

Polityka bezpieczeństwa

dr inż. Krzysztof Cabaj

Plan wykładu

- Wstęp
- Bezpieczeństwo na poziomie organizacji
- Bezpieczeństwo na poziomie kraju, świata
- Podsumowanie

Bezpieczeństwo

- „Security is a process, not a product.”

Bruce Schneier 2000

- Produkty zapewniają nam pewne bezpieczeństwo, ale w dynamicznie zmieniających się warunkach w celu zapewnienia realnego bezpieczeństwa trzeba w organizacji wdrożyć cały proces wykrywania, reakcji i wprowadzania zmian
- Duża część udanych ataków związana jest ze zmianami w otoczeniu

Przykład

- Ataki robaków na początku lat 2000
- W dużej mierze ograniczone przez zastosowanie zapór ogniowych
- Rozpoczęcie ataków wykorzystujących błędy w przeglądarkach – na które zapory ogniowe w dużej mierze są nieskuteczne

Przykład

- Ale z drugiej strony
- Atak związany z „przepełnieniem bufora” jest znany od lat `70 ... a stale odkrywane są kolejne, nowe aplikacje, które zostały zaatakowane z wykorzystaniem tego błędy

Plan wykładu

- Wstęp
- Bezpieczeństwo na poziomie organizacji
 - Polityka bezpieczeństwa
 - Szacowanie ryzyka
- Bezpieczeństwo na poziomie kraju, świata
- Podsumowanie

Polityka bezpieczeństwa

- „Polityka bezpieczeństwa jest dokumentem w którym jasno i zwięźle wyrażono, co mają osiągnąć mechanizmy zabezpieczeń”

R.Anderson Inżynieria Zabezpieczeń

Polityka bezpieczeństwa – przykład negatywny !!!

Polityka bezpieczeństwa Megacorp. Inc.

1. Niniejszą politykę zaaprobowало kierownictwo firmy.
2. Cały personel powinien się stosować do zasad niniejszej polityki.
3. Dane powinno się udostępniać tylko osobom, dla których stanowią „wiedzę konieczną”.
4. Wszelkie naruszenia zasad niniejszej polityki należy niezwłocznie zgłaszać służbom ochrony.

Polityka bezpieczeństwa – przykład pozytywny

- „Każde uznanie musi mieć odpowiadające mu i równe obciążenie, a wszystkie transakcje powyżej 1000 USD muszą być autoryzowane przez kierownika”.
- „Kontrola dostępu: Każdy identyfikowalny zapis kliniczny będzie oznaczony listą kontroli dostępu zawierającą osoby i grupy osób, które mogą go czytać i dopisywać do niego dane. System będzie zapobiegał uzyskiwaniu dostępu do zapisu przez osoby, których nie ma na liście kontroli dostępu”.

Polityka bezpieczeństwa – tworzenie i efekty

- Na początku definiujemy „model zagrożeń” – czyli jakie zagrożenia i ataki bierzemy pod uwagę
- Potem tworzymy „politykę bezpieczeństwa”, która definiuje co będziemy chronili i zarys tego w jaki sposób
- Na końcu wybieramy odpowiednie „mechanizmy zabezpieczeń” aby spełnić wymagania opisane w polityce bezpieczeństwa

Szacowanie ryzyka

- Główne pytanie co chronić i ile wydać na ochronę
- Dwa podejścia
 - ilościowe – inwentaryzujemy wszystkie zasoby, i oceniamy ile będzie kosztowała nas jego utrata/atak
 - jakościowe – stosowane do dużych organizacji jak miasta czy państwa gdzie nie jest możliwa inwentaryzacja wszystkich zasobów

Podejście ilościowe - SLE

- Definicje
 - SLE (ang. Single Loss Expectancy) – koszt jednego zdarzenia, liczony ze wzoru $SLE = AV * EF$
 - AV (ang. Asset Value) – wartość zasobu
 - EF (ang. Exposure Factor) – współczynnik zniszczenia

Przykłady liczenia SLE

- Kradzieże kasjerów
 - $AV = 1\,000\,000$ PLN wartość pieniędzy w oddziale
 - $EF = 0.005\%$ - procentowa strata jednej kradzieży
 - $SLE = 1\,000\,000 * 0,00005 = 50$ PLN
- Zalanie serwerowni
 - $AV = 10\,000\,000$ PLN – koszt sprzętu w serwerowni
 - $EF = 50\%$
 - $SLE = 10\,000\,000 * 0,5 = 5\,000\,000$ PLN

Podejście ilościowe - ALE

- Definicje
 - ALE (ang. Annual Loss Expectancy) – roczna oczekiwana strata, liczona ze wzory
 $ALE = SLE * ARO$
 - ARO (ang. Annualized Rate of Occurrence) – „roczna liczba zdarzeń”

Przykłady liczenia - ALE

- Kradzieże kasjerów
 - $SLE = 50 \text{ PLN}$
 - $ARO = 10\,000$
 - $ALE = SLE * ARO = 500\,000$
- Zalanie serwerowni
 - $SLE = 5\,000\,000$
 - $ARO = 1\% - \text{woda stuletnia}$
 - $ALE = 5\,000\,000 * 0,01 = 50\,000$

Plan wykładu

- Wstęp
- Bezpieczeństwo na poziomie organizacji
- Bezpieczeństwo na poziomie kraju, świata
 - CERT
 - Podejście do ujawniania błędów
 - Wolontariat/dzielenie się informacjami/ Open-Source Intelligence (OSINT)
- Podsumowanie

CERT

- 2 października 1988 w Internecie zostaje wypuszczony robak Morrisa
- Szacuje się, że zainfekował 10% (około 6000) podłączonych wtedy maszyn
- Jednym z efektów tego działania było powołanie przez DARPA CERT/CC (Computer Emergency Response Team/Coordination Center)

CERT

- CERT/CC powstał przy Carnegie Mellon University (CMU) w Pittsburgu
- Określenie CERT jest zarejestrowanym znakiem CMU i nazwa podlega licencjonowaniu
- Podobną rolę w innych organizacjach bez potrzeby licencjonowania pełnią zespoły CSIRT (ang. Computer Security Incident Response Team)

CERT-y w Polsce

- Do lipca 2016 w Polsce działały trzy zespoły CERT
 - cert.pl – przy NASK
 - cert.orange.pl – przy Orange
 - Rządowy Zespół Reagowania na Incydynty Komputerowe - cert.gov.pl – prowadzony przez ABW

Narodowe Centrum Cyberbezpieczeństwa

- 4 lipca 2016 zostało oficjalnie otwarte Narodowe Centrum Cyberbezpieczeństwa (NCC, NC Cyber) działające w ramach NASK
- W ramach jednego z zespołów ma powstać CERT Narodowy
- NC Cyber ma być forum wymiany informacji pomiędzy instytucjami państwowymi a biznesem
- Umowy o współpracy z NCC podpisały między innymi Polkomtel, Orange, T-Mobile i Netia

Narodowe Centrum Cyberbezpieczeństwa

NC CYBER

BADANIA I ROZWÓJ

TELEKOMUNIKACJA

PROJEKTY STRATEGICZNE

EDUKACJA

REJESTR .PL

NC CYBER

NC Cyber - Narodowe Centrum Cyberbezpieczeństwa

Narodowe Centrum Cyberbezpieczeństwa (NC Cyber) działa w strukturze NASK. Głównym zadaniem Centrum jest dbałość o bezpieczeństwo cyberprzestrzeni RP m.in. poprzez opracowywanie narodowych planów ochrony. NC Cyber współpracuje w tym zakresie z administracją, biznesem oraz ze środowiskiem naukowym. Centrum funkcjonuje jako ośrodek wczesnego ostrzegania, który działając w systemie 24/7/365 monitoruje i zarządza trybem informowania o zagrożeniach sieciowych. Centrum zajmuje się również obsługą zgłoszeń szkodliwych i nielegalnych treści ([Dyżurnet.pl](https://dyzurnet.pl)).



Stan aktualny

- Zgodnie z dyrektywą NIS i jej implementacją w prawie polskim (ustawa z 5 lipca 2018) powołane zostają trzy zespoły CSIRT poziomu krajowego :
 - CSIRT NASK - www.nask.pl/pl/dzialalnosc/csirt-nask/ ,
 - CSIRT GOV - csirt.gov.pl ,
 - CSIRT MON - csirt-mon.wp.mil.pl .

Podejście do ujawniania błędów

- Błędy w aplikacjach były, są i będą
- Pytanie w jaki sposób reagować na ich wyszukiwanie i w jaki odpowiedzialny sposób informować o nich
- Niestety częsty organizacja zamiast skorzystać z informacji i szybko poprawić błąd ... (prawnie) atakują osobę wykrywającą błąd i informującą właściciela
- To odstrasza ludzi uczciwych ... a przestępcy i tak będą atakowali systemy

Odpowiedzialne ujawnienie informacji

- Co może zrobić osoba, która wykryła błąd
 - Poinformować producenta i w pełni współpracować z nim, często ze strony firmy była „słaba” współpraca i trwało to tygodnie, miesiące, lata ...
 - Zastosować pełne ujawnienie (ang. Full Disclosure) – podać do publicznej wiadomości wszystkie informacje bez wcześniejszego informowania
 - Zastosować odpowiedzialne ujawnienie, najpierw poinformować producenta, ale ujawnić informacje publicznie po określonym, rozsądnym czasie

Płacenie za błędy

- Niektóre firmy (Microsoft, Google) zastosowały inną politykę, wprowadzając jasną ścieżkę informowania i reakcji na wykryte błędy, plus dodatkowo przy spełnieniu odpowiednich warunków płacą za wykryte, tak zwane Bug Bounty
- Podobną inicjatywę zaproponował i sponsoruje Facebook oraz Microsoft, a dotyczy ona produktów o otwartym kodzie

The Internet Bug Bounty

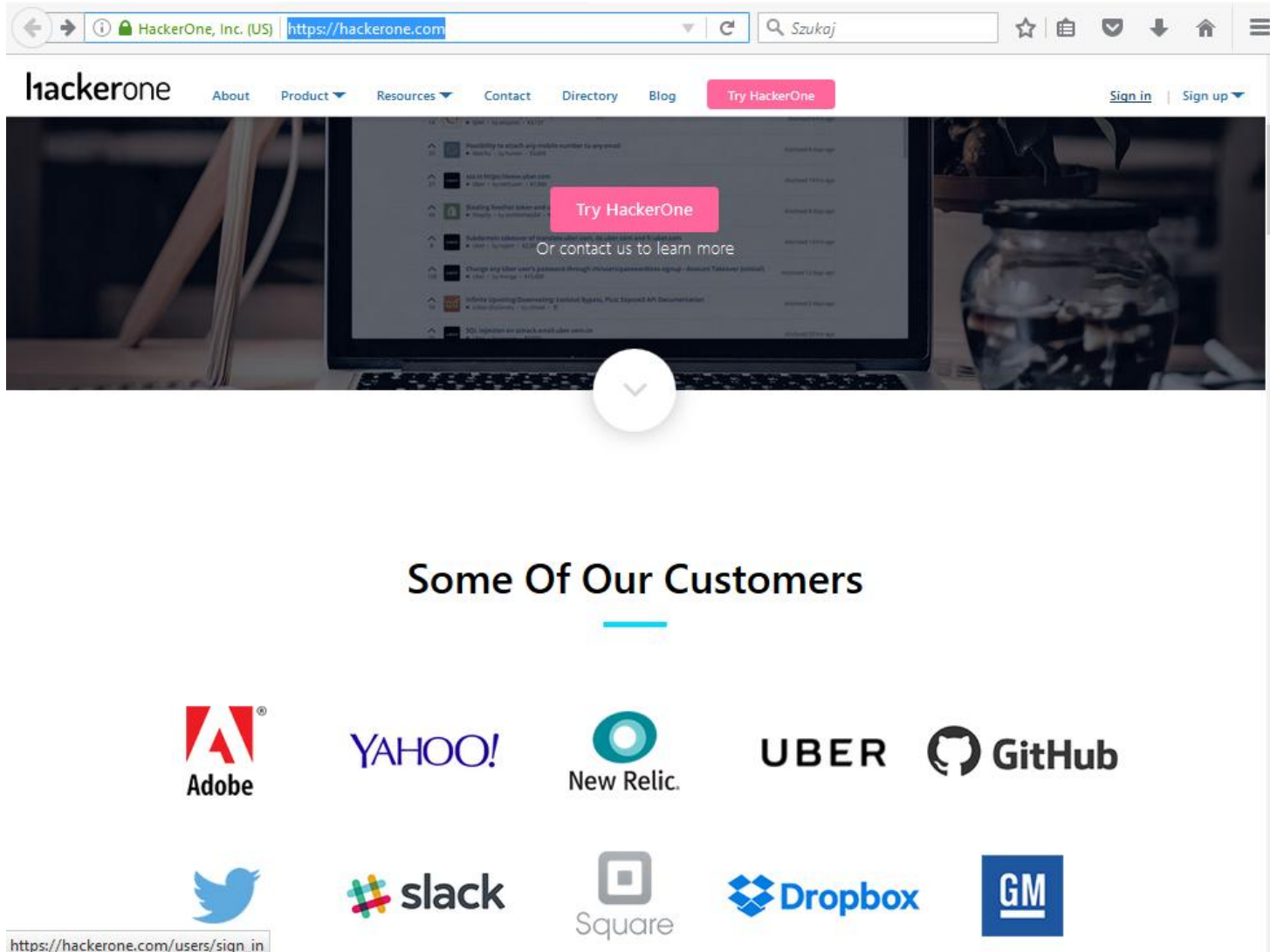


<https://hackerone.com/> (strona archiwalna)

Firma HackerOne

- Popularność programów Bug Bounty była inspiracją do powstania firmy HackerOne (<https://hackerone.com/>), której celem jest łącznie „dobrych hackerów” (White Hats) z potencjalnymi klientami
- Firma także świadczy usługi polegające na obsłudze zgłoszeń oraz wstępnej ich analizie

Firma HackerOne



Wolontariat/dzielenie się informacjami/ Open-Source Intelligence (OSINT)

- Przestępcy aktualnie „wygrywają” ponieważ otwarcie dzielą się wiedzą
- Niestety firmy, organizacje, Rządy Państw niechętnie dzielą się informacjami o atakach – z powodu utraty „dobrego” imienia
- W sieci istnieją pewne ogólnie dostępne zasoby związane z udostępnianiem informacji i analiz dotyczących cyberbezpieczeństwa
- *Zachęcam do umieszczania w tych źródłach (gdzie jest taka możliwość) wykrytych próbek malware-u*

Sybiektywna, osobista lista źródeł

- Lista interesujących witryn i systemów
 - <https://www.dshield.org/>
 - <https://malwr.com/>
 - <https://ransomwaretracker.abuse.ch/tracker/>
 - <http://www.malware-traffic-analysis.net>
 - <https://www.virustotal.com/>

https://www.dshield.org/

Threat Level: **GREEN**

Hand



SANS ISC InfoSec Forums

Keyword, Domain, Port, IP or Header

Search

Email

[Sign Up for Free!](#)

Contact Us

Diary

Podcasts

Jobs

News

Tools

Data

FORUMS

[Auditing](#)

[Diary Discussions](#)

[Forensics](#)

[General Discussions](#)

[Industry News](#)

[Network Security](#)

[Penetration Testing](#)

[Software Security](#)

[← Next Thread](#) [Previous Thread →](#)

Searching for malspam



Introduction

About a week ago, I stopped seeing the daily deluge of malicious spam (malspam) distributing Dridex banking trojans or Locky ransomware. Before this month, I generally noticed multiple waves of Dridex/Locky malspam almost every day. This malspam contains attachments with zipped .js files or Microsoft Office documents designed to download and install the malware.

I haven't found much discussion about the current absence of Dridex/Locky malspam. Since the actor(s) behind Dridex started distributing Locky in back in February 2016 [1], I can't recall any lengthy absence of this malspam.



MalwareTech

@MalwareTechBlog

Dridex and Locky haven't been active on twitter, Necurs C&Cs down, wonder if some of the guys got hit in the recent arrests?

RETWEETS

15

LIKES

19



Brad



214 POSTS

ISC HANDLER

http://www.malware-traffic-analysis.net

www.malware-traffic-analysis.net/2016/06/09/index2.html

Szukaj

MALWARE-TRAFFIC-ANALYSIS.NET

2016-06-09 - BOLETO MALSPAM


From: COBRACAPI Cobranças <notificacao@0.s1x49kk0.com.br>
Reply-To: COBRACAPI Cobranças <notificacao@0.s1x49kk0.com.br>
Date: Wednesday, June 8, 2016 at 9:32 AM
To: <handlers@sans.org>
Subject: Enc.: Boleto em Atraso COBRACAPI
Resent-Date: Thu, 9 Jun 2016 16:34:12 GMT



Bom dia
Estamos enviando boleto mes de maio atualizado.
Aguardamos o pagamento caso o não pagamento da divida acarretara multa e juros de mora de 5% (cinco por cento) ao mês.
Boleto Num: 4744648644

https://malwr.com/

[Home](#) [Analyses](#) [Search](#) [Submit](#) [About](#) [kcabaj](#)

malwr 

[Quick Overview](#)
[Static Analysis](#)
[Behavioral Analysis](#)
[Network Analysis](#)
[Dropped Files](#)
[Comment Board \(0\)](#)

[Domains \(3\)](#) [Hosts \(4\)](#) [HTTP \(7\)](#) [IRC \(0\)](#) [SMTP \(0\)](#)

HTTP Requests

URI	DATA
http://195.154.69.90/upload/_dispatch.php	<pre>POST /upload/_dispatch.php HTTP/1.1 Accept: */* Accept-Language: en-us Referer: http://195.154.69.90/upload/ x-requested-with: XMLHttpRequest Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip, deflate Cache-Control: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022) Host: 195.154.69.90 Content-Length: 826 Connection: Keep-Alive</pre>

https://ransomwaretracker.abuse.ch/tracker/

ransomware tracker						Home	Mitigation
General filters: Remove filter (Show all) Online hosts							
Filter by threat: Botnet C&Cs Payment Sites Distribution Sites							
Filter by malware: TeslaCrypt CryptoWall TorrentLocker PadCrypt Locky CTB-Locker FAKBEN PayCrypt DMALocker							
Dateadded (UTC)	Threat	Malware	Host (?)	Domain Registrar (?)	IP address (ASN, Country)		
2016-06-09 08:31	Payment Site	TorrentLocker	● de2nuvwegoo32oqv.tortodorf.li		(n/a)		
2016-06-08 07:23	Payment Site	TorrentLocker	● stgg5jv6mqiibmax.torclasses.li		(n/a)		
2016-06-08 07:09	Payment Site	TorrentLocker	● de2nuvwegoo32oqv.tordrims.li		(n/a)		
2016-06-06 08:41	Distribution Site	Locky	● bogialai.com	P.A. VIET NAM COMPANY LIMITED	125.253.121.16 (🇻🇳 Vietnam)		
2016-06-06 06:48	Botnet C&C	Locky	● bddadevlpkwrmud.xyz	Namecheap	208.100.26.234 (🇺🇸 United States)		
2016-06-05 08:53	Botnet C&C	DMALocker	● www.actioncompass.online	Namecheap	5.8.63.31 (🇷🇺 Russian Federation)		
2016-06-04 10:10	Payment Site	TorrentLocker	● de2nuvwegoo32oqv.torfigth.li		(n/a)		
2016-06-02 23:32	Botnet C&C	Locky	● 51.255.107.20		51.255.107.20 (🇫🇷 France)		
2016-06-02 23:32	Botnet C&C	Locky	● 82.196.6.154		82.196.6.154 (🇳🇱 Netherlands)		
2016-06-01 14:28	Distribution Site	Locky	● auburnac.org	Wild West Domains, LLC	23.229.160.9 (🇺🇸 United States)		
2016-06-01 14:28	Distribution Site	Locky	● davidcandy.website.pl	Consulting Service Sp. z o.o.	193.218.152.119 (🇵🇱 Poland)		
2016-06-01 14:28	Distribution Site	Locky	● nitalholdings.com	GODADDY.COM, LLC	192.186.196.34 (🇺🇸 United States)		
2016-06-01 14:28	Distribution Site	Locky	● f7space.zg5.ru	REGTIME-RU	91.223.216.57 (🇺🇦 Ukraine)		
2016-06-01 14:28	Distribution Site	Locky	● nuzzledot.com	GODADDY.COM, LLC	23.229.147.2 (🇺🇸 United States)		
2016-06-01 14:28	Distribution Site	Locky	● tipsforall.in	GoDaddy.com, LLC (R101-AFIN)	43.242.215.197 (🇮🇳 India)		

https://www.virustotal.com/

[Społeczność](#)[Statystyki](#)[Dokumentacja](#)[FAQ](#)[O VirusTotal](#)[Polski](#)[Dołącz do społeczności](#)

VirusTotal to darmowy serwis, który **analizuje podejrzone pliki i adresy URL** oraz umożliwia szybkie wykrycie wirusów, robaków, trojanów i innych typów złośliwego oprogramowania.

[Plik](#)[URL](#)[Szukaj](#)

Plik nie został wybrany

Wybierz plik

Maksymalna wielkość pliku: 128MB

Poprzez kliknięcie na 'Przeskanuj', akceptujesz [zasady serwisu](#) i pozwalasz VirusTotal, aby współdzielić ten plik z całą społecznością. Sprawdź naszą [politykę prywatności](#), aby uzyskać więcej informacji.

Przeskanuj!

Open-Source Intelligence (OSINT)

- Przykładowy sposób wykrycia różnego typu maszyn biorących udział w masowym ataku – przykład zagrożenia Locky
- Locky – ransomware atakujący od połowy lutego 2015 roku
- Infekcje najczęściej poprzez SPAM zawierający plik JavaScript (czasem spakowany jako zip) albo dokument MS Office-a z makrem
- Skrypt lub makro ściąga właściwy kod Locky-iego

Open-Source Intelligence (OSINT)

- Znalezienie informacji dotyczącej nowej kampania np. na podstawie nowych adresów serwerów C&C albo dystrubucyjnych
- Informacje te można znaleźć np. w serwisach malware-traffic-analysis albo ransomwaretracker
- Pobranie próbki zagrożenia do dalszej analiz np. bezpośrednio ze strony malware-traffic-analysis albo przeszukanie serwisu malwr.com
- Analiz i wykrycie nowych adresów
- Iteracyjne przeszukania bazy malwr.com

Open-Source Intelligence (OSINT)

- Wyniki dla przykładowej kampanii Locky-iego
 - Start około 10 maja 2016 ostatnie próbki 12 maja 2016
 - Wykryto 88 serwerów dystrybucyjnych
 - 41 serwerów dystrybucyjnych działało (*14 działało dzisiaj o północy !!! – 2016.06.14*)
 - Przeanalizowano 39 unikalnych próbek (posiadających różne wartości funkcji skrótu)
 - Wykryto 3 listy DGA
 - Wykryto 10 zahardkodowanych adresów C&C

Uzyskane dane to tak zwane IoC (Indicator of Compromise)

Plan wykładu

- Wstęp
- Bezpieczeństwo na poziomie organizacji
- Bezpieczeństwo na poziomie kraju, świata
- Podsumowanie

Cele mechanizmów bezpieczeństwa

- Jakie są cele wprowadzania mechanizmów bezpieczeństwa
 - Odstraszenie
 - Wykrycie
 - Alarm
 - Powstrzymanie
 - Reakcja
 - Edukacja
- Idealnie aby cały projekt systemu bezpieczeństwa był spójny i obejmował wszystkie wymienione funkcje

Reakcja na incydenty

- ang. Incident response
- Aktualnie dużą rolę przykłada się do wykrywania oraz prewencji ataków
- Jednak najważniejsze jest odpowiednie zareagowanie na nie
 - wyjaśnienie co dokładnie się stało, jak doszło do naruszenia/awarii
 - jakie są rzeczywiste straty
 - czy będą podjęte jakieś dalsze kroki prawne
 - co można zrobić aby nie doszło do kolejnych incydentów tego typu !!!

Edukacja użytkowników

- Coraz więcej osób pracuje z wykorzystaniem komputera, poczty elektronicznej, Internetu
- Użytkownicy podatni na socjotechnikę – ponieważ nikt im tego nie wytłumaczył
- W organizacji powinno wprowadzić się tak zwane „Security Awareness Campaign” – proste „pogadanki”, treningi na co zwracać uwagę, aby nie stać się ofiarą metod socjotechniki

Czy mają Państwo pytania ...

Czy mają Państwo pytania ...

... poza tymi dotyczącymi egzaminu ;)

Egzamin

- Egzamin testowy - 30 pytań w których należy wpisać w puste pola jeden/dwa wyrazy
- 0p/1p/2p za pytanie – razem do zdobycia 60 punktów
- Wymagane uzyskanie z egzaminu co najmniej 31p
- Terminy
 - termin zerowy 2019.06.11 (zgłoszenia, warunek lab > 30)
 - I termin 2019.06.14
 - II termin 2019.06.24