

AMNESTY INTERNATIONAL








WEBINAR SECURITY

GOEDE DOELEN
NEDERLAND

WAT EN WIE

VERSCHILLENDE SOORTEN BEDREIGINGEN

- **Malware attacks**
 - Virussen , ransomware waardoor bestanden geblokkeerd raken, maar ook nieuwe zaken zoals juice jacking.
- **Social engineering**
 - Aanvallers doen zich voor als bekenden, met gebruikmaking van buitgemaakte informatie.
- **Supply Chain attacks**
 - Besmetting via gekoppelde systemen, zoals bijvoorbeeld bij een webshop.
- **Man-in-the-middle attack**
 - Omleiden van emailberichten, aanpassen van DNS, onveilige Wi-Fi.
- **Denial of service**
 - Zwaar belasten van systemen zoals websites zodat deze onderuit gaan.
- **Injection Attacks**
 - Stelen informatie door het uitvoeren van SQL-commando's, het verkeerd reageren van een website.

	Viruses Worms Trojans Ransomware Cryptojacking	Spyware Adware Fileless malware Rootkits
	Baiting Pretexting Phishing Vishing (voice phishing)	Smishing Piggybacking Tailgating
	Wi-Fi eavesdropping Email hijacking	DNS spoofing IP spoofing HTTPS spoofing
	HTTP flood DDoS SYN flood DDoS UDP flood DDoS ICMP flood NTP amplification	
	SQL injection Code injection OS command injection LDAP injection	XML eXternal Entities (XXE) Injection Cross-Site Scripting (XSS)

MET WIE HEBBEN WE TE MAKEN

- State Actors
 - Overheden, ongelimiteerde middelen, omzeilt normale bevestigingen en moeilijk detecteerbaar
- Hackers
 - Aanvallen kunnen tegenwoordig op het dark web eenvoudigweg gekocht worden.
- Malicious Insiders
 - Medewerkers met een dubbele agenda, onderdeel van social engineering.
- AI Cyber aanvallen
 - AI kan gebruikt worden om bedreigingen tegen te gaan, maar ook om aanvallen te verzorgen.

What are the applications of AI in cybersecurity?

1. Breach risk prediction
2. Phishing detection
3. Malware detection & prevention
4. User authentication
5. Spam filtering
6. Password protection
7. Bot identification
8. Behavioural analysis
9. Network segmentation & security
10. Fraud detection
11. Threat intelligence
12. Incident response
13. Vulnerability management
14. Identity & access management

KEN JE MEDEWERKERS

- Onboarding and offboarding
 - Vaststellen identiteit, aanmaken en snel verwijderen digitale accounts
- Identity Management
 - Goed systeem voor digitale identiteit, zoals M365, Okta, OneLogin, security tokens.
- Role Based Access Control
 - Geef medewerkers een rol die bepaalt wat de digitale bevoegdheden zijn.
- Zero Trust
 - Alleen toegang voor apparatuur van de eigen organisatie.

MAATREGELEN

FYSIEKE BEVEILIGING

- Bewaking bij de voordeur
 - Een glimlach is moet niet voldoende zijn om binnen te komen.
- Kamers en gebieden
 - Bepaal veiligheidszones in het gebouw.
- Beheerde apparatuur
 - Mogelijkheid om apparatuur op afstand te wissen bij diefstal
- Datadragers
 - Zorg voor goede vernietiging van oude apparatuur.

PHYSICAL SECURITY BASICS

INFORMATION SECURITY BEGINS WITH STRONG PHYSICAL SECURITY

Lapses in physical security can expose sensitive organisational data to identity theft, with potentially serious consequences.

For example:

An employee accidentally leaves a flash drive on a coffeehouse table. When he returns hours later to get it, the drive - with hundreds of identifiable references to individuals saved on it - is gone.

Another employee throws stacks of old organisational bank records into the rubbish, where a criminal finds them after business hours.

A burglar steals files and computers from your office after entering through an unlocked window.

HOW TO PROTECT EQUIPMENT & PAPER FILES

HERE ARE SOME TIPS FOR PROTECTING INFORMATION IN PAPER FILES AND ON HARD DRIVES, FLASH DRIVES, LAPTOPS, POINT-OF-SALE DEVICES, AND OTHER EQUIPMENT



STORE SECURELY

When paper files or electronic devices contain sensitive information, store them in a locked cabinet or room.



LIMIT PHYSICAL ACCESS

When records or devices contain sensitive data, allow access only to those who need it.



SEND REMINDERS

Remind employees to put paper files in locked file cabinets, log out of your network and applications, and never leave files or devices with sensitive data unattended.



KEEP STOCK

Keep track of and secure any devices that collect sensitive information. Only keep files and data you need and know who has access to them.

TRAIN YOUR EMPLOYEES



Include physical security in your regular employee trainings and communications. Remind employees to:

SHRED DOCUMENTS

Always shred documents with sensitive information before throwing them away.

ERASE DATA CORRECTLY

Use software to erase data before donating or discarding old computers, mobile devices, digital copiers, and drives. Don't rely on "delete" alone. That does not actually remove the file from the computer.

PROMOTE SECURITY PRACTICES IN ALL LOCATIONS

Maintain security practices even if working remotely from home or on business travel.

KNOW THE RESPONSE PLAN

All staff should know what to do if equipment is lost or stolen, including whom to notify and what to do next.

DE BASIS

- Software updates
 - Zorg dat de laatste versies van apps gebruikt worden en pas systeem-updates toe.
- Beveilig je bestanden
 - Pas documentclassificatie toe waardoor bepaalde bestanden versleuteld worden.
- Complexe wachtwoorden
 - Dwing ingewikkelde wachtwoorden af, gebruik passwordmanager app.
- Versleutel opslag
 - Alleen laptops met encrypted disks mogen worden toegepast.
- Beperkingen aan inlog
 - Pas MFA toe, pas geofiltering en login-analyse toe.

DIGITAL SECURITY BASICS

CYBER CRIMINALS TARGET ORGANISATIONS OF ALL SIZES, AND AMNESTY IS TARGETED MORE THAN MOST

Knowing some digital security basics and putting them into practice will help you protect your organisation and reduce the risk of a cyber-attack.

PROTECT YOUR FILES & DEVICES



UPDATE YOUR SOFTWARE

This includes your apps, web browsers, and operating systems. Set updates to happen automatically.



SECURE YOUR FILES

All files should be saved in a sanctioned cloud storage solution such as SharePoint. Make sure you store your paper files securely, too.



REQUIRE STRONG PASSWORDS

Use strong passwords for all laptops, tablets, and smartphones. Don't leave these devices unattended in public places. A strong password is at least 12 characters that are a mix of numbers, symbols, and capital lowercase letters. Never reuse passwords and don't share them on the phone, in texts, or by email.



ENCRYPT DEVICES

Encrypt devices and other media that contain sensitive personal information. This includes laptops, tablets, smartphones, removable drives, backup tapes, and cloud storage solutions.



LIMIT LOGIN ATTEMPTS

Limit the number of incorrect login attempts allowed to unlock devices. This will help protect against intruders.



USE MULTI-FACTOR AUTHENTICATION

Require multi-factor authentication to gain access to your network and resources, or at the least, to access areas of your network with sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or an identity check via a telephone call.

NETWERK EN WIFI

- Goede firewall
 - Pas een next generation firewall toe die cyber-info tot zich neemt.
- Segmenteer intern netwerk
 - Bepaal protect surfaces en limiter toegang tussen netwerksegmenten.
- Wi-Fi
 - Splits in SSID voor medewerkers via login en voor gasten via WPA2 encryptie.

DIGITAL SECURITY *CONTINUED*

PROTECT YOUR WIRELESS NETWORK



SECURE YOUR ROUTER

Change the default name and password, turn off remote management, and log out as the administrator once the router is set up.

USE AT LEAST WPA2 ENCRYPTION

Make sure your router offers WPA2 or WPA3 encryption, and that it's turned on. Encryption protects information sent over your network so it can't be read by outsiders.

MAKE SMART SECURITY YOUR BUSINESS AS USUAL



TRAIN ALL STAFF

Create a culture of security by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities. If employees don't attend, consider blocking their access to resources.



HAVE A 'BUSINESS CONTINUITY' PLAN

Have a plan for saving data, running the organisation, and notifying partners if you experience a breach.

EMAIL

- DMARC
 - Stel je email network goed in zodat berichten vertrouwd worden.
- Bescherm tegen phishing
 - Stel anti-spam filters in en plaats berichten in quarantaine, herschrijf links.
- Forwarding
 - Zorg dat berichten niet automatisch naar privé mailadressen worden doorgestuurd.
- Digitale omgevingen
 - Splits omgeving medewerkers en externe vrijwilligers, gebruik subdomains.

DIGITAL SECURITY – PHISHING

YOU GET AN EMAIL THAT LOOKS LIKE IT'S FROM SOMEONE YOU KNOW

It seems to be from one of your organisation's suppliers and asks that you click on a link to update your business account. Should you click? Maybe it looks like it's from your boss and asks for your network password. Should you reply? In either case, probably not. These may be phishing attempts.



HOW PHISHING WORKS

YOU GET AN EMAIL OR TEXT

It seems to be from someone you know, and it asks you to click a link, or give your password, business bank account, or other sensitive information.

IT LOOKS REAL

It's easy to spoof logos and make up fake email addresses. Scammers use familiar company names or pretend to be someone you know.

IT'S URGENT

The message pressures you to act now — or something bad will happen.

WHAT HAPPENS NEXT

If you click on a link, scammers can install ransomware or other programs that can lock you out of your data and spread to the entire company network. If you share passwords, scammers now have access to all those accounts.

WHAT YOU CAN DO

BEFORE YOU CLICK ON A LINK OR SHARE ANY OF YOUR SENSITIVE BUSINESS INFORMATION:

CHECK IT OUT

Use techniques such as hovering over a hyperlink to see the actual link behind it. Look up the website or phone number for the company or person behind the text or email. Make sure that you're getting the real company and not about to download malware or talk to a scammer.

TALK TO SOMEONE

Talking to a colleague might help you figure out if the request is real or a phishing attempt. However, don't forward something suspicious to a colleague and increase the risk it poses.

If you are familiar with the sender and have a known, trusted method of contacting them, different to the suspicious contact method used, such as a saved phone number, get in touch with them and confirm that they really need information from you. Remember to use a pre-existing contact method you know to be correct though, and not any provided in the suspicious email or text.

ON PREMISE EN CLOUD

- Back-up
 - Zorg voor een goede externe back-up en snapshots van informatiesystemen.
- Security groups
 - Beperk toegang tot cloud-opslag op basis van security groups.
- Security baselines
 - Pas geadviseerde instellingen toe voor alle cloud-structuren (CIS framework)
- Security monitoring
 - Benut de veiligheidsanalyse en waarschuwingen vanuit het cloud-platform

PHISHING *CONTINUED*

HOW TO PROTECT YOUR ORGANISATION



BACKUP YOUR DATA

Use a cloud storage solution such as SharePoint which includes automatic backups, or carry out regular, manual backups. That way, if a phishing attack happens and hackers get to your network, you can restore your data. Make data backup part of your routine operations.



KEEP YOUR SECURITY UP TO DATE

Always install the latest patches and updates. Look for additional means of protection, like email authentication and intrusion prevention software, and set them to update automatically on your computers. On mobile devices, you may have to do it manually.



ALERT YOUR STAFF

Share with them this information. Keep in mind that phishing scammers change their tactics often, so make sure you include tips for spotting the latest phishing schemes in your regular training.



DEPLOY A SAFETY NET

Use email authentication technology to help prevent phishing emails from reaching your organisation's inboxes in the first place.

WHAT IF YOU FALL FOR A PHISHING SCHEME

ALERT OTHERS

Talk to your colleagues and share your experience. Phishing attacks often happen to more than one person in an organisation.

LIMIT THE DAMAGE

Immediately change any compromised passwords and disconnect from the network any computer or device that's infected with malware.

FOLLOW YOUR ORGANISATION'S PROCEDURES

These may include notifying specific people in your organisation or contractors that help you with IT.

NOTIFY PARTNERS

If your data or personal information was compromised, make sure you notify the affected parties — they could be at risk of identity theft. Within Amnesty, if you're not sure how to go about this, consult with the [Data Protection Officer](#) for advice.

REPORT IT

Report suspected phishing emails using a method such as the in-built 'Report' button in Outlook, or your organisation's designated method. Ideally, any confirmed phishing emails should then be shared by the person(s) responsible for information security to your local, trusted government body responsible for cyber security, such as the UK's "Suspicious Email Reporting Service" (SERS): report@phishing.gov.uk. Finally, let the organisation or person that was impersonated know about the phishing scheme.

MENSEN EN PROCEDURES

BEWUSTWORDING

- E-learning
 - Modules op het gebied van security en privacy, al dan niet verplicht.
- Password managers
 - Introductie van password managers zoals Dashlane.
- Herhaal de boodschap
 - Blijf de boodschap uitdragen, standup bijvoorbeeld.
- Commitment management
 - Zorg dat Directie en het MT aan boord zijn.

DATALEKKEN EN RANSOMWAR

- Protocol
 - Zorg dat je protocollen voor malware- en ransomware-aanvallen hebt liggen.
- Communicatie
 - Houdt communicatie naar de buitenwereld in eigen hand en doe het snel.

DIGITAL SECURITY - RANSOMWARE

SOMEONE IN YOUR ORGANISATION GETS AN EMAIL

It looks legitimate — but with one click on a link, or one download of an attachment, everyone is locked out of your network. That link downloaded software that holds your data hostage. That's a ransomware attack.

The attackers ask for money or cryptocurrency, but even if you pay, you don't know if the cybercriminals will keep your data or destroy your files. Meanwhile, the information you need to run your organisation and sensitive details about your partners, employees, and company are now in criminal hands. Ransomware can take a serious toll on your organisation.

HOW IT HAPPENS



SCAM EMAILS

with links and attachments that put your data and network at risk. These phishing emails make up most ransomware attacks.



INFECTED WEBSITES

that automatically download malicious software onto your computer.



CRIMINALS CAN START A RANSOMWARE ATTACK IN A VARIETY OF WAYS

SERVER VULNERABILITIES

which can be exploited by hackers.



ONLINE ADS

that contain malicious code — even on websites you know and trust.

DATALEKKEN EN RANSOMWARE

- Ontkoppel
 - Ontkoppel apparatuur en isoleer informatiesystemen zo snel mogelijk
- Analyseer
 - Bepaal welke objecten gecompromiteerd zijn en bepaald de MITRE attack chain
- Herstel
 - Soms kan dit automatisch (SOAR), vaak alleen handmatig.



ACTIONS TAKEN	Process blocked File quarantined
SEVERITY	Low
OBJECTIVE	Falcon Detection Method
TACTIC & TECHNIQUE	Malware via PUP
TECHNIQUE ID	CST0013
SPECIFIC TO THIS DETECTION	This file is classified as Adware/PUP based on its SHA256 hash.

RANSOMWARE *CONTINUED*

HOW TO PROTECT YOUR ORGANISATION



HAVE A PLAN

How would your business stay up and running after a ransomware attack? Put this plan in writing and share it with everyone who needs to know.



BACK UP YOUR DATA

Regularly save important files to a drive or server that's not connected to your network. Make data backup part of your routine business operations.



KEEP YOUR SECURITY UP TO DATE

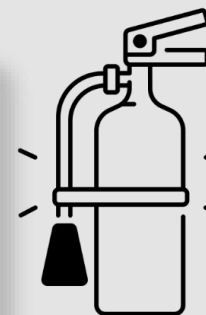
Always install the latest patches and updates. Look for additional means of protection, like email authentication, and intrusion prevention software, and set them to update automatically on your computer. On mobile devices, you may have to do it manually.



ALERT YOUR STAFF

Teach them how to avoid phishing scams and show them some of the common ways computers and devices become infected. Include tips for spotting and protecting against ransomware in your regular orientation and training.

WHAT TO DO IF YOU'RE ATTACKED



LIMIT THE DAMAGE

Immediately disconnect the infected computers or devices from your network. If your data has been stolen, take steps to protect your company and notify those who might be affected.

CONTACT THE AUTHORITIES

Report the attack right away to your local, trusted government body responsible for information.

NOTIFY PARTNERS

If your data or personal information was compromised, make sure you notify the affected parties — they could be at risk of identity theft.

KEEP YOUR BUSINESS RUNNING

Now's the time to implement that plan. Having data backed up will help.

SHOULD I PAY THE RANSOM?

Law enforcement doesn't recommend that, but it's up to you to determine whether the risks and costs of paying are worth the possibility of getting your files back. However, paying the ransom may not guarantee you get your data back.

STANDAARDEN EN NIEUWIGHEDEN

VOLWASSENHEID BEVEILIGING

• Frameworks

- Frameworks als NIST helpen je te bepalen waar je staat en wat nog niet ingekleurd is.
- Zie <https://www.nist.gov/cyberframework>

• Assessment tools

- Invuloefeningen waarmee je bepaalt hoe ver je bent.
- Zie <https://www.soc-cmm.com/downloads/latest/>
- Zie <https://www.enisa.europa.eu/topics/incident-response/csirt-capabilities/csirt-maturity>

• Best practices

- Vastgestelde beste configuraties voor bijvoorbeeld M365.
- Zie <https://www.cisecurity.org/controls>

Table 1- Overview of SIM3v2i parameters ¹²

Parameter number	Parameter description	Parameter number	Parameter Description
O-1	Mandate	T-6	Resilient Messaging
O-2	Constituency	T-7	Resilient Internet Access
O-3	Authority	T-8	Incident Prevention Toolset
O-4	Responsibility	T-9	Incident Detection Toolset
O-5	Service Description	T-10	Incident Resolution Toolset
O-6	Public Media Policy	P-1	Escalation to Governance Level
O-7	Service Level Description	P-2	Escalation to Press Function
O-8	Incident Classification	P-3	Escalation to Legal Function
O-9	Participation in CSIRT Systems	P-4	Incident Prevention Process
O-10	Organisational Framework	P-5	Incident Detection Process
O-11	Security Policy	P-6	Incident Resolution Process
H-1	Code of Conduct/Practice/Ethics	P-7	Specific Incident Processes
H-2	Staff Resilience	P-8	Audit & Feedback Process
H-3	Skillset Description	P-9	Emergency Reachability Process
H-4	Staff Development	P-10	Best Practice Internet Presence
H-5	Technical Training	P-11	Secure Information Handling Process
H-6	Soft Skills Training	P-12	Information Sources Process
H-7	External Networking	P-13	Outreach Process
T-1	IT Assets & Configuration	P-14	Governance Reporting Process
T-2	Information Sources List	P-15	Constituency Reporting Process
T-3	Consolidated Messaging System(s)	P-16	Meeting Process
T-4	Incident Tracking System	P-17	Peer Collaboration Process
T-5	Resilient Voice Calls		

Protect



- **Manage access to assets and information** – Create unique accounts for each employee and ensure that users only have access to information, computers, and applications that are needed for their jobs. Authenticate users (e.g., passwords, multi-factor techniques) before they are granted access to information, computers, and applications. Tightly manage and track physical access to devices.
- **Protect sensitive data** – If your enterprise stores or transmits sensitive data, make sure that this data is protected by encryption both while it's stored on computers as well as when it's transmitted to other parties. Consider utilizing integrity checking to ensure only approved changes to the data have been made. Securely delete and/or destroy data when it's no longer needed or required for compliance purposes.

- **Conduct regular backups** – Many operating systems have built-in backup capabilities; software and cloud solutions are also available that can automate the backup process. A good practice is to keep one frequently backed up set of data offline to protect it against ransomware.
- **Protect your devices** – Consider installing hostbased firewalls and other protections such as endpoint security products. Apply uniform configurations to devices and control changes to device configurations. Disable device services or features that are not necessary to support mission functions. Ensure that there is a policy and that devices are disposed of securely.
- **Manage device vulnerabilities** – Regularly update both the operating system and applications that are installed on your computers and other devices to protect them from attack. If possible, enable automatic updates. Consider using software tools to scan devices for additional vulnerabilities; remediate vulnerabilities with high likelihood and/or impact.
- **Train users** – Regularly train and retrain all users to be sure that they are aware of enterprise cybersecurity policies and procedures and their specific roles and responsibilities as a condition of employment.

INZICHT

- SIEM

- Security Information and Event Management
- Centraal overzicht, gevoed door logfiles van kritische systemen
- Playbooks voor het opvolgen van events
- Zie bijvoorbeeld <https://azure.microsoft.com/en-us/products/microsoft-sentinel/>
- Zie bijvoorbeeld https://www.splunk.com/en_us/home-page.html

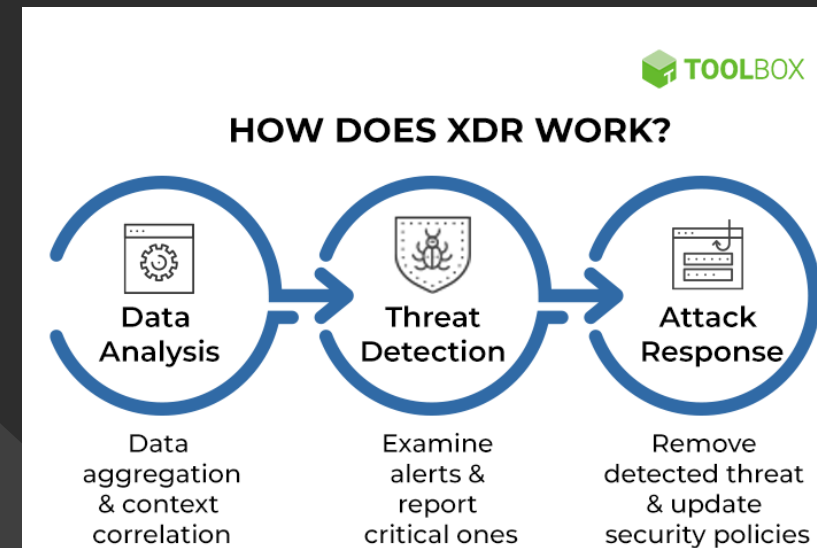
- SOC

- Security Operation Center
- In beginsel 24*7 monitoring system door een externe partij



REAGEREN EN HERSTELLEN

- XDR
 - Extended Detection and Response
 - Alles omvattende aanpak van detectie van incidenten en opvolging
 - Zie bijvoorbeeld <https://www.paloaltonetworks.com/cyberpedia/what-is-xdr>
 - Zie bijvoorbeeld <https://nl.sentinelone.com/>
- SOAR
 - Security Orchestration, automation and response
 - Is een belangrijk maar alweer wat ouder concept dat wordt opgenomen in SIEM en XDR



VRAGEN EN CONTACT

- Ed van Velzen
- e.vanvelzen@amnesty.nl
- 020 7733770