

Človek ako súčasť informačného systému

Hlavné výzvy účinnej ochrany

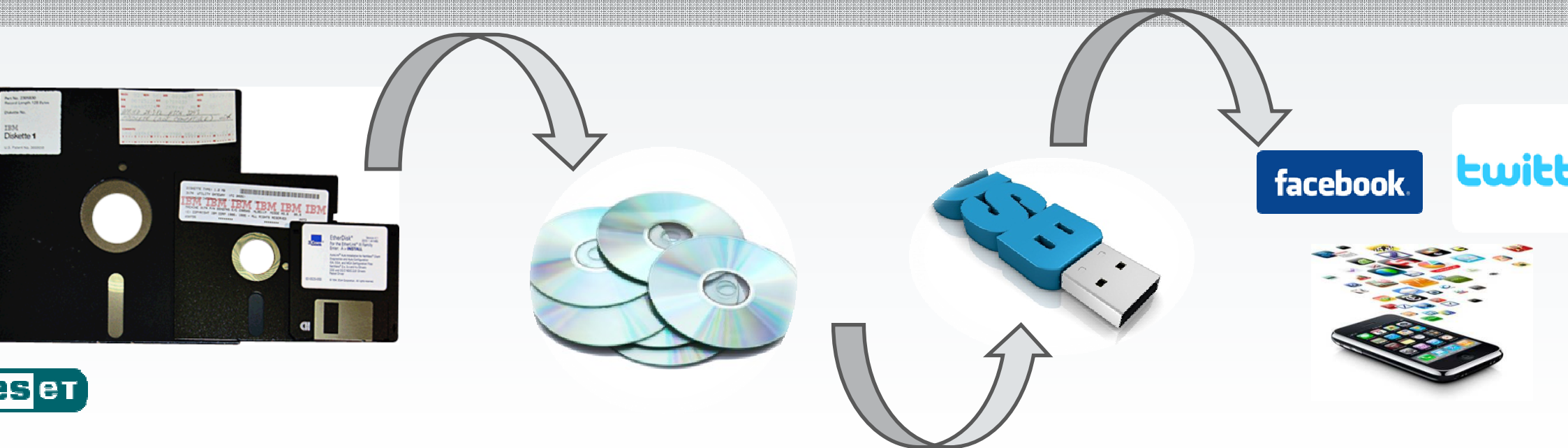
Peter Katrinec

ESET Services

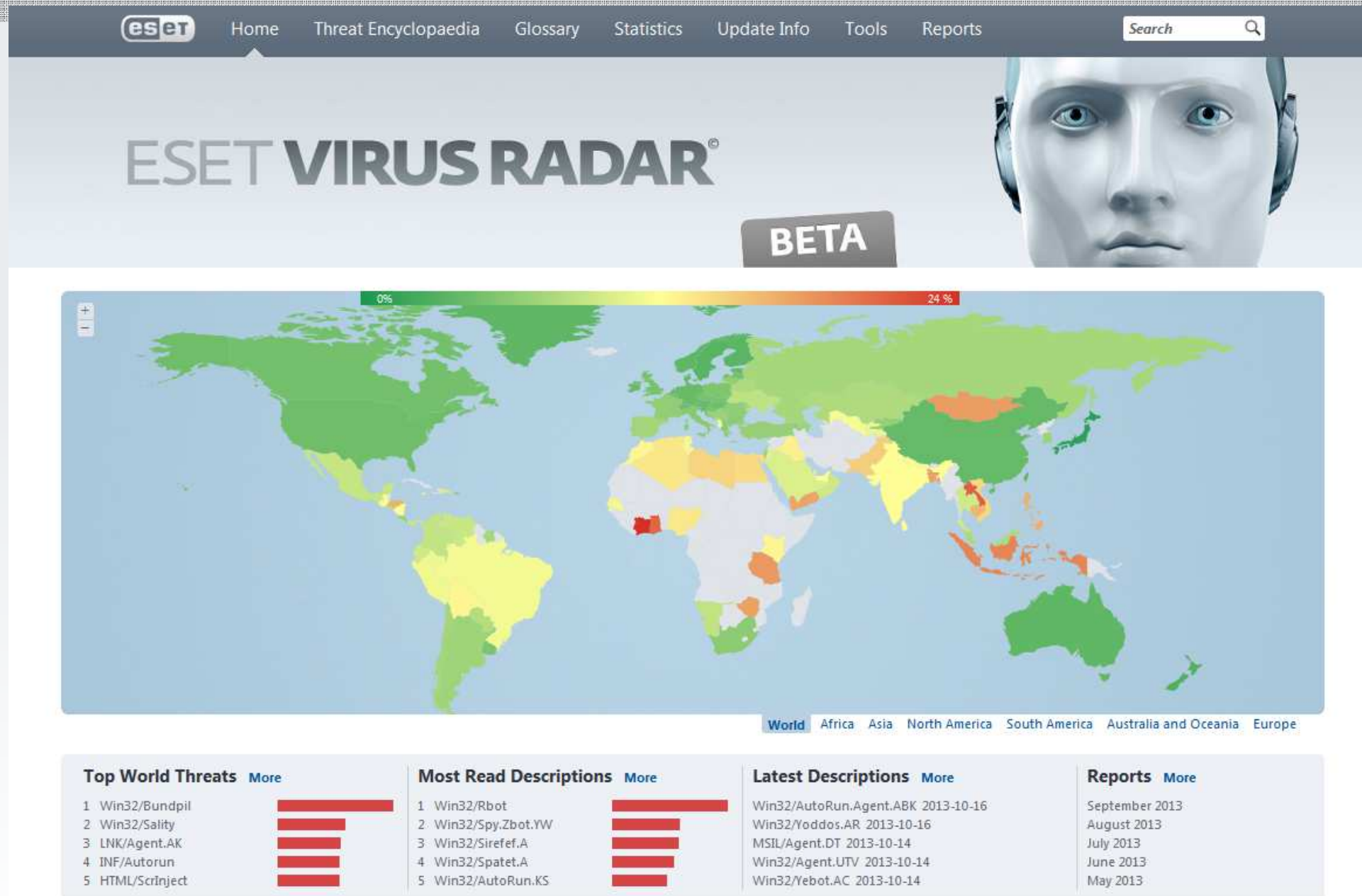
AGENDA

- Škodlivý kód a techniky sociálneho inžinierstva
- Sociálne inžinierstvo – útok na človeka
- Človek ako súčasť systému - reálny stav povedomia
- Odporúčenie, ako znížiť riziko

Kde všade je člověk zranitelný?



Čo hovoria štatistiky?



ESET VIRUSRADAR - Top 10 / Slovensko

Top Threats

Slovakia

Month

Threat Name

Cha

- 1 [VBS/CoinMiner](#)
- 2 [HTML/IFrame](#)
- 3 [Win32/TrojanDownloader.Small.AAB](#)
- 4 [VBS/TrojanDownloader.Agent.NID](#)
- 5 [JS/Kryptik.RE](#)
- 6 [HTML/Ransom](#)
- 7 [Win32/Adware.MultiPlug](#)
- 8 [Java/Exploit.Agent.PUE](#)
- 9 [JS/Adware.Yontoo](#)
- 10 [JS/Chromex.Agent.D](#)

Slovakia

Month



Zostávajúci čas: 47:56:09



PIN kód

Odoslať

Kde môžem získať peňažné poukážku
PaySafeCard?

Prehľad predajcov: PaySafeCard dostanete v mnohých supermarketoch, trafikách. PaySafeCard dostanete na viac ako 101 čerpacích staniciach Agipu a OMV, vo vybraných pobočkách stávkovej kancelárie Tipsport, všetkých predajných miestach GÖ Tabaku a vo CBA.



VAROVANIE! Vaš osobný počítač je uzamknutý z bezpečnostných dôvodov by z nasledujúcich dôvodov:

Ste obvinený z prezerania/skladovania a/alebo distribúcia pornografických materiálov zakázané obsahu (detská pornografia/zvierackosť atď) za ste porušil Všeobecnú deklaráciu o boji proti šíreniu detskej pornografie a obvinený z trestného činu podľa článku 161 trestného zákonníka Slovenskej republiky.

Článok 161 trestného zákonníka Slovenskej republiky ustanovuje ako trest odňatia slobody v trvaní 5-11 rokov.

Tiež ste osoba podozrivá z porušenia "zákon o autorskom práve a právach súvisiacich s právom" (stahovanie pirátskej hudby, videa neletenzionného softvéru) a použitia a/alebo šírenie obsahu chráneného autorským právom. Tým ste osoba podozrivá z porušenia článku 148 trestného zákonníka Slovenskej republiky.

Článok 148 trestného zákonníka Slovenskej republiky, musí byť trest pokuty 150 až 550 základných jednotiek alebo odňatia slobody na dobu 3-7 rokov.

S počítačom došlo k neoprávnenému prístupu k obmedzenému prístupu verejnosti k informáciám a informáciám celoštátneho významu v Internete.

Neautorizovaný prístup si môžete dojednať zámerne z sebeckých motívov alebo neoprávneným prístupom môže dôjsť bez vášho vedomia alebo súhlasu, ako váš osobný počítač môže byť napadnutý škodlivým softvérom. Preto, ste podozrenie, že skúmate, neúmyselné porušenie článku 215 trestného zákonníka Slovenskej republiky (ďalej len "zákon neopatrní a nedbalé používanie počítačov/PC").

Článok 215 trestného zákonníka stanovuje pre Slovenskú republiku ako trest pokuty až do výšky €100.000 eur a/alebo trest odňatia slobody na dobu od 5 do 8 rokov.

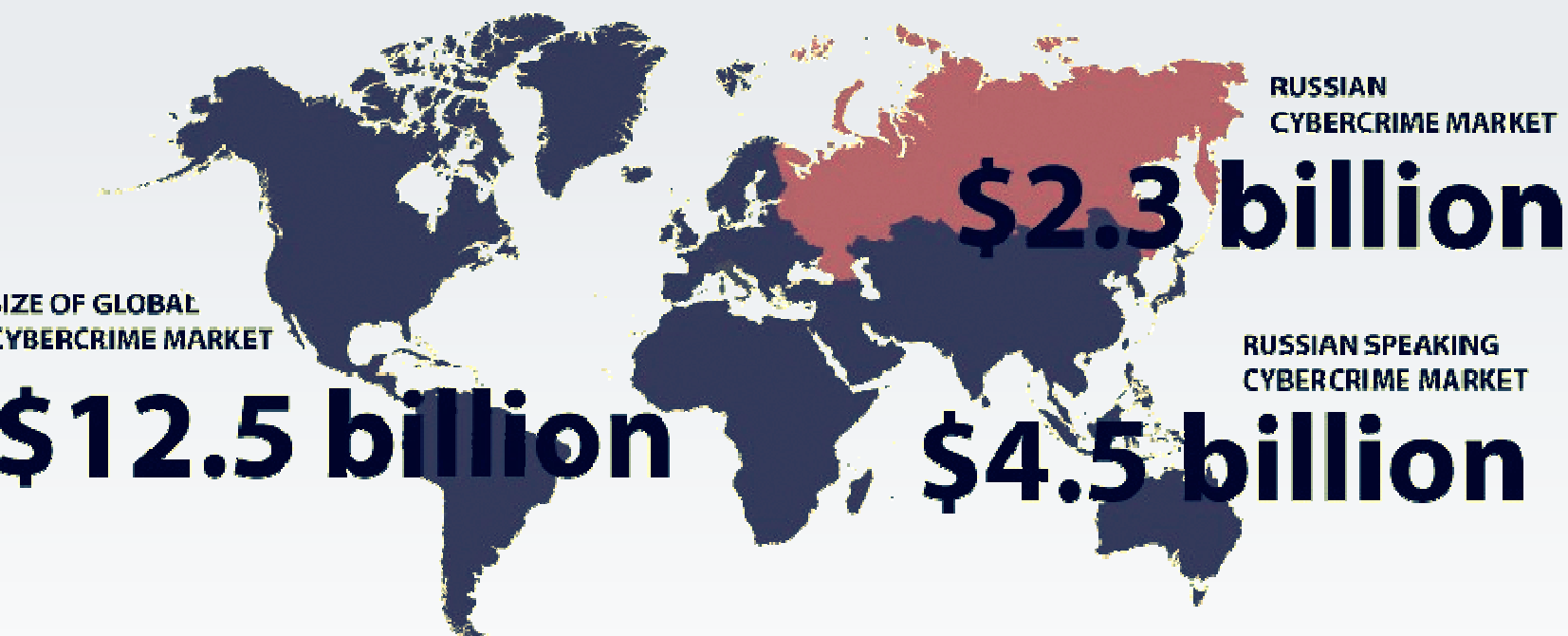
Tiež v analýze informácií uložených na vašom osobnom počítači, bolo zistené, že z počítača na pravidelnom základe je hromadné rozosiľovanie nevyžiadanej pošty, si zámerne zariadil žoldniera motívy alebo osoby, ktoré bez vášho vedomia alebo súhlasu, ako váš počítač môže byť napadnutý škodlivým softvérom. Tieto pošty šíria škodlivý softvér alebo zakázané pornografické materiály. Preto, ste účtované vyšetrenie neúmyselné porušenie Satja 301 Trestného zákona Slovenskej republiky (ďalej len "zákon o boji proti šíreniu spamu a malware (vírusy)").

Článok 301 trestného zákonníka Slovenskej republiky stanovuje sankciu pokuty až do výšky €250.000 eur a trest odňatia slobody až na 5 rokov.

Vezmite prosím na vedomie, že vaše osobné údaje a Vaša poloha je identifikovaná a proti vám môžu byť stuhani počas 96 hodín porušenie podľa trestného zákona, ako je popísané vyššie. Spís

Svet kybernetického zločinu

Total Cybercrime Market *IN U.S. DOLLARS*

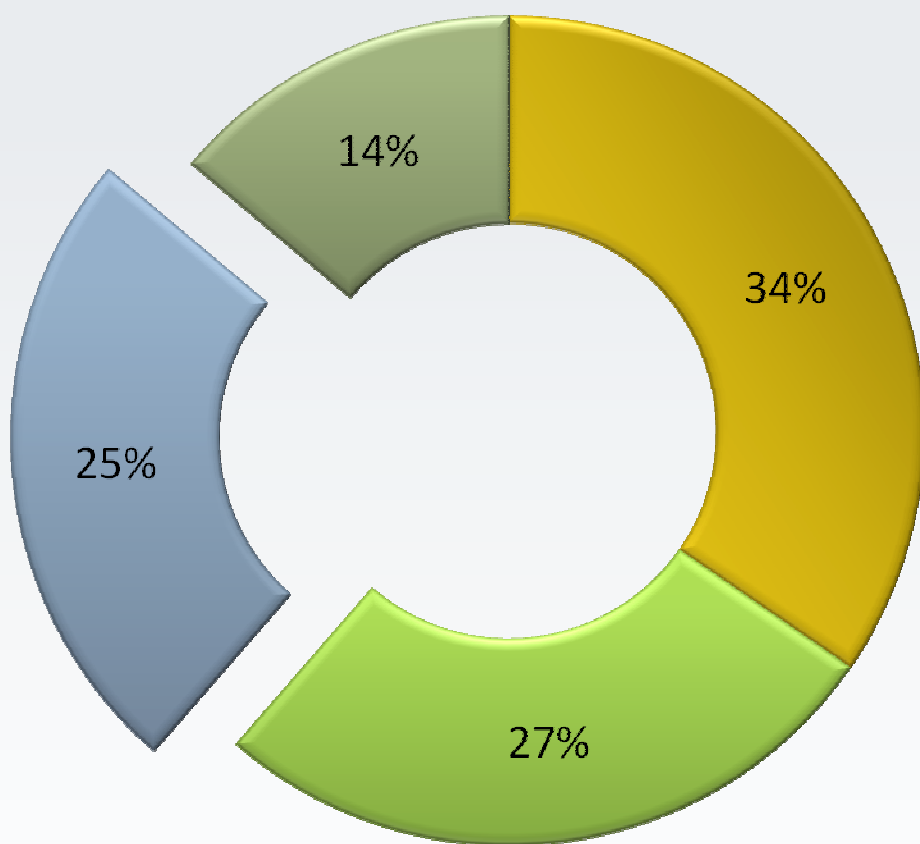


Online fraud: 41%
Spam: 36%
Internal market: 10%
DDos: 5,6%

Source: <http://www.group-ib.com/>

Štatistika o budovaní povedomia v oblasti IB

Organizujete programy pre zvýšenie bezpečnostného povedomia zamestnancov a školenia o informačnej bezpečnosti?



- Len pri prijatí nového zamestnancu
- Nie, neorganizujeme školenia o informačnej bezpečnosti
- Áno, systematicky vzdelávame zamestnancov
- Len v prípade výskytu bezpečnostného incidentu



**SOCIAL
ENGINEERING**
The clever manipulation
of the natural human
tendency to trust.

Sociálne inžinierstvo vo svete

zloději ukradli desetitunový most a zaujali celý svět

12 10:38

Pozornost médií ze všech koutů světa získali čeští zloději, kteří za bílého dne u Horního Slavkova ukradli desetitunový most z oceli.

st desetitunový
před několika

ivního Správy
li, ukradli ještě

Columnists on ENRIAN.ru
Sacred Monsters of Ru
Daniel Kalder

RUS ENG DEU FRA
12/07 07:12 11:00 180000 40 500
01/08 08:00 10:00 180000 40 500
FEATURES, OPINION & ANALYSIS

STRANGE
Steal 10-Ton Rail

01/08 08:00 10:00 180000 40 500
FEATURES, OPINION & ANALYSIS

01/08 08:00 10:00 180000 40 500
FEATURES, OPINION & ANALYSIS

01/08 08:00 10:00 180000 40 500
FEATURES, OPINION & ANALYSIS

01/08 08:00 10:00 180000 40 500
FEATURES, OPINION & ANALYSIS

01/08 08:00 10:00 180000 40 500
FEATURES, OPINION & ANALYSIS

01/08 08:00 10:00 180000 40 500
FEATURES, OPINION & ANALYSIS

01/08 08:00 10:00 180000 40 500
FEATURES, OPINION & ANALYSIS

Slovensko Krimi v SR



V banke sa vydával za konateľ'a, odišiel s

SME blog

[Správy](#) [Regióny](#) [Služby](#) [Nakupujte](#)

sme.sk > [blog.sme.sk](#) > [cernek.blog.sme.sk](#) > Nezaradené

[DISKUTUJTE](#) [VYTLAČIŤ](#) Pošlite: [E-MAILOM](#) [NA FACEBOOK](#) [VYBRALI SME](#) [ĎALŠIE](#)

karma článku: 15,96 ; prečítané: 16842 x

Falošný kontrolór úradu ochrany osobných údajov

Prišiel pán v obleku. Predstavil sa ako inšpektor úradu ochrany osobných údajov. Ja som v práci ešte nebol a kolega je zvyknutý na kontroly rôzneho charakteru. Minulý rok sme ich mali z rôznych inštitúcií asi osem či deväť. Z času na čas nás dokonca navštívi aj človek, ktorý kontroluje poradie vlajok v mojej kancelárii (nestrielam si, to je fakt). Nepovažoval teda túto „milú“ návštevu za nič mimoriadne. Dokonca ani dôvod plánovanej pokuty - kamerový systém, sa mu nezdal nijako neopodstatnený. Pánovi „inšpektorovi“ len vysvetlil, že zbytočne sa vyhráža tisíckami eur a zbytočne to sťahuje na 500 €, momentálne riešime, ako zaplatíme faktúru za plyn.

Doporučil mu, nech sa porozpráva so mnou, „predsa len, pán riaditeľ je štatutár...“, keď to ale veci pomôže, je ochotný okamžite kamery odstrániť. Pán „inšpektor“ pochopil, že tu nepochodí. Bol ale láskavo ochotný vrátiť sa neskôr. Kolega mi samozrejme okamžite zavolať a už riešil, kde vezmeme peniaze.

Existuje len málo zákonov, ktoré si myslím, že ovládam, ale zákon o ochrane osobných údajov mi naozaj nie je cudzí. Prišlo mi to divné celé. Spôsob vykonania kontroly aj dôvod pokuty. Nedávno sa zákon novelizoval, tak som si chcel overiť, či predsa len nie je dôvod takejto, i keď mimoriadne novátorskej kontroly a najmä dôvodu okamžitého udeľovania pokuty.

Jozef

Píšem o tom, čo stojí za to. O tom, čo stretávam dnes a možno stretnem zajtra. Píšem o tom, na čo som prišiel a chcem vám povedať.

Celková karma: 15,88 (VIP)

O mne:

Som človek a vnímam tento život, verím, že existuje dôvod prečo vznikol. Pracujem ako riaditeľ súkromnej spoločnosti. Popri tom "šéfujem" Matici

počke banky hotovost' 350-tisíc eur. Polícia



Foto: SITA/AP

Operátor ich prepojil priamo na oddelenie, kde leží Catherine. Službukonajúca sestra ich tvrdeniu uverila a poskytla im krátku informáciu o aktuálnom stave prominentnej pacientky.

Sociálne inžinierstvo vo svete

Varovanie! Na území Slovenska a Česka ohrožujú kybernetickí zloději

7. október 2013
Zdroj: noviny.sk

BRATISLAVA - Ak používate internet bankingu, mali by ste byť na vzhľad svojich západných susedov úradujú kybernetickými zločincami. Ohrožujú účty niekoľkých bankových klientov. Pôsobí na území Slovenska a Česka aj Česká bankovní asociácia. Nebezpečenstvo sa týka iba na klasické počítače, no prenikajú aj do smartphonov.

Kto si aplikáciu nainštaloval, mal problém

Čoraz viac svojich aplikácií. Práve na smartphony sa v posledných dňoch úradovali v Česku. Okrem falošných bankovníckych stránok sa objavili aj aplikácie. Stačil na to jednoduchý trik.

„Pozmenená webová stránka tvrdila, že banka pre nich pripravila nové zabezpečenie tohto internetového bankovníctva,“ hovorí F. Matoušek. Ten, kto si túto aplikáciu nainštaloval, mal problém. SMS bankovníckych zloději.



ČESKÁ BANKOVNÍ ASOCIACE

Tisková zpráva

Česká bankovní asociace varuje před novou formou hackerských útoků

Podobné případy se objevily i v dalších evropských státech

Praha, 4. 10. 2013 – České bankovníctví zaznamenalo v těchto dnech novou formu hackerských útoků. Jejich cílem je ovládnout klientův počítač, získat tak přístup k jeho internetovému bankovníctví a následně převést peníze na útočníkův účet. Podle odborníků na kybernetiku je útok rafinovanější než většina předchozích případů. Vyznačuje se tím, že se snaží obejít i standardně používanou dvoufaktorovou autentizaci ovládnutím nejen počítače, ale i chytrého telefonu. „Systémy bank napadeny nejsou, útok míří primárně na klienty, a proto považujeme za nezbytné klienty především varovat. Cílem útoku může být kterýkoliv uživatel internetového bankovníctví,“ řekl Jan Matoušek, náměstek výkonného ředitele ČBA.

Podle informací expertů na zabezpečení bankovních systémů jsou útoky hackerů vedeny prostřednictvím viru (trojského koně). Ten se snaží v několika stupních obejít autentizaci klienta tak, aby útočníci mohli provádět neautorizované transakce na jeho účtu. Zejména pokud klient nechá v zavazadlech počítačovou kartu, je možné jeho účet napadnout. Novým zjištěním je pak to, že se útočníci snaží napadnout i mobilní telefony, a získat tak přístup i k účtům klientů, kteří používají při práci s internetovým bankovníctvím ověřovací SMS zprávy. K tomu dochází tak, že je klient nevědomky přesměrován do podvrženého internetového bankovníctví, a zde je vyzván k instalaci programu (škodlivého malware) na svůj chytrý telefon.

Vedle České republiky byly podobné hackerské útoky zaznamenány také v dalších evropských státech – především ve Velké Británii, Portugalsku nebo Turecku.

Sociálne inžinierstvo vo svete

ODAY Tech follow us      

all on the show social media tips your gadgets trending

Social Media

Family robbed after teen posts photo of Facebook

Rosa Golijan
NBC News

May 29, 2012 at 10:53 AM ET

On Thursday, a teenage girl posted a photo of a "large sum of cash" on Facebook. About seven hours later, two robbers arrived at her family's home. Unsurprisingly, this incident prompted local authorities to issue a warning about the dangers of posting photographs online.



According to BBC News, the 17-year-old girl was helping her 72-year-old savings when she decided to snap a photo of the money and post it on Facebook. **local police force** explains that this social media activity occurred in Sydney, Thursday. At 11:30 p.m. on the same day, a house about 75 miles south-west of Sydney was robbed. The girl's mother, a 58-year-old man and a 14-year-old boy were home at the time.

Svet Svet



Muž sledoval nahú ženu v bazéne, jej manžel mu vykradol dom

Autor: SITA, 11. júla 2013 14:41

Nahá žena rozptýľovala svojho suseda, kým jej manžel odcudzil predmety v hodnote asi dvetisíc dolárov.

BRATISLAVA 11. júla (WEBNOVINY) - Istý Stephen Amaral z mesta Crossville v Tennessee zažil nepríjemné prekvapenie po tom, ako dovolil susedovej manželke kúpať sa v jeho bazéne bez plaviek.

Kým ju totiž 20 minút sledoval, jej muž mu vykradol dom.

Dvojica najprv prišla za Amaralom s tým, či by si žena nemohla zaplávať v jeho bazéne. Keď jej to dovolil, manžela poslala po cigarety. Následne sa Amarala spýtala, či sa môže vyzliecť, s čím nemal problém. V skutočnosti ho ale chcela rozptýliť, aby jej muž mohol vniknúť do domu.



Ilustračné foto: Mountfield

"Priniesol som jej uterák, usušila sa a zrazu bola opäť celá mokrá," povedal pre televíziu WKRN.

Týka sa problém aj nás?

Výsledky testov v organizáciách na Slovensku
z roku 2013

Phisingové emailové testy



Phishingové emailové testy

Na phishingový email s podvrhnutou linkou alebo prílohou kliklo:

S linkou: **63 %** cieľových osôb (60 z 95)

S prílohou: **42 %** cieľových osôb (23 z 55 pokusov)

Spolu úspešných: **55 %** pokusov

Phishingové testy – možné dôsledky

- Presmerovanie na web stránky s falošným obsahom (link)
- Spustenie škodlivého kódu v internej sieti (príloha)
- Vytvorenie komunikačného kanálu do internej siete
- Spustenie „keylogger“ – odosielanie zaznamenaných údajov
- Pripojenie PC do botnetu
- Prevzatia kontroly nad PC
 - Zmena, vymazanie, krádež údajov z lokálneho PC alebo sieťových úložísk

Phishingové útoky je možné realizovať na veľký počet adresátov.



Testy prenosnými médiami (Baiting)

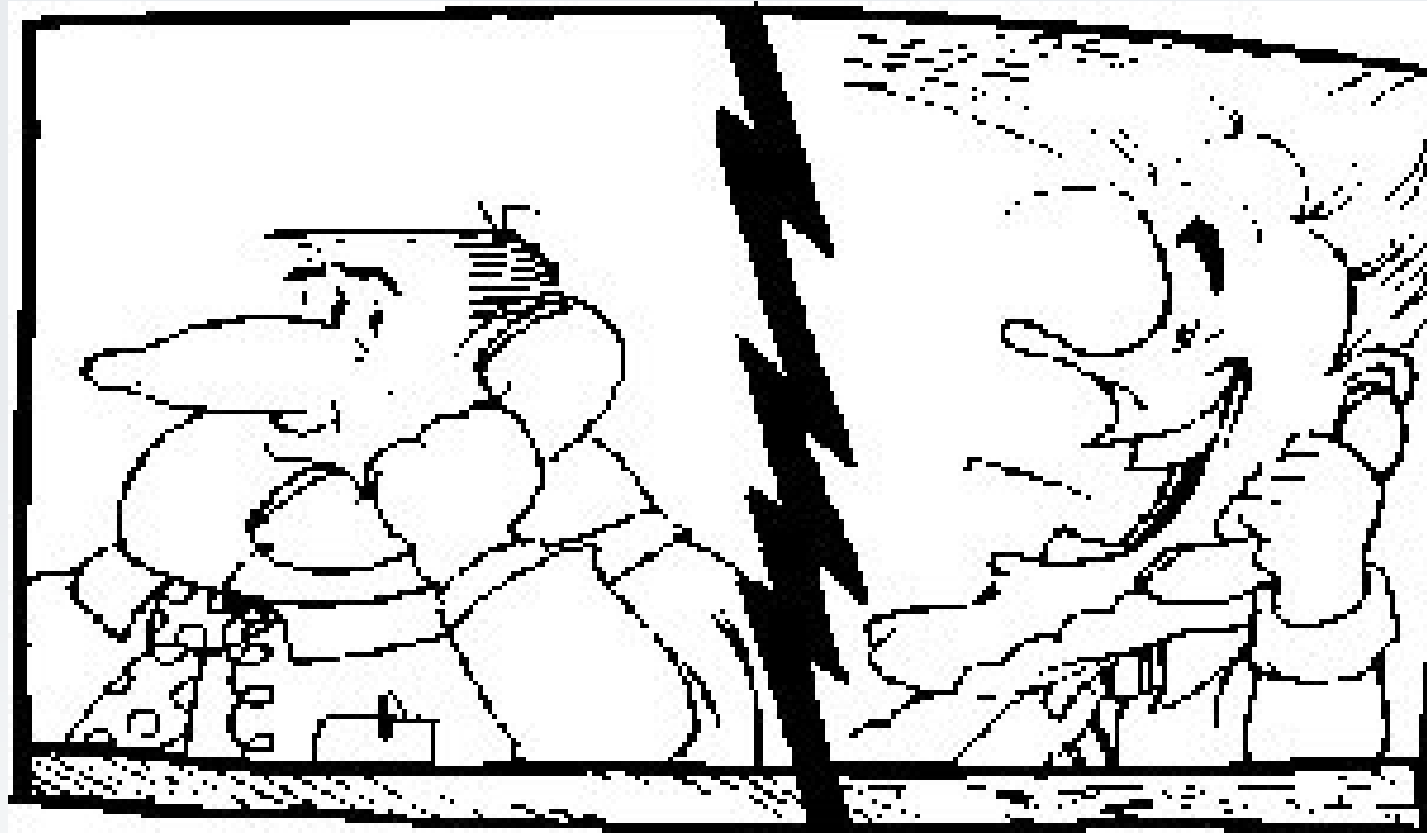
Náhodne zanechané USB a DVD v priestoroch organizácie.
Preveruje sa postup zamestnancov pri nájdení takéhoto média.



V testoch „ožilo“ **22 %** prenosných médií vložených do
zariadení cieľovej organizácie.

- Spustenie škodlivého kódu v internej sieti
 - Zmena, vymazanie, krádež údajov z lokálneho PC alebo sieťových úložísk
 - Spustenie „keylogger“ – odosielanie nazbieraných údajov
 - Pripojenie PC do botnetu
 - Vytvorenie komunikačného kanálu do internej siete

Telefonické testy



"HI! I'M THE SECURITY ADMINISTRATOR
AND I'M CHECKING A SYSTEM PROBLEM.
WHAT'S YOUR USER ID AND PASSWORD?"

Telefonické testy – s podporou emailu alebo sms

V rámci testov sme sa snažili získať:

- prístup k PC cieľovej osoby (cez Teamviewer)
- prístupové meno a heslo – donútiť k zmene hesla
- prístup k zákazníckemu kontu na web portáli organizácie
- scan aktuálnej rámcovej zmluvy



Úspešnosť testov: **72 %** (23 z 32 pokusov)

Telefonické testy – bez podporných médií

V rámci testov sme sa snažili získať informácie:

- o výške platu zamestnanca
- osobné údaje zamestnanca (napr. rodné číslo)



Úspešnosť testov: **100%** (5 z 5 pokusov)

Telefonické testy – možné dôsledky

- Únik citlivých alebo osobných údajov
 - možné šetrenie zo strany Úradu na OOÚ
 - pokuta
- Problémy spôsobené reálnym klientom – strata dôvery
- Strata dôvery vlastných zamestnancov
- Straty finančné
- Neželaná medializácia
- Strata dobrého mena



Ďalšie úspešne vykonané typy testov

- Test fyzického prieniku do priestorov organizácie
- Prehľadávanie odpadkov



Ako postupovať v snahe ochrániť
informačné aktíva?

Opatrenia pre ochranu IS

- Odobrať bežným užívateľom administrátorské práva
- Skenovať prichádzajúce emaily a typy príloh
- Implementovať technické riešenie na filtrovanie emailov s podvrhnutou adresou odosielateľa
- Zablokovať prijímanie emailov, ktoré prichádzajú z externej siete a predstierajú, že prichádzajú z interného prostredia (internej domény)
- Okrem odôvodnených a schválených prípadov zablokovať aplikácie pre vzdialený prístup tak, aby nebolo možné vytvoriť spojenie s externým prostredím
- Zaviesť proces pre aktualizovanie programového vybavenia na pracovných staniciach
- Spúšťať Internetový prehliadač v tzv. sandboxe

Opatrenia pre ochranu človeka



Budovanie povedomia a informovanie ľudí o:

- Informačných aktívach a ich hodnote
- Hrozbách pri narábaní s IKT pr
- Vhodných (zavedených) postupoch na riešenie bezpečnostného incidentu
- Pravidelne budovať bezpečnosť
- **Testovať zamestnancov**



Formy komunikácie

- Definovanie a zverejnenie požadovaných postupov v interných smerniciach na intranete.
- Školenia pre budovanie základného povedomia o IB
 - E-Learning
 - Interaktívne školenia
- „Marketingová“ komunikácia
 - Články v interných časopisoch
 - Marketingové kampane – videá, plagáty, súťaže
- Zamestnanci s reálnou skúsenosťou.



Budovanie bezpečnostného povedomia a vzdelávanie

welivesecurity
news, views and insight from the ESET security community



Securing Our eCITY

Domov ► Prihlásiť sa na stránku



**Training
Center**



Prečo?



Priestor pre Vaše otázky.



Ďakujem za pozornosť

Peter Katrinec

IS Security Sales Consultant

telefón: +421 (2) 3224 4693

mobil: +421 (917) 393 006

e-mail: katrinec@eset.sk

<http://www.eset.com/sk/firmy/services>

