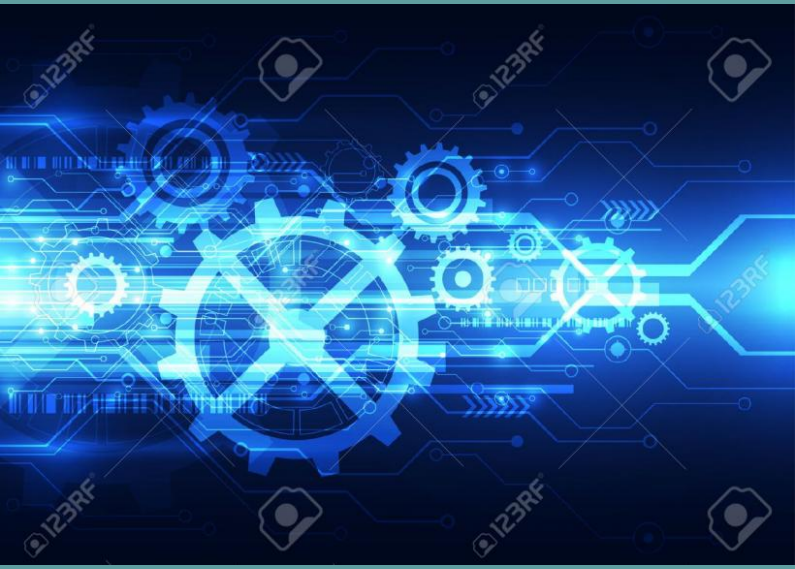
DFIR - Knowledge to stop bad things

Digital Forensics and Incident Response



Version 3

For use across the industry

Indhold

1. Velkommen til Defencia

Her kommer viden fra undervisningen i klassen

1.1 DFIR intro

* * *

1.1.1 Handle the attack and initiate DFIR

What do you do in case your company was exposed to a cyberattack? On this website, you will find inspiration, to handle and report the incident.

1.1.2 Lydfil

You can download the following as an audio file in 8:37 minutes

emergency handeling final (MP3, 7.90 MB) (Danish)

1.1.3 What is it ?

Here I will come up with my suggestions on how to prepare for an event.

(UPDATE - 29-01-2022 siden er lavet i punktform, det er ønsket at uddybe senere)

1.1.4 Where to start

Do you have no security in place at all. Then call a friend! I actually mean that 100% seriously. You probably would not start an expedition to Mt. At the top from day 1 without preparation, which you probably would not do without a few good pieces of advice.

Find out what you are most dependent on in your business. For example, it could be your website, without it there is no sale No matter what you have going on, make sure you get on with it. The [CIS controls] (https://www.cisecurity.org/) are a good place to start.

What you can learn here is how to do a risk assessment (based on CIS-RAM) and look at what controls they recommend. From there, you can start planning your protection.

My recommendation is that you look in the direction of the [CREST procurement guide] (https://www.crest-approved.org/wp-content/uploads/CSIR-Procurement-Guide-1.pdf) to deal with cyber attacks. This is because you need to have a very basic plan for what you want to do, whether your plans are in place or not. This is equivalent to investing in a fire blanket and a fire extinguisher, even if you have not set up escape plans and alarms.

1.1.5 What do you need to have ready (physically and practically)?

1. Overall IT Security Plan + What Users May and May Not *(Acceptable Use Policy)*
2. Event management for crashes and safety incidents. Define when it is an event and a security event?
3. Documents that contain telephone numbers and escalation schedule for incidents, so as to minimize doubts
4. Establishment of "War room" and who is on which items. War room is the meeting room where those who handle the situation are stationed. Here is an updated list outside the room recommendable, so there is no doubt about who to contact)
5. The data protection officer must be involved and informed in the event of personal data loss and keep in touch with [the Danish Data Protection Agency] (https://www.datatilsynet.dk/sikkerhedsbrud/anmeld-sikkerhedsbrud)
6. A room where all data including the information is collected (where only authorized personnel who have access, in case of insider threat)

In addition, a task distribution, so that there is someone who facilitates the practical. Food, drink and other necessities are often something you overlook and mean a lot to those who work hard. It may be necessary to have some that can run after missing items like Hard Drives, USB drives or the like if one is miss-

ing. Then technicians or managers should not let go of what they are working on and thereby waste valuable time.

1.1.6 Preparation of digital technologies

1. Computer hardware such as laptop, USB storage, Hard drives.
2. Software such as virtualization, screenshots, software for securing online data (OSINT tools). mm.
3. Jumpbag (See below)
4. Analysis lab for Malware, logs and network traffic etc.

1.1.7 Writeblock capabilities

In order to be able to secure correctly, it is important to be able to be write-protected correctly. So that you do not write data to the disk you are securing. This contaminates the evidence. Write protection can be achieved in several ways. Below are a few examples of how to achieve write protection for your task.

1.1.8 Software

Software write protection, it can see via a live boot image, such as caine or paladin. It is intended that the system is installed on a USB and thereby you can boot your PC from this USB and achieve write protection. It costs nothing to download and use.

Software write protection can also be achieved by software you install on your PC. An example of this is Safe block (Link here). Which, however, costs some money. It allows you to write-protect all the devices you connect to the system. Which means you have sata and USB in one function. It gets a little cheaper in purchasing, compared to hardware equipment.

The website digitalforensics.com has made a good list of equipment. [Read more here] (https://www.digitalforensics.com/blog/software-write-blockers-overview/)

1.1.9 Hardware

Hardware write protection is an electronic device that is inserted between the hard disk and the computer and thereby achieves write protection.

It is often a device that works via the USB port. It is quite simple to use and there is no speed reduction if you use USB 3.x

They can be used for all operating systems and secure via FTK (win 10) and DD (Linux / Mac). It is a one-time investment you have to make.

Below are 2 examples of write protection from Weibetech.

Weibetech has a function such as reading out the serial number and product name. Weibetech FUD 5.5 costs around 3,000 to 4,000 Danish kroner

The top of the pop here at the time of writing is Tableau from guidance software. It has made a line up of different solutions where adapter boxes can be connected with their own cable. The price is here on the friendly side of 8,000 Danish kroner. There are prices for every taste. It can be a good investment if one needs data secure media like hard drives. If you can make a combination of hardware and software so that you can perform different tasks, then you are better off.

Remember This is what suits YOUR task to be purchased for, you are building YOUR toolbox

1.1.10 Files for your inspiration to the prepreation

dfir 2022 (PDF, 98.66 KB)

trussel og haendelser (PDF, 111.46 KB)

dfir severity chart (DOCX, 11.17 KB)

dfir severity chart (PDF, 37.38 KB)

dfir escalation chart ark1 (PDF, 52.66 KB)

1.2 Important questions

Questions for incidents.

1.2.1 1.1 Important questions to ask during an attack.

It can provide important insights into how we can get out of trouble.

What have happened, what do we have of indicators?

1.2.2 1.1.1 What have the artefacts been used to / for?

- ➔ Have the files been run?
- ➔ How did they get in?
- ➔ With what input?
- ➔ With what output?
- ➔ Created as a service?
- ➔ Are they set to autorun? (Is autorun enabled or disabled?)
- ➔ Are the artifacts removed subsequently or are they freely available?
- ➔ Do we know what files do? (test on sandbox)

1.2.3 1.1.2 Who have used the files?

- ➔ local user, domain user, remote user?
- ➔ What are your Rights?
- ➔ Are there any domain admins at all?
- ➔ Who have run the files?
- ➔ Which user level did the files run on (admin, normal user?)

1.2.4 1.1.3 Where were the artefacts found?

- ➔ Shell bag, MRU, Event Logs, Services, MFT, NTFS?
- ➔ Memory?
- ➔ Data Streams?
- ➔ Where they payload from other connected IPs / URLs
- ➔ Path to File / Registry DB

1.2.5 1.1.4 When are artefacts from?

- ➔ What data layers are timestamps downloaded?
- ➔ Where are the remaining timestamps?
- ➔ Do we Trust the time stamps or are they obfuscated by malware.

1.2.6 1.1.5 What files have we selected and on what basis?

- ➔ How we have classified files as interesting?
- ➔ What is the filtration method is used?
- ➔ Which search criteria?
- ➔ What analysis methods?

1.3 Prepare

Content

1.3.1 Course and peripherals

My overall thought is that everyone should be able to get started with forensic and attack management without it having to cost the entire budget. At the very least, one must be able to make a Proof Of Concept (POC). Below is my bid on what to use.

Below are the needs / requirements that are set to be able to get started properly with Security Incident Respons, Malware analysis and Forensics. You can easily get to know software with small discontinued computers, and from there work your way up. If one needs to scale up or expand. There is a lot of software that is smart in licenses, so it might be very smart to just see what your needs are before you

If you need to work with this field professionally, it is recommended that you have access to some hardware that can do something and not just a discontinued PC. There may also be some licensed software.

Hardware requirements In order to be able to participate in the course, it can be my recommendation work on the topic is done on a stand alone machine. We work with malware that can infect the system, even if you take precautions.

The computer you use must be able to run virtualization software, which places demands on what hardware you have with you. However, most computers can run virtualization software.

1.3.1.1 Minimum PC requirements

I5 processor or equivalent 16 gb ram 250 gb or more hard drive and an SSD Some USB sticks (We are going to use forensics software, which requires a fast hard drive.) If you can find a computer with the above specifications, or above, things will run better and more "painlessly".

We aim in the teaching to be able to run 2 virtual systems, in addition to the installed operating system. If you do not do this, there will be a minor functionality that is lost. The example of what it looks like is shown on the board. There will also be instructions in setting up this, so that the student can continue working on, for example, a desktop computer elsewhere.

1.3.1.2 Peripheral accessories

You must have a USB stick of at least 16 gb and preferably a few. It is best if you have USB 3.0, as other smaller versions can present challenges from time to time.

This is for data collection and we need a bootable USB stick with Caine Linux or Paladin Linux (requires registration and possible donation)

The software we will use on the course will be open source and available for free.

Then some of my examples will use VMware, as there are some things that are a little better to use here. For example, the network setup.

Before the course day, you can easily prepare to download some software.

1.3.1.3 Forensics Software:

- ➔ FTK_Imager (free and requires registration) = https://accessdata.com/products-services/forensic-toolkit-ftk/ftkimager
- ➔ Autopsy (free) = https://www.autopsy.com/
- ➔ Caine linux (free) = https://www.caine-live.net/
- ➔ Rufus (free) = https://rufus.ie/
- ➔ Dumpit (free) = https://github.com/thimbleweed/All-In-USB/tree/master/utilities/DumpIt
- ➔ Magnet axiom ram capture (free and requires registration) = https://www.magnetforensics.com/resources/magnet-ram-capture/
- ➔ Virtualization Software
- ➔ Virtualbox (free) = https://www.virtualbox.org/

1.3.1.4 Images for virtual machines

Windows 7 and 10 (free / 90 day trial license for VMware and Virtualbox) = https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/

Remnux Linux (free) = https://remnux.org/

1.3.1.5 Log analysis

Splunk (free and requires registration) = https://www.splunk.com/

Netmon freemium (free and requires registration) = https://logrhythm.com/products/logrhythm-netmon-freemium/

Backup Image software (No requirement, nice to have) If something should go wrong, it is a good idea to have ongoing backups of your data. It will make a re-establishment easier

There are more options. I use terabytes for windows which cost a bit but are worth it all. Link = https://www.terabyteunlimited.com/image-for-windows.htm

1.3.1.6 Registrations

It is a good idea to have an alternative email to register software with. So you do not use your work email.

We will use software that requires registration, such as Splunk, FTK imager, VMware and Paladin

1.3.1.7 Network

At the school, a wireless network is set up which the students can use to go on when malware is used.

The network I bring with me is 2 options below (It is absolutely not a requirement as I set up equipment

for the purpose)

https://www.gl-inet.com/products/gl-ar150/

https://www.gl-inet.com/products/gl-ar750s/ (For information, both routers can be purchased at amazon.co.uk if you so desire.)

Both routers can connect to an existing network and from there make an encapsulation of the network we are working on. We connect to a VPN outside the school network. In this way, we minimize the risk of infecting our own network.

Should the above give rise to questions, you are welcome to contact the e-mail below

You can download a PDF here with what it requires.

SIR krav til udstyr (PDF, 134.93 KB)

1.3.2 emergency management

Under construction

You will gain more knowledge in how to handle bad situatiuons

1.3.2.1 Know your capabilities

One of the absolus most important aspects of getting started, is to know you capabilities. You have align expectations with management. Its important to know if there are capabilities that needs to be handled elsewhere, like fx forensics or malware reverse

engineering. These 2 examples requires special knowledge, and is somewhat expensive to maintain in a corporation. Therefore many might choose to hire in the specialists for these purposes.

You might want to start with creating a good description of the capabilities, there will be carreid out in the event of a incident. Even you might not have the above capabilities, but in most cases you might have the ability to create a triage. Triage is the introductory investegations, that is where you analyze for a set amount of time, ex 2-4 hours before passing on the assignment to 3´rd party. There is still alot of answers you are able to find, in this task.

1.3.2.2 Prepare for the worst

- ➔ What is the worst that can happen to your business
- ➔ Which systems have log data? (cloud services, network equipment, computers, websites, etc.)
- ➔ How can you collect such data? (If you report to the Police, they will ask for data that can "recreate" the scenario)
- ➔ How can you recover data? Do you have plans in place for backup? and do the plans and the backup work?
- ➔ What tools do you want in place? and where is it gathered?

These are just some of the questions you need to ask yourself. There are many scenarios that can happen

in a business. The most important thing is that you identify what is important to you so that you can risk assess your systems and protect them according to best practices.

1.3.2.3 Create an overview

- ➔ Define who does what in case something goes wrong. Is there a war room and a board with who is on the task?
- ➔ Who is responsible for the incident and who communicates what is happening?
- ➔ Distribute the responsibility to those who have to collect data and if it is a large company, share a data manager. So data is stored and described correctly and with time stamps.
- ➔ What data is compromised?

> *" Should authorities or the Police be contacted? & In that case, get them on board early in the process. There may be some good advice to pick up. Here you can ask for an IT outpost from NC3 (They are located in all police districts in Denmark))*

1.3.2.4 Collection of data

If you want to report the incident to the police? so you should be aware that they will probably ask what data you have that includes the incident? and how they can be shared with the authorities. Here it is important that you have a copy of the data seen in the statement, and describe them so that those who have to

look at the case know what they are looking at. Keep in mind that there are many different data sources, so describing what you can see in data is really important for those who need to analyze data.

1.3.2.5 Stop the attack

1.3.2.6 Analyze, Learn and use it

1.3.3 Jump-bag

In order to keep track of the pieces, it is a good idea to plan your pieces so that they can be used when needed. This reduces the time spent getting started.

1.3.3.1 The purpose

Mentioned before, then it is a good idea to assemble the pieces. Thereby, everything you need is only 1 place. The things in the bag are important components and must remain in the bag in peacetime, otherwise it loses its value right there when you need to use it. It also gathers all its documentation including contingency plans, contact information for vital partners, incident handling and management. It is important that it is written out, in case of crashes, attacks, or anything else that is to blame for things not working.

1.3.3.2 Content

The content is first and foremost what you need and there is no fact list here. I have written down something that I want in my bag.

- ➔ Pen and paper - probably the most overlooked and yet the most important. To be able to make notes and write times and who you talked to. I even use my SIR_checklist to make sure I have it all with me.
- ➔ Printed documentation of contingency plans, contact information for vital partners, Incident handling and management.
- ➔ Hard drives - preferably different sizes and with space if you need to make a data security.
- ➔ USB - USB keys can be a good thing if you need to have copies of data or pass on data. It's a cheap way to share data-bearing media.

- Tool set - a good tool set is indispensable so that equipment can be disassembled when needed. Some sets come with lids that can be used as a screw collector. (Tip - a small magnet can come in handy if there are few screws. IFixit sets have a lid that can be used for the purpose.
- Antistatic bracelet is also a good detail.
- A multitool, can come in handy in many respects.
- Headlamp - good working light is not out of the way.
- Write protection - USB with Caine Linux, Hardware or software write protection.
- Computer - preferably one with Linux, so it's easier to deal with malware. If necessary, have a computer with the company image so that you can test the latest virus definitions with the purchased Antivirus suite. Remember power supply!
- Water, something to eat about eg muslibar or similar. That with water and musli bar is not some crazy thing if you are going for several hours. (Before establishing "who does what" and managing the logistics for food, shift schedules and calls, etc.)
- Personal belongings like deodorant, toothbrush (It is not my invention, would have liked to have had it during some of the incidents I have participated in)
- Cables - Network cables, USB cables (USB A to mico-usb, USB C, etc.), USB to SATA, Adapter devices for SSD NVME / M.2 hard drives (Remember that there are several types)
- Card reader for several formats.
- Possibly a small network router and a switch. So a small separate network can be used. (gl inet rout-

ers are perfect for this purpose as they have VPN capacity as both server and client and thereby encapsulate the network)
- ➔ Camera is often overlooked. If you need to document something, then a picture can be really good to have as documentation. The camera can be standalone or from the phone. The latter is probably more valuable, as you often have control of the power in the phone than on a camera lying in a bag 😉

1.3.3.3 Things that may be worth considering

- ➔ Powerbank
- ➔ SD card as extra.
- ➔ Headphones from shielding you from noise in large room office
- ➔ USB drive with write protection option (such as kangaroo or netac). Can be used for several tasks.

1.3.3.4 Write protection

Write protection - write protection is the technology that ensures that no data is changed when securing equipment. This is probably the most vital of all equipment. Since it must be able to secure data in the right way.

1.3.3.5 Hardware write protection

This is a device that is put between data-bearing media and your computer. Often requires adapters and

many hardware write protectors can not be used for USB, so a software solution is cheaper.

1.3.3.6 Software write protection

Work the same way. Here you boot up on a USB medium and run a live image and or install software on your workstation. Then you can connect the devices you need.

The hardware components are more expensive, they cost from approx. 3,500.- D.kr. And up after.

The software costs from approx. 2,000.- D.kr. and up after, from proprietary solutions. Caine Linux does not cost anything and is quite good software for the purpose and gets the job done.

1.3.3.7 Computer

Having one or more computers is always a good idea. A computer with the company's Image and settings, as a kind of test. So if you need to test the defenses on a standard machine, then you have one at hand.

1.3.3.8 TIP:

It might be a good idea to ally with a supporter, for reinstallation of the above PC. In case of any accident / error.

Having a computer with Linux and maybe Kali Linux is a good idea. If you need a relatively secure environment to work with malware files. In this context, a Lin-

ux PC is perhaps a little more "immune" on a windows network. (Remember nothing is 100%)

1.3.3.9 Service wheel / maintenance

The above is not worth much if it is not updated or reviewed once in a while. It is really important that there is control over the bag and the documents that are in it. If it is not maintained and updated, then it is something that is going to take time. It is often time you do not have, or want to spend.

Previously where I worked, I sealed the bag with strips so I could see that no arrow fingers had been in the bag.

Make a list of the effects you want in your bag so it's easier to work with.

1.3.3.10 Assistive technology

As part of a contingency plan, it can be smart to have some tools that are deployable in case of attack. As ex velociraptor

A DFIR server for eg velociraptor from [velocidex] (https://github.com/Velocidex/velociraptor) (This is a thought to be tested. It might make sense to have a server where files could be downloaded from or uploaded via FTP / SFTP) so that there is collection on all artifacts in one place and in a closed environment.

1.3.4 Software

Here is a overview of the software that we take a closer look at. There may be replacements along the way so this may change at short notice.

1.3.4.1 Autopsy

Autopsy is for many better known as sleuthkit, which came to Linux many years ago. It is today developed for Windows as well, and work on several operating systems.

We use it in Windows, where it is a really good piece of developed software. Can do a lot of things and is fast. We look at what we can get out of Autopsy and how we use ingest modules, which are the functions you can use in the software.

License = Free open Source.

1.3.4.2 Autopsy Plugins

Here are a collection of the plugins that you can install on Autopsy. This wil give the tool extra leverage towards yor investegations.

Lunk to the Pluginsite on github

1.3.4.3 Vmware / Virtualbox

This is the virtualization software I / we use in class. For teaching, I use VMware as it has become my favorite software. That's why I thought it was a little more

rounded and more delicious to use. The compatibility works a little more smoothly here for me.

Virtualbox is quite nice and good software. It's free and easy to get started with if you need to virtualize your computers.

License VMware costs = $ 200 and a 50% discount is given on upgrading the version (at the time of writing) License = Virtualbox is free

1.3.4.4 Emeditor

Emeditor is a text editor that is unknown to most people I meet. It is a simple editor in many respects, which supports a lot of different code languages, searches and regex etc.

The reason I invested in this editor is that it can open text files up to 250 GB in size. It is an advantage once in a while if you are sitting in a Windows environment and have to look down in large files. You can also use powershell for this with high probability, but here I have the opportunity to look down in the files with an app and it is convenient.

License = $ 259 for a lifetime license or $ 40 annually in license.

A note: i use this on a personal license. I think the program is worth every penny. The software are updated on a regular basis. I am not sponsored to write this.

1.3.4.5 Splunk / SOF-ELK

SIEM (System Incident and Event Monitor) is monitoring, indexing of logs and events in the company. It is used in class to analyze logs and other log data.

Splunk is quick to install on a windows machine and get started analyzing logs. Since the software is predefined in what logs it can index. Splunk is free up to 500 MB per. day. Then it costs money. Do not know the prices at the time of writing, but rumors will say that it is not cheap software. For our needs, however, it costs nothing.

License = Unknown

SOF-ELK is made by Phil Hagen from SANS and is available to download for free. It has been developed over time and has many great features built into it. Can lots of functionality, but at the same time requires that you know Elastic Searc, Kibana and Logstash to customize logs. A little more convoluted. However, it must be said that common log formats are recognized and indexed.

License = Free

1.3.4.6 Linux

Linux does not require the big intro. If I have a laptop with Linux, or a virtual machine with Linux, then in many respects I have a multitool right there. Linux can do a lot with few funds and is free... .. Nuff said!

License = free

1.3.4.7 Simplemind pro

A simple tool for making mind maps, and clarifying thoughts and concepts. Can be used as a summary of topics. It is not a DFIR tool, but do not underestimate a mind map.

Proversion has slightly more options in terms of exports and designs

License = $ 28 for single license, lifetime license for Windows (Read more here)

1.3.4.8 Screenpresso

Underrated tool in many ways. The ability to record images, video and audio is often overlooked. It is an invaluable tool for the work when documenting what one is doing.

License = at the time of writing free, or $ 45 for a single license, one-time investment. (Read more here)

1.3.4.9 Windows

Windows does not require introduction either. It is an operating system like so many others. A standalone license can be purchased as an OEM

I get a trial license which works 90 days, which is fine for my purpose and has full functionality, like Windows 7, 8, 10. (The Edge program is here)

License = Volume license or OEM, which is set at 699.- Danish kroner.

1.3.4.10 FTK imager

We will use FTK imager, which is free. But is licensed to Access Data. We use the software to secure data with, for AD1, DD, E01 etc.

FTK can assist you in the aquisition of data from media such at SD cards, Harddrives and other hardware (Plrase be adviced that media such as USB might require a seperate writeblocker, like those for SATA drives).

1.3.4.11 DD / DC3 DD / DCFL DD

The little tool for linux that can be used to secure data with. Is quite efficient and easy to use. It does exactly what you ask. There are several versions of the same program, which are customized with some extra features like HASHing and progress bar, etc.

```
DF -ls (Show mounted disks)

dd if=/dev/urandom of=/dev/null status=progress (defines DD
is used, IF = indput file og OF= Output File )
```

1.3.4.12 Note programs

A good system for storing notes is important. You can not remember everything, so it is important to have a

place where your notes are available. There are many different programs for it. Some free others cost money. I can recommend Standard Notes, which is a note program that works really well for me. It's not perfect, but has the features I'm looking for, namely security, easy to use, synchronized across platforms and just work. Then the program uses strong encryption (See their article)

License = free or purchase extra features for approx. $ 99 for a 5 year plan.

1.3.4.13 HASHtool for filhash

One of the most important things in the subject is to be able to demonstrate file integrity. So therefore it is also good to have a program that can calculate HASH values next to files and text. Linux and Mac have it built-in as features in the Terminal (such as md5sum filename.txt)

For windows, there are HASHtools which are located in the path finder, so you can calculate the hash value simply by right-clicking.

We have seen Dirhash for recursivly calculate the HASH values

Link to the software DirHash

Below is an example

```
    Calculate
    DirHash.exe C:\Users\testuser\Downloads\test -
sumRelativePath -sum sha256 -progress -t test

    Verify
    DirHash.exe C:\Users\testuser\Downloads\test SHA256 -
verify test
```

1.3.4.14 Wireshark

Wireshark is without a doubt one of the programs that comes in handy. It's easy to make a .PCAP file and then analyze it. The analysis part can wireshark too, albeit a bit cumbersome, since requires you know a lot of filters. There are also programs that can help with this, such as network mines, netmon freemium, tshark (Part of wireshark). There are probably many other great tools out there.

The most important thing is that we can make a network recording for our machines and exercises and then try to analyze it afterwards.

1.3.4.15 Cyberchef

One of the newer shots at the tribe is Cyberchef (Github). It is a program developed by GCHQ in England. It is a small tool that can edit, search convert and everything else. It is for small amounts of data and large amounts of data. It is a small app that works offline in a browser.

It is definitely worth taking a look at.

License = free

1.3.4.16 Python framework

Python is a code language that you should have installed if you are working with the above. As there are many small tools or you can develop them yourself

License = free

1.3.4.17 KAPE

KAPE is one of the tools that has been developed to know a lot. It can generally collect and analyze data, based on the modules you use pre-installed or even installed.

The tool is used for collecting data in a triage, and then parse the content afterwards. Like MFT, Prefetch files, logs and more. Takes the bulk out of the datacollection and can be extended with your own scripts.

License = free for private and costs a license for commercial use.

1.3.4.18 Flare VM

Flare VM is the collection of tools we use for our malware analysis. The system is based on Windows.

In class I do an intro and there is a video showing the installation (Requires login to the guide on the page)

License = free

1.3.4.19 Remnux

Remnux is the Linux based malware analysis platform which is also used in class.

License = free

Note to analyze Pcaps

```
tshark -q -r trickster.pcap -T fields -e dns.qry.name
The list is unsorted

 > dns.txt
saves the file in dns.txt

cat dns.txt | sort
Filters what is the domains

cat dns.txt | sort | uniq
Sorts uniques
```

1.3.4.20 Nmap

Should probably also be mentioned here. It is an indispensable tool in the event of incidents. If malicious actors have put equipment on your network. Then being able to scan your network for devices can be an important step. Of course, this requires that you know your units (assets) in advance and have a list of

them. (as recommended in the CIS controls and ISo27001)

Nmap is also available for Windows and can be installed via the terminal on unix based systems. (ex sudo apt-get install nmap)

License = free / Open source

1.3.4.21 Velociraptor

One of the tools that I play around with a bit is the velociraptor. It is a small agent that can be installed on all devices during a security attack.

The agent can be accessed securely via a console, on the server you define. From there, you can query down on the individual machines or to the entire network. You can scan for artifacts and ex Yara rules. The client is an inherited species of GRR developed by Google and Michael Cohen (who created Velociraptor)

The application is quite smartly made. You have an installation file and from there the program creates a server yaml and a client yaml file. Which can be sent to clients with client yaml. Then the installation file will act as a client or server. Server yaml should only be located 1 place.

The clients have via the yaml file, a secure connection via SSH access to secure communication between client and server. Which means that in theory you can install the application on a VPS (Virtual Private Server) and query your clients over the Internet.

The purpose is to create transparency in its perhaps compromised network.

Read more here on medium

License = Free and Open source

1.3.4.22 Volatility

Volatility Analysis of memory is also one of the areas we are going to look at. Since the memory in a system can contain information about malware etc.

We'll look at what the difference is between version 2 and 3.

Volatility fingers with the Velociraptor and KAPE programs

License = free and open source.

Note to volatiltiy Only for analyzing the file

Reference volatility https://github.com/volatilityfoundation/volatility/wiki/Command-Reference (Info om profiler vol.exe --info | more)

Make a dumpfile from dumpit, FTK, magnet ramdump Remember the output is the same as the amount of RAM.

Volatility 2.6 examples Image info volatility-2.X.standalone.exe pslist -f Filnavn.dmp imageinfo Processliste volatility-2.X.standalone.exe pslist -f

Filnavn.dmp(eller raw, mem, wmem) --profile=Win10x64 volatility-2.5.standalone.exe pslist -f Filnavn.mem --profile=Win10x64 dumps/ (Netscan) volatility-2.5.standalone.exe netscan -f Filnavn.mem --profile=Win10x64

Volatility3 example

vol.py -f "I:\TEMP\DESKTOP-1090PRO-20200708-114621.dmp" windows.psscan.PsScan (Shows the proceses running)

For more see this cheatsheet or press vol.py -h for help

volatility 3 cheatsheet (PDF, 161.55 KB)

1.4 Detect

The detection in this section, is not you EDR, Anti-malware solutions, IDS, IPS or similar. This is dedicated the tools to identify the unknown.

1.4.1 Loki

Loki is a tool for detecting Yara and HASH values, that you have discovered in handling an incident.

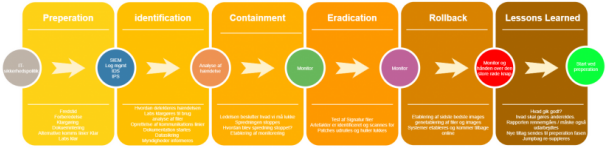
Link to the tool

1.4.1.1 What the tool can do

Quite simple, you can run the tool on a cmd and scan the files or folders, with the known hashes and yara

rules that you can create or pull from the repository.

1.5 The phases



1 *Faserne*

The phases are the periods you as a company have to go through to handle an attack. Here you get the outline of the phases based on my own experience (and the textbook's). You can access a more detailed area if you are in the class

1.5.1 Preparation

Peace time where you prepare all the activities and tools (both software and hardware) before something goes wrong. here you will also have control of all the documents to be used during an attack. These are the plans, processes and procedure that come out of an Incident.

Here we talk about the link to governance, IT security policy, IT contingency plan, IT crash plans and IT attack management

1.5.2 Identification and analysis phase (Identification)

This phase is when something goes wrong. It escalates to the type of incident, whether it is safety related or common crashes.

When the plan is activated, it is based on an assessment that it is security related.

It must start with data collection and identification of what has happened and how it has come in. The behavior of the malicious files must be analyzed. What they do of new malicious actions and what domains IP addresses they contact.

1.5.3 Lockdown (Containment)

When we have become wiser about how we are affected and what has happened. Then we can start looking at how we utilize our knowledge to block the attack. Of course, this requires that we have some tools / technologies to assist us with the shutdown.

A few examples.

If we know domains and IP addresses, they can be blocked in eg DNS, Firewall, Proxy etc. If we know files that are created, then they can be blocked in the anti-malware solution on end points, servers, IPS etc. If we know the HASH of the files, then they can be detected by a scan. If we know the characteristics, then we can create YARA rules, which give an alarm when we see

patterns. (alarm only) If we know the spread, we can, for example, close shared drives

These are some of the examples of detection and blocking. It can vary from incident to incident.

If you find out that something was missing to analyze, or new data has been added. This does not prevent you from going back and doing a new analysis of the malware or artifact.

1.5.4 Recovery (Rollback / Restore)

Once we have stopped the attack, it is important for us to be able to find out when "day zero" was. That is, the separate date where we can identify when the incident took place and we can recreate from before this date / time

1.5.5 Monitor phase

If you have an attack that has been more extensive, you can implement a monitor phase.

It can be a few days up to weeks and months where you intensify your monitoring. If something happens, you can press the "big red button" and lock your environment down again, so you inhibit a possible re-infection.

1.5.6 Back to normal (Post incident / Lessons Learned)

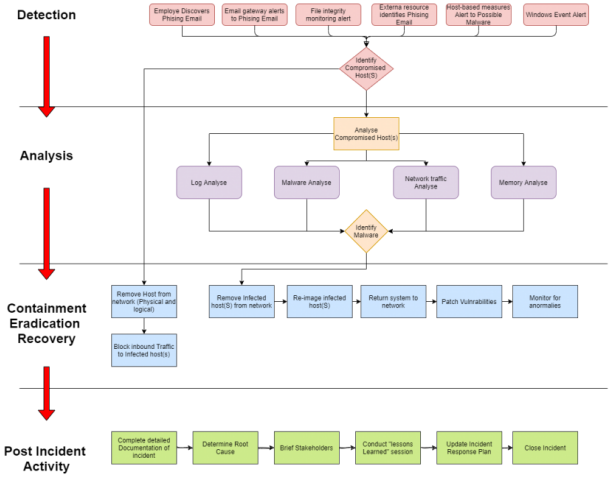
Here we start normal operation and end the process / phases themselves.

We gather for a meeting where you turn what went well or badly. Get the air cleaned if it got a little hectic. What we learned is collected and from there a report is prepared as a summary of what we learned and how it is introduced in the plans we have.

So we have an updated "Business Continual Plan" which gives the company "Continual Service Improvement"

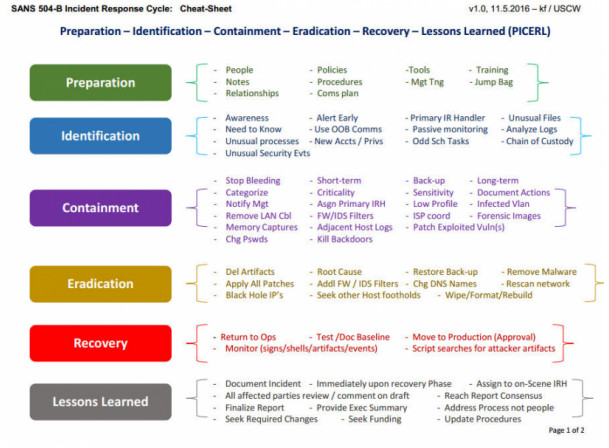
1.5.7 Flow in the phases

It is an excerpt for the NIST way (with 4 phases)



➔ NIST 4 phases *

1.5.8 SANS version



Can be downloaded from [SANS website] (https://www.sans.org/media/score/504-incident-response-cycle.pdf)

1.6 DFIR links

1.6.1 Mixed

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

https://github.com/Neo23x0

https://www.iocbucket.com/openioceditor

https://github.com/google/grr

https://winpmem.velocidex.com/docs/

http://edmands.net/Edmands.net/JumpBag.html

https://www.malware-traffic-analysis.net/2020/07/13/index2.html

https://www.netresec.com/?page=PcapFiles

https://github.com/meirwah/awesome-incident-response#memory-imaging-tools

https://github.com/orlikoski/CDQR

http://detect-respond.blogspot.com/2013/03/the-py-ramid-of-pain.html

https://github.com/gchq/CyberChef

1.6.2 Memory forensics

https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples

https://volatility-labs.blogspot.com/2019/10/volatility-malware-and-memory-forensics-training.html

https://www.andreafortuna.org/2017/08/07/volatility-my-own-cheatsheet-part-7-analyze-and-convert-crash-dumps-and-hibernation-files/

https://www.forwarddefense.com/pdfs/Memory-Analysis-with-Volatility.pdf

https://digital-forensics.sans.org/media/volatility-memory-forensics-cheat-sheet.pdf

https://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf

1.6.3 Lenny Zeltzer og Didier Stevens

https://zeltser.com/

https://zeltser.com/automated-malware-analysis/

https://zeltser.com/malware-sample-sources/

https://blog.didierstevens.com/programs/virustotal-tools/

1.6.4 Data collection

https://github.com/orlikoski/CyLR/releases

1.6.5 Virtual appliances.

https://securityonionsolutions.com/

https://cybersecurity.att.com/products/ossim

https://cybersecurity.att.com/products/ossim/download

https://wazuh.com/

1.6.6 Malware analyse

https://github.com/rshipp/awesome-malware-analysis

https://github.com/Yara-Rules/rules

https://github.com/JusticeRage/Manalyze

https://remnux.org/

https://www.circl.lu/misp-images/latest/

https://www.youtube.com/watch?v=QlQS4gk_lFU (Sandbox setup)

https://www.malwarearchaeology.com/cheat-sheets

https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/

https://evasions.checkpoint.com/ (Evasion teknikker)

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/

1.6.7 Online Malware analysis sandbox

https://urlscan.io/

1.6.8 Network analysis

https://hackertarget.com/tshark-tutorial-and-filter-examples/

https://danielmiessler.com/study/tcpdump/

https://www.wireshark.org/docs/man-pages/tshark.html

1.7 Hashing

1.7.1 What is a HASH value?

Is a method of cryptographically calculating the value of a file, a bit like DNA for us humans. HASH algorithms have been around for many years and have been used for many different functions. It has been possible to store hashes of passwords in databases to mask the code itself.

You can see more here Wikipedia HASH-værdi

* * *

1.7.2 How do we use it in forensics?

HASH is used to calculate the value of files, so you have a unique value representation for a file. That way you can identify if 2 files are the same.

You often see this if you download an ISO file with for example [Kali linux] (https://www.kali.org/get-kali/#kali-live) and look at SUM. This is the calculated value of the total file "kali.ISO".

When you download the .ISO file, you can calculate the HASH value yourself and compare the value between the calculating value you made together with the value on the supplier's website.

* * *

1.7.3 What tools are there?

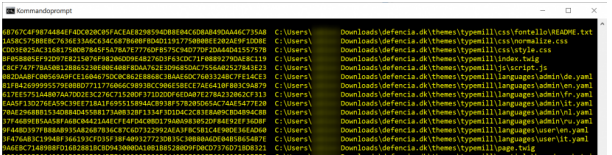
There are a myriad of tools out there, and many of them made open source or freely available. Below are a few tools that can be used to calculate HASH values at the file and folder level. In the Autopsy program, you can also calculate HASH values and compare with the [NIST database (NSRL)](https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library- nsrl / nsrl-download)

HASHtools calculates HASH for file or multiple files

2*Enkelt fil sammenlignet med websitet Havde der været mismatch havde linjen været rød!*

[Dirhash](#) (Calculates HASH for folders + subfolders)

```
DirHash.exe C:\Users\<username>\Downloads\mappe -sum -t
output_mappe -progress
```



3*The hash of the defencia.dk files has been calculated here*

below is a method to verify the content.

```
DirHash.exe C:\Users\<username>\Downloads\mappe sha256 -
verify output_mappe -progress
```

4verificeret og OK

* * *

If you use Linux or Mac, you use the code below

```
lablo@linux$ sha1sum filnavn
```

2. Forensics

Her kommer en masse gode tips og tricks til forensics og processer.

2.1 Labs for analysis

On this page you will get some knowledge about how to prepare your labs with space and hardware and software requirements.

2.1.1 Preparing Labs

Something that can be a really good idea. It is to have labs ready to use when analyzing or examining something in depth. There are many different labs, each with their own purpose out there, which may be worth spending some time on.

Below is my bid on some of them as we also get to look at it in class. I have aimed for us to be able to use older hardware and not the latest.

It is my experience that it is often the reality that one gets something laid off instead of investing in "latest and greatest", which costs so Elvis comes back. :)

2.1.2 Forensic Lab

A forensic lab requires its machine, as it is a big heavy task to analyze and process data for a digital investigation. The requirements are disk write and read speed, RAM and processor power.

Digital forensic tools compile an index / database of artifacts on a system which requires a lot of RAM available. like 16 gb or more. During that, you will experience being hampered in the speed of the analysis.

The processor is also put under pressure if it is to analyze and traverse through a lot of data. You will find that when forensic programs start analyzing, it takes between 80 - 100 percent of the processor power. Here it can be an advantage with more cores as it increases the speed considerably.

Last thing one must have is disk speed. This is probably the most important point to be able to make a faster review of data. A pile of data often needs to be read, which must then be analyzed. So the faster disk speed you have available, the faster you can analyze. However, this does not mean that you do not have to spend many hours waiting. Forensic tools use a lot of filters and search criteria for analysis. Which by their very nature will take time.

Do you have an eg x number of GB SATA 7200RPM older hard drive versus a new X number of GB NVME PCI-E hard drive. Then you will speed up the speed considerably as the newer hard drive is up to 20 times faster. In practice, this means that you can save many hours in the analysis work.

I have not tested what the difference is, but I assume it is more than double the speed of analysis.

2.1.3 Example of Hardware for the task

RAM -128 GB memory Hard disks - 1 pc 500 GB NVME PCI-E for OS / 2 pcs 2 TB for image analysis and storage of Index / 1 8TB + hard disk for storage in case of large images or temporary storage of data. Processor - Intel I9 Extreme or Ryzen threadripper Graphics - GTX 3080 or AMD XT 6900 *must support CUDA technology.*

[Sumuri Talino workstations] (https://sumuri.com/hardware/forensic-workstations/) are some of the ones on the market that specialize in building such machines. They focus on cooling and stability. Their position is that if the above is in place. Then the machine lasts 2-3 times longer than a cheaper workstation.

2.1.3.1 Can less do it?

Yes, it can easily do that. If you have an older computer standing, it can easily be used. Do you have e.g.

- ➔ 16 gb ram
- ➔ I7 processor (also of older date)
- ➔ SATA SSD hard drive with storage space for the task. graphics card at best

Then you will be able to do a survey. It just takes a little longer than with the machine above. It is up to you how much to invest. Personally, I would start with the latter example the first year or 2. Then you can

build knowledge around how to use your forensic hardware for research.

Autopsy - See the Autopsy page

2.1.4 Labs in general

Just a few thoughts on the environment for virtualization.

I have kept in mind that you have some older hardware that has been brought to life for the purpose.

Need to make a PC for the purpose new as well as old. Would it be my recommendation to start with VMware or Virtualbox installed on a Linux machine. Ubuntu or Linux mint *(It's a bit 2 pages of the same thing)* . Linux does not require as much ground resources to run, so you have more juice and power available for the virtual machines.

2.1.5 Linux

Kali https://www.kali.org/ ubuntu https://ubuntu.com/

2.2 A pair of virtual machines for the purpose

2.2.1 Security Onion

Is a cool project that is worth having a look at.

Security Onion is a complete setup of SIEM (Bridge, zeek), analysis, capture and incident response management and much more. It is an ISO you download and can install in a virtual machine or as a hardware installation.

Link to main page for Security Onion

2.2.2 Malware lab

Being able to do an analysis of a piece of unknown malware can make a big difference. Finding out how it spreads, what it creates of new files and processes, what it contacts on the Internet is to name a few. It can give the company a head start on how we can block further proliferation.

You can see the specifications under hardware for the task. The same is true here as well. It is important that you have enough RAM as you may have to run mult-

iple machines at the same time. processor and disk speed also have something to say. If you use virtual Linux computers, then they are often a little easier to run as they do not require as much.

Remnux https://remnux.org/ Flare vm https://github.com/mandiant/flare-vm

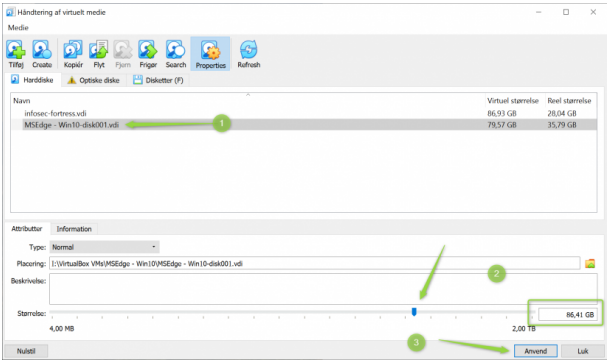
2.2.3 Log lab

Sof elk https://github.com/philhagen/sof-elk/blob/main/VM_README.md Splunk https://www.splunk.com/

2.2.4 Extending Hard Disk Space on Virtualbox and Vmware

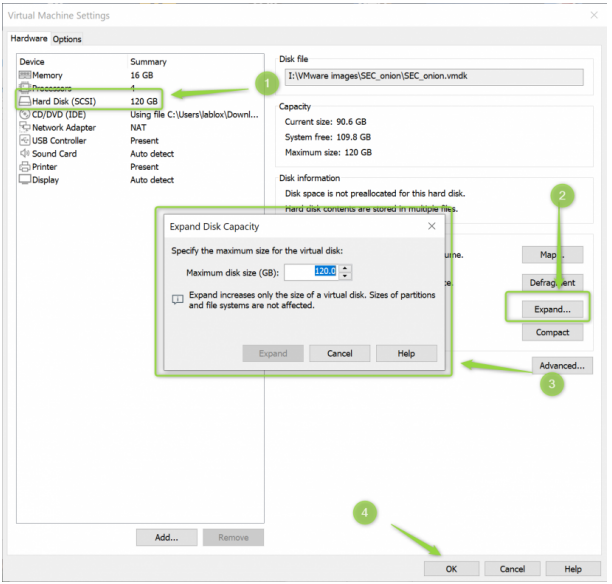
Sometimes hard disk space needs to be expanded in the virtual lab. It is relatively easy if you know where to look. Here is just a sketch of how to expand the existing space. This may be necessary on eg FlareVM, as there is not much space allocated on the VM you download from Microsoft.

```
Filer -&gt; håndtering af virtuelle medier -&gt; vælg din
VM og juster hvor meget plads du skal bruge på slideren.
Klik anvend og luk
```

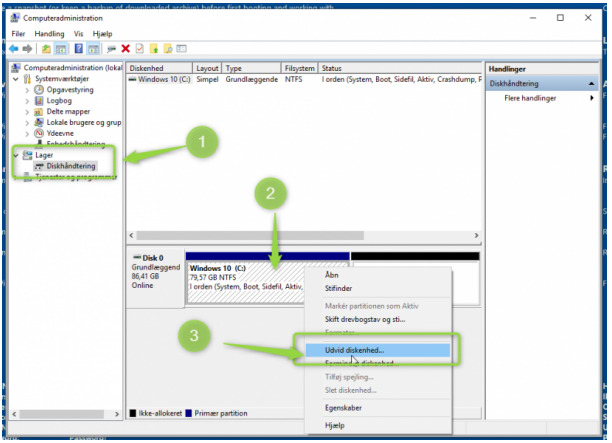


2.2.4.1 VmWare

Click settings -> hard drive - > expand and select your size and click OK



Start up your FlareVM and type *computer administration* and click under *disk management*



After selecting *disk management* , right-click on the hard disk you want to expand and select *expand disk drive* . Then there is a small guide where you click *next* and *next* , then you select the space to be expanded with and click OK.

This way you can expand your C: \ drive with more space. It can come in handy if you have slightly larger data to load. Note After installing FlareVM, there is by definition not much space on the system, so it is recommended that you perform this operation.

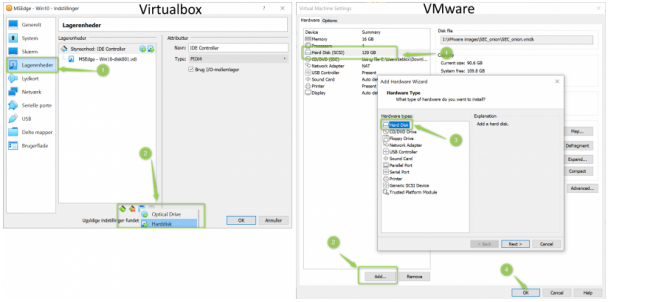
2.2.4.2 Extra space on an additional disk drive

It is also another easy methodology you can use. If you have set up a lab for analyzing logs or network

traffic, then it might be nice to have an extra hard drive on your virtual device. It can be done quite easily for both virtual box and Vmware.

VMware click on *edit virtual machine* and click on *hard drive* and select *add* and follow the wizard. Then you create an additional storage file for your device, with the size you want (and have room for)

Virtualbox you can select *settings* and *storage units* and select add (On plus)



Startyour virtual machine and select *disk management* and add the hard disk as an additional logical drive in Windows. Now you can use the disk as a disk 2.

2.3 Forensic data

2.3.1 Write protection

Write protection is a security so that data on a medium is not tampered with. You can read but not write. This ensures that no time stamps are made on the medium.

When a media needs to be secured according to best practices. Then it must be optimally secured with write protection to ensure that the proof is not tampered with. Write protection is used for this.

If you do not use it, then your system will make time stamps and thereby "contaminate" the proof.

If for some reason you can not make a data fuse correctly, then you need to start up and secure the proof with normal connection. It is important that what has been done is described correctly and preferably with witnesses and perhaps even consider filming the session.

It does not always go as planned, so it is the second best solution you have to resort to

& gt; Can not plant the proof? & gt; & gt; Yes, you can easily do that. It's easy, just connect the device to a system and copy data as with an external hard drive. & gt; & gt; Hiding it has happened ... It's hard and to my knowledge not done yet by anyone!

2.3.2 Storage

How is data stored? It is everything from the handing over of the proof, to the storage of data digitally and physically. Where is the data located? Who has access to data? Is it locked securely in a room where there is a code lock with a log of who enters and leaves the room?

2.3.3 Exchange of data / images

How to exchange data between partners and authorities.

2.4 Autopsy

2.4.1 What is Autopsy?

Autopsy is a forensic framework that originated from The Sleuth Kit (TSK) which is known from the Linux world. Autopsy has been used worldwide, by various investigators within digital investigation. It can provide a number of useful features like carve for data, extract web cache, visited websites, data from hives like registry, hashing of data and compare with known files and much more. It can do a lot, here I will cover the areas that we need in the course attack management. Du indlæser data fra imagefiler som ofte er E01 (encase 01) og DD (linux, står for Data Definition*)

```
wget * Source: https://en.wikipedia.org/wiki/Dd_(Unix)
```

2.4.2 Where do I get Autopsy?

Autopsy can be downloaded [free here] (https://www.autopsy.com/) Run the installation and click OK for the popup banners that require java and internet access.

2.4.3 Configuring Autopsy

There is not much to configure in autopsy, it works directly after installation.

You need to tell Autopsy where the output is to be saved. That folder will contain data which is indexed from the readings and can fill a part. Which is several gigabytes, so make sure there is enough space if you do multiple studies. It is also the output folder to which data is exported when you extract evidence from an image.

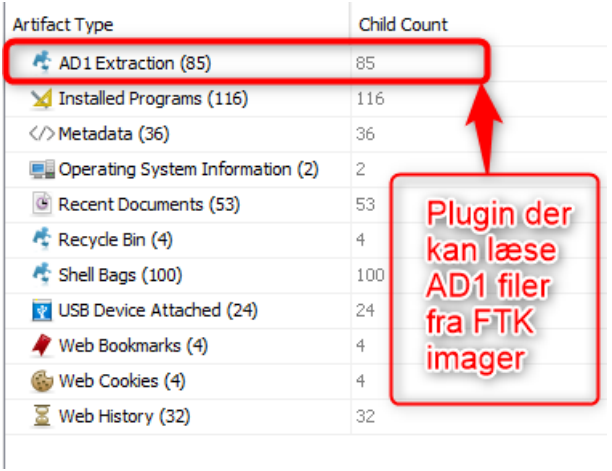
2.4.4 What are Ingestmodules?

Ingest modules are the automation built into autopsy. These are modules that are designed to look for specific data, such as databases, GPS data, carve data (such as old deleted files), search history, etc.

There are a number of pre-installed ingest modules in the program that you can use right away. I would

recommend that you take a look at the other modules one can download.

Github - Autopsy - Ingestmodules



5 *Fra autopsy ingest moduler. AD1 understøttes ikke fra installationen. Det skal installeres seperat*

2.4.5 Plugins for Autopsy?

Download a module and copy them to

```
C:\Users\UserFolder\AppData\Roaming\autopsy\python_module
```

2.4.6 Which surveys are good for?

You can do a number of surveys, such as what has been searched for on the web, you can search for malware. Which files have been accessed, encrypted containers and images.

What is important to know with Autopsy is that it requires training to use the program, as it requires you to know what you are looking for. Other software has developed search filters for different scenarios, it is often licensed software and costs a lot of money. As it requires a lot of development.

[] (media / live / 2022-01-29-22h32-57.png "Data source summary") {. center loading = "lazy" width = "450" height = "308"}

➔ What are the files on the secured image *

2.4.7 Add an image for study

Coming later

2.4.8 Try it yourself

You can play around a bit with Autopsy. Download one of the image files from the links below and let autopsy index the files.

Cfreds er NIST´s reference filer.

ENISA is ENISA´ s database over reference files.

2.4.9 A few tips

When you need to let Autopsy look through data, it is tempting to just select all the modules. I personally can not recommend it, as it requires quite a lot of computing power and often takes a really long time to run a module through (Depending on the nature of your hardware).

If you choose several modules, you can be lucky that it works. I have just experienced that they crash / stall and nothing more happens. It's a little boring to find out after many hours of driving.

I recommend that you take 1-3 modules at a time. Then the probability of a positive outcome is greater.

2.5 Chain Of Custody

To be able to make a correct securing of a proof, it requires that you have the right workflow. Here you will learn more about Chain Of Custody (COC). The most important thing is that effects and data integrity can be demonstrated in the process. So if there is to be a lawsuit, then there can be no doubt about what has been done.

‘ *TIP: Doubts will always be seen in a lawsuit. That is the most important task of the defense. The more reason you've been here, the more you minimize the prosecutor can doubt your conduct!*

The more thorough you have been here, the more you minimize the prosecutor can doubt your conduct!
`

2.5.1 Data collection and security workflow.

When collecting data and effects for study, then documents, documents, documents!

It's super important you describe

- ➔ Time
- ➔ Location
- ➔ Who was present *(In the case of personnel matters, that HR was also present)*
- ➔ How many effects were collected
- ➔ What data was collected and how Description of the procedure
- ➔ How was data secured? with or without write protection and why?
- ➔ Who is responsible for the effects until they are stored in the forensic room or the safe.
- ➔ A description / list of handovers between colleagues, so as to preserve who has had hands on the effects (this is the heart of COC right here)

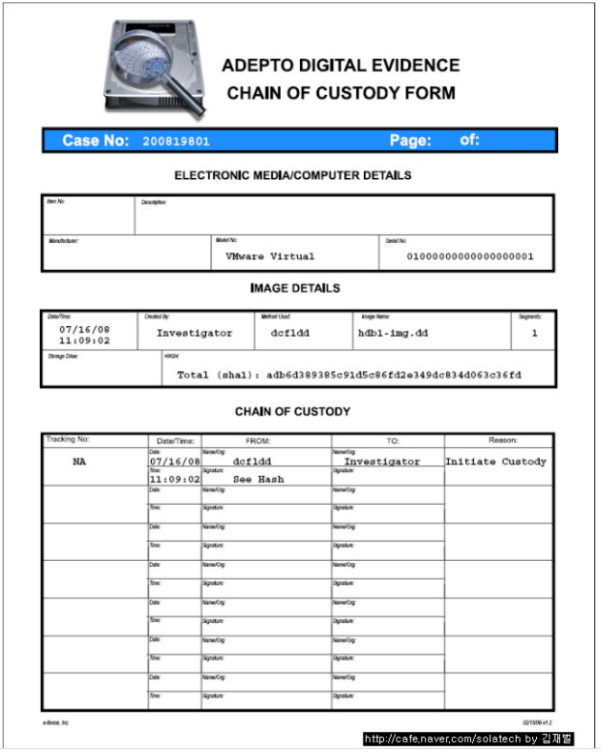
DISCLAIMER - The above list is not inexhaustible, I may have overlooked areas!

2.5.2 When the proof changes hands

Example of what it looks like. It can be said to be automated.

There is a signature for the handover and what effects it is about.

Helix Adepto Drive Dump Log-COC-200819801-.pdf



ADEPTO DIGITAL EVIDENCE
CHAIN OF CUSTODY FORM

Case No: 200819801 Page: of:

ELECTRONIC MEDIA/COMPUTER DETAILS

Item No:	Description:		
Manufacturer:		Model No: VMware Virtual	Serial No: 01000000000000000001

IMAGE DETAILS

Date/Time:	Created By:	Method Used:	Image Name:	Segments:
07/16/08 11:09:02	Investigator	dcfldd	hdb1-img.dd	1
Storage Drive:	MD5/SHA: Total (sha1): adb6d389385c91d5c86fd2e349dc834d063c36fd			

CHAIN OF CUSTODY

Tracking No:	Date/Time:	FROM:	TO:	Reason:
NA	Date: 07/16/08 Time: 11:09:02	Name/Org: dcfldd Signature: See Hash	Name/Org: Investigator Signature:	Initiate Custody
	Date: Time:	Name/Org: Signature:	Name/Org: Signature:	
	Date: Time:	Name/Org: Signature:	Name/Org: Signature:	
	Date: Time:	Name/Org: Signature:	Name/Org: Signature:	
	Date: Time:	Name/Org: Signature:	Name/Org: Signature:	
	Date: Time:	Name/Org: Signature:	Name/Org: Signature:	
	Date: Time:	Name/Org: Signature:	Name/Org: Signature:	
	Date: Time:	Name/Org: Signature:	Name/Org: Signature:	

e-fense, Inc. ©2006 v1.2

http://cafe.naver.com/soletech by 김재범

The above is please borrowed here

2.5.3 Under transport

For at sikre effekters fysiske integritet, så kræver det at man ved vigtige sager kan transportere effekterne korrekt. Så man kan påvise at der ikke er "pillet" ved effekten.


FELTERNE SKAL UDFYLDES MED KUGLEPEN OG BLOKBOGSTAVER
Kosternummer
DK-S-
Effektbeskrivelse
Sikret fra
Sikret af:
Dato
Underskrift
Fortsættelsespåtegninger:
Dato
Underskrift
Bemærkninger
NORAD
Udløbsdato: 30/04/2022
scenesafe
evidence recovery systems

Such bags can be purchased. An example is [miladan.dk] (https://miladan.dk/product/ds-crime/) or [Scenesafe] (https://scenesafe.co.uk/)

2.5.4 Write protection

In order to be able to secure correctly, it is important to be able to be write-protected correctly. So that you do not write data to the disk you are securing. This contaminates the evidence.

Write protection can be achieved in several ways. Below are a few examples of how to achieve write protection for your task.

Software Software write protection, it can see via a live boot image, such as caine or paladin. It is intended that the system is installed on a USB and thereby you can boot your PC from this USB and achieve write protection. It costs nothing to download and use.

Software write protection can also be achieved by software you install on your PC. An example of this is Safe block (Link here). Which, however, costs some money. It allows you to write-protect all the devices you connect to the system. Which means you have sata and USB in one function. It gets a little cheaper in purchasing, compared to hardware equipment.

The website [digitalforensics.com] (https://www.digitalforensics.com/blog/software-write-blockers-overview/) has made a good list of equipment.

2.5.5 Hardware

Hardware write protection is an electronic device that is inserted between the hard disk and the computer and thereby achieves write protection.

It is often a device that works via the USB port. It is quite simple to use and there is no speed reduction if you use USB 3.x

They can be used for all operating systems and secure via FTK (win 10) and DD (Linux / Mac). It is a one-time investment you have to make.

Below are 2 examples of write protection from Weibe-tech and Coolgear. It is 2 pages of the same case which is write protection.

Weibetech is a little more delicious finish and with function as invention of serial number and product name. Where Coolgear is completely basic, with buttons for write protection.

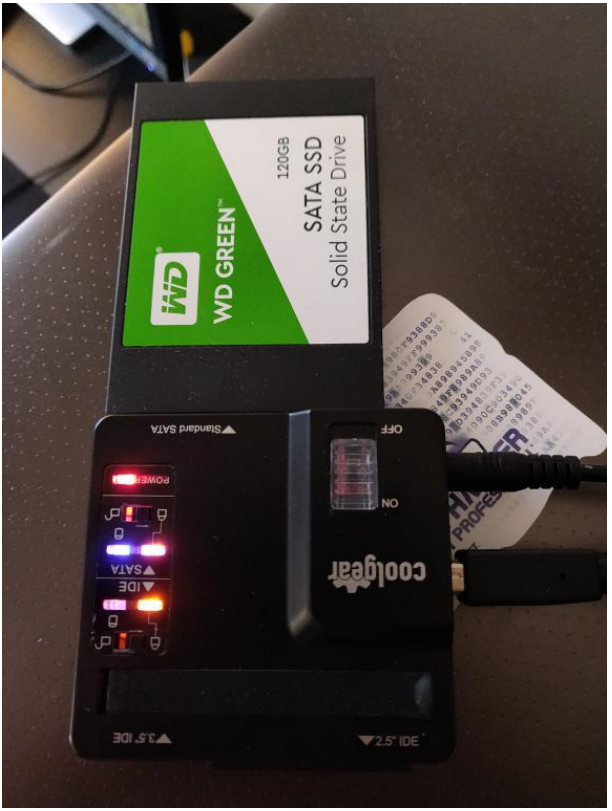
Weibetech FUD 5.5 costs around 3,000 to 4,000 Danish kroner

Coolgear SATA / IDE writeblock costs approx. 750.- incl VAT and freight from the USA. (Has been removed from the supplier's website. It is not known if there will be any replacement)

The top of the pop here at the time of writing is Tableau from guidance software. It has created a lineup of different solutions where adapter boxes can be connected with their own cable. The price is here on the friendly side of 8,000 Danish kroner.

There are prices for every taste. It can be a good investment if one needs data secure media like hard drives. If you can make a combination of hardware and software so that you can perform different tasks, then you are better off.

Remember, this is what should fit the detop YOUR task to be purchased for 🙂



6 *Coolgear is the slightly discount version of a write protector. It works fine and is cheap (and unfortunately discontinued)*

2.6 Datacollection

2.6.1 Why is proper data security important?

Data security and collection is one of the important things in case of an attack. There are many reasons for this, such as if you report the attack to the authorities or need to understand what has happened.

If the attack is to end in court, then it is important that there has been control of the process. If there is not, then there is a possibility that the case may fall in court. Here you get knowledge about how a good data security can be performed.

2.6.2 What data do we have?

What data do you have available if things go wrong? If you need to get logs out of a computer, then you will often be able to retrieve the computer and data secure. But if you have a cloud service, how are you? Do you know how data can be retrieved? These are just some of the questions that you have to ask yourself before you get hit.

2.6.3 How should we collect data?

The most important thing is to have described your process for the collection. The more careful you look the better.

- ➔ Date and time of start and end time
- ➔ performed by whom

- ➔ what data is retrieved?
- ➔ tools have been used (version of the tool)
- ➔ is data from a tool (antivirus, IDS, IPS, network equipment and what version of software did it have?)
- ➔ how integrity checks are made
- ➔ what does the data contain and what format and fields are there?

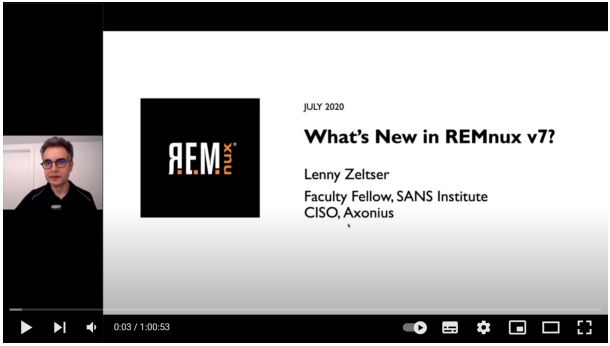
2.6.4 Integrity and data collection

once you have collected data, then you should make an integrity thej

more will come later. (0504-2022)

2.7 Malware analysis

This page is inspired by the video of Lenny Seltzer



2.7.1 Download Remnux

https://remnux.org/#distro

```
lablo@linuxserver$ Sudo apt-get update
```

remnux update (Takes some time the first time)

2.7.2 Transfer files to remnux

sshd start (for at starte FTP) Ifconfig for IP

sftp://IP-adress

> User: remnux > pass: malware

Extract zip files with password

sudo apt-get install p7zip-full

extract file 7z x filenavn.zip -> herefter bliver du promptet for kodeord

Your are ready.

* * *

Static analysis of the file

for API calls, strings and

yara-rules filename What happens then?

(Update clam = freshclam) clamscan filename What happens then?

---------- SCAN SUMMARY ----------

Known viruses: 8921175 Engine version: 0.102.4 Scanned directories: 0 Scanned files: 1 Infected files: 0 Data scanned: 0.48 MB Data read: 0.46 MB (ratio 1.04:1) Time: 16.517 sec (0 m 16 s)

manalyze filename What happens then

(Trickster = meadow and Finnish language and compile date 20 May 2015)

peframe filename What happens then

(Maybe can be used for yara ???? Yara rules take effect)

pecheck filename Entropy gives a hint about packaged files / compressed files / payload More info about what happens in the file (look for overlay)

strings filename

Do we see anything here?

Pestr filename is there any difference?

What about floss filename?

Maybe it can be used?

md5sum filename copies to virus total What happens then?

Xorsearch filename http

(Searching for http or whatever might be interesting)

* * *

a little more emulation before detonation.

binee filename

gives apikald

can be used for debugger later

capa -vv filename

Watch for api cold

Copy offset into ghidra so you can see what is happening in decompiled code

Fakedns together with inetsim

starts a dns server and responds like the internet

2.7.1 Sample sharing

- ➔ Check if the HASH can be found on some of the online services. Many times you can find the HASH value without dividing the sample. So you do not reveal yourself to those who watch (it sounds sneaky, but opponents keep an eye)
- ➔ Examine whether you are allowed to share the malware by the company / partner.

- ➔ The zip format is frequently used, but you should consider using the 7-Zip format to better hide the contents of the archive.
- ➔ The "infected" password is often used, as many sandbox labs can use the code to extract the file.
- ➔ Instead of emailing the sample as an attachment, consider sending the researcher a link where they can download the file.
- ➔ Specify the hash for the malware sample using a modern algorithm such as SHA256 so that the recipient can confirm that they have got the correct file.

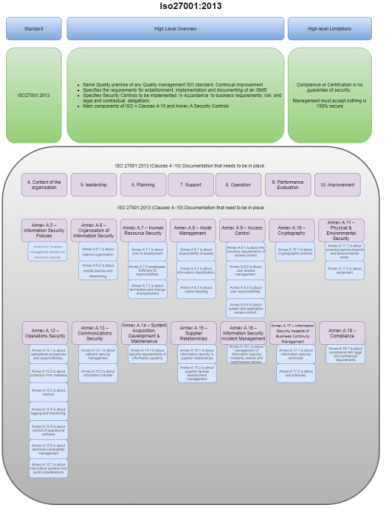
The Above is inspired by Lenny Zeltzer

3. Governance

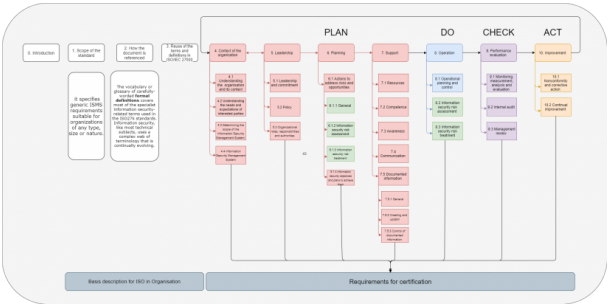
Her kommer lidt mere viden fra faget governance. Det er blot som supplement til undervisningen.

isms iso2700x final (MP3, 10.23 MB)

Her kan du hente en kort intro til ISMS (Information Security Management System. Det er ISMS forklaret



7 *Det er Klausulerne og Anneks A samlet*



8*PDCA cyklus forklaret i sammenhæng med klausulerne. Det er processen der bliver illustreret.*

3.1 GDPR

- Governance
- GDPR

➔ Obligations of the data controller
➔ The 6 data protection principles
  ➔ ** 1 Transparency and legitimacy: **
  ➔ ** 2 Purpose Limitation: **
  ➔ ** 3 Data minimization: **
  ➔ ** 4 Accuracy: **
  ➔ ** 5 Storage period limitation: **
  ➔ ** 6 Confidentiality and Integrity: **
➔ (7) Accountability and compliance

- Data subject rights

➔ Duty to provide information
➔ Right of access

➔ Right to rectification
➔ The right to be forgotten
➔ Right to limit treatment
➔ Data portability
➔ Objection
➔ Prohibition of automatic individual decisions and profiling

- ISO Handling - ISO27701
- Data breach with GDPR´s eyes

➔ Anatomy of data breach

- Data Mapping
- ISO 27701: 2013

GDPR = General Data Protection Regulation

Effective May 25, 2018

The General Data Protection Regulation (GDPR) is a law that deals with data protection for all citizens of the European Union (EU) and the European Economic Area (EEA). The purpose of this law is to enable individuals to have control over the personal information provided.

3.1.1 Obligations of the data controller

As a data controller in collaboration with your possible data processors, you must, among other things, ensure that you:

- ➔ Allowed to process the information that you and your data processors are in possession of (if you have a treatment authorization) Keeps a record of your treatment activities
- ➔ Is able to comply with the rules on the data subjects' rights, such as the duty to provide information or the right of access.
- ➔ Report any breaches to the Danish Data Protection Agency within 72 hours
- ➔ Have a data processor agreement with the data processors that process personal data on your behalf
- ➔ Can document to the Danish Data Protection Agency that you have ensured data protection with appropriate technical and organizational measures so that no unintentional, unreasonable or illegal processing takes place.

3.1.2 The 6 data protection principles

3.1.2.1 1 Transparency and legitimacy:

personal data must be processed in a lawful and secure manner and must be easily accessible.

Transparency

- ➔ It must be communicated how data is collected and how data is used. If data is passed on to third parties, this must be stated.
- ➔ Openness and honesty are the key words here.

Justification

- ➔ Data The controller is open and honest about function and its operation.
- ➔ Processes data only in the direction one would expect and does not misuse data
- ➔ Does not use data in directions not described or justified.

3.1.2.2 2 Purpose Limitation:

Data should only be collected and used for the stated purposes.

- ➔ The regulation describes that personal data can be collected for specific and explicitly described purposes
- ➔ Terms and conditions for the protection of privacy, must inform the user about how extensive data is processed (If data is collected, then these must not be brought to sister companies that can use data for marketing)
- ➔ However, data may be stored for archives, for statistics, security, historical research (Data must be Pseudonymised and encrypted, will be valid methods to anonymize data)

3.1.2.3 3 Data minimization:

Only necessary data are collected for processing.

Data collected and processed must be relevant, sufficient and limited. Do not collect more data than is

olutely necessary.

Book example Applying for a job, it will not be appropriate to ask for health data

Reference is made to data mapping (chapter 9 in the book) (It is not a requirement, but a necessity to demonstrate below)

Which covers

- ➔ Data exist
- ➔ Where the data is located
- ➔ Under what regulations data is kept

3.1.2.4 4 Accuracy:

Users may request to delete or correct inaccurate personal data.

Data must be kept up to date and accurate

- ➔ Which ensure that data processing and becomes more accurate.
- ➔ Which requires processes that ensure data is kept up to date. (We know this from emails sent from our service providers who want us to update the information they have about us) Inaccuracies can occur, as if a buyer has placed an order and he changes address subsequently. Then data does not need to be updated. Unless buyer makes new order.
- ➔ Inaccuracies sometimes have to be saved, for the sake of history. Such as in the case of misdiagnosis.

As this will be important for future treatments. Track history is saved.

Notice: 47 Recital 71 of the Regulation makes this abundantly clear: 'The data subject must have the right not to be subject to a decision which may include a measure which assesses personal aspects relating to him or her which are based solely on automated processing, and which produces lawful effects relating to him or her, similarly significantly affecting him or her, such as automatic rejection of an online credit application or e-recruitment practice without any human intervention. Do not make machine cuts without the influence of a person.

3.1.2.5 5 Storage period limitation:

Personal data should only be stored for the period necessary for the purpose of processing purposes.

- ➔ Personal data may no longer be stored for the purpose for which the data is used.
- ➔ How data is stored (not on which media) but how data is stored. it is stored encrypted or in multiple instances across multiple databases. Do not use data (or can justify it) .... Delete it!
- ➔ Data stored must be subject to legal and contractual requirements. Which can demonstrate that

data is deleted and that Automation ensures data deletion after eg a given period.
- ➔ Data that is saved falls under DSAR (Data Subject Access Request) better known as data portability. As secure we as customers have access to the stored data.

3.1.2.6 6 Confidentiality and Integrity:

Organizations must protect personal data from unauthorized or illegal processing under the GDPR.

- ➔ The most important principle from a financial point of view.
- ➔ If data breaches occur, then it is relatively easy to prove that data has not been secured properly. If this had been done correctly, then the breach would not have occurred in the first embrace. (In Denmark, it will be the Data Inspectorate that can assess this)
- ➔ Companies need to secure data so that it can not be misused or leaked. For example, data can be encrypted and a log is kept of who accesses data at a given time. Integrity must ensure the consistency of data while data is stored
- ➔ Reference is made to the CIA model and ISO 27001 ISMS

3.1.3 (7) Accountability and compliance

- ➔ Article 5, para. 2, is short but extremely important: The controller is responsible for and able to dem-

onstrate compliance with § 1 Accountability
- ➔ This is a seventh principle, which claims that the data controller is responsible for ensuring compliance with the previous six data processing principles and for being able to demonstrate this compliance.
- ➔ It places demands on its own suppliers (Read supplier agreements on compliance with GDPR rules)

3.2 Data subject rights

A few points about the rights of data subjects.

- ➔ Duty to provide information
- ➔ Right of access
- ➔ Right to rectification
- ➔ Right to delete ("right to be forgotten")
- ➔ Right to limitation of treatment
- ➔ Right to data portability
- ➔ Right to object
- ➔ Prohibition of automatic individual decisions and profiling

3.2.1 Duty to provide information

Articles 13 and 14

The data subject has the right to receive information when the data controller collects information. A distinction is made between information obtained directly from the data subject or the information received from others than the data subject. In both cases, the data controller has a duty to provide information,

unless the data subject knows the information in advance.

3.2.2 Right of access

Article 15

The data subject has the right to receive the data controller's confirmation of whether personal data about the data subject and the right of access are processed therein.

3.2.3 Right to rectification

Article 16

The data subject has the right to have incorrect personal data about himself corrected by the data controller without undue delay

Example We see it when we have set up a website, or log on to a page where it has been a while. Then we are asked to correct the information, or check if the information is correct.

3.2.4 The right to be forgotten

Article 17 states that the data subject has the right to request that personal data about him / her be deleted if one of several alternative grounds is present.

The "right to be forgotten" was replaced during the negotiations by a less comprehensive "right to erasure".

One of the grounds is that the processing is not lawful, for example that Article 6 (f) of

3.2.5 Right to limit treatment

The data subject has the right for the data controller to restrict or block the processing of information about the data subject. This must be done through labeling of information so that future processing is limited, cf. the definition in art. 4, No. 3.

The data controller is obliged to limit / block processing when the data subject disputes the accuracy of the information, in the event of illegal processing but not deletion, in the determination of a legal claim or when the data subject objects, cf. art. 18 (1a-1d).

3.2.6 Data portability

Article 20

According to the Regulation, the data subject has the right to transfer his personal data from one system to another, without being prevented from doing so by the data controller. There is also a requirement that the information must be provided to the data subject in a structured and usable electronic format.

3.2.7 Objection

Article 21

The data subject has the right to object to an otherwise lawful processing if special circumstances so

require.

3.2.8 Prohibition of automatic individual decisions and profiling

Article 22

The data subject has the right not to be the subject of a decision based solely on automatic processing, including profiling, which has legal effect or similarly significantly affects the person concerned, unless the decision is necessary for the conclusion or performance of a contract, is authorized in EU law or the national law of the Member States or is based on the express consent of the data subject. [

Article 12:

https://www.retsinformation.dk/eli/lta/2018/502 (Dansk) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679#page=39

The clear and short https://en.wikipedia.org/wiki/Personal Data Regulation

3.2.1 ISO Handling - ISO27701

Relatively new standard, as it was released in August 2019, and should be able to merge ISO and GDPR better together.

So that ISMS contains GDPR compliant personal data. The intended application of ISO / IEC 27701 is to expand the existing ISMS, with privacy specific controls and thus create PIMS to enable effective privacy management in an organization. The DPO (Data Protection Officer) can provide the necessary documentation that applicable personal requirements are met (PIMS = Privacy Information Management System)

- ➔ The PIMS framework may look like an ISMS.
- ➔ ISMS is targeted at several focus areas
- ➔ PIMS can only target personal data processing
- ➔ PIMS must support the core components of a Privacy framework.

3.2.2 Data breach with GDPR´s eyes

Violation of security, leading to erroneous or illegal destruction, loss, alteration, unauthorized disclosure of, or access to, transfer of personal data. Saved or processed.

GDPR does not focus on other breaches, but only on loss of privacy.

3.2.2.1 Anatomy of data breach

Data can be transmitted online and TOR (refer to Darknet) Data corrupted or made inaccurate / altered In other words, a breach of the CIA model

Data breaches do not happen by themselves and there have been breaches of vulnerabilities or threats

have been overlooked. (Angry employees who smash data, or abuse rights)

Or vulnerabilities that have been overlooked, ignored or were ignorant about.

3.2.3 Data Mapping

GDPR does not directly require data mapping It is considered a “best practice” to have a mapping of data, as it can be a difficult exercise to clarify data if one does not.

As the book describes, "you can not protect what you do not know / know", here are 3 definitions

➔ Data exist
➔ Where is it and under what guidelines is it stored

This will be a difficult task if you have not examined your data before.

4 elements of data flow

Data Items: The information itself and or a data set

Format: How is data stored? USB, storage cloud etc.

Transfer methods: transfer of data from A to B and how data is transported and which encryption.

Locations: Where is the data physically located?

Data mapping is significant in relation to DPIA and risk assessment. to inform about areas where we

need to be vigilant

3.2.4 ISO 27701: 2013

GDPR proposes to introduce a PIMS (Personal Information Management System). There is an explicit requirement organizations must have below in place

The ability to ensure ongoing confidentiality, treatment system integrity, availability and robustness and services The ability to restore the availability of and access to personal information in a timely manner in the event of a physical or technical incident Processes for regular testing, assessment and evaluation of the effectiveness of technical and organizational measures to ensure the safety of processing.

This really means that organizations need to integrate data protection and privacy, which requires a more comprehensive approach to information security. Companies engaged in treatment systems and services. as with safety, continuity and continuous safety testing (primarily in the form of penetration testing). This is where ISO 27001 comes in.

3.3 Paragraphs

Her finder du nogle af de straffelove vi har i Danmark. Som retter sig imod cyberangreb.

3.3.1 Forbrydelser mod personlig frihed

- § 263a = Distribution of means of distribution dissemination of this
- § 264 = Unauthorised access
- § 235 = Child pornography paragraph

3.3.2 Formueforbrydelser

- § 279 = Fraud
- § 279 a = Data fraud
- § 281 = Extortion
- § 288 = Robbery
- § 290 a = Money laundering
- § 291 = Vandalism
- § 293 = Theft (DDoS 293, stk 2, that uses theft.)*
- § 193 = Public disturbance
- § 299 b = Copyright
- (§268 = Slander=

1. a serious accusation is untrue or
2. an accusation has been made or spread through the content of a mass media, and the accusation is suitable for significantly harming the victim.)

3.3.3 A little lawstuff (danish)

- https://danskelove.dk/straffeloven
- https://danskelove.dk/nis-loven
- https://anklagemyndigheden.dk/da/soeg-i-vidensbasen

*(https://www.computerworld.dk/art/225949/dansk-teenager-fanget-efter-ddos-angreb-mod-kl) (https://ekstrabladet.dk/112/dansk-politi-med-i-ka-empe-aktion-150.000-mistaenkt/7492889)

3.4 Links to Governance

Below is a linkcollection of goodies

- → https://gdpr.eu/category/news-updates/
- → https://www.datatilsynet.dk/generelt-om-databeskyttelse/vejledninger/
- → https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/
- → https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles
- → https://sikkerdigital.dk/virksomhed/sammen-mod-cybertrusler/bahne/
- → https://startvaekst.virk.dk/node/1884/security-report/recommendations/pdf
- → https://www.ncsc.gov.uk/section/information-for/small-medium-sized-organisations
- → https://www.nist.gov/privacy-framework/privacy-framework
- → https://www.danskerhverv.dk/politik-og-analyser/it-og-tele/agenda—logning/
- → https://www.cert.dk/da/tjenester/sikkerhedshaendelser
- → https://dkr.dk/it/it-kriminalitet-i-tal/
- → https://crest-approved.org/
- → https://anklagemyndigheden.dk/da/soeg-i-vidensbasen
- → https://www.retsinformation.dk/eli/lta/2006/988

➔ https://brs.dk/

3.5 Intelligence i virksomheden

- Governance
- GDPR

➔ Obligations of the data controller
➔ The 6 data protection principles
  ➔ ** 1 Transparency and legitimacy: **
  ➔ ** 2 Purpose Limitation: **
  ➔ ** 3 Data minimization: **
  ➔ ** 4 Accuracy: **
  ➔ ** 5 Storage period limitation: **
  ➔ ** 6 Confidentiality and Integrity: **
➔ (7) Accountability and compliance

- Data subject rights

➔ Duty to provide information
➔ Right of access
➔ Right to rectification
➔ The right to be forgotten
➔ Right to limit treatment
➔ Data portability
➔ Objection
➔ Prohibition of automatic individual decisions and profiling

- ISO Handling - ISO27701
- Data breach with GDPR´s eyes

➔ Anatomy of data breach

- Data Mapping
- ISO 27701: 2013
- Paragraphs

➔ Forbrydelser mod personlig frihed
➔ Formueforbrydelser
➔ A little lawstuff (danish)

- Links to Governance
- Intelligence i virksomheden

➔ Get started
➔ What is RSS
➔ Trustworthiness
➔ RSS læsere
➔ What can I use it for?
➔ App
➔ My method
➔ what is good about a payment solution
➔ Sharing with colleagues and friends
➔ Conclusion
➔ Resources

3.5.1 Get started

In my opinion, one of the things you can do easily and relatively cheaply is to monitor the media to obtain "intelligence". The word Intelligence spreads over a wide field, here I will keep an eye on news via RSS, or said in Danish news from the security front.

on this page you get my view on how to make news news to your advantage and it is not sponsored in any

way.

Back when Google had their RSS reader, I started keeping an eye on websites and news sites. I have always thought this has given me value, as I get the news served and can sort, mark and keep an eye on keywords.

3.5.2 What is RSS

What is a news RSS reader? It is actually a technology that has been used for several years and one of the co-founders of the format is [Aaron Swartz] (https://en.wikipedia.org/wiki/Aaron_Swartz)

RSS means Really Simple Syndication which translated is an update feed. The purpose is you can "subscribe" to your website's news feed and keep up to date with news every time some new material or stories are published. It's smart, because you can keep an eye on many websites at once. However, it does require that you have an RSS reader.

3.5.3 Trustworthiness

Although we have a lot of good social media that can feed data to us, I am a supporter of getting it directly from the source, so I am sure there are no others who have interpreted the story for me. Through my RSS reader, I can keep an eye on whether the story is on several media that I have selected myself. Which, in my opinion, can add to some validity and credibility.

It can be difficult to distinguish good sources from bad sources. It has certainly not gotten any easier with time. One must preserve his critical sense and common sense.

3.5.4 RSS læsere

There are many types of RSS readers. I want my must be online and be able to work with keywords so I can keep an eye on specific topics.

A few examples of RSS services.

➔ Inoreader
➔ Feedly
➔ Newsblur
➔ The Old Reader

The above is taken from this article from [lifewire.com] (https://www.lifewire.com/top-free-online-rss-readers-3486649)

I even use Inoreader Pro, which costs 80 euros a year. Which I thought is OK in terms of how often I use it. It is a service that can potentially save a lot of money if you get on the cutting edge of something.

3.5.5 What can I use it for?

You can keep an eye on vendor websites. Then you are at the forefront when they release new versions of their software or come up with new features or

bug fixes. It's super easy and is worth its weight in gold.

You can keep an eye on when someone finds errors / vulnerabilities in software, or when there are critical vulnerabilities loose on the web. It can be beneficial if you can manage to mitigate against problems before they occur or hit you.

You get a quick overview of all the news that comes, and you can sort through them yourself.

3.5.6 App

There is an app for Inoreader (and for the others as well). The app for Inoreader has gotten better with time. Since it crashed a lot for me in the beginning, which is not cool if one has to read news. It was often associated with the amount of articles. They have an app and it works, which is fine for me, I use the online and browser version whenever I can.

3.5.7 My method

How to keep up with the news flow and new upcoming threats? Here is my example of how to handle that task. The starting point is Inoreader and its functionality. There are others out there like Feedly, blurnews fm. Of course, you have to choose the one you liked best.

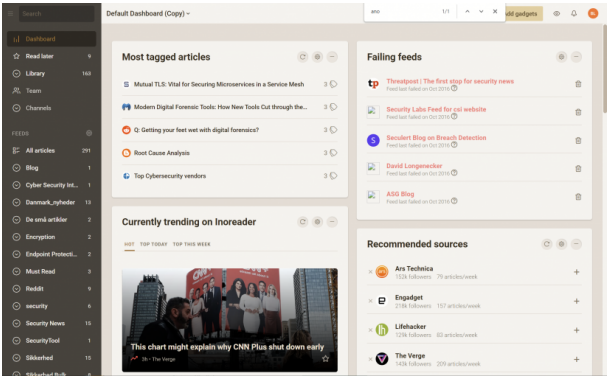
What is a news RSS reader? It is actually a technology that has been used for several years and one of the

co-founders of the format is [Aaron Swartz] (https://en.wikipedia.org/wiki/Aaron_Swartz)

RSS means Really Simple Syndication which translated is an update feed. The purpose is you can "subscribe" to your website's news feed and keep an eye on news every time some new material or stories are published. It's smart, because you can keep an eye on many websites at once. However, it does require that you have an RSS reader.

I started with the old free Google reader, which they turned off in 2011, which was a shame. It was free and worked really well. Since then, I have switched to [Inoreader] (https://www.inoreader.com/), which has a free version and a pro version. I have taken the pro version here as a starting point, as it provides a few more features which are worth the money in my opinion.

The price is about 600.- kroner per year for the pro service Se priserne her



3.5.8 what is good about a payment solution

often some useful things come with it. Feedly, Leo has their AI as they sell, as their weapon against too much news.

Inoreader has their gene method to cut through the piles.

The first thing you will become familiar with is the common way of monitoring RSS websites. Namely, to add a URL in the program, then you will receive all the stories. It's kind of nice and good, because then you can just skim through the ones you have chosen.

Inoreader has a few tricks up its sleeve that make this easier. You can do several things, namely set up "highlighters". When you look through the news, your search words are marked with a color, which makes it

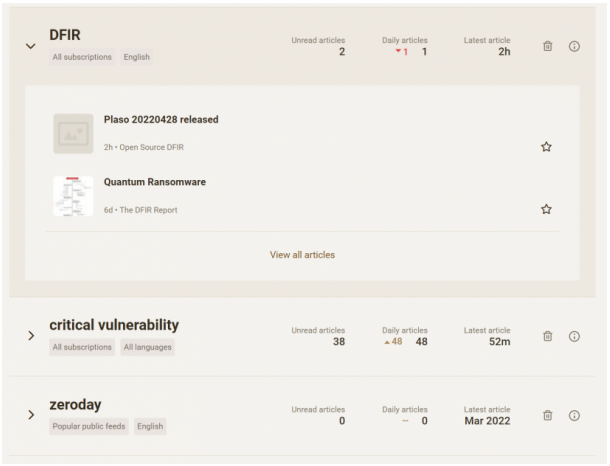
easier to recognize the words that may be interesting (you can download my list of words that can be added). It makes it very easy to look through the articles and see what is marked with the colors.

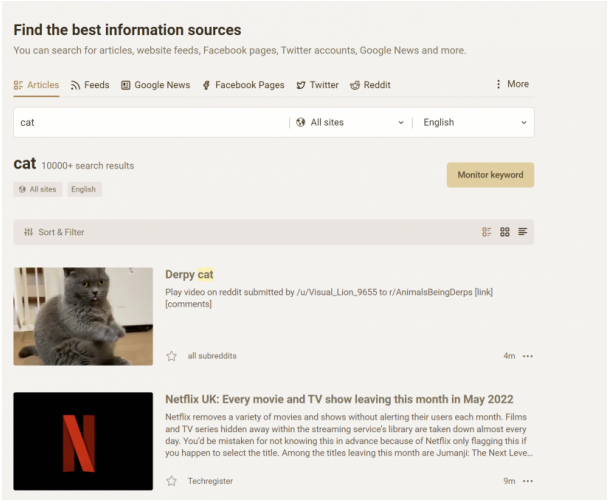
Where things take more speed is where you can set up automation and let inoreader find articles their database and match where you are looking and you still have your highlighters. This means that you can still cut through the amount of data easily and clearly.

From there, you can then make an extract for a website.

9*Colors are highlighters*

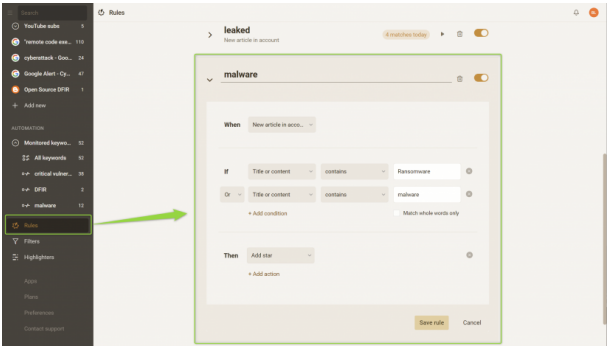
Below are examples of keywords I have put a search engine on. Then the articles containing the features will be displayed. quite smart if you want to keep an eye on many articles.


DFIR
All subscriptions
English
Unread articles
2
Daily articles
1
1
Latest article
2h
Plaso 20220428 released
2h • Open Source DFIR
Quantum Ransomware
6d • The DFIR Report
View all articles
critical vulnerability
All subscriptions
All languages
Unread articles
38
Daily articles
48
48
Latest article
52m
zeroday
Popular public feeds
English
Unread articles
0
Daily articles
0
Latest article
Mar 2022

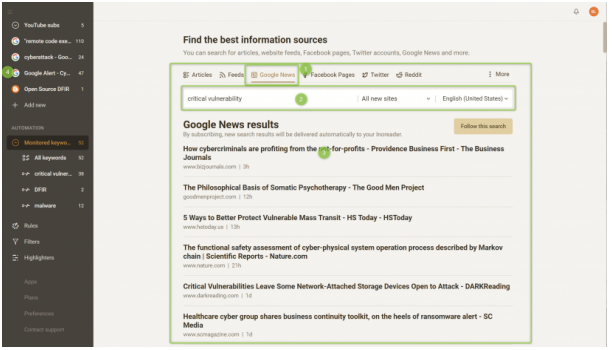


10 *Here I have searched for cats and here Inoreader finds articles with the topic from their link databases*

Here's an example of how I can set up rules so that automations can mark articles with stars so that it sorts out a caveat lot of indifferent articles that do not relate to the topic.



One of the super cool things about Inoreader is that you can create a search function for google news. Which is pretty cool, because then you also see articles outside of your RSS sites.



11 *Der oprettes en "mappe" med google news på dit søge kriterie.*

I have used Inoreader there for the last couple of years and bought their offers on black friday , singles day , valentines , can you see where I want to go? It's about saving a little money when you can, and the above options are no exception.

I have no problem paying for such a service. Whether it's Feedly, Inoreader or others, it does not matter to me. As long as I can make use of some automation that can make sense in terms of digging through the article flow.

3.5.9 Sharing with colleagues and friends

If you have colleagues or friends who want to see some of the news you have. Then there is an opportunity for you to share your feed directly on your website. Which is pretty smart, however, requires that you set up some very precise search filters so that it is not all that important no matter what is presented.

Se eksempel her

3.5.10 Conclusion

What is my recommendation is that you look through the market for offers and tests of RSS readers. There are many out there and some of them are programs that one installs. Here, however, I would argue that a service like Inoreader has its advantage, as it is online and is constantly updated with features. What makes the difference is the automation and highlighters, which run 24/7. It also means you do not have to have

any PC running, I appreciate that. In a busy day, this solution is, in my opinion, worth all the money. Since I save a lot of time to spot things in the articles.

So you might be thinking, I do not overwrite articles? after all, perhaps that is not to say with certainty. It requires gaining experience and tuning services to your needs, so I believe that loss of important articles is minimized.

For me, the criterion is that I see weaknesses in the software that I use or that is in the company.

I was looking in the direction of feedly, which has some AI to read articles for me. It's super smart, whether it works in practice, I do not know at the time of writing, as I have not bought the product or tested with the 30 day "trial". Since I have to register with more data than I want to provide. Feedly uses LEO, which is their AI for corporate, so they keep an eye on new data and monitor the Internet for important security-related news. What the price is I do not know, have a notion that it costs so the earth shakes. For that reason, I am happy with Inoreader, which costs about 600 kroner a year, which suits me and makes super good sense for my monitoring of the network.

Hope it gives you inspiration to do your own monitoring, then it's just about getting started. :)

3.5.11 Resources

Here is my list of keywords I use.

keyworkds (TXT, 1.36 KB)

Opml fil with all my feeds

4. Infosec og diverse

Her finder du indhold om generelle emner inde for informations sikkerhed. Det er ikke kun begrænset til virksomheder og deres tankegang. Det er også omfattende grundlæggende IT-hygiejne

4.1 Blandet viden fra feltet.

På de sider vil jeg tage fat i emner som nogle de fleste forældre og familimedlemmer oplever, har oplevet, eller måske kommer til at opleve.

Det er tiltænkt som en velment guide til forældre, unge og ældre som gerne vil have hjælp til at højne sikkerheden i hjemmet.

Min tilgang er, at det skal være nemt og forståeligt, så det giver mening derude. Der er mange rigtig gode hjemmesider som giver gode råd, hvilket er fint. Det er bare sjældent man konkretisere det, da det bliver for teknisk. Hvilket også er rigtigt, men der skal altså noget teknik til engang i mellem og så er det her du/i må ringe til en ven

- Governance
- GDPR

➔ Obligations of the data controller
➔ The 6 data protection principles
  ➔ ** 1 Transparency and legitimacy: **
  ➔ ** 2 Purpose Limitation: **
  ➔ ** 3 Data minimization: **

➔ ** 4 Accuracy: **
➔ ** 5 Storage period limitation: **
➔ ** 6 Confidentiality and Integrity: **
➔ (7) Accountability and compliance

- Data subject rights

➔ Duty to provide information
➔ Right of access
➔ Right to rectification
➔ The right to be forgotten
➔ Right to limit treatment
➔ Data portability
➔ Objection
➔ Prohibition of automatic individual decisions and profiling

- ISO Handling - ISO27701
- Data breach with GDPR´s eyes

➔ Anatomy of data breach

- Data Mapping
- ISO 27701: 2013
- Paragraphs

➔ Forbrydelser mod personlig frihed
➔ Formueforbrydelser
➔ A little lawstuff (danish)

- Links to Governance
- Intelligence i virksomheden

➔ Get started
➔ What is RSS
➔ Trustworthiness
➔ RSS læsere
➔ What can I use it for?
➔ App
➔ My method
➔ what is good about a payment solution
➔ Sharing with colleagues and friends
➔ Conclusion
➔ Resources

- Infosec og diverse

➔ Blandet viden fra feltet.

- Falske Opkald

➔ Du kan tage det roligt

- Chat

➔ Skal det anmeldes?
➔ Links til yderligere professionel hjælp

- Apps
- Kodeord ord og Multifaktor godkendelse (MFA)

➔ Første overvejelse
➔ Næste overvejelse
➔ Online kodeords tjenester
➔ Offline kodeords manager.
➔ 2 Faktor godkendelse

➔ Multi Faktor godkendelse
➔ Links til officielle guides og koder.

- Rejse sikkererhed

➔ Hvad er jeg bekymret for ?
➔ På rejsen
➔ Netværk og gratis hotspots
➔ VPN hvad er det ?
➔ Rejserouter
➔ Backup af rejsedata / papir / pas
➔ Kryptering og USB
➔ Egen VPN tjeneste
➔ Backup af data
➔ Versionering af backup og filer
➔ Backup rutine
➔ Deling af filer
➔ Lagerplads
➔ Gratis vs. Betalingstjeneste
➔ Online vs Offline
➔ Online backup
➔ Versionering af backup og filer
➔ Backup rutine
➔ Deling af filer
➔ Lagerplads
➔ Gratis vs. Betalingstjeneste
➔ Online vs Offline (NAS)
➔ Genskabelse (hastighed og tilgængelighed)
➔ Placering af data
➔ Kryptering af data
➔ Bittorrent sync

5. Falske Opkald

Der er mange borgere i danmark, som oplever at bliver ringet op af fremmede, som bebuder at de kommer fra en stor techvirksomhed, som eks. Apple, Microsoft mv.

De oplyser at du har virus på din PC og vil meget gerne hjælpe dig med at fikse problemet. Hvilket jo lyder rigtigt fint, men er roden til en dårlig oplevelse.

Deres virkemiddler er, at de presser på og understreger vigtigheden af de skal have adgang for, at kunne fikse dig problem. De snakker ofte om hackere og udenlandske aktører for at det skal lyde mere farligt.

Deres telefonnummer er ofte fra udlandet og har et langt nummer.

5.1 Du kan tage det roligt

Hvis du bliver ringet op, så tag det roligt.

Spørg specifikt ind til hvad det er for en virus, det være sig navn, link til online hjemmeside, karakteristika, hvad den gør. Vær vedholdene, for de kan ikke svare 🙂

Oplys ikke noget personligt, som eks. bankoplysninger eller login til nemid eller lign. Det er det som de går efter.

Giv aldrig adgang til din PC. Får de adgang, så går de efter dine loginoplysninger og forsøger med din egen

hjælp at logge på din netbank. Derfra vil de begynde at flytte rundt på penge og samtidig oplyse dig, at det er for din egen beskyttelse.

Spørg dem hvad en lastbil siger når den bakker ? og læg røret på. Alternativt spild deres tid.

Eksempel her

6. Chat

Overalt hvor vi færdes har chat og beskedtjenester poppet op. De unge mennesker kommunikere på et utal af platforme og hertil kommer der flere og flere nye tjenester op hverdag.

Jeg abstrahere her på siden fra tjenesten og fokusere på hvad man med enklte virkemiddler kan gøre for at sikre sig uanset hvor man bevæger sig.

Det behøves ikke at blive understreget, at man ikke skal dele informationer på tjenester hvor man ikke kender modtageren, og heller ikke selvom man kender modtageren. Skal noget deles er det en god ide, det sker i den fysiske verden. Vel vidende, at noget kan være nemmer at dele på en besked.

Hvis skaden er sket? Hvis uheldet er ude, så er det vigtigste her, at REAGERE !

Gemmer man sig og tror problemet forsvinder, så tager man fejl. Det vigtigste er, at man dokumentere hvad der sket og hvordan det er sket og hvor det er sket. Så præcist som muligt.

Vent med at slette beskeder, det er vigtige beviser hvis der skal afhjælpes et problem. Det er uanset om nyndighederne er involveret eller ej!

Dokumenter hvad der sket optagelser, Screenshots, billeder eller beskeder fra de medier som er anvendt.

Optagelser kan udføres på en windows PC ved at taste **Win + ALT + r** for at optage. På mac **CMD+SHIFT+5**

Screenshots kan som regel tages med volume ned og funktions knappen. Sket på print scr knappen.

Billeder kan være taget med **digital kamera eller anden mobil**. Lavpraktisk og effektivt.

Beskederne skal man ikke slette, så har man dem som bevis.

Få **mor eller far, pædagog, skolelære med andre ord en voksen** til at hjælpe med at tage affære!

6.1 Skal det anmeldes?

Hvis der er sket billede deling af seksuel karakter og der er tale om billeder med mindreårige. Så vil jeg mene det skal anmeldes, er man i tvivl, så anmeld og dokumenter.

Politiet kan hjælpe med at vurdere omfanget. De har også ressourcer til at kunne tage affære. Pas på med at dele billeder og oplysninger på de åbne medier om folk. Det kan være fristende, men du kan ende i problemer for at dele informationerne og krænke krænkeren. Ja det er vildt, men sager som dette har der været mange af. Tag hellere en snak i foreningen, skolen, arbejdet mv. **Undlad de åbne medier, da det har konsekvenser begge veje.**

Anmeldelsen kan ske her til Politiet

6.2 Links til yderligere professionel hjælp

Børnsvilkår

Sikreside

Sikkerdigital

7. Apps

Hvis du er forældre og skal følge med de unges vaner hvad nye apps angår, så er det en udfordringer er større end de fleste. Det skifter hurtigere end vi andre skifter sokker.

Der er mange ting man kan gøre for at blive klogere på hvad det er for nogle apps.

Kig på indstillingerne som regl de 3 streger eller tandhjulet. Se hvad du har muligheder for at indstille. Som eks. lokation, deling af billeder og video mv. Har man ikke mulighed for dette? så er det måske en indikation for at den app ikke er så god. Kigger man i indstillingerne, så bliver man ofte overasket over hvor meget man deler.

Google er din ven her. Fordi alle andre gør det, så er det ikke nødvendigvis en god ide. Google kan fortælle dig, om der er andre som dig, der har lavet en gennemgang af appen.

Eksempelvis har fyiplayitsafe og business insider kigget på tiktok. Som mange unge mennesker bruger. Min personlige overbevisning, så er det ikke verdens bedste app, af mange årsager. Linket beviser meget godt min bekymring.

Kodeord er et nødvendigt onde og svært at komme uden om. Der findes mange måder at huske, oprette og gemme koder på.

Er man totalt paranoid, så er man tilbøjelig til at skulle huske alle koder i hovedet, så Internettet er skrevet ned. Det er muligvis den bedste løsning. Har man over 50 koder, så kan det godt være den strategi ikke bliver så let mere.

8. Kodeord ord og Multifaktor godkendelse (MFA)

8.1 Første overvejelse

Det første man skal gøre op, hvad er det værste der kan ske hvis jeg ikke har et stærkt og unikt kodeord? er det til privat eller arbejdsbrug?

- ➔ Stærkt fordi, det skal ikke være let at knække
- ➔ Unikt fordi du skal kun bruge din kode 1 sted. Så bliver det kompromitteret, så er det kun 1 sted du skal genoprette koden på og ikke 10 steder.
- ➔ Arbejde versus ikke arbejde. Det er anbefalsesværdigt at man opsplitter de 2 ting, så hvis man er rigtig uheldig, så udstiller man ikke private koder sammen med arbejdskoder og derved minimere skaden.

8.2 Næste overvejelse

Det næste man skal gøre op med sig selv, er om man skal anvende kodeordsmanager, som skal være offline eller online? eller huske koderne?

8.3 Online kodeords tjenester

For almindelige brugere så vil en kodeordsmanager være at foretrække. Det er de, på grund at de virksomheder som sælger denne service, lever af at lev-

ere sikkerhed og de holder deres tjeneste opdateret og sikker.

Denne løsning her nævnt er online og koster penge. Som beløber sig til 75 – 200 kroner årligt, afhængigt at om det er til enkelt personer eller familie abonnementer.

Her til skal det nævnes, at det på det kraftigste anbefales, at anvende 2 Faktor (2FA) for at højne beskyttelsen for dine koder på sådanne tjenester. nedenstående er et par eksempler på tjenester.

Lastpass

Bitwarden

1 password

8.4 Offline kodeords manager.

Du kan gemme dine koder i et program, som kan ligge på et drev, USB eller andet steds. Det er en løsning der kan være rigtig god hvis du skal gemme koder på jobbet og kun være på jobbet for at kunne anvende dem.

Programmerne er ofte gratis. Foreskellen er her, at du skal huske at dine koder skal med på eks. en USB, hvis du skal på farten. Det kræver at man husker dem og at USB ikke ryger i vaskemaskinen og derved mistes data. Nedenstående er et par eksempler. Nogle af prgrammerne anvender også 2FA godkendelse

Keepass

Passwordsafe

8.5 2 Faktor godkendelse

Du kender 2FA fra nemid. Du taster kodeord og brugernavn og så derefter en 2 FA kode, for at verificere dig til hjemmesiden eller tjenesten. Det kræver at du har et kort, app, nøgle mv. for at identificere dig. Denne anden faktor kan være svær at identificere og kopiere for kriminelle, hvilket besværliggøre deres arbejde markant for, at hacke dig og dine koder.

8.6 Multi Faktor godkendelse

MFA (Multi Factor Authentication) er fremtidens måde, og ligner lidt ovenstående. Her anvendes flere faktorer som godkendelse. det kan eks. være fingeraftryk, app, nøgle, SMS med videre. Nedenstående er et par eksempler på 2FA og MFA

DUO

Yubi key

Microsoft MFA

Google MFA

Det kan være biometriske foranstaltninger også.

8.7 Links til officielle guides og koder.

CIS Password guide

Nist password guide

9. Rejse sikkererhed

Når man skal på rejse, så er det afslapning og hygge med familie, kæreste eller bare sig selv. Jeg har været i Asien nogle gange og har selv oplevet hvordan netværk kan være en befrielse at komme i nærheden af. Da netværk i de lande er knap så udbygget som i Danmark.

Her skal man netop være opmærksom, da ens parader er sænket. Her på siden kommer nogle konkret og lette bud at have med på rejsen, som øger din sikkerhed betragteligt.

9.1 Hvad er jeg bekymret for ?

Ret og slet, at miste mine data og blive bestjålet for kontanter via online svindel. Denne trussel er reel og tilstedeværende. Når du er på netværk du ikke kender, så ved du heller ikke hvem der kigger med. Det lyder måske som om jeg har sølvpapir hatten på, ja det har jeg. Spørg bankerne om hvor mange der er svindlet op til 1, 2 og flere år efter rejsen.

9.2 På rejsen

Når du skal på rejsen, så kommer der her nogle råd du kan tage med for en bedre og mere sikker oplevelse. Dette er ikke en 100% liste, jeg vil dog vove at påstå, at det kan fjerne mange hovedpiner fra din rejse og tiden efter hjemkomst. Du ved ikke hvem der

kigger med, og jo nedenstående sker derude og mere end du tror.

9.3 Netværk og gratis hotspots

Hvis du har rejst steder hvor dækning af netværket eller internettet har være dårligt, så er det ofte rart at kunne have et WiFi neværk man kan koble på, for at læse mails og surfe gode oplevelser i nærområdet.

Der er en lille hage her. Ofte er de netværk man besøger åbne for alle og en hver. Hvilket er her din hovedpine starter. De kriminelle ved godt at der kommer udlændinge, som har adgang til flere penge end de har, så der er folk derude, som forsøger at overvåge netværk i de områder hvor der er fri adgang, som f.eks. på hoteller og cafeer.

Den nemme løsning er at undgå disse netværk og anvende din teleudbyders internet (hvor det nu måtte være muligt, 3.dk har internetdækning via mobilen de fleste steder i verden). På den måde er du ikke på nettet og det er sværere at opsnappe trafikken mellem din enhed og det du surfer. Med mindre du er i et land med et regime der overvåger telenettet (Læs VPN).

9.4 VPN hvad er det ?

Skal du bruge netværket på stedet, som kan være usikkert. Så er der en simpel løsning der hedder VPN (Virtuel Private Network). Denne løsning giver dig mul-

igheden for at lave en sikret og krypteret forbindelse ud fra det usikre netværk du sidder på. Ved at kryptere den trafik der går ind og ud fra din computer eller telefon, så kan dem som lytter med på netværket ikke se hvad der bliver sendt frem og tilbage.

Sådan en løsning kan laves på mange måder. Der er tjenester som sælger VPN muligheder. Mange hjemmeroutere har også muligheden for at opsætte en openvpn forbindelse. Bemærk at dette vil kræve en statisk IP for at sikre sig at man kan logge på systemet hver gang. Du kan sagtens anvende en statisk adresse, blot husk på at du kan risikere din IP til routeren kan blive ændret.

9.5 Rejserouter

Den lette løsning på rejsen er en lille rejserouter. Med den lille router, forbinder du til eksisterende netværk og samtidig opretter du dit eget private netværk. Hvilket betyder at du kun forbinder til din router. Routeren håndtere således forbindelsen ud af huset. Det smarte her er at den kan anvende en VPN forbindelse, så alt trafik bliver sendt igennem denne VPN forbindelse.

Ovenstående er eksempler på routere til formålet fra Gli net Sådanne løsninger koster fra 250 til 800 D.kr. og fungere fint med op til 12-15 enheder via WiFi. forskellene består ofte i hastigheden, om der er 2,4 eller 5 gHz til rådighed. Har mulighed for TOR (The Onion Router) installeret og om der kan laves fildeling mv.

Personligt syntes jeg det er en god investering, da man kan sætte routeren hvor det bedste signal er, der fra kan man "repeate" signalet videre til dine enheder.

Lille Router Gl inet 150 Mellem router (på vej ud/stadig et godt køb) GL AR750 (slate) Største og nyeste GL MT 1300 (Beryl) via egen hjemmeside hvor der kommer moms.

12*Mit udvalg af rejseroutere... er måske gået all in ;)*

9.6 Backup af rejsedata / papir / pas

Backup af dine data, så det stadig er til at få fat i Skal man ud i den store verden, så kan backup af dine data være værdifulde, som eks. kopi af pas, kørekort, billetter mv.

Du kan ligge filerne på en cloudtjeneste, som du kan tilgå ved hjælp af internetforbindelse. Husk at sådanne data er følsomme data og bør krypteres, som f.eks. med programmer som boxcryptor.

Så er uheldet ude, så kan du stadig få data fra "skyen"

9.7 Kryptering og USB

En USB med ovenstående data, kan også være en nyttig ting.

Igen husk kryptering, så hvis du er uheldig at miste din USB, så kan disse data ikke misbruges. Du kan kryptere med Filevault (Mac), Bitlocker (Windows) eller LUKS (Linux). Der findes også løsninger fra Boxcryptor som er en nem og tilgængelig måde at opnå kryptering på.

Et billede fra et hotel i Hanoi Vietnam. Access point fordelt på alle etager. Simpel og ikke effektiv løsning. 🙂 Et par links til billige VPN tjenester.

Et tip, på stacksocial.com har de ofte tilbud på VPN og livstids abonnement, dvs man betaler 3-500 kroner for et abonnement og er en engangs betaling.

13*Billede fra et hotel i Hanoi Vietnam.... der er 5 routere til hver etage på en lang ledning fra loftet... Smart .. eller!! :D*

HUSK!!!

Inden du kaster dig afsted i et indkøbsgalore, så vokser træerne ikke himmelen.

Du kan risikere at opleve en hastigheds nedsættelse da det kræver trafikken til internettet skal krypteres og sendes ud af huset, for at du opnår en ny IP-adresse.

Betaler du for en VPN tjeneste, så låner du en andens udstyr med andre ord. Hvilket betyder at i teorien så kan tjenesteudbyderen se hvad du laver. Ja deres hjemmeside siger 100 anonymitet. Just saying !!!

Hvilken en er så bedst ? Aner det ikke !! .... Der er så mange at det er lige meget.

De større tjenester er Keepsolid (VPN unlimited)

9.8 Egen VPN tjeneste

Ovenstående routere kan også anvendes i hjemmet, som en VPN server. Da de har en service der understøtter Openvpn og Wireguard som begge er VPN tjenester og på mange punkter de-dacto standarden for de VPN tjenester der er derude.

Din router har måske allerede en openvpn server installeret, som kan aktiveres. Så kan du starter tjenesten og danne et certifikat, som kan flyttes til en anden PC og eller telefon. Husk lige om du har dynamisk eller statisk IP-adresse. Da en dynamisk IP-adresse kan finde på at skifte, hvilket ligger implicit i navnet.

Så vil du kunne koble på dit hjemmenetværk ude fra sikkert via en VPN. Husk, at er du i tvivl om hvad du laver her, så lad være med at aktivere noget som helst ! .... og spørg en ven!

> Er du i tvivl om du er komporomitteret? > > Så er du ikke i tvivl! > > Tag dine forholdsregler. Skift koder og betalingskort! > > Det fjerner meget hovedpine

9.9 Backup af data

Hvis du lige som jeg har en masse gode ferie billeder og måske et par videoer fra ferien. Eller vigtige filer i privaten eller på jobbet, så er en backup super vigtig. En backup er ikke bare en kopi af ens filer. Jeg vil her give et bud på nogle af de overvejelser der skal til for at du sikre dine minder og digitale ejendom.

Du skal naturligvis træffe din egen beslutning om hvordan du bakker dine data op. Nedenstående skal ses som nogle tanker omkring dette emne.

9.10 Versionering af backup og filer

En simpel men vigtig funktion er versionering. Hvis man laver en fejl og skal genskabe fra tidligere version, så er det her versionering kommer ind. Det kan være en god ting at have gamle versioner af sit dokument hvis man opdager fejlen senere i tiden.

Husk at se om en udbyder eventuelt måtte have den service. Det koster sikker lidt mere og kan være pengene værd. Det kræver også mere plads på systemet.

9.11 Backup rutine

En backup rutine er en vigtig del af hverdagslivet for private og virksomheder. For os private kan det være en god ide, at lave backups hver gang, at der bliver foretaget en ændring til en fil, hvilket betyder at man sender filen til sin backuptjeneste. På den måde opnår du tæt på realtime backup.

9.12 Deling af filer

At have en backup funktion er en ting, men nogle gange kan det være rat at have muligheden for at dele store filer. Du kender sikkert at du skal sende videoen fra ferien til familien og nu bliver du begrænset i at kunne sende kun 20 mb hvor filen fylder 1 gb.

Så kan man hos mange tjenester oprette et delings link og sende linket i mailen og derved dele filer der er langt større end det som tjenesteudbyder tillader (som eks gmail.com og live.com). Det er en funktion der er ret almindelig i dag hos de fleste udbydere, men værd at have i tankerne.

9.13 Lagerplads

Ikke uvæsenlig funktion. Man betaler ofte for den mængde af plads man bruger. Der findes nogle tjenester som tilbyder ubegrænset backup. HUSK at læse det med småt, for der kan være begrænsninger i deres services og nogle udbydere kan finde på at ændre deres services, selvom man har købt en tjeneste.

Har selv på et tidspunkt anvendt en service som i dag er lukket. Servicen hed Bitcasa og tilbød ubegrænset plads for noget der lignende 700.- D.kr. om året hvilket var billigt på tidspunktet. De druknede i egen success om man så må sige. Så det resulterede i at mange brugere, incl. mig selv blev utilfreds og smuttede fra dem. Så huske det med småt.

9.14 Gratis vs. Betalingstjeneste

Gratis har en pris = vores data. Tjenester som dropbox, googledrev mv. kan være fint hvis man har filer der skal deles eller gemmes online. ofte er man begrænset af mindre mængde af data der kan gemmes, eller sende. Betaler man for tjenesten, så er der ofte mere plads, flere funktioner og ens data er dine data. Tidligere har Google fotos, måtte bruge dine fotos til reklameformål uden at spørge om lov, efter som man indgik den aftale med google imod at bruge deres tjeneste gratis (ved i skrivende stund ikke om det er sådan mere)

9.15 Online vs Offline

NAS betyder Network Attached Storage og er en slags harddisk på dit neværk. Du kan se dine filer ved at skrive IP-adressen. Så kan du se filerne som var det på dine lokale computer.

Offline

→ Du har filerne lokalt og er hurtigt at overføre

- → Du har kontrol over hvor filerne er placeret og hvem der har adgang *
- → Du betaler kun en gang for det hardware du har stående
- → Dit hardware har ofte flere funktioner indbygget (server, backup, noteblok, "lokal cloudtjeneste" med mulighed for at redigere dokumenter)

- → Systemet har ofte et raidsystem som gør at hvis disken står af kan du skifte den. Hvis raid controlleren står af, så dør hele systemet.

Du kan tilgå tjenesten via producentens app via mobiltelefonen. Det kan nogle gang give lidt udfordringer, da man utilsigtet får delt filer med resten af verden uden man ved det. Derfor skal man have adgang til filerne uden for ens netværk, så skal man overveje en VPN forbindelse. Så man opretter en sikkerforbindelse hjem til dit netværk, hvor dine filer er.

- → Kører 24/7/365 og koster strøm og larmer
- → Koster mange penge hvis man skal have et system med meget plads
- → Kræver en hurtig Internetforbindelse med høj upload hastighed, hvis du skal sende filer ud af huset.
- → Går udstyret ned, så kræver det en sekundærbackup, som en online tjeneste eller offsite (NAS på anden lokation)
- → Kræver netværksopsætning for deling ud på internettet og gøres det forkert, så kan man gøre sit netværk usikkert.

Ovenstående kan kombineres med nedenstående. hvis du har en computer der er koblet op til NAS. Herfra kan man sætte sin backup til at synkronisere til tjenesten.

9.16 Online backup

Plusser

- ➔ Kører i baggrunden ved hjælp af et program/service hvor du vælger dine mapper og filer du vil backe up. Ret nemt at konfigurere
- ➔ Kan køre med versionering af filerne.
- ➔ Du kan dele filerne med links og har en hurtig forbindelse til download
- ➔ Mange tjenester er "installere og glem", da de selv klare backupdelen.
- ➔ Du skal ikke selv rode med opdateringer og konfigurering, det er sat op for dig.

Minusser

- ➔ Koster et abonnement
- ➔ kræver en hurtig upload hastighed, da filer synkroniseres med tjenesten.
- ➔ Kan tage lang tid og genskabefiler, i tilfælde af nedbrud. (Nogle tjenester tilbyder at sende en harddisk via posten, som nogle gange kan være hurtigere)
- ➔ Man er ikke i kontrol over hvor data ligger. Anvender man amerikanske tjenester, så er servicen ikke så god, som sammenlignet med tjenester inde for

vores egene himmelstrøg. (Som hvis man skal have logs eller support fra dem)
- ➔ Tager lang tid at backe up, hvis man har mange filer, og det kan ødelægge internettets hastighed i hjemmet, mens man overføre filer.
- ➔ ofte er der en begrænsning på hvor meget data man kan have. (det variere ofte er det 1 - 5 TB data, som ofte er rigeligt for de fleste)

Hvis du lige som jeg har en masse gode ferie billeder og måske et par videoer fra ferien. Eller vigtige filer i privaten eller på jobbet, så er en backup super vigtig. En backup er ikke bare en kopi af ens filer. Jeg vil her give et bud på nogle af de overvejelser der skal til for at du sikre dine minder og digitale ejendom.

Du skal naturligvis træffe din egen beslutning om hvordan du bakker dine data op. Nedenstående skal ses som nogle tanker omkring dette emne.

9.17 Versionering af backup og filer

En simpel men vigtig funktion er versionering. Hvis man laver en fejl og skal genskabe fra tidligere version, så er det her versionering kommer ind. Det kan være en god ting at have gamle versioner af sit dokument hvis man opdager fejlen senere i tiden.

Husk at se om en udbyder eventuelt måtte have den service. Det koster sikker lidt mere og kan være pengene værd. Det kræver også mere plads på systemet.

9.18 Backup rutine

En backup rutine er en vigtig del af hverdagslivet for private og virksomheder. For os private kan det være en god ide, at lave backups hver gang, at der bliver foretaget en ændring til en fil, hvilket betyder at man sender filen til sin backuptjeneste. På den måde opnår du tæt på realtime backup.

9.19 Deling af filer

At have en backup funktion er en ting, men nogle gange kan det være rat at have muligheden for at dele store filer. Du kender sikkert at du skal sende videoen fra ferien til familien og nu bliver du begrænset i at kunne sende kun 20 mb hvor filen fylder 1 gb.

Så kan man hos mange tjenester oprette et delings link og sende linket i mailen og derved dele filer der er langt større end det som tjenesteudbyder tillader (som eks gmail.com og live.com). Det er en funktion der er ret almindelig i dag hos de fleste udbydere, men værd at have i tankerne.

9.20 Lagerplads

Ikke uvæsenlig funktion. Man betaler ofte for den mængde af plads man bruger. Der findes nogle tjenester som tilbyder ubegrænset backup.

HUSK at læse det med småt, for der kan være begrænsninger i deres services og nogle udbydere kan

finde på at ændre deres services, selvom man har købt en tjeneste.

Har selv på et tidspunkt anvendt en service som i dag er lukket. Servicen hed Bitcasa og tilbød ubegrænset plads for noget der lignende 700.- D.kr. om året hvilket var billigt på tidspunktet. De druknede i egen success om man så må sige. Så det resulterede i at mange brugere, incl. mig selv blev utilfreds og smuttede fra dem. Så huske det med småt.

9.21 Gratis vs. Betalingstjeneste

Gratis har en pris = vores data. Tjenester som dropbox, googledrev mv. kan være fint hvis man har filer der skal deles eller gemmes online. ofte er man begrænset af mindre mængde af data der kan gemmes, eller sende.

Betaler man for tjenesten, så er der ofte mere plads, flere funktioner og ens data er dine data.

Tidligere har Google fotos, måtte bruge dine fotos til reklameformål uden at spørge om lov, efter som man indgik den aftale med google imod at bruge deres tjeneste gratis (ved i skrivende stund ikke om det er sådan mere)

9.22 Online vs Offline (NAS)

Det er altid det store spørgsmål. Der er fordele og ulemper ved begge dele. jeg har nedenstående fors

øgt at ridse op hvad der er fordele og ulemper. Listen er ikke uudtømmelig.

NAS betyder Network Attached Storage og er en slags harddisk på dit neværk. Du kan se dine filer ved at skrive IP-adressen. Så kan du se filerne som var det på dine lokale computer.

Offline

- ➔ Du har filerne lokalt og er hurtigt at overføre
- ➔ Du har kontrol over hvor filerne er placeret og hvem der har adgang *
- ➔ Du betaler kun en gang for det hardware du har stående
- ➔ Dit hardware har ofte flere funktioner indbygget (server, backup, noteblok, "lokal cloudtjeneste" med mulighed for at redigere dokumenter)

– Systemet har ofte er "raid" system som gør at hvis disken står af kan du skifte den. Hvis raidkontrollern står af, så dør hele systemet. – Du kan tilgå tjenesten via producentens app via mobiltelefonen. Det kan nogle gang give lidt udfordringer, da man utilsigtet får delt filer med resten af verden uden man ved det. Derfor skal man have adgang til filerne uden for ens netværk, så skal man overveje en VPN forbindelse. Så man opretter en sikkerforbindelse hjem til dit netværk, hvor dine filer er. – Kører 24/7/365 og koster strøm og larmer – Koster mange penge hvis man skal have et system med meget plads – Kræver en hurtig Internetforbindelse med høj upload hastighed, hvis du skal sende filer ud af huset. – Går udstyret ned, så

kræver det en sekundærbackup, som en online tjeneste eller offsite (NAS på anden lokation) – Kræver netværksopsætning for deling ud på internettet og gøres det forkert, så kan man gøre sit netværk usikkert.

Ovenstående kan kombineres med nedenstående. hvis du har en computer der er koblet op til NAS. Herfra kan man sætte sin backup til at synkronisere til tjenesten.

Online

- ➔ Kører i baggrunden ved hjælp af et program/service hvor du vælger dine mapper og filer du vil backe up. Ret nemt at konfigurere
- ➔ Kan køre med versionering af filerne.
- ➔ Du kan dele filerne med links og har en hurtig forbindelse til download
- ➔ Mange tjenester er "installere og glem", da de selv klare backupdelen.
- ➔ Du skal ikke selv rode med opdateringer og konfigurering, det er sat op for dig.

– Koster et abonnement – kræver en hurtig upload hastighed, da filer synkroniseres med tjenesten. – Kan tage lang tid og genskabefiler, i tilfælde af nedbrud. (Nogle tjenester tilbyder at sende en harddisk via posten, som nogle gange kan være hurtigere) – Man er ikke i kontrol over hvor data ligger. Anvender man amerikanske tjenester, så er servicen ikke så god, som sammenlignet med tjenester inde for vores egene himmelstrøg. (Som hvis man skal have logs eller support fra dem) – Tager lang tid at backe up, hvis

man har mange filer, og det kan ødelægge internettets hastighed i hjemmet, mens man overføre filer. – ofte er der en begrænsning på hvor meget data man kan have. (det variere ofte er det 1 – 5 TB data, som ofte er rigeligt for de fleste)

9.23 Genskabelse (hastighed og tilgængelighed)

Skal du genskabe dine data, som jo sagtens kan se. Så er det en god ide, at se hvordan ens tjenesteudbyder gør dette. Det kan ofte tage lang til at downloade filerne igen. Som beskrevet ovenstående, så er det måske en fordel, at du kan få tilsendt en harddisk.

9.24 Placering af data

Ikke uvæsentlig for hvordan dine data bliver opbevaret. Jeg vil til hver en tid anvende en tjeneste hvor jeg ved at mine data er inde for Skandinavien. Da jeg underviser på KEA, så kan jeg sagtens anvende Google som tjenesteudbyder, for at opnå brugervenlighed og tilgængelighed. De data jeg gemmer her, er heller ikke personlige eller kritiske. Mine personlige data som billeder og filer vil jeg ikke gemme på sådanne tjenester, af den grund, jeg ikke ved hvem der reelt har adgang til data.

9.25 Kryptering af data

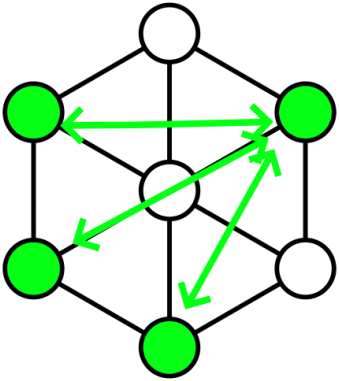
Har man data man vil passe særligt godt på. Så kan man anvende service som kryptere ens filer med god kryptering (AES 256). På den måde sikre du dig imod at andre kigger med.

Boxcryptor er en tjeneste man installere på de systemer hvor man vil sikre data. Når det er installeret, så kryptere boxcryptor alle ens data inden data forlader ens computer. Så har du stadig kontrol over data og ikke andre kan kigge med.

9.26 Bittorrent sync

Dette her er lidt kontroversielt, da man deler data via bittorrent. Bittorrent er en fildelings metode hvor man deler filen en til en, eller en til mange. Jo flere der har en fil, jo flere mere hastighed vl man kunne dele med. Da man splitter netværks belastningen ud. Kræver der er flere systemer (computere) som er online og tændt samtidig for at man kan opnå den ønskede effekt.

Nedenstående illustration viser tanken bag.



Bittorrent Sync (Resilio.com)

Er en af de tjenester der kan tilbyde softwaret, som du selv skal installere. Nogle vil mene at softwaren ikke er sikkert nok!

9.27 Litteratur

Litteratur SIR og Governance på KEA Nedenstående er den litteratur som bliver anvendt i faget. Der tages

forbehold for fejl og ændringer.

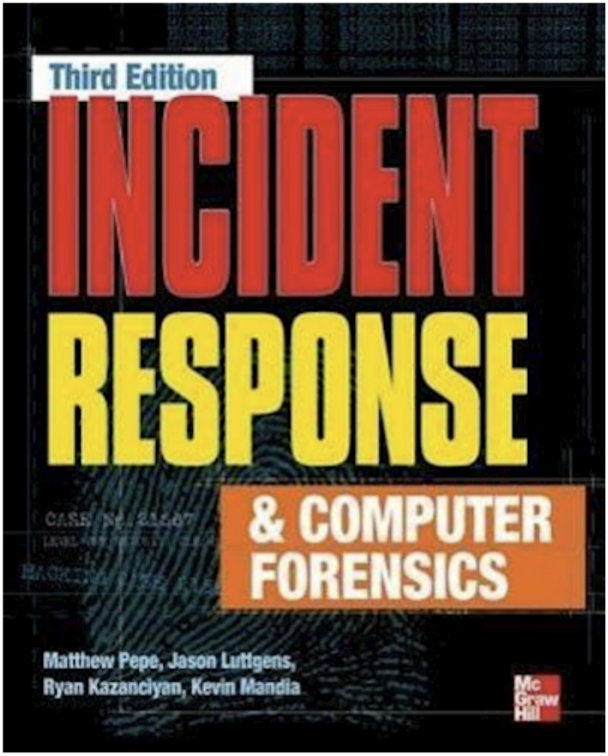
9.27.1 Download this webpage as E-book

I have compiled the webpage into a E-book, so you can use it at your disposal.

dfir knowledge stop bad things (PDF, 14.45 MB)

9.27.2 Security Incident Response – SIR

In my education i use the book "Incident Response & Computer Forensics, Third Edition"



Paperback : 642 pages ISBN-13 : 9780071798686

Image borrowed from Amazon This book goes hand in hand with the way I am trained in the field. I think it

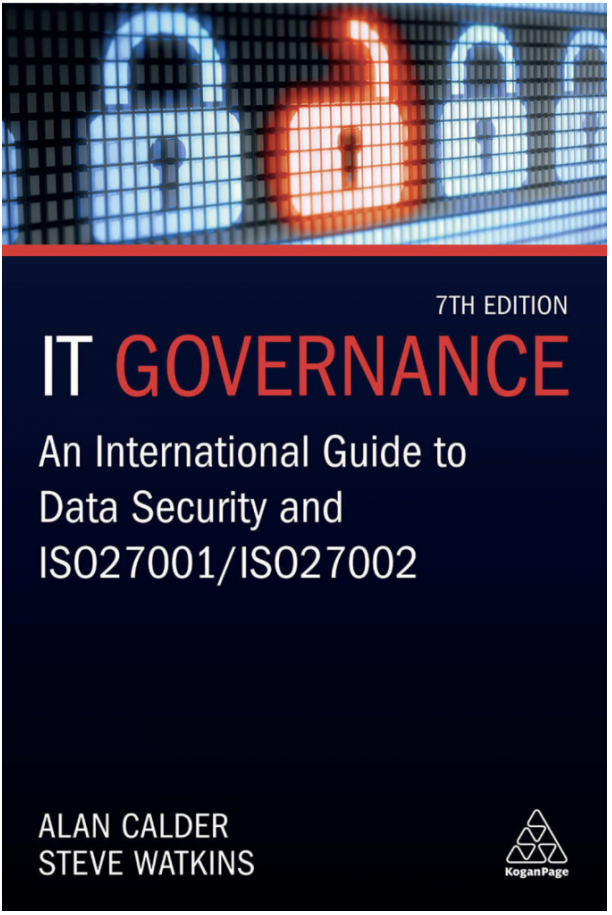
has many good elements, which are worth their weight in gold in SIR/DFIR.

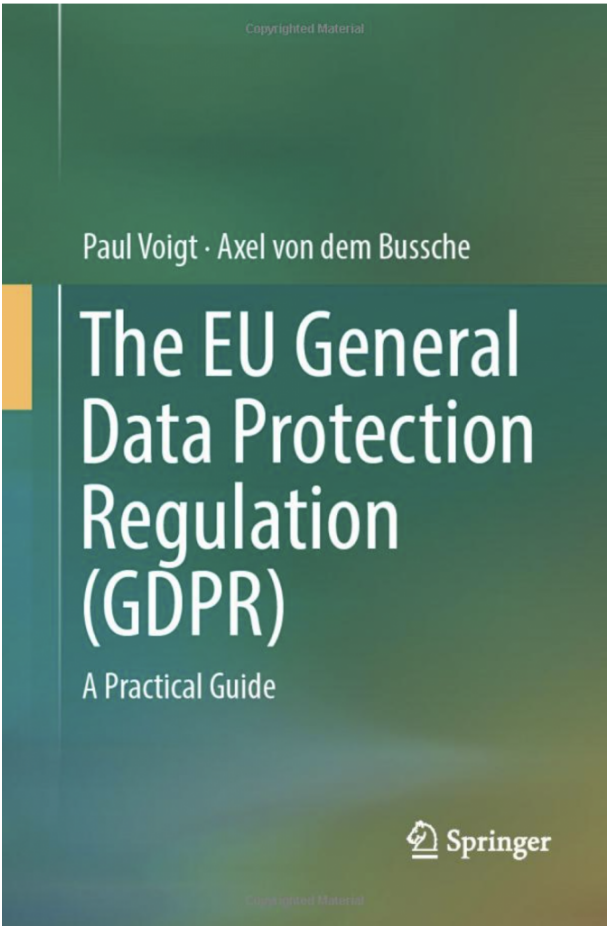
9.27.3 Governance

I faget Governance anvendes 2 bøger

De giver en god introduktion til selve faget og er skrevet af 2 herrer inde for feltet. Som har haft med dette emne/r at gøre i mange år.

IT-governance og GDPR

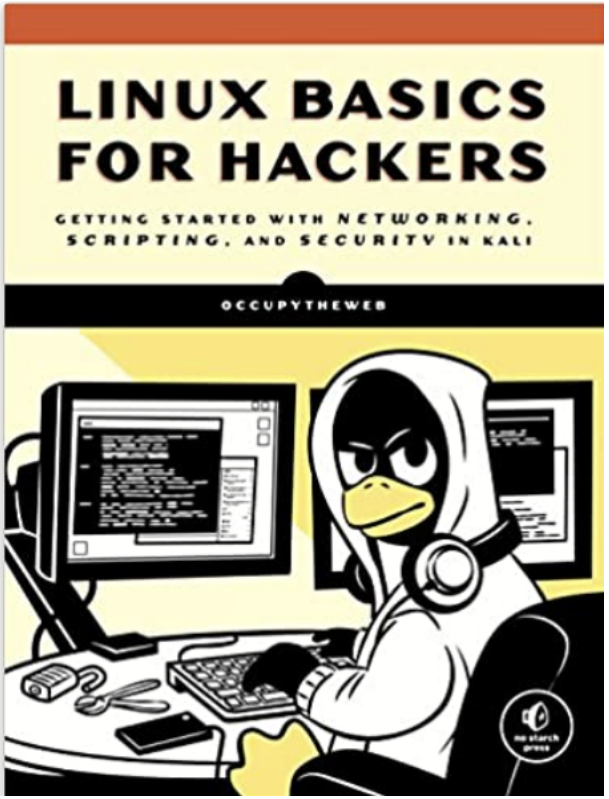

7TH EDITION
IT GOVERNANCE
An International Guide to Data Security and ISO27001/ISO27002
ALAN CALDER
STEVE WATKINS
KoganPage


Copyrighted Material
Paul Voigt · Axel von dem Bussche
The EU General Data Protection Regulation (GDPR)
A Practical Guide
Springer
Copyrighted Material

Billede lånt fra amazon

9.27.4 Linux

Hvis du ikke har arbejdet i Linux, så kan det være en fordel, at du investere i en bog som kan guide dig. Bliver anvendt i andre fag også.



Kan købes her [på Amazon]

9.27.5 Nice 2 haves

Her er et par eksempler på andre gode bøger som giver et godt indblik i ovenstående. Det er ikke påkrævet, det er blot nogle af de bøger jeg læner mig op af også.

Malware analysis

Practical Malware Analysis

Computer forensics

Incident respons (2014)

En anbefalses værdig bog, som er en investering værdig! must have, hvis du kigger i retning af DFIR

Applied Incident Response

Practical Cyber Forensics

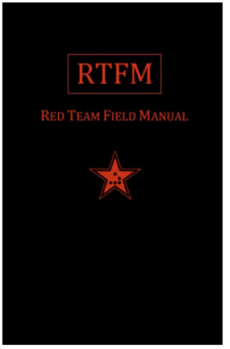
9.27.6 Opslags bøger

Nedenstående bøger er gode opslagsværker, som kan være rare at have.

Billeder lånt fra Amazon.co.uk

Billeder lånt fra Amazon.co.uk

Blue Team Field Manual (Godt opslagsværk, som tager udgangspunkt i det OS der er til rådighed, uden man skal installere ekstra software)



Blue Team Field Manual (Godt opslagsværk, som tager udgangspunkt i det OS der er til rådighed, uden man skal installere ekstra software)

Red Team Field Manual (samme her, et godt opslagsværk, som tager udgangspunkt i det OS der er til rådighed, uden man skal installere ekstra software)

Purple Team Field Manual (Ved ikke helt hvad denne er endnu, Det er en ny bog og den er bestilt 🙂)

Operators Handbook (Godt opslagsværk, men lidt uoverskueligt sammenlignet med ovenstående)

9.28 Backup

Her kommer min personlige holdninger om backup. længere nede kan du se læse om kryptering.

Nogen gange er det bedre med en video. Christopher Barnat der har kanalen på Youtube "Explaining Computers". Har lavet en udemærket video om emnet og det gode ved den video er, at tankegangen passer på rigtigt mange mennesker og mindre virksomheder (faktiske også de store).

Der er tale om nogle få grundprincipper. Her får du en intro til 3-2-1 princippet.

9.29 Mine anbefalinger

9.29.1 Jottacloud

Jottacloud er et rigtigt godt bud på en god cloud løsning der ligger fysisk i skandinavien, nemlig Norge. Det fungere ved at du kan installere en app der sikre at alle filer bliver backuppet live, så du ikke skal tænke på yderligere. Du har adgang via appen eller websiden.

Prisen er i skrivende stund 690.- D.Kr. om året for ubegrænset backup (for 1 bruger). Der finde familie abonnementer, som går fra 1 til 10 terabytes. Hvilket koster 50 til 370 D.Kr. per måned. Det kan naturligvis virke dyrt, men taget i betragning at der er rigeligt med plads for størstedelen af brugeren for 1 terabyte. Så er min personlige holdning, at det er billigt.

Sikkerheden kan altid diskuteres "er jeg så sikker". I forhold til backup og genskabelse, ja så er servicen ret stabil og der er version styring, så man kan rulle tilbage til tidligere versioner, hvilket kan komme til brug ved fx ransomware.

Kan jottacloud se med i mine filer? Teoretisk set ja. Det er svært at påvise de ikke kan, da filerne bliver krypteret i transit (når de sendes) og også når de ligger på serveren (hvilket kun er over for 3 part). Jottacloud besidder krypteringsnøglerne og kan per definition kigge med i dine gemmer.

Om de gør det eller ej, ved jeg ikke. Det kan dog undgåes forholdsvis let og enkelt. Læs lidt længere nede på siden. Det beskriver jeg boxcryptor, som er en tjeneste der tilbyder kryptering af filer til netop cloud tjenester, uanset hvor de ligger.

9.29.2 Pcloud

Pcloud er en rigtig god leverandør af cloud tjeneste og lager. Det er lidt ala Jottacloud, men ligger i Schweiz og er også det de kalder en sikker cloud.

Pcloud har som jottacloud en app der kan backup, eller sende filer til cloudtjenesten. Programmet opretter et virtuelt drev på ens computer, som var det en ekstra harddisk. Hvilket er smart, for så kan du tilgå alle dine filer direkte fra cloudtjenesten.

Grunden til jeg nævner Pcloud er at de går skridtet videre i forhold til deling og sikkerhed.

Kryptering, tilbydes ved et tilkøb. Det giver adgang til en krypteret mappe, som du kender nøglen til. Det gør at dine filer kan ligge på deres cloudtjeneste, hvor Pcloud ikke kan kigge med. Det er lidt et modsvar til boxcryptor, bare bygget ind i deres tjeneste og fungere ret godt.

I forhold til deling, så kan du dele et link med andre og sætte kode, udløbsdato på, hvilket ikke er muligt i jottacloud, som det er i dag. Du kan oprette en mappe og modtage filer i denne fra andre. Det kræves desværrer at dem der skal sende filer til dig, skal have en konto hos Pcloud. Det kan man dog få gratis, men alligevel en bøvlet måde, i forhold til fx Onedrive som kan modtage filer i en mappe uden man skal oprette koder eller lignende.

9.29.3 Boxcryptor

Boxcryptor er en billig og nem løsning på kryptering. Tjenesten opretter et virtuelt drev på din PC eller Mac (og linux ved en portable installation). De filer der ligger dernede, bliver krypteret med AES256 kryptering (sikreste kryptering for forbrugere).

Når du arbejder med filerne hernede i mappen, så bliver de krypteret løbende. Det bevirker, at hvis du synkronisere dine filer med en cloud tjeneste, så er der ikke nogen af de tjenester der har adgang eller kendskab til dine krypterings nøgler. Det gør at du kan vælge den udbyder du syntes, uden at skulle spekulere på om andre kigger med.

9.29.4 Kryptering

Skal man benytte kryptering? svaret er afhængigt af hvad du skal gemme? Er der tale om følsomme data, så vil jeg anbefale kryptering. Hvordan du skal kryptere, er helt op til dig.

Veracrypt er en gratis løsning derude, som også opretter et virtuelt drev eller fuld disk kryptering på din PC eller Mac. Tag et kig på det som alternativ til boxcryptor.

Du kan finde videoer for begge løsninger på youtube, af den grund vil jeg ikke skrive så meget om det her.

9.30 Linux

9.30.1 Intro til Linux

Har du ikke arbejdet med Linux før. Så ved jeg godt at det kræver lidt ekstra arbejde for at lige komme i gang med det. Det godet er, at der er masser at hjælp på nettet og mange af tingene er ikke så svære som det kan se ud.

Først og fremmest så er Linux gratis og open source. Det er anderledes i forhold til Windows, på udseende, funktion og system krav mv. Så selv om mange af tingene ligner, så er der en stor forskel. Linux kræver ikke så mange ressourcer, som Windows. Hvilket bevirker, at du kan puste liv i en gammel PC. Du har sikkert hørt den sætning før? ... men det passer faktisk.

Det kommer også til udtryk i klassen, når vi skal rode med Terminalen (Se længere nede).

Der findes mange forskellige versioner af Linux, af udseende, installeret software. Som i Linux kaldes pakker. Måden man styre de pakker på er forskellig fra version til version af Linux. Hertil kan nævnes at der findes RPM (Redhat Package Manager) og DPKG (Debian Package). I overordnede træk er det måden systemerne styre deres software pakker.

I klassen arbejder vi med Debian baserede Linux (eksempelvis Ubuntu, Linux mint, Debian, Remnux mf.).

9.30.2 Terminalen

Terminalen er der hvor jeg syntes Linux har sin magt. For mange også en lille tur op af bakke. Da det er mange nye kommandoer, flag og måder at arbejde med en usexet tekstboks på, da du som læser det her, sikkert er vant til Windows eller Mac (som også har en terminal).

Nedenstående er et eksempel på hvordan en terminal ser ud. Også kaldt Command Line Interface (CLI)

```
lablo@linuxserver$ Sudo apt-get update
```

9.30.3 Video

![Intro til linux]

9.31 Om mig

9.31.1 Hvad er Defencia?

Det er en sammensætning af Defence og CIA (Confidentiality - Integrity - Avalibility)

Nedenstående er taget fra mit andet site og forklarer lidt om mig.

9.31.2 Hvad er skrivebeskyttet?

Skrivebeskyttelse er den skriveblokering, man sætter mellem en harddisk og en computer, når man sikre data. Derved ændres der ikke på harddiskens tidsstemplinger.

9.31.3 Hvorfor det skrivebeskyttet?

Syntes det indikere på en sjov måde emnet.

9.31.4 Hvorfor denne side ?

Jeg ville gerne have en side hvor jeg kan dele mine opgaver, viden og undervisnings materiale på KEA.

Denne her side er baseret på egen viden og erfaring. Jeg søger inspiration af de bedste inde for branchen, og respektere hvad andre kan og ved.

For mig er det sjovt at undervise og det er det jeg bruger min fritid på. Jeg syntes på mange måder viden og

læring skal deles, det er måden vi kan bedst forebygge og beskytte os imod angreb.

Hvis jeg kan inspirere en eller bare 2 til at undgå eller håndtere et angreb i virksomheden eller privaten.

Så er det mission accomplished!

9.31.5 Hvem er bag?

En almindelig dansker med interesse for Information og IT-sikkerhed og lysten til at dele den viden. ;)

9.32 Intelligence

Hvordan holder man trit med nyhedsstrømmen og nye upcoming trusler? Her kommer mit eksempel på hvordan man kan klare den opgave. Der er taget udg-

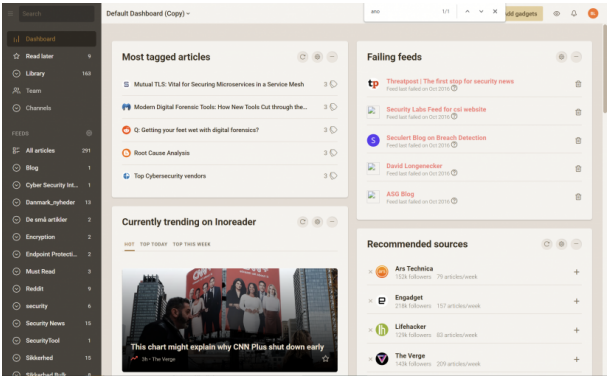
angs punkt i Inoreader og dens funktionalitet. Der findes andre derude som Feedly, blurnews fm. Du skal naturligvis vælge den du syntes bedst om.

Hvad er en nyheds RSS læser? Det er faktisk en teknologi som har været benyttet en del år og en af medstifterne af formatet er Aaron Swartz

RSS betyder Really Simple Syndication som oversat er en opdaterings strøm. Formålet er du kan "tilmelde" din en hjemmesides nyheds strøm og holde øje med nyheder, hver gang der publiseres noget nyt materiale eller historier. Det er jo smart, så kan du nemlig holde øje med mange hjemmesider på en gang. Det kræver dog at du har en RSS læser.

Jeg startede med den gamle gratis Google reader, som de slukkede for i 2011, hvilket var ærgerligt. Den var gratis og fungerede rigtigt godt. Sidenhen har jeg skiftet til Inoreader, som har en gratis version og en pro version. Jeg har taget udgangspunkt i pro versionen her, da den giver lidt flere features som er pengene værd efter min mening.

Prisen er ca 600.- kroner om året for pro servicen Se priserne her


Search
Default Dashboard (Copy)
Dashboard
Read later 9
Library 163
Team
Channels
FEEDS
All articles 291
Blog 1
Cyber Security Int... 1
Danmark_nyheder 13
De små artikler 2
Encryption 2
Endpoint Protecti... 2
Must Read 3
Reddit 9
security 6
Security News 15
SecurityTool 1
Sikkerhed 15
Most tagged articles
Mutual TLS: Vital for Securing Microservices in a Service Mesh 3
Modern Digital Forensic Tools: How New Tools Cut through the... 3
Q: Getting your feet wet with digital forensics? 3
Root Cause Analysis 3
Top Cybersecurity vendors 3
Failing feeds
Threatpost | The first stop for security news
Feed last failed on Oct 2016
Security Labs Feed for cui website
Feed last failed on Oct 2016
Seculert Blog on Breach Detection
Feed last failed on Oct 2016
David Longenecker
Feed last failed on Oct 2016
ASG Blog
Feed last failed on Oct 2016
Currently trending on Inoreader
HOT TOP TODAY TOP THIS WEEK
This chart might explain why CNN Plus shut down early
3h · The Verge
Recommended sources
Ars Technica
152k followers 79 articles/week
Engadget
218k followers 157 articles/week
Lifehacker
129k followers 82 articles/week
The Verge
143k followers 209 articles/week

10. Medlemsområde

for at se mere skal du være logget ind. For at få adgang skal du være deltager på KEA

10.1 Opgaver

Er kommer links til nogle af mine opgaver. Det vil også blive delt på fronter. **HUSK fronter er den formelle kommunikations kilde fra skolen**

10.2 Opgave 1 Download Frenzy

En god ide, er at oprette en e-mail som du kan benytte til registreringer, hvis du ikke vil modtage reklame fra virksomhederne efterfølgende. Har men en registrerings e-mail for virksomheden som alle kollegaerne kan logge på, så minimere i også at skulle modtage e-mails eller blive ringet op af alle mulige sælgere.

10.2.1 Forensics Software:

- ➔ FTK_Imager (gratis og kræver registrering) = https://accessdata.com/products-services/forensic-toolkit-ftk/ftkimager
- ➔ Autopsy (gratis) = https://www.autopsy.com/
- ➔ Autopsy Hashsæt = http://sourceforge.net/projects/autopsy/files/NSRL/
- ➔ Autopsy plugins = https://github.com/markmckinnon/Autopsy-

Plugins
- Caine linux (gratis) = https://www.caine-live.net/
- Rufus (gratis) = https://rufus.ie/
- Dumpit (gratis) = https://github.com/thimbleweed/All-In-USB/tree/master/utilities/DumpIt
- magnet axiom ram capture (gratis og kræver registrering) = https://www.magnetforensics.com/resources/magnet-ram-capture/
- Kape = https://www.kroll.com/en/insights/publications/cyber/kroll-artifact-parser-extractor-kape
- CyLR = https://github.com/orlikoski/CyLR
- Cyber chef = https://github.com/gchq/CyberChef
- Security Onion = https://securityonionsolutions.com/ (PCAP analyse)
- Wireshark = https://www.wireshark.org/download.html
- Bruteshark = https://github.com/odedshimon/BruteShark

10.2.2 Virtualiserings Software

Virtualbox (gratis) = https://www.virtualbox.org/ Eller VM ware (betalt) = https://www.vmware.com/dk.html

10.2.3 Diverse

7zip = https://www.7-zip.org/ (Evt som portable app = google portable apps) Hashtools = https://www.binaryfortress.com/HashTools/

10.2.4 Images til virtuelle maskiner

Windows 7 og 10 (gratis / 90 dages prøve licens for VMware og Virtualbox) = https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/ Remnux Linux (gratis) = https://remnux.org/

10.2.5 Log analyse

Splunk (gratis og kræver registrering) = https://www.splunk.com/ Netmon freemium (gratis og kræver registrering) = https://logrhythm.com/products/logrhythm-netmon-freemium/ SOF-ELK = http://for572.com/sof-elk-vm

10.2.6 Backup Image software (Ikke noget krav, nice to have)

Hvis noget skulle gå galt, er det en god ide, at have løbende backups af dine data. Det vil gøre en reetablering lettere

Der er flere muligheder. Jeg anvende terabyte for windows, som koster lidt, men er det hele værd. Link = https://www.terabyteunlimited.com/image-for-windows.htm

10.3 Opgave 2 Install Fest

Når Remnux linux og Win 10 Image er downloadet, så skal du have indlæst det i dit favorit virtualiserings værktøj

Installere/importere i Virtualiserings værktøjet

Importer Virtualbox https://docs.oracle.com/cd/E26217_01/E26796/html/qs-import-vm.html

Importer til VMware Open file og peg på filen og vælg import. Derefter kan filen slettes.

Dokumentere dine installationer / og fund Det er altid en god ide, at lave et lille skriv på hvor hentede du hvad. Det letter dit arbejde når du skal sætte andre ind i hvad du har haft arbejdet med, også som almindelig dokumentation af opsætning mv.

Allerede nu skal du hente SIR_tjeklisen og SIR_addendum fra fronter. Næste gang får du brug for den Tjeklisten er ikke 100% fuldstændig, du skal have noget ekstra papir ved hånden, så du kan dokumenter dine fint Klargør dit miljø

10.3.1 Opdater Remnux

(Husk det er engelsk keyboard)

10.3.2 Installer FlareVm

Åben op for overførsel Vmware Settings - shared folder, enable, vælg folder du vil dele og gem I gæste miljøet vælg stifinder og naviger til /MNT/Downloads og derfra kopier filerne til din ønskede mappe

10.3.3 Virtualbox

enable drag and drop Installere Programmer På din Host, installere FTK, Autopsy, Hashtools mv. af det du har downloadet. Opret en mappe med de tools som du skal bruge senere (eks. dumpit, 7zip mv)

10.4 Faserne - udvidet

Faserne er de perioder man som virksomhed skal igennem for at håndtere et angreb. Her får du omridset af faserne baseret på min egen erfaring (og lærebogens). Du kan få adgang til et mere detaljeret område hvis du er med i klassen

10.4.1 Forberedelse (Preperation)

Fredstid hvor man forbereder alle de aktiviteter og værktøjer (både software og hardware) inden noget når galt. her vil man også have styr på alle de dokumenter der skal benyttes under et angreb. Det er de planer, processer og procedure der kommer ud af et Incident.

Her snakker vi om sammenkædningen til governance,IT-sikkerhedspolitik, IT-beredskabsplan, IT-nedbrudsplaner og IT-angrebshåndtering

10.4.2 Identifikation og analyse fase (Identification)

Denne fase er når noget går galt. Der eskaleres til hvilken type incident, om det er sikkerheds relateret

eller almindelige nedbrud.

Når planen aktiveres, så er det baseret på en vurdering, af at det er sikkerheds relateret.

Der skal startes op med indsamling af data og identifikation af hvad der er sket og hvordan det er kommet ind. Der skal analyseres på hvordan de skadelige filer opføre sig. Hvad de laver af nye skadelige handlinger og hvilke domæner IP-adresser de kontakter.

10.4.3 Lockdown (Containment)

Når vi er blevet klogere på hvordan vi er ramt og hvad der er sket. Så kan vi begynde at kigge på hvordan vi udenytter vores viden til at blokkere for angrebet. Det kræver naturligvis at vi har nogle reskaber/teknologier til at assistere os med nedlukningen.

Et par eksempler.

Kender vi domæner og IP-adresser, så kan de blokkeres i fx DNS, Firewall, Proxy mv. Kender vi filer der bliver oprettet, så kan de blokkeres i antimalware løsningen på end points, servere, IPS mv. Kender vi filernes HASH, så kan de detekteres ved en scanning. Kender vi karakteristika, så kan vi oprette YARA regler, som giver en alarm når vi ser mønstre. (kun alarmering) Kender vi spredningen, så kan vi fx lukke for delte drev

Det er nogle af de eksempler på detektion og blokering. Det kan varierer fra hændelse til hændelse.

10.4.4 Recovery (Rollback / Restore)

Når vi har stoppet angrebet, så er det vigtigt for os, at vi kan finde ud af hvornår "dag nul" var. Det vil sige den skille dato, hvor vi kan identificere hvornår hændelsen fandt sted og vi kan genskabe fra før denne dato/tidspunkt

10.4.5 Monitor fase

Har man et angreb der har været mere omfattende, så kan man implementer en monitorfase.

Det kan være et par dage op til uger og måneder, hvor man intensivere sin overvågning. Sker der noget, så kan man trykke på "den store røde knap" og låse sit miljø ned igen, så man hæmmer en eventuel re-inficering.

10.4.6 Back to normal (Post incident / Lessons Learned)

Her påbegynder vi normal drift og afslutter selve forløbet /faserne.

Vi samles til et møde hvor man vender hvad der gik godt eller skidt. Får renset luften hvis det blev lidt hektisk. Der bliver samlet op på hvad vi lærte og derfra bliver der udarbejdet en rapport som opsummere på hvad vi lærte og hvordan det bliver indført i de planer vi har.

Så vi har en opdateret "Business Continual Plan " som giver virksomheden "Continual Service Improvement"

10.5 Medie filer

Indhold kommer når undervisningen kommer igang. Links kommer også på Fronter.

10.6 Forensic eksempel

Content

10.7 Windows CMD

Lige et par windows kommandoer. Nogle af dem er gode i tilfælde af, man skal kigge efter hvad der sket på sit udstyr.

* * *

Run commands

- Calc - Calculator
- Cfgwiz32 - ISDN Configuration Wizard
- Charmap - Character Map
- Chkdisk - Repair damaged files
- Cleanmgr - Cleans up hard drives
- Clipbrd - Windows Clipboard viewer
- Cmd - Opens a new Command Window (cmd.exe)
- Control - Displays Control Panel
- Dcomcnfg - DCOM user security
- Debug - Assembly language programming tool
- Defrag - Defragmentation tool
- Drwatson - Records programs crash & snapshots

- Dxdiag - DirectX Diagnostic Utility
- Explorer - Windows Explorer
- Fontview - Graphical font viewer
- Ftp - ftp.exe program
- Hostname - Returns Computer's name
- Ipconfig - Displays IP configuration for all network adapters
- Jview - Microsoft Command-line Loader for Java classes
- MMC - Microsoft Management Console
- Msconfig - Configuration to edit startup files
- Msinfo32 - Microsoft System Information Utility
- Nbtstat - Displays stats and current connections using NetBios over TCP/IP
- Netstat - Displays all active network connections
- Nslookup- Returns your local DNS server
- Ping - Sends data to a specified host/IP
- Regedit - egistry Editor (remote = åben regedit og vælg filer og tag "connect Network Registry"
- Regsvr32 - egister/de-register DLL/OCX/ActiveX
- Regwiz - Reistration wizard
- Sfc /scannow - Sytem File Checker
- Sndrec32 - Sound Recorder
- Sndvol32 - Volume control for soundcard
- Sysedit - Edit system startup files (config.sys, autoexec.bat, win.ini, etc.)
- Taskmgr - Task manager
- Telnet - Telnet program
- Tracert - Traces and displays all paths required to reach an internet host
- Winipcfg - Displays IP configuration
- access.cpl - Accessibility Options

- hdwwiz.cpl - Add New Hardware Wizard
- appwiz.cpl - dd/Remove Programs
- timedate.cpl - Date and Time Properties
- desk.cpl - Display Properties
- inetcpl.cpl - Internet Properties
- joy.cpl - Joystick Properties
- main.cpl keboard - Keyboard Properties
- main.cpl - Mouse Properties
- ncpa.cpl - Network Connections
- ncpl.cpl - Network Properties
- telephon.cpl - Phone and Modem options
- powercfg.cpl - Power Management
- intl.cpl - Regional settings
- mmsys.cpl sounds - Sound Properties
- mmsys.cpl - Sounds and Audio Device Properties
- sysdm.cpl - System Properties
- nusrmgr.cpl - User settings
- firewall.cpl - Firewall Settings (sp2)
- wscui.cpl - Security Center (sp2)

draft