

QSR ECO

PENETRAČNÍ TESTOVÁNÍ

Petr Dočekal | Information Security Consultant

IT Infrastructure & Integration BU / IT Infrastructure Division / Security

petr.docekal@asseco-ce.com



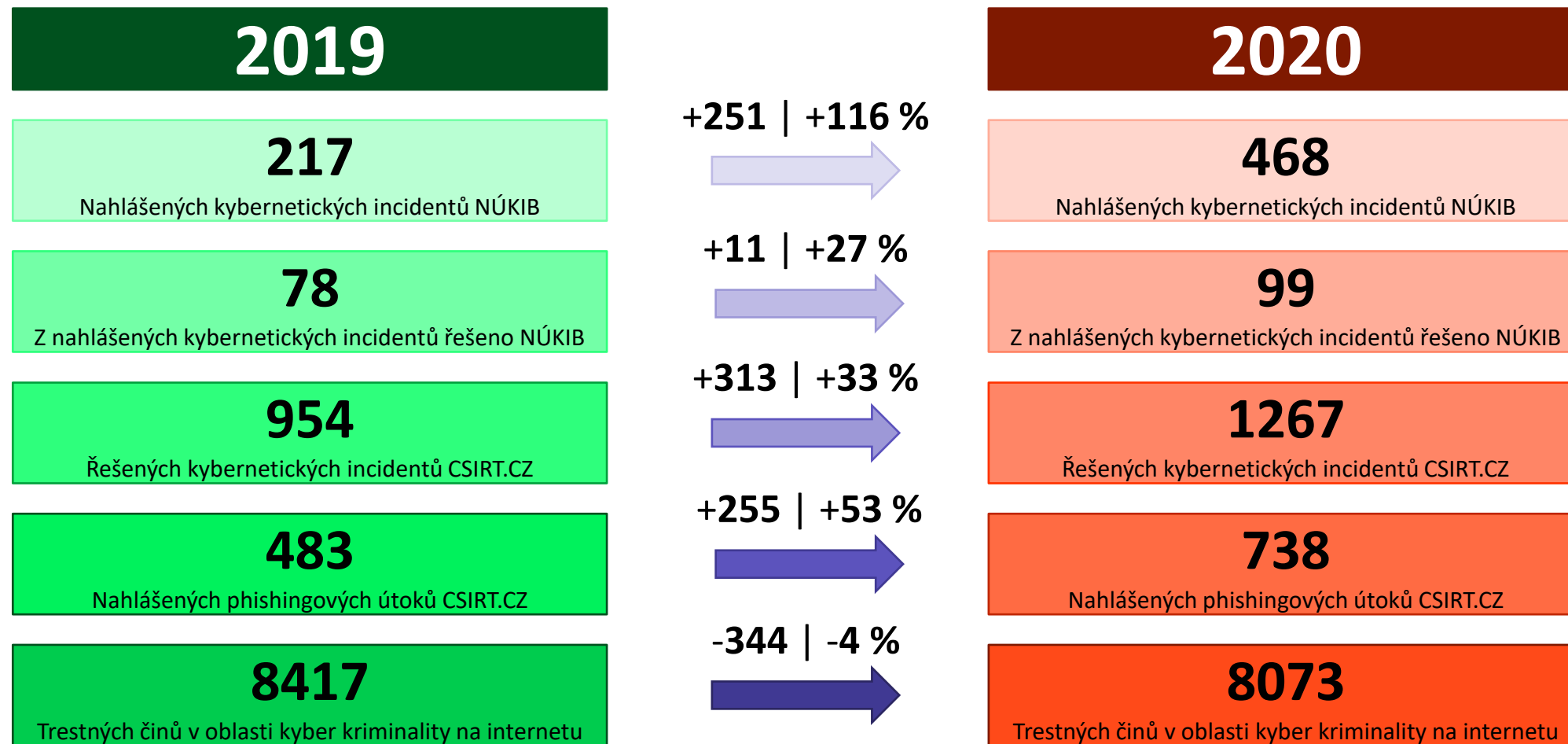
PENETRAČNÍ TESTOVÁNÍ

AGENDA

- Úvod do problematiky
 - Trend incidentů
 - Statistika z námi provedených testů
- Popis penetračních testů
 - Popis jednotlivých služeb
- Závěr

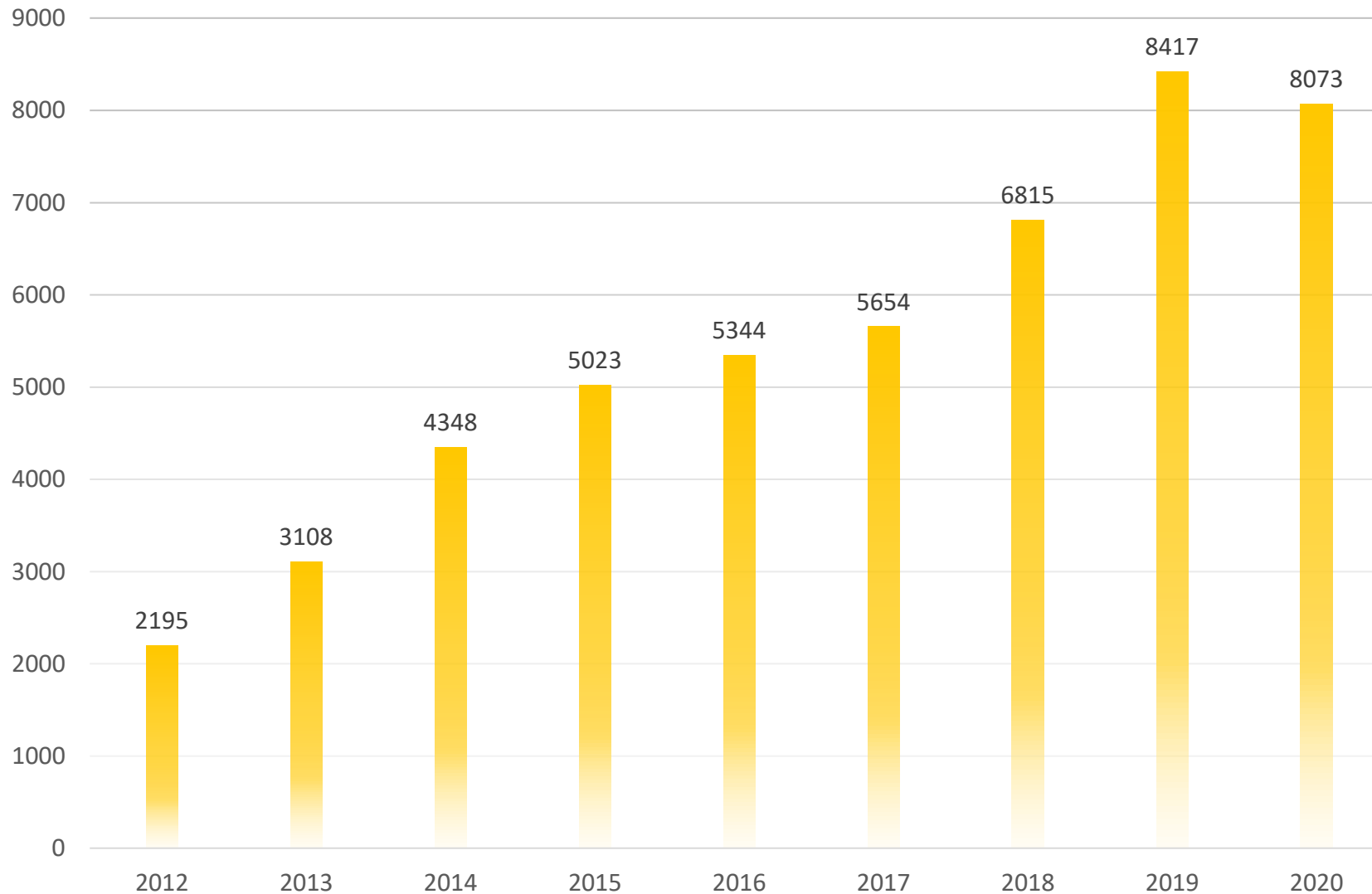
Úvod do problematiky

Incidenty v číslech | 2019–2020



Zdroj: NÚKIB

Nárůst kybernetické kriminality v ČR | 2011–2020



Rok 2019 a 2020 | Zdravotnictví

ČESKO
Ukl...
mili...
ROZHOV...
PRAHA
Beneš...
ochran...
že je zle...

World Africa Americas Asia Australia China Europe India Middle East United Kingdom

North Korean hackers suspected of targeting vaccine maker AstraZeneca in cyberattack, Reuters reports

By Nada Bashir, Chris Liakos, Yoonjung Seo, Sophie Jeong and Angus Watson, CNN
Updated 1548 GMT (2348 HKT) November 27, 2020




Pfizer/BioNTech vaccine data hacked from European Medicines Agency

12/10/2020

RELATED QUOTES

BNTX +3.19% ▲ PFE +0.28% ▲

U.S. drug company Pfizer and its German partner BioNTech said late on Wednesday that documents relating to their COVID-19 vaccine were "unlawfully accessed" after a cyberattack on Europe's medicines regulator.



© iStockphoto.com/Andreas Frenn, Photo: Getty Images

Europe's largest private hospital operator Fresenius attacked with Snake ransomware

Vladimír Kozmokolovský · May 8, 2020 · 34 · 2 minutes read

Fresenius, Europe's largest private hospital operator and major provider of products and services for dialysis, was affected during Snake ransomware cyberattack.

According to KrebsOnSecurity sources, the incident disrupted some systems, but care for the patients continues.

Germany-based Fresenius company includes four independent companies: Fresenius Medical Care, a leading provider of services for people with kidney failure; Fresenius Helios, Europe's largest private hospital operator; Fresenius Kabi, a pharmaceutical company; and Fresenius Environmental Care, a facility manager.

Hackers accessed vaccine documents in cyber-attack on EMA

Papers relating to Pfizer/BioNTech vaccine reportedly targeted in attack on European Medicines Agency

l brněn...
y v desítk...
eznovém kybernetické...
n, informoval její ředite...
říklad o některá...
o o internetový...
ed možnými hackerský...
ech úřad pro



▲ The European Medicines Agency HQ in Amsterdam, where it moved from London in 2019. Photograph: Robin Utrecht/Res/Shutterstock

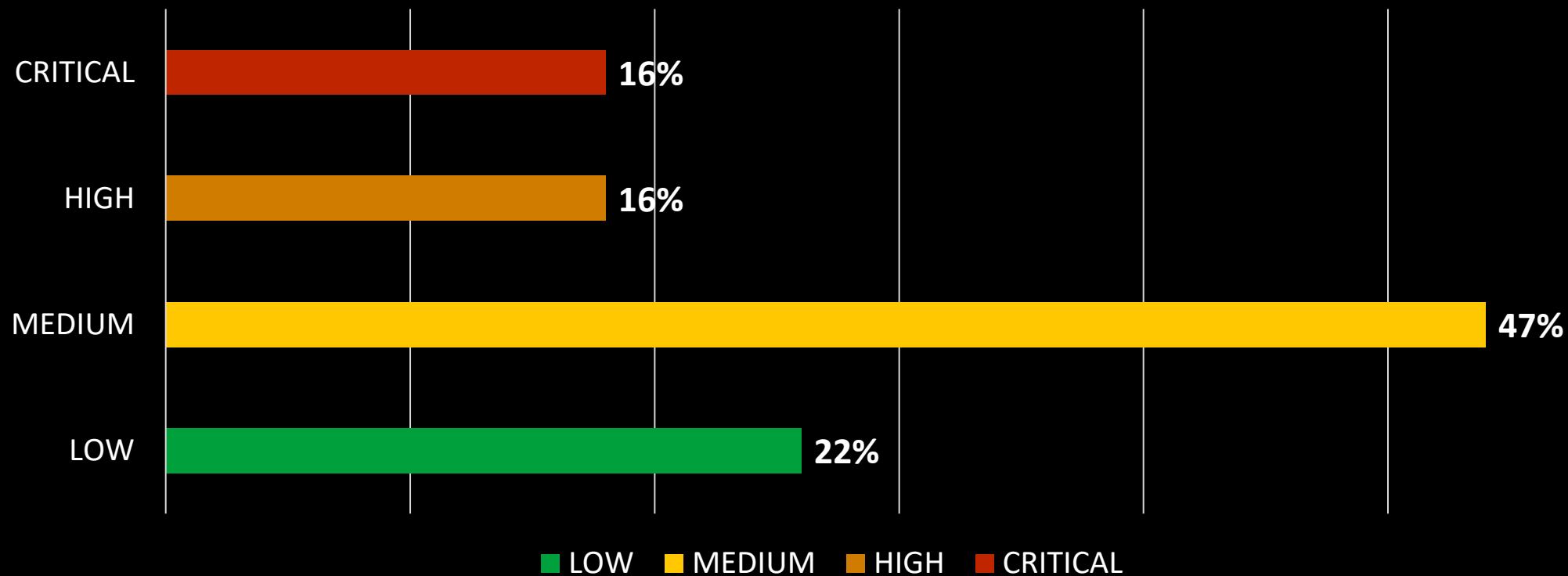
*“It takes 20 years to
build a reputation and
few minutes of cyber-
incident to ruin it.”*

Stephane Nappo



Nálezky penetračních testů

% vyjádření nálezů



Typy nálezů penetračních testů



Zastaralé a zranitelné
komponenty



Nedostatečná
konfigurace



Získání autentizačních
údajů



Cross-Site
Scripting



Nedostatečná
kryptografie

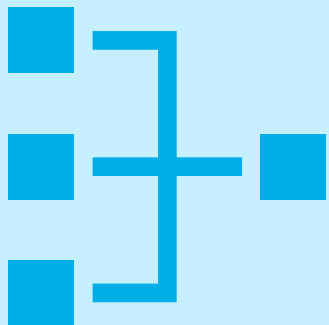


Vyzrazení
informací

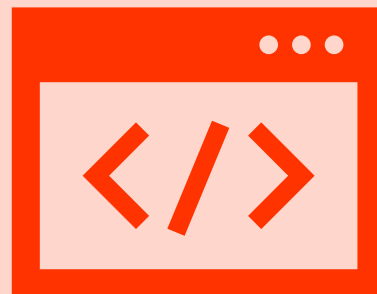
Popis služeb

Služby

**INFRASTRUKTURNÍ
PEN. TESTY**



**WEBAPP
PEN. TESTY**



**SOCIÁLNÍ
INŽENÝRSTVÍ**



Infrastrukturní penetrační testování



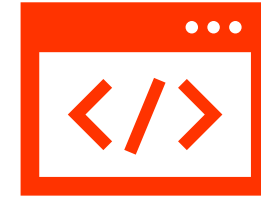
- Interní penetrační test infrastruktury
- Externí penetrační test infrastruktury

NIST
**National Institute of
Standards and Technology**
U.S. Department of Commerce



MITRE | **ATT&CK™**

Penetrační testování webových aplikací



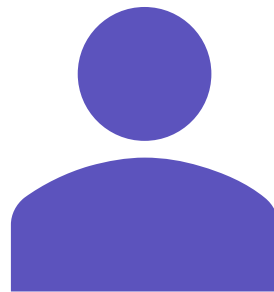
- OWASP TOP10
- OWASP WSTG – Web Security Testing Guide



Sociální inženýrství



- Spear-phishing
 - Odcizení přihlašovacích údajů / spuštění „škodlivého“ kódu
- Vishing
 - Odcizení přihlašovacích údajů



Závěr

Na zamyšlení | Způsob myšlení hackerů

Vyřešte rovnici:

$$20 \times \underline{\hspace{2cm}} + \underline{\hspace{2cm}} = 65\,535$$

$$20 \times 3\,275 + 35 = 65\,535$$

$$20 \times 65\,535 \div 20 = 65\,535$$

$$\cancel{20} \times \underline{\hspace{2cm}} + 65\,535 = 65\,535$$

OUTSIDE THE BOX THINKING

Zdroj: HACKTHEBOX.EU

Shrnutí

- Rostoucí trend v oblasti kybernetických incidentů
- Časté nálezy z penetračních testů
- Popis služeb v oblasti penetračních testů
- Způsob myšlení hackerů

Technology for
business, solutions
for **people.**



Technology for business, solutions for people.

Asseco Central Europe



Budějovická 778/3a

140 00 Praha, Czech Republic



+420 234 292 500



sales@asseco-ce.com



www.asseco.com/ce



linkedin.com/company/asseco-central-europe

Legal disclaimer

This presentation is the property of Asseco Central Europe (Asseco CE) business group. Information presented serves for marketing purposes only and constitutes neither an offer to sell nor a solicitation to buy. Asseco CE accepts no liability whatsoever for any loss arising directly or indirectly from the use of, reliance of any information contained in this presentation or for any omission of the information. The processing, copying, recording on information carriers, as well as making this presentation or any part thereof available in any way to third parties requires the prior consent of Asseco CE member.