VirtualStudy.pl

Advanced Persistent Threat

czyli jak działają zorganizowane grupy przestępcze w sieci

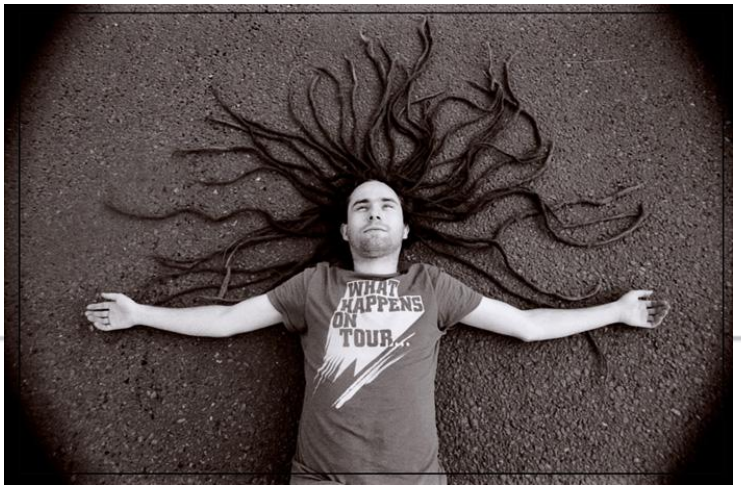
23.11.2011

LogicalTrust

Borys Łącki

VirtualStudy.pl

- Testy penetracyjne, audyty, szkolenia, konsultacje
- www.bothunters.pl - blog o cyberprzestępstwach
- www.logicaltrust.net - testy penetracyjne i audyty bezpieczeństwa
- Prelekcje: Securecon, SEConference, SekIT, Open SourceSecurity, Software Freedom Day, Pingwinaria, Grill IT, XIX Górska Szkoła Informatyki, (...)
- Członek PTI oraz aktywny uczestnik stowarzyszenia ISSA
- Działalność pro publico bono: nk.pl, allegro.pl, wykop.pl itp.

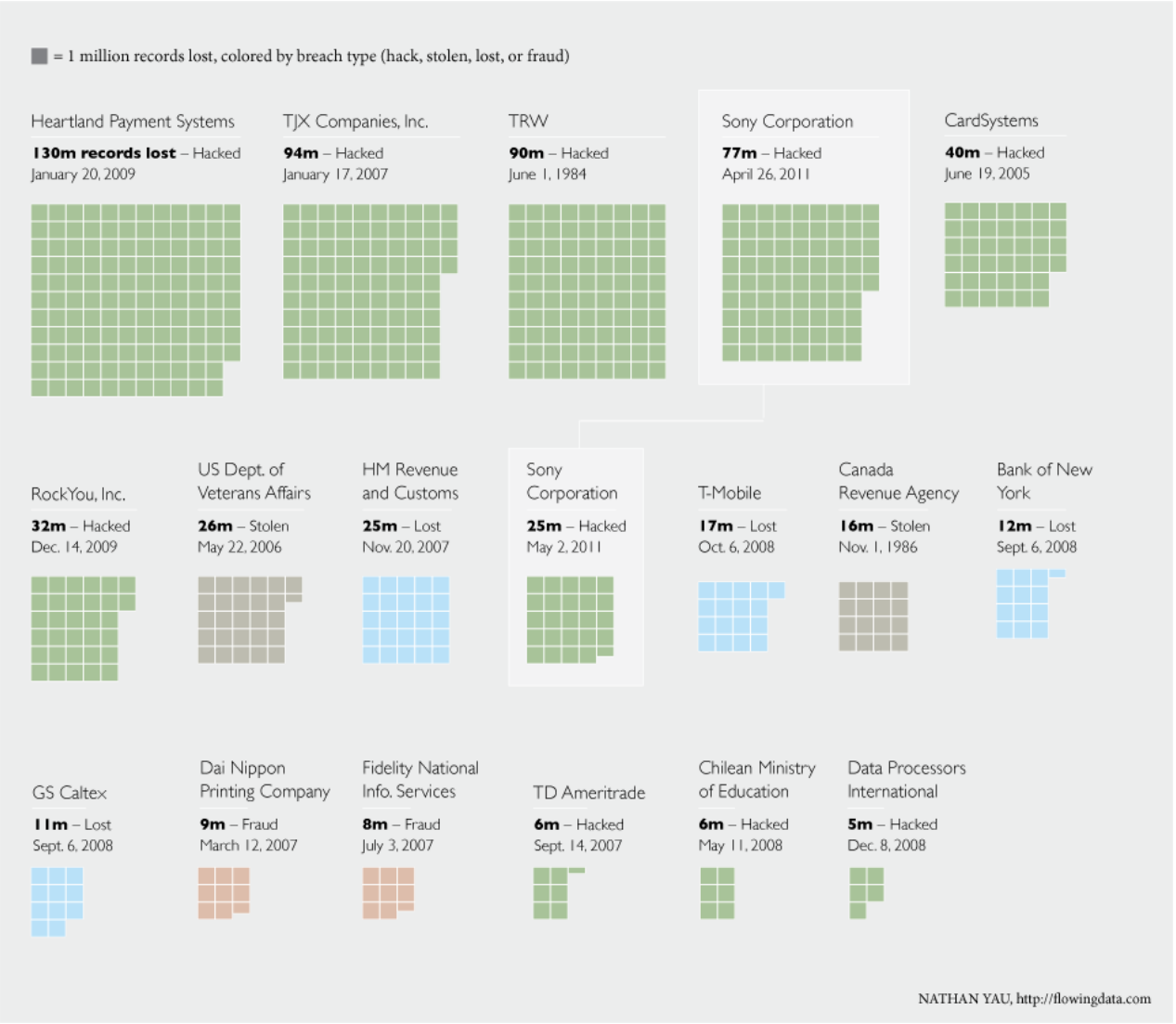


Advanced Persistent Threat

VirtualStudy.pl

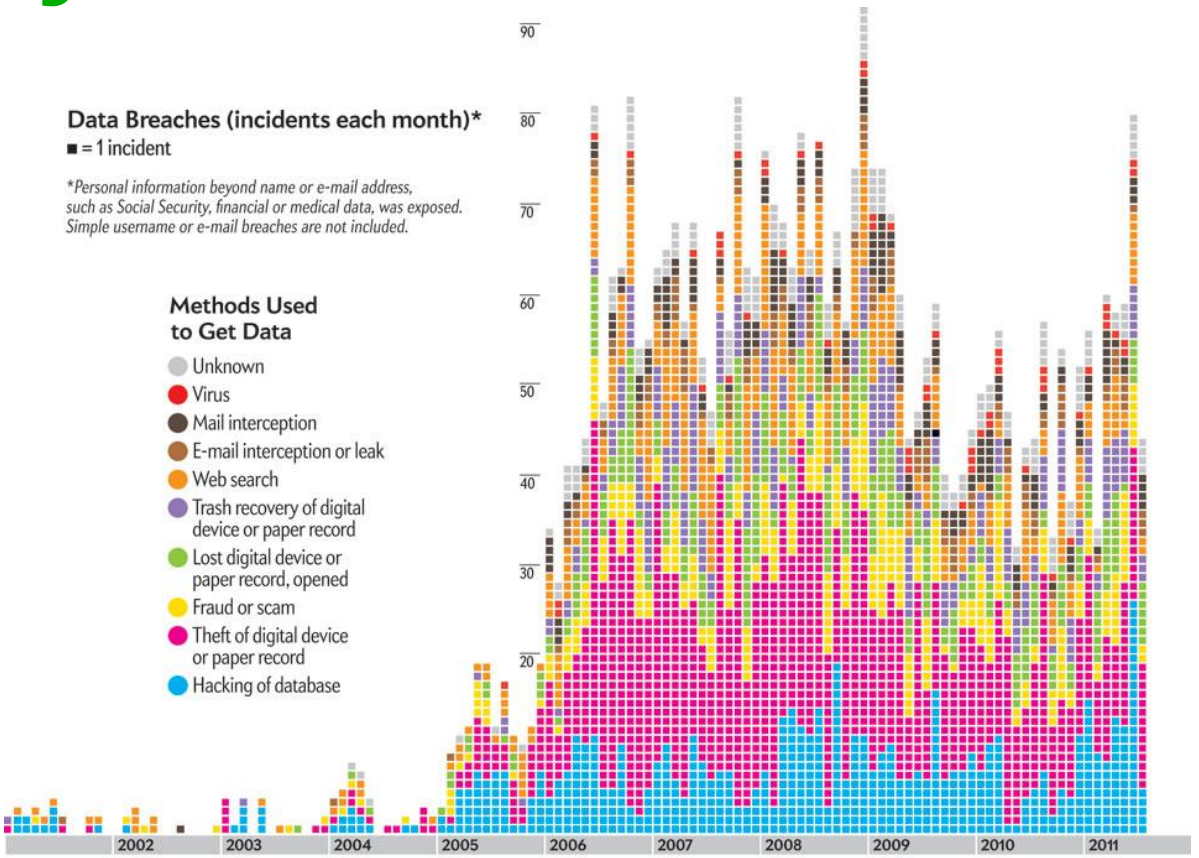
„Stres związany z ochroną informacji w firmie, jest większy niż podczas rozwodu lub wypadku samochodowego...”

Statystyki


= 1 million records lost, colored by breach type (hack, stolen, lost, or fraud)
Heartland Payment Systems
130m records lost – Hacked
January 20, 2009
TJX Companies, Inc.
94m – Hacked
January 17, 2007
TRW
90m – Hacked
June 1, 1984
Sony Corporation
77m – Hacked
April 26, 2011
CardSystems
40m – Hacked
June 19, 2005
RockYou, Inc.
32m – Hacked
Dec. 14, 2009
US Dept. of Veterans Affairs
26m – Stolen
May 22, 2006
HM Revenue and Customs
25m – Lost
Nov. 20, 2007
Sony Corporation
25m – Hacked
May 2, 2011
T-Mobile
17m – Lost
Oct. 6, 2008
Canada Revenue Agency
16m – Stolen
Nov. 1, 1986
Bank of New York
12m – Lost
Sept. 6, 2008
GS Caltex
11m – Lost
Sept. 6, 2008
Dai Nippon Printing Company
9m – Fraud
March 12, 2007
Fidelity National Info. Services
8m – Fraud
July 3, 2007
TD Ameritrade
6m – Hacked
Sept. 14, 2007
Chilean Ministry of Education
6m – Hacked
May 11, 2008
Data Processors International
5m – Hacked
Dec. 8, 2008
NATHAN YAU, http://flowingdata.com

Statystyki

VirtualStudy.pl



Largest Breaches of All Time (records compromised, date reported)

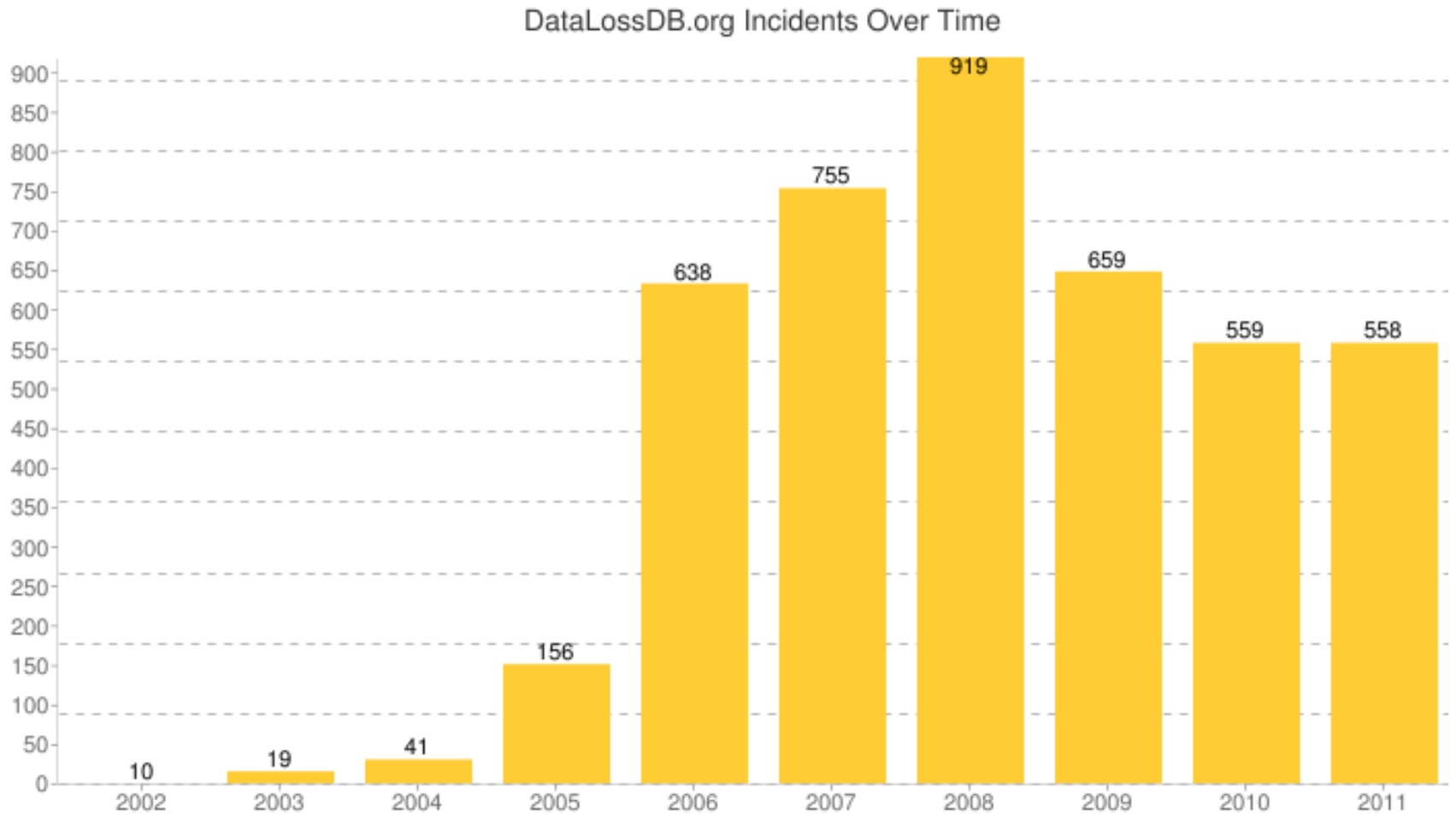
TRW	CardSystems Solutions	U.S. Dept. of Veterans Affairs	TJX Companies, Inc.	HM Revenue and Customs	T-Mobile	Heartland Payment Systems	RockYou	Sony Corporation	Sony Corporation
90 million	40 million	27 million	94 million	25 million	17 million	130 million	32 million	77 million	25 million
June 1, 1984	June 19, 2005	May 22, 2006	Jan. 17, 2007	Nov. 20, 2007	Oct. 6, 2008	Jan. 20, 2009	Dec. 14, 2009	April 26, 2011	May 2, 2011

† In July data about some 35 million users on Cyworld and Nate (South Korean sites) were swiped, but the types of data are still being verified.

LogicalTrust

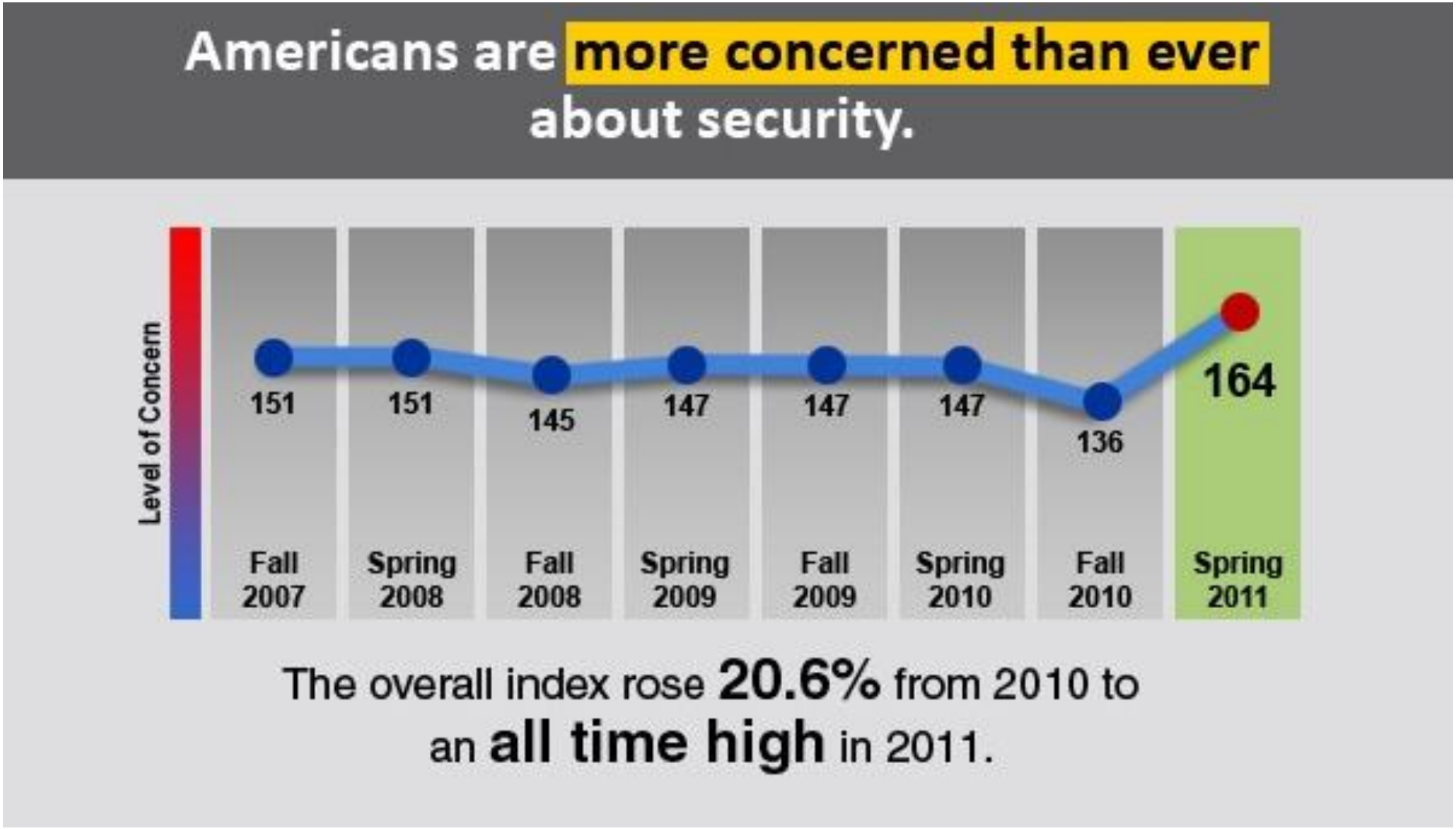
Statystyki

VirtualStudy.pl



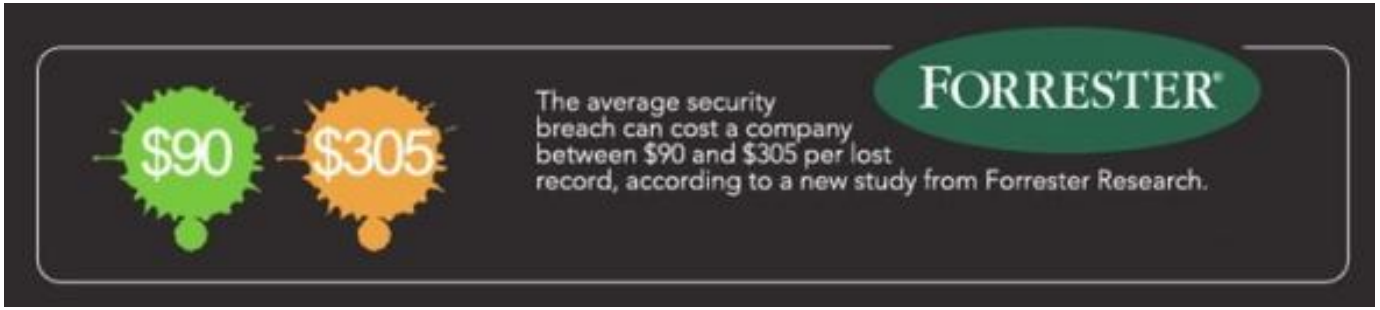
LogicalTrust

Statystyki

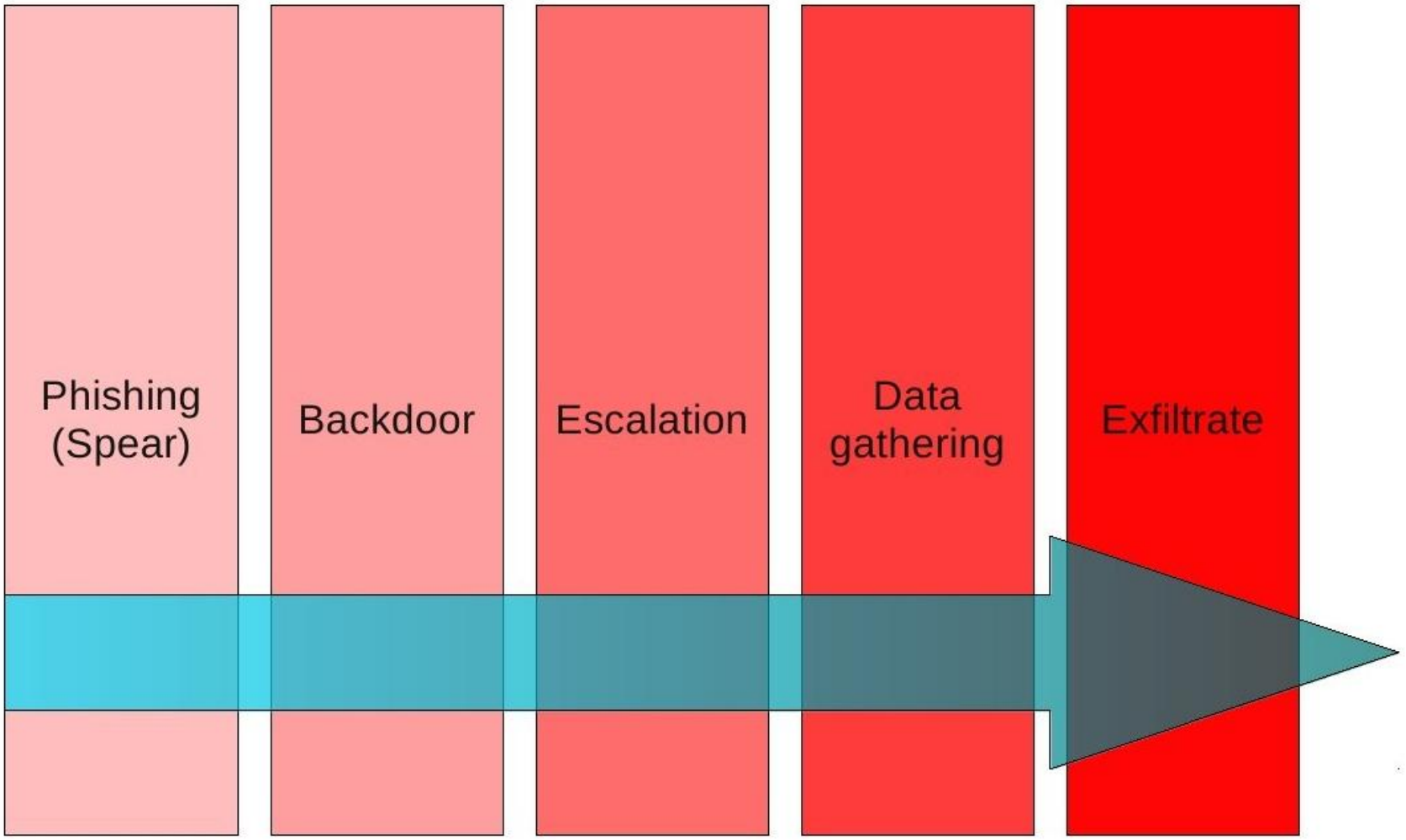

Americans are more concerned than ever about security.
Level of Concern
151
151
145
147
147
147
136
164
Fall 2007
Spring 2008
Fall 2008
Spring 2009
Fall 2009
Spring 2010
Fall 2010
Spring 2011
The overall index rose 20.6% from 2010 to an all time high in 2011.

Statystyki


Case study 1:
TJX
Security breach:
In Dec. 2006, hackers stole information from 45.7 million customer creditand debit cards.
45.7
Cost:
Nearly $1.7 billion plus the company faced a number of legal claims from customers and shareholders affected by the breach.
$1.7
Case Study 2:
Security breach:
Lost 26.5 million personal records in a data breach
26.5
Financial cost:
A coalition of veterans groups filed a class actior seeking $1,000 in damages for each person, a payout that could eventually reach $26.5 billion.
$26.5
Intangible cost:
Tarnished reputation
Case Study 3:
ChoicePoint
Security breach:
Hackers stole personal information on over 163,000 consumers.
166,000
Consequences:
The day the breach was reported, the data broker's stock value fell 3.1 percent. By late February, the company's stock value had plummeted nearly 9 percent.
3.1%


$90
$305
FORRESTER
The average security breach can cost a company between $90 and $305 per lost record, according to a new study from Forrester Research.

Advanced Persistent Threat



Advanced Persistent Threat

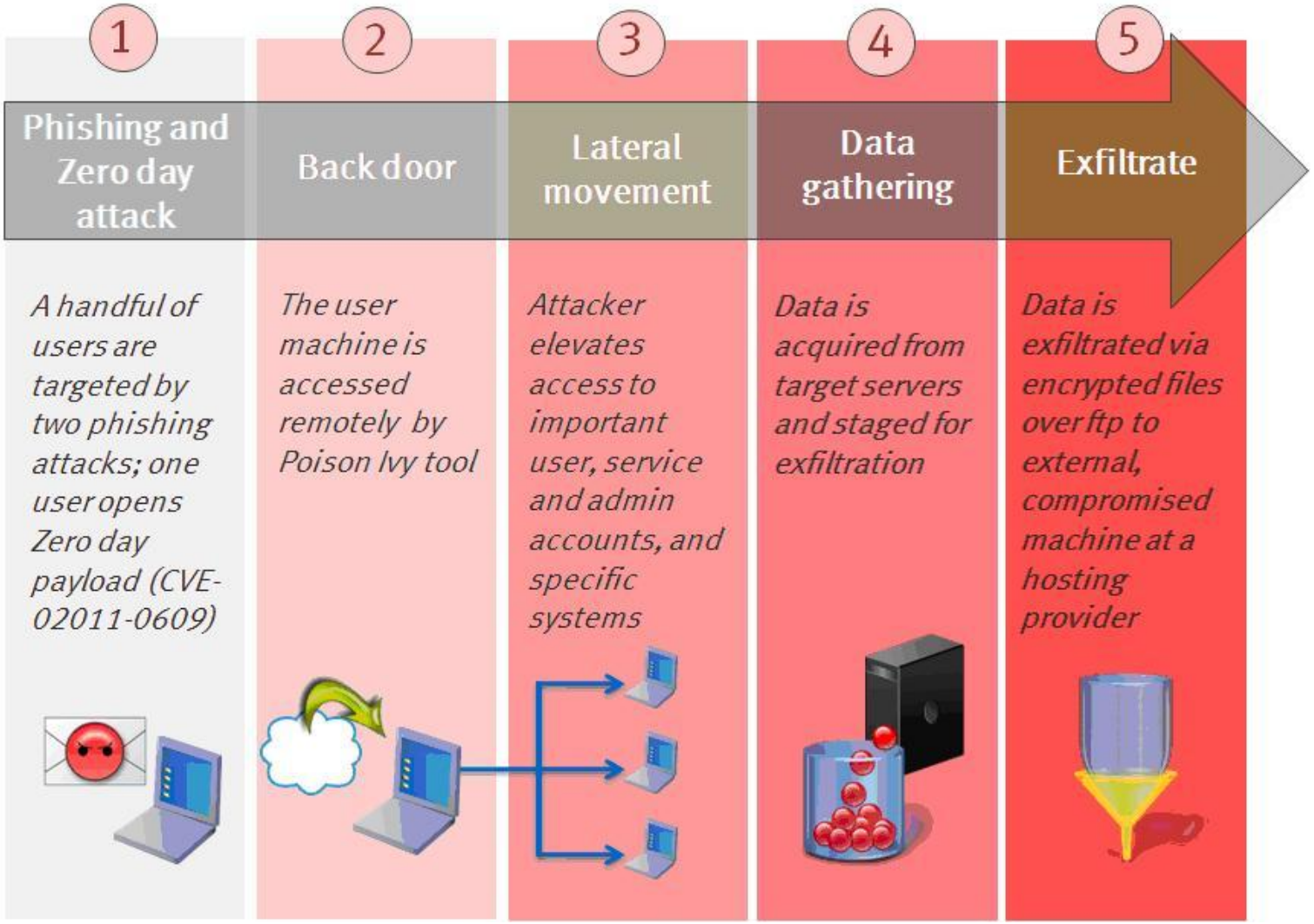
Advanced Persistent Threat

VirtualStudy.pl

RSA

RSA

VirtualStudy.pl



RSA

VirtualStudy.pl

- Złośliwe oprogramowanie przygotowane kilka godzin przed atakiem
- Dwie różne wiadomości e-mail w 2 dni, do dwóch małych grup (mało ważni pracownicy)
- Temat: *2011 Recruitment Plan*
- Pracownik otwiera załącznik (2011 Recruitment plan.xls) z wiadomości z folderu *Junk*
- Zero-day exploit - Adobe Flash vulnerability (CVE-2011-0609)

RSA

VirtualStudy.pl

- Trojan: Poison Ivy
- Poszukiwania nowych użytkowników, uprawnień, zasobów
- Nowe konta + eskalacja uprawnień → uprawnienia administratorów
- FTP - Zaszyfrowane archiwa RAR
- Atak został wykryty - Computer Incident Response Team

RSA – fail

- Junk folder
- Segmentacja sieci
- Oprogramowanie - białe listy
- Network firewall
- DNS Blacklisting
- Połączenia wychodzące
- Monitoring - konta administratorów
- Dwustopniowe uwierzytelnianie
- Wymiana tokenów

VirtualStudy.pl

DigiNotar SSL CA

LogicalTrust

DigiNotar SSL

VirtualStudy.pl

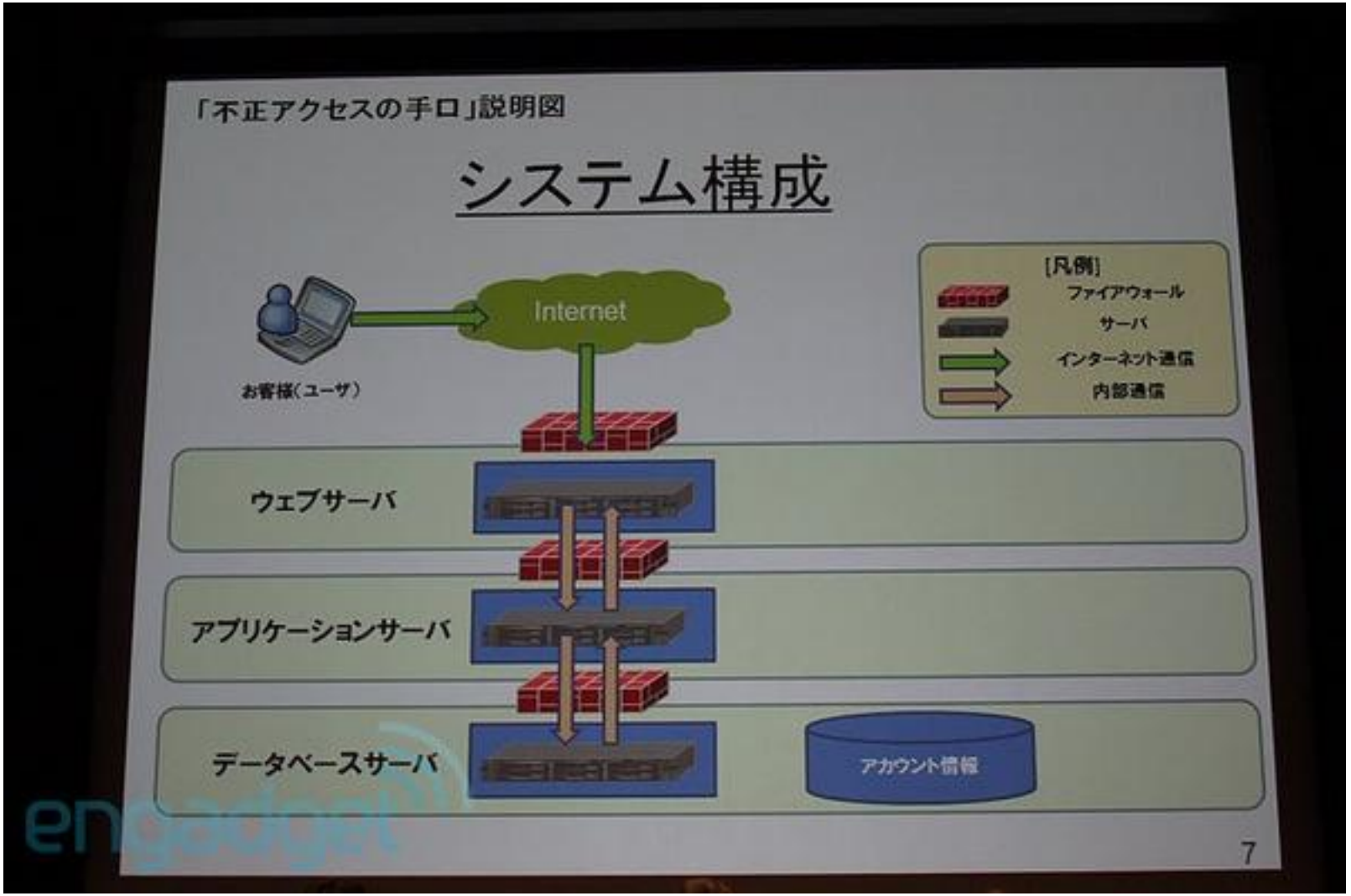
- **06.06.2011** - przejęcie systemów
- **17 - 22.06.2011** - największa aktywność cyberprzestępców
- **19.06.2011** - wykrycie włamania - 128 fałszywych cert.
- **20.06.2011** - analizy certyfikatów
- **21.06.2011** - 129 fałszywych certyfikatów
- **27.06.2011** - *.google.com oraz 75 fałszywych certyfikatów
- **28.06.2011** - testy fałszywych certyfikatów z Iranu
- **29.06.2011** - *.google.com kolejna blokada
- 300 000 adresów IP - 99% z Iranu

DigiNotar SSL - fail

VirtualStudy.pl

- Brak centralnego logowania
- Wszystkie serwery CA w jednej domenie Windows
- Hasła słabej jakości
- Segmentacja sieci
- Brak aktualizacji oprogramowania na serwerach publicznych
- Brak oprogramowania AV
- Dwustopniowe uwierzytelnianie (VASCO)
- Aktywny IPS

?



SONY

Sony

VirtualStudy.pl

- **2011-04-04** Atak DDoS - Anonymous (pozew GeoHot PS3)
- **2011-04-20** Sony PSN Offline
- **2011-04-26** (17-19.04) - (PSN) Hacked - 77 milionów nazwisk, adresów e-mail, dat urodzin, loginów, haseł itp.
- **2011-04-27** Czytelnicy Ars Technica zgłaszają problemy z kartami kredytowymi
- **2011-04-28** Pierwsze pozwy Sony PSN związane z utratą danych
- **2011-05-02** Sony Online Entertainment (SOE) hacked, SOE Network Offline - 24.6 miliony dat urodzenia, adresów e-mail, numerów telefonów (w tym 12 700 kart płatniczych i dat ważności)
- **2011-05-05** Sony zatrudnia ekspertów od informatyki śledczej

Sony

VirtualStudy.pl

- **2011-05-07** Utrata 2 500 „nieaktualnych” danych (głębokie ukrycie)
- **2011-05-14** Przywrócenie działania PlayStation Network (24 dni awarii)
- **2011-05-17** Konta PSN – problem ze zmianą hasła
- **2011-05-18** Zatrudnia firmę Prolexic (DDoS)
- **2011-05-20** Strona phishingowa odkryta na jednym z serwerów Sony
- **2011-05-21** Kradzież 1 220 wirtualnych $ - 128 kont
- **2011-05-21** Podmiana strony Sony Music Indonezja
- **2011-05-22** SQL injection - 8 500 kont, adresów e-mail, haseł - Sony BMG Grecja

Sony

VirtualStudy.pl

- **2011-05-23** SQL Injection - Japonia (www.sonymusic.co.jp) - LulzSec
- **2011-05-24** Sony Erricson – 2 000 rekordów, adresy e-mail, hasła, konta
- **2011-05-25** Sony uruchamia program ochrony tożsamości
- **2011-06-02** LulzSec publikuje ponad 1 milion haseł, adresów e-mail, domowych adresów, dat urodzenia oraz haseł administratorów
- **2011-06-02** Sony BMG Belgia – adresy e-mail, konta, hasła (brak szyfrowania)
- **2011-06-02** Sony BMG Holandia – konta, hasła (brak szyfrowania)
- **2011-06-03** SQL Injection - Sony Europe (apps.pro.sony.eu)

Sony

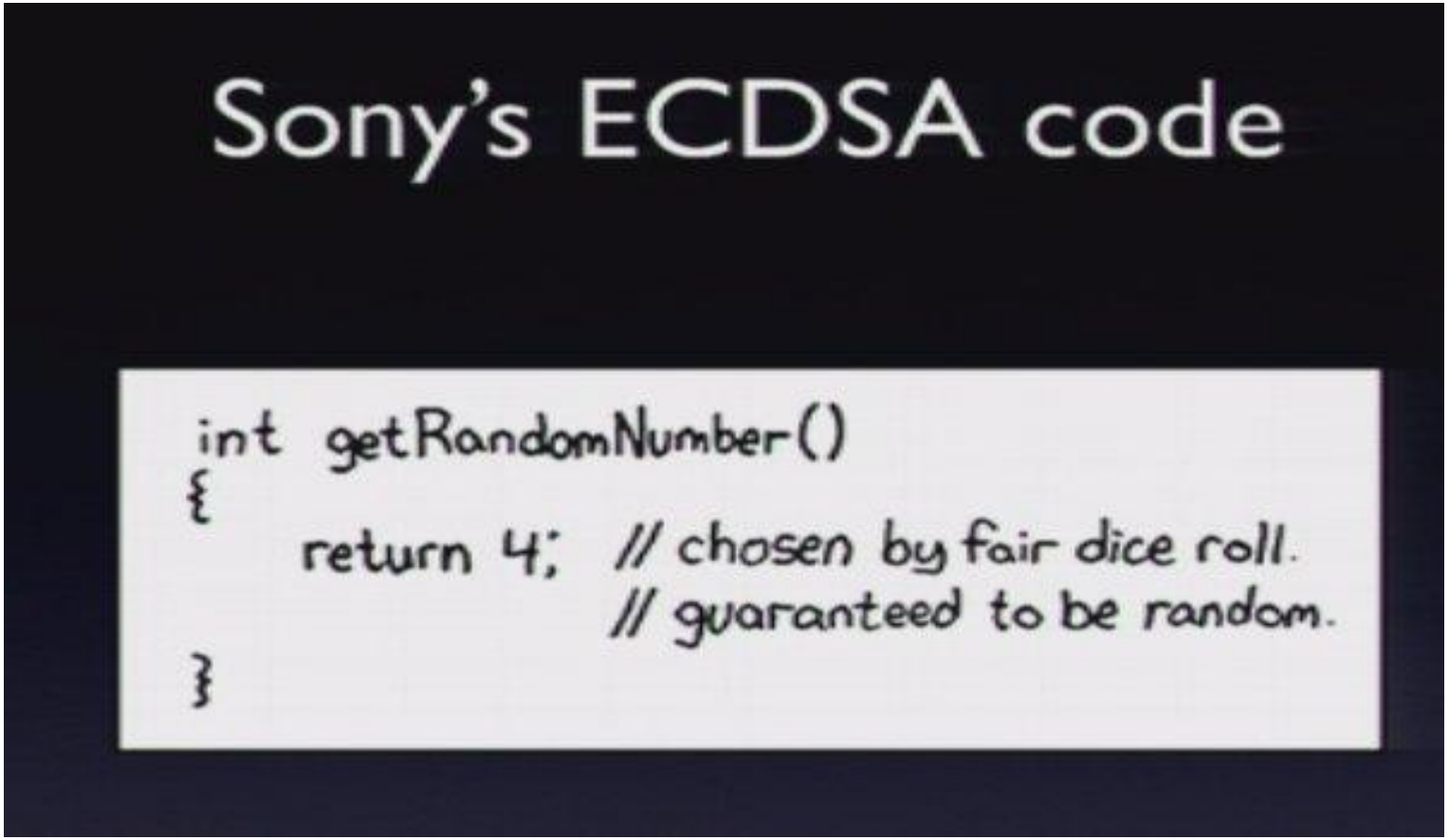
VirtualStudy.pl

- **2011-06-05** SQL Injection - Sony Pictures - Rosja (www.sonypictures.ru)
- **2011-06-06** Publikacja 54 MB szczegółowych danych Sony Computer Entertainment Developer Network (w tym kody źródłowe) - LulzSec
- **2011-06-06** Sony BMG – ujawnienie map wewnętrznych sieci - LulzSec
- **2011-06-08** SQL injection - Sony Portugalia (sonymusic.pt)
- **2011-06-20** SQL injection – Sony Francja SQLI (sonypictures.fr)
- **2011-07-06** Publikacja fałszywych informacji o celebrytach – Sony Irlandia (sonymusic.ie)
- **2011-10-12** Kradzież 93 000 kont PSN – brute force

Sony - fail

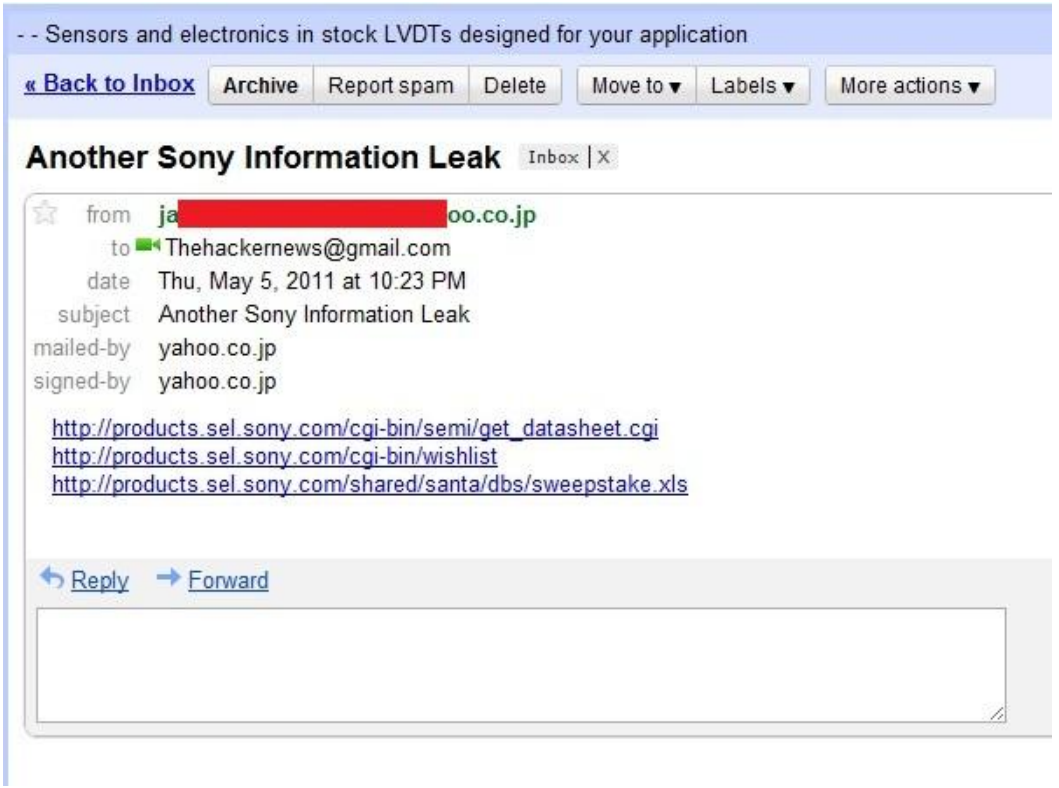
VirtualStudy.pl

- Zaawansowany kod ECDSA



Sony - fail

- Zaawansowany kod ECDSA
- *Głębokie ukrycie*



Sony - fail

VirtualStudy.pl

- Zaawansowany kod ECDSA
- *Głębokie ukrycie*
- SQL injections
- Hasła bez szyfrowania
- Nieaktualne oprogramowanie serwerowe
- PO incydentach Sony tworzy stanowisko Security Information Officer
- 8% unikalnych haseł, 1% haseł zawierających znaki alfanumeryczne, *seinfeld password winner 123456 purple sweeps contest princess maggie 9452*

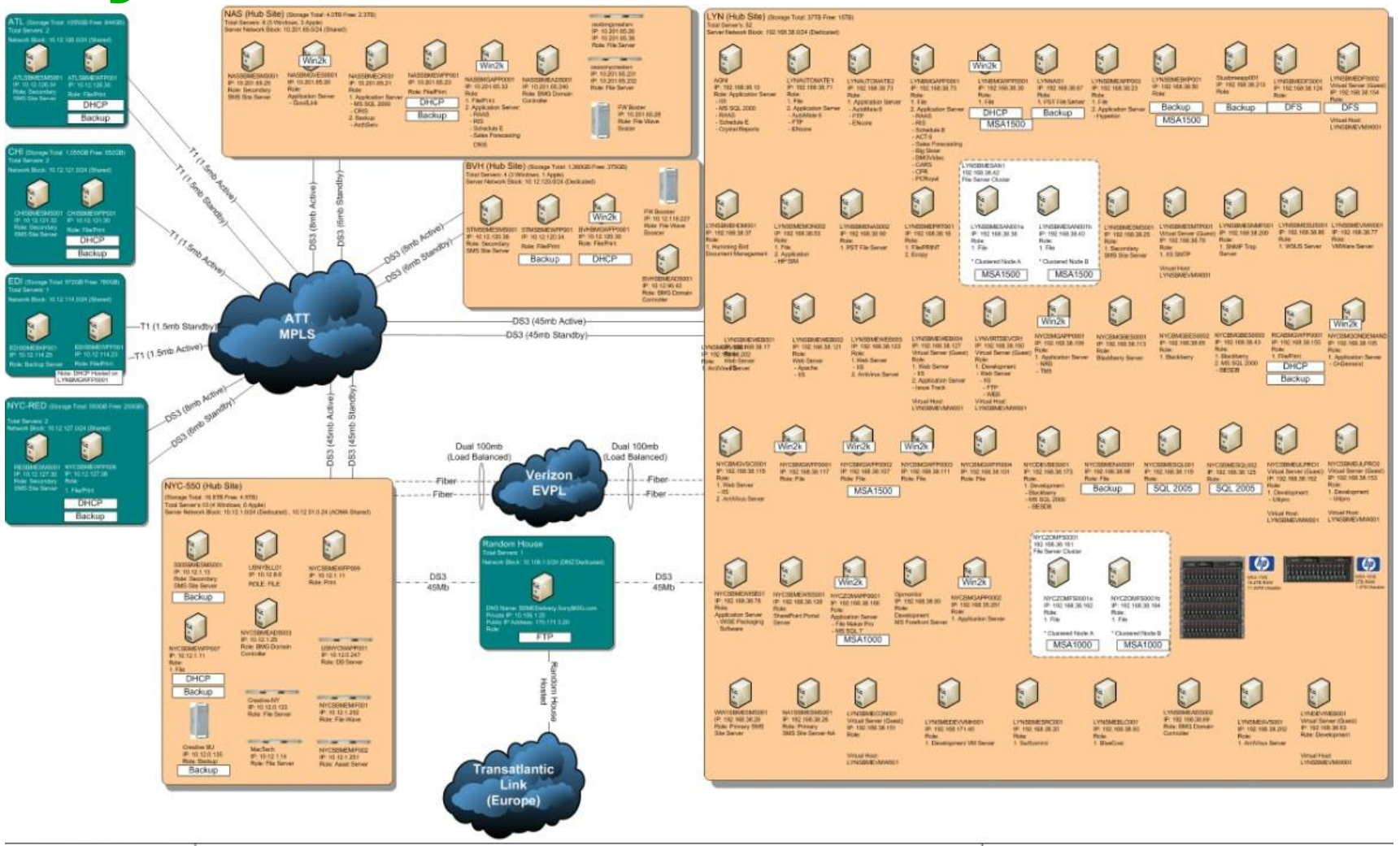
Sony - fail

VirtualStudy.pl

Location	Function	Make	Model	Name	MGMT IP Address
550 MAD	Firewall	Juniper	SSG550	FW-SBME-NYC-US01	
550 MAD	Firewall	Juniper	SSG550	FW-SBME-NYC-US02	
550 MAD	Firewall	Juniper	SSG140	FW-SBME-MPAS-01	
550 MAD	IPS	TIPPING POINT	200E	IPS-SBMEWAN-NYC-US01	10.12.0.26
550 MAD	IPS	TIPPING POINT	200E	IPS-SBMEWAN-NYC-US02	10.12.0.27
550 MAD	IPS	TIPPING POINT	200E	IPS-SBME-FW-NYC-US01	
550 MAD	IPS	TIPPING POINT	200E	IPS-SBME-FW-NYC-US02	
550 MAD	IPS	TIPPING POINT	1200	IPS-SBME-FW-NYC-US01	10.12.0.24
550 MAD	IPS	TIPPING POINT	1200	IPS-SBME-FW-NYC-US02	10.12.0.25
550 MAD	IPS	TIPPING POINT	110	IPS-SBME-MPAS-01	TBD
LDT	Firewall	Juniper	SSG550	FW-SBME-LYND-US01	
LDT	Firewall	Juniper	SSG550	FW-SBME-LYND-US02	
LDT	IPS	TIPPING POINT	200E	IPS-SBME-FW-LYN-US01	192.168.38.3
LDT	IPS	TIPPING POINT	200E	IPS-SBME-FW-LYN-US02	192.168.38.4
LDT	IPS	TIPPING POINT	200E	IPS-SBMEWAN-LYN-US01	192.168.38.5
LDT	IPS	TIPPING POINT	200E	IPS-SBMEWAN-LYN-US02	192.168.38.6
NASH	Firewall	Juniper	SSG550	FW-SBME-NASHV-US01	
NASH	Firewall	Juniper	SSG550	FW-SBME-NASHV-US02	
NASH	IPS	TIPPING POINT	50	IPS-SBME-FW-NASHV-US01	10.201.65.11
NASH	IPS	TIPPING POINT	50	IPS-SBME-FW-NASHV-US02	10.201.65.12
1745RH	Firewall	Juniper	SSG140	IPS-SBME-FW-1745-US01 (FUTURE)	
1745RH	Firewall	Juniper	SSG140	IPS-SBME-FW-1745-US02 (FUTURE)	

Sony - fail

VirtualStudy.pl



SONY BMG MUSIC ENTERTAINMENT

Infrastructure Managed Server Environment

Updated By: Alex Moldoveanu

Last Updated: 8-26-09

Version 1.1

LogicalTrust

Sony - fail

VirtualStudy.pl

LogicalTrust

Google

Google

VirtualStudy.pl

- Operacja Aurora – 12.01.2010
- Adobe, Juniper, Intel, Yahoo, Symantec, Dow Chemical, Morgan Stanley... - 34 firmy (ponad 200)
- Okres świąteczny
- Kradzież własności intelektualnej, dostęp do kont pocztowych aktywistów praw człowieka
- Kilkanaście sposobów zaawansowanego szyfrowania, dziesiątki rodzajów złośliwego oprogramowania

Google

- IM, e-mail, social network
- Internet Explorer 0-day (MS10-002) - metasploit
- Trojan.Hydraq - Złośliwe oprogramowanie podszywające się pod komunikację SSL, brak sygnatur AV
- Inne firmy – także atak z użyciem PDF (??)
- Serwery zarządzające w Illinois, Texas, Taiwan

Google - fail

VirtualStudy.pl

- HBGary Responder Professional 2.0 ;]
- DNS blackholing
- DEP
- JavaScript
- IE 6
- *The construction of the botnet would be classed as “old-school”, and is rarely used by professional botnet criminal operators today*

VirtualStudy.pl

Brooks-Jeffrey Marketing

Brooks-Jeffrey Marketing

VirtualStudy.pl

- 78 różnych organów ścigania w całej Ameryce
- Prywatne e-maile z 300 kont, 7 000 haseł (ftp, ssh, cpanel), adresów, telefonów, kody źródłowe, kopie zapasowe
- *„the most the hackers got from their organization were email addresses and there were no critical details like names, social security numbers or other personal information details on their server”* - Anonymous użyli skradzionych danych z kart płatniczych i zasilili konta organizacji ACLU oraz Bradley Mining Support Network

Brooks-Jeffrey Marketing - fail

VirtualStudy.pl

- SQL injection
- Shell injection
- Dostęp do prywatnych kluczy
- Separacja sieci, serwerów

```
$username = $_GET['username'];
$password = $_GET['password'];

include "../config/connect.php";
sleep(2);
$query = "select * from dymin_user where username = '$username'
'$password'";
```

Brooks-Jeffrey Marketing - fail

VirtualStudy.pl

```
safe_query($query){
if(strpos(getcwd(),'admin')){
        shell_exec("echo '".date("Y-m-d H:i:s")."|".$query.
_logs/".str_replace("www.","",$_SERVER['HTTP_HOST']."."));
}
tabase = DATABASE;
```

```
$file_to_include = $_GET['filename'];

include "$file_to_include";
?>
```

```
$GD_USER = 'admin';
$GD_PASS = '8w667nHzx%X
$GD_SERV = 'localhost';

$options = getopt("n::o

$query = 'SHOW DATABASE
```

The SUN

The Sun

VirtualStudy.pl

- Anonymous, LulzSec – publikują fałszywe wiadomości w serwisie WWW
- 2009 – podatność XSS w podatnym serwerze WWW
- Podatność w CMS
- Przejęcie kolejnych serwerów

The Sun

VirtualStudy.pl

- Brak aktualizacji systemu
- Podatności webowe w publicznym serwerze
- Brak separacji sieci
- Brak logowania
- Brak monitorowania

Barracuda

Barracuda

VirtualStudy.pl

- Producent Web Application Firewall
- Okno czasowe – kilka godzin
- Skradziono tysiące poufnych danych klientów i pracowników
- SQL injection: *www.barracudanetworks.com/ns/customers/customer_verticals.php?v=11*

Barracuda - fail

VirtualStudy.pl

User	Password	Host
[redacted]ntral	*41A239FC71F557165F3A230A896BD632D4FCFB30	%
[redacted]re_web	*F30B410BDF71148B1DABFE7C5E0BC507DFB8005E	%
[redacted]tzel	*E89B9EB951090B77D2AF87E18598BE0F91A1E40C	%
[redacted]ans	*2EACC9BB3AD33C48DF3A59D4C671DA79DE3BA676	%
[redacted]olfe	*4436EB550303BE5EA882CEF49B7077F48893C501	%
[redacted]	*55D70C13E222E7C2351D536DC6704B89ACFCABFD	%
[redacted]	*532D8DB4936EE911E89F38346DCC2DE9650181BB	%
[redacted]eth	*532D8DB4936EE911E89F38346DCC2DE9650181BB	%
[redacted]a_web	*55D70C13E222E7C2351D536DC6704B89ACFCABFD	10.8.0.7
[redacted]a_web	*55D70C13E222E7C2351D536DC6704B89ACFCABFD	10.8.1.128
[redacted]ats	*CB48ECE8D7C5A55DC74CA1BDA16DB04DE5744587	10.8.4.64
[redacted]	*DD1403EFB2CEA8801F08F3144D3D07202ACD1EA8	216.129.105.100
[redacted]ats	*DD1403EFB2CEA8801F08F3144D3D07202ACD1EA8	216.129.105.12
[redacted]ntral	*94814B42A852B72BBD3B67F491FB5F85A1E92E1D	216.129.105.40
[redacted]ats	*94814B42A852B72BBD3B67F491FB5F85A1E92E1D	64.235.144.14
[redacted]ghmode	*4B121F3076A98824A6184D8C5D1EC4B9EF73C7C3	69.36.255.100
[redacted]	*B1366C7EB3C2A9432C6717332E8BEFE11D41CE06	69.36.255.100
[redacted]a_web	*B1366C7EB3C2A9432C6717332E8BEFE11D41CE06	69.36.255.110
[redacted]etest	*3AA4EA3E94AF1CB00FD4CDA0C3CB8DF36BF91D48	localhost
[redacted]e	*7C3529971EE22AD58BDD65C61BF5772A5AE9D434	localhost
[redacted]	*2EACC9BB3AD33C48DF3A59D4C671DA79DE3BA676	localhost
[redacted]ghmode	*2EACC9BB3AD33C48DF3A59D4C671DA79DE3BA676	localhost
[redacted]	*DD1403EFB2CEA8801F08F3144D3D07202ACD1EA8	localhost

LogicalTrust

Barracuda - fail

VirtualStudy.pl

- Polityka haseł - *zombie, password*
  - MD5
  - PrawieSolenie haseł
  - Powtarzalność haseł

Barracuda - fail

VirtualStudy.pl

- Polityka haseł - *zombie, password*
  - MD5
  - PrawieSolenie haseł
  - Powtarzalność haseł
- Segmentacja bazy danych, uprawnień
- 22 bazy danych (w tym testowe)

igivetest, igivetestsucks dev_new_barracuda, new_barracuda_archive

VirtualStudy.pl

Oak Ridge National Laboratory

LogicalTrust

Oak Ridge National Laboratory

VirtualStudy.pl

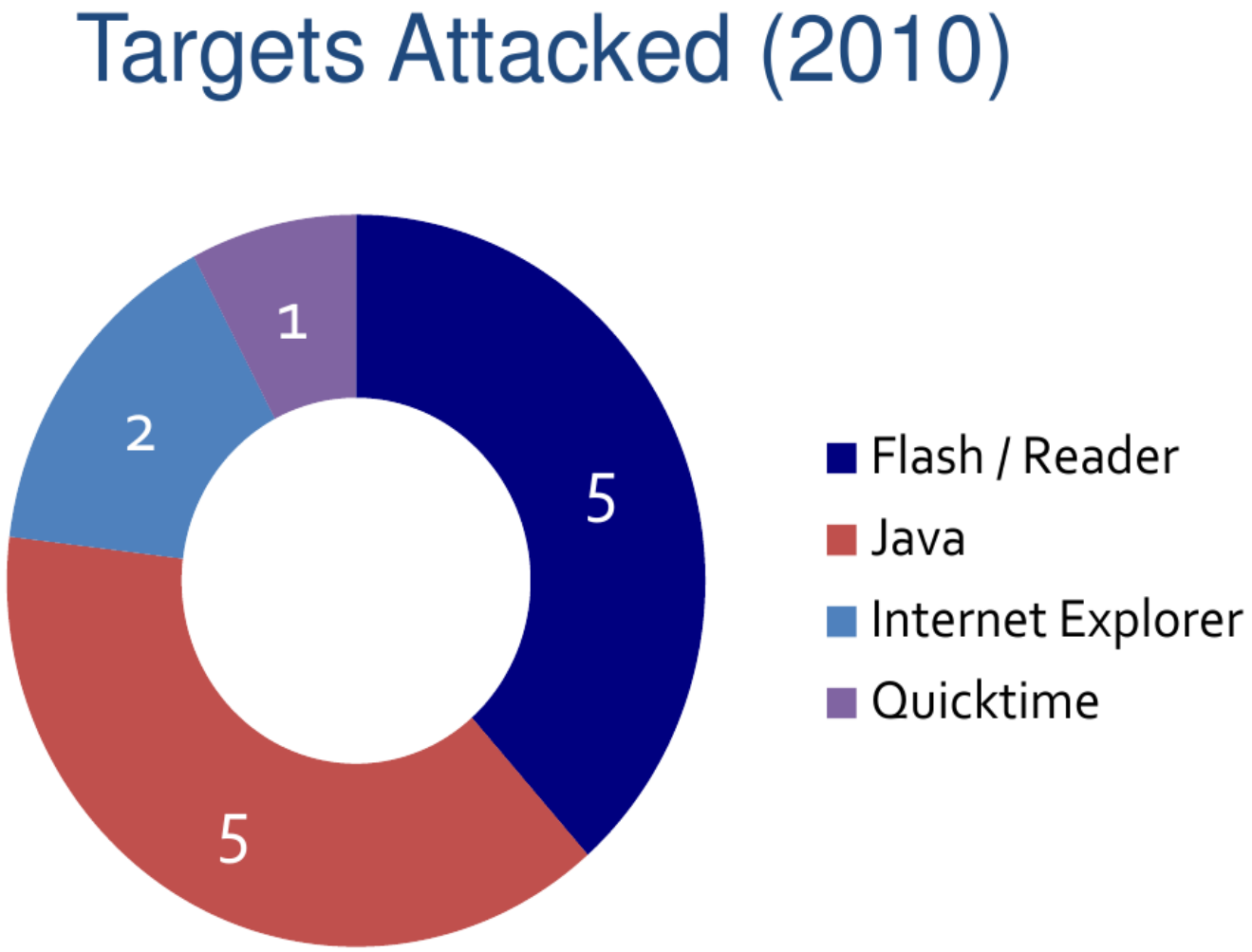
- Badania związane z cyberbezpieczeństwem, analiza złośliwego oprogramowania, phishingu, podatności w oprogramowaniu
- 07.04.2011 - Spear-phishing wysłany do pracowników

  OD: Dział HR Temat: Zyski pracownika i odnośnik do strony WWW
- Internet Explorer zero-day – aktualizacja 12.04.2011 (ms11-018)
- 530 pracowników (z 5 000) otrzymało wiadomość, 57 osób uwierzyło, 2 zainfekowane systemy
- Zaszyfrowane dane (kilkadziesiąt MB) zostały wysłane w świat
- 2007 – podobny atak, 7 różnych wiadomości e-mail z niebezpiecznymi załącznikami – wyciek gigabajtów danych

Obrona

Obrona

Obrona



Obrona

VirtualStudy.pl

Effective Defenses (2009-2010)

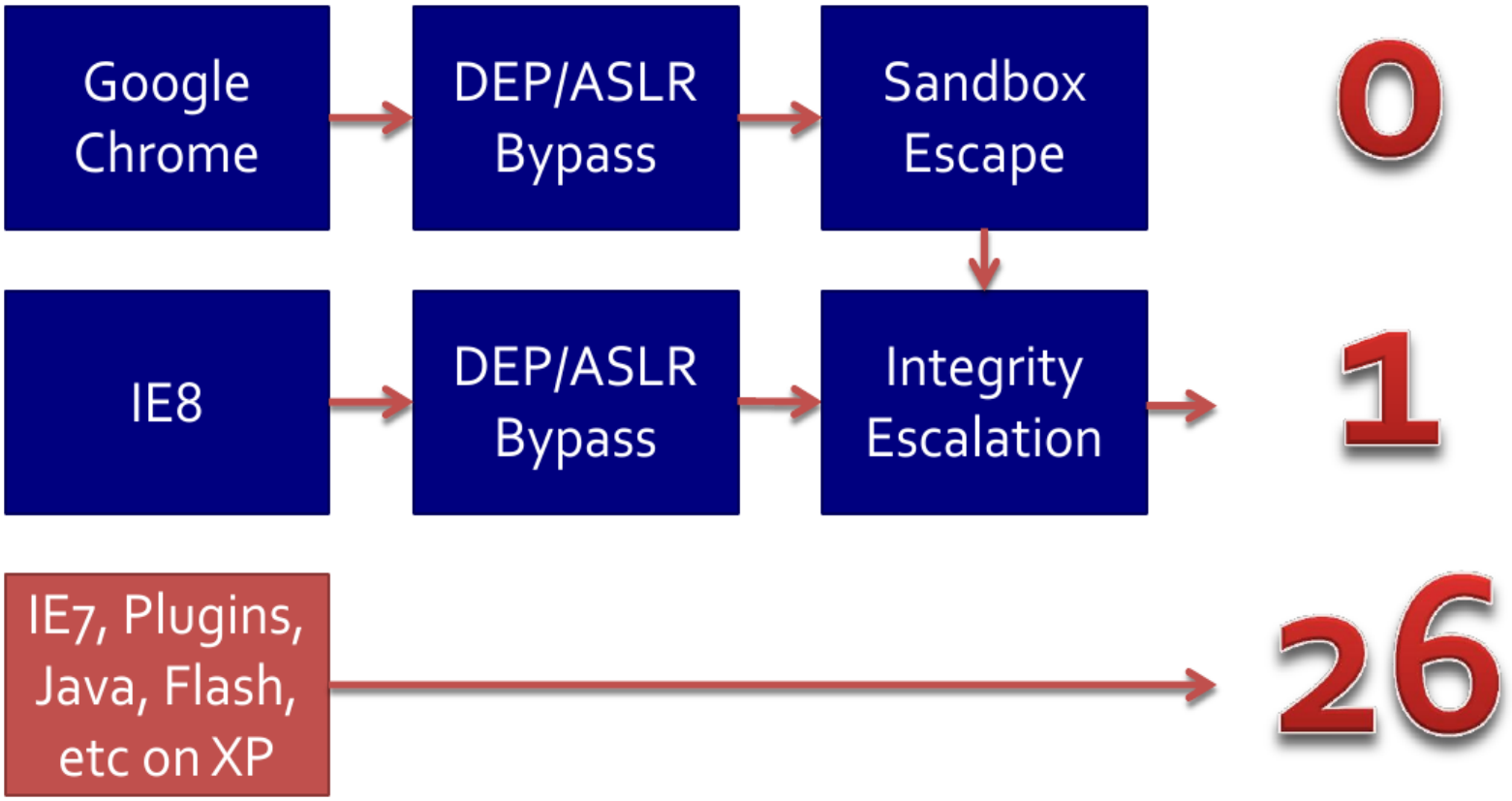
Memory Corruption (19)	
Defeated by DEP	14
Defeated by ASLR	17
Defeated by EMET	19

Logic Flaws (8)	
No Java in Internet Zone	4
No EXEs in PDFs	1
No Firefox or FoxIt Reader	2

Obrona

VirtualStudy.pl

Attack Graph Traversals (2009-2010)



Obrona - incydent

VirtualStudy.pl

Poważny incydent bezpieczeństwa jest jak ruchome piaski – im bardziej panikujemy, tym jest gorzej...

- Przestań panikować i zatamuj *krwawienie* - skup się na rozwiązaniu problemu – przestępców będziesz ścigał później
- Nie ufaj nikomu i niczemu
- Nie wydawaj pieniędzy na siłę, to nie rozwiąże Twoich problemów
- Działaj szybciej niż kiedykolwiek
- Dbaj o Public Relations ale z głową
- Przeproś, wykaż się kompetencjami, przedstaw plan napraw

Obrona

VirtualStudy.pl

- **Polityka haseł**
- **Aktualizacje systemów i aplikacji**
- **Edukacja użytkowników**
- **Segmentacja sieci**
- **Testy penetracyjne :]** www.logicaltrust.net
- **Ograniczenia kont (Administratorów)**
- **Aplikacje bezpieczeństwa na hostach: AV, FV,** (DEP,ASLR, SEHOP, EATAF, HSA, NPA)

Obrona

VirtualStudy.pl

- Białe listy aplikacji
- Centralne, zsynchronizowane logowanie
- Filtry zawartości WWW (in/out)
- Dwustopniowe uwierzytelnianie
- Firewall (Ipv6)
- Używanie przeglądarek WWW oraz aplikacji z opcją Sandbox
- Zarządzanie fizycznym dostępem

Obrona

VirtualStudy.pl

- WiFi – WPA2, zarządzanie wyłącznie z sieci wewnętrznej
- Porządek – OS, Sieć, Urządzenia
- Dezaktywacja funkcjonalności
- Urządzenia przenośne
- Full Disk Encryption
- Backup/Disaster Recovery Plan

Obrona

VirtualStudy.pl

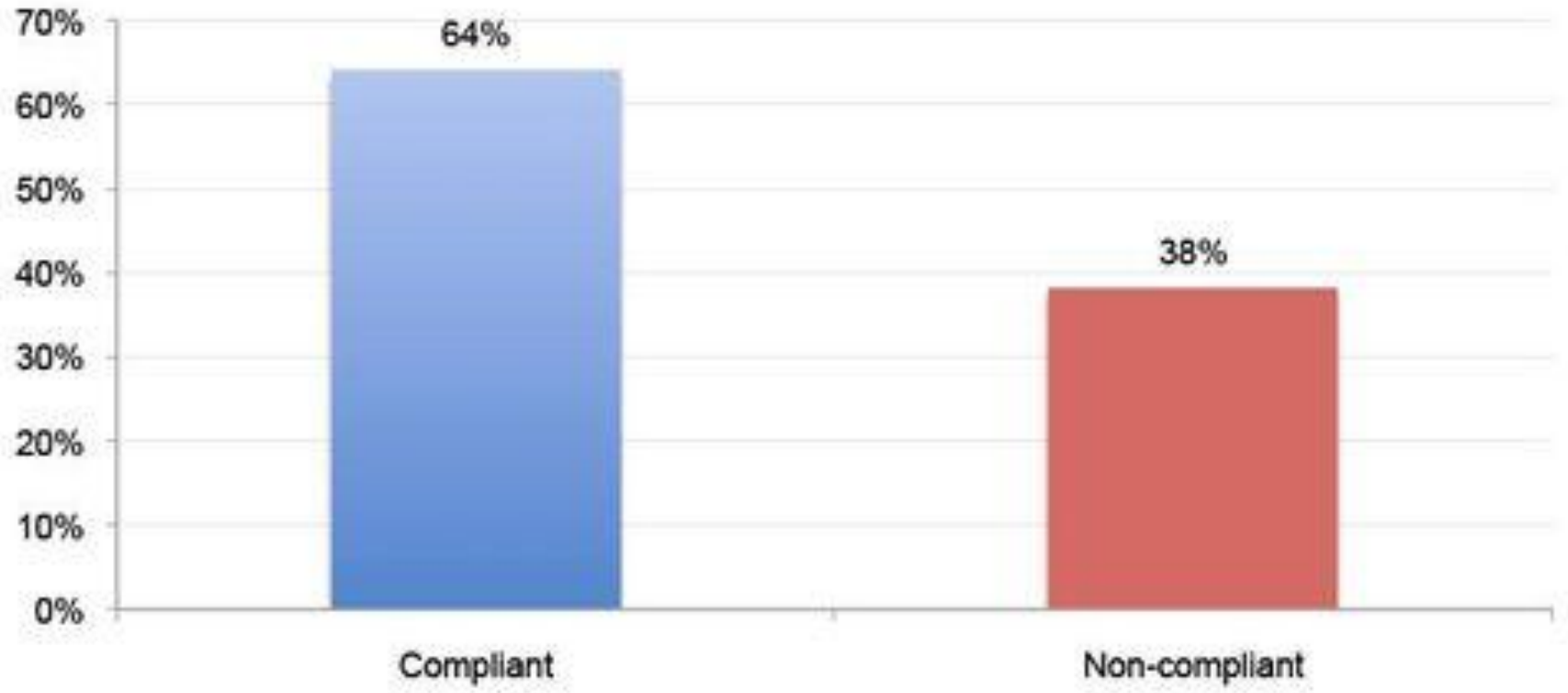
- Data Loss Prevention
- Migracja do nowych OS - Windows Vista, 7
- Dokumentacja
- Security team
- IDS/IPS
- Komunikacja z zewnętrznymi podmiotami

Obrona

VirtualStudy.pl

Bar Chart 6: Data breach of cardholder data for compliant and non-compliant groups

Each bar defines the percentage of companies that did not experience a breach over the past 24 months



Źródła

http://attrition.org/security/rants/sony_aka_sownage.html
http://blog.eset.com/2011/05/31/enterprise-security-the-ten-commandments
http://blog.eset.com/2011/10/05/u-s-government-security-incidents-up-650-over-5-years
http://blog.imperva.com/2011/04/pcis-impact-on-security-quantified.html
http://blog.rootshell.be/2011/07/19/lulzsec-vs-the-sun-a-case-study/
http://blogs.cisco.com/security/cisco-csirt-on-advanced-persistent-threat/
http://blogs.rsa.com/rivner/anatomy-of-an-attack/
http://computer-forensics.sans.org/blog/2011/09/06/diginotar-incident-response-report-no-logging-weak-password-no-protected-network
http://datalossdb.org/
http://flowingdata.com/2011/06/13/largest-data-breaches-of-all-time/
http://h30499.www3.hp.com/t5/Following-the-White-Rabbit-A/Quicksand/ba-p/2407798
http://krebsonsecurity.com/2011/04/fbi-20m-in-fraudulent-wire-transfers-to-china/
http://luciusonsecurity.blogspot.com/2011/05/fourteen-potential-problems-for-sony-to.html
http://mashable.com/2011/05/07/security-fears-infographic/
http://net-security.org/secworld.php?id=11820
http://technologyspectator.com.au/analysis/daily-infographic/real-cost-sonys-data-breach
http://thehackernews.com/2011/05/thn-hacker-news-exclusive-report-on.html
http://www.acunetix.com/blog/news/barracuda-networks-breached/
http://www.acunetix.com/blog/news/us-police-servers-breached-in-new-anonymous-attack/
http://www.dsd.gov.au/infosec/top-mitigations/top35mitigationstrategies-list.htm
http://www.emergency-response-planning.com/news/bid/45178/INFOGRAPHIC-The-Cost-of-Data-Security
http://www.emergency-response-planning.com/news/bid/47018/INFOGRAPHIC-The-Cost-of-Security-Breaches
http://www.infosecurity.us/blog/2011/10/14/infographic-data-breaches-a-decade-of.html
http://www.morfiblog.pl/2011/04/26/aplikacje-w-szklance-emet/
http://www.novainfosecportal.com/2011/05/08/moms-guide-to-the-nsas-home-security-guidelines/
http://www.theprivatebusinessowner.com/2011/10/why-small-businesses-should-fear-data-breaches-infographic/
http://www.troyhunt.com/2011/06/brief-sony-password-analysis.html
http://www.wired.com/threatlevel/2010/01/operation-aurora/
http://www.wired.com/threatlevel/2011/04/oak-ridge-lab-hack/
http://www.youtube.com/user/ImpervaChannel

Pytania?

VirtualStudy.pl

Dziękuję za uwagę...

www.bothunters.pl

www.logicaltrust.net

b.lacki@logicaltrust.net