Welcome to

Basal it-sikkerhed i en altid accelererende verden

2024

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

Slides are available as PDF, kramse@Codeberg
it-sikkerhed-accelererende-verden.tex in the repo security-courses

slides are also available on Github

Plan for today

Talk about the current world of information security

What a crazy place we are in with a flood of vulnerabilities

Resource shortage – man power, skillz etc.

Goals:

Point to a way out of the forever *patch everything now*-cycle

Give a high level view – don't try to remember everything

An inspiration to do the basics, before buying into the latest craze

General AI and large language models (LLM) won't solve most problems, machine learning does solve some

We have solutions – some have been around since the 70s and 80s

Every Year

- Same problems last year? Same problems EVERY year
- Last year was a nightmare of break-ins and data leaks
- Data leaks, GDPR, ransomware, ...

Try not to panic, but there are lots of threats

Are we loosing the battle?

Har du haft snakken med din CISO?

IT-sikkerhed:
Vi vil gerne bede om 10 millioner til IT-sikkerhed i budget næste år
CTO/CIO/CISO:
Umuligt
IT-sikkerhed:
OK, fair nok. Så skal vi bare bede om **100 millioner til Ransomware**, tak.
Husk også at uddanne CFO i bitcoin transaktioner.

- Er ovenstående urealistisk?

Demant 2019

- For året 2019 rapporterede vi et tab i omsætning på **575 millioner kroner**. Det i sig selv er alvorligt. Hvad angår vores opmærksomhed på it-sikkerhedsområdet, har it-hændelsen været med til at understrege nødvendigheden af, at tage dette felt seriøst. Angreb mod it-infrastruktur er uden tvivl en af de største trusler mod en virksomhed, og det kan gå galt, hvis man ikke er i stand til at lukke ned for skaden og bruge sin back-up.

...

- På det konkrete plan har vi fået et mantra der lyder **'Active Directory is king, and backup is Queen'**. Men mere overordnet har vi også lært at Fokus skal helt op på øverste niveau i virksomheden, at man skal skaffe høj faglig indsigt i sikkerhed og trusler, og at det er et arbejde, der skal være under konstant observation og udvikling.

Kilde: https://dit.dk/Nyheder/2021/Demant

- Vi taler altså om tab i størrelsesorden tre-cifrede millionbeløb!

Overlapping Security Incidents

New data breaches nearly every week, these from danish news site version2.dk

Problem, we need to receive data from others

Data from others may contain malware

Have a job posting, yes
- then HR will be expecting CVs sent as .doc files

Paranoia defined

par·a·noi·a
/ˌparəˈnoiə/

noun
noun: **paranoia**

1. a mental condition characterized by delusions of persecution, unwarranted jealousy, or exaggerated self-importance, typically elaborated into an organized system. It may be an aspect of chronic personality disorder, of drug abuse, or of a serious condition such as schizophrenia in which the person loses touch with reality.
   synonyms: persecution complex, delusions, obsession, psychosis More
- suspicion and mistrust of people or their actions without evidence or justification.
  "the global paranoia about hackers and viruses"

Origin

GREEK
para
irregular
GREEK
noos
mind
GREEK
paranoos
distracted
MODERN LATIN
paranoia
early 19th cent.

More

Source: google paranoia definition

Use appropriate paranoia, and yes, hot pink red blinking is an appropriate threat level

Hackers don’t give a shit

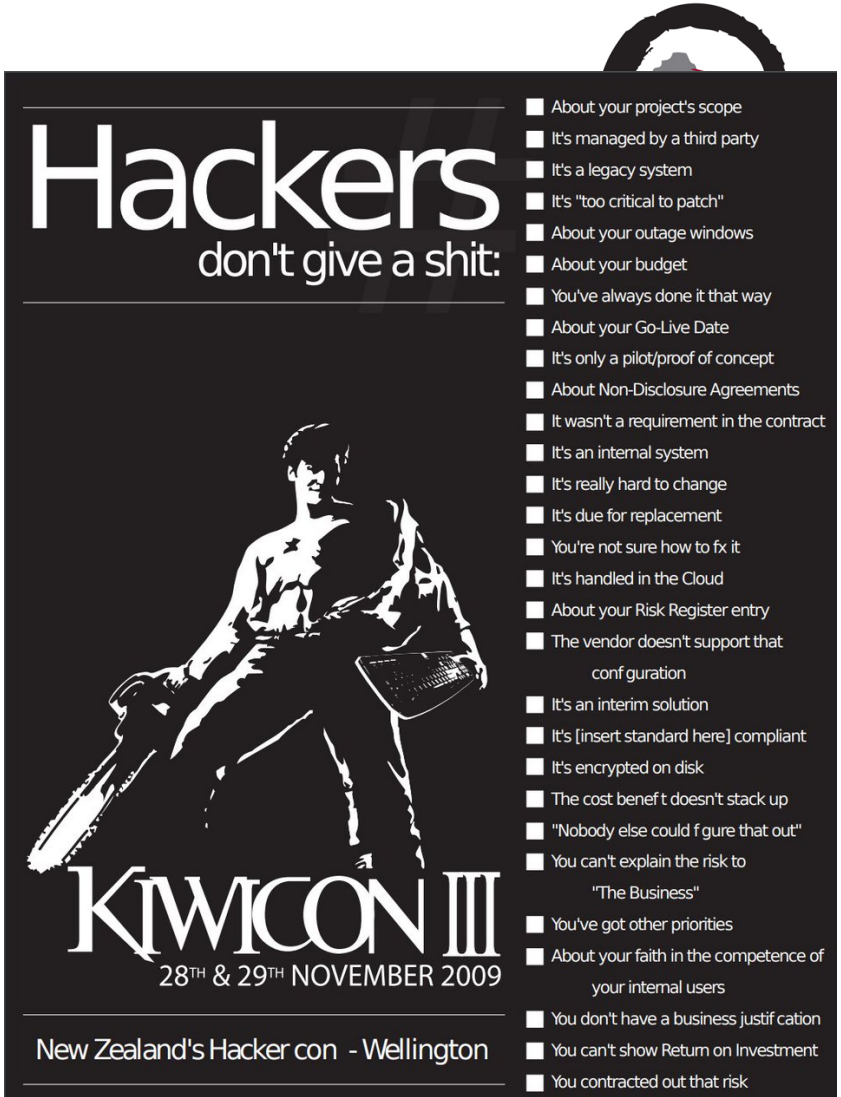
Your system is only for testing, development, ...

Your network is a research network, under construction, being phased out, ...

Try something new, go to your management

Bring all the exceptions, all of them, update the risk analysis figures - if this happens it is about 1mill DKK

Think like attackers - don’t hold back



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

Goals of Security

Prevention - means that an attack will fail

Detection - determine if attack is underway, or has occured - report it

Recovery - stop attack, assess damage, repair damage

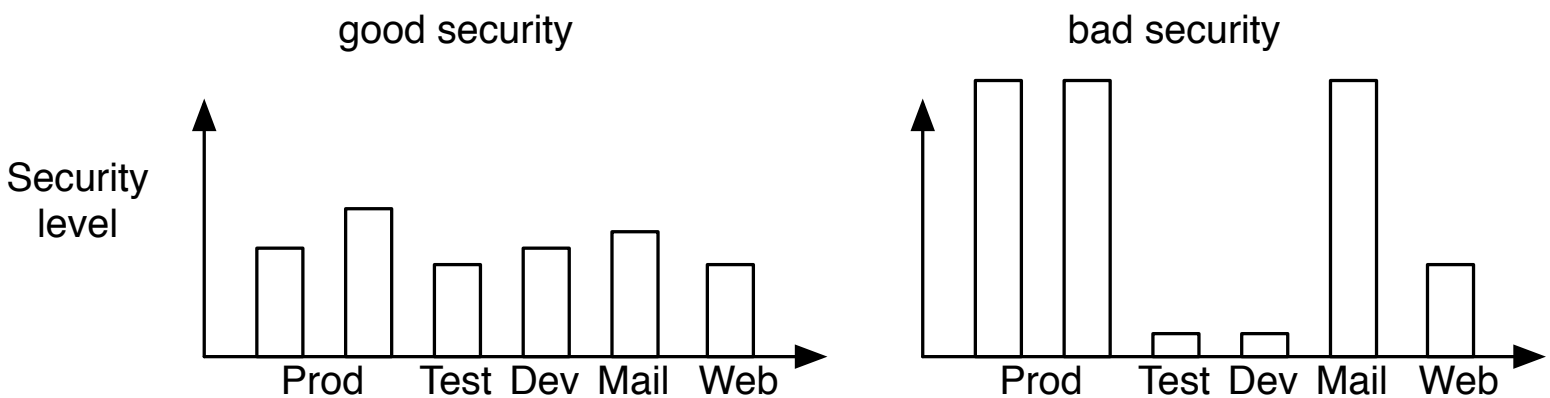
Policy and Mechanism

Definition 1-1. A *security policy* is a statement of what is, and what is not, allowed.

Definition 1-2. A *security mechanism* is a method, tool or procedure for enforcing a security policy.

Quote from Matt Bishop, Computer Security section 1.3

Balanced security



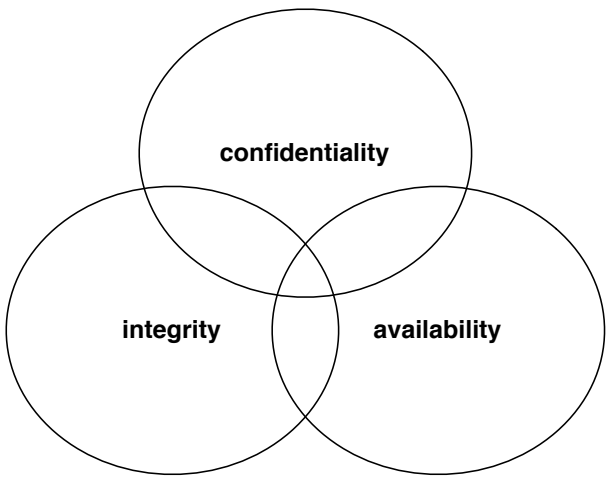
Better to have the same level of security

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

Confidentiality Integrity Availability



We want to protect something

Confidentiality - data kept secret

Integrity - no unauthorized changes to data

Availability - data and systems are available to authorized uses when they need them

Trusted Computing Base

Definition 20-6. A *trusted computing base* (TCB) consists of all protection mechanisms within a computer system – including hardware, firmware, and software – that are responsible for enforcing a security policy

Quote from Matt Bishop, Computer Security

Keeping this small, simple and understandable help keeping systems more secure.

Example the Qubes OS depend on few security-critical components:
https://www.qubes-os.org/doc/security-critical-code/

Intrusion Kill Chains

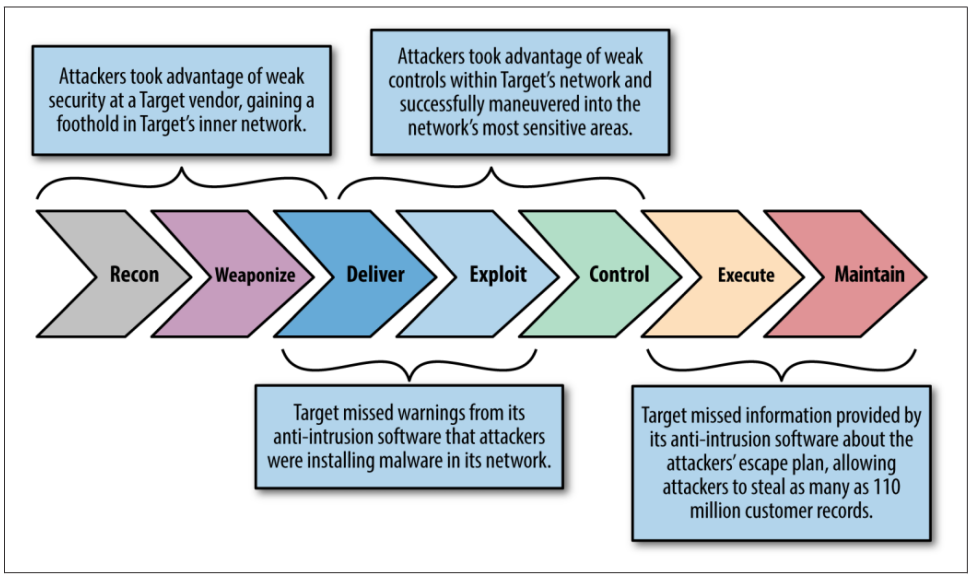


Figure 7-1. The kill chain

- See also *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Eric M. Hutchins , Michael J. Cloppert, Rohan M. Amin, Ph.D. Lockheed Martin Corporation, 2011

  https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Vulnerabilities - CVE

Common Vulnerabilities and Exposures (CVE):

- classification
- identification

When discovered each vuln gets a CVE ID

CVE maintained by MITRE - not-for-profit org for research and development in the USA.

National Vulnerability Database search for CVE.

Sources: http://cve.mitre.org/ og http://nvd.nist.gov

also checkout OWASP Top-10 http://www.owasp.org/

Local vs. remote exploits

Local vs. remote angiver om et exploit er rettet mod en sårbarhed lokalt på maskinen, eksempelvis opnå højere privilegier, eller beregnet til at udnytter sårbarheder over netværk

Remote root exploit - den type man frygter mest, idet det er et exploit program der når det afvikles giver angriberen fuld kontrol, root user er administrator på Unix, over netværket.

Zero-day exploits dem som ikke offentliggøres – dem som hackere holder for sig selv. Dag 0 henviser til at ingen kender til dem før de offentliggøres og ofte er der umiddelbart ingen rettelser til de sårbarheder

Separation of duty

> **Separation of duties** (SoD; also known as Segregation of Duties) is the concept of having more than one person required to complete a task. In business the separation by sharing of more than one individual in one single task is an internal control intended to prevent fraud and error.

Quote from https://en.wikipedia.org/wiki/Separation_of_duties

> **Separation of function**. Developers do not develop new programs on production systems because of the potential threat to production data.

Computer Security, Matt Bishop, 2019

Danish: Funktionsadskillelse

Lipners Integrity Matrix Model

	OBJECTS							
SUBJECTS	Production Data	Production Code	Develop. Code & Test Data	Develop. Sys. Prog.	S/W Tools	Sys. Prog.	Re-pair Code	Audit Data
System Mgr.	R	R	R	R	R	R	R	RW
Prod. User	RW	R				R		W
App'n. Prog.			RW		R	R		W
Sys. Program				RW	R	R		W
Sys. Control	RW	RW	RW	RW	RW	RW	RW	W
Repair	RW	R				R	R	W

Figure 12. Effects of Commercial Lattice Model with Integrity

Non-Discretionary Controls for Commercial Applications, Steven B. Lipner, IEEE Symposium on Security and Privacy, and Fifth Seminar on the DoD Computer Security Initiative, 1982

Mitre ATT&CK Framework

MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK™

- Source: https://attack.mitre.org/ Great resource for attack categorization
- examples of attack methods used by real actors
- Hint browse the ATT&CK 101 Blog Post https://medium.com/mitre-attack/att-ck-101-17074d3bc62

The dangers of logging in as the root user

> A huge advantage that Unix and Linux operating systems have over Windows is that Unix and Linux do a much better job of keeping privileged administrative accounts separated from normal user accounts. Indeed, one reason that older versions of Windows were so susceptible to security issues, such as drive-by virus infections, was the common practice of setting up user accounts with administrative privileges, without having the protection of the User Access Control (UAC) that's in newer versions of Windows.

Source: *Mastering Linux Security and Hardening* (MLSH), third edition

- Agreed, but I may be biased
- Mac OS X made it very simple to run administrative tasks, so you didn't need to run as root
- Modern Linux user interfaces make similar attempts with `pkexec`, `kdesudo`, `gksudo` etc.
- Windows is getting better, many organisations in DK are removing administrative access to regular users, even KEA

The advantages of using sudo

Used properly, the sudo utility can greatly enhance the security of your systems, and it can make an administrator's job much easier. With sudo , you can do the following:

- Assign certain users full administrative privileges, while assigning other users only the privi- leges they need to perform tasks that are directly related to their respective jobs.
- Allow users to perform administrative tasks by entering their own normal user passwords so that you don't have to distribute the root password to everybody and their brother.
- Make it harder for intruders to break into your systems. If you implement sudo and disable the root user account, would-be intruders won't know which account to attack because they won't know which one has admin privileges.
- Create sudo policies that you can deploy across an entire enterprise network, even if that network has a mix of Unix, BSD, and Linux machines.
- Improve your auditing capabilities because you'll be able to see what users are doing with their admin privileges.

Source: *Mastering Linux Security and Hardening* (MLSH), third edition

Why use Sudo conclusion

Main thing about sudo is that you do NOT give out the root password to anybody! They will use their own credentials and can be limited to single commands, scripts and even parameters. You could have a single sudoers file for your own organisation, that includes groups of servers, user groups etc.

Sidenote: sudo also has a number of CVEs unfortunately

Principle of Least Privilege

Definition 14-1 The *principle of least privilege* states that a subject should be given only those privileges that it needs in order to complete the task.

Also drop privileges when not needed anymore, relinquish rights immediately

Example, need to read a document - but not write.

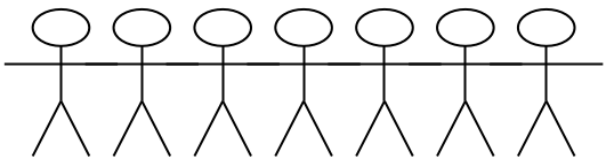
Database systems can often provide very fine grained access to data

Fokus on the basics

- User management - including administrative users
- Asset management
- Laptop security
- Penetration testing
- Firewalls and segmentation
- VPN everywhere
- TLS and VPN settings, encryption
- DNS and email security
- Syslog and monitorering
- Incident Response and response

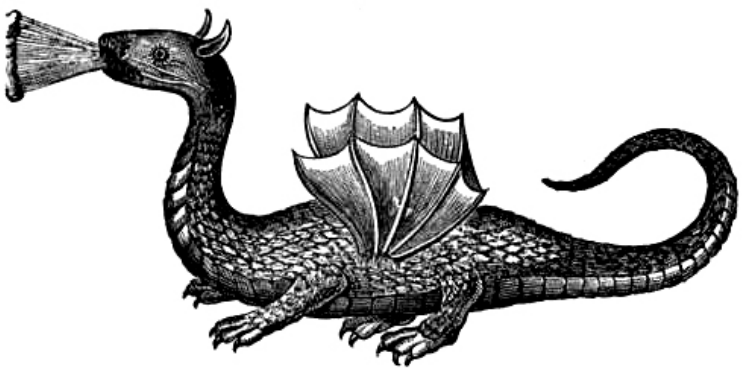
Vi skal allesammen hjælpe hinanden! Ovenstående er listen jeg giver studerende og virksomheder

Fokus: User management



- Relevant for alle organisationer
- Er måden vi sikrer godkendte brugere kan udføre opgaver
- Kodeord bruges til at forhindre uautoriseret adgang
- Har I styr på brugerid?
- Hvor er brugere oprettet?
- Hvor hurtigt kan I fjerne "een bruger"eller "deaktivere en bruger"alle steder!
- Er det et kludetæppe - ja, mange steder er det

Local administrator?

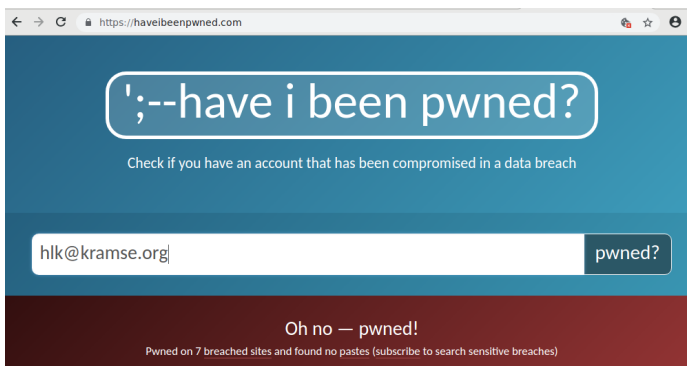


- Findes der systemer som er helt åbne, med lokal administrator
- Er det stadig nødvendigt
- Vi bør bruge Principle of Least privilege
- Vi ved hvordan, for det fortalte Jerome Saltzer og Michael Schroeder i deres 1975 artikel
  The Protection of Information in Computer Systems
  https://en.wikipedia.org/wiki/Saltzer_and_Schroeder%27s_design_principles

Passwords vælges ikke tilfældigt

Source: https://wpengine.com/unmasked/

Your data has already have been owned by criminals



Your data is already being sold, and resold on the Internet

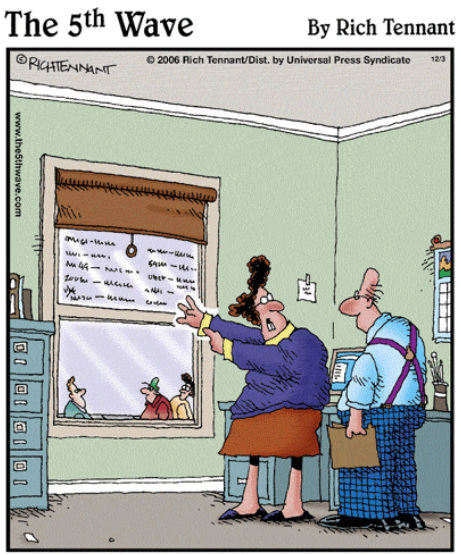
Stop reusing passwords, use a password safe to generate and remember

Check you own email addresses on https://haveibeenpwned.com/

They have an API you can integrate to avoid re-using already leaked passwords

https://www.troyhunt.com/introducing-306-million-freely-downloadable-pwned-passwords/

Opbevaring af passwords



"Don't be silly — of course my passwords are safe. I keep them written on my window, but then I pull the shade if anyone walks in the room."

- Use password managers! Available as cloud connected, local only, teams based
- You will have to investigate which one to choose, but find one!

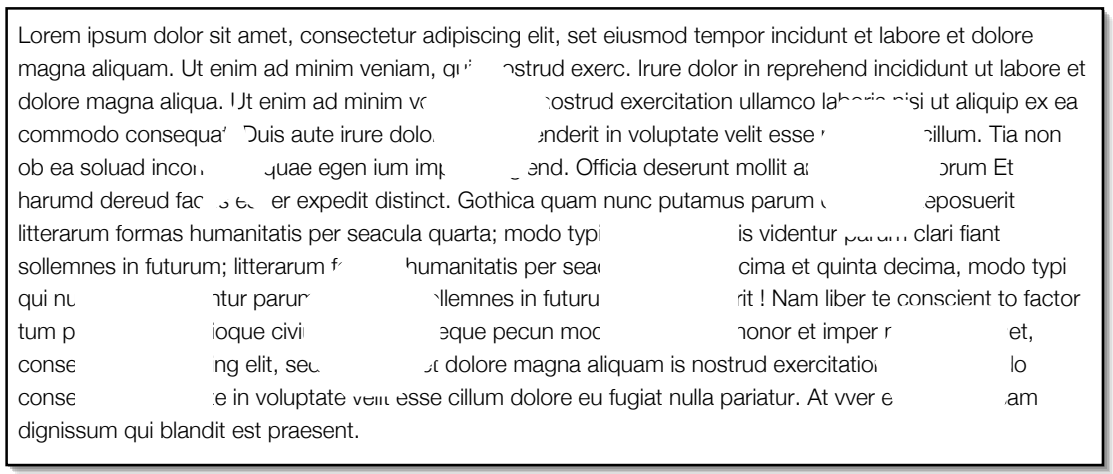
Fokus: Laptop sikkerhed

- Relevant for alle
- Hvordan sikrer vi at vi ikke mister værdierne, hardware og data typisk

Secure Laptops

- Laptops (og mobile enheder)
- Hvad kendetegner en laptop? og en telefon?
- Hardware naturligvis, en Macbook koster officielt mere end en brugt mellemklassebil
- - og husk brugen af laptops – de er dyre, men indholdet er ofte mere værd!
- Er laptops sikre, og hvad betyder det?

Are your data secure - data at rest



Stolen laptop, tablet, phone - can anybody read your data?

Do you trust ”remote wipe”

How do you in fact wipe data securely off devices, and SSDs?

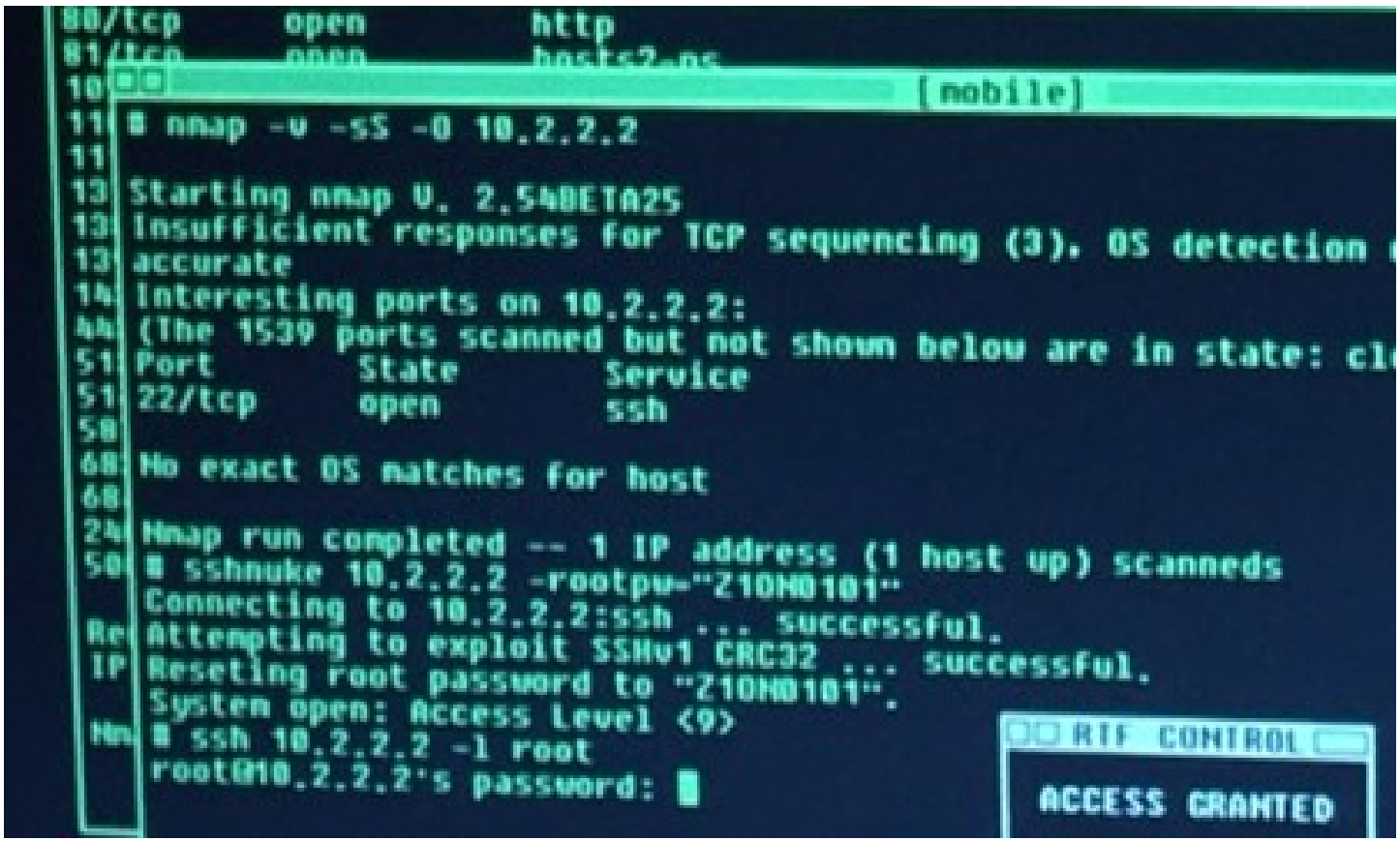
Encrypt disk and storage devices before using them in the first place!

Start Attacking from the Inside

- Now imagine you were in control of a company laptop
- Do you have a large internal world wide network?
  Having a large open network may cost you **1.9 billion DKK - ref Maersk case**
- Try scanning everything, start in a small corner, expand
- Scan all you danish segments, one by one, then the nordic, then the world
- Yes, things may break - FINE, BREAKING is GOOD

Better to break while we are ready to un-break

Nmap the world



Hackers work all the time trying to break stuff

Blue teams can use hackertools, and become more effecient:

- Nmap, Nping http://nmap.org
- Wireshark - http://www.wireshark.org/
- Aircrack-ng http://www.aircrack-ng.org/
- Metasploit Framework http://www.metasploit.com/
- Burpsuite http://portswigger.net/burp/
- Kali Linux http://www.kali.org

Most popular hacker tools https://tools.kali.org/ and http://sectools.org/

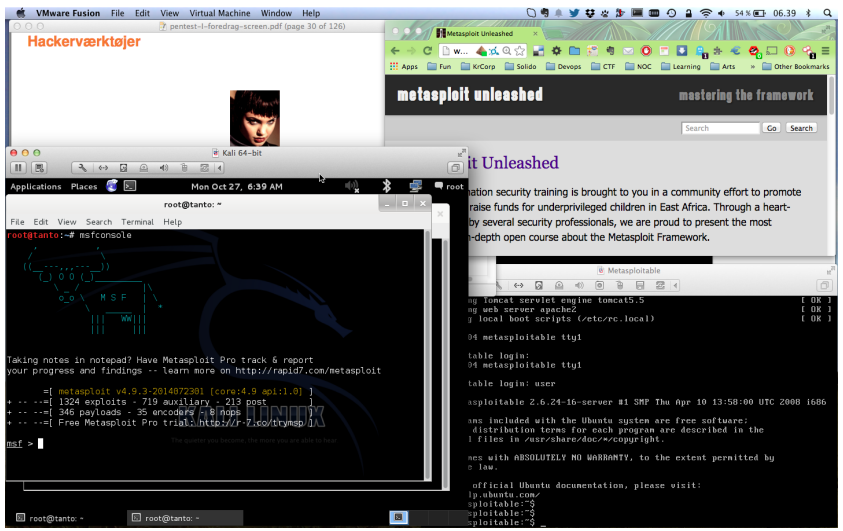
Kali Linux the pentest toolbox

Kali http://www.kali.org/

100.000s of videos on youtube alone, searching for kali and $TOOL

Also versions for Raspberry Pi, mobile and other small computers

Hackerlab setup

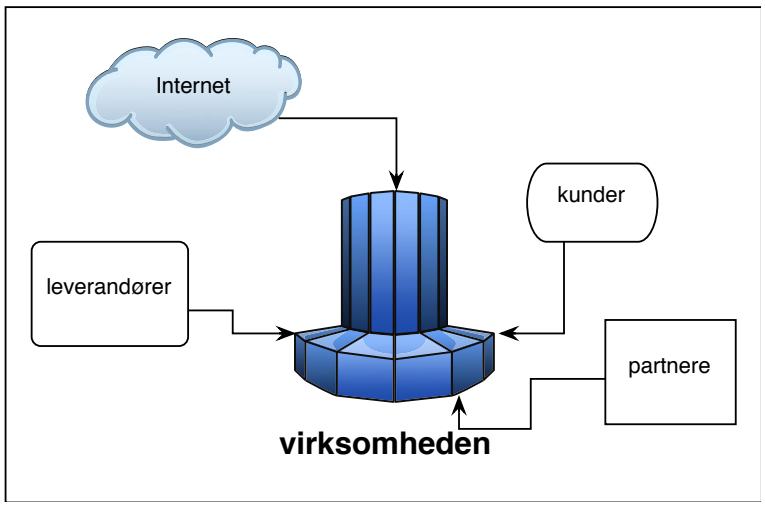


- Create hacker labs, encourage hacker labs!
- Software Host OS: Windows, Mac, Linux
- Virtualisation software: VMware, Virtual box, HyperV pick your poison
- Hackersoftware: Kali Virtual Machine https://www.kali.org/ ,

Hacking is not magic

- Hacking only requires some ninja training
- We have been doing this since 1995 when SATAN was released
- Listen, Plan, Act, Do hacking
- Be curious, and honest – let our students play with fire in special networks

Fokus: Firewalls og segmentering

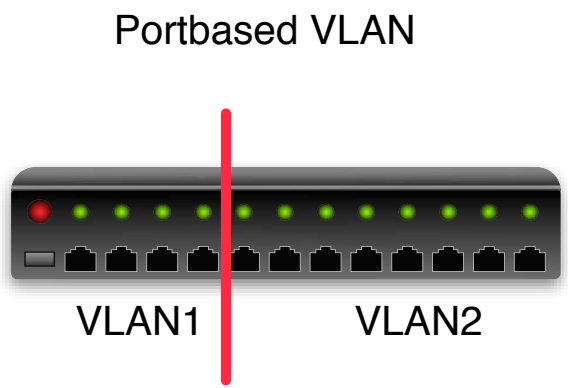


- Hvis du har et netværk, så bør du have en firewall
- En firewall tillader autoriseret trafik og blokerer resten
- Hvornår har du sidst set din løsning efter?
- Hvor lang tid tager det at se en 5.000 linier Cisco ASA config igennem?

Imagine Attacks from the Inside

- Now imagine you were in control of a company laptop
- Do you have a large internal world wide network?
  NotPetya cost Maersk about 1.9 billion DKK
- entry thought to be via software update of M.E.Doc [uk] an Ukrainian tax preparation program
- Attackers are very creative and have a large attack surface to most companies

Together with Firewalls - Virtual LAN (VLAN)



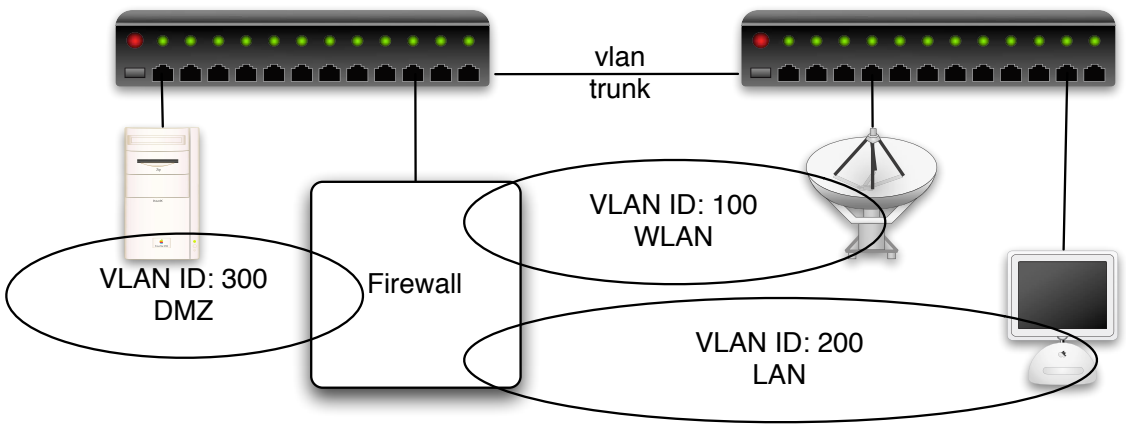
Managed switches often allow splitting into zones called virtual LANs

Most simple version is port based

Like putting ports 1-4 into one LAN and remaining in another LAN

Packets must traverse a router or firewall to cross between VLANs

Virtual LAN (VLAN) IEEE 802.1q



Using IEEE 802.1q VLAN tagging on Ethernet frames

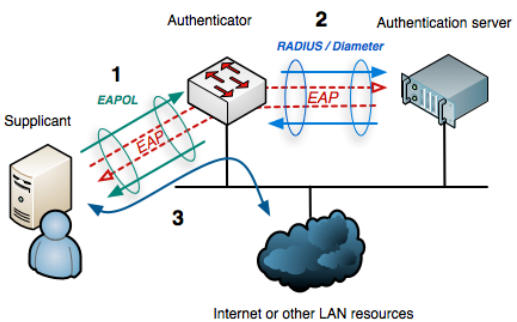
Virtual LAN, to pass from one to another, must use a router/firewall

Allows separation/segmentation and protects traffic from many security issues

Used in most, if not all, Wi-Fi networks – each SSID has a VLAN behind it

Network Access Control – Connecting clients more securely

Talking about standard, another useful one:
IEEE 802.1x – Port Based Network Access Control



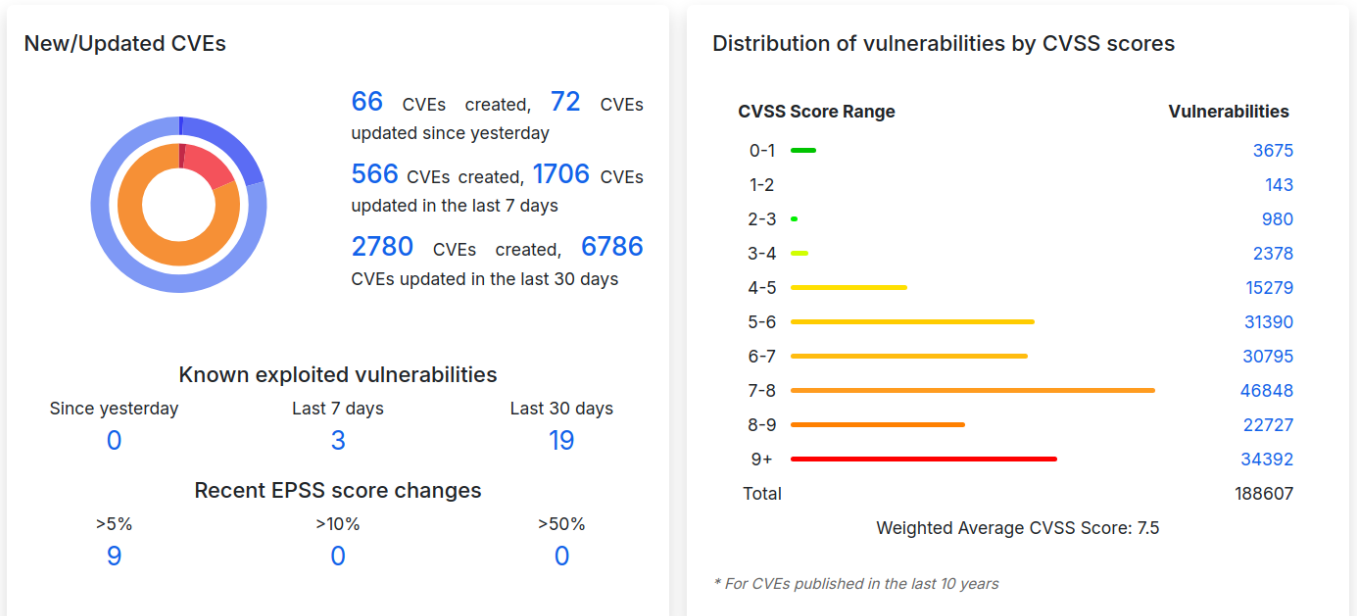
Authentication protocol ensures user validation before port access

Can authenticate using username and then password or certificate

Typically RADIUS and 802.1x which can use LDAP or Active Directory

Already used in Wi-Fi networks, so can be turned on for wired Ethernet ports

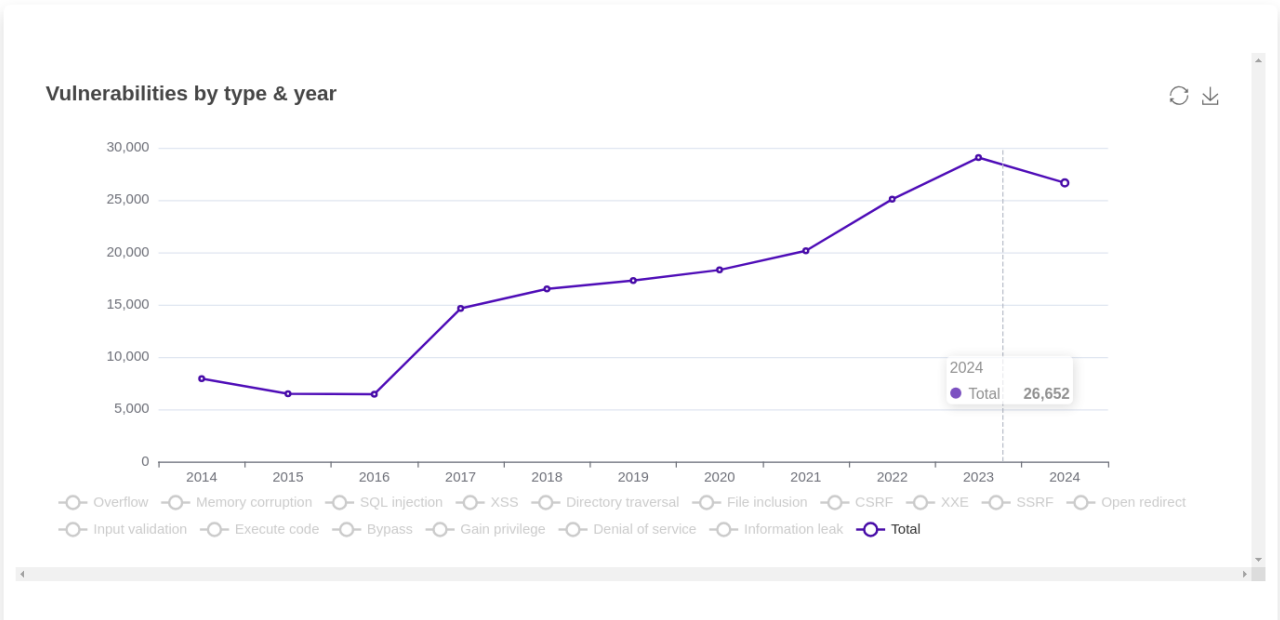
Vulnerabilities are everywhere!



Source: CVEdetails.com on 2024-09-02

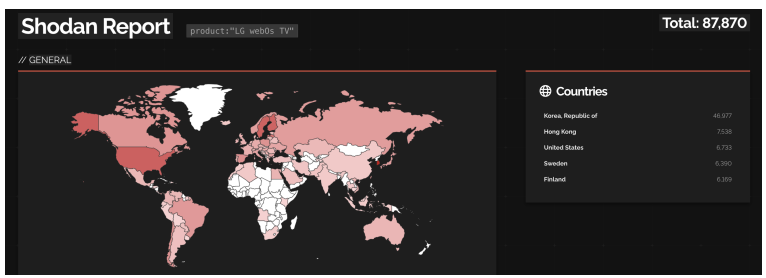
- This is crazy! https://www.cvedetails.com/

Vulnerabilitiesby type & year



Source: CVEdetails.com on 2024-09-02 Graph on the web site is interactive https://www.cvedetails.com/

LG TVs 2024 – CVE-2023-6317 up to CVE-2023-6320



90,000+ LG TVs Vulnerable to Authorization Attacks Due to WebOS Vulnerabilities

Bitdefender Labs has revealed a critical security flaw in over 90,000 LG smart TVs running the company's proprietary WebOS platform.

If exploited, the vulnerability could allow attackers to gain unauthorized access to the TV's functions and potentially the user's home network.

Source: https://cybersecuritynews.com/lg-tvs-vuauthorization-attacks/

D-Link NAS devices accessible via “backdoor” account CVE-2024-3273

92,000+ internet-facing D-Link NAS devices accessible via “backdoor”

A vulnerability (CVE-2024-3273) in four old D-Link NAS models could be exploited to compromise internet-facing devices, a threat researcher has found.

The existence of the flaw was confirmed by D-Link last week, and an exploit for opening an interactive shell has popped up on GitHub.

“The vulnerability lies within the `nas_sharing.cgi` uri, which is vulnerable due to two main issues: a backdoor facilitated by hardcoded credentials, and a command injection vulnerability via the system parameter,” says the discoverer, who goes by the online handle “netsecfish”.

The “backdoor” account has messagebus as the username and doesn’t require a password.

Source: https://www.helpnetsecurity.com/2024/04/08/cve-2024-3273/

XZ backdoor

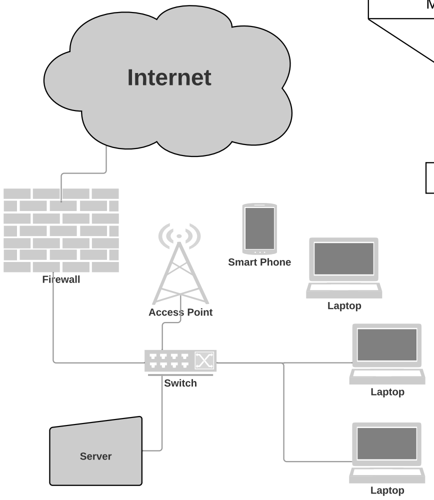
This month, only days ago it surfaced that someone injected backdoors into some software named XZ. *Inside the failed attempt to backdoor SSH globally — that got caught by chance*

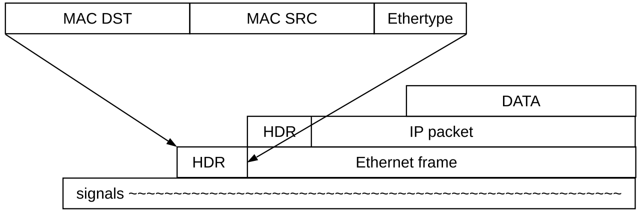
> What happened here is now well documented elsewhere, so I shall not recap it much, but essentially somebody appears to have hijacked the open source XZ project by social engineering the volunteer developer into handing over maintainer access after they cited some mental health issues, used the package XZ Utils to piggy back into systemd loading liblzma, which in turn loaded XZ, allowing sshd to be hooked to trojan it on Linux distributions that use systemd.
>
> The **trojan allows somebody a private key to hijack sshd to execute commands**, amongst other functions. It is highly advanced.

Source: https://doublepulsar.com/inside-the-failed-attempt-to-backdoor-ssh-globally-that-got-caught-by-chance-bbfe628

- Post by AndresFreundTec https://mastodon.social/@AndresFreundTec/112180083704606941

Protection, building secure and robust networks





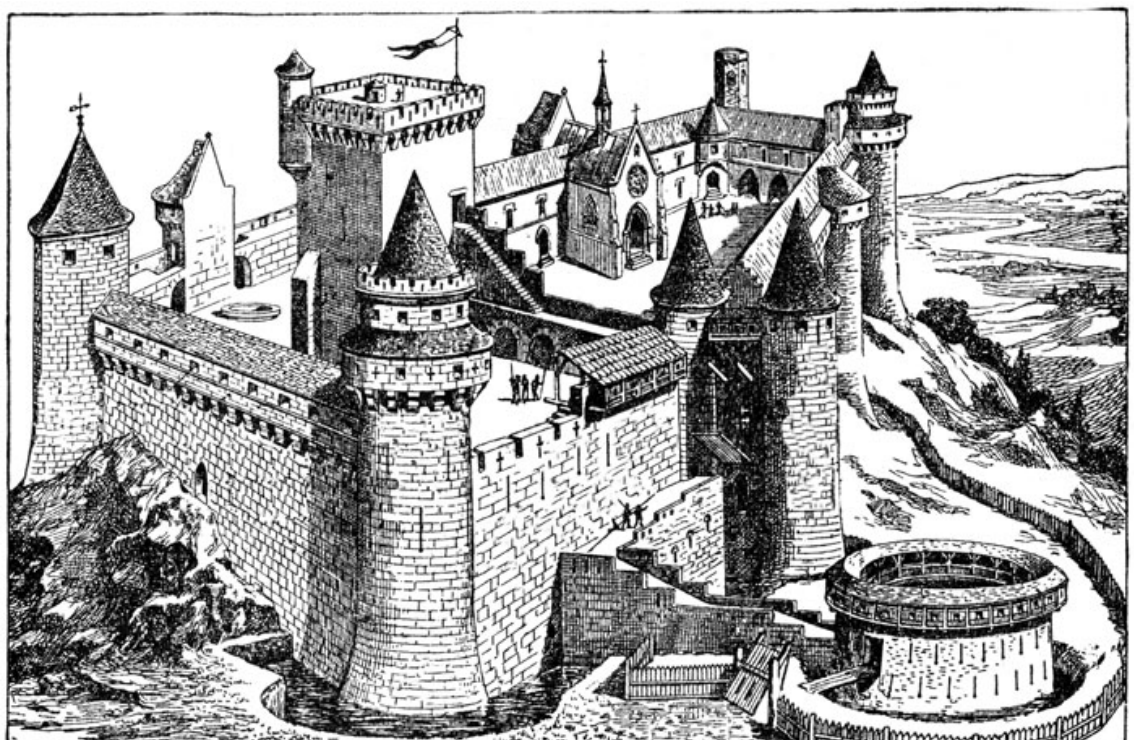
Ethernet frames contain packets

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Example Internet IPv4 Packet Header

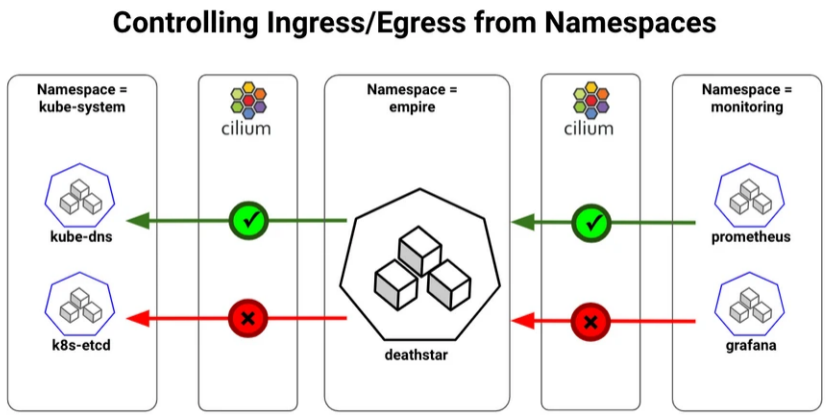
- We should prefer security mechanisms that does NOT require us to keep patching every month
- Can we change our networks to avoid this? Yes!

Defense in depth



Picture originally from: http://karenswhimsy.com/public-domain-images

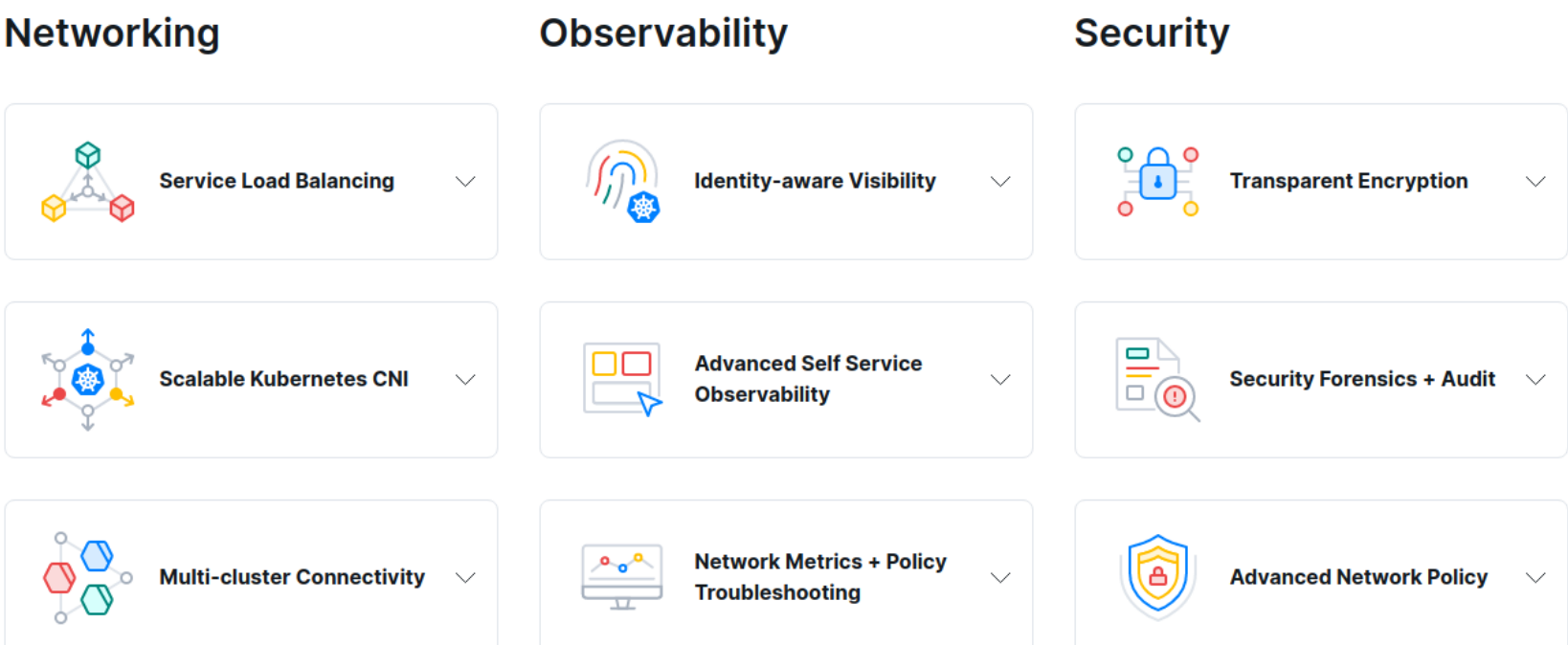
Cilium overview



Kubernetes provides Network Policies for controlling traffic going in and out of the pods. Cilium implements the Kubernetes Network Policies for L3/L4 level and extends with L7 policies for granular API-level security for common protocols such as HTTP, Kafka, gRPC, etc

Source: picture and text from https://cilium.io/blog/2018/09/19/kubernetes-network-policies/

Security is more than blocking!



- A lot of features relate to *security*

Fokus: VPN alle steder

- VPN er relevant for alle der har data af værdi
- Sikrer data der flyttes
- Virtual Private Network dækker over klienter der kobler op, og site-2-site

Fokus: DNS og email

- Vi er afhængige af email, modtagelse og afsendelse
- Når vi modtager skal det helst gå hurtigt
- Når vi sender skal vi ikke ende i spam mappen
- Phishing, hvem kan sende *fra vores domæne*

Various key attack types, clients and employees

- Phishing - sending fake emails, to collect credentials
- Spear phishing - targetted attacks
- Person in the middle - sniffing and changing data in transit
- Drive-by attacks - web pages infected with malware, often ad servers
- Malware transferred via USB or email
- Credential Stuffing, Password related, like re-use of password, see slide about being pwned

If we all wait a bit, and not click links immediately

Hackers try to create "urgency", click this or loose money

Storing query logs, old school or needed?

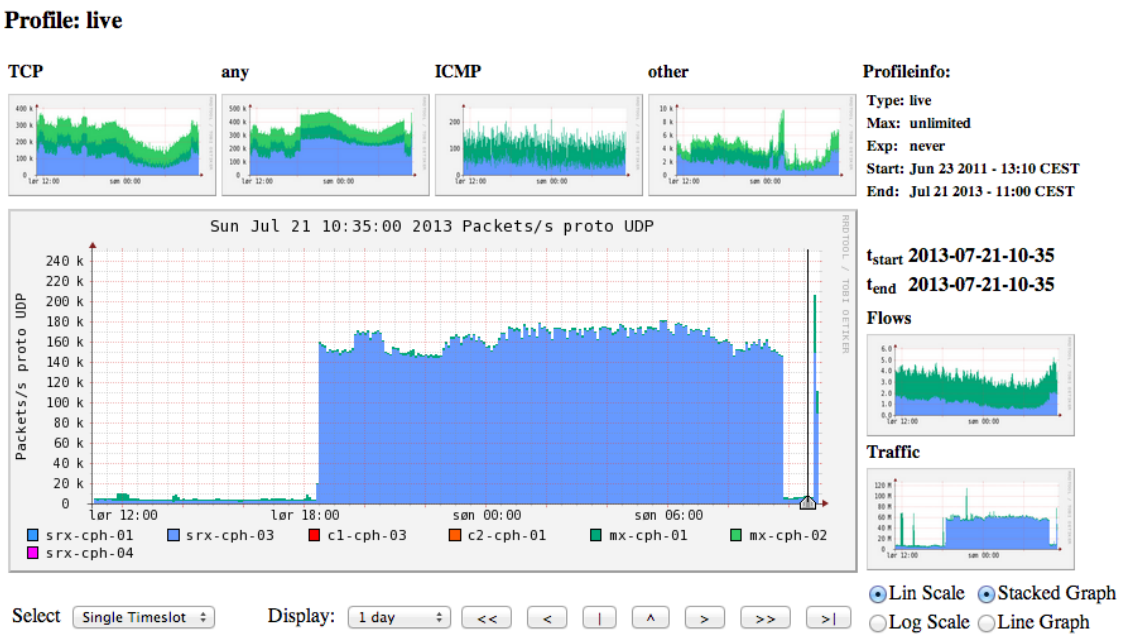
- policy/protocols/ssl/expiring-certs.bro
- policy/protocols/ssl/extract-certs-pem.bro
- policy/protocols/ssl/heartbleed.bro
- policy/protocols/ssl/known-certs.bro
- policy/protocols/ssl/log-hostcerts-only.bro
- policy/protocols/ssl/validate-certs.bro
- policy/protocols/ssl/validate-ocsp.bro
- policy/protocols/ssl/weak-keys.bro

- DNS query logs, keep it for at least a week?
  - with DSC and PacketQ https://github.com/DNS-OARC/PacketQ
- SSL/TLS log with Zeek/Suricata

  https://www.zeek.org/sphinx-git/script-reference/scripts.html
- Log with Elasticsearch?

  https://www.elastic.co/guide/en/elasticsearch/guide/current/index.html
- Uetisk? eller smart hvis man vil spore hvor malware kom ind
- **Vi må nok som medarbejdere acceptere mere logning, men selvfølgelig ikke som privatpersoner og borgere**

Network visibility: Netflow with NFSen



An extra 100k packets per second from this netflow source (source is a router)

Logging can show what happens/happened.

Fokus: Incident Response og reaktion

- Fortsat fra logningen ... hvad så nu!
- Hvis du har en sikkerhedshændelse skal den håndteres
- jo hurtigere og mere effektivt det håndteres jo bedre

Lifeguard training photo by Margarida CSilva on Unsplash

Øv krisesituationer

- Lav rollespil
- Lav tabletop exercises

Building Secure Infrastructures

A real-life setup of an infrastructure from scratch can be daunting!

You need:

- Policies
- Procedures
- Incident Response

Running systems which require

- Configurations
- Settings
- Supporting infrastructure – networks
- Supporting infrastructure – logging, dashboarding, monitoring

Building something *secure* is **hard work!**

Existing infrastructures

or even worse you inherited an infrastructure

Multiple networks, with different vendors, rules

Multiple generations of services, applications, technologies

Built over decades

Varying to no documentation

Organizational challenges

Ingrained culture – frozen in time

How do you get started improving security?

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

Risk management defined

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*

Center for Internet Security CIS Controls

The CIS ControlsTM 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

Center for Internet Security CIS Controls 7.1

- The five critical tenets of an effective cyber defense system as reflected in the CIS Controls are:
- **Offense informs defense:** Use knowledge of actual attacks that have compromised systems to provide the foundation to continually learn from these events to build effective, practical defenses. Include only those controls that can be shown to stop known real-world attacks.
- **Prioritization:** Invest first in Controls that will provide the greatest risk reduction and protection against the most dangerous threat actors and that can be feasibly implemented in your computing environment. The CIS Implementation Groups discussed below are a great place for organizations to start identifying relevant Sub-Controls.
- **Measurements and Metrics:** Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.
- **Continuous diagnostics and mitigation:** Carry out continuous measurement to test and validate the effectiveness of current security measures and to help drive the priority of next steps.
- **Automation:** Automate defenses so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the Controls and related metrics. Source: CIS-Controls-Version-7-1.pdf

Inventory and Control of Hardware Assets

CIS controls 1-6 are Basic, everyone must do them.

> 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

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.

Spørgsmål og mere debat

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