





Welcome to

Workshop 3: cybersikkerhed i virksomheder

Cyber Security CISO for a Day

Henrik Kramselund he/him han/ham hkj@zencurity.com @kramse  

Slides are available as PDF, kramse@Github
cyber-security-ciso-for-a-day.tex in the repo security-courses

ATU hos KEA Maj, 2022

Time schedule



14:00 - 16:00 including breaks

14:00 - 14:20 – Introduction to Security

14:20 - 14:40 – Exercises 1 + 2

Summary part 1 and break

15:00 - 15:20 – Exercises 3 + 4

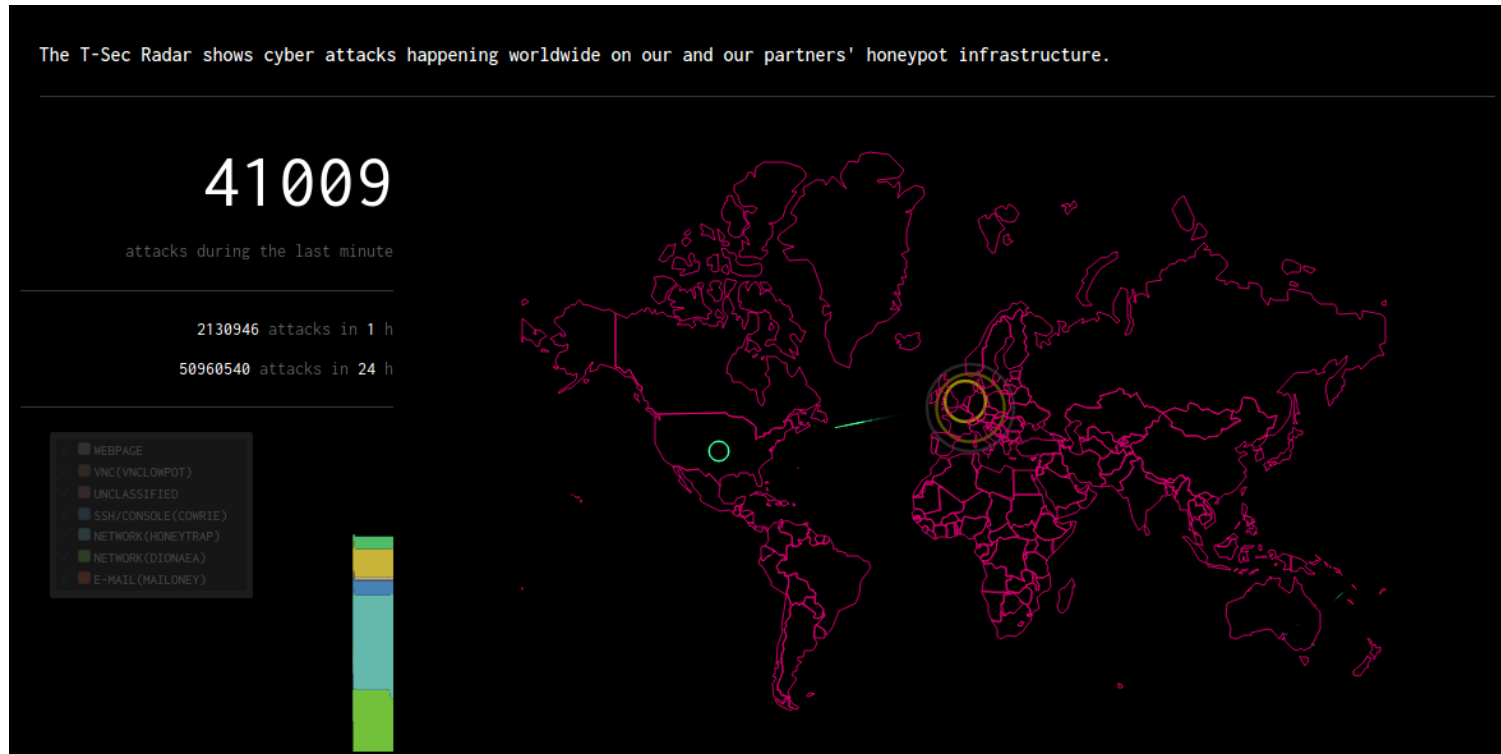
15:20 - 15:40 – Exercises 5 + 6

15:45 Summary, conclusion, last questions

All slides are in english, exercises in Danish!

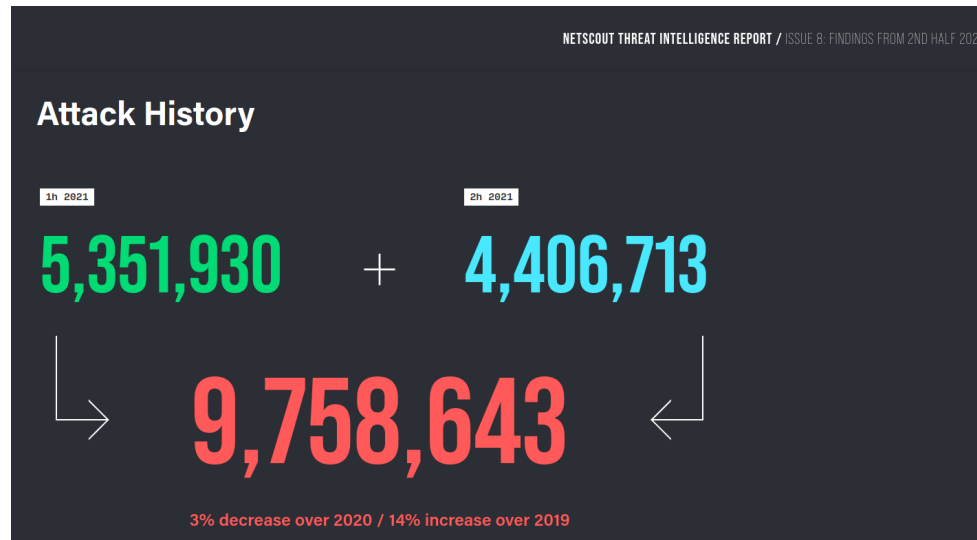
Hint: Don't panic if the plan breaks!

Introduction: Attack overview



Source: <http://www.sicherheitstacho.eu/>

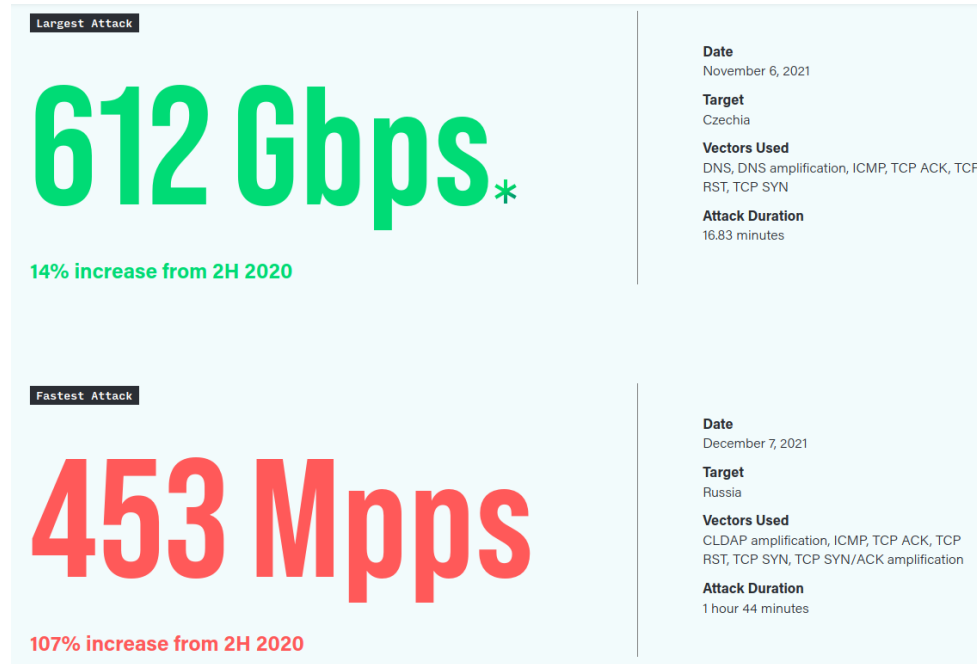
DDoS Attacks Still a Problem



Security attacks and DDoS is very much in the media

Source: [linkhttps://www.netscout.com/threatreport/global-ddos-attack-trends/](https://www.netscout.com/threatreport/global-ddos-attack-trends/)

DDoS Attacks are HUGE








Extremely hard to protect against from a small network

Source: [linkhttps://www.netscout.com/threatreport/global-ddos-attack-trends/](https://www.netscout.com/threatreport/global-ddos-attack-trends/)

Ransomware Attacks are Common

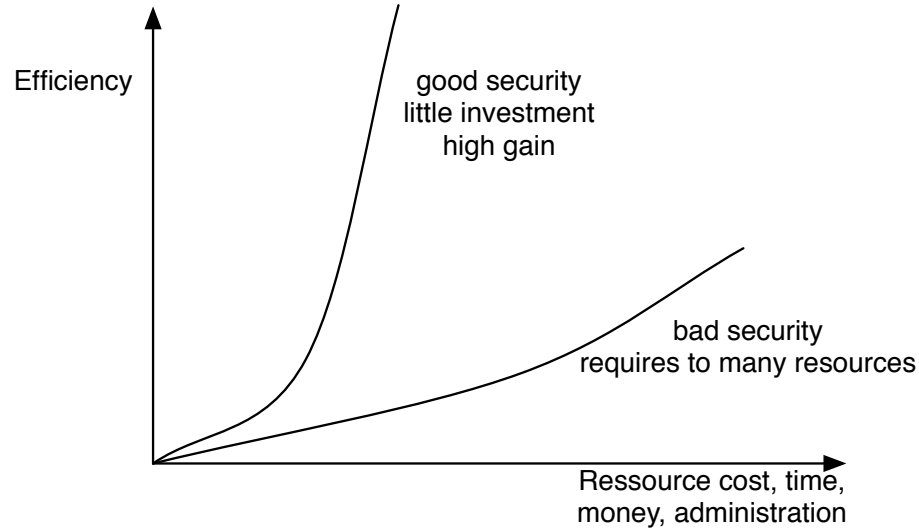


	<p>Avaddon</p> <p><u>Avaddon</u> ransomware was first seen in February 2020 and by June 2020 had quickly evolved into ransomware as a service (RaaS). In January 2021, the group evolved again to include DDoS attacks in its extortion repertoire.</p> <p>READ MORE +</p>
	<p>REvil</p> <p>Although currently not operational due to a global takedown, <u>REvil</u> was a prominent user of RaaS. With its highly adaptable encryptors and decryptors, REvil provided infrastructure and services for communicating with victims, as well as a leak site for releasing stolen data if the victim refused to pay the ransom.</p> <p>READ MORE +</p>
	<p>BlackCat</p> <p>One of the newest ransomware groups, <u>BlackCat</u> (aka ALPHV), was discovered in November 2021. Operating as a RaaS, the group quickly gained notoriety for its sophistication and innovation.</p> <p>READ MORE +</p>
	<p>AvosLocker</p> <p>First seen in summer 2021, <u>AvosLocker</u> is simple but effective ransomware that has utilized triple extortion from the start. AvosLocker operators advertise in underground networks for affiliates with active directory experience, as well as for "access brokers" who potentially could provide access to compromised systems.</p> <p>READ MORE +</p>
	<p>Suncrypt</p> <p>Initially appearing in October 2019, <u>Suncrypt</u> was one of the first ransomware groups to launch DDoS attacks. Along with data encryption and theft, Suncrypt extorts its victims by threatening to attack infrastructure or networks.</p> <p>READ MORE +</p>

Make sure to backup your data! Test your backups!

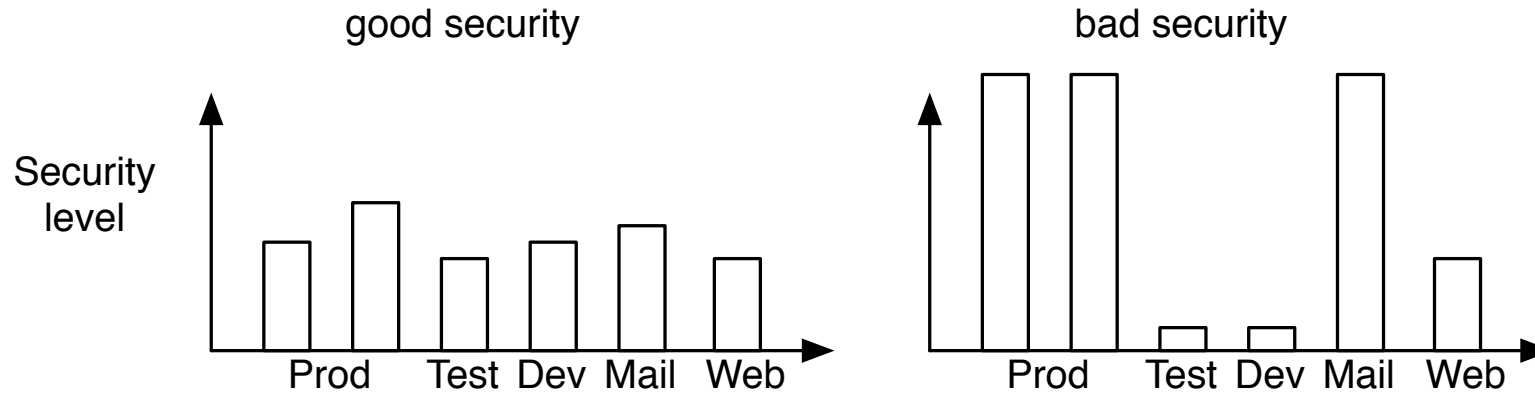
Source: [linkhttps://www.netscout.com/threatreport/global-ddos-attack-trends/](https://www.netscout.com/threatreport/global-ddos-attack-trends/)

What can we do? – Good security



You always have limited resources for protection - use them as best as possible
Good security comes from structured work

Balanced security



Better to have the same level of security

If you have bad security in some part - guess where attackers will end up

Hackers are not required to take the hardest path into the network

Realize there is no such thing as 100% security

Work together



Team up!

We need to share security information freely

We often face the same threats, so we can work on solving these together

My daily job – Security engineering a job role



On any given day, you may be challenged to:

- Create new ways to solve existing production security issues
- Configure and install firewalls and intrusion detection systems
- Perform vulnerability testing, risk analyses and security assessments
- Develop automation scripts to handle and track incidents
- Investigate intrusion incidents, conduct forensic investigations and incident responses
- Collaborate with colleagues on authentication, authorization and encryption solutions
- Evaluate new technologies and processes that enhance security capabilities
- Test security solutions using industry standard analysis criteria
- Deliver technical reports and formal papers on test findings
- Respond to information security issues during each stage of a project's lifecycle
- Supervise changes in software, hardware, facilities, telecommunications and user needs
- Define, implement and maintain corporate security policies
- Analyze and advise on new security technologies and program conformance
- Recommend modifications in legal, technical and regulatory areas that affect IT security

Source: <https://www.cyberdegrees.org/jobs/security-engineer/>
also https://en.wikipedia.org/wiki/Security_engineering



Information Risk Management

Life is full of risk.

Risk is the possibility of damage happening and the ramifications of such damage should it occur. *Information risk management (IRM)* is the *process* of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level. There is no such thing as a 100 percent secure environment. Every environment has vulnerabilities and threats to a certain degree. The skill is in identifying these threats, assessing the probability of them actually occurring and the damage they could cause, and then taking the right steps to reduce the overall level of risk in the environment to what the organization identifies as acceptable.

Source: Shon Harris *CISSP All-in-One Exam Guide*

Security Controls and Frameworks



Multiple exist

- CIS controls Center for Internet Security (CIS) <https://www.cisecurity.org>
- PCI Best Practices for Maintaining PCI DSS Compliance v2.0 Jan 2019
- NIST Cybersecurity Framework (CSF)
Framework for Improving Critical Infrastructure Cybersecurity
<https://www.nist.gov/cyberframework>
<http://csrc.nist.gov/publications/PubsSPs.html>
- National Security Agency (NSA)
<http://www.nsa.gov/research/publications/index.shtml>
- NSA security configuration guides
http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml
- Information Systems Audit and Control Association (ISACA)
<http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/default.aspx>



“A goal without a plan is just a wish.”

Antoine de Saint-Exupéry

The CIS Controls™ are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. The CIS Controls are developed by a community of IT experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors including retail, manufacturing, healthcare, education, government, defense, and others.

Source: <https://www.cisecurity.org/CIS-Controls-Version-7-1.pdf>

Kom igang med CIS



CIS-kontrollerne består af 20 praktiske, pragmatiske kontroller, som er målbare og med direkte henvisning til, hvordan de implementeres samt forslag til, hvilke KPI'er der bør opstilles for målinger.

Forskellen på CIS-kontrollerne og fx ISO27001 er, at du ikke kan blive certificeret efter CIS, men til gengæld opdateres CIS-kontrollerne løbende, og de indeholder prioriterede lister af, hvad du i praksis skal gøre for din cybersikkerhed. Det australske forsvar har fx vist, at hvis man implementerer de første fire kontroller fuldt ud, kan man mitigere op mod 90+% af alt malware.

Dansk artikel fra Deloitte, version 7 men version 8 er ude <https://www2.deloitte.com/dk/da/pages/risk/articles/vi-stiller-skarpt-pa-cis-kontroller.html>

Exercises



CIS controls 1-6 are Basic, everyone must do them. Today I have replaced 6 with 10.

- **CIS Control 1: Inventory and Control of Hardware Assets**
- **CIS Control 2: Inventory and Control of Software Assets**
- **CIS Control 3: Continuous Vulnerability Management**
- **CIS Control 4: Controlled Use of Administrative Privileges**
- **CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers**
- **CIS Control 10: Data Recovery Capabilities**

We will now start the exercises, two controls at a time!

First decide, if this was a real company, how would you implement these?

1,2,3,4,5 and then 10?

Inventory and Control of Hardware Assets



CIS Control 1:

Inventory and Control of Hardware Assets

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

What is connected to our networks?

What firmware do we need to install on hardware?

Where IS the hardware we own?

What hardware is still supported by vendor?

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Inventory and Control of Software Assets



CIS Control 2:

Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that all unauthorized and unmanaged software is found and prevented from installation or execution.

What licenses do we have? Paying too much?

What versions of software do we depend on?

What software needs to be phased out, upgraded?

What software do our employees need to support?

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Øvelse 1 + 2



- Nu skal I *implementere* CIS kontrollerne 1 og 2
- Det foregår ved at I prøver at tænke på dem som om I var en CISO – Chief Information Security Officer, IT-sikkerhedschef
- Tænk på dem med jeres viden om IT, jeres egne IT-systemer

Continuous Vulnerability Management



CIS Control 3:

Continuous Vulnerability Management

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

Scan for updates automatically

Update when vendors publish critical patches

Listen to news sources about software and vulnerabilities

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Controlled Use of Administrative Privileges



CIS Control 4:

Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

Remove local administrator from Windows workstations

Change default passwords

Use good passwords

Log if somebody tries to break in

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Øvelse 3 + 4



- Nu skal I *implementere* CIS kontrollerne 3 og 4
- Det foregår ved at I prøver at tænke på dem som om I var en CISO – Chief Information Security Officer, IT-sikkerhedschef
- Tænk på dem med jeres viden om IT, jeres egne IT-systemer

Secure Configuration for Hardware and Software



CIS Control 5:

Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Create secure configuration – check security settings

Select security mechanisms

Automate security settings

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Data Recovery Capabilities



CIS Control 10:

Data Recovery Capabilities

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it

Backup is critical

If we loose orders we loose money

Data loss, means production capacity loss

Separation of duty – can one person delete both production and backup

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Øvelse 5 + 10



- Nu skal I *implementere* CIS kontrollerne 5 og 10
Bemærk ikke 5 og 6, nummer 10 er nemmere og vigtigere for jer
- Det foregår ved at I prøver at tænke på dem som om I var en CISO – Chief Information Security Officer, IT-sikkerhedschef
- Tænk på dem med jeres viden om IT, jeres egne IT-systemer

Hændelseslog og Økonomi



Tag et stykke papir eller en computer

- Vi er blevet afbrudt i vores vigtige arbejde med CIS kontroller
- Vi skal udfylde en Hændelseslog og der er nogle økonomiske aspekter
- Når der sker en sikkerhedshændelse skal den helst håndteres effektivt
- Hvis man ikke har sikkerhedsprocedurer på plads bliver det typisk længerevarende og dyrere

March 2021: ProxyLogon/ProxyShell CVE-2021-26855 CVSS:3.0 9.1 / 8.4



In March 2021, both Microsoft and IT Professionals had a major headache in the form of an Exchange zero-day commonly known as ProxyLogon. The vulnerability, widely considered the **most critical to ever hit Microsoft Exchange**, was quickly exploited in the wild by suspected state-sponsored threat actors, with US government and military systems identified as the most targeted sectors. **Ransomware variants such as DoejoCrypt were soon actively exploiting unpatched Exchange instances**, attempting to monetise the vulnerability.

A follow-up exploit, dubbed ProxyShell, was evolutionary in nature and targeted on-premise Client Access Servers (CAS) in **all supported versions of Exchange Server**. Due to the **remotely accessible nature of Exchange CAS**, any unpatched instances would be vulnerable to Remote Code Execution. **High profile victims included the European Banking Authority and the Norwegian Parliament.**

Source - for this description:

<https://chessict.co.uk/resources/blog/posts/2022/january/2021-top-security-vulnerabilities/>

ProxyLogon CVE-2021-26855 CVSS:3.0 9.1 / 8.4



ProxyLogon is the formally generic name for CVE-2021-26855, a vulnerability on Microsoft Exchange Server that allows an attacker bypassing the authentication and impersonating as the admin. We have also chained this bug with another post-auth arbitrary-file-write vulnerability, CVE-2021-27065, to get code execution. All affected components are vulnerable by default!

As a result, **an unauthenticated attacker can execute arbitrary commands on Microsoft Exchange Server through an only opened 443 port!**

Sources: <https://proxylogon.com/>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855>

Incident Handling: ProxyLogon



Hvis jeres gruppe har implementeret CIS Control 2: Inventory and Control of Software Assets, noter følgende:

- Hændelseslog: Marts Proxylogin - nem oprydning, ingen nedetid
- Økonomi: Marts Proxylogin oprydning EUR 3.000

Hvis jeres gruppe ***IKKE*** har implementeret CIS Control 2: Inventory and Control of Software Assets, noter følgende:

- Hændelseslog: Marts Proxylogin – mailservere inficeret 3 steder, ekstern hjælp nødvendig, nedetid 2 dage
- Økonomi: Marts Proxylogin oprydning EUR 3.000
- Økonomi: Marts ProxyLogon hændeshåndtering ekstern hjælp EUR 10.000

June 2021: PrintNightmare CVE-2021-34527 CVSS:3.0 8.8 / 8.2



In June, Microsoft released a critical security update to address weaknesses in the Printer Spooler service on Windows desktop and server platforms. Unfortunately, it was released out-of-band outside of the standard patch Tuesdays due to the severity. Microsoft even released patches for Windows 7, an supported operating system that does not normally receive updates.

Initially categorised by Microsoft as a local privilege escalation on Windows, security researchers subsequently identified an additional **Remote Code Execution (RCE)** vector resulting in an updated advisory from Microsoft. As ever, the ability to test and deploy patches in a time-sensitive manner is key to minimising the impact of such vulnerabilities.

Additionally, PrintNightmare had the additional horror factor of dropping during the **summer holiday season in the northern hemisphere**. Our consultants continue to see systems vulnerable to PrintNightmare on client engagements, which can be trivially leveraged to obtain privilege escalation on unpatched Windows systems.

Source - for this description:

<https://chessict.co.uk/resources/blog/posts/2022/january/2021-top-security-vulnerabilities/>

See also <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527>

Incident Handling: PrintNightmare



Hvis jeres gruppe har implementeret CIS Control 2: Inventory and Control of Software Assets, noter følgende:

- Hændelseslog: Juni PrintNightmare - nem oprydning, ingen nedetid
- Økonomi: Juni PrintNightmare oprydning EUR 3.000

Hvis jeres gruppe ***IKKE*** har implementeret CIS Control 2: Inventory and Control of Software Assets, noter følgende:

- Hændelseslog: Juni PrintNightmare – servere inficeret, geninstallation nødvendig, nedetid 3 dage
- Økonomi: Juni PrintNightmare oprydning EUR 3.000
- Økonomi: Juni PrintNightmare hændelseshåndtering ekstern hjælp EUR 10.000

Da denne skete i ferien er der desværre også brugt mere tid på at håndtere sagen, alle sætter ekstra EUR 3.000 på listen med teksten "Grundet ferie og manglende ressourcer 3.000"

September 2021: ForcedEntry



Apple didn't escape the wrath of critical zero-day vulnerabilities in 2021, with ForcedEntry made public in September. The concern was not just that it could escape in-built sandbox controls and be leveraged against **almost all iOS versions at the time**, but also that it was in the form of a **one-click exploit meaning that no user interaction was needed**. A threat actor would simply require the target victim's phone number or email address to send a weaponised GIF. **Furthermore, iMessage was affected on macOS and watchOS, giving the exploit a significant attack surface of well over a billion devices.**

An analysis released at the end of 2021 confirmed a highly complex exploit which is believed to have been created by the NSO Group, creators of the Pegasus platform, albeit with the sophistication of nation-state actors. Given the nature of the attack and the level of complexity, high profile individuals are likely to be the intended targets of such exploits, only used sparingly against targeted victims.

Source - for this description:

<https://chessict.co.uk/resources/blog/posts/2022/january/2021-top-security-vulnerabilities/>

See also <https://en.wikipedia.org/wiki/FORCEDENTRY>

Incident Handling: ForcedEntry



Hvis jeres gruppe har implementeret CIS Control 1+2, og ingen Apple telefoner har noter følgende:

- Hændelseslog: September ForcedEntry - nem oprydning, ingen nedetid
- Økonomi: September ForcedEntry oprydning EUR 1.000

Hvorfor er det ikke EUR 0?

Hvis jeres gruppe har Apple telefoner noter følgende:

- Hændelseslog: September ForcedEntry – Apple telefoner inficeret, ekstern hjælp nødvendig
- Økonomi: September ForcedEntry oprydning EUR 3.000
- Økonomi: September ForcedEntry hændeshåndtering ekstern hjælp EUR 10.000

November 2021: Log4Shell



It would not be possible to discuss 2021 in the context of vulnerabilities without the mention of Log4Shell. **A widely used Java-based logging library caused headaches for Security professionals worldwide.** Many scrambled to quantify their use of Log4j within their estates.

A zero-day exploit quickly followed, confirming the worst - **Remote Code Execution (RCE) was indeed possible.** However, what made the nature of the vulnerability even more challenging was the ability to exploit a backend logging system from an unaffected front end host. For example, an attacker can craft a weaponised log entry on a mobile app or webserver not running Log4j. The attacker could make their way through to backend middleware itself running Log4j, which significantly extends the attack surface of the vulnerability.

The NCSC even took the step of recommending the update was immediately applied, whether or not Log4Shell was known to be in use. As is commonly the case with critical vulnerabilities, two successive Log4j patches were subsequently released in the week following the original addressing Denial of Service (DoS) and a further RCE. This further increased workloads of Security and IT teams just as they thought the worst of 2021 had been and gone.

Source - for this description:

<https://chessict.co.uk/resources/blog/posts/2022/january/2021-top-security-vulnerabilities/>

See also <https://en.wikipedia.org/wiki/Log4Shell>

Incident Handling: Log4Shell



Hvis jeres gruppe har implementeret CIS Control , noter følgende:

- Hændelseslog: Marts xxx - nem oprydning, ingen nedetid
- Økonomi: Marts xxxx oprydning EUR 3.000

Hvis jeres gruppe ***IKKE*** har implementeret , noter følgende:

- Hændelseslog: Marts xxx – mailservere inficeret 3 steder, ekstern hjælp nødvendig, nedetid 2 dage
- Økonomi: Marts xxx oprydning EUR 3.000
- Økonomi: Marts xxx hændelseshåndtering ekstern hjælp EUR 10.000

March 2022: Dirty pipe Linux CVE-2022-0847



This is the story of CVE-2022-0847, a vulnerability in the **Linux kernel since 5.8** which allows overwriting data in arbitrary read-only files. This leads to **privilege escalation because unprivileged processes can inject code into root processes.**

It is similar to CVE-2016-5195 “Dirty Cow” but is easier to exploit.

The vulnerability was fixed in Linux 5.16.11, 5.15.25 and 5.10.102.

Sources: <https://dirtypipe.cm4all.com/> <https://thestack.technology/dirty-pipe-exploited-linux-vulnerability-cve-2022-0847>
<https://access.redhat.com/security/cve/CVE-2022-0847>

Incident Handling: Dirty pipe



Hvis jeres gruppe har implementeret CIS Control 1+2 og ingen Linux har, noter følgende:

- Hændelseslog: Marts Dirty pipe - nem oprydning, ingen nedetid
- Økonomi: Marts Dirty pipe oprydning EUR 3.000

Hvis jeres gruppe har Linux , noter følgende:

- Hændelseslog: Marts Dirty pipe – servere inficeret, ekstern hjælp nødvendig, nedetid 2 dage
- Økonomi: Marts Dirty pipe oprydning EUR 3.000
- Økonomi: Marts Dirty pipe hændeshåndtering ekstern hjælp EUR 10.000



ESET researchers have discovered and analyzed three vulnerabilities affecting various Lenovo consumer laptop models. The first two of these vulnerabilities – CVE-2021-3971, CVE-2021-3972 – affect UEFI firmware drivers originally meant to be used only during the manufacturing process of Lenovo consumer notebooks. Unfortunately, they were mistakenly included also in the production BIOS images without being properly deactivated. These affected firmware drivers can be activated by attacker to directly disable SPI flash protections (BIOS Control Register bits and Protected Range registers) or the UEFI Secure Boot feature from a privileged user-mode process during OS runtime. It means that exploitation of these vulnerabilities would allow attackers to deploy and successfully execute SPI flash or ESP implants, like LoJax or our latest UEFI malware discovery ESpecter, on the affected devices.

Source:

also: <https://www.welivesecurity.com/2022/04/19/when-secure-isnt-secure-uefi-vulnerabilities-lenovo-consumer-laptops/>

See also: <https://www.bleepingcomputer.com/news/security/lenovo-uefi-firmware-driver-bugs-affect-over-100-laptop-models/>

Incident Handling: Lenovo UEFI



Hvis jeres gruppe har implementeret CIS Control 1+2, og ingen Lenovo computere har noter følgende:

- Hændelseslog: Marts Lenovo UEFI - ingen Lenovo computere, ingen nedetid
- Økonomi: Marts Lenovo UEFI oprydning EUR 0

Hvis jeres gruppe har Lenovo computere, noter følgende:

- Hændelseslog: Marts Lenovo UEFI – Lenovo computere udskiftet hos 10 medarbejdere, nedetid 1 dag for hver 10 medarbejdere
- Økonomi: Marts Lenovo UEFI oprydning EUR 5.000
- Økonomi: Marts Lenovo UEFI hændeshåndtering udskiftning af udstyr EUR 10.000

Konklusion: Kaos og panik







- Vi startede godt, struktureret arbejde!
- Vi blev afbrudt ... og det sker tit
- Vi blev ikke færdige! Det bliver man sjældent i virkeligheden
- Microsoft frigiver opdateringer for mere end 100 sårbarheder om måneden
- Al software har sikkerhedsproblemer, og skal opdateres!

Contact information



- Henrik Kramselund, he/him internet samurai mostly networks and infosec
- Network and security consultant Zencurity, teach at KEA and activist
- Master from the Computer Science Department at the University of Copenhagen, DIKU
- Email: hkj@zencurity.dk Mobile: +45 2026 6000

You are welcome to drop me an email