Introduction – what, why, how

Martin Stanek

Department of Computer Science
Comenius University
stanek@dcs.fmph.uniba.sk

Security of IT infrastructure (2024/25)

Content

What could go wrong – few examples

Vulnerabilities, classifications

Real world

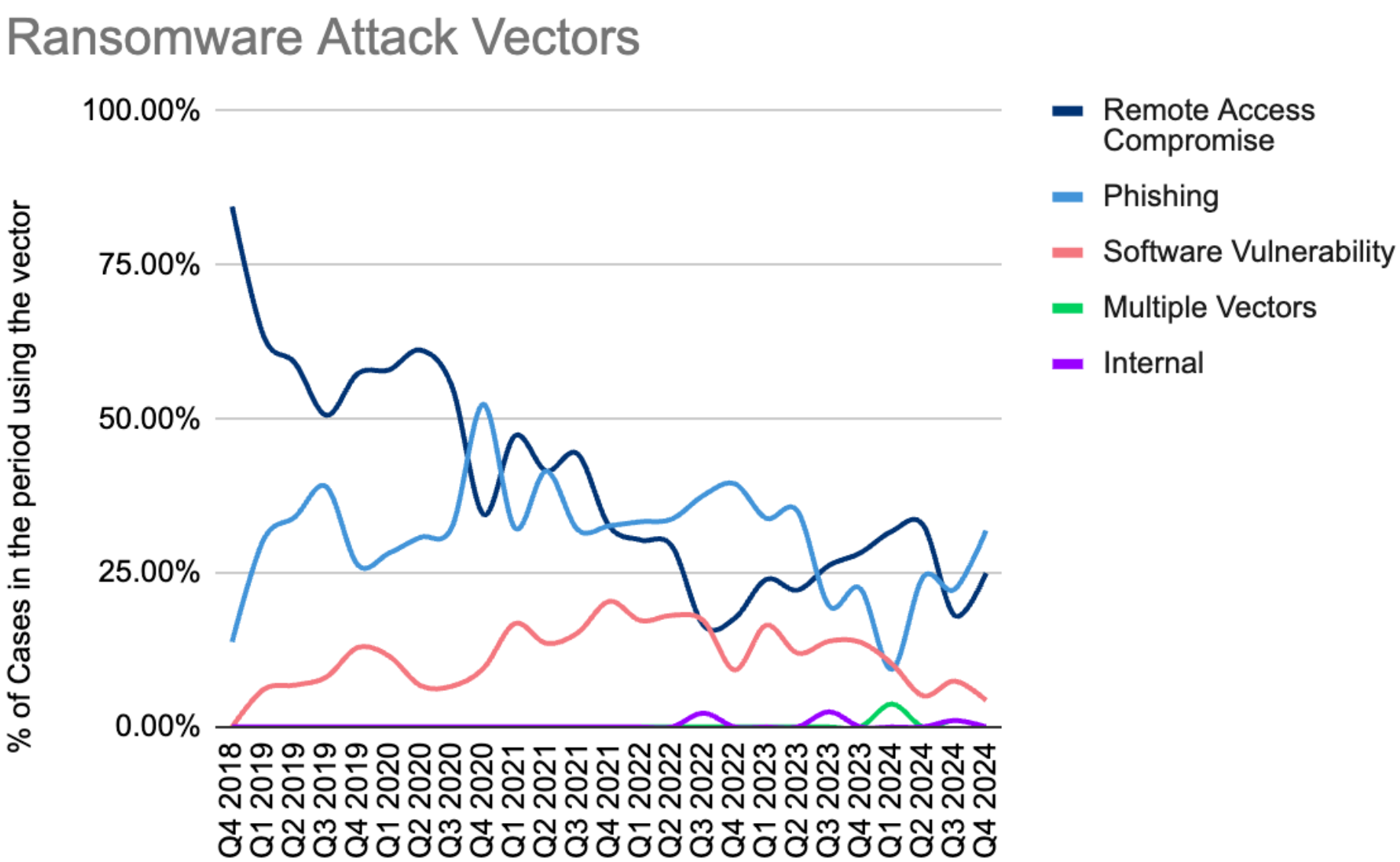
- Statistics, surveys
- Controls, regulatory and compliance frameworks

What could go wrong?

- Ransowmare
- Supply chain attacks
- People – social engineering, phishing
- Vulnerabilities
- …

Ransomware

- Johnson Controls (2023)
  - Dark Angels ransomware gang ($51 mil. ransom, 27 TB of data stolen)
  - unauthorized access, data exfiltration, deployment of ransomware
  - shut down large portion of IT
  - cost of response and remediation: 27 mil. USD
- Colonial Pipeline (2021)
  - pipeline system for gasoline, diesel and jet fuel
  - DarkSide malware, billing infrastructure affected, 100 GB exfiltrated
  - pipeline shutdown as a prevention
  - ransom paid within hours (75 BTC $\sim$ 4.4 mil USD) – decryption tool too slow
  - panic buying, fuel shortages, state of emergency declared by POTUS
  - pipeline operations restored after six days
  - DarkSide: "*our goal is to make money, and not creating problems for society*"



source: https://www.coveware.com/blog/2025/1/31/q4-report

Supply chain attacks

- abusing third-party tools or services
- download an update or a new library infected with a malware
- XZ Utils
  - compression formats: xz and lzma
  - backdoor introduced in February 2024, found in March 2024
  - altered behavior of `sshd` via systemd
  - allowing remote access for an attacker
  - "Jia Tan" – a campaign (2021-2024) to become a co-maintainer of XZ Utils
  - could be devastating; limited real impact
    mostly caught in unstable/beta branches of Linux distributions
- jQuery
  - distribution of trojanized versions of jQuery (May – July 2024)
  - npm registry: cdnjquery, footersicons, jquertyi, jqueryxxx, …
  - capture all user data entered into forms on infected pages

Supply chain problems

- Crowdstrike
  - security software
  - faulty update for Falcon (agent), July 2024
  - 8.5 million Windows systems crased, unable to restart normally
  - manual intervention needed

Vulnerability: HTTP/2 Rapid Reset

- Cloudflare, Google, AWS (CVE-2023-44487)
  - first exploited and observed in August 2023
  - Cloudflare: peak DDoS – 201 million requests/s (botnet with only 20.000 machines)
  - Google: peak DDoS – 398 million requests/s
  - AWS: peak DDoS – 155 million requests/s
- root cause
  - HTTP/2 features: stream multiplexing and concurrency
  - abusing ability to reset (cancel) stream immediately
  - sending large number of requests that are immediateley reset
- fixed in various web server and reverse proxy implementations

Vulnerabilities: Ivanti

- zero-day vulnerabilities in SSL VPN appliances
  - first exploitation observed in December 2023
  - over 1700 devices compromised worldwide (January 2024, source: Volexity)
  - CVE-2023-46805: authentication bypass in Ivanti Connect Secure
  - CVE-2024-21887: command injection vulnerability in ICS and Ivanti Policy Secure
  - CVE-2024-21888: privilege escalation in ICS and Ivanti Policy Secure
  - CVE-2024-21893, CVE-2024-22024:access restricted resources without authentication
- recommendations: assume accounts compromise, hunt for malicious activities, ...
- CISA Emergency Directive 24-01, additional 2 Supplemental Directions

Vulnerability: Log4Shell

- reported by Alibaba Cloud Security Team (CVE-2021-44228 and few other)
- publicly disclosed in December 2021
- unnoticed since 2013
- problems with Log4j library (*see picture*)
  - string substitution while logging
  - for example remote data from evil LDAP server, log4j deserializes Java class and executes it
- impact: RCE, easy to exploit
- almost everyone need to patch/fix/mitigate
- CISA Emergency Directive 22-02

Security incidents and failures

- various causes (or their combination): human factor, criminal activities, technical vulnerabilities etc.
- impact: “nothing” happened, loss of reputation, cost of repair/replacement of data and systems, direct financial loss, bankruptcy etc.

Vulnerabilities (usually SW):

- reality is worse (unpublished vulnerabilities, weak passwords, misconfiguration, etc.)
- National Vulnerability Database (nvd.nist.gov)
- various other sources exist
  - more sources and vulnerabilities covered, faster publication, additional detail (e.g. how to fix), …
- Known Exploited Vulnerabilities Catalog
  - subset of NVD, managed by CISA
  - https://www.cisa.gov/known-exploited-vulnerabilities-catalog

NVD

- operated by NIST
- vulnerabilities (software flaws) published:

year	2019	2020	2021	2022	2023	2024
count	17305	18349	20155	25043	28817	39999

- includes additional information
  - classification (categories, severity score etc.)
  - affected software
  - links to other sources

NVD – the most prevalent categories in 2024

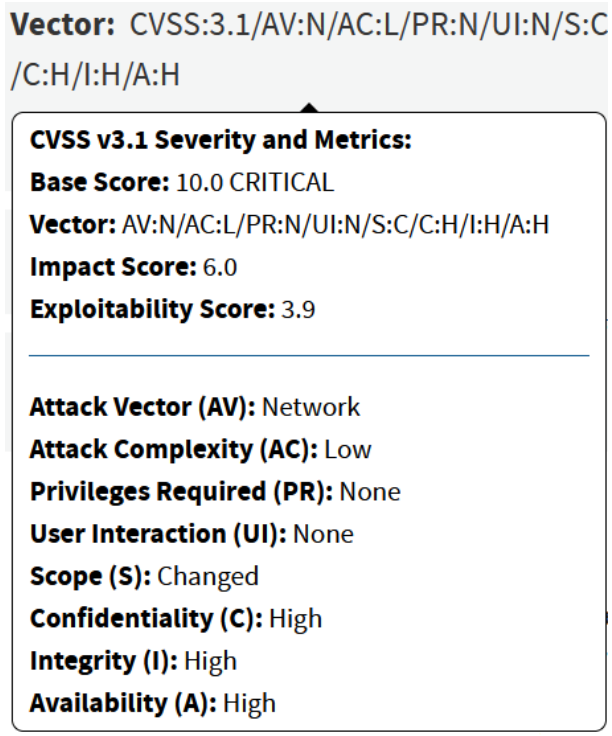
nvd.nist.gov/general/visualizations/vulnerability-visualizations/cwe-over-time

%	CWE	Title
NVD-CWE-noinfo	30,19	Insufficient Information
CWE-79	14,87	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-787	9,03	Out-of-bounds Write
CWE-476	6,05	NULL Pointer Dereference
CWE-416	5,43	Use After Free
NVD-CWE-Other	4,83	Other
CWE-89	4,68	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-125	3,19	Out-of-bounds Read
CWE-352	2,58	Cross-Site Request Forgery (CSRF)
CWE-862	2,57	Missing Authorization
CWE-22	2,51	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-78	1,57	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-120	1,43	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-434	1,29	Unrestricted Upload of File with Dangerous Type
CWE-190	1,16	Integer Overflow or Wraparound
CWE-362	1,13	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-77	1,10	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-863	1,10	Incorrect Authorization
CWE-94	0,90	Improper Control of Generation of Code ('Code Injection')
CWE-287	0,75	Improper Authentication
CWE-502	0,65	Deserialization of Untrusted Data
CWE-306	0,62	Missing Authentication for Critical Function
CWE-798	0,59	Use of Hard-coded Credentials
CWE-119	0,56	Improper Restriction of Operations within the Bounds of a Memory Buffer
…	…	…

Examples … (1)

CVE-2021-44228 (CWE-502 Deserialization of Untrusted Data)

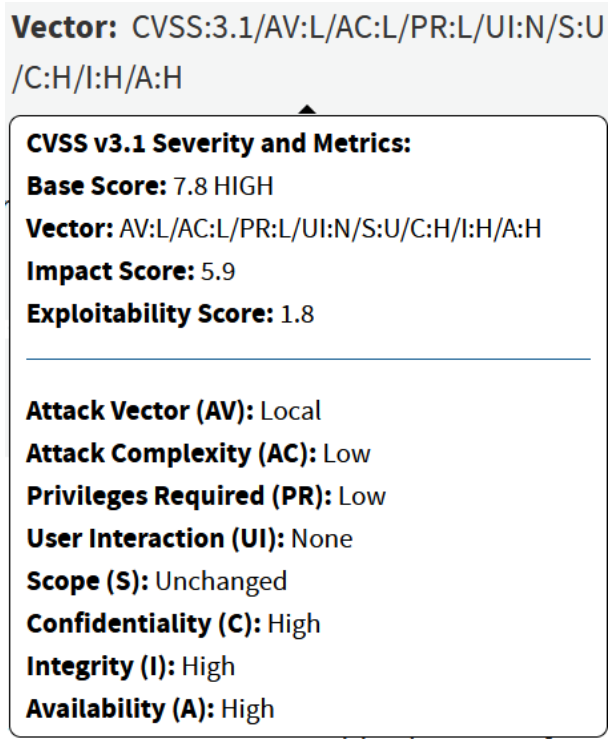
Apache Log4j2 2.0-beta9 through 2.15.0 (…) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. ….



Examples … (2)

CVE-2022-22960 (CWE-269 Improper Privilege Management):

VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a privilege escalation vulnerability due to improper permissions in support scripts. A malicious actor with local access can escalate privileges to 'root'.

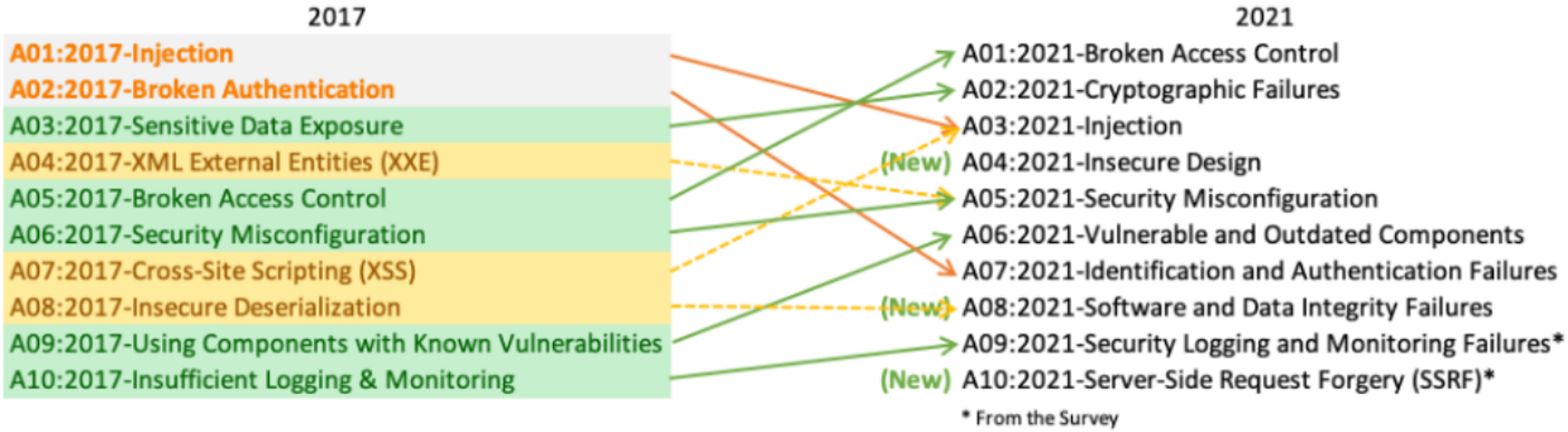


Other classifications (MITRE)

- Common Vulnerabilities and Exposures (cve.mitre.org)
  - vulnerabilities ~ NVD (NVD contains more information)
- Common Weaknesses Enumeration (cwe.mitre.org)
  - buffer overflows, XSS, CSRF, code injection, etc.
- Common Attack Pattern Enumeration and Classification (capec.mitre.org)
  - attack hierarchies, description, prerequisites, mitigation, CWE link, etc.
- ATT&CK – Adversary tactics and techniques (attack.mitre.org)
  - knowledge base, ATT&CK for Enterprise, ATT&CK for Mobile
- Common Platform Enumeration (MITRE → NIST, nvd.nist.gov/products/cpe)
  - dictionary for IT systems, software, and packages
  - can describe version, release, platform etc.

OWASP: Open Web Application Security Project

- primarily for web applications – vulnerabilities, attacks, risks
- OWASP Top 10 (most critical web application security risks, 2021)
  - OWASP Top 10:2025 planned for the first half of 2025
- Web Security Testing Guide (v4.2, 2020)
- Application Security Verification Standard (v4.0.3, 2021)
- Mobile Application Security Testing Guide (v1.7.0, 2023)
- Mobile Application Security Verification Standard (v2.1.0, 2024)

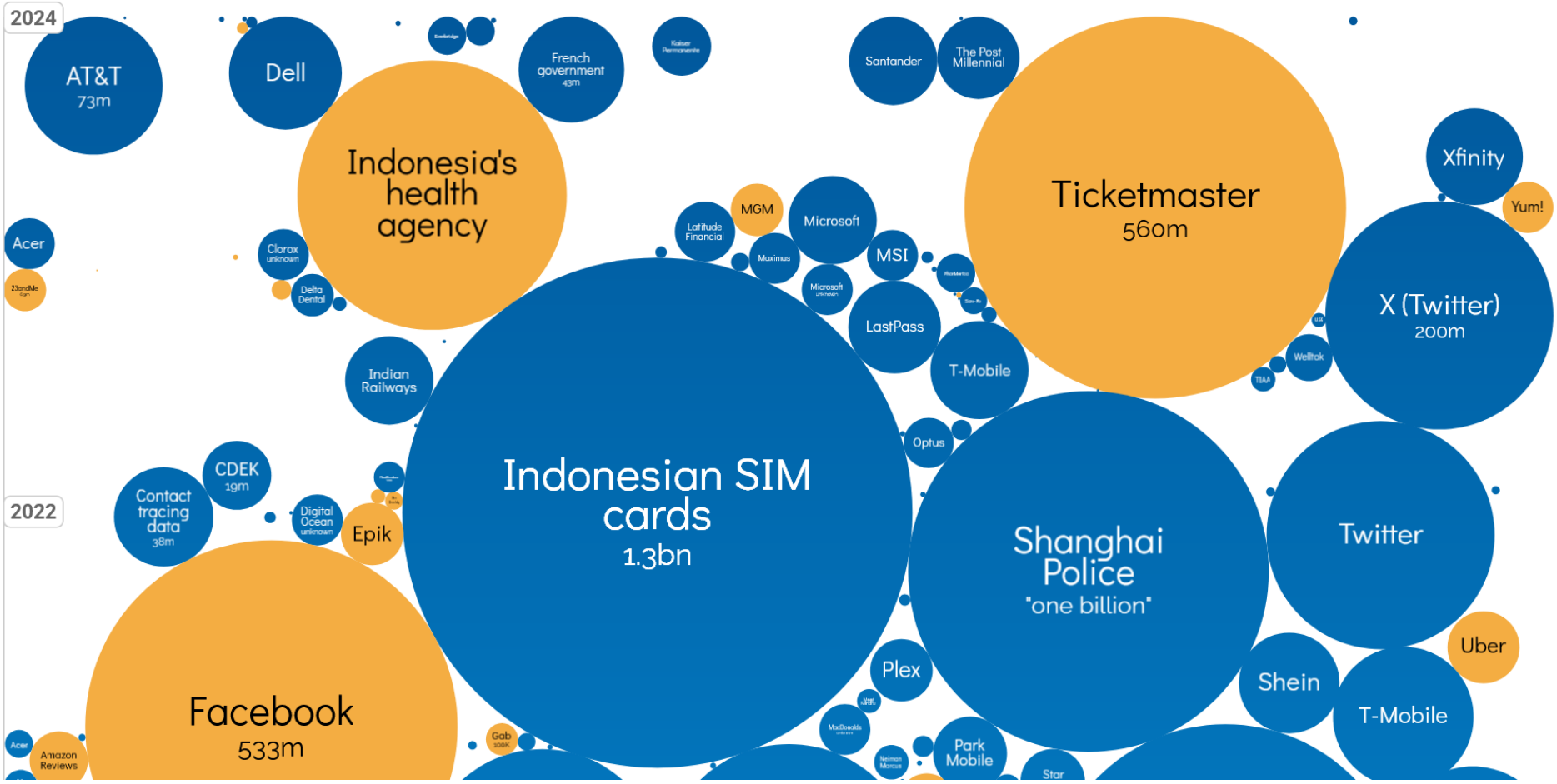


source: OWASP, owasp.org/www-project-top-ten

Real world

- not everything is published or shared
- sometimes you just don't know yet
- sometimes you are just lucky

https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



EY Global Information Security Survey 2021

- more than 1.000 respondents
- senior cybersecurity professionals (e.g. CISO)
- *extremely confident in their organization's cybersecurity risk*
  - 9% in 2021 (20% in 2020)
- the problems:
  - insufficient budget – realigned cybersecurity, cost-reduction
  - complex new regulations – drain of time and resources
  - deteriorating relationship with business leaders

Verizon: 2024 Data Breach Investigations Report

- summary of 1 year (incidents Nov 22 – Oct 23)
- global coverage, detailed, 100 pages, victims in 94 countries
- Incident: A security event that compromises the integrity, confidentiality or availability of an information asset.
- Breach: An incident that results in the confirmed disclosure – not just potential exposure – of data to an unauthorized party.
- datasets contributed by various security vendors
- 30 458 security incidents, and 10 626 confirmed data breaches
- the report provides details for 10 industries

Verizon – 2024 DBIR – patterns in incidents

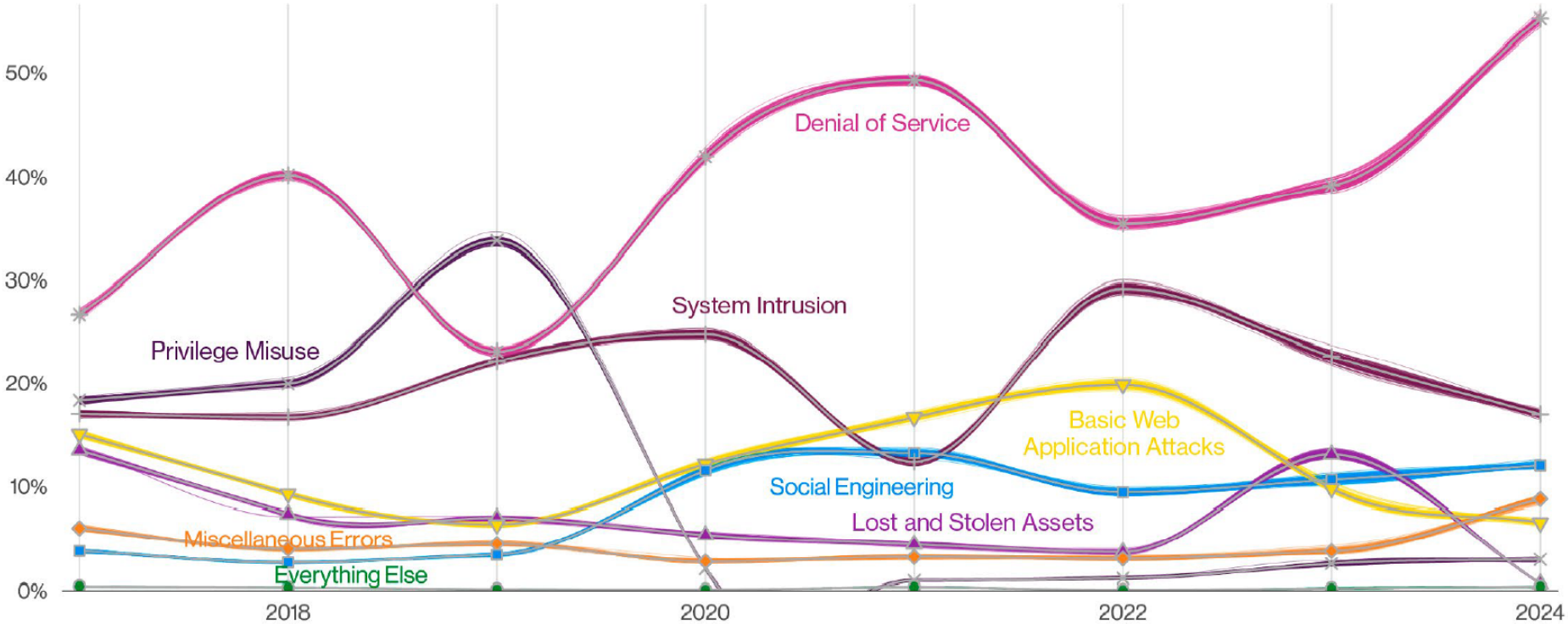


Figure 26. Patterns over time in incidents

Verizon – 2024 DBIR – patterns in breaches

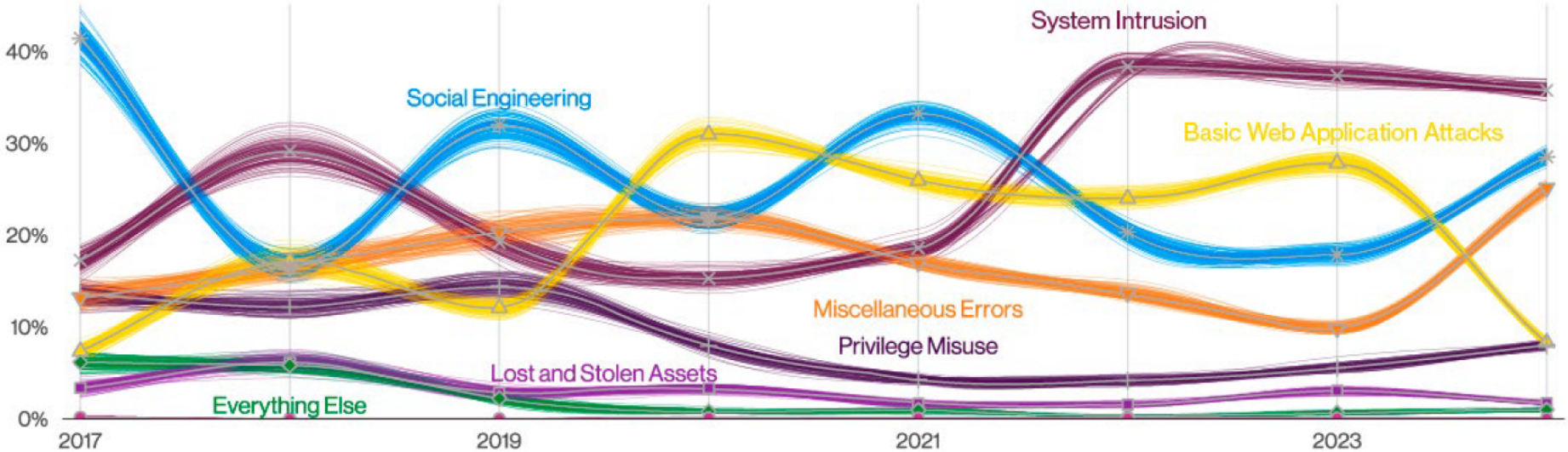


Figure 27. Patterns over time in breaches

Verizon – 2024 DBIR – some observations

- breaches – threat actors
  - internal (35%, mostly Miscellaneous Errors) vs. external (65%)
  - motives: > 90% financial
- breaches – action:
  - exploit vulnerabilities (10%) vs. use of stolen credentials (24%)
  - ransomware (23%)
- the median time to click on a malicious link after the email is opened: 21 seconds + additional 28 seconds to enter data
- CISA KEV vulnerabilities:
  - 55 days ~ 50% of vulnerabilities unremediated
  - 180 days ~ 20% of vulnerabilities unremediated
  - 365 days ~ 8% of vulnerabilities unremediated

What to do – Controls, regulatory and compliance frameworks

What to do – regulatory and compliance frameworks

- NIST SP 800-53 (Release 5.1.1) Security and Privacy Controls for Information Systems and Organizations (2023)
  - supplemental material – mappings, control catalog, templates
- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls
  - best practice recommendations on information security controls
  - open to interpretation (good and bad)
- NIST Cybersecurity Framework (Version 2.0, 2024)
  - set of desired cybersecurity activities and outcomes using (easy to understand) common language

NIST Cybersecurity Framework

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

What to do – regulatory and compliance frameworks (2)

- Australian Government Information Security Manual (2024)
- ISACA: COBIT 5 Framework
- Payment Card Industry – Data Security Standard version 4.0.1 (PCI DSS, 2024)
- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti, ...
- Zákon č. 95/2019 Z. z. o ITVS, Vyhláška č. 179/2020 Z. z. (spôsob kategorizácie a obsah bezpečnostných opatrení)
- Zákon č. 367/2024 Z. z. o kritickej infraštruktúre ...
- CIS Critical Security Controls (v8.1, 2024)
  - 18 controls, 153 safeguards
  - implementation groups IG1 (essential cyber hygiene), IG2 and IG3

CIS Controls v8.1 – controls

https://www.cisecurity.org/controls/

1. Inventory and Control of Enterprise Assets
2. Inventory and Control of Software Assets
3. Data Protection
4. Secure Configuration of Enterprise Assets and Software
5. Account Management
6. Access Control Management
7. Continuous Vulnerability Management
8. Audit Log Management
9. Email and Web Browser and Protections
10. Malware Defenses
11. Data Recovery
12. Network Infrastructure Management
13. Network Monitoring and Defense

CIS Controls v8.1 – controls (2)

14. Security Awareness and Skills Training
15. Service Provider Management
16. Application Software Security
17. Incident Response Management
18. Penetration Testing

UK: Cyber Essentials Scheme

https://www.ncsc.gov.uk/cyberessentials

- Cyber Essentials: Requirements for IT infrastructure (v3.1, 2023)
  - just basic controls, 16 pages
  - clear guidance what is in scope and what to do
- Cyber Essentials (self-assessment, verification)
- Cyber Essentials Plus (hands-on technical verification)
- Technical control themes:
  1. Firewalls
  2. Secure configuration
  3. Security update management
  4. User access control
  5. Malware protection