

Synergie fyzické a kybernetické bezpečnosti v moderním datacentru

Konference CRA security

Michal Polívka | Architekt kybernetické bezpečnosti

18. října 2022 | Žižkovská televizní věž

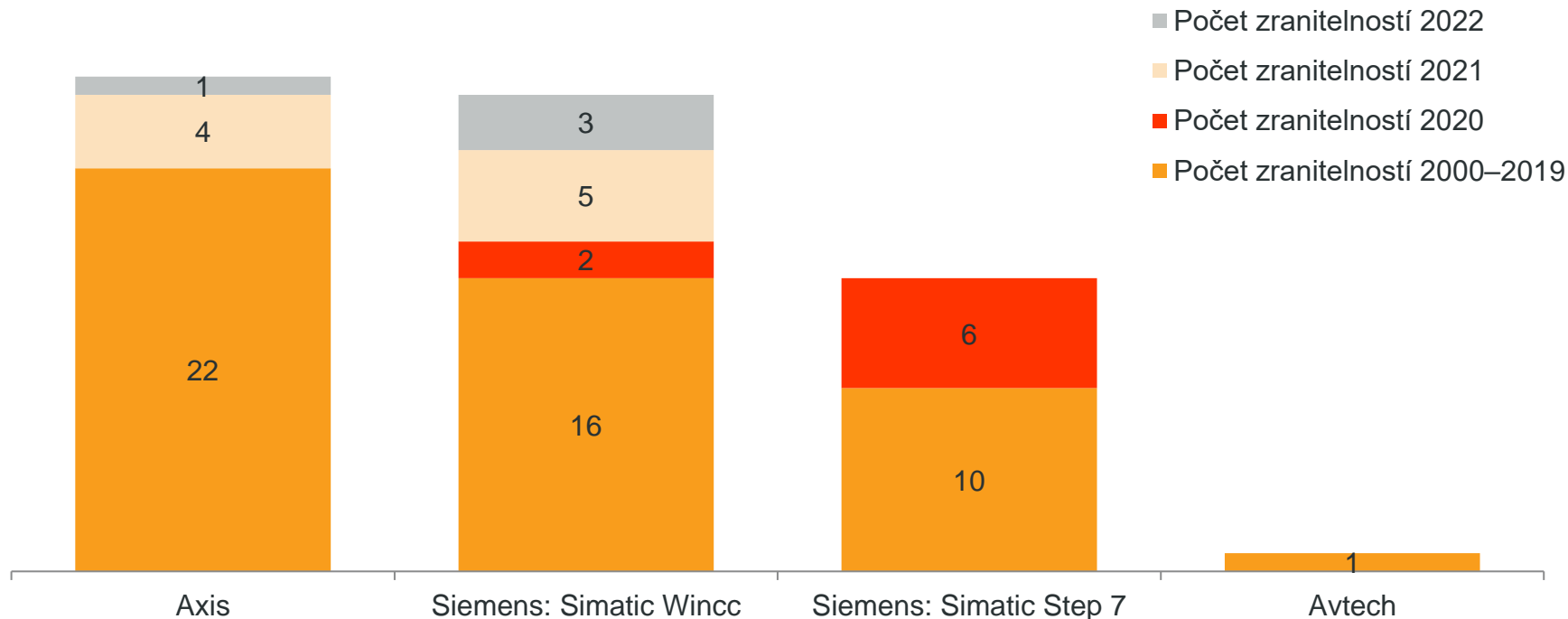
TLP CRA: GREEN (ZELENÁ)

<https://www.lupa.cz/clanky/foto-ceske-radiokomunikace-rozsirily-datacentrum-dc-tower/>



Vybrané produkty a počet evidovaných chyb

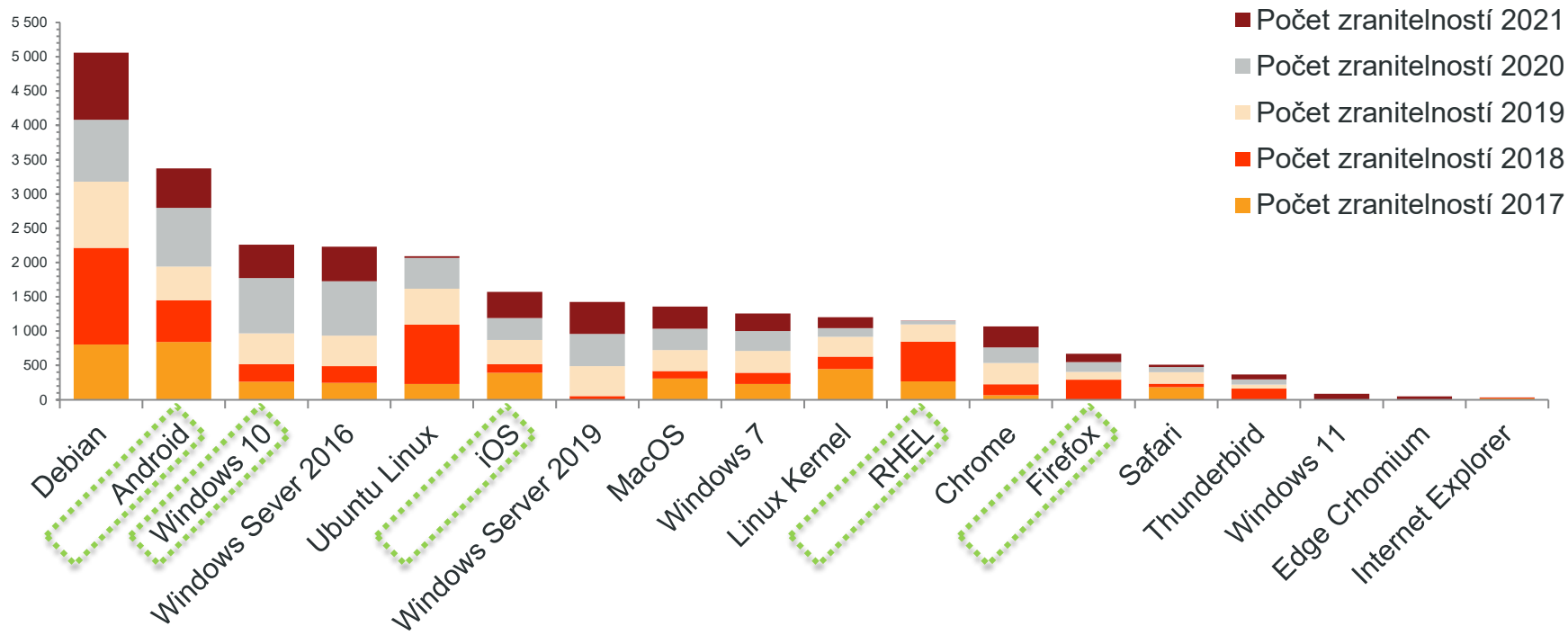
Srovnání počtu CVE 2017–2021



<https://www.cvedetails.com/>

TOP produkty v počtu evidovaných chyb

Srovnání počtu CVE 2017–2021



<https://www.cvedetails.com/top-50-products.php>

<https://www.cvedetails.com/>



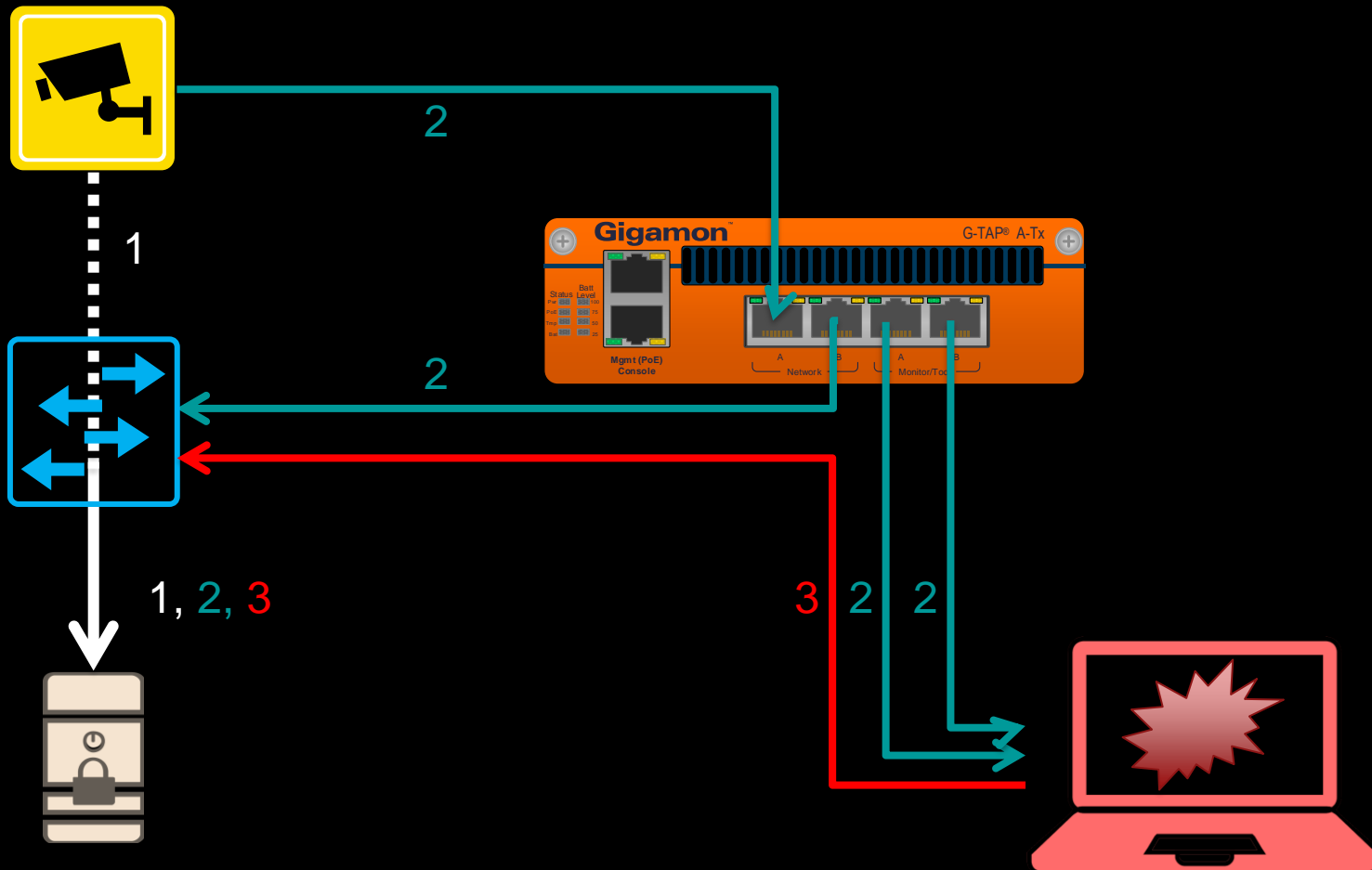
<https://www.exploit-db.com/>





<https://www.ceskatelevize.cz/porady/1097181328-udalosti/207411000100617/cast/34910/>





Bezpečnostní testy technologií

uz01@RHEL-v

```
uz01@RHEL-v:~# hping3 -c 10000 -d 120 -S -w 64 -p 443
--flood [redacted].[redacted].[redacted].[redacted]
HPING [redacted].[redacted].[redacted].[redacted] (eth1 [redacted].[redacted].[redacted].[redacted]): S set, 40
headers + 0 data bytes

--- [redacted].[redacted].[redacted].[redacted] hping statistic ---
3 packets transmitted, 0 packets received, 100% packet
loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

The following is an automated response sent to you by
the QRadar event custom rules engine:

Start Time:

Oct 3, 2022 9:11:14 AM CEST

Rule Name:

Monitoring switch ■■-SW-30 - ■■ | CRA

Event Name:

Link Up

Event Description:

Category:

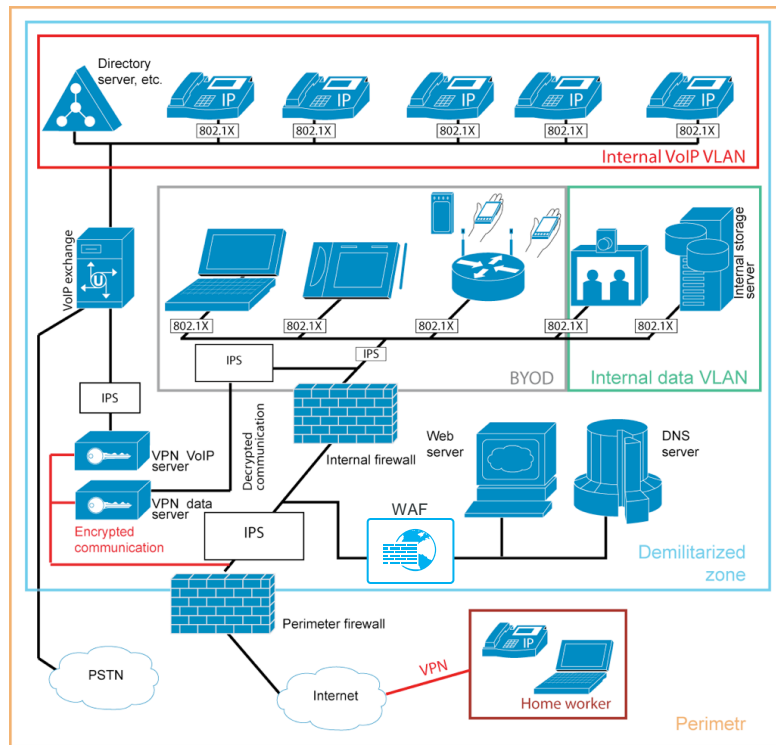
Information

Payload:

<190>%LINK-I-Up: gi1/14

Sít'ová infrastruktura datacentra

DC core vs. podpůrná infrastruktura



NetFlow



IDS

ARP Cache poisoning

Port stealing

switch spoofing

VLAN hopping

MAC flooding

double tagging

ČSN EN 50600

ANSI/TIA-942-B

Tier Classification System (Uptime Institute)

<https://csnonline.agentura-cas.cz/>

https://tiaonline.org/wp-content/uploads/dlm_uploads/2021/01/TIA-942-Standard_OnePager-110220.pdf

<https://uptimeinstitute.com/tiers>

ANSI/TIA-942-B:2017

Certificate of Conformance Constructed Facilities

This is to certify that the constructed data center facilities of
České Radiokomunikace a.s.
located at
Data Centre DC Tower (PHMO)
Mahlerovy sady 2699/1,
Prague 3
Czech Republic

has been independently assessed and found to conform to the requirements of:

ANSI/TIA-942-B:2017

Rated 2

since 19-March-2018
for the following scope(s):

 Architecture: Rated 2	 Mechanical: Rated 2	 Electrical: Rated 2	 Telecom: Rated 2
--	--	--	---

CERTIFICATE NUMBER: 42020181803190010
This certificate is valid from 19-Mar-18 until 18-Mar-21,
subject to yearly surveillance audits.

Audited by:

Ivan Lov
Certification Manager

Validated by:


Surveillance audits due by:  

Issued by:
www.tia-942.org

This certificate can be verified at www.tia-942.org.
Lack of fulfillment of certification terms and conditions may render this certificate invalid. This certificate
remains the property of www.tia-942.org, to whom it must be returned upon request.

DISA STIG	https://public.cyber.mil/stigs/
CIS	https://downloads.cisecurity.org/
PCI DSS	https://www.pcistandard.cz/pcidss/
NIST 800-171	https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
ACSC Essential Eight	https://www.cyber.gov.au/acsc/view-all-content/essential-eight https://www.cyber.gov.au/sites/default/files/2020-06/PROTECT%20-%20Essential%20Eight%20in%20Linux%20Environments%20%28June%202020%29.pdf
NIST HIPAA Security Rule Toolkit	https://csrc.nist.gov/projects/security-content-automation-protocol/hipaa

CRA 

ČESKÉ RADIOKOMUNIKACE