Aktuální rizika v oblasti kybernetické bezpečnosti

Miroslav Nečas, TOVEK

Agenda

Trocha teorie

- Aktiva
- Zranitelnosti
- Hrozby
- Opatření

Aktuální kybernetické útoky

- Typy útoků
- Příklady
- Motivace

Co jsou rizika?

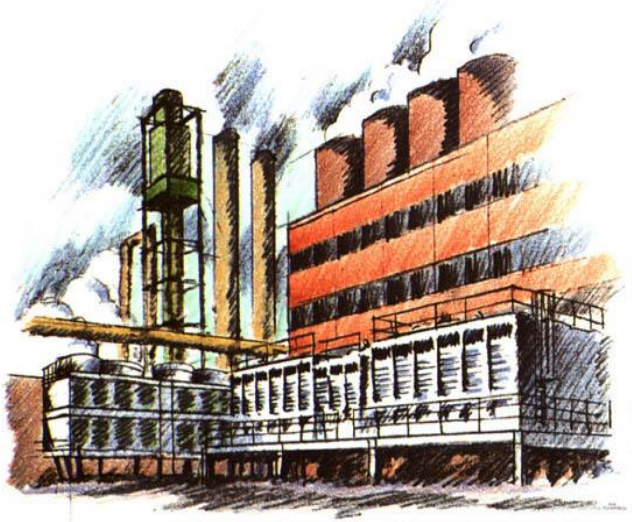
Aktiva: definice v rámci KII

c) primární aktivum: informace nebo služba, kterou zpracovává nebo poskytuje informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém,

d) podpůrné aktivum: technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému,

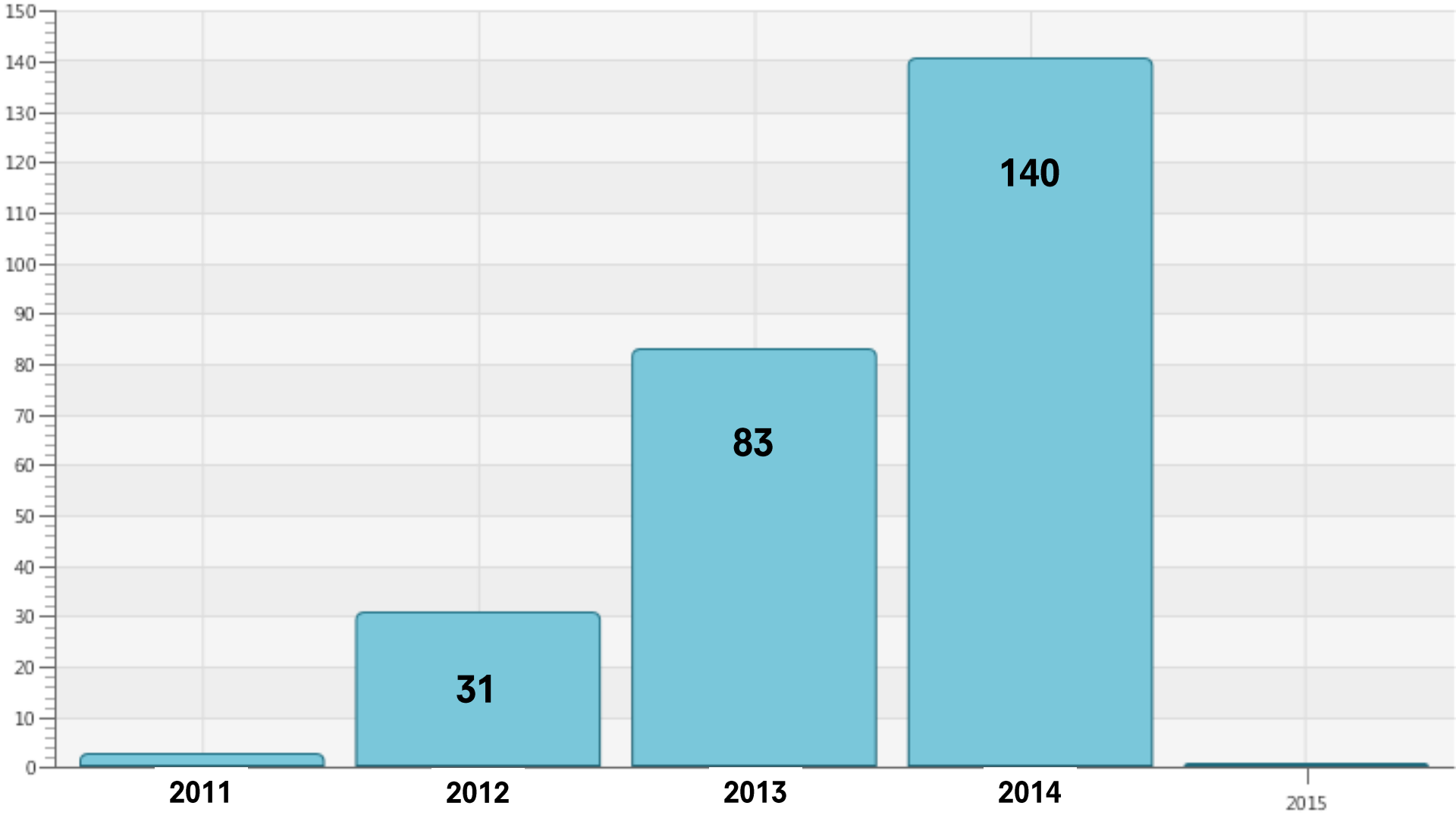
Vyhláška o kybernetické bezpečnosti § 2

Aktiva: o co můžeme přijít



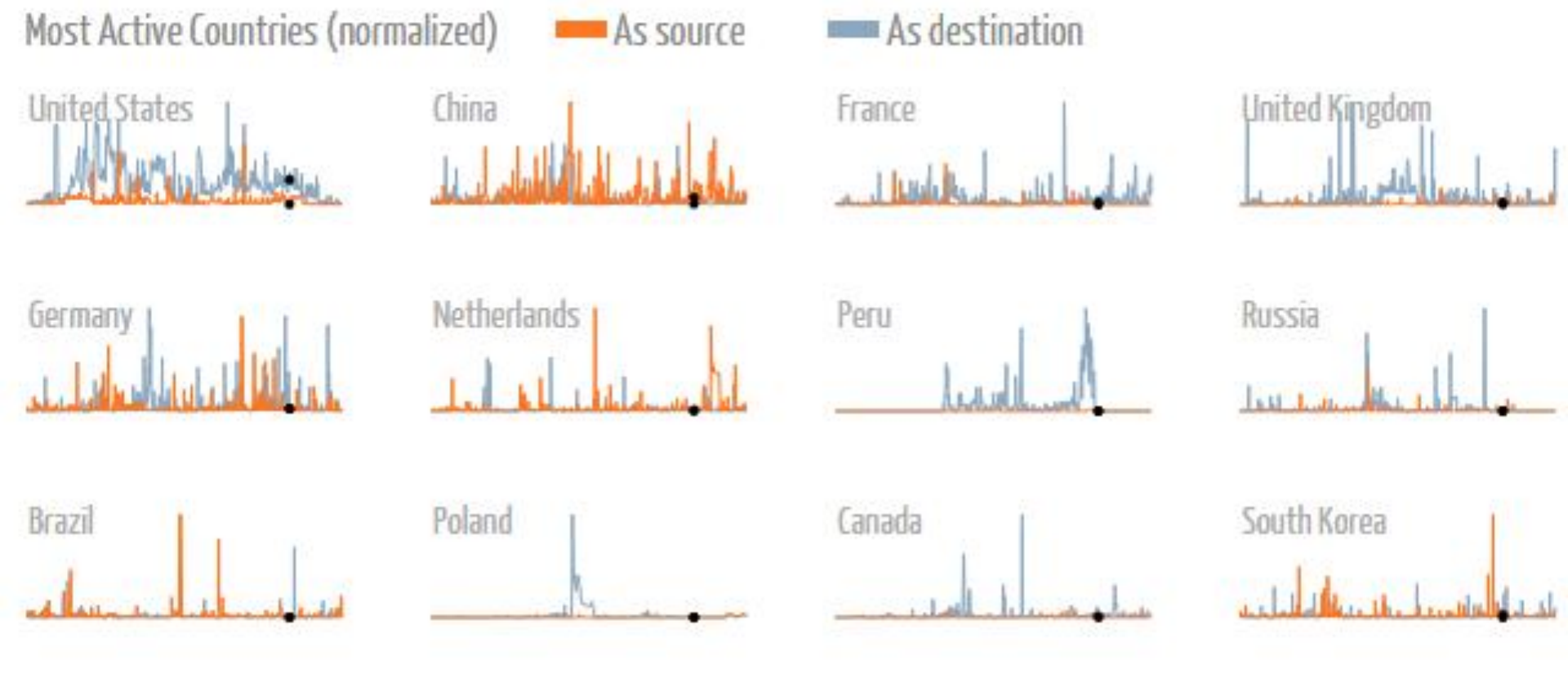
Hrozba: kybernetický útok, ČR

Zdroj: projekt CYBERDEF



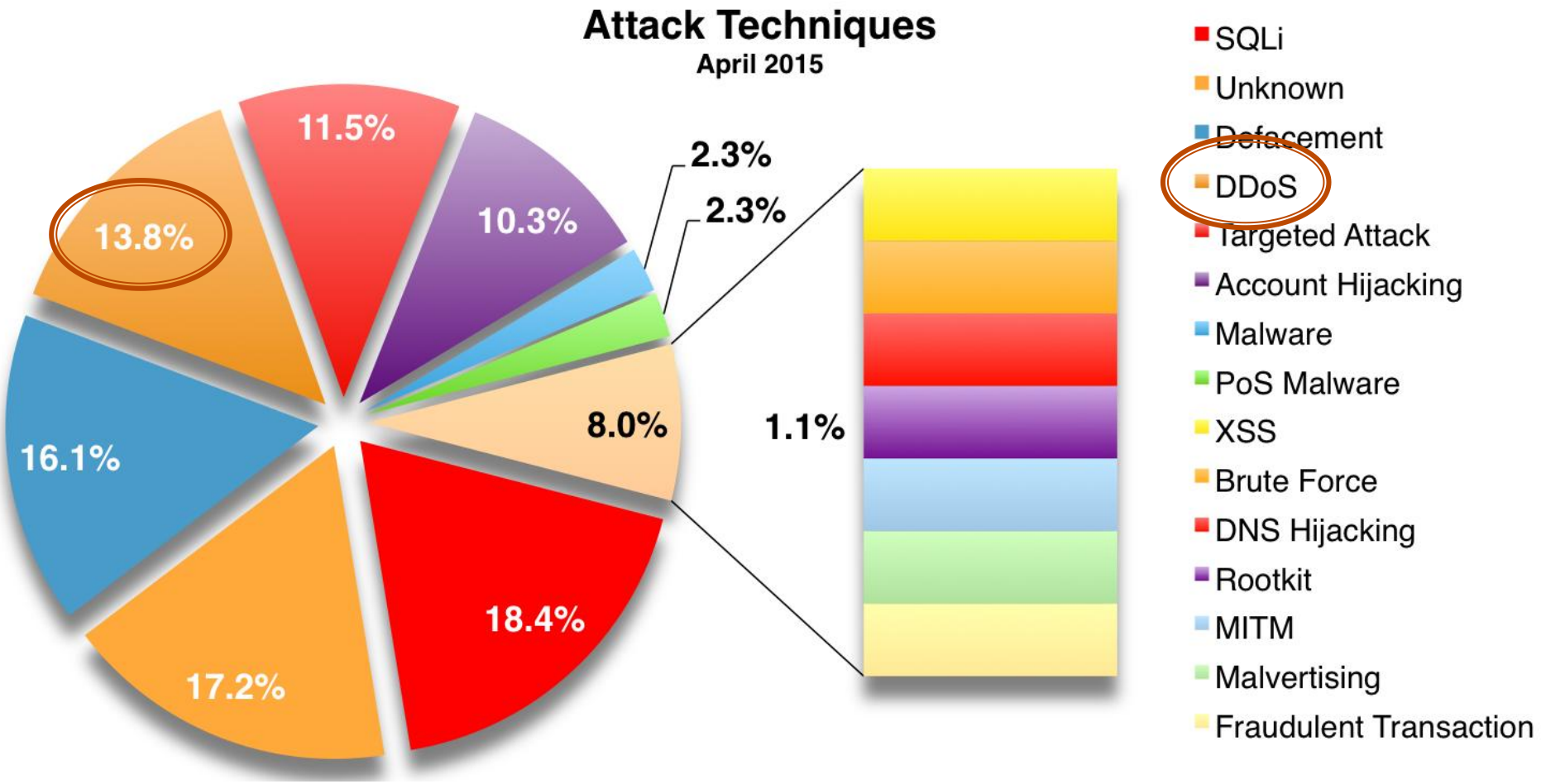
DDOS útoky

Zdroj: http://www.digitalattackmap.com/



Metody útoků 04/2015

Zdroj: http://hackmaggeddon.com/



Vybrané útoky 04/2015

Zdroj: hackmaggeddon.com

14.4. 2015 - DDoS útok: on-line poker

Betair, Unibet, PokerStars

17.4. 2015 – SQLi útok: fiocruz.br

zcizeno 1300 uživatelských jmen a hesel

19.4. 2015 – DDoS: týrání zvířat

#OpNullDenmark, #OpBEAST

17.4. 2015 – SQLi útok: FAB Defense

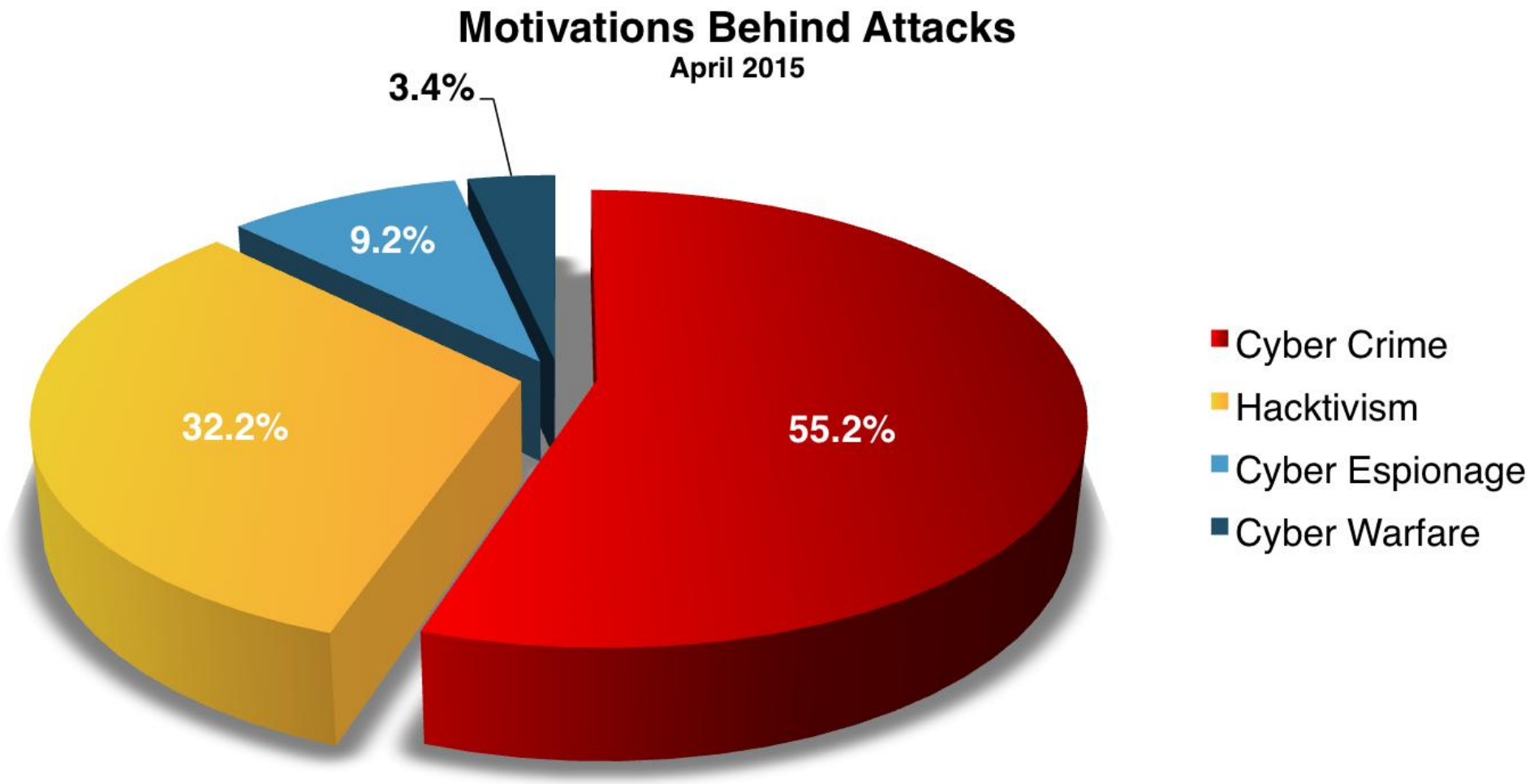
hesla a detaily o mezinárodních zakázkách

23.4. 2015 – MITM útok: SIGAINT

kompromitování anonymizační sítě Tor

Motivace útoků 04/2015

Zdroj: http://hackmaggeddon.com/

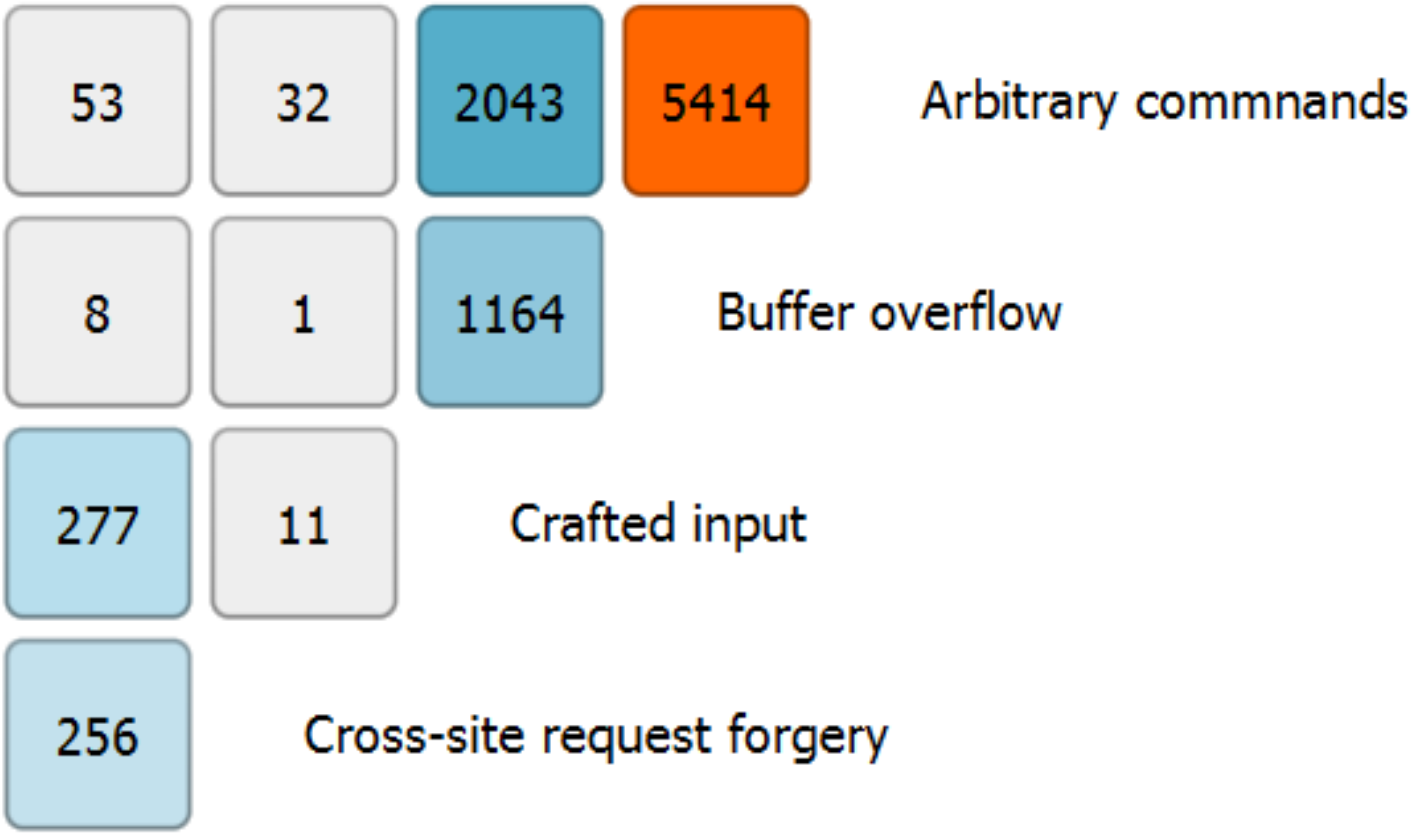


Útok na objednávku

What ill do:
Ill do anything for money, im not a pussy :) if you want me to destroy some bussiness or a persons life, ill do it!
Some examples:
Simply hacking something technically
Causing alot of technical trouble on websites / networks to disrupt their service with DDOS and other methods.
Economic espionage
Getting private information from someone
Ruining your opponents, bussiness or private persons you dont like, i can ruin them financially and or get them arrested, whatever you like.
If you want someone to get known as a child porn user, no problem.

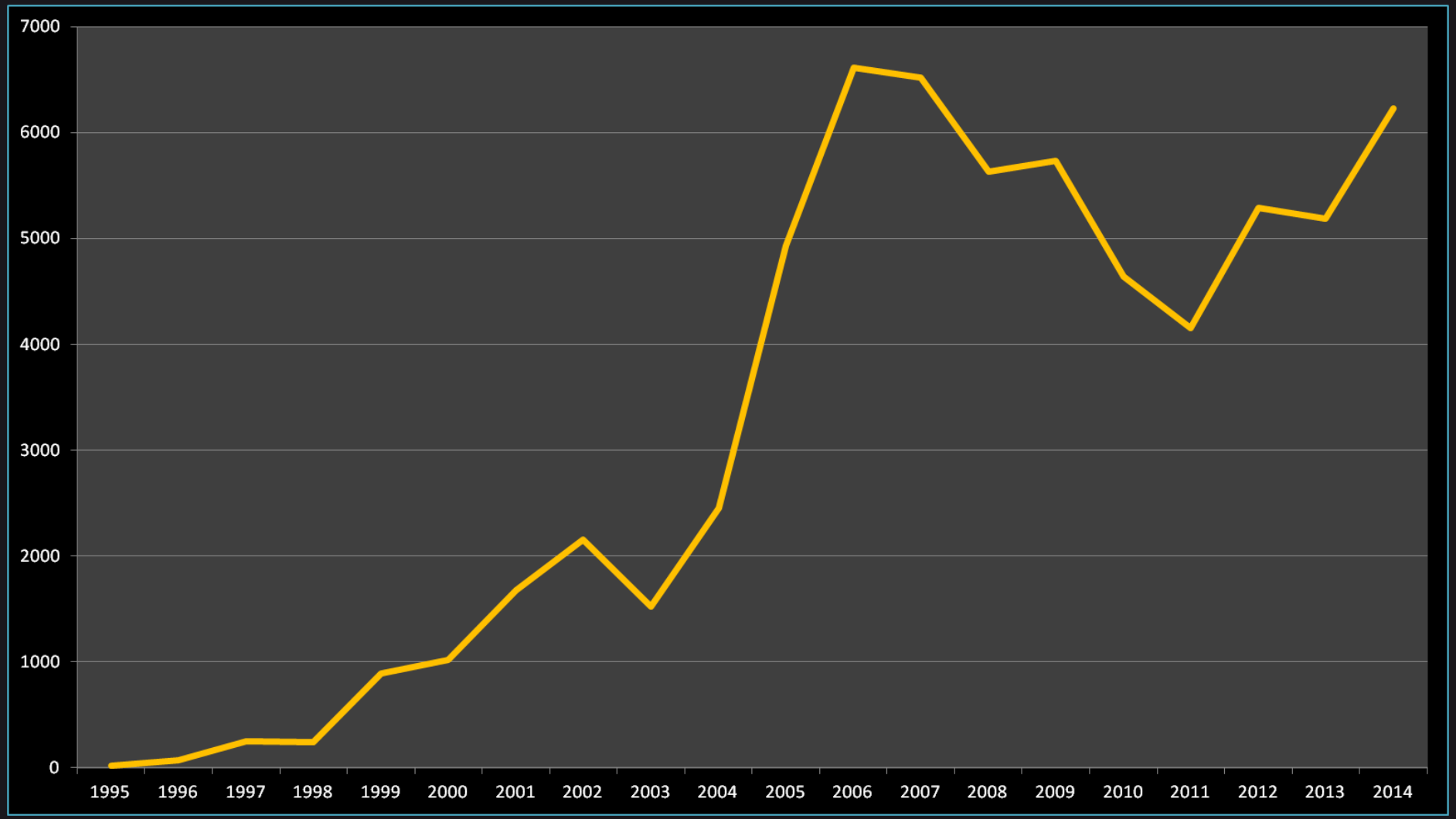
Product	Price	Quantity
Small Job like Email, Facebook etc hacking	200 EUR = 0.737 ฿	1 X Buy now
Medium-Large Job, ruining people, espionage, website hacking etc	500 EUR = 1.842 ฿	1 X Buy now

Útoky cílí na zranitelnosti



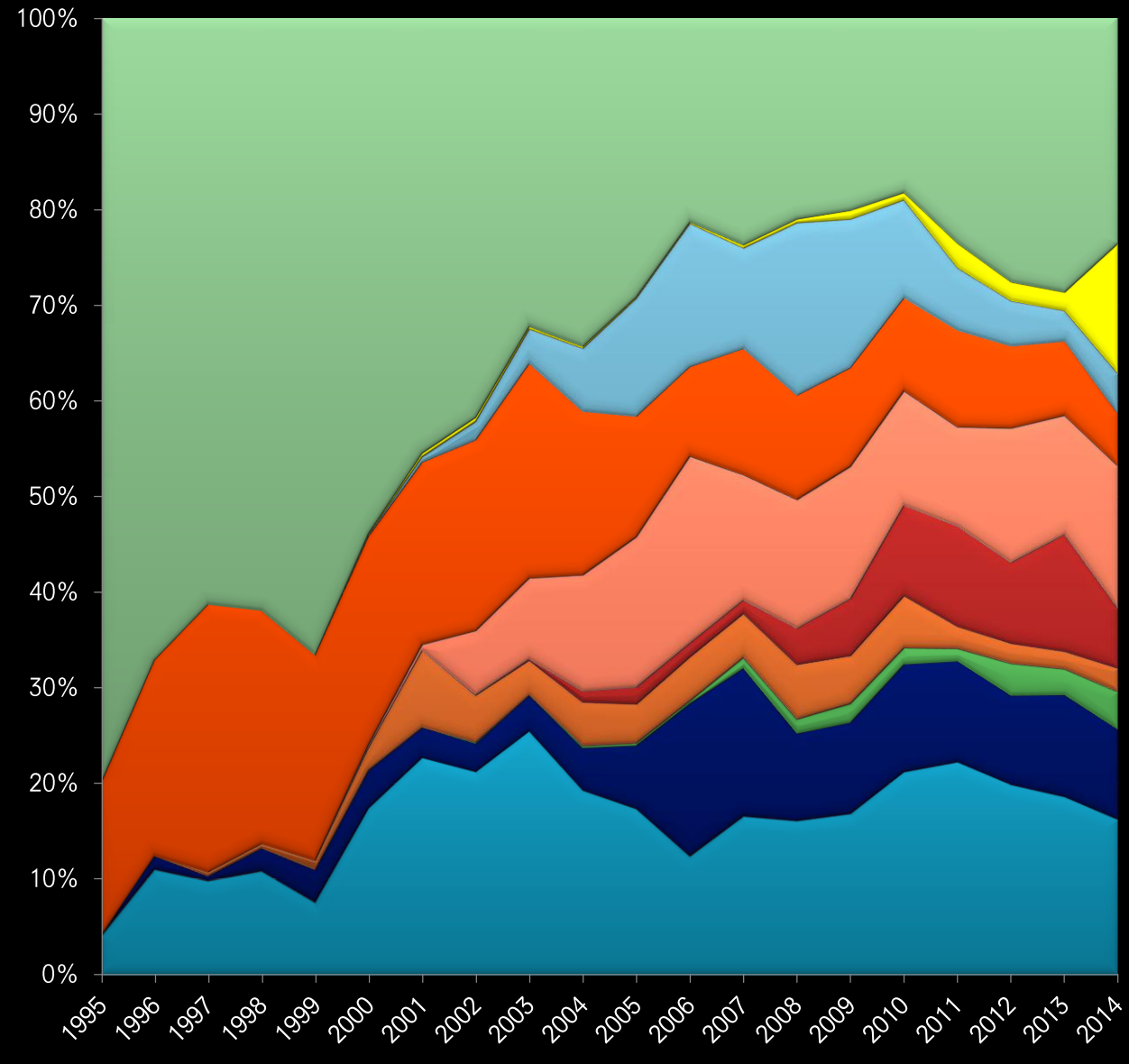
Zdroj: projekt CYBERDEF

Publikované zranitelnosti



Zdroj: projekt CYBERDEF

Vývoj zranitelností v čase



- Ostatní
- Man-in-the-middle
- SQL injection
- Buffer overflow
- Cross-site scripting
- Unknown vectors
- Directory traversal
- Cross-site request forgery
- Crafted input
- Arbitrary commnands

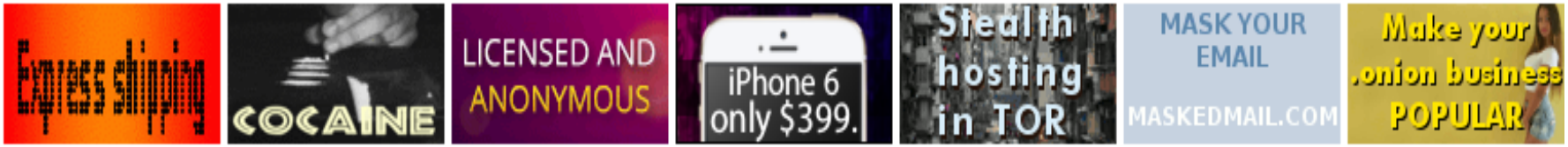
Zdroj: projekt CYBERDEF

Zranitelnosti z šedé zóny

Search for: xss Search! Extended

Search for xss. Search results: xss : 761. Results 1-10 of 629. Search took 0.518 seconds

Sort by: relevancy | last modified date | title



1. New-Crew - SQL Injection / XSS / LFI / RFI / etc... [7.212%]

... New-Crew › Websecurity SQL Injection / XSS / LFI / RFI / etc... Benutzer, die ... Forum abonnieren SQL Injection / XSS / LFI / RFI / etc... Thema / Verfasser ... Scripting ---- Sqli -- SQL Injection / XSS / LFI / RFI / etc... -- Anonymität -- ...

- http://b35qeko6utigphvd.onion/forumdispl... - 15438 bytes [text/html] - Thu, 21 Aug 2014, 13:00:35 BST

[Cached copy]

2. New-Crew - SQL Injection / XSS / LFI / RFI / etc... [7.212%]

... New-Crew › Websecurity SQL Injection / XSS / LFI / RFI / etc... Benutzer, die ... Forum abonnieren SQL Injection / XSS / LFI / RFI / etc... Thema / Verfasser ... Scripting ---- Sqli -- SQL Injection / XSS / LFI / RFI / etc... -- Anonymität -- ...

Zdroj: Torch

0-day zranitelnosti

Index » Special Offers & Free Samples
» MyBB 1.6.12 SQLi Vulnerability - Works on all versions (0day)

Pages: 1

Timmy 2014-03-25 05:29:57 #1

Vendor

Registered: 2014-01-31
Posts: 404

Exploit :

search.php?action=results&sid[0]=9afaea732cb32f06fa34b1888bd237e2&sortby=&order=

Demo :

http://community.mybb.com/search.php?action=results&
sid[0]=9afaea732cb32f06fa34b1888bd237e2&sortby=&order=

Error :

Warning [2] mysqli_real_escape_string() expects parameter 2 to be string,
array given - Line: 874 - File: inc/db_mysqli.php PHP 5.4.19

-1~dotdeb.1 (Linux)

Exm :

http://my-bb.ir/search.php?action=results&sid[0]=9afaea732cb32f06fa34b1888bd237e2&

Co jsou rizika

Účelnost a účinnost opatření

Děkuji vám za pozornost

Miroslav Nečas
necas@tovek.cz