178** alarmów. Wśród zanotowanych alarmów: **62 292** alarmów miało priorytet pilny - niosło duże ryzyko przełamania zabezpieczeń, **30 505** alarmów miało priorytet wysoki tzn. wymagało wzmożonej uwagi w kontekście zagrożenia wskazanego w alarmie.

UNIWERSYTET OPOLSKI

Zagrożenia w polskiej cyberprzestrzeni – Raporty Roczne 2017

- CERT Polska wskazuje, iż dużym zagrożeniem jest w Polsce dystrybucją złośliwego oprogramowania (2,5-krotny wzrost liczby incydentów - z ok. 11 proc. do ok. 27 proc) różne warianty oprogramowania typu ransomware oraz tzw. bankery, czyli złośliwe oprogramowanie ukierunkowane na klientów bankowości elektronicznej i mobilnej. ***Głównymi drogami infekcji są wiadomości e-mail z załącznikami oraz exploit kity.***
- Najczęstszym typem incydentu są oszustwa komputerowe **zwłaszcza phishing**, stanowiący w 2017 r. ok. 41% wszystkich przypadków (spadek o 12%).
- Od kilku lat niezmiennie najczęściej atakowanymi usługami są usługi zapewniające zdalny dostęp do danego zasobu teleinformatycznego (SSH, telnet). Najczęstszym scenariuszem **próby przełamania zabezpieczeń** w tym przypadku są ataki słownikowe (brute-force). Dużą liczbę przepływów można zauważyć również na porcie 25/TCP należącym do usługi SMTP. Udany atak może spowodować w efekcie wysyłanie niechcianych wiadomości e-mail.

UNIWERSYTET OPOLSKI

Przykłady podejrzanych wiadomości pocztowych

Fakure: n 85798

Koper Radoslaw <sale@4seed.org>

Wysłano: pt. 2018-11-30 04:34

Do: iod

Wiadomość | WT329113.pdf.rar (1 KB)

Dobry wieczor,

W zalaczeniu skan prokury

Zegnaj

Koper Radoslaw
GRUPA OKNOPLAST

UNIWERSYTET OPOLSKI

Przykłady podejrzanych wiadomości pocztowych

11/30FV_6283

Od **Małgorzata Gawęda** Data **Dzisiaj 06:23**

Dzień dobry,
przesyłamy fakturę, którą znajdą Państwo w załączniku.
Z poważaniem,
Małgorzata Gawęda
"Effi" Sp. z o.o.

FS1130_5.rar (~938 B)

Faktura n 155/242

Artur Polgrabski [mail@staffingfortworth.com]

Wysłano: pt. 2018-12-07 09:09
Do: jacnaj

Witaj

Niepoprawnie zapłaciłeś rachunek na kwotę 28 pz. Pilne sprawdzenie danych http://hangouts.essaywriting.mobi/innova/vpn5.html?email=5dddd@f56af

Pozdrawiam

Artur Polgrabski

GK WOJAS

UNIWERSYTET OPOLSKI

Przykłady podejrzanych wiadomości pocztowych

for <najgebauer@uni.opole.pl>; Sat, 7 Jul 2018 18:14:59 +0000 (UTC)
Received: from rupavahini.lk (lihini.rupavahini.lk [203.94.67.129])
by fortimail.uni.opole.pl with ESMTP id w67IEwP7023648-w67IEwP8023648
for <iod@uni.opole.pl>; Sat, 7 Jul 2018 20:14:59 +0200
Received: from localhost (localhost.localdomain [127.0.0.1])
by rupavahini.lk (Postfix) with ESMTP id 64CF8B6C8A15
for <iod@uni.opole.pl>; Sat, 7 Jul 2018 23:55:26 +0530 (IST)

Oferujemy szybką pożyczkę na wyciągu, bez przedstawiania dokumentów finansowych, takich jak na przykład certyfikat, wyciągi.

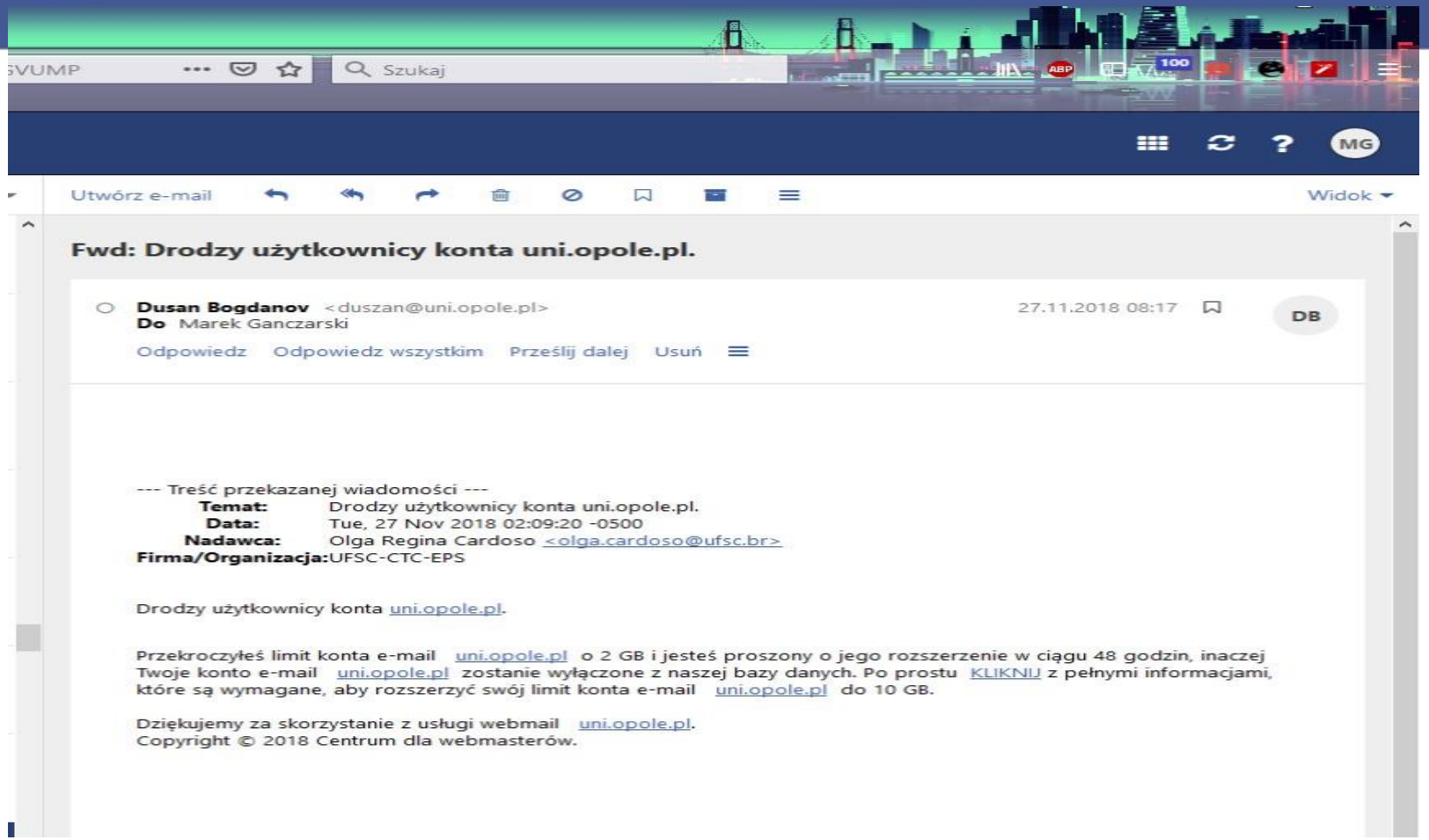
Zalety produktu:
- kwota pożyczki do 15 000 000,00 PLN
- Okres kredytowania do 300 miesięcy
- Nie ma weryfikacji dochodu u pracodawcy
- Wysokie przyznanie
- Szybki proces

Oferta skierowana jest zarówno do pośredników finansowych, jak i do klientów zainteresowanych pożyczką.

Skontaktuj się z nami, aby uzyskać więcej informacji: amaretta.i.tinney02@gmx.us

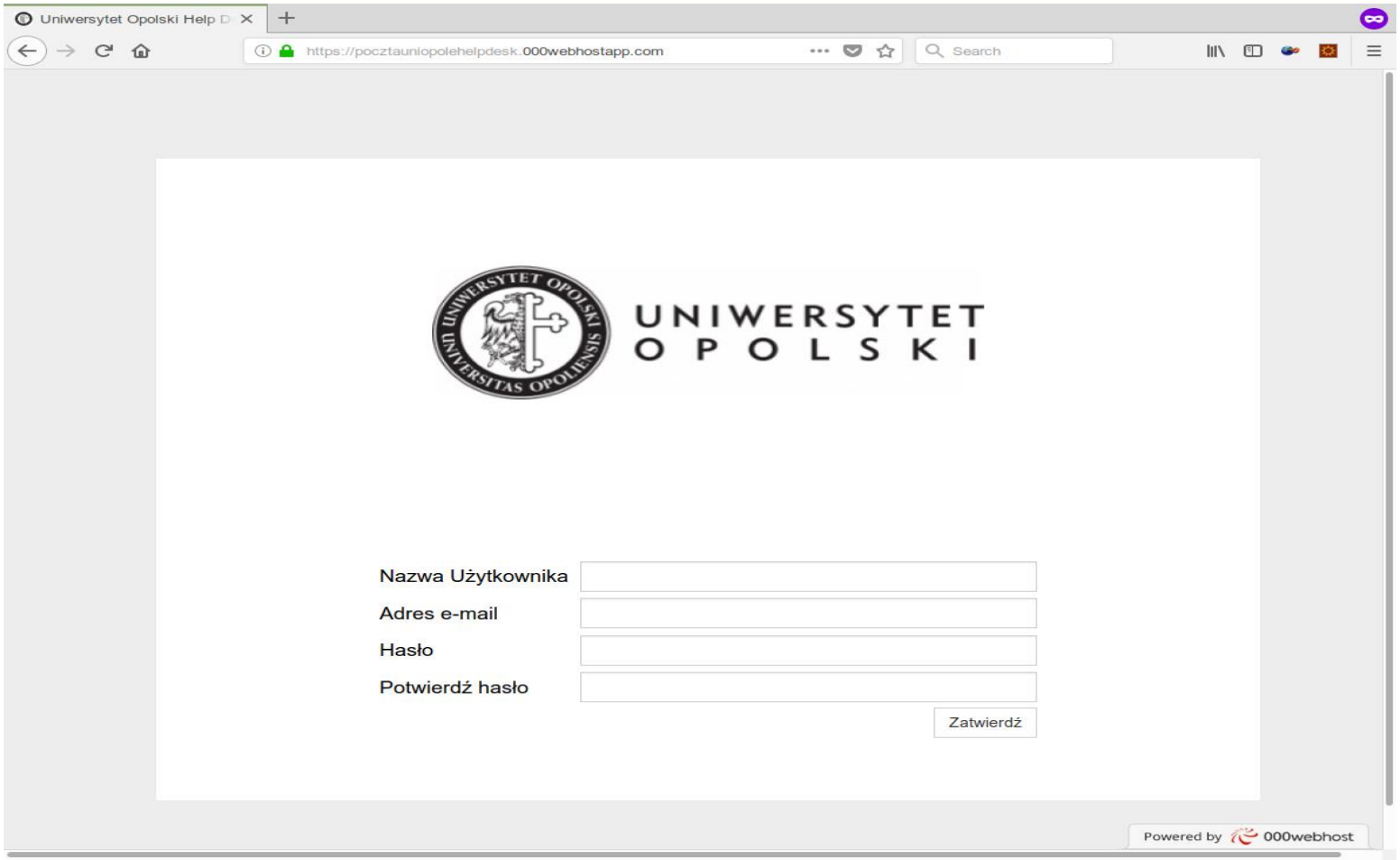
UNIWERSYTET OPOLSKI

Przykłady podejrzanych wiadomości pocztowych



UNIWERSYTET OPOLSKI

Przykłady podejrzanych wiadomości pocztowych



UNIWERSYTET OPOLSKI

Przykłady podejrzanych wiadomości pocztowych

Od: DHL Express (Poland) Sp. z o.o, 85110240229 <dmnmispnhkf@iran-firmware.ir>
Do: iod@uni.opole.pl
DW:
Temat: List Przewozowy dla Twojej przesylki, 85110240229

Dzien dobr,

Staralismy sie dostarczyc twoja przesylke 6.12.2018.

Konto / Numer kwitu: T85110240229
Wpłacający: iod@uni.opole.pl
Usluga (T): potwierdzenie odbioru
Prosimy o wplate: 8333,36 PLN
Statusu: Zawiadomienie wyslane

Pobierz faktura <http://filtroco.com/fnzoro/jubtmfeq.php>

Z powazaniem,
DHL Express (Poland).

UNIWERSYTET OPOLSKI

Katalog zagrożeń dla systemów teleinformatycznych Uczelni.

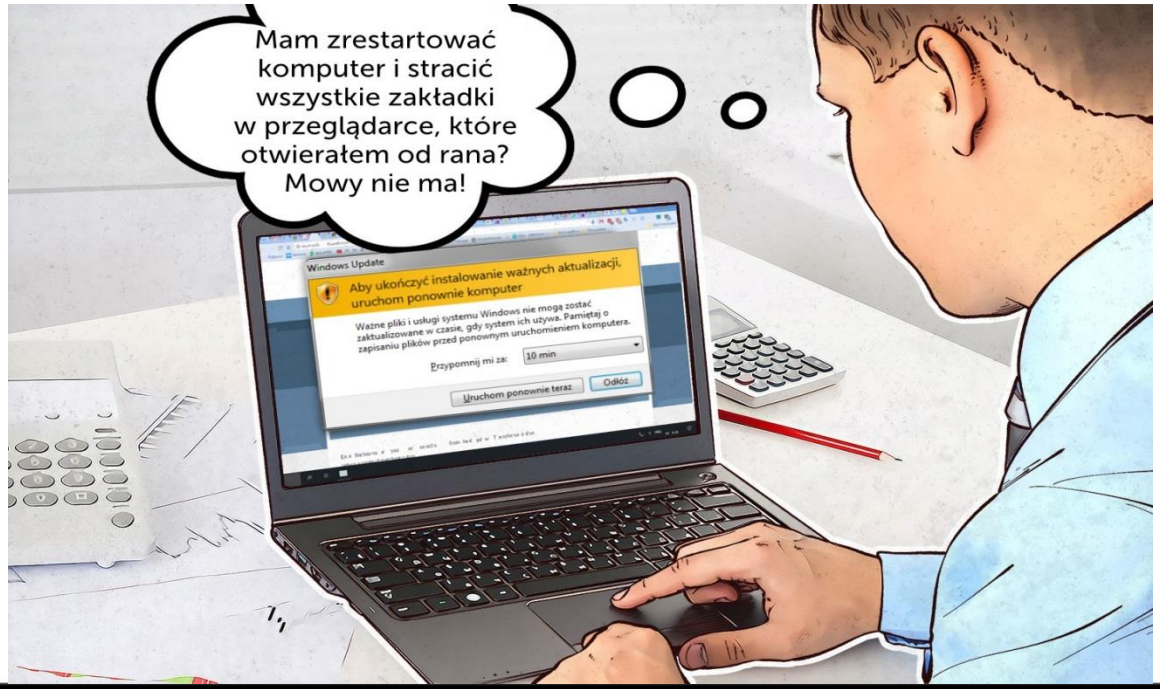
Działania celowe:

- ❑ oprogramowanie złośliwe;
- ❑ przełamanie zabezpieczeń;
- ❑ publikacje w sieci Internet;
- ❑ gromadzenie informacji;
- ❑ sabotaż komputerowy;
- ❑ czynnik ludzki;
- ❑ cyberterroryzm.

Katalog zagrożeń dla systemów teleinformatycznych Uczelni.

Działania niecelowe:

- ❑ wypadki i zdarzenia losowe;
- ❑ czynnik ludzki.



Źródło: https://plblog.kaspersky.com/

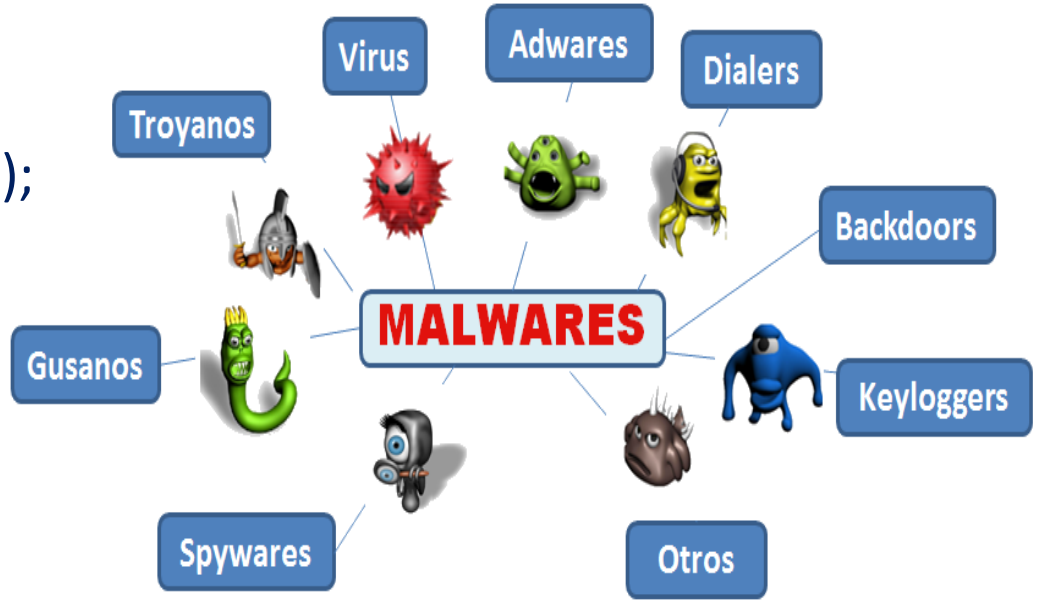
UNIWERSYTET OPOLSKI

Złośliwe oprogramowanie (z ang. Malware)

Oprogramowanie, którego działanie powoduje szkody dla użytkownika.

Do szkodliwego oprogramowania zalicza się m. in:

- wirusy;
- robaki;
- konie trojańskie (trojany);
- spyware;
- adware;
- rootkit;
- spam.



UNIWERSYTET OPOLSKI

Wirusy

Programy, które zarażają inne programy poprzez dodanie do nich kodu wirusa, **w celu uzyskania dostępu do komputera** przy uruchamianiu zainfekowanego pliku. Ta prosta definicja przedstawia podstawowe działanie wirusa - infekcję. Szybkość rozprzestrzeniania wirusów jest mniejsza niż robaków.

Źródło: http://www.uczen.tokraw.pl/

UNIWERSYTET OPOLSKI

Robaki

Szkodliwe oprogramowanie, które do rozprzestrzeniania się wykorzystuje zasoby sieci. Klasa ta nazwana została robakami z powodu jej specyficznego działania przypominającego “pełzanie” z komputera na komputer przy użyciu sieci, poczty elektronicznej i innych kanałów informacyjnych. Dzięki temu tempo rozprzestrzeniania się robaków jest bardzo szybkie.

Źródło: http://www.komputerswiat.pl/

UNIWERSYTET OPOLSKI

Ransomware (od ransom = okup i malware)

Rodzaj złośliwego oprogramowania, które uniemożliwia użytkownikowi dostęp do jego danych (najczęściej przez zaszyfrowanie), a do przywrócenia go wymaga wpłacenia okupu.

Źródło: https://www.linkedin.com/

UNIWERSYTET OPOLSKI

Phishing

W tradycyjnym rozumieniu tego słowa phishing oznacza podszywanie się (przede wszystkim z wykorzystaniem poczty elektronicznej i stron WWW) pod znane marki celem wyłudzenia wrażliwych danych.

Źródło: https://www.avast.com/

UNIWERSYTET OPOLSKI

Exploit kit

Rodzaj złośliwego oprogramowania wykonywanego na serwerze WWW, starającego się wykorzystać lukę w oprogramowaniu klienckim użytkownika odwiedzającego stronę (np. w przeglądarce WWW, wtyczkach do odtwarzania wideo) do wykonania poleceń na jego komputerze.

Źródło: https://www.scmagazine.com/

Trojan

Rodzaj złośliwego oprogramowania, w którym złośliwy kod jest częścią innego programu lub dokumentu, który wygląda na nieszkodliwy.

Źródło: http://www.komputerswiat.pl/

UNIWERSYTET OPOLSKI

Bot (inaczej: zombie)

Komputer, nad którym, dzięki działającemu na nim złośliwemu oprogramowaniu, pełną kontrolę posiada inna osoba niż właściciel.

Botnet – wiele botów zarządzanych wspólnie przez jedną osobę lub grupę osób.

Źródło: https://linuxsecurityblog.com/

UNIWERSYTET OPOLSKI

Przykłady wykorzystania złośliwego oprogramowania do uderzenia w infrastrukturę krytyczną

W 2010 r. po raz pierwszy wykryto „**Stuxnet**” - malware, który wielu uważa za przełomowy w dziejach IT.

Program wycelowany został w ściśle określoną instalację komputerową (sterowniki PLC Siemensa wykorzystywane w wirówkach do wzbogacania uranu). Przypuszcza się, że głównym celem ataku Stuxnet-a był Iran i najprawdopodobniej jego przemysł nuklearny. W grudniu 2010 prezydent Iranu Mahmud Ahmadineżad przyznał, że wirus spowodował "problemy w niewielkiej liczbie wirówek używanych do wzbogacania uranu”. Chińska agencja Xinhua poinformowała, że obecność Stuxnet-a stwierdzono w komputerach 115 krajów, a w samych Chinach miał zainstalować się na 6 milionach jednostkach roboczych. Mimo takiego spektrum działania Stuxnet wyrządził szkody tylko w jednym kraju – w Iranie.

UNIWERSYTET OPOLSKI

Ransomware Petya uderza w Ukrainę

(27 czerwca 2017 r.)

Atak hakerów sparaliżował komputery rządu Ukrainy oraz wielu tamtejszych banków, firm transportowych i przedsiębiorstw, a nawet elektrownię w Czarnobylu. Ofiarami ataku padły również polskie firmy współpracujące z ukraińskimi, które były połączone z zainfekowaną siecią.

Ekran infekcji Petyą

UNIWERSYTET OPOLSKI

Mechanizm ataku ransomware Petya

Źródłem ataku było popularne oprogramowanie "M.E.doc", z którego korzysta wiele firm na Ukrainie do zarządzania dokumentami (oprogramowanie jest odpowiednikiem polskiego oprogramowania Płatnik). Sprawca ataku podmienił aktualizację na złośliwą wersję. Poprzez funkcję automatycznej aktualizacji zaciągnięta została wersja złośliwa, którą następnie uruchomiono w sieciach ukraińskich firm.

UNIWERSYTET OPOLSKI

Mechanizm ataku ransomware Petya

w 2017 r. zaawansowanego ataku ukierunkowanego na polski sektor bankowy dokonała (najprawdopodobniej) północnokoreańska grupa

Lazarus, znana z próby kradzieży miliarda dolarów z banku centralnego w Bangladeszu w 2016 roku.

Do infekcji ofiar wykorzystano witrynę Komisji Nadzoru Finansowego, czyli instytucję cieszącą się zaufaniem publicznym.

2017 r to także globalne ataki oprogramowania szyfrującego **Wannacry i NotPetya.**

UNIWERSYTET OPOLSKI

WANNACRY OUTBREAK

UNIWERSYTET
OPOLSKI

Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

   X86GcZ-7PRNBE-3mNFMp-z88VnG-uF5nhF-4wzxwZ-XdNrr6-FYG89D-xk4rNz-9yPzJS

If you already purchased your key, please enter it below.
Key: _

UNIWERSYTET OPOLSKI

Podstawowe działania zabezpieczające przed cyberatakami

- inwentaryzacja autoryzowanego i nieautoryzowanego sprzętu oraz oprogramowania;
- utwardzająca konfiguracja sprzętu i oprogramowania na laptopach, stacjach roboczych i serwerach oraz urządzeń sieciowych takich jak zapory sieciowe i rutery;
- utrzymywanie i analiza dzienników bezpieczeństwa;

UNIWERSYTET OPOLSKI

Podstawowe działania zabezpieczające przed cyberatakami

- kontrola używania uprawnień administracyjnych;
- ochrona przed programami i kodami złośliwymi;
- kontrola urządzeń bezprzewodowych;
- przeciwdziałanie wyciekowi danych;
- reagowanie na incydenty;
- szkolenia z zakresu bezpieczeństwa teleinformatycznego.

Zapobieganie atakom na systemy informatyczna

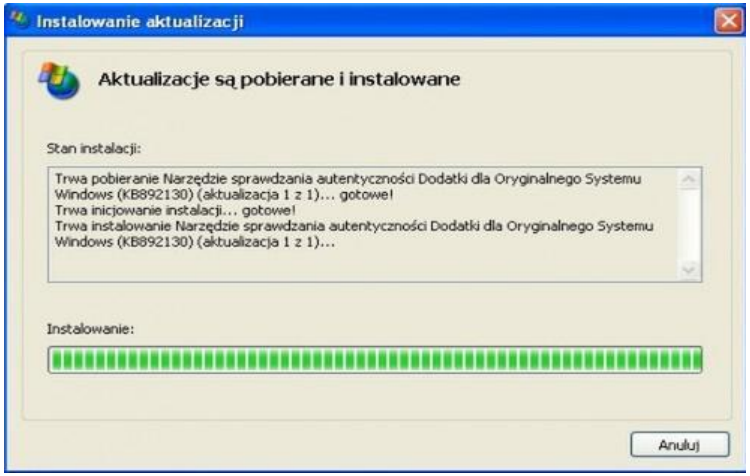
1. Białe listy aplikacji.

Technika ta polega na blokowaniu obcych aplikacji na komputerze i dopuszczeniu uruchamiania tylko autoryzowanych.

Źródło: https://www.pcmatic.com/whitelist

2. Aktualizowanie systemu operacyjnego.

Należy systematycznie aktualizować system operacyjny i zainstalowane na nim oprogramowanie, aby załatać nowo wykryte luki, które mogłyby zostać wykorzystane przez różne zagrożenia.



Źródło: http://gadzetomania.pl/

3. Ograniczenie dostępu do uprawnień administratora.

Administrator posiada dostęp do wszystkich plików na dyskach twardych oraz do wszystkich gałęzi rejestru. Kiedy podczas surfowania po Internecie z wykorzystaniem konta administratora do systemu przedostaje się wirus i zaczyna działać niepostrzeżenie w tle, dostaje on takie same uprawnienia do wykonywania zmian w systemie jakie ma administrator.

Źródło: https://www.jsweb.uk/

4. Aktualizowanie aplikacji (Adobe Reader, Flash Player, Java) oraz przeglądarek internetowych.

Nowsze przeglądarki lepiej chronią przed wirusami, oszustwami, wyłudzeniami i innymi zagrożeniami. Nieaktualne przeglądarki zawierają luki w zabezpieczeniach, które usuwane są w aktualizacjach.

Źródło: https://browser-update.org/

5. Hasła i zabezpieczenie dostępu do systemu.

Używanie **silnych** oraz unikalnych haseł **dla każdego** z urządzeń i kont online.

Włączenie weryfikacji dwuetapowej (biometria, token).

Źródło:www.credy.pl/jak-stworzyc-silne-skuteczn

6. Kopie zapasowe

Ważnych dla użytkownika danych i systemu operacyjnego. Przechowywanie kopii zapasowych zarówno w chmurze jak i poza siecią.

7. Użytkownik systemu

Najłatwiejszym sposobem na ominięcie nawet najbardziej zaawansowanych zabezpieczeń jest zaatakowanie użytkownika systemu.

Zachowanie czujności, wiedza dotycząca zagrożeń i zdrowy rozsądek są w stanie zapobiec większości ataków na systemy informatyczne.

Źródło: https://publicdomainvectors.org

UNIWERSYTET OPOLSKI

Akty prawne dotyczące ochrony cyberprzestrzeni

- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.
- Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej z 2013 r.;
- **Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej** z dnia 5 listopada 2014 r.
- Doktryna Cyberbezpieczeństwa RP z 22 stycznia 2015 r.
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 (zwana Dyrektywą NIS (Network and Information Systems Directive)) z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.
- **Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej** na lata 2017 – 2022.

UNIWERSYTET OPOLSKI

Akty prawne dotyczące ochrony cyberprzestrzeni

- **<u>Ustawa z dnia 5 lipca 2018 r o krajowym systemie cyberbezpieczeństwa</u> (Dz.U. 2018 poz. 1560)**
- Rozporządzenie Ministra Cyfryzacji z dnia 10 września 2018 r. w sprawie warunków organizacyjnych i technicznych dla **podmiotów świadczących usługi z zakresu cyberbezpieczeństwa** oraz wewnętrznych struktur organizacyjnych **operatorów usług kluczowych** odpowiedzialnych za cyberbezpieczeństwo (Dz.U z 2018 poz. 1806).
- Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu **usług kluczowych oraz progów istotności** skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz.U. 2018 poz. 1806).
- Rozporządzenie Rady Ministrów z dnia 2 października 2018 r. w sprawie zakresu działania oraz trybu pracy **Kolegium do Spraw Cyberbezpieczeństwa** (Dz.U. 2018 poz. 1952).
- Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999).
- Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz.U. 2018 poz. 2080)
- Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie **progów uznania incydentu za poważny** (Dz.U. 2018 poz. 2180).

UNIWERSYTET OPOLSKI

Bibliografia

- Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z dnia 5 listopada 2014 r..
- Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022.
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.
- Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej z 2013 r..
- Doktryna Cyberbezpieczeństwa RP z 22 stycznia 2015 r..
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 (zwana Dyrektywą NIS (Network and Information Systems Directive)) z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

UNIWERSYTET OPOLSKI

Bibliograia

- https://www.proxymo.pl/blog/2016/08/cyberbezpieczenstwo/.
- https://www.asd.gov.au/publications/protect/top_4_mitigations.ht.
- Krajobraz bezpieczeństwa polskiego Internetu, 2017, Raport roczny z działalności CERT Polska.
- CERT.GOV.PL - Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2017 roku
- https://mc.gov.pl/.
- http://www.komputerswiat.pl/nowosci/bezpieczenstwo/2017/26/kolejny-globalny-atak-ransomware-petya-zaatakowal-takze-polske.aspx.
- https://itsecurityenthusiast.wordpress.com/2010/10/07/wirus-stuxnet-usuwanie-infekcji/.
- https://www.cert.pl/publikacje/
- https://csirt.gov.pl/