Univerzita Tomáše Bati
Fakulta aplikované informatiky

Open source metodiky a nástroje v Cyber Security

Motivace a možnosti pro jejich využití

Jan Kincl | j_kincl@utb.cz | LinkedIn

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
21.07.2022

Laboratoř penetračního testování

PT LAB

O laboratoři

- https://ptlab.fai.utb.cz/ | LinkedIn
- Kybernetická a aplikační bezpečnost | Kryptografie | Pen. testy

- **Ing. David Malaník, Ph.D.** – vedoucí laboratoře

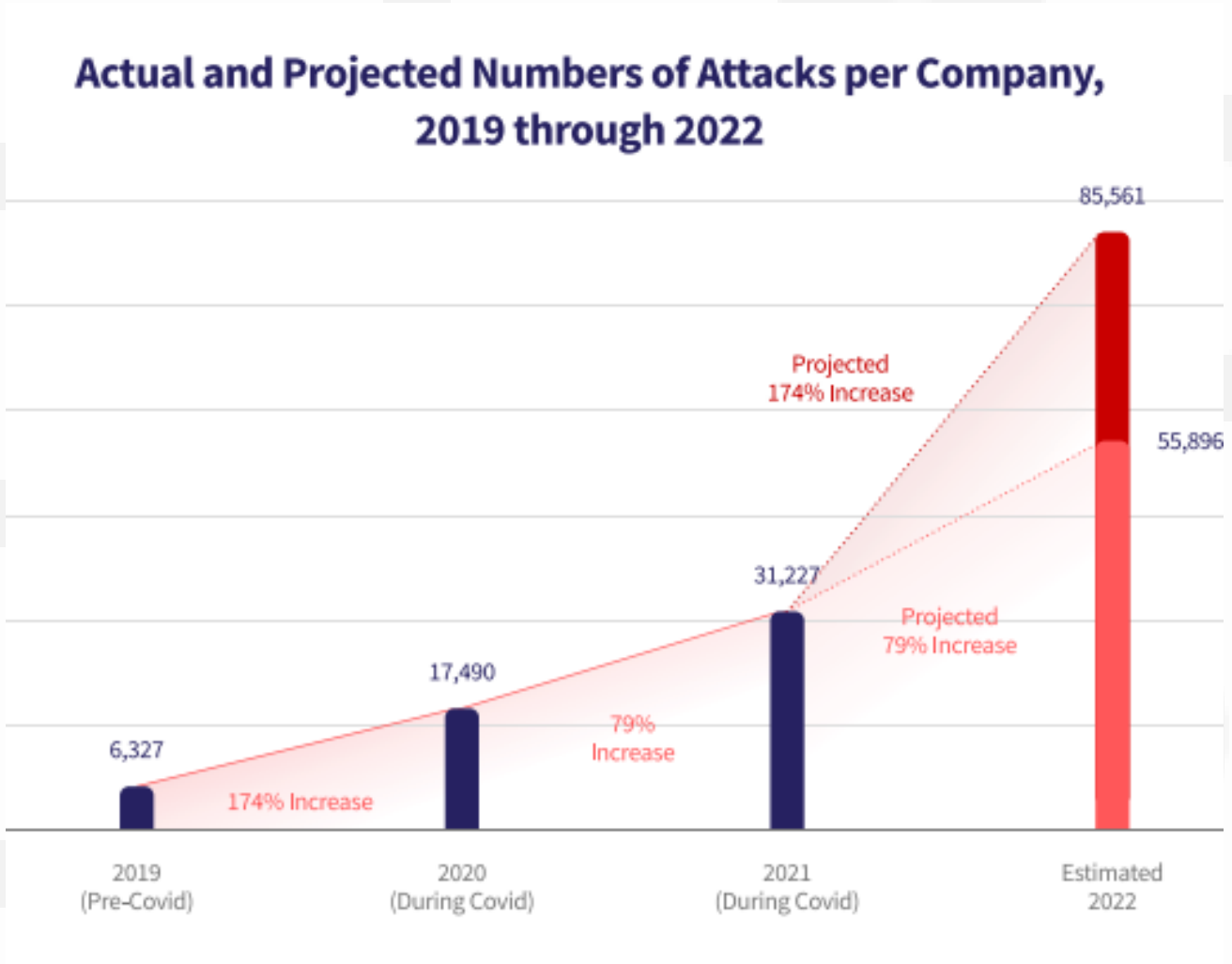
- **Ing. Jan Kincl** – junior researcher
  - Monitoring a správa infrastruktur | networking | mobilní malware

Motivace

- Dlouhodobá bezpečnostní **situace není dobrá**
  - Ztráty 2021: cca. **US$ 6 bil.** | Ransomware: ⌀US$ 170 000 - S$ 1.85 mil - 23 dní
  - Narůstající intenzita útoků na infrastruktury
  - Negativní vliv pandemie **COVID 19 | konflikt na Ukrajině**
    - Útoky více cílené, větší intenzita …
- **Potřeba** důsledného **zabezpečování** infrastruktur
  - **Limitace** správcovského týmu
    - Lidské zdroje, finance pro provoz
- Možné **řešení** ? --> Open Source

GRAFY

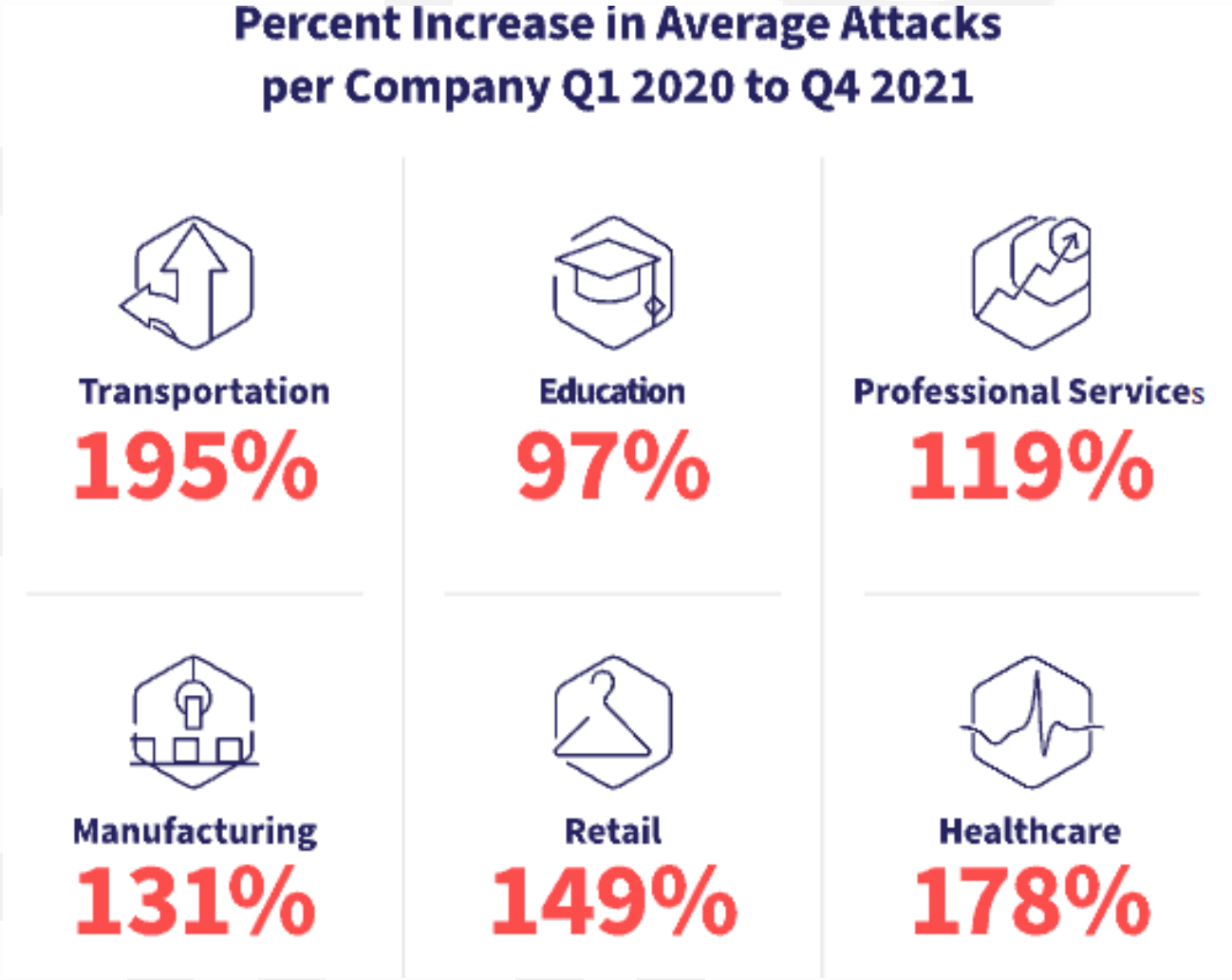
Odhad vývoje počtu útoků na firmy



https://go.coro.net/cyberthreats2022

GRAFY

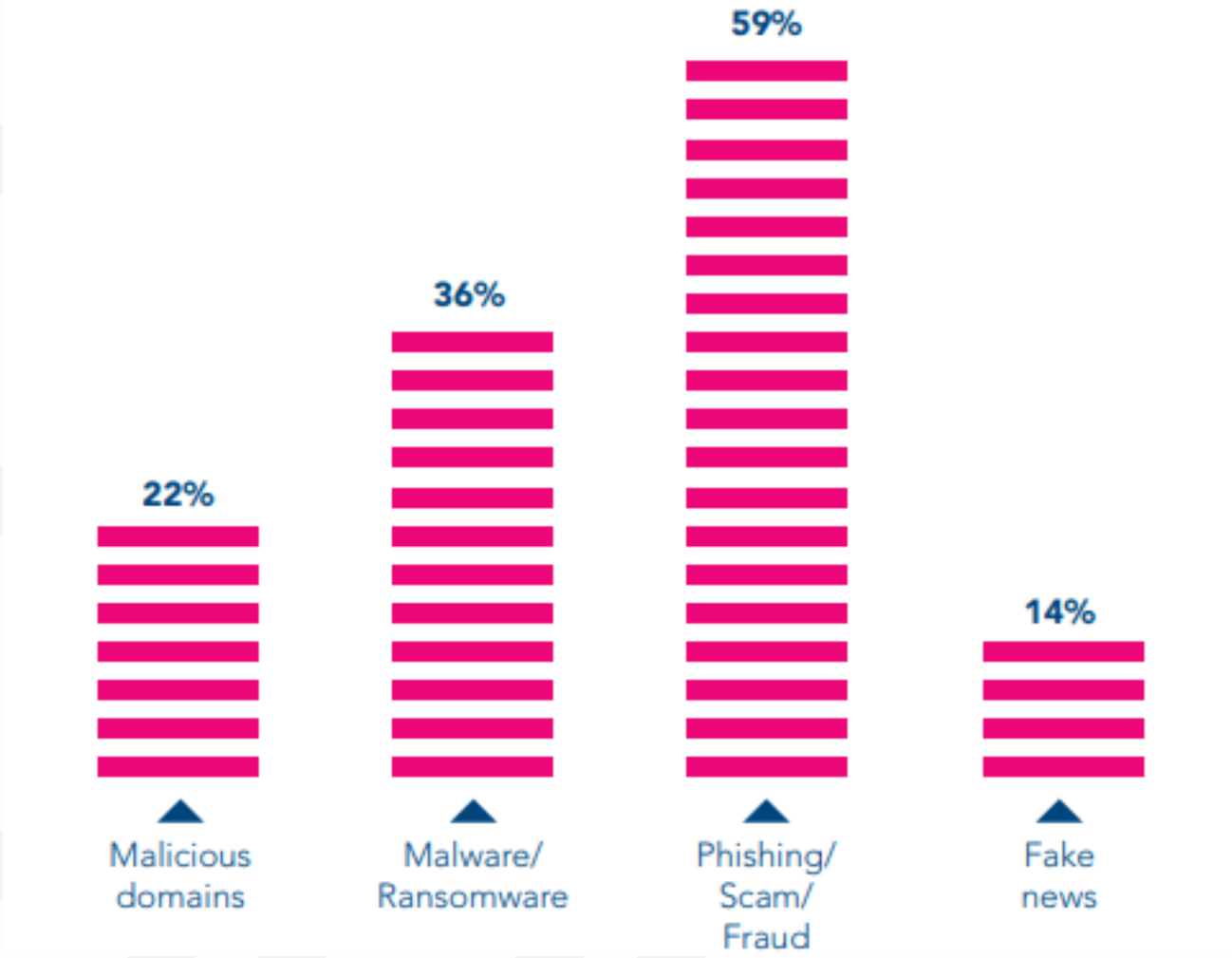
Procentuální nárůst počtu útoků na firmy, dle odvětví



https://go.coro.net/cyberthreats2022

GRAFY

Výskyt klíčového slova COVID-19 v jednotlivých typech útoků



https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

Open source metodiky a jak je použít

- **OSSTMM** - *Open Source Security Testing Methodology Manual*
  - Organizace **ISECOM**
  - **Metodika** pro provádění **bezpečnostních testů**
  - Stanovuje **sérii kroků a vhodných zaměření**
  - **Doporučuje oblasti,** na které je **vhodné se zaměřit** při zajišťování bezpečnosti
    - *Analýza | Metodika práce | Testování bezdrátových sítí | „Lidská" bezpečnost …*

- **OWASP** – *Open Web Application Security Project*
  - Organizace vyvíjející open source metodiky a nástroje pro zajištění bezpečnosti
  - **OWASP Web Security Testing Guide**
    - Metodika pro testování bezpečnosti webových aplikací a služeb
  - **OWASP Mobile Security Testing Guide**
    - Metodika pro testování bezpečnosti mobilních aplikací
  - Obě metodiky zahrnují postupy, doporučené nástroje a ukázkové příklady

Open source metodiky a jak je použít

- **OSINT** - *Open Source Inteligence*
  - Získávání **informací z veřejně dostupných zdrojů**
  - Využívání **open source nástrojů**

- **OTX** – *Open Threat Exchange*
  - Platforma pro sdílení informací ohledně hrozeb kybernetického bezpečnosti
    - Výzkum | validace výsledků | odhalování trendů | návrh opatření

Open source metodiky a jak je použít

- **Možnosti využití:**
  - **OSSTMM –** možný **základ pro**:
    - **Stanovení** firemních **bezpečnostních politik**
      - Splnění certifikací ISECOM, norem ISO 27000, rozšíření COBIT, ITIL …
    - **Stanovení** průběhu a zaměření **penetračního testu** – **vím co objednat**
      - Požadavky, kritéria, cíle pro testování, kontakty apod.
  - **OWASP Web a Mobile** security testing guide
    - Postupy pro vývojářské týmy pro **zajištění bezpečnosti aplikací**
      - Korektní vývoj, práce se zařízeným, ošetření vstupů apod.
- **Cílem** zajistit **bezpečnost infrastruktury** nebo **produktu** společnosti
  - Nákladem ,,pouze“ vlastní práce při implementaci, **know-how zdarma**

Důležité pojmy, se kterými se lze potkat

- **CWE -** *Common Weakness Enumeration* (*https://cwe.mitre.org/*)
  - Obecný seznam běžných SW a HW zranitelností

- **CVE -** *Common Vulnerabilities and Exposures* (*https://cve.mitre.org/*)
  - Konkrétní identifikátory odhalených zranitelností a jejich zneužití

CVE	Vulnerability Name	Vendor and Product	Type
CVE-2021-44228	Log4Shell	Apache Log4j	Remote code execution (RCE)

- **CVSS -** *Common Vulnerability Scoring Systém*
  - Standart pro posuzování závažnosti zranitelností | skóre 0 – 10
  - (*https://nvd.nist.gov/vuln-metrics/cvss*)

Zajímavé open-source nástroje, které lze využít

- **Zabbix** – kompletní řešení pro realizaci monitoringu infrastruktury
  - Systémové metriky | detekce definovaných incidentů | aut. Management …
- **AlienVault** – Open Threat Exchange SIEM systém
  - Řešení pro bezpečnostní monitoring zařízení, detekci zranitelností, podezřelého chování, průniku do infrastruktury …
- **Have I Been Pwned?** – možnost kontroly úniku uživatelských údajů
- **Mail-tester** – možnost testu míry „Spamovosti“ vašeho mailu
- **OWASP ZAP** – bezpečnostní skener webových aplikací
- **Security Headers** – nástroj pro kontrolu HTTP Response Headers webových služeb
- **SSL Server Test** – nástroj pro kontrolu SSL konfigurace webových služeb

Zajímavé open-source nástroje, které lze využít

- **OSINT Framework** – nástroj pro vyhledávání OSINT vhodných nástrojů
- **GNURadio**– Rodina open source nástrojů pro zpracování signálů
- **MISP** – Malware Information Sharing Platform
- **Malice** – ,,Open source VirusTotal“
- **OpenCTI** – *Open cyber threat intelligence* – sdílená vědomostní báze cyber security
- **OpenTitan** – Projekt cílící na korektní a bezpečný návrh mikroprocesorů
- **Lockdoor Framework** – open source framework využitelný při penetračních testech
- **Cuckoo** – Nástroj pro automatizovanou analýzu malwaru
- **Kali Linux**
- **Kitploit** - ,,studnice“ zajímavých nástrojů a informací při práci s bezpečností

Zajímavé open-source nástroje které lze využít

AlienVault

Náhled výsledku bezpečnostního auditu zařízení, vytvořeno pomocí AlienVault

Risk: High
Application: https
Port: 443
Protocol: tcp
Script ID: 11127

CVSS Base Vector:
AV:N/AC:L/Au:N/C:P/I:P/A:P

Summary:
It was possible to kill the web server by
sending an invalid request with a too long header (From, If-Modified-Since, Referer or Content-Type)

Impact:
An attacker may exploit this vulnerability to make your web server
crash continually or even execute arbitrary code on the target system.

Solution:
Upgrade your software or protect it with a filtering reverse proxy.

CVSS Base Score:
7.5

Výhody a přínosy

- **Komunitní základ** jednotlivých metodik a nástrojů
  - **Obrovské množství** poskytovaných **dat** při detekci zranitelností
  - **Flexibilní** komunitní **vývoj** nástrojů
  - **Velmi rychlá reakce** na **nové hrozby** a problémy | **OWASP Top10**
  - **Rozsáhlá komunita** uživatelů a vývojářů
- Podpora zajištění úrovně kybernetické bezpečnosti
  - **Vodítka a pomůcky** pro vývojářské týmy, IT oddělení, SecOps, SOC apod.
  - **Základ** pro nastavení **bezpečnostních politik** společnosti
  - „První krůčky“ k **zisku certifikací**
- **ZDARMA –** alespoň pořizovací náklad

Univerzita Tomáše Bati
Fakulta aplikované informatiky

Děkuji za pozornost

Open source metodiky a nástroje v Cyber Security

Motivace a možnosti pro jejich využití

Jan Kincl | j_kincl@utb.cz | LinkedIn

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
21.07.2022

Laboratoř penetračního testování

PT LAB