

Metody boje proti moderní kriminalitě

Daniel Kefer

Security 2009, 18.2.2009



Agenda

- Co je to moderní kriminalita?
- Významné případy z nedávné historie
- Trendy v moderní kriminalitě
- Možnosti obrany

Moderní kriminalita

- Nelegální činnost, při které dochází k využití aktuálních slabin informačních technologií a systémů
- Výskyt:
 - Bankovníctví
 - Pojišťovnictví
 - Telekomunikace
 - Státní správa
 - Průmysl
 - ...

Významné případy

Société Générale

- leden 2008 - Jérôme Kerviel
- ztráta 4,9 miliardy Euro
- ztráta díky nevydařeným arbitrážním obchodům nad rámec Kervielových pravomocí
- překročeny finanční limity, využití přístupových údajů kolegů
- dodnes řada nevyřešených otázek kolem případu
- spolu s Kervielem viněni další spolupracovníci



Významné případy

Sinowal

- vlna 2007 - 2008
- též Torpig nebo Mebroot
- trojský kůň napadající klientské počítače
- vykrádání přístupových údajů do ebankingových aplikací, čísel platebních karet, a hesel ke správě webových aplikací
- šířen pomocí „drive-by download“
- celkem kompromitováno:
 - 270 000 bankovních účtů
 - 240 000 čísel platebních karet
 - 2 000 domén
- dle zpráv postiženy banky na celém světě vyjma Ruska

Twitter & Barack Obama

- 

[Home](#)
[Profile](#)
[Find People](#)
[Settings](#)
[Help](#)
[Sign out](#)



BarackObama


[@barackobama](#)

Follow

Name Barack Obama
Location Chicago, IL
Web <http://www.barack...>
166,766 following 155,035 followers 264 updates

Updates

Favorites

Search

advanced

Actions

block BarackObama

Following



What is your opinion on Barack Obama? Take the survey and possibly win \$500 in free gas.

<http://www.cpaclicks.com/secure.asp?e=casxepnzzqk&d=0&l=0&o=0&p=0&subID1=0&subID2=0&subID3=0&subID4=0&subID5=0>

4 minutes ago from web

We just made history. All of this happened because you gave your time, talent and passion. All of this happened because of you. Thanks



[Home](#)
[Profile](#)
[Find People](#)
[Settings](#)
[Help](#)
[Sign out](#)





foxnews

[Follow](#)

Name Fox News
Location New York, NY
Web <http://www.foxnews...>

0 following
85,668 followers
updates

Updates

Favorites

Actions

block foxnews

Breaking: Bill O Riley is gay

90 minutes ago from web

HEALTH: Monday Meal Makeover: Turkey Taco Lettuce Wraps
<http://tinyurl.com/8khpqg>
about 1 hour ago from Perl Net::Twitter

HEALTH: Teen Died After Blood Clot Diagnosed as Stomach Bug
<http://tinyurl.com/9K8cbk>
about 1 hour ago from Perl Net::Twitter

BUSINESS: Tyson President, CEO Dick Bond Leaving Company
<http://tinyurl.com/8d6xba>
about 1 hour ago from Perl Net::Twitter

BUSINESS: Financial Stocks Follow Market Lower <http://tinyurl.com/7Aqt53>
about 1 hour ago from Perl Net::Twitter

BUSINESS: AT&T, Verizon Tumble On Downgrade; Leap Wireless Gains <http://tinyurl.com/785bhx>
about 1 hour ago from Perl Net::Twitter

BUSINESS: U.S. Construction Spending Down 0.6% In November
<http://tinyurl.com/8frhwd>
about 1 hour ago from Perl Net::Twitter

FOX LIFE: Coroner for Anna Nicole Smith's Son Says Travalta Autopsy Could Take Weeks <http://tinyurl.com/8hy6tj>
about 1 hour ago from Perl Net::Twitter

Významné případy

Česká spořitelna

- od roku 2006 – úvěrový/zaměstnanecký fraud na jedné z poboček v Praze
- na pobočce smluvená osoba schvalovala úvěry
- celkem asi 300 úvěrů, systém bílých koňů
- celková ztráta 50 milionů Kč

Významné případy

- Bernard Madoff – 1960-2008 – zpronevěra 50 miliard dolarů
- DuPont – 2006 – zaměstnaný vědec ukradl data v hodnotě 400 milionů dolarů
- 2009 – trojský kůň Pinch – 4 000 infikovaných počítačů denně
- 2009 – trojský kůň Downadup/Conficker – až 2 miliony infikovaných počítačů denně!
- ...

Trendy v moderní kriminalitě

Finanční krize

- stoupá finanční motivace hackerů
- hrozbu představují propuštění zaměstnanci
- možnost zneužití omezování výdajů organizacemi

Nacházení nových zranitelností

- Tradiční zdroje – OS, Browsery, Webové servery, DNS...
- Webové aplikace (80% útoků, př. nově Clickjacking)
- SCADA – Supervisory Control and Data Acquisition (př. AREVA)

Trendy v moderní kriminalitě

Rozvoj Web 2.0

- uživatelé nejsou zvyklí na přítomnost nedůvěryhodného obsahu na zavedených serverech
- prohlížeče nejsou z bezpečnostního hlediska připraveny na tuto technologii (oddělení důvěryhodného a nedůvěryhodného obsahu)
- již se vyskytly četné bezpečnostní problémy na Web 2.0 projektech (Facebook, LinkedIn...)
- rostoucí intenzita útoků na klientskou stranu (malware)
- útočník má zaručen vysoký přísun nových obětí (SEO...)

Trendy v moderní kriminalitě

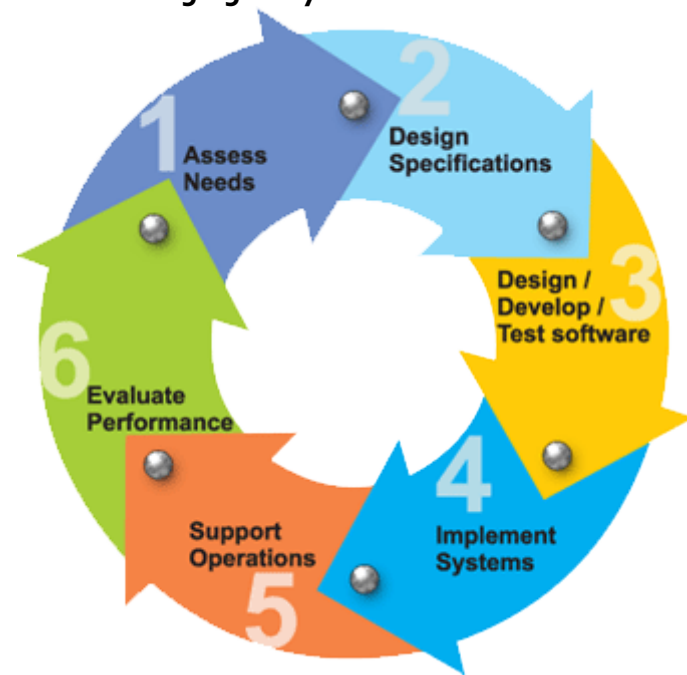
Rozvoj „chytrých zařízení“

- UPS
- tiskárny
- mobilní zařízení



Možnosti obrany

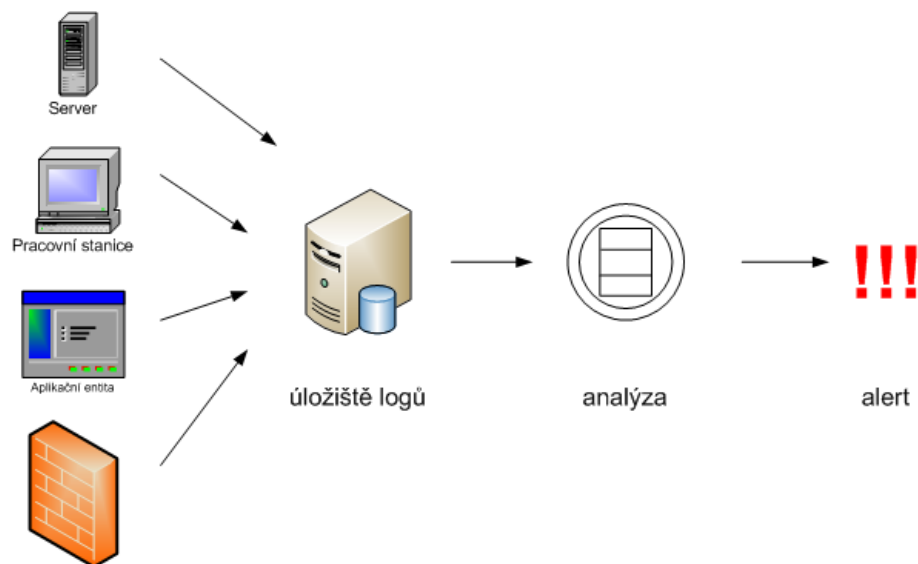
- vnímání problematiky bezpečnosti na opravdu komplexní úrovni
- „Think out of the box!“
- antivirová ochrana – oproti různým tvrzením její význam evidentně neklesá
- vnímání bezpečnosti jako jednoho z klíčových aspektů libovolného systému, její aplikace v rámci celého životního cyklu



Možnosti obrany

SIEM – Security Information Event Management

- řeší problém nasazení velkého množství aplikací v rámci organizace
- není nijak jednoduše možné spravovat velký počet aplikací, natož v nich vyhodnocovat bezpečnost
- princip spočívá v centralizovaném vyhodnocování logů aplikací a systémů



Možnosti obrany

Fraud detection/prevention systems

- systémy detekce podvodu
- celosvětově se rozšiřující metoda redukce nelegální činnosti
- detekce potencionálně nebezpečných událostí na základě detekce anomálií
- využití podobného principu jako SIEM, ale obvykle komunikace přímo s aplikací
- analýza za použití pokročilejších metod (neuronové sítě, bayesiánské metody...)
- možnost využití externích dat (registry, geolokace...)
- též FDS formou služby

Možnosti obrany

Fraud detection/prevention systems

- oblasti nasazení:
 - banky – ebanking, peněžní systémy, karty, úvěry, pobočkový systém...
 - pojišťovny – pojistné podvody
 - telekomunikační operátoři
 - průmysl, energetika
 - informační systémy

Děkuji za pozornost

daniel.kefer@cleverlance.com

