FREE WEBINAR

Modern Cybersecurity

+ Live demo of most common hacks
+ Building blocks of modern strategy
+ Action plan when attacked

MARCH 7 - 13:00 CET

Lars Veelaert
Former Hacker

Stef Vermeulen
Cyber Insurance Expert

Gijs van Laer
Former CISO DPG Media

Presented by XFA × CyberContract

XFA × CyberContract

Your expert panel of today

Stef Vermeulen

Cyber insurance expert

& GM at CyberContract

Lars Veelaert

Former hacker

& CEO at XFA

Gijs Van Laer

Former DPG Media CISO

& CTO at XFA

Agenda of the day

1. How real is the risk?	
● Cyber attack impact → real life cases	Stef
● Easy to be hacked! → live hacking demo	Lars
2. Modern cybersecurity strategy	
● Helpful framework & essential measures	Gijs
3. What to do when hacked?	
● Preventive & reactive action plan	Stef

WRAP-UP and **2 exclusive offers**

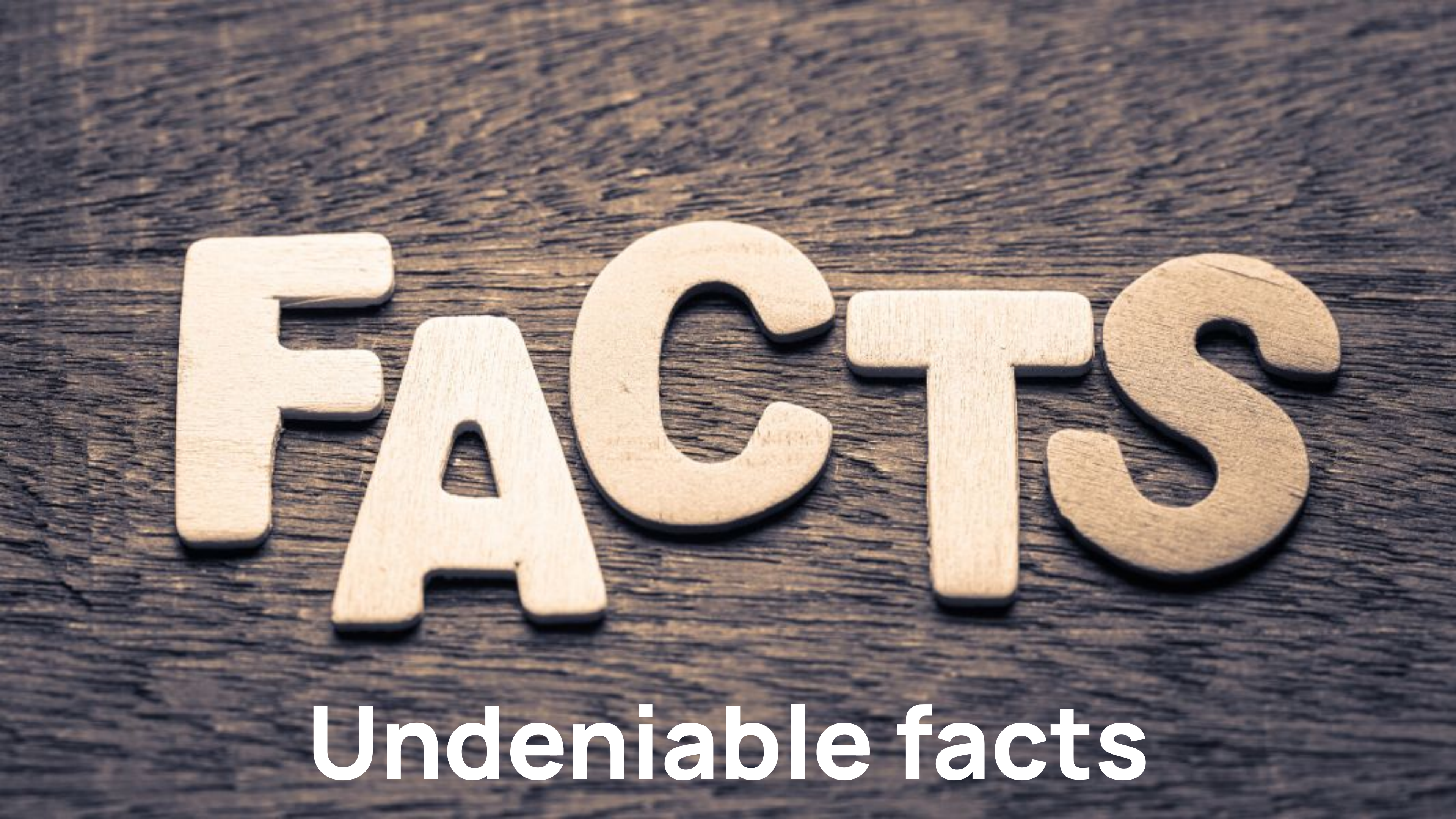
XFA × CyberContract

Stef Vermeulen

Cyber insurance expert
& GM at CyberContract

Topic

How real is the risk



Undeniable facts

Undeniable Fact: Change is the only constant

The times we live in today continuously impose different challenges tomorrow

Undeniable fact: **100% safe does not exist**

AI Scam
Hong Kong Company Loses Over $25 Million To A Deepfake of The CFO

If you did not start working on your digital safety today, when will you?

Todays reality

Reality today: **Our lives depend on software**

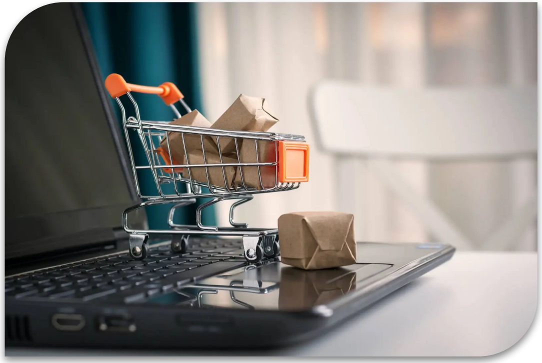
- The chance you do not use software is ZERO
  - Personal & Professional
- Working with software implies risk
  - Do you know the SBOM?
- Risk is not always in your hands

- About your competitors:

Outbeating competition requires being ***unique***

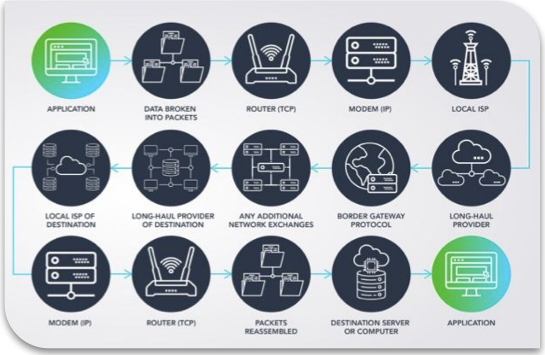
Being unique requires ***innovation***

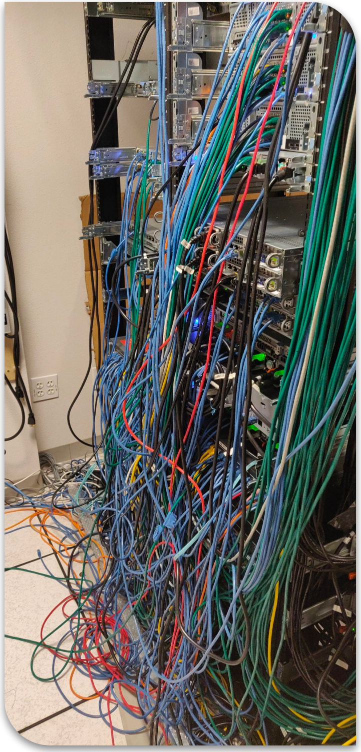
Innovation requires ***software***



Reality today: Cybersecurity is very broad & technical

- Ordering shoes requires just a few clicks
    - The internet traffic, the route taken, the physical, the functional points touched, the supply chain of the shoe shop…
    - An **incomprehensible gigantic amount of possible weak points** with each their open digital doors
- Broad, hard to understand topic
    - Both functional and technical
- House with doors and windows
- Digital world with digital doors and digital windows

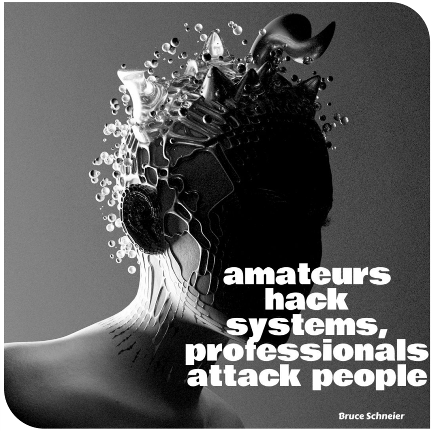




Reality today: **Humans as the weakest link**

- **It won’t happen to us**
  - Money is to be sought at large corporations
  - We use a password, so we are safe
  - We fully rely on our IT partner, Cloud software… they know what they are doing
- What **direct value** do I have/feel/experience from installing an update?
  - Device is offline for a couple of minutes, maybe new UI, maybe issues…
- MFA? Password Manager?
  - **Pppppffff…**

ONCE I MADE
AN OBVIOUS PHISHING EMAIL
AND THE MALICIOUS URL WAS IN THE
"REPORT PHISHING" BUTTON I ADDED



Reality today: Welcoming cybercriminals on a red carpet

- Cybercrime is on a **global industrial uncontrollable scale**, whilst business owners do not lose their sleep over it
- WormGPT, FraudGPT, BADGPT, Ransomware as a Service
- IoT devices with **open doors**
- When things go wrong, all of a sudden there is budget, if not bankrupt

Security budget before a data breach
Security budget after a data breach

I DON'T ALWAYS THINK ABOUT CYBER SECURITY
BUT WHEN I DO, IT'S USUALLY TOO LATE

Myth Busting

Myth: Cybersecurity costs nothing but money

BUSTED

- CyberSecurity is a **pure cost** with no benefits!

- Calculate **Return On Investment**
- You cannot prioritize what you can't measure
  - Identify your business critical processes
  - Calculate the interruption/total absence of those processes
  - What effort/cost is needed to protect those processes
- Cybersecurity has an "under the hood" kind of ROI
  - Monitor attempted hacks
    - False alerts - what if they were critical?
    - Critical alerts - avg timeframe of 277 days needed to identify and contain a data breach
- Overcome Ransomware
  - Average of 4-6 months of total monthly salary cost
  - 38% of the expenses come from customer churn, downtime and new business acquisition cost
- 100% safe does not exist
  - When "shit hits the fan" you want to be helped
  - **The cost of a Cybersecurity strategy is a fraction from an incident cost**

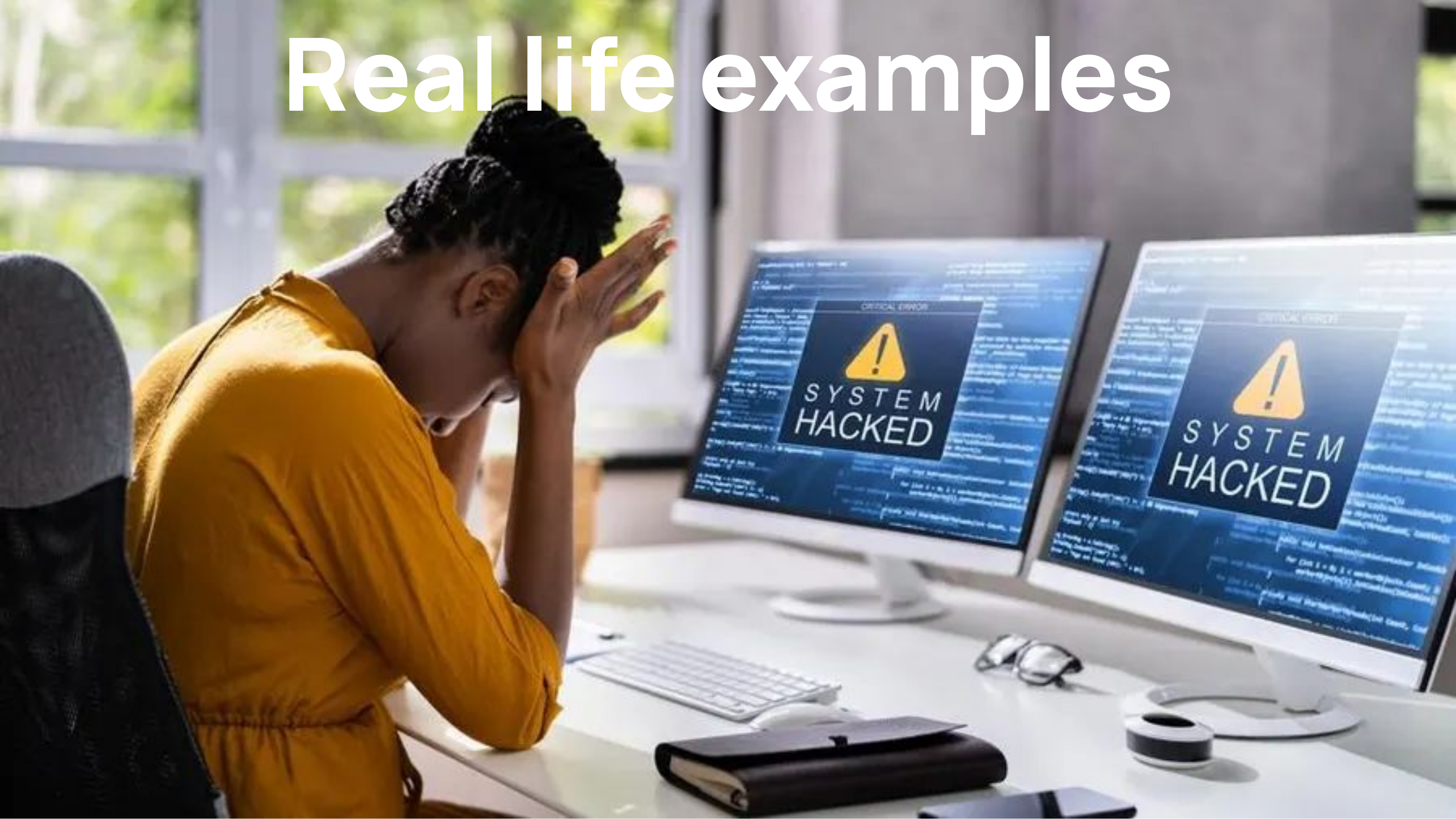
Myth: Cyberinsurance is nothing but expensive

- Cyberinsurance is something my company cannot afford, it’s **expensive**

- You do not get into your car thinking: I am gonna drive really insecure now
  - You buy a safe car, you drive around seatbelts fastened, in a way to avoid accidents
  - Same applies to cybersecurity, but the correct mindset is not applied
- 100% secure does not exist
  - Why do you have car, fire, life… insurance?
  - Times have changed, need for a different mindset
- When things go wrong
  - You want to be helped, 1st moments are crucial
  - Hotline, IT Forensic services, Legal Services
- How to secure your **business continuity**?
  - By insuring the risk
  - **For a lot of company owners,
    their car is better insured than their business continuity**

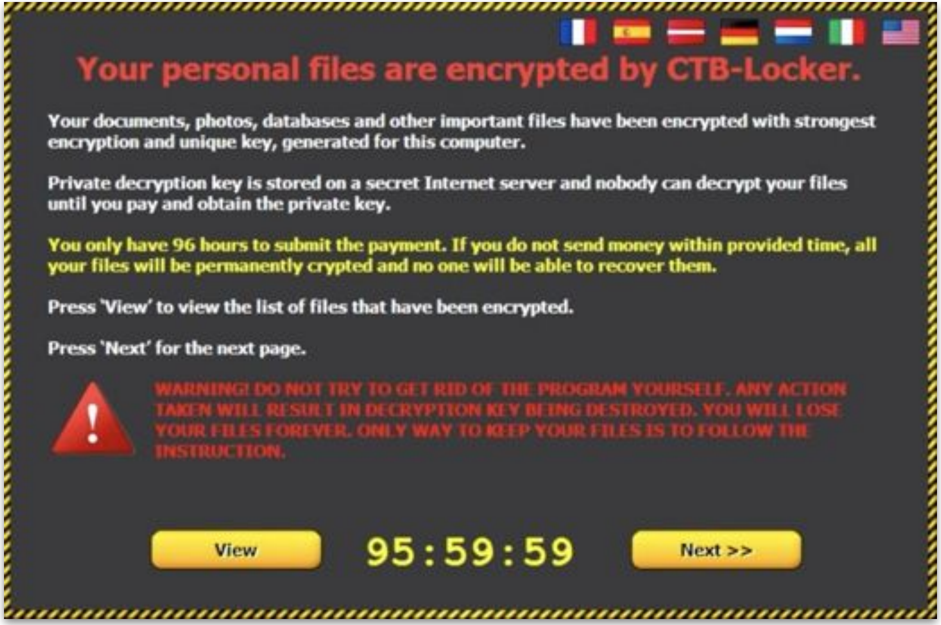
BUSTED

Real life examples



Real life cases: **business continuity with CyberContract**

- **The broker**
    - Mail with request for quotation
    - Word attachment for clarification
    - Open start cryptolocker unseen
    - After 1 week everything infected
    - Then everything blocked
- **Cost breakdown**
    - Forensic service: € 2,000
    - Recovery efforts: € 25,000
    - Setting up new environment: € 15,000
    - Reconstruction of data: € 60,000
    - Loss of profit: € 34,000
- **Total cost: € 136,000**



Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

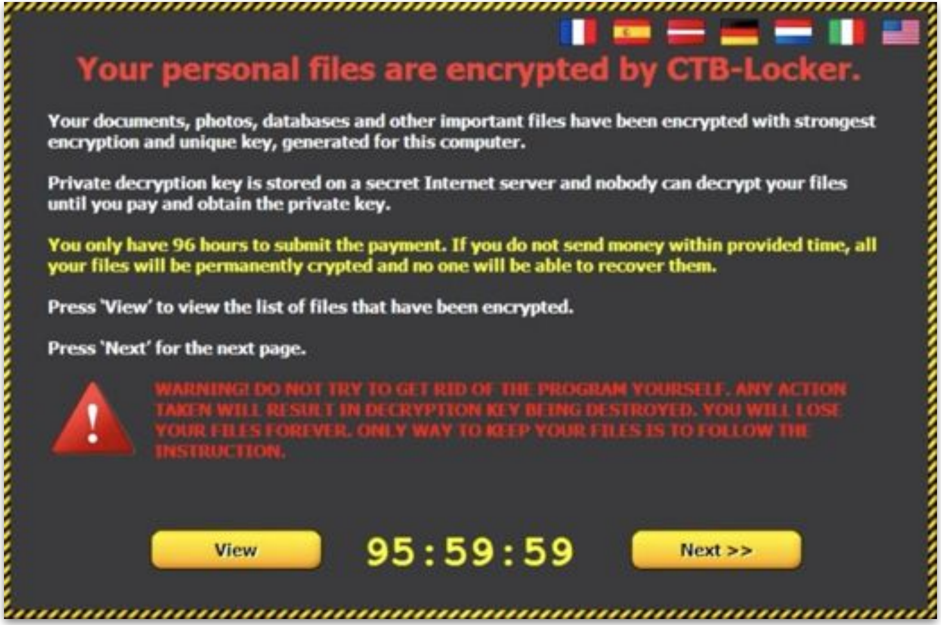
Real life cases: **business continuity with CyberContract**

HOTLINE
Broker calls hotline
IT forensic services on site
Policy pays costs

RECONSTITUTION
IT partner work on data recovery
Policy pays costs

PROFIT LOSS
The time the broker was inactive
Policy covers loss of profits

LEGAL EXPERTISE
Legal help to recover
Policy pays costs



Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

Real life cases: **business continuity with CyberContract**

- **THE PRODUCTION COMPANY**
  - Mail from trusted contact at supplier
  - Outstanding invoice, change of account number
  - Transferred, money has disappeared
  - Inbreak on mailserver
  - Hackers were reading for 4 months
- **COST BREAKDOWN**
  - Forensic services: € 2.300
  - Setting up new environment: € 900
  - Cybertheft: € 139.700
- **TOTAL COST: € 140.900**

Real life cases: business continuity with CyberContract

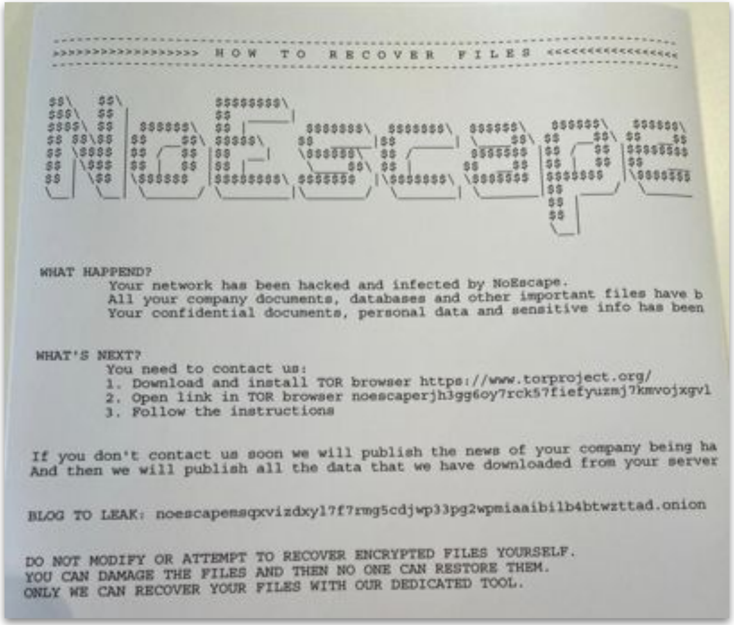
HOTLINE
Conduct IT Forensic investigation
Compile report on burglary
Policy pays costs

SANITIZING SYSTEMS
Verify all accounts & systems
Set up MFA
Policy pays costs

CYBERTHEFT
Intrusive theft
Policy pays costs

Real life cases: **business continuity with CyberContract**

- **THE CONSULTANCY FIRM**
  - All IT services at IT partner
  - Citrix environment
  - Friday night print out of all printers at all branches
  - All systems down
  - Ransom demand
- **COST BREAKDOWN**
  - Forensic Services: €3.000
  - IT Partner: €25.000
  - Legal Services: €5.000
- **TOTAL COST: €33.000**



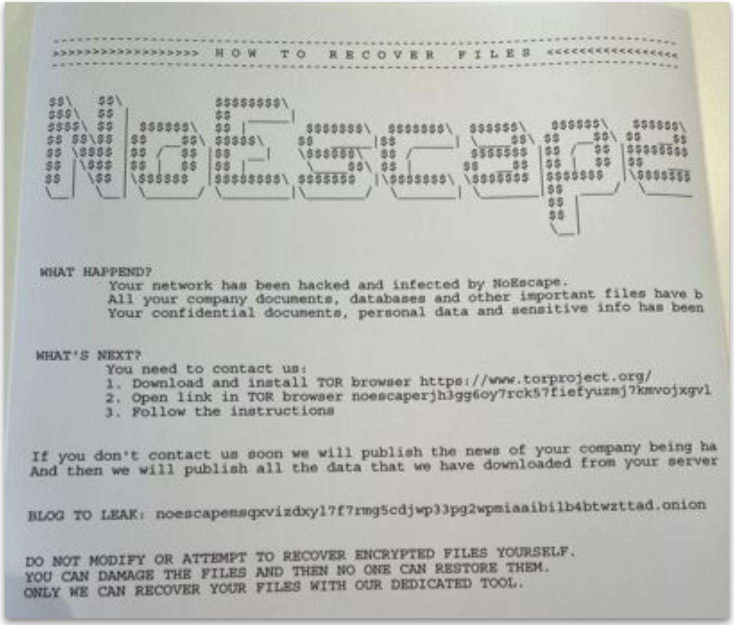
```
>>>>>>>>>>>>>>>>>>> H O W   T O   R E C O V E R   F I L E S <<<<<<<<<<<<<<<<<<

WHAT HAPPEND?
        Your network has been hacked and infected by NoEscape.
        All your company documents, databases and other important files have b
        Your confidential documents, personal data and sensitive info has been

WHAT'S NEXT?
        You need to contact us:
        1. Download and install TOR browser https://www.torproject.org/
        2. Open link in TOR browser noescaperjh3gg6oy7rck57fiefyuzmj7kmvojxgvl
        3. Follow the instructions

If you don't contact us soon we will publish the news of your company being ha
And then we will publish all the data that we have downloaded from your server

BLOG TO LEAK: noescapemsqxvizdxyl7f7rmg5cdjwp33pg2wpmiaaibilb4btwzttad.onion

DO NOT MODIFY OR ATTEMPT TO RECOVER ENCRYPTED FILES YOURSELF.
YOU CAN DAMAGE THE FILES AND THEN NO ONE CAN RESTORE THEM.
ONLY WE CAN RECOVER YOUR FILES WITH OUR DEDICATED TOOL.
```

Real life cases: business continuity with CyberContract

HOTLINE
CEO calls hotline, Friday night
IT Forensic investigation
Policy pays costs

LEGAL HELP
Help to get uncooperative IT Partner to move
Policy pays costs

IT PARTNER
Build up from scratch



```
>>>>>>>>>>>>>>>>>> HOW TO RECOVER FILES <<<<<<<<<<<<<<<<<<

WHAT HAPPEND?
        Your network has been hacked and infected by NoEscape.
        All your company documents, databases and other important files have b
        Your confidential documents, personal data and sensitive info has been

WHAT'S NEXT?
        You need to contact us:
        1. Download and install TOR browser https://www.torproject.org/
        2. Open link in TOR browser noescaperjh3gg6oy7rck57fiefyuzmj7kmvojxgvl
        3. Follow the instructions

If you don't contact us soon we will publish the news of your company being ha
And then we will publish all the data that we have downloaded from your server

BLOG TO LEAK: noescapemsqxvizdxyl7f7rmg5cdjwp33pg2wpmiaaibilb4btwzttad.onion

DO NOT MODIFY OR ATTEMPT TO RECOVER ENCRYPTED FILES YOURSELF.
YOU CAN DAMAGE THE FILES AND THEN NO ONE CAN RESTORE THEM.
ONLY WE CAN RECOVER YOUR FILES WITH OUR DEDICATED TOOL.
```

Real life cases: **business continuity with CyberContract**

- **THE WHOLESALER**
  - Employee finds USB flash drive
  - In PC to see who it belongs to
  - Virus, hackers place orders themselves
- **COST BREAKDOWN**
  - Forensic investigation: € 5.000
  - Cleaning up systems: € 2.900
  - Theft of goods: € 14.000
- **TOTAL COST: € 21.900**

Real life cases: business continuity with CyberContract

HOTLINE
Employee calls hotline
IT Expert arrives on site
Policy pays costs

LEGAL HELP
Define which legal steps to take
Policy pays costs

CYBER THEFT
Policy pays the costs of the cybertheft

XFA × CyberContract

Disclaimer: all information and techniques shown are shared for educational purposes.
Do not attempt to recreate.

Lars Veelaert
Former hacker
& CEO at XFA

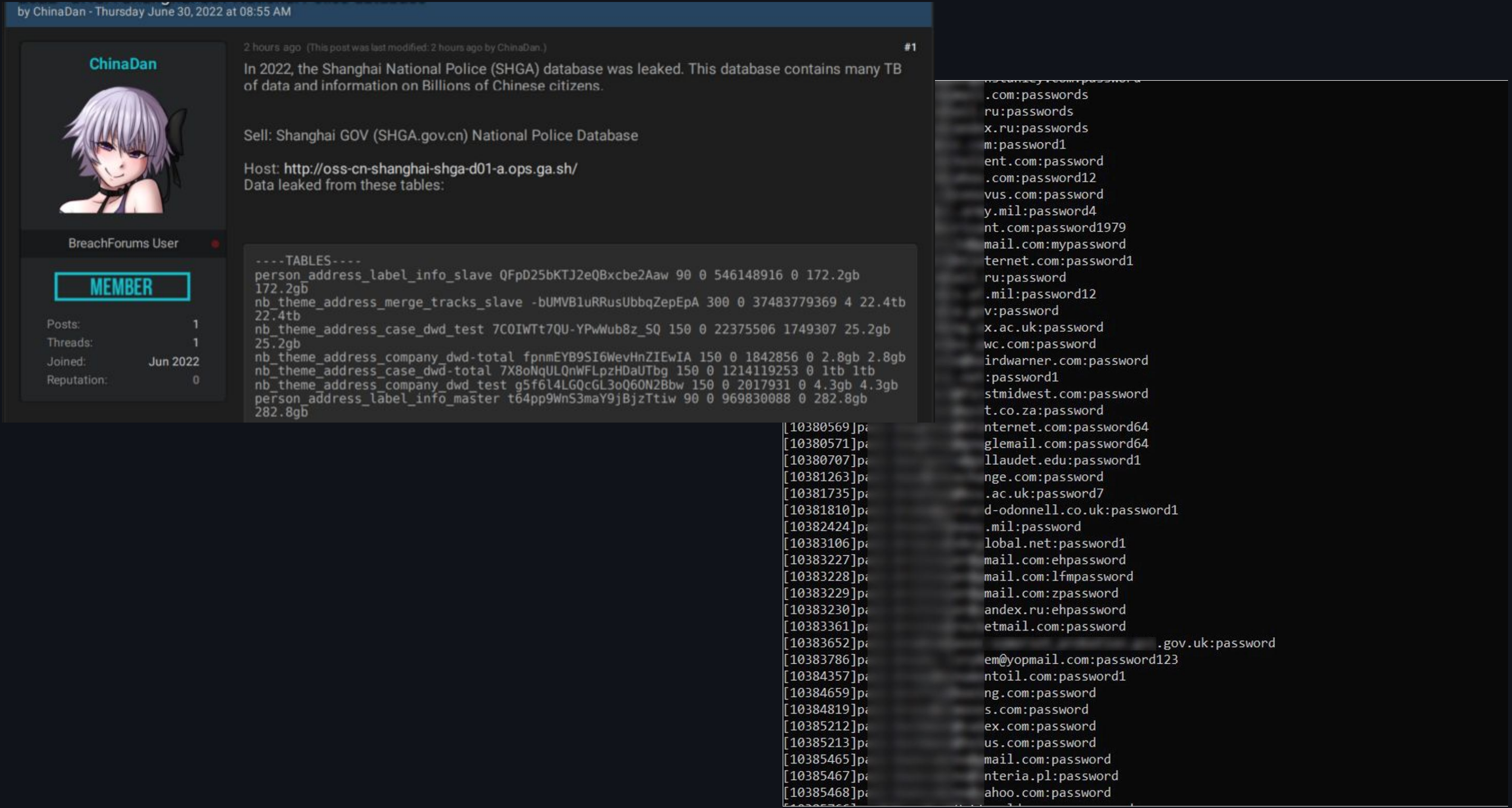
Topic

The hacker’s point of view

5 common cyber attacks explained

Cyber Attack #1

Password Databases & Phishing



by ChinaDan - Thursday June 30, 2022 at 08:55 AM

ChinaDan

BreachForums User

MEMBER

Posts:	1
Threads:	1
Joined:	Jun 2022
Reputation:	0

2 hours ago (This post was last modified: 2 hours ago by ChinaDan.) #1

In 2022, the Shanghai National Police (SHGA) database was leaked. This database contains many TB of data and information on Billions of Chinese citizens.

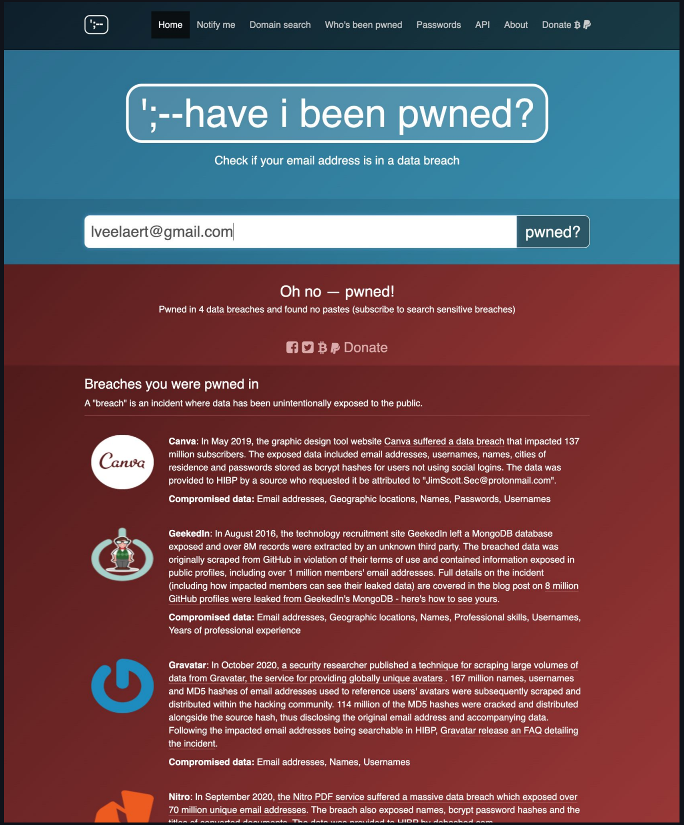
Sell: Shanghai GOV (SHGA.gov.cn) National Police Database

Host: http://oss-cn-shanghai-shga-d01-a.ops.ga.sh/
Data leaked from these tables:

```
----TABLES----
person_address_label_info_slave QFpD25bKTJ2eQBxcbe2Aaw 90 0 546148916 0 172.2gb
172.2gb
nb_theme_address_merge_tracks_slave -bUMVB1uRRusUbbqZepEpA 300 0 37483779369 4 22.4tb
22.4tb
nb_theme_address_case_dwd_test 7COIWTt7QU-YPwWub8z_SQ 150 0 22375506 1749307 25.2gb
25.2gb
nb_theme_address_company_dwd-total fpnmEYB9SI6WevHnZIEwIA 150 0 1842856 0 2.8gb 2.8gb
nb_theme_address_case_dwd-total 7X8oNqULQnWFLpzHDaUTbg 150 0 1214119253 0 1tb 1tb
nb_theme_address_company_dwd_test g5f6l4LGQcGL3oQ6ON2Bbw 150 0 2017931 0 4.3gb 4.3gb
person_address_label_info_master t64pp9WnS3maY9jBjzTtiw 90 0 969830088 0 282.8gb
282.8gb
```

```
[redacted].com:passwords
ru:passwords
x.ru:passwords
m:password1
ent.com:password
.com:password12
vus.com:password
y.mil:password4
nt.com:password1979
mail.com:mypassword
ternet.com:password1
ru:password
.mil:password12
v:password
x.ac.uk:password
wc.com:password
irdwarner.com:password
:password1
stmidwest.com:password
t.co.za:password
[10380569]pa nternet.com:password64
[10380571]pa glemail.com:password64
[10380707]pa llaudet.edu:password1
[10381263]pa nge.com:password
[10381735]pa .ac.uk:password7
[10381810]pa d-odonnell.co.uk:password1
[10382424]pa .mil:password
[10383106]pa lobal.net:password1
[10383227]pa mail.com:ehpassword
[10383228]pa mail.com:lfmpassword
[10383229]pa mail.com:zpassword
[10383230]pa andex.ru:ehpassword
[10383361]pa etmail.com:password
[10383652]pa [redacted].gov.uk:password
[10383786]pa em@yopmail.com:password123
[10384357]pa ntoil.com:password1
[10384659]pa ng.com:password
[10384819]pa s.com:password
[10385212]pa ex.com:password
[10385213]pa us.com:password
[10385465]pa mail.com:password
[10385467]pa nteria.pl:password
[10385468]pa ahoo.com:password
```

Stolen Data is sold on **dark-net forums**



Check if your email address is in a data breach

lveelaert@gmail.com

Oh no — pwned!

Pwned in 4 data breaches and found no pastes (subscribe to search sensitive breaches)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public.

Canva: In May 2019, the graphic design tool website Canva suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Compromised data: Email addresses, Geographic locations, Names, Passwords, Usernames

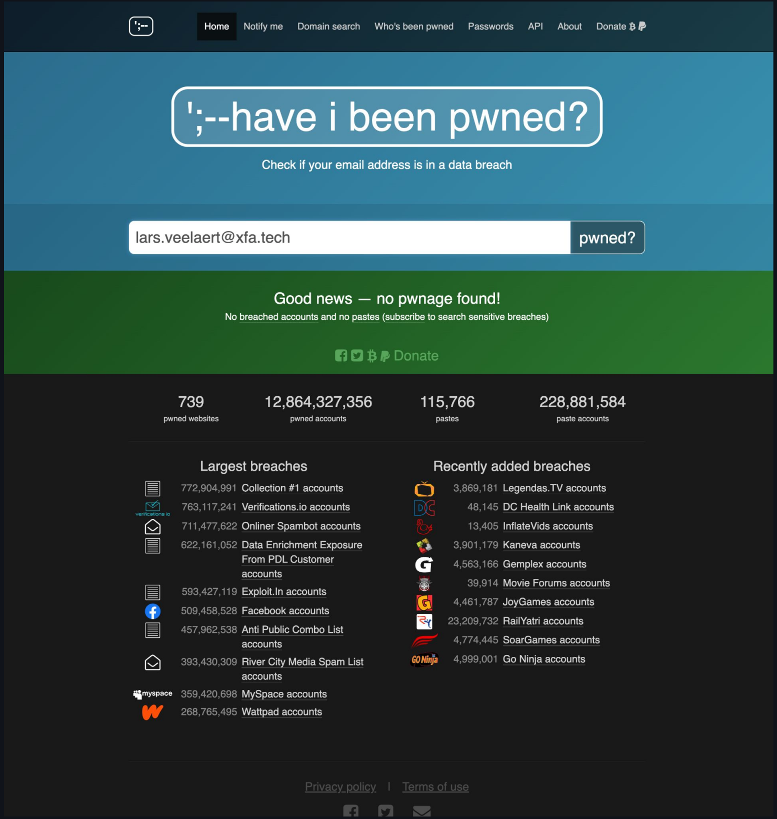
GeekedIn: In August 2016, the technology recruitment site GeekedIn left a MongoDB database exposed and over 8M records were extracted by an unknown third party. The breached data was originally scraped from GitHub in violation of their terms of use and contained information exposed in public profiles, including over 1 million members' email addresses. Full details on the incident (including how impacted members can see their leaked data) are covered in the blog post on 8 million GitHub profiles were leaked from GeekedIn's MongoDB - here's how to see yours.

Compromised data: Email addresses, Geographic locations, Names, Professional skills, Usernames, Years of professional experience

Gravatar: In October 2020, a security researcher published a technique for scraping large volumes of data from Gravatar, the service for providing globally unique avatars . 167 million names, usernames and MD5 hashes of email addresses used to reference users' avatars were subsequently scraped and distributed within the hacking community. 114 million of the MD5 hashes were cracked and distributed alongside the source hash, thus disclosing the original email address and accompanying data. Following the impacted email addresses being searchable in HIBP, Gravatar release an FAQ detailing the incident.

Compromised data: Email addresses, Names, Usernames

Nitro: In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of converted documents. The data was provided to HIBP by dehashed.com.



Check if your email address is in a data breach

lars.veelaert@xfa.tech

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)

739	12,864,327,356	115,766	228,881,584
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

772,904,991	Collection #1 accounts
763,117,241	Verifications.io accounts
711,477,622	Onliner Spambot accounts
622,161,052	Data Enrichment Exposure From PDL Customer accounts
593,427,119	Exploit.In accounts
509,458,528	Facebook accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
359,420,698	MySpace accounts
268,765,495	Wattpad accounts

Recently added breaches

3,869,181	Legendas.TV accounts
48,145	DC Health Link accounts
13,405	InflateVids accounts
3,901,179	Kaneva accounts
4,563,166	Gemplex accounts
39,914	Movie Forums accounts
4,461,787	JoyGames accounts
23,209,732	RailYatri accounts
4,774,445	SoarGames accounts
4,999,001	Go Ninja accounts

Privacy policy | Terms of use

Try it yourself: https://haveibeenpwned.com

Cyber attack #1 - Password Databases & Phishing

What is it?

- Your password has been leaked (phishing, stolen or guessed)
- It is made available in online databases
- (maybe) you reuse it for multiple accounts

Things you should know

- HaveIBeenPwnd.com
- 100 Billion passwords are leaked online (~ 19 passwords per person on internet)
- Cost to the hacker: Laptop + 50 EUR (price of database on black market)

How to prevent

- Use Multi-factor-authentication
- Use different passwords
- Use a password manager to prevent phishing / usage of unique passwords

Cyber Attack #2

RCE / Ransomware

Cyber attack #2 - RCE / Ransomware

What is it?

- Executing arbitrary code remotely using an exposed software vulnerability in a system
- Used to fully compromise a target (e.g. ransomware, corporate espionage, …)
- Attack vector based on specific vulnerability (e.g. email, SMS, network, …)

Things you should know

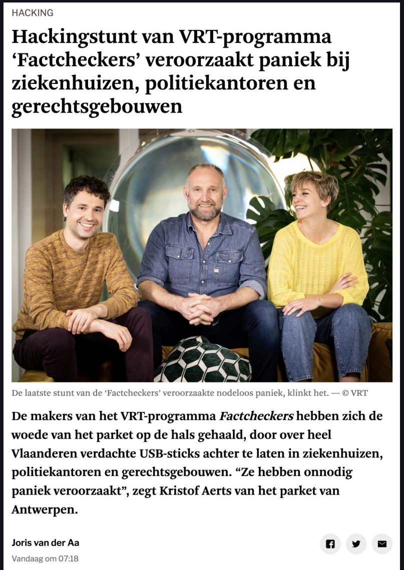
- Demo: ‘EternalBlue’-exploit used in the worldwide ‘WannaCry’-ransomware attack (2017)
- Exploits almost always rely on known vulnerabilities, that have been fixed
- Patch available › Exploit ‘in the wild’ takes about 2-4 weeks.
- Vulnerabilities are found every day: https://www.cvedetails.com/

How to prevent

- Update all your software quickly (OS, browser, PDF-reader, email-client, …)
- Take ‘years of updates’ into account when buying new hardware

Cyber Attack #3

Rubber Ducky & BadUSB



HACKING

Hackingstunt van VRT-programma ‘Factcheckers’ veroorzaakt paniek bij ziekenhuizen, politiekantoren en gerechtsgebouwen

De laatste stunt van de ‘Factcheckers’ veroorzaakte nodeloos paniek, klinkt het. — © VRT

De makers van het VRT-programma *Factcheckers* hebben zich de woede van het parket op de hals gehaald, door over heel Vlaanderen verdachte USB-sticks achter te laten in ziekenhuizen, politiekantoren en gerechtsgebouwen. “Ze hebben onnodig paniek veroorzaakt”, zegt Kristof Aerts van het parket van Antwerpen.

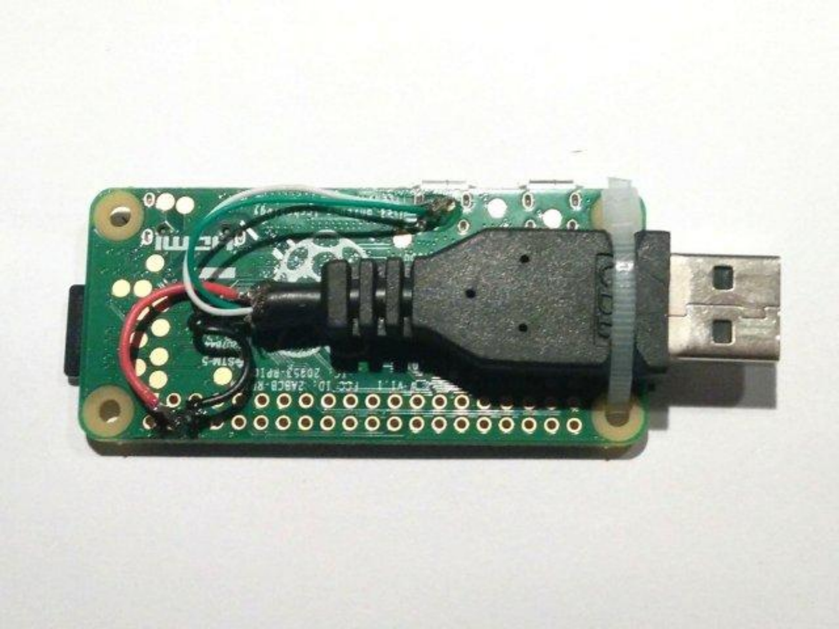
Joris van der Aa

Vandaag om 07:18

Recently in the news

“If it quacks like a keyboard, it’s a keyboard”

$50 (gov. tracking included)



$7 (shipping included)

Tools used to inject keystrokes

Cyber attack #3 - Rubber Ducky & BadUSB

What is it?

- Using the trust of everyday USB devices to bypass controls e.g. type out a full virus through your keyboard

Things you should know

- Trained humans type 40 words / minute
- Rubber ducky types over 1000 words / minute
- The average payload takes 50 words ~ 3 seconds
- Cost to the hacker: Laptop + ~7 EUR per device

How to prevent

- Don’t plug in random USB devices
- Lock your device when walking away (everywhere)
- Modern OS’es will ask confirmation
- Play the “Koffiekoeken”-game at work

Cyber Attack #4

Man In The Middle

Cyber attack #4 - Man In The Middle

What is it?

- … listening for unencrypted traffic
- … exploiting sensitive information (credentials, financial information, …)
- … injecting extra phishing / malware

Things you should know

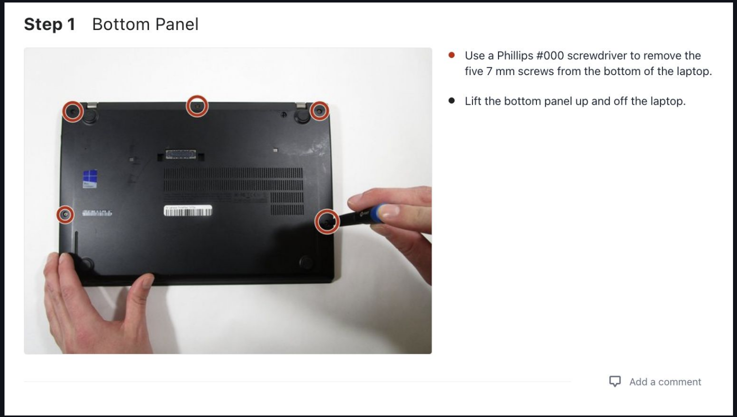
- HTTPS / TLS is enough, you don’t need a VPN (and it’s hard to do well)
- Hln.be is not HIn.be
- Cost to the hacker: Laptop + 150 EUR

How to prevent

- Use up-to-date modern Browser
- Use up-to-date operating System
- Watch your domain name & warnings

Cyber Attack #5

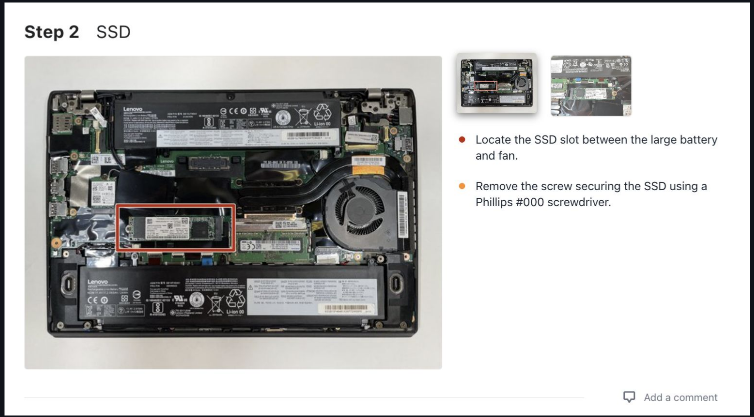
Data Scraping



Step 1 Bottom Panel

- Use a Phillips #000 screwdriver to remove the five 7 mm screws from the bottom of the laptop.
- Lift the bottom panel up and off the laptop.

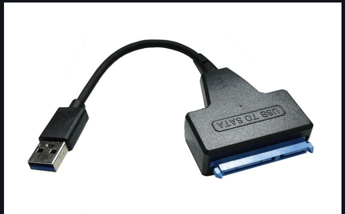
Add a comment

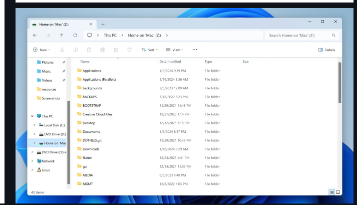


Step 2 SSD

- Locate the SSD slot between the large battery and fan.
- Remove the screw securing the SSD using a Phillips #000 screwdriver.

Add a comment





Name	Date modified	Type	Size
Applications	1/9/2024 9:39 PM	File folder	
Applications (Parallels)	1/16/2024 8:36 AM	File folder	
backgrounds	7/6/2023 12:09 AM	File folder	
BACKUPS	7/18/2022 8:23 PM	File folder	
BOOTSTRAP	11/29/2021 11:48 PM	File folder	
Creative Cloud Files	12/21/2023 1:14 PM	File folder	
Desktop	12/12/2023 7:15 PM	File folder	
Documents	1/8/2024 8:37 PM	File folder	
DOTFILES.git	11/29/2021 10:47 PM	File folder	
Downloads	1/16/2024 8:29 AM	File folder	
flutter	12/24/2023 4:41 PM	File folder	
go	12/14/2021 11:05 PM	File folder	
MEDIA	8/6/2023 5:48 PM	File folder	
MGMT	12/6/2022 1:03 PM	File folder	

42 items

The typical laptop averages 6 screws to SSD / HD

How to break into an unencrypted laptop

No your password won't protect you

Cyber attack #5 - Disk Scraping

What is it?

- Extracting data from the device (unencrypted) hard drive using various methods
- Method 1: Take the disk out, mount with a USB adapter
- Method 2: Replace (unsigned) authentication code of OS

Things you should know

- Your OS password does not protect your data
- A stolen sensitive (unencrypted) laptop is considered a data leak (GDPR/HIPAA)

How to prevent

- Enable your built-in device encryption (this does NOT impact performance)
  - macOS: System Settings › Privacy & Security › Filevault
  - Windows: Settings › Privacy & Security › Device Encryption
  - Linux: Configure LUKS
  - iOS & Android: Have a pincode set › (enables automatically)

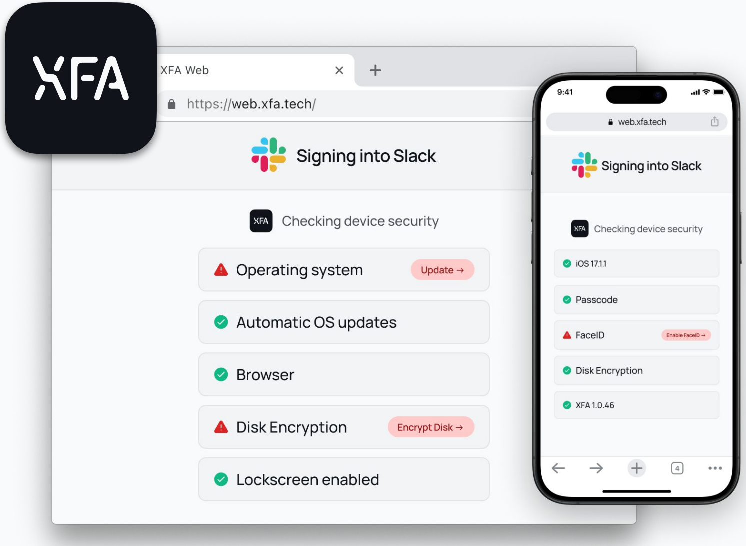
Key Takeaways

A hacker’s point of view

Key takeaways

- Use **password manager**
- Keep your **browser** up-to-date
- Keep your **OS** up-to-date
- **Lock** your device
- **Encrypt** your device

› resolves most of your risk



XFA Web

https://web.xfa.tech/

Signing into Slack

Checking device security

- Operating system — Update →
- ✓ Automatic OS updates
- ✓ Browser
- Disk Encryption — Encrypt Disk →
- ✓ Lockscreen enabled

9:41

web.xfa.tech

Signing into Slack

Checking device security

- ✓ iOS 17.1.1
- ✓ Passcode
- FaceID — Enable FaceID →
- ✓ Disk Encryption
- ✓ XFA 1.0.46

+40%

of the devices used for work
are **unknown / unsafe**

33%

Security incidents
are **related to devices**

Gijs Van Laer

Former DPG Media CISO
& CTO at XFA

Topic

Strategic framework

Where companies used to start with Cybersecurity

Companies thought their network was a castle…

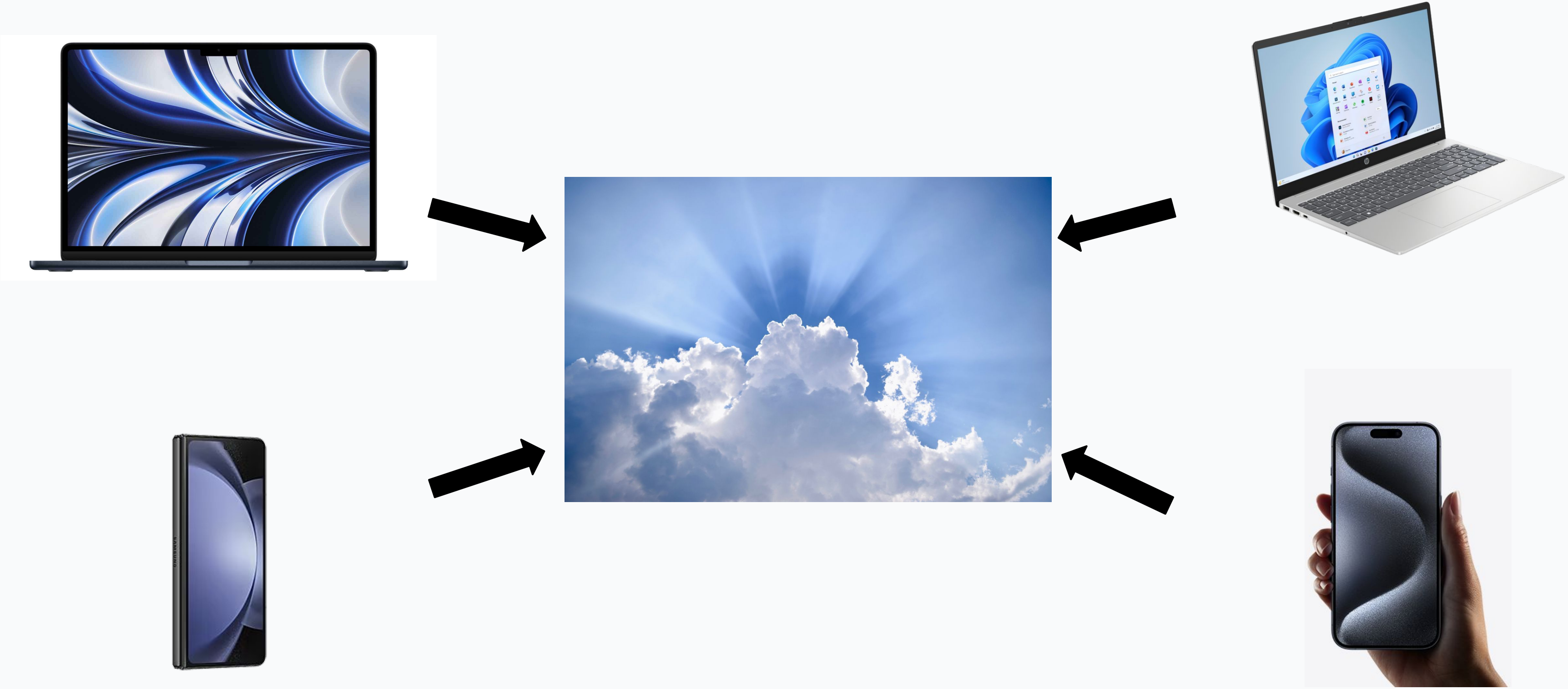
…but over the years it became more like a soap bubble

Connecting remotely, with any device

Classic approach: connecting remotely into a trusted network

Embrace the new reality

Modern approach: login into the cloud (SaaS applications)

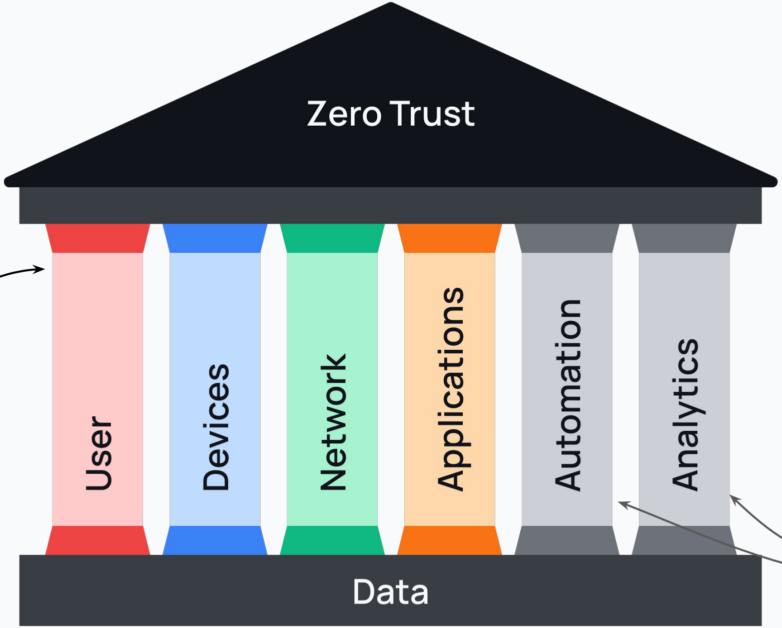


XFA × CyberContract

Do not trust the network

And build around what you control

SMEs should start with 4 first pillars



Not focus of this webinar, these become important when first pilla are covered

Six Pillars of a Zero Trust Security Model

Cybersecurity framework - building blocks

Pillar: Users

Objectives:

- Secure authentication

Tools:

- Identity provider (if possible move to single-sign-on)
- Multi-factor authentication
- Password Manager

Cybersecurity framework - building blocks

Pillar: Devices

Objectives:

- Up to date devices
- Up to date browsers
- Disk encryption
- Backups

Tools:

- Enforced checks on endpoints
- Device management
- Keep data in the cloud

Cybersecurity framework - building blocks

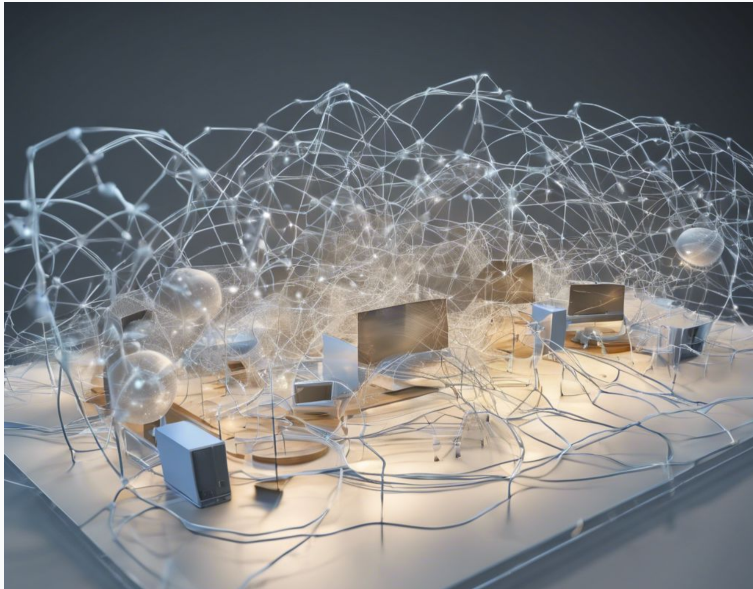
Pillar: Network

Objectives:

- All network traffic encrypted

Tools:

- HTTPS Everywhere
- DNS-over-HTTPS



Cybersecurity framework - building blocks

Pillar: Applications

Objectives:

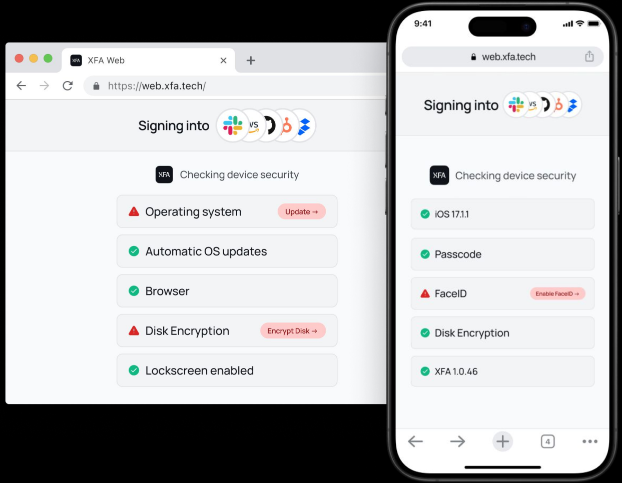
- Isolation between applications
- Secure vendors - secure versions of applications

Tools:

- Default isolation with SaaS applications
- Review your vendor (security and privacy efforts, maybe certification, e.g. ISO27001, SOC2,...)
- Keep used software up to date
- If you build software yourself:
  - Secure Development Lifecycle
  - Use OWASP as the best resource for secure development
  - Keep used libraries up to date

About XFA - true optimal device security

With XFA, **only safe devices** can access your business applications



XFA Web

https://web.xfa.tech/

Signing into

Checking device security

- Operating system — Update →
- Automatic OS updates
- Browser
- Disk Encryption — Encrypt Disk →
- Lockscreen enabled

9:41

web.xfa.tech

Signing into

Checking device security

- iOS 17.1.1
- Passcode
- FaceID — Enable FaceID →
- Disk Encryption
- XFA 1.0.46

- Performing **essential security checks** *during login*
- **Enforcing** your security policy
- **Full coverage**, light & privacy respecting → *also possible with BYOD, freelancers, …*
- Simplifying device **compliance** *(ISO27001, SOC2, ..)*

Stef Vermeulen

Cyber insurance expert
& GM at CyberContract

Topic

Prevention before the rescue

Modern CyberSecurity: **The combination of actions**

- What good is a closed front door when the side door is still open?
- Your company is as safe as your best employee is having a bad day
- Mindset!

Backup
Ctrl
ANTIVIRUS
FORTINET
SIEM
Zero Trust
Role-Based
Access Control

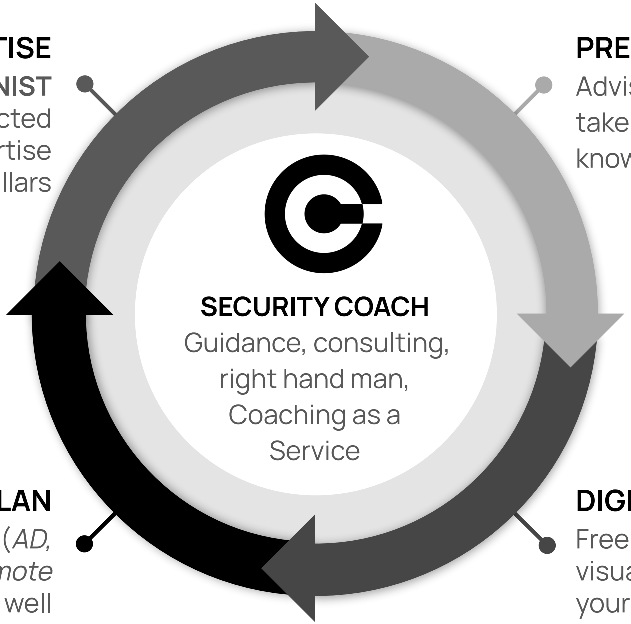
ALL YOUR CYBER SECURITY EFFORTS
THAT ONE EMPLOYEE CLICKING A PHISHING LINK

Modern Cybersecurity?

- What is the consequence of stepping into an insured car without brakes?
- Do you get into your car thinking “today I am going to drive very unsafe”?

- Modern cybersecurity requires a **Proactive & Reactive approach**
  - You buy a safe car, you drive safely, different actions to arrive safely
  - But when the car breaks down, you have an accident… you want to be helped
- **Applying Modern Cyber Security results in being Cyber Resilient**
  - Prevention before the rescue

Modern CyberSecurity: PROACTIVE



SECURITY COACH
Guidance, consulting, right hand man, Coaching as a Service

EXPERTISE
Following the 5 pillars of the **NIST** framework, we provide selected partners with their specific expertise in each of the pillars

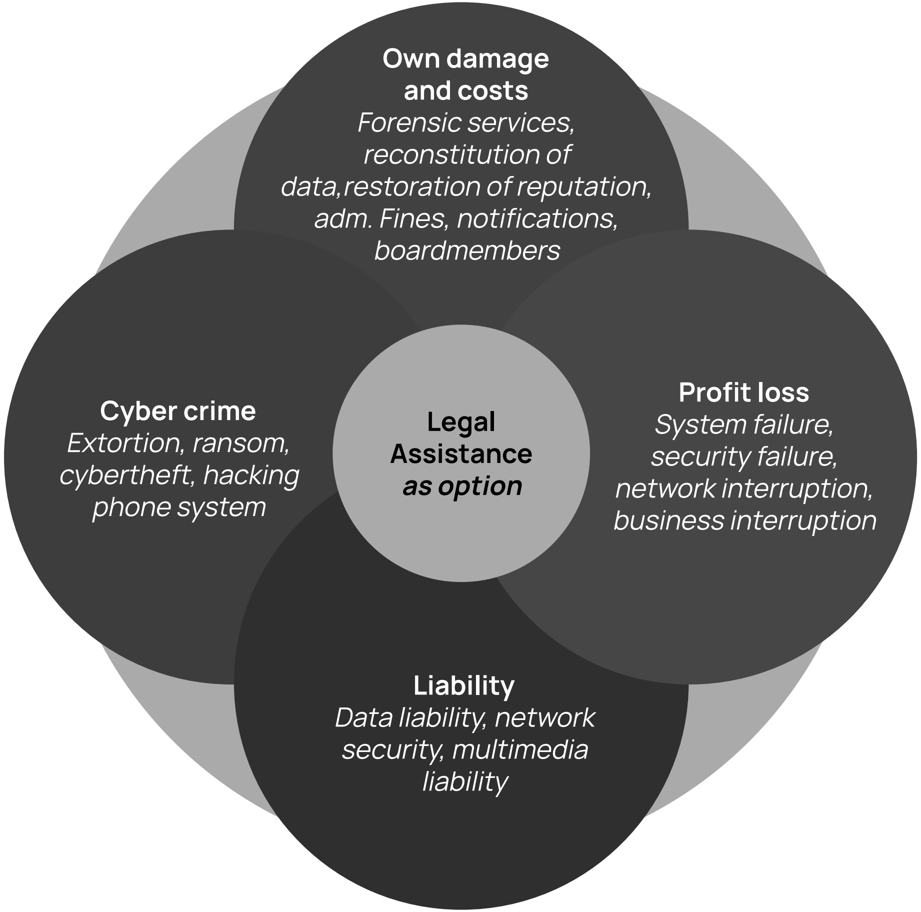
PREVENTION
Advise on **easy actions** you should take today, awareness, safety culture, knowledge sharing....

DIGITAL FOOTPRINT
Free **external** scan to visualise how hackers look at your company (Ceeyu.io)
Free **internal** scan to detect unsafe endpoints (xfa.tech)

ACTION PLAN
Audits on **technical** level (*AD, Network, infrastructure, remote access, IoT, pentesting…*) as well as on a **functional** level (*Legal, policies, procedures, playbooks…*)

Modern CyberSecurity: **REACTIVE**

- 100% safe does not exist
  - **Insure** the rest-risk
- Our policy is primarily **solution oriented**
  - Incident Management
    - 24/7 Hotline
    - IT Forensic Services
    - Legal Services
  - Recovery
    - Financial
    - Liability & Claims
    - Reputation
    - ...



Own damage and costs
Forensic services, reconstitution of data,restoration of reputation, adm. Fines, notifications, boardmembers

Cyber crime
Extortion, ransom, cybertheft, hacking phone system

Legal Assistance
as option

Profit loss
System failure, security failure, network interruption, business interruption

Liability
Data liability, network security, multimedia liability

Wrap-up

Ready to optimize your cybersecurity?

What about some help...
and **2 exclusive offers**

Let’s help you optimize your cybersecurity

XFA

Free devices diagnose

via XFA *3 months FREE*

You will find out:

- Listing of ALL devices used for work
  (incl. computers, smartphones, tablets, chromebooks)
- Identification of all unsafe devices
- Key security checks that are missing

Send mail to info@xfa.tech
Mention reference: **MODERN CYBERSECURITY**

CyberContract

Free External diagnose

For **anyone** attending this webinar.
You will get actionable insight in all the open digital doors and windows
(performed by Ceeyu.io)

+ 2 Hours Free Consulting

For the best LinkedIn post about this webinar.
Our CyberSecurity Coach
guiding you from cybersecurity
to cyber resilience.

Thank you

XFA × CyberContract