Welcome to

It-sikkerhedsupdate kort

2024

Henrik Kramselund he/him han/ham xhek@kea.dk @kramse

Slides are available as PDF, kramse@Codeberg https://codeberg.org/kramse/security-awareness-2024.tex in the repo security-courses

slides are available on Github

Goal for today

What are the things on the table for a responsible it-security strategy. Which subjects are most important, and what are the threats, if you dont get started immediately with the top 10 priorities.

- Plan:
- Approx 4h, with breaks
- Less presentation, more dialog
- Inspiration for solving the tasks, prioritizing the tasks
- I dont have tailer made solutions or easy answers for your organisation

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!

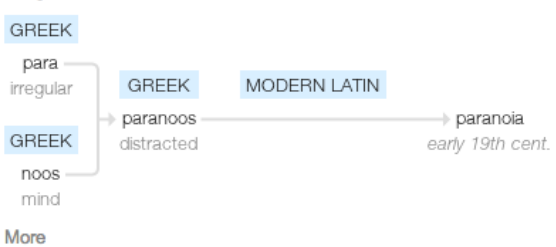
Paranoia defined

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



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, ...

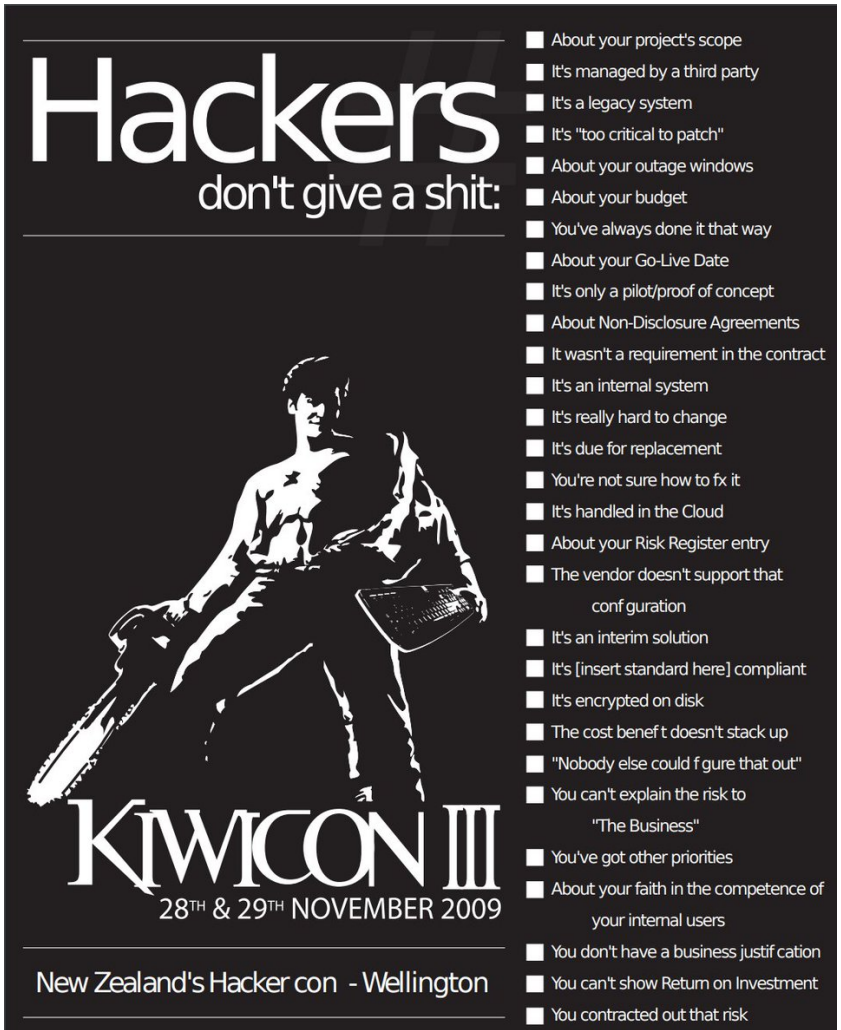
Your network is a research network, under construction, being phased out, ...

Try something new, go to your management

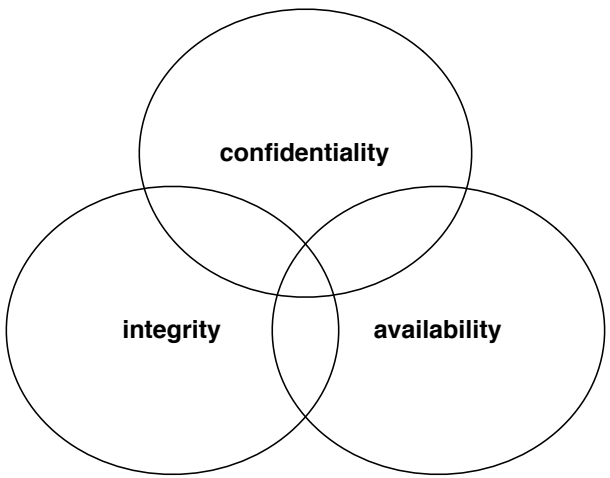
Bring all the exceptions, all of them, update the risk analysis figures - if this happens it is about 1mill DKK

Ask for permission to go full monty on your security

Think like attackers - don’t hold back



Confidentiality Integrity Availability



We want to protect something

Confidentiality - data kept secret

Integrity - no unauthorized changes to data

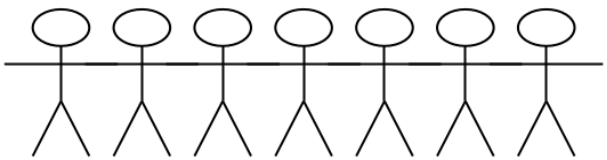
Availability - data and systems are available to authorized uses when they need them

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

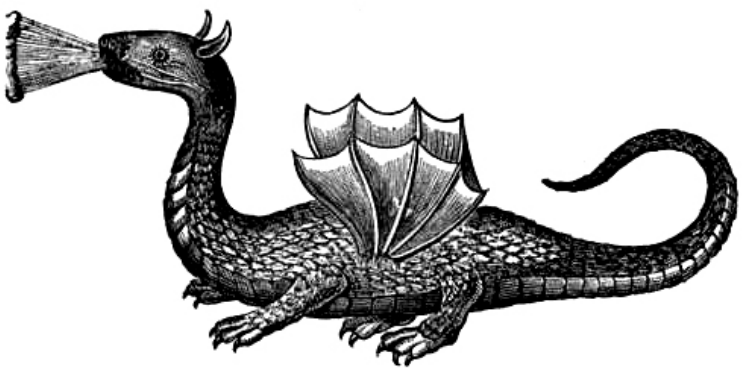
Vi skal allesammen hjælpe hinanden!

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?

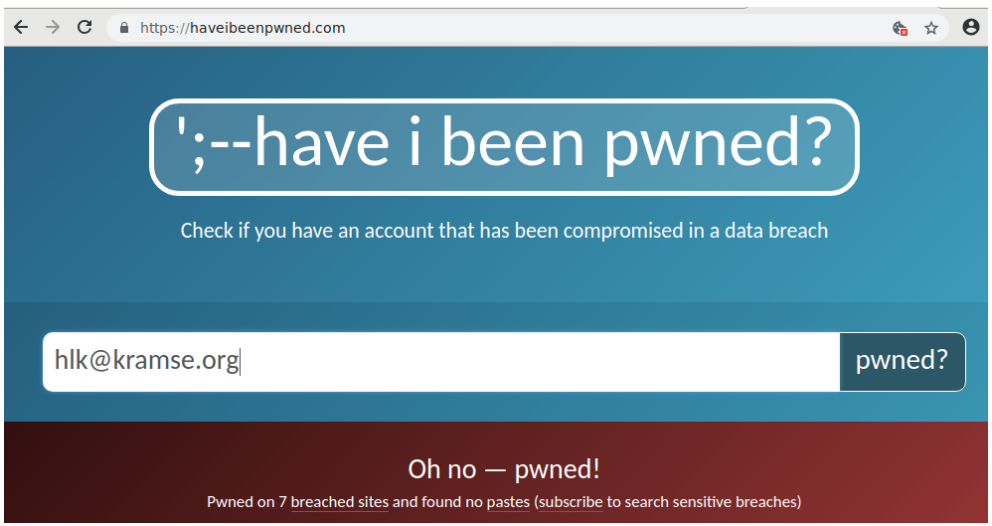


- Findes der systemer som er helt åbne, med lokal administrator
- Er det stadig nødvendigt
- Vi bør bruge Principle of Least privilege

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

Brug mere sikre passwords

Pwned Passwords overview

Pwned Passwords are more than half a billion passwords which have previously been exposed in data breaches. The service is detailed in the launch blog post then further expanded on with the release of version 2. The entire data set is both downloadable and searchable online via the Pwned Passwords page.

I kan forhindre brugere i at vælge passwords der ALLEREDE er lækket

I kan bruge deres API eller download

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!

- Software - licenser, indkøb, brug, opgraderingspriser
- Virtuelle maskiner - er en server et asset, eller er det data?
- IP adresser
- Data arkiver - GDPR

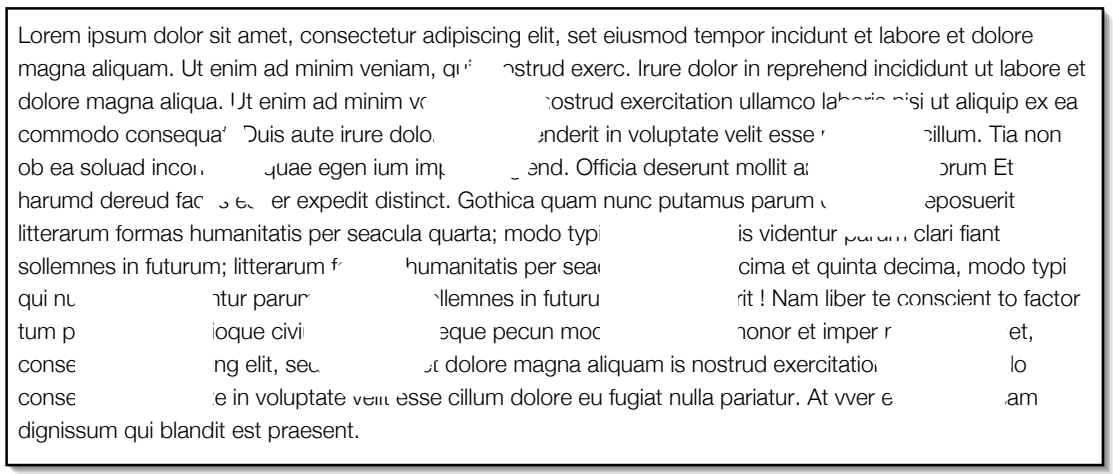
Fokus: Laptop sikkerhed

- 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!

Recommendations - Comply Everywhere, Act Anywhere

Laptop storage must be encrypted

Firewall must be enabled

Next suggestion:

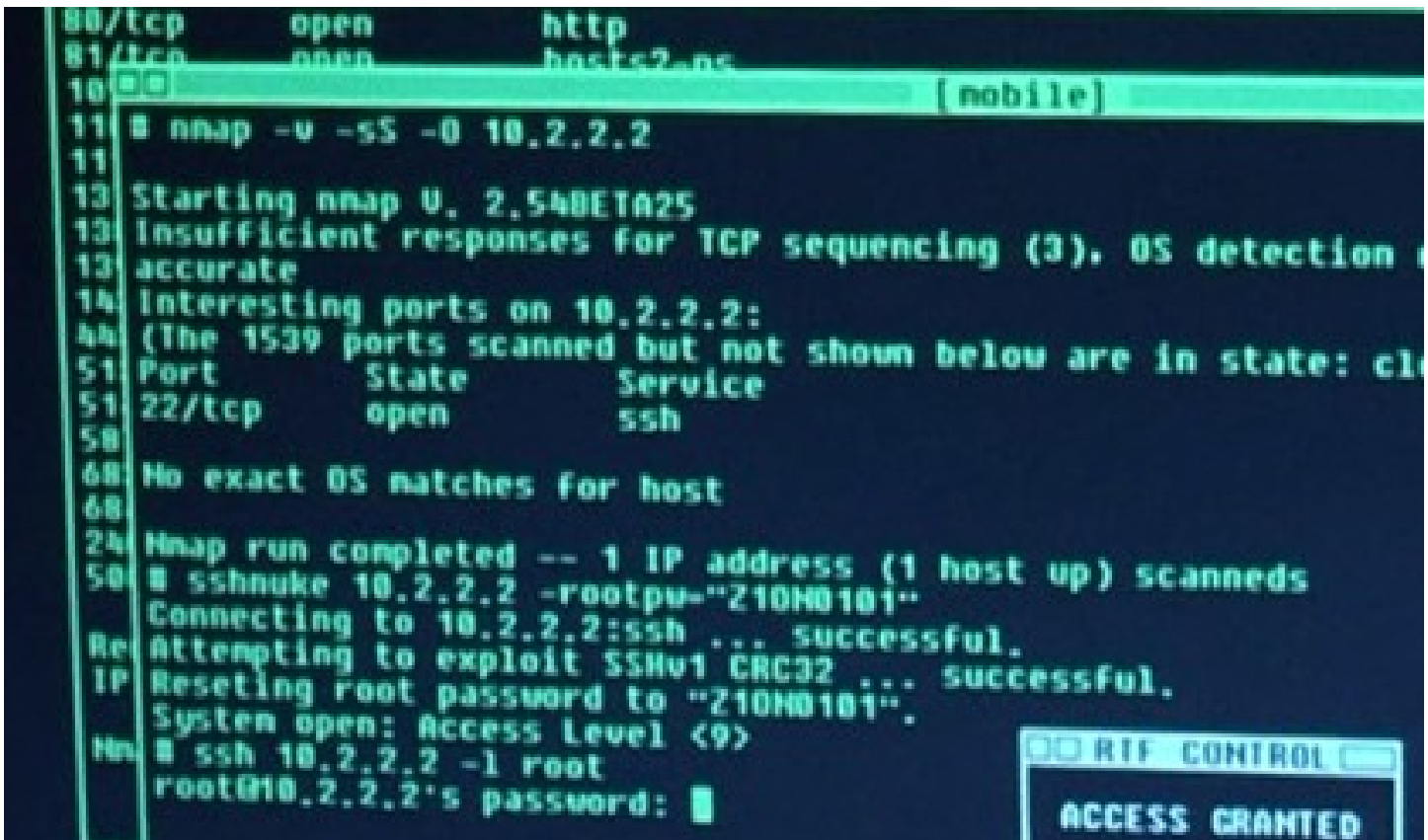
- Try sniffing data from a laptop, setup Access Point/Monitor port
- Portscan your laptop networks - use Nmap
- Write an email to everyone in your organisation:
  "Hi All, we need to identify laptops without full disk encryption
  - come see us, we have christmas cookies left, Best regards IT"

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



Hackertools are for everyone!

Hackers work all the time 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/

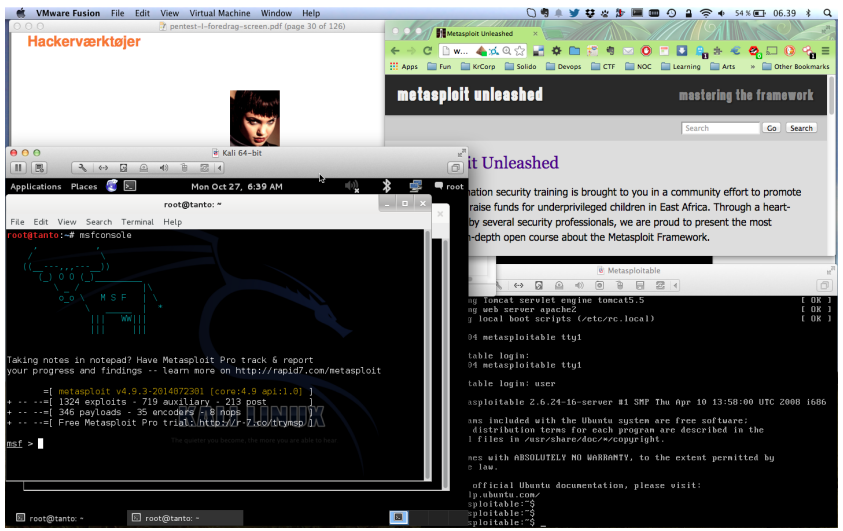
Kali Linux the pentest toolbox

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

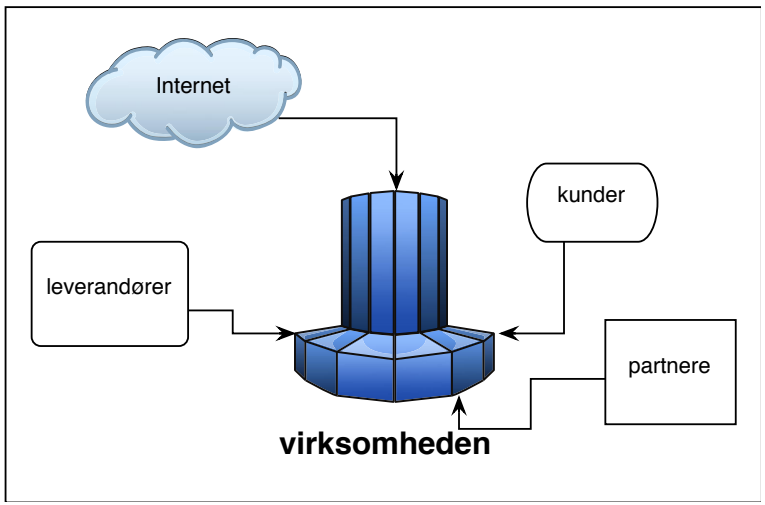


- Create hacker labs, encourage hacker labs!
- Software Host OS: Windows, Mac, Linux
- Virtualisation software: VMware, Virtual box, HyperV pick your poison
- Hackersoftware: Kali Virtual Machine https://www.kali.org/ ,

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

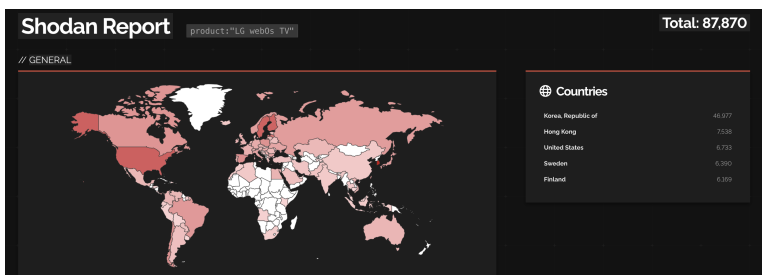


- Hvis du har et netværk, så bør du have en firewall
- En firewall tillader autoriseret trafik og blokerer resten
- Hvornår har du sidst set din løsning efter?
- Hvor lang tid tager det at se en 5.000 linier Cisco ASA config igennem?

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

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.

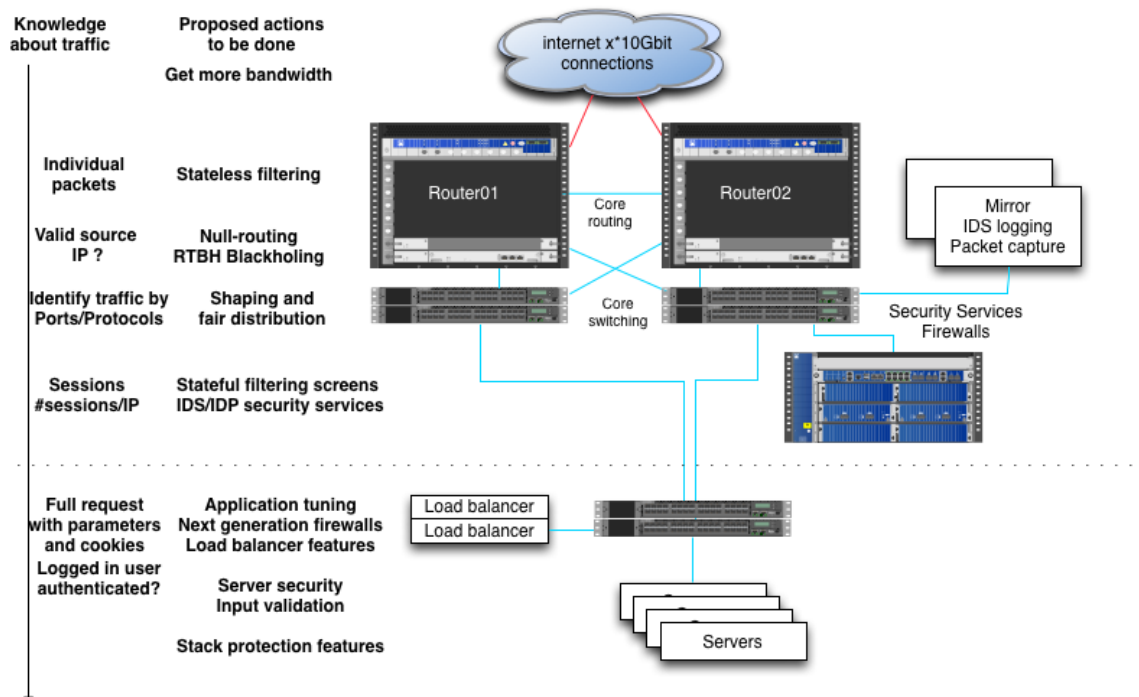
The existence of the flaw was confirmed by D-Link last week, and an exploit for opening an interactive shell has popped up on GitHub.

“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.

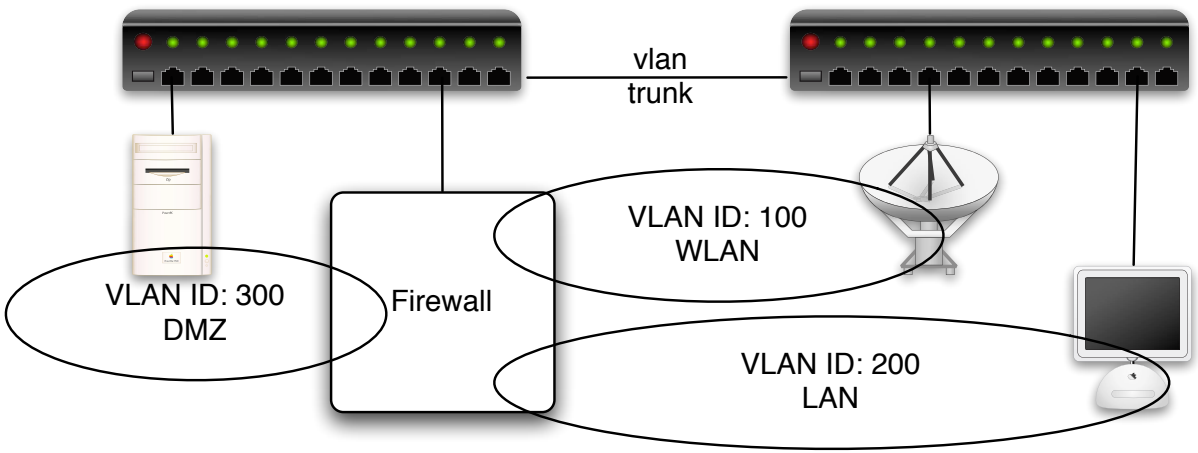
Source: https://www.helpnetsecurity.com/2024/04/08/cve-2024-3273/

Big firewalls



Big firewalls are not a single device

IEEE 802.1q VLANs

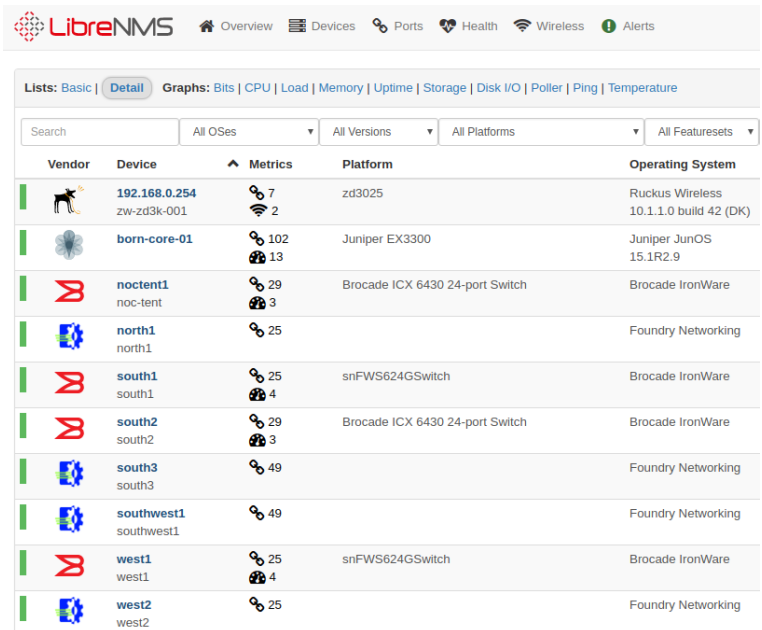


Med 802.1q tillades VLAN tagging på Ethernet niveau

Data skal omkring en firewall eller en router for at krydse fra VLAN1 til VLAN2

VLAN trunking giver mulighed for at dele VLANs ud på flere switches

Netværk generelt



- Måske også på tide lige at se om der er opdateringer til switche
- Jeg anbefaler LibreNMS https://www.librenms.org/

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

Indicators of Compromise and Signatures

An IOC is any piece of information that can be used to objectively describe a network intrusion, expressed in a platform-independent manner. This could include a simple indicator such as the IP address of a command and control (C2) server or a complex set of behaviors that indicate that a mail server is being used as a malicious SMTP relay.

When an IOC is taken and used in a platform-specific language or format, such as a Snort Rule or a Bro-formatted file, it becomes part of a signature. A signature can contain one or more IOCs.

Source: Applied Network Security Monitoring Collection, Detection, and Analysis, 2014 Chris Sanders

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

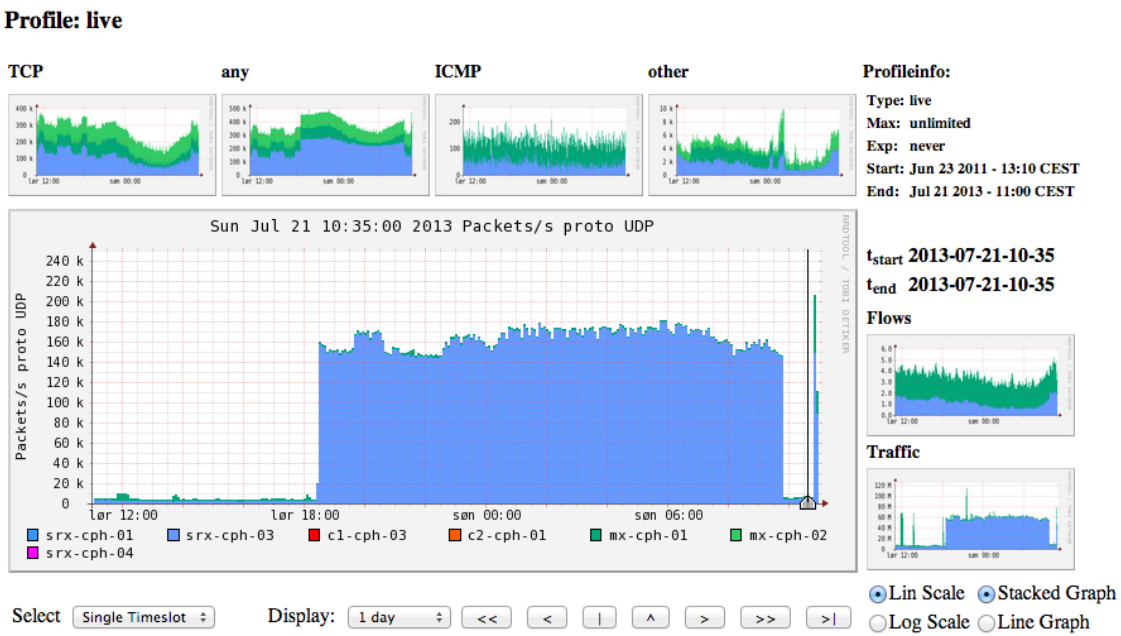
- DNS query logs, keep it for at least a week?
  - with DSC and PacketQ https://github.com/DNS-OARC/PacketQ
- SSL/TLS log with Bro/Suricata

  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

Network visibility: Netflow with NFSen



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

Also look into Elastiflow! https://github.com/robcowart/elastiflow

How to get started

How to get started searching for security events?

Collect basic data from your devices and networks

- Netflow data from routers
- Session data from firewalls
- Logging from applications: email, web, proxy systems

Centralize!

Process data

- Top 10: interesting due to high frequency, occurs often, brute-force attacks
- *ignore*
- Bottom 10: least-frequent messages are interesting

Case: Maltrail

Maltrail is a malicious traffic detection system, utilizing publicly available (black)lists containing malicious and/or generally suspicious trails, along with static trails compiled from various AV reports and custom user defined lists, where trail can be anything from domain name (e.g. `zvpprsensinaix.com` for Banjori malware), URL (e.g. `http://109.162.38.120/harsh02.exe` for known malicious executable), IP address (e.g. `185.130.5.231` for known attacker) or HTTP User-Agent header value (e.g. `sqlmap` for automatic SQL injection and database takeover tool). Also, it uses (optional) advanced heuristic mechanisms that can help in discovery of unknown threats (e.g. new malware).

https://github.com/stamparm/maltrail

Next steps for monitoring

In our network we are always improving things:

Suricata IDS http://www.openinfosecfoundation.org/
More graphs, with **automatic identification** of IPs under attack
Identification of **short sessions without data** - spoofed addresses
Alerting from **existing** devices
Dashboards with key measurements

Conclusion: Combine tools!

Logstash pipeline

```
input { stdin { } }
output {
  elasticsearch { host => localhost }
  stdout { codec => rubydebug }
}
```

- Logstash receives via **input**
- Processes with **filters** - grok
- Forward events with **output**
- Today many tools can produce JSON with fields already
- Elastic also have defined: Elastic Common Schema (ECS)
  https://www.elastic.co/guide/en/ecs/current/index.html

Logstash as SNMPtrap and syslog server

```
input {
  snmptrap {
    host => "0.0.0.0"
    type => "snmptrap"
    port => 1062
    community => "xxxxx"
  }
  tcp {
    port => 5000
    type => syslog
  }
  udp {
    port => 5000
    type => syslog
  }
}
```

- We run logstash on port 5000 - but use IPtables port forwarding

Maybe you have a device sending SNMP traps right now ...

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

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

Øv krisesituationer

- Lav rollespil
- Lav tabletop exercises

Spørgsmål og mere debat

Henrik Kramselund he/him han/ham

xhek@kea.dk @kramse