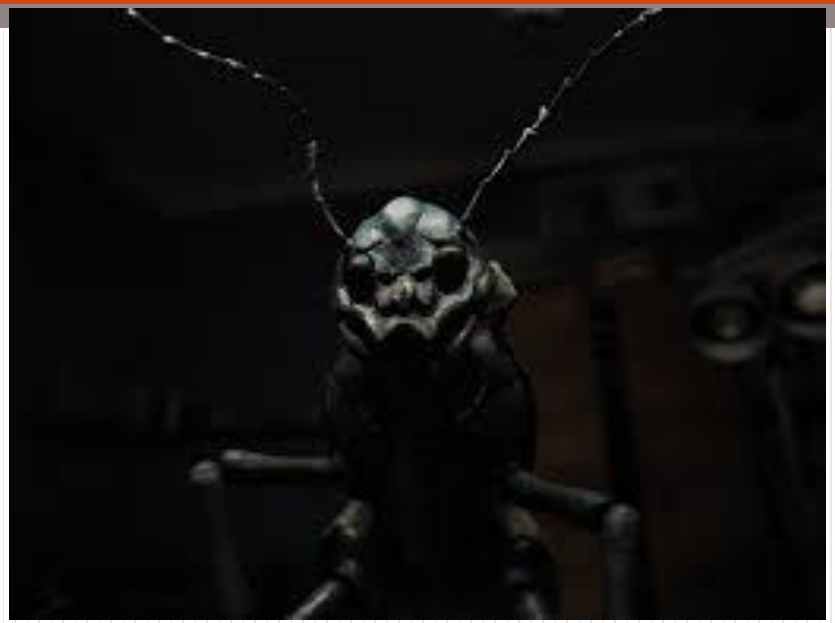
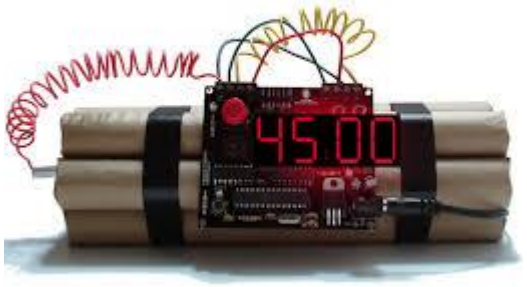
Chrobák v hlave



Čo by ste stihli za najbližších 90 minút ?



- Pospať si
- Vybaviť maily
- Hodiť pár fotiek na Instagram
- Pridať nový status na Facebook
- Stiahnuť si novú muziku
  - ...prípadne si vypočuť tú už skôr stiahnutú ...
- Pozrieť si dobrý film
- Prípadne sa niečo nové naučiť, či ?

- **Internet je GENIÁLNA VEC a bez neho by dnes človek možno aj umrel ...** ☺

Človek ktorý vydržal rok bez Internetu

Čo iné sa dá stihnúť (aj za menej ako 90 minút)

- Prísť o dobré meno
- Prísť o súkromie
- Prísť o peniaze
- Prísť o firmu
- Prísť o život ... :-/

Reklamný blok: Kto som

- Peter Matej (Ing., v IT 30 rokov, 25 rokov security)
- „pôvodom“ kybernetik, potom: OS admin, networker, „hacker“, pedagóg, školiteľ, security architekt, analytik, konzultant, „security evanjelista“ ?

emsec
effectively managed security

intas®
internet security

- Živím sa šetrením peňazí iným spoločnostiam

Vaša dnešná seminárna „úloha“ ?

KOMUNIKOVAŤ TÉMU
INFORMAČNÁ BEZPEČNOSŤ

Information security: slide 14/50 (aj takto sa dá prednášať ☺)

- **pridelenie prístupových práv** do určených informačných systémov osobných údajov prevádzkovateľa v rozsahu nevyhnutnom na plnenie jej úloh v rozsahu jej pracovného a funkčného zaradenia,
- **opätovné poučenie,** ak došlo k podstatnej zmene jej pracovného alebo funkčného zaradenia, a tým sa významne zmenil obsah náplne jej pracovných činností, alebo sa podstatne zmenili podmienky spracúvania osobných údajov alebo rozsah spracúvaných osobných údajov v rámci jej pracovného alebo funkčného zaradenia,
- **porušenie povinnosti mlčanlivosti** uloženej podľa § 22 ods. 2 zákona č. 122/2013 Z. z., ak je to nevyhnutné na plnenie úloh súdov a orgánov činných v trestnom konaní podľa osobitného zákona alebo vo vzťahu k Úradu na ochranu osobných údajov Slovenskej republiky (ďalej len „úrad“) pri plnení jeho úloh podľa zákona č. 122/2013 Z. z.; ustanovenia o povinnosti mlčanlivosti podľa osobitných predpisov tým nie sú dotknuté,
- **vykonávanie spracovateľských operácii** s osobnými údajmi v mene prevádzkovateľa, vrátane osobitnej kategórie osobných údajov, v rozsahu nevyhnutnom na plnenie pracovných úloh vyplývajúcich z pracovného zaradenia,
- **odmietnutie vykonať pokyn k spracúvaniu osobných údajov,** ktorý je v rozpore so všeobecne záväznými právnymi predpismi alebo dobrými mravmi,
- **na profesionálny prístup kontrolného orgánu** pri výkone kontroly,

Sociálne inžinierstvo

Manipulácia človeka za účelom získania istých pre „manipulanta“ prospešných výhod.

Spôsoby útokov v soc. inžinierstve

- Zber voľne (verejne) dostupných dát o cieli útoku
  - Aj vyberanie smetných košov
- Fyzický „útok“ / kontakt (servisný pracovník, údržba ...)
- Psychologický útok

Najčastejšie použité metódy

- Podvodný mail, alebo falošná web stránka
- Telefonický hovor
- Doručenie reklamných materiálov na CD, DVD
- Pohodenie USB / ponechanie na záujmovom mieste
- Prípadne iné zariadenie... SD karta
- Ponuka vyskúšať službu zadarmo

Štúdie „správania sa“

Universität des Saarlandes, Germany
f.gassmann@mx.uni-saarland.de

Abstract. We report the results of a field experiment where we sent to over 1200 university students an email or a Facebook message with a link to (non-existing) party pictures from a non-existing person, and later asked them about the reasons for their link clicking behavior. We registered a significant diference in clicking rates: **20% of email versus 42.5% of Facebook recipients clicked.** The most frequently reported reason for clicking was **curiosity (34%),** followed by the explanations that the message **fit recipient's expectations (27%).** Moreover, 16% thought that they might know the sender. These results show that people's decisional heuristics are relatively easy to misuse in a targeted attack, making defense especially challenging.

Štúdie „správania sa“ 2

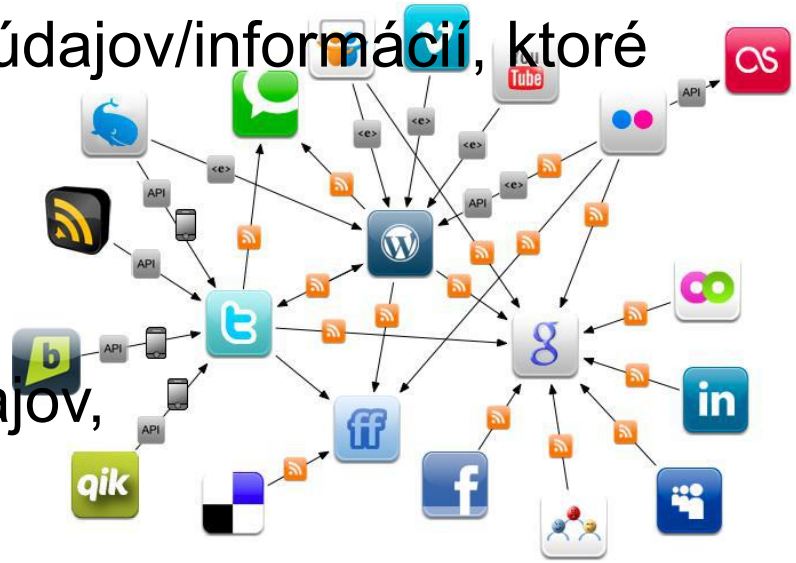
- Reakcia „bežného“ človeka – 2 experimenty:
  - University of Illinois Urbana-Champaign campus - 297 USB rozhodených po univerzitnom komplexe – obsahovali súbor „final exam“ alebo „spring break pictures“ a linku na dotazník.
  - University of Illinois Urbana-Champaign, University of Michigan a Google – 6 univerzitných komplexov

  - Rovnaký výsledok – cca 50% USB kľúč použilo (u 68% bol dôvod obyčajná zvedavosť)

  Dôsledky môžu byť zničujúce !

Riziko sociálnych sietí

- Obrovská centralizácia osobných údajov/informácií, ktoré predtým neboli nikde publikované
- Znížená ostražitosť užívateľov
- Masové správanie sa užívateľov
- Obrovské množstvo osobných údajov, správania sa, umožňuje využívať nové metodiky sledovania správania sa používateľa a predikovania jeho reakcie
- Centralizácia fotiek, videí, komentárov, ktoré sú jednoducho spojiteľné s konkrétnou osobou
- Zjednodušený prístup k osobným informáciám jednotlivca



1. príbeh: Sophie Curtis

„Neveriaci Tomáš“ resp. reportérka v novinách The Telegraph (UK)

https://www.telegraph.co.uk/technology/internet-security/11153381/How-hackers-took-over-my-computer.html

Sophie Curtis - The Telegraph

- Etický hacking reportérky novín The Telegraph - postup
- Podpísanie zmluvy s hack tímom spoločnosti Trustwave
- Scan sociálnych sietí s cieľom zistiť správanie sa a záujmy „cieľa“ (Facebook, Twitter, LinkedIn)
- Zisťovanie zraniteľností a príprava exploitu
- Podhodenie falošného kontaktu a falošnej témy na spracovanie do novín, ukážka témy v archivovanom tvare v pdf-ku

  = falošný .rar s falošným .pdf bol v skutočnosti .exe súbor
- Inštalovanie malého kódu do počítača
- Vytvorenie BotNet a prevzatie kompletnej kontroly nad počítačom
- Ovládanie kamery, mikrofónu, scan obrazovky, ...

2. príbeh: Ryba na háčiku

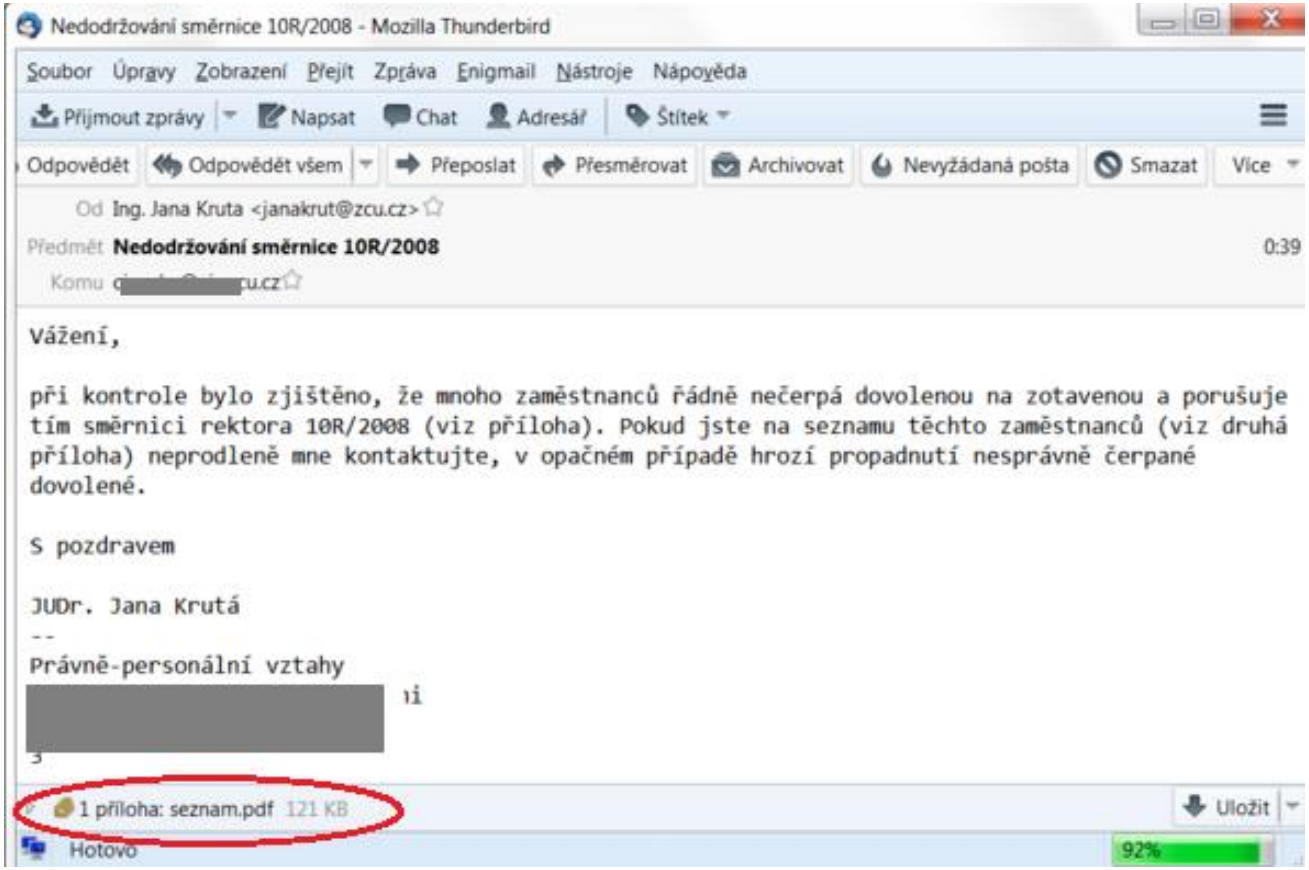
Nevinný mail, ktorý zlatú rybku donútil zaplatiť privysoké výkupné

Rybárčenie = Phishing

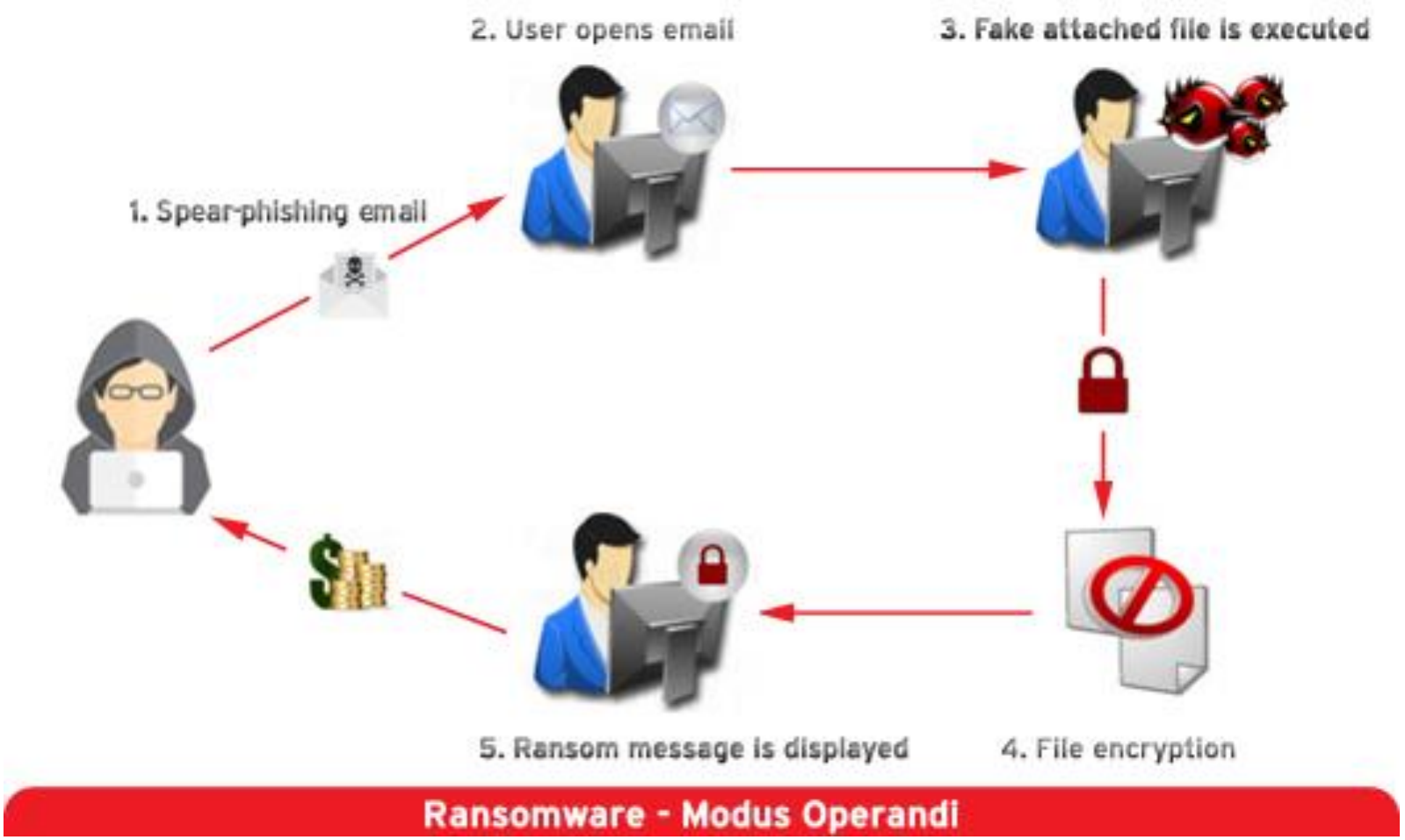
- Ak chcete úlovok, musíte použiť návnadu ...
- **Toto nie je návod !**

„nevinný, neškodný mail“

- Sociálne inžinierstvo – „každý“ je na sociálnych sieťach a prezentuje svoje záujmy / hobby / pracovné povinnosti



Kto by podozrieval pdf, však ...?



... A máme problém

Dôsledky konania

- Tím externých pracovníkov analyzoval pár dní celú firemnú komunikáciu, aby zistili, čo vlastne uniklo
- Forenznou analýzou sa zistilo, že počítač z C&C servera okrem Ransomware zrejme stiahol aj iný malware, ktorý mal sledovať heslá a tok dokumentov v sieti spoločnosti
- Aj keď nakoniec nič vážne neuniklo, pracovníčka dostala „hodinovú výpoveď“ § 68 Zákonník práce „závažne porušenie pracovnej disciplíny“ ☹
- ? A ...áno, existujú postupy ako riziko znížiť

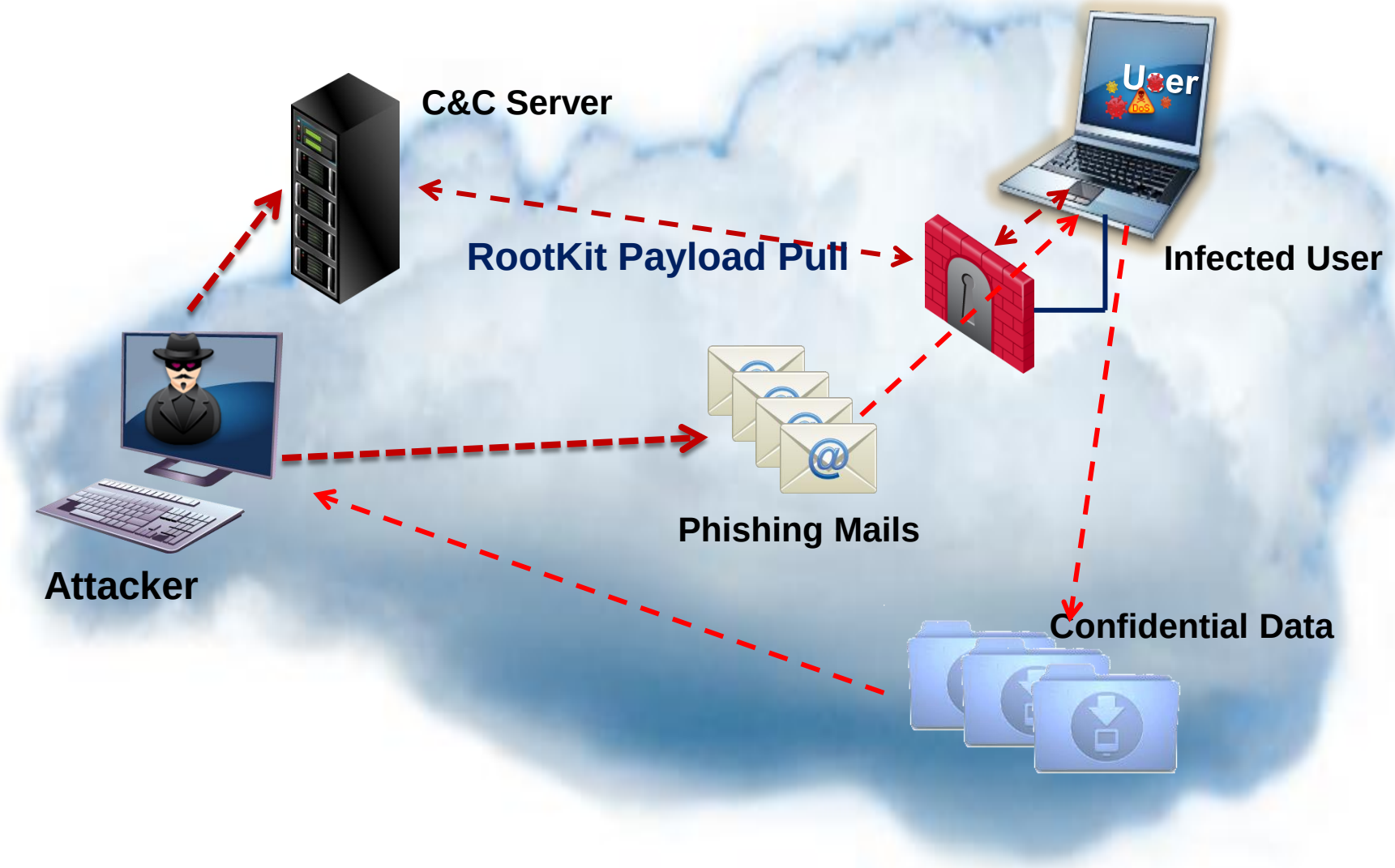
3. príbeh: „Sociálny inžinier“

Návod, ako prísť o milión dolárov

Malá firma, obchod s poľnohospodárskou technikou

- Z pohľadu útočníka možno nezaujímavá spoločnosť
- Žiadna banka... Čo už sa dá takej firme ukradnúť cez internet ...?

Začalo to „nevinne“ ...



Osudný omyl

- Monitorovaný spôsob komunikácie s dodávateľom
- Po zaslaní objednávky prišiel falošný mail od „dodávateľa“ s informáciou o zmene banky dodávateľa
- Obchodné oddelenie konalo rutinne a nepreverilo zmenu banky
- 1 milión dolárov opustilo firmu a skončilo na dočasnom účte v Anglicku
- Na omyl sa prišlo až po urgencii na zaplatenie od reálneho dodávateľa

OOOPS !

CHANDLERS MACHINERY LTD

Suppliers of

Agricultural and Industrial Machinery

PRO-FORMA INVOICE NO. 30644

Aprilie 18 2016

Sales Manager: William Saveron
CHANDLERS MACHINERY LTD.
Numarul de inregistrare: 01683985
Numar de TVA: GB 116258775
BELTON, GRANTHAM LINCOLNSHIRE, NG32 2LX
Marea Britanie
Tel: +44 (0) 7594 20 29 77
Fax: +44 0872 111 7477
Email:support@worldwide-equipment-providers.com
Web: www.worldwide-equipment-providers.com

Vehicle ID	Denumire produse si/sau servicii	Qty	Pret	Subtotal
TJX748	2009 John Deere X748	1	€ 2.335,00 (EUR)	€ 2.335,00 (EUR)
	Transport din Marea Britanie in Romania	1	0	0
	TVA	20%	€ 467,00 (EUR)	€ 467,00 (EUR
			Total:	€ 2.802,00 (EUR)

Mijloc de plata: Transfer prin cont bancar

Pasul următor: plata valorii facturii (EUR 2.802) trebuie trimisa prin transfer bancar, direct in contul companiei:

Titular de cont: CHANDLERS MACHINERY LTD
Numele bancii: BARCLAYS BANK PLC
IBAN: GB69 BARC 2076 9033 6453 63
Numar de cont: 33645363
Cod Sortator: 20-76-90
Cod Swift/BIC: BARCGB22
Tara: Marea Britanie

Mr. William Saveron/ *Sales Manager*
CHANDLERS MACHINERY LIMITED

CHANDLERS MACHINERY LTD Lincolnshire 18-APR-2016 United Kingdom VAT GB 116258775

Koniec smutný a nepoučiteľný

- Peniaze skončili v Nigérii ... nevymožiteľné

4. príbeh: STUXNET

Kybernetická zbraň, ktorá ochromila Iránsky jadrový program

Jadrový program v IRÁNE

Trocha histórie

- 2003 – Irán rozmiestňuje rakety s dlhým doletom schopné niesť jadrové hlavice (nemá ich)
- 2004 – 40 ton uránu → HF6 (hexafluoridový plyn)
  = praktický krok k výrobe atómovej zbrane
- 2005 – USA je za „tvrdý zásah“ a sankcie, Rusko poskytuje technické vybavenie a špecialistov
- 2006/1 Irán obnovuje jadrový program
- 2006/3 164 centrifúg je funkčných
- 2006 – 31. júl sankcie OSN
- 2006/8 15 nových pokročilých centrifúg ☹

Otázka... Ako ďalej ?

NATANZ, IRAN -- CLOSE-UP

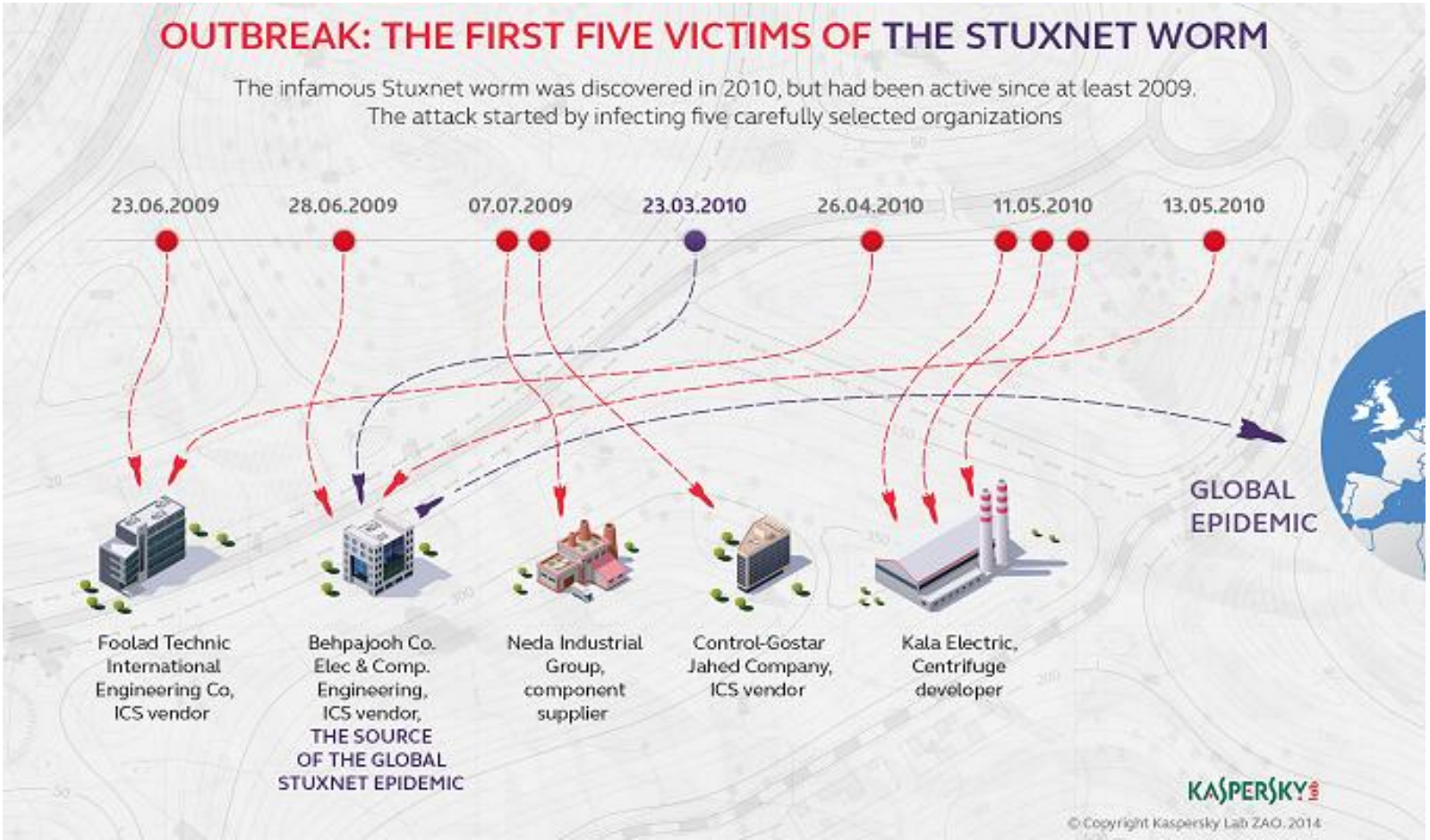
INSTITUTE FOR SCIENCE AND INTERNATIONAL SECURITY

IMAGE CREDIT: DIGITALGLOBE
DATE OF IMAGE: 16 SEPTEMBER 2002

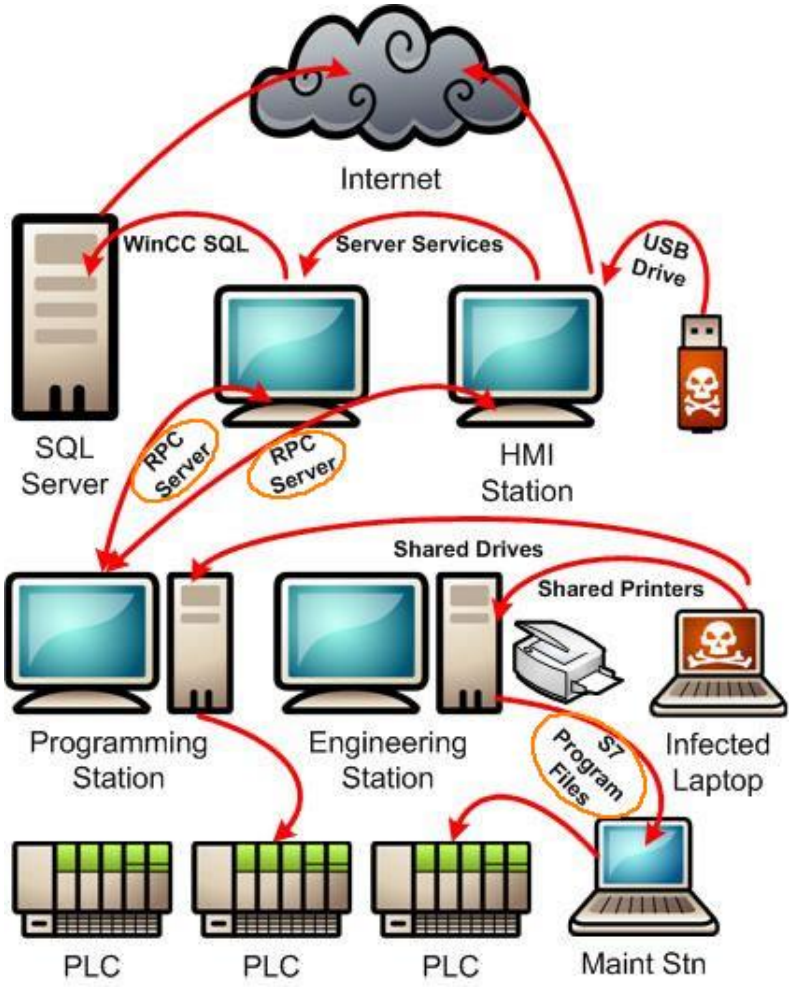
THE GAS CENTRIFUGE URANIUM ENRICHMENT PLANT AT NATANZ, IRAN.

Irán: Natanz – jadrový výskum

Cieľ však nie je pripojený na I-net



Ako sa to mohlo stať (a zrejme stalo)



Špecifiká STUXNETu

- Stuxnet je Advanced Persistent Threat (APT) zameraný na špecifický cieľ.
- Vo svojom čase – keď ho objavili- cca 2010 – bol najkomplikovanejším vírusom / worm aký bol kedy napísaný.
- Vírusy majú v priemere 10k bytes veľkosť. Stuxnet mal 500 KB (a žiadna grafika !).
- Je nezvyčajné, ak dnes vírus obsahuje čo i len jednu zero-day zraniteľnosť. Stuxnet ich mal 4.
- Stuxnet sa tiež správal ako rootkit – schovával svoju prítomnosť a aktivitu
- Bol to prvý virus, ktorý obsahoval kód na Supervisory Control and Data Acquisition (SCADA) systém.

Dôsledky Stuxnetu

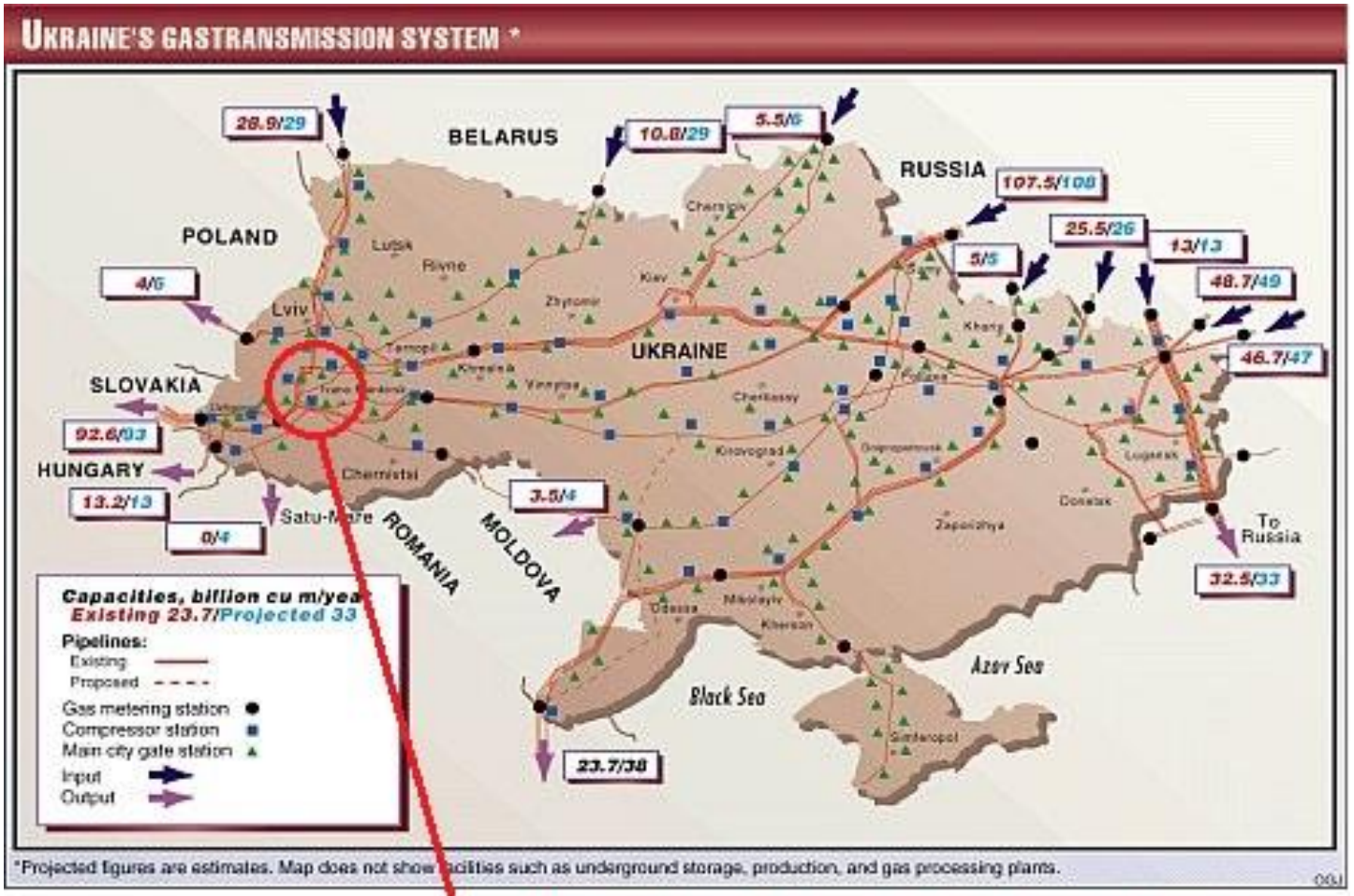
- Koncom roka 2009 alebo začiatkom roka 2010 Irán vyradil z prevádzky a nahradil približne 1 000 centrifúg IR-1 v závode na obohacovanie paliva (FEP) v Natanz
- Stuxnet výrazne spomalil jadrový program Iránu a to „jemnejšie“ ako by to urobil priamy vojenský vpád
- Stuxnet však ukázal, že je možné napadnúť aj systémy, ktoré nie sú priamo pripojené na Internet. Položil základy novej hrozbe: Grid attack

The Institute for Science and International Security:
http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/

5. príbeh: BlackOut

Útoky na energetickú sústavu

23.December 2015



Location of power system outage

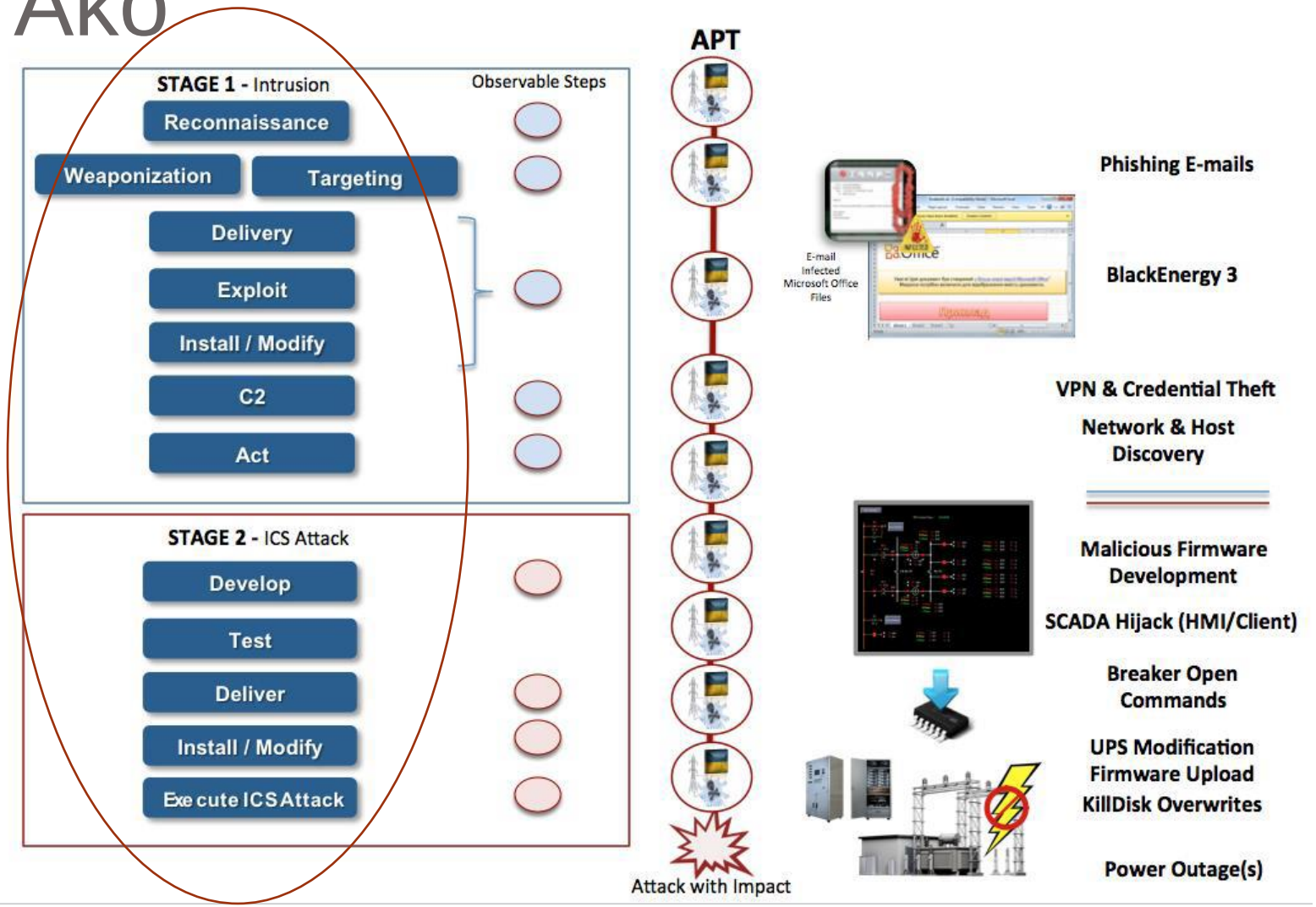
23.December 2015

- Prvý známy a úspešný kyber útok na energetickú infraštruktúru (power **grid attack**)
- Napadnuté 3 distribučné spoločnosti
- Vypnutých viac ako 30 transformátorovní
- Cca 230 000 ľudí bez elektrickej energie
- Výpadok od 1 do 6 hodín

Podrobnejšie: *Robert M. Lee; Michael J. Assante; Tim Conway (18 March 2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case (PDF). E-ISAC.*

Ako

APT = Advanced Persistent Threat



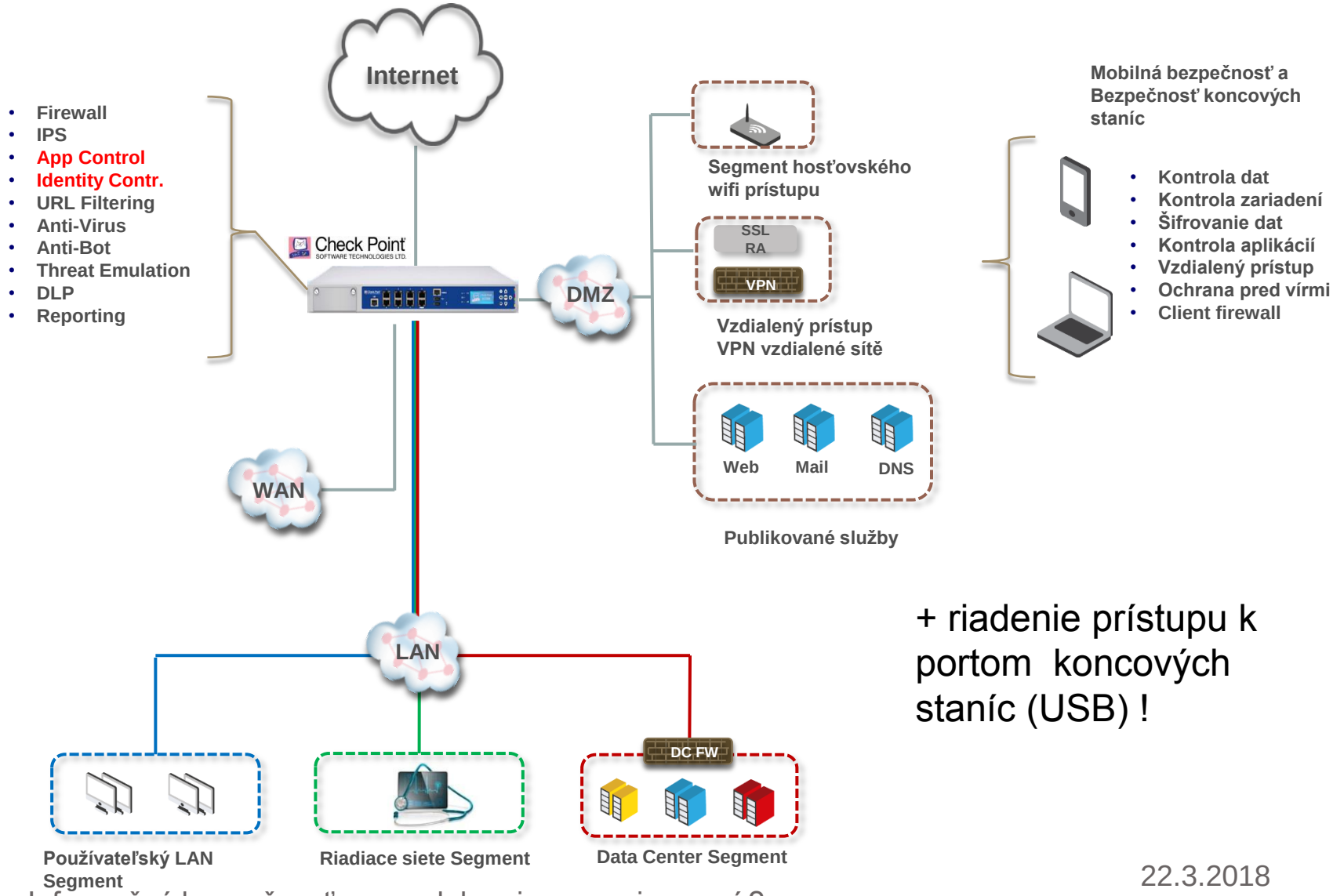
Podrobnejšie: *Robert M. Lee; Michael J. Assante; Tim Conway (18 March 2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case (PDF). E-ISAC.*

6. príbeh: Slovensko

RansomWare s úspešným koncom

... Ale „bolelo to“

Strategické riešenia - design



+ riadenie prístupu k portom koncových staníc (USB) !

Funkčný DRP vás môže zachrániť

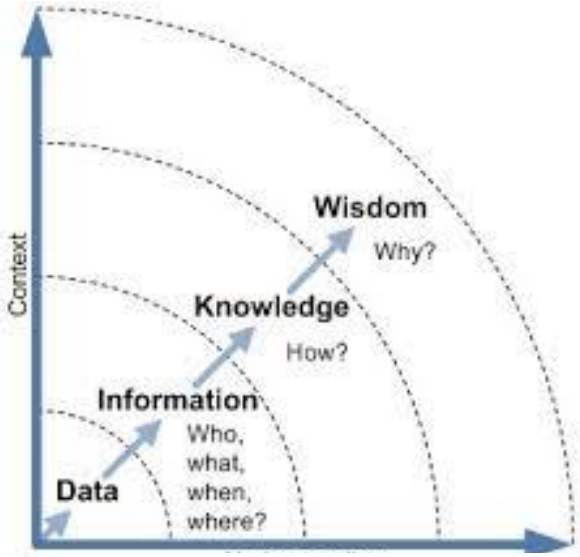
Je dobré mať istenie (dobré istenie !)

Čo je Informačná bezpečnosť ?

What „Wiki“ says?

Information security, sometimes shortened to **InfoSec**, is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.
It is a general term that can be used regardless of the form the data may take (e.g., electronic, physical).
Information security's primary focus is the balanced protection of the confidentiality, integrity and availability of data (also known as the CIA triad) while maintaining a focus on efficient policy implementation,
all without hampering organization productivity

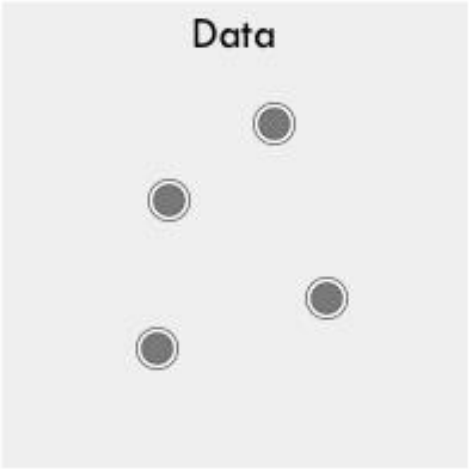
Čo hovorí norma (ISO/IEC 27002) ?

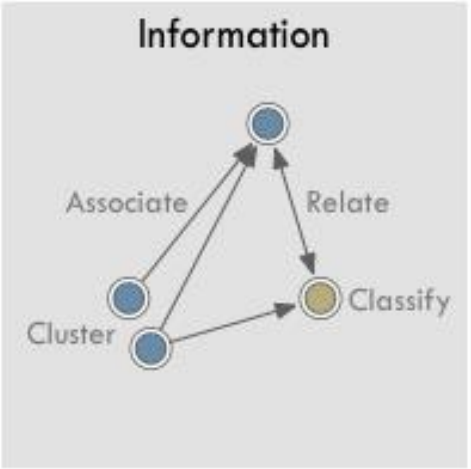


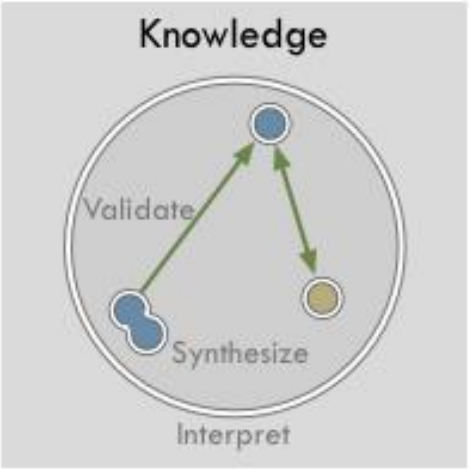
Definícia informačnej bezpečnosti:
vymedzenie, implementácia, manažment a vyhodnocovanie koherentných systémov, ktoré „merateľne“ zabezpečujú:

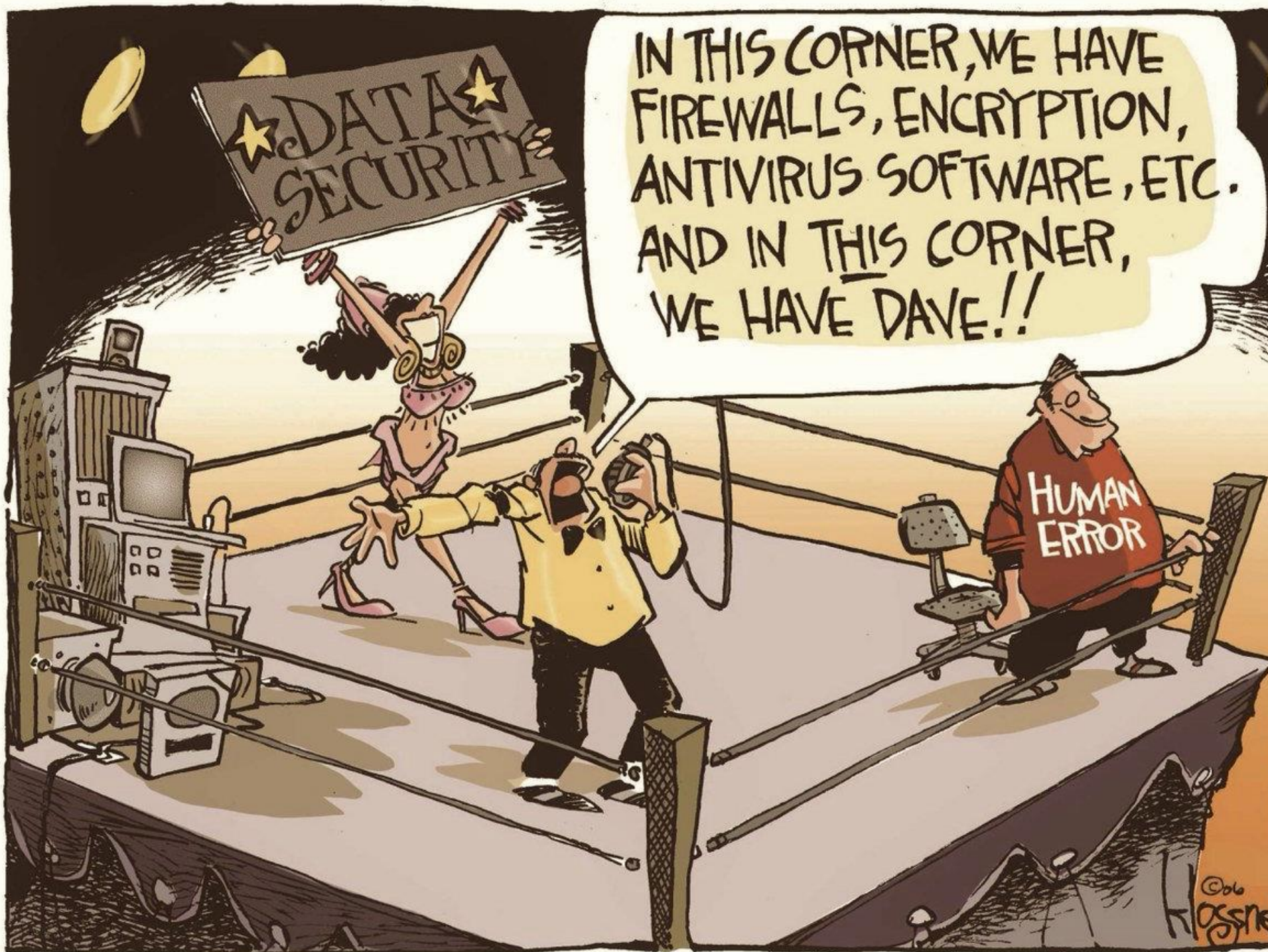
- Dôvernosť (Confidentiality)
- Integritu (Integrity)
- Dostupnosť (Availability)

ISO/IEC 27002








DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
©06

Prečo sa zaoberať s IB/IS?
1. Zákonné dôvody

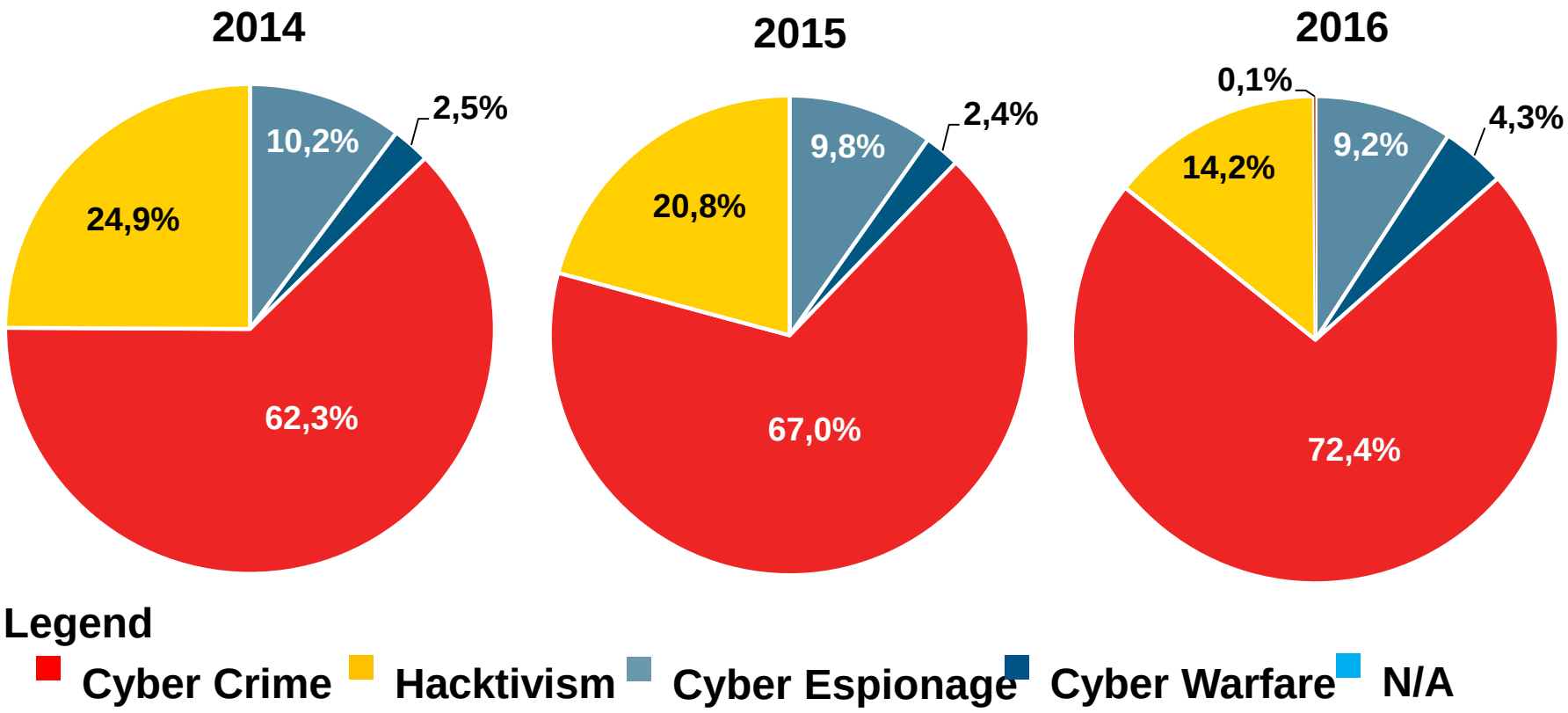
- Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy ...
- Zákon 45/2011 Z. z. - Zákon o kritickej infraštruktúre ...
- Zákon č. 351/2011 Z. z. o elektronických komunikáciách ...
- Zákon č. 18/*2018* Z. z. o *ochrane osobných údajov ...*
- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti ...

Prečo sa zaoberať s IB/IS?
2. Pragmatické dôvody

Vlastním niečo o čo by som nerád prišiel

- Ako organizácia:
  - Financie
  - Zmluvy (odberateľské, dodávateľské)
  - Výrobné postupy
  - Patenty
  - .....
- Ako osoba:
  - Financie
  - Priateľstvá a vzťahy
  - Výsledky práce
  - Fotky, videá, hudba
  - ....

Späť ku kyber útokom: Kto a Prečo



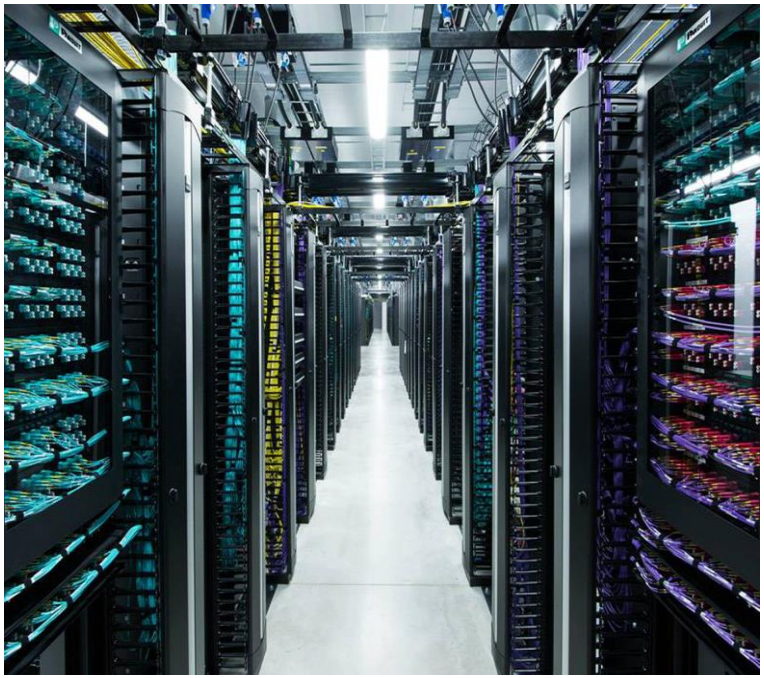
Source: Hackmageddon, http://www.hackmageddon.com/category/security/cyber-attack-statistics/

Cieľ útoku ? KTOKOĽVEK !?

Kedysi analógový svet je dnes digitálny.

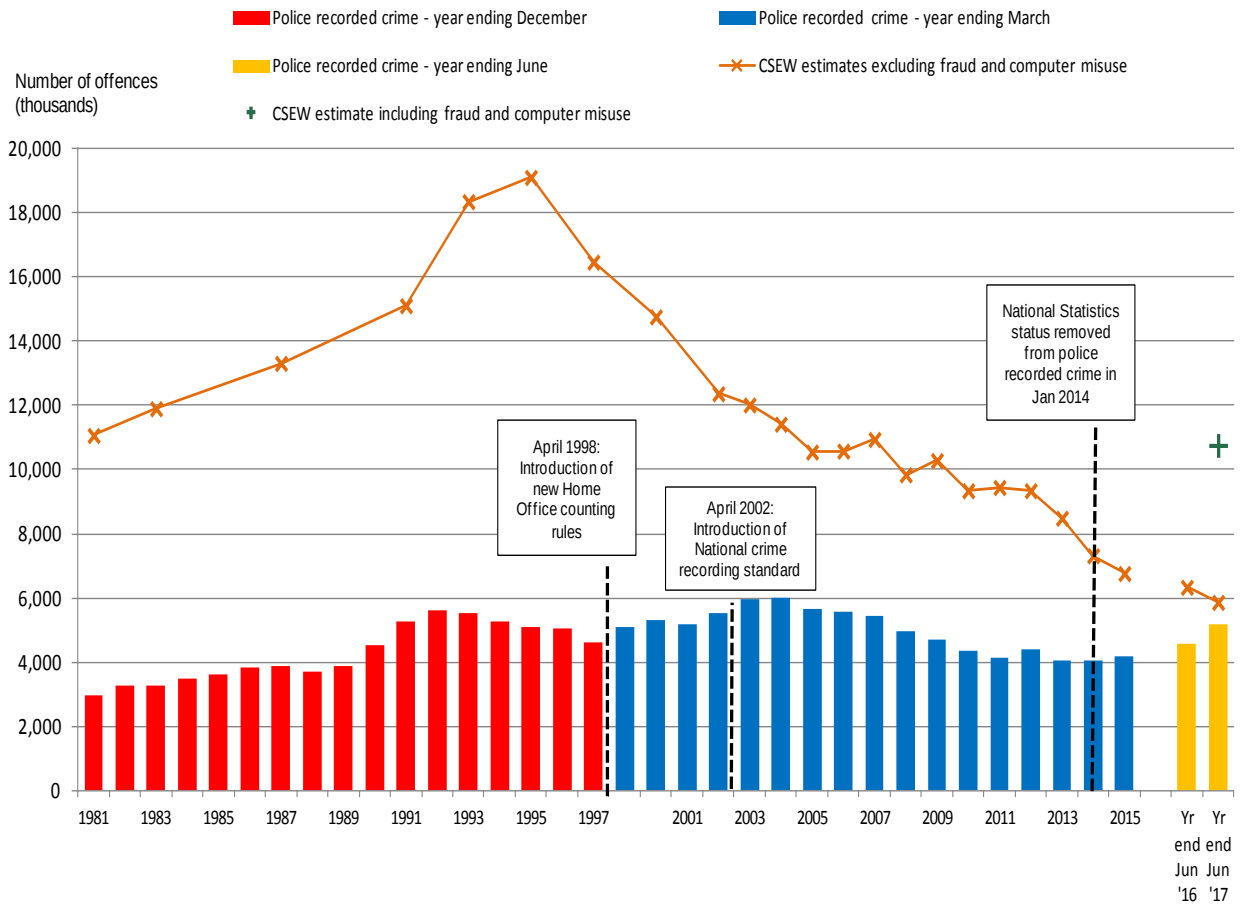
STASI archív, bývalý východný Berlín*

Facebook datacentrum, Lulea, Švédsko**



- *http://afish.ca/2017-Deutsche-Demokratische-Republik-The-Stasi-Archives
  **https://www.cnet.com/news/facebook-turns-on-data-center-at-edge-of-the-arctic-circle/

Podľa štatistík vraj kriminalita klesá.



- **Zdroj: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesbulletintables**

Digitálna kriminalita už prekonáva tú klasickú.

Table E1: Fraud and computer misuse by loss (of money or property) - number and rate of incidents and number and percentage of victims, year ending June 2017 CSEW (Experimental Statistics)[1,2]

England and Wales

Offence group[3]	Number of incidents (thousands)	Rate per 1,000 adults	Adults aged 16 and over: Number of victims (thousands)[4]	Adults aged 16 and over: Percentage victims once or more[4]
FRAUD[5]	3 339	72	2 765	6,0
With loss, no or only partial reimbursement	567	12	500	1,1
With loss, fully reimbursed	1 858	40	1 550	3,3
Without loss	915	20	801	1,7
Bank and credit account fraud	2 513	54	2 062	4,5
With loss, no or only partial reimbursement	269	6	211	0,5
With loss, fully reimbursed	1 671	36	1 396	3,0
Without loss	573	12	510	1,1
Consumer and retail fraud[6]	727	16	674	1,5
With loss, no or only partial reimbursement	276	6	268	0,6
With loss, fully reimbursed	185	4	165	0,4
Without loss	266	6	241	0,5
All other fraud[7,8]	100	2	79	0,2
With loss, no or only partial reimbursement	23	0	21	0,0
With loss, fully reimbursed	1	0	1	0,0
Without loss	76	2	57	0,1
COMPUTER MISUSE	1 607	35	1 252	2,7
Computer virus[9]	1 071	23	824	1,8
With loss, no or only partial reimbursement	303	7	276	0,6
With loss, fully reimbursed	4	0	4	0,0
Without loss	764	17	554	1,2
Unauthorised access to personal information (including hacking)	535	12	458	1,0

- **Medziročný nárast len pri podvodoch o 21%.**

Zdroj: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables

Kriminalita a digitálny svet

- **Kriminalita neklesá,**
- **presúva sa online ako všetko ostatné.**

„Živná pôda“ pre Kyberkriminalitu

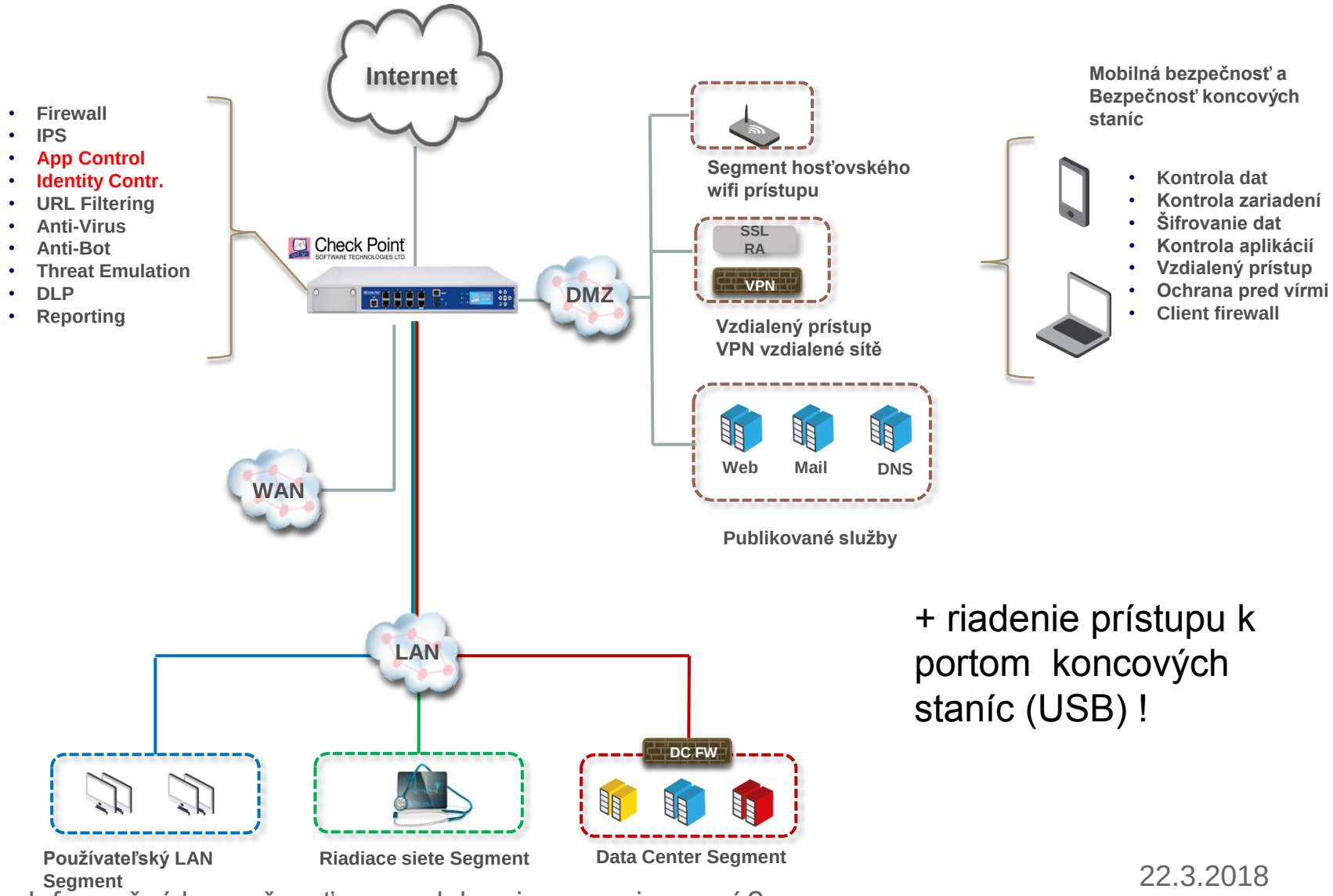
- Závislosť spoločnosti od Internetu
- Kyberkriminalita sa stala výnosným globálnym biznisom
  - Crime-as-a-Service
- Minimálna bezpečnostná gramotnosť obrovského množstva používateľov
- Previazanosť personálnych a pracovných IKT nástrojov
- Protokolová sada TCP/IP

Svet bude SMART ...či ?

Strategické bezpečnostné rozhodnutia

- Zodpovedný prístup k **osobným údajom** (vlastným a cudzím)
- Vybudovanie a udržiavanie strategického bezpečnostného riešenia (na produktoch svetových lídrov)
- Dôsledné poznanie vlastnej siete, komunikácie, aplikácií, včasné rozpoznanie podozrivej komunikácie
- Poznanie komunikačných potrieb, predikcia riešení, ich testovanie až tak nasadenie do produkčného prostredia
- Funkčné plány riešenia havarijných situácií (aj v IT)
- Rozumné regulačné opatrenia v oblasti informačnej a dátovej bezpečnosti (nariadenia, smernice, opatrenia) a kontrola ich dodržiavania

Strategické riešenia – start design



+ riadenie prístupu k portom koncových staníc (USB) !

Viacvrstvová ochrana perimetra: Threat Prevention Solution

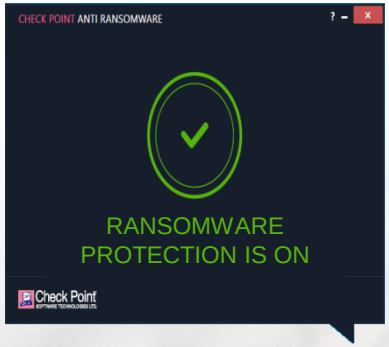
KNOWN

UNKNOWN

Antivirus	Blocks download of known malware infested files
IPS	Stops exploits of known vulnerabilities
Anti-Bot	Prevents bot damage from infected devices
Threat Emulation	Stops unknown zero-day malware in files
Threat Extration	Removes potentially malicious content from files

Anti-Ransomware

ONGOING



BEHAVIORAL ANALYSIS

Constantly monitor for ransomware specific behaviors

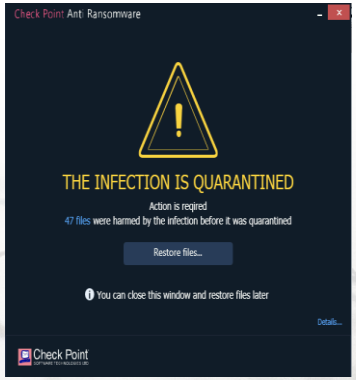
DATA SNAPSHOTS

Continuously create short-term file backups

UPON DETECTION

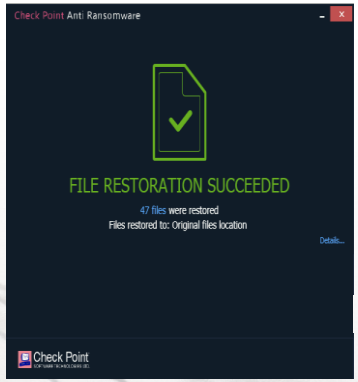
ANALYZE

Initiate forensic analysis to analyze attack details



QUARANTINE

Stop and quarantine all elements of the attack



RESTORE

Restore encrypted files from snapshots

Čo na záver ?

Raz aj human(oid) bude SMART !

Court unseals details on **Stuxnet** leak probe
Politico (blog) - Jan 11, 2018
The court records say that on June 1, 2012, the day an excerpt from Sanger's book appeared in the Times outlining the **Stuxnet** operation against Iran, a former ... The court records were made public as a **result** of a court application filed last year by the Reporters Committee for Freedom of the Press, which ...

Cyberattacks could lead to use of nuclear weapons
New Atlas - Jan 11, 2018
The world's nuclear weapons may be more vulnerable to cyber attacks than previously thought and could **result** in an accidental missile launch ... The study sites the **Stuxnet** virus, which crippled the Iranian nuclear weapon program when it was introduced through a thumb drive, and reports that the ...

Will Trump go nuclear over cyber warfare?
IT PRO - Feb 2, 2018
Yes, cyber attacks can be extremely disruptive, but they are generally speaking not destructive and don't **result** in mass casualties. ... While there's never been any official confirmation (and there probably never will be), it's widely thought that the **Stuxnet** virus was crafted as a joint enterprise by US and ...

Giving Cyber Threats the Nuclear Treatment
Innovation & Tech Today (satire) (press release) (blog) - Jan 20, 2018
Regardless of whether the decision was right or wrong, the **results** were devastating. Seventy-two ... The creation of **Stuxnet** continued to up the ante, as the virus was used against a nation-state (Iran) during the Bush administration in the 2000s for the purpose of disabling nuclear capability. With this new ...

Will explosive data exfiltration continue in 2018?
Help Net Security - Jan 23, 2018
"As a **result**, we should expect to see escalations and variations of similar attack vectors this year." ... A nation-state with this power can bombard critical infrastructure through increasingly sophisticated variations of attacks, sabotaging core services using attacks derived from **Stuxnet** and Duqu.