Today
IT-Security Ausblick
by

TEMS SECURITY SERVICES

Work smarter
Not harder

PHILIP BERGER

MICHAEL MEIXNER

Agenda

- Es war einmal vor 20 Jahren …
- Cyber Kill Chain
- Huhn oder Ei Problem des Hackers
- Weiterbildung
- Passwörter
- Zero Trust Concept / Model
- Die falsche Sicherheit
- Software

tems security

HOL

Kein Ausblick ohne Rückblick

Es war einmal vor 20 Jahren …

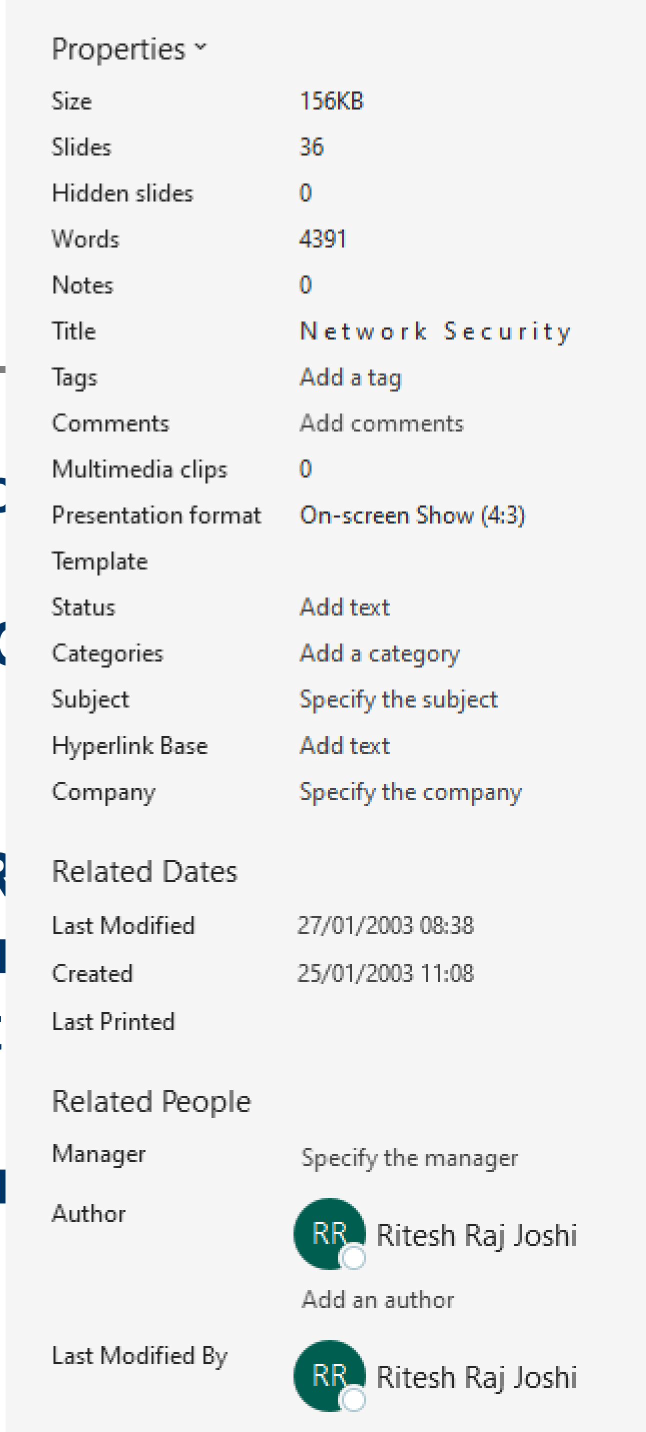
tems security

Netwo pplications

CAN IT (

Ritesh R
Manage
Mercant

ritesh@r



Properties

Size	156KB
Slides	36
Hidden slides	0
Words	4391
Notes	0
Title	Network Security
Tags	Add a tag
Comments	Add comments
Multimedia clips	0
Presentation format	On-screen Show (4:3)
Template	
Status	Add text
Categories	Add a category
Subject	Specify the subject
Hyperlink Base	Add text
Company	Specify the company

Related Dates

Last Modified	27/01/2003 08:38
Created	25/01/2003 11:08
Last Printed	

Related People

Manager	Specify the manager
Author	RR Ritesh Raj Joshi Add an author
Last Modified By	RR Ritesh Raj Joshi

Quelle: Internet

Network Security Applications

- **Mistakes People Make that Lead to Security Breaches**
  - **The Ten Worst Security Mistakes IT People Make**

1. ⏰ Connecting systems to the Internet before hardening them.
2. Connecting test systems to the Internet with default accounts/passwords.
3. ⏰ Failing to update systems when security holes are found.
4. Using telnet and other unencrypted protocols for managing systems, routers, firewalls, and PKI.
5. Giving users passwords over the phone or changing user passwords in response to telephone or personal requests when the requester is not authenticated.
6. ⏰ Failing to maintain and test backups.
7. ⏰ Running unnecessary services : ftpd, telnetd, finger, rpc, mail, rservices
8. ⏰ Implementing firewalls with rules that don't stop malicious or dangerous traffic - incoming and outgoing.
9. ⏰ Failing to implement or update virus detection software.
10. ⏰ Failing to educate users on what to look for and what to do when they see a potential security problem.

Quelle: Internet

Network Security Applications

Mistakes People Make that Lead to Security Breaches

The Seven Worst Security Mistakes Senior Executives Make

1. Assigning untrained people to maintain security and providing neither the training nor the time to make it possible to learn and do the job.
2. Failing to understand the relationship of information security to the business problem - they understand physical security but do not see the consequences of poor information security.
3. Failing to deal with the operational aspects of security: making a few fixes and then not allowing the follow through necessary to ensure the problems stay fixed.
4. Relying primarily on a firewall
5. Failing to realize how much money their information and organizational reputations are worth.
6. Authorizing reactive, short-term fixes so problems re-emerge rapidly.
7. Pretending the problem will go away if they ignore it.

Quelle: Internet

Network Security Applications

Security Best Practices

- **Benefits of implementing best security practices:**
- To make it so difficult for an attacker to gain access that he gives up before he gets in
- Many sites have minimal or no security - attackers usually gain access relatively quickly and with a low level of expertise
- With some security, chances of an attacker exploiting its systems are decreased significantly - the intruder will probably move on to a more vulnerable site
- “The idea is not that you should protect a system to the point it cannot be compromised, but to secure it at least enough so that most intruders will not be able to break in, and will choose to direct their efforts elsewhere”
- e.g. it is just like putting iron bars and locks on our windows and doors - we do it not to "keep the robbers out", but to persuade them to turn their attention to our neighbors

Quelle: Internet

Network Security Applications

- **Security Best Practices**
  - **Backup**
    - Maintain full and reliable backups of all data, log files
    - Archive all software (purchased or freeware), upgrades, and patches off-line so that it can be reloaded when necessary
    - Backup configurations, such as the Windows registry and text/binary configuration files, used by the operating systems or applications
    - Consider the media, retention requirements, storage, rotation, methods (incremental, differential, full) and the scheduling
    - Keep copy of a full backup in a secure off-site location for disaster recovery

Quelle: Internet

Network Security Applications

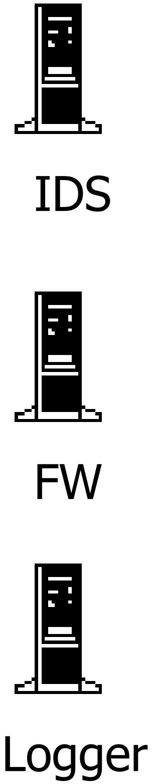
- ## Security Best Practices
  - ### Password Policies
    - While there are promising technologies on the horizon that could replace passwords as a method of authenticating clients, at present we are reliant on passwords
    - Use secure authentication like PKI, digital certificates, ssh, etc.
    - A password policy should define the required characteristics of accepted passwords for each system:
      - Minimum length
      - Composition; alpha, upper or lower case, numeric, special
      - Effective life
      - Uniqueness (how often a password can be reused)
      - Lockout properties; under what conditions, and for how long
      - These characteristics differ from system to system because each has different capabilities

Quelle: Internet

Network Security Applications

Security Best Practices

Enable and Monitor Logging and Auditing on a 24x7 basis



- "Prevention is ideal, but detection is a must"
- We must realize that “No prevention technique is full-proof”
- New vulnerabilities are discovered every week that you may not be aware of
- Constant vigilance is required to detect new unknown attacks
- Once you are attacked, without logs, you have little chance of finding what the attackers did
- You can not detect an attack if you do not know what is occurring on your network
- Logs provide the details of what is occurring, what systems are being attacked, and what systems have been compromised
- If any log entries that don't look right, and investigate them immediately

Quelle: Internet

Hacking
1x1

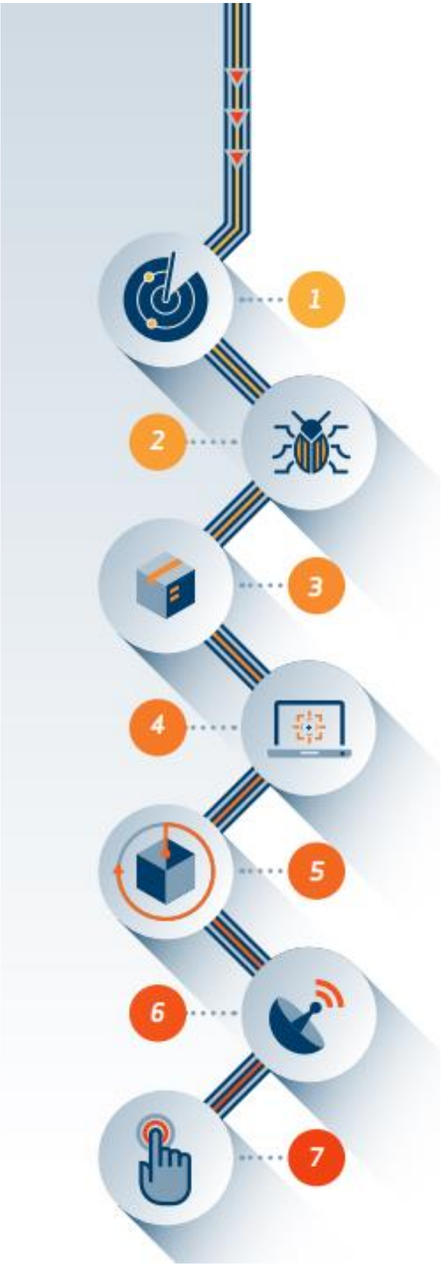
tems security

Hacking 1x1

1. Cyber Kill Chain

tems security

Hacking workflow



RECONNAISSANCE

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND & CONTROL (C2)

ACTIONS ON OBJECTIVES (what`s next?)

THE LOCKHEED MARTIN CYBER KILL CHAIN ®

Source: https://www.lockheedmartin.com/

Hacking 1x1

2. Wie finde ich verwundbare Systeme?

tems security

Huhn oder Ei

https://crt.sh/

https://dnsdumpster.com/

https://www.shodan.io/

https://www.exploit-db.com/

https://www.cvedetails.com/vulnerability-list/

tems security

Weiterbildung in IT-Security?

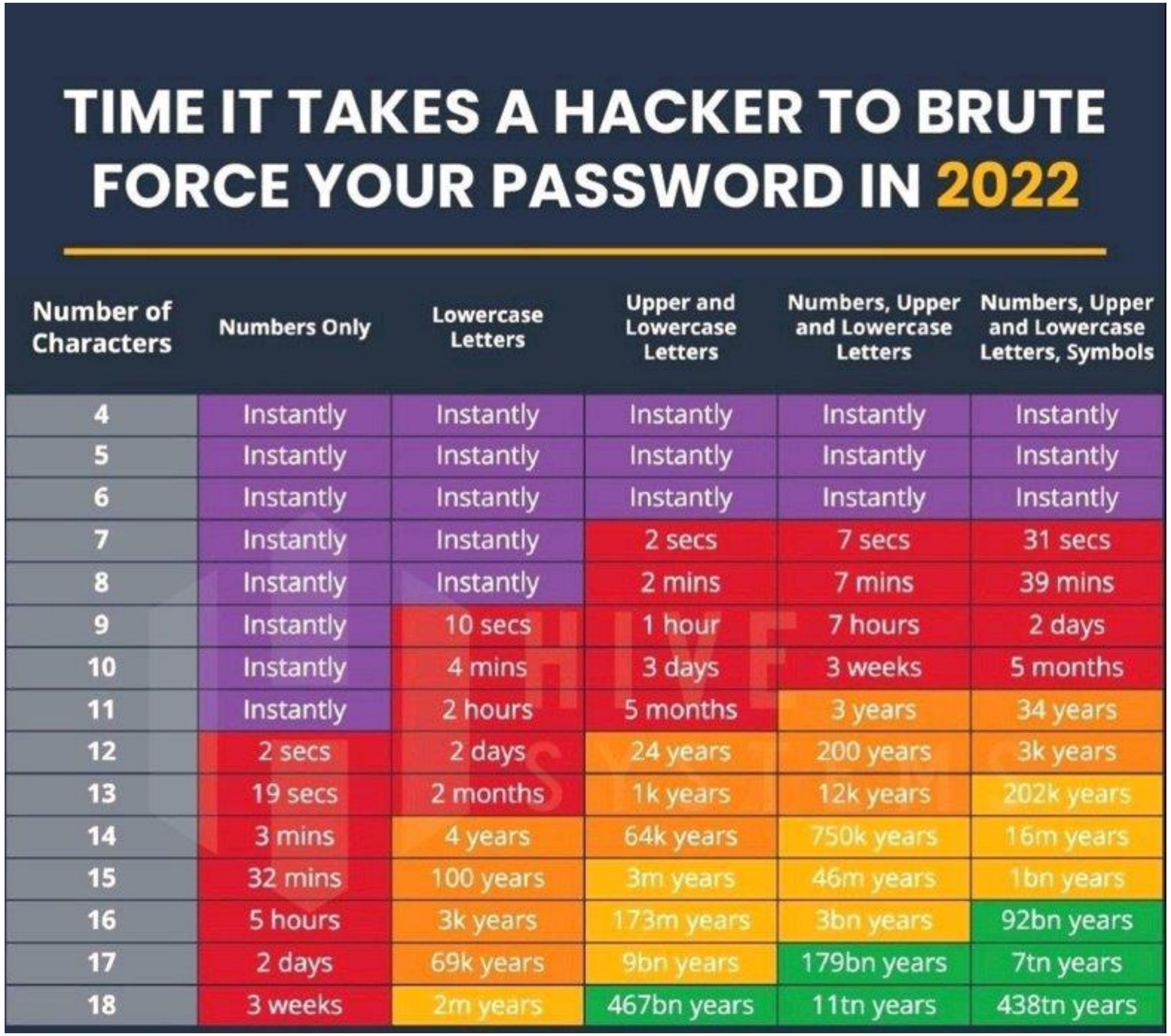
tems security

Rules of the game

- The hacker needs **only one Vulnerability or Misconfiguration** and the hacker has access to a company network.
- A company can catch the hacker with **only through command or lateral movement** within the network and we are able to detect the hacker.

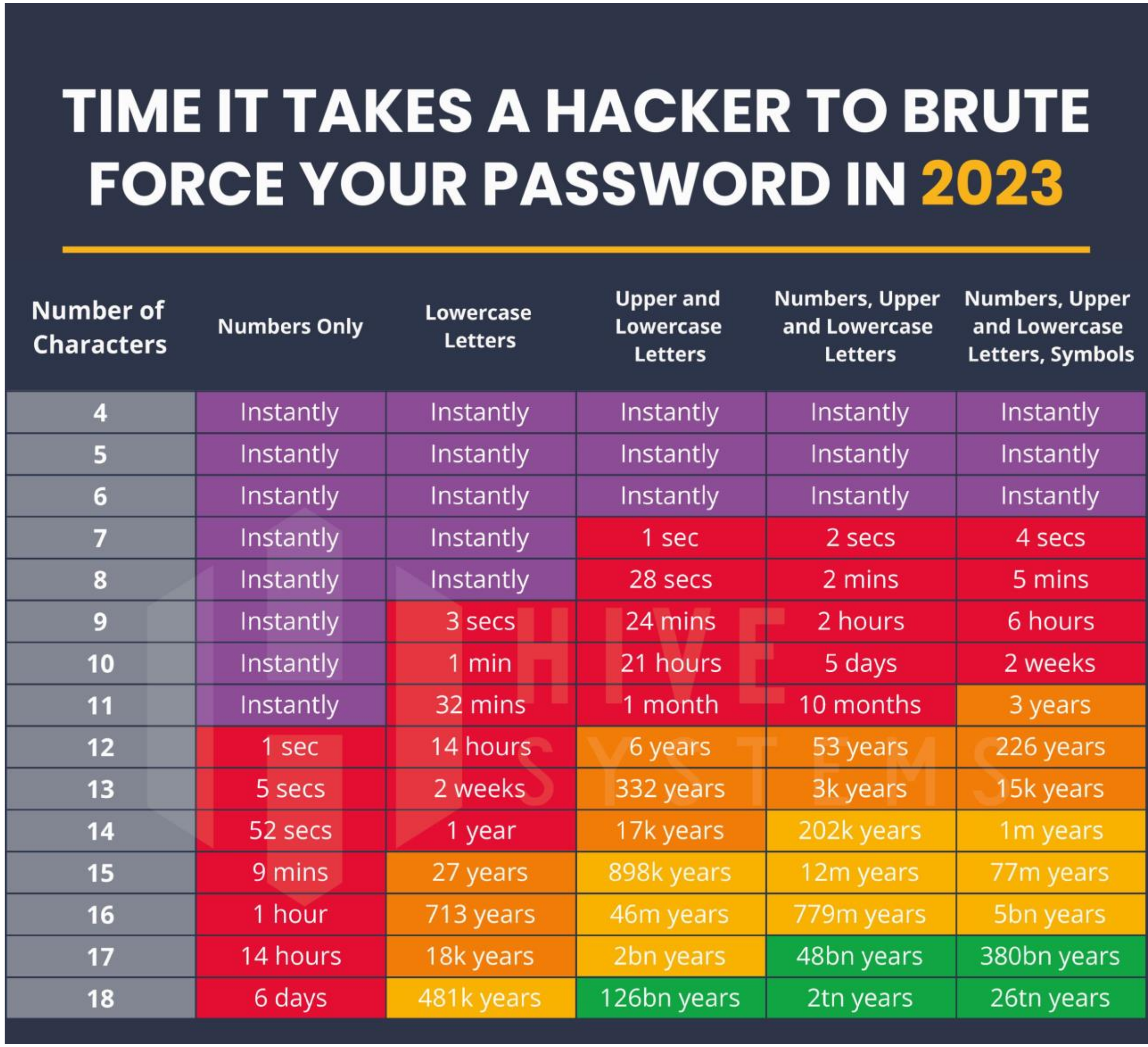
Training and knowledge are the key factor for success.

Passwörter



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

Aktuelle IT-Security unbewusste Gefahren

tems security

Zero-Day-Lücke: Leck in Barracudas ESG

CVE-2023-23397 Addresses NTLM Vulnerability

An attacker can exploit the vulnerability by sending a specially-formatted appointment to a user. The appointment is already expired and its *PidLidReminderFileParameter* property points to a UNC path, which provokes Windows to send the user's login name and their NTLM password hash (a technique used in other attacks like this example). When Outlook processes the message, the attacker gets the user credentials and can use them to compromise the account. Because the message is an appointment, Outlook doesn't open it in its preview pane and processes the calendar item behind the scenes, so the user might not even be aware that they received a malicious appointment.

Multifaktor Authentifizierung

tems security

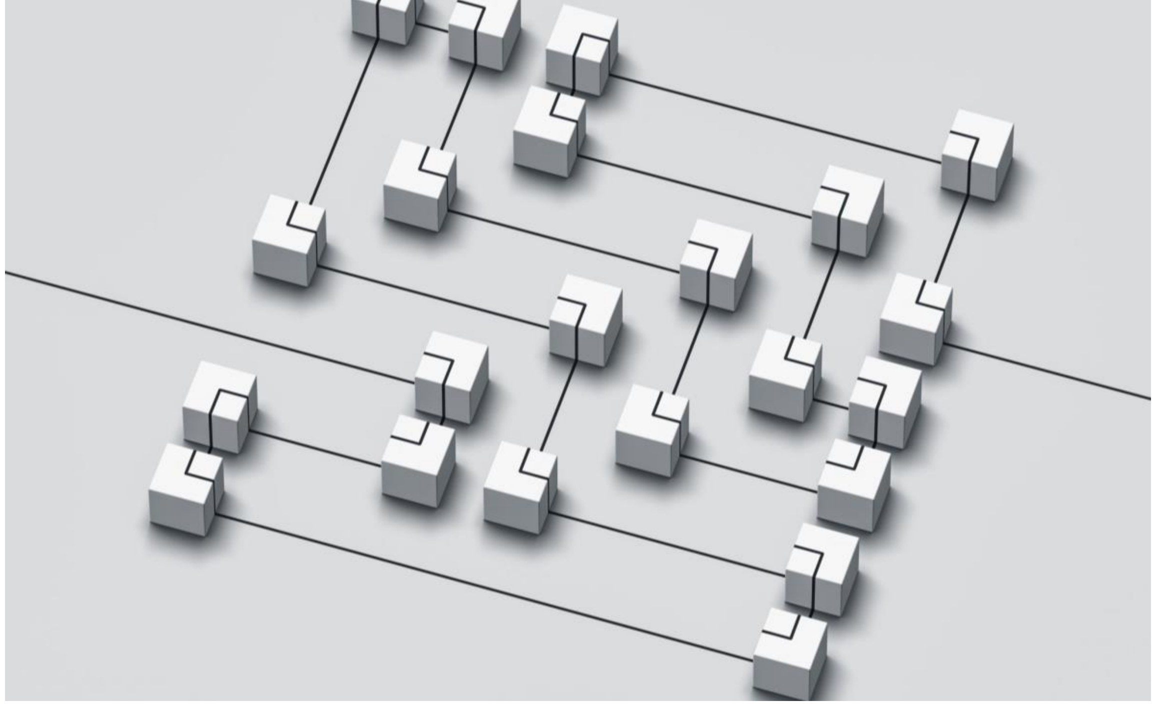
Digital Supply Chain Attack

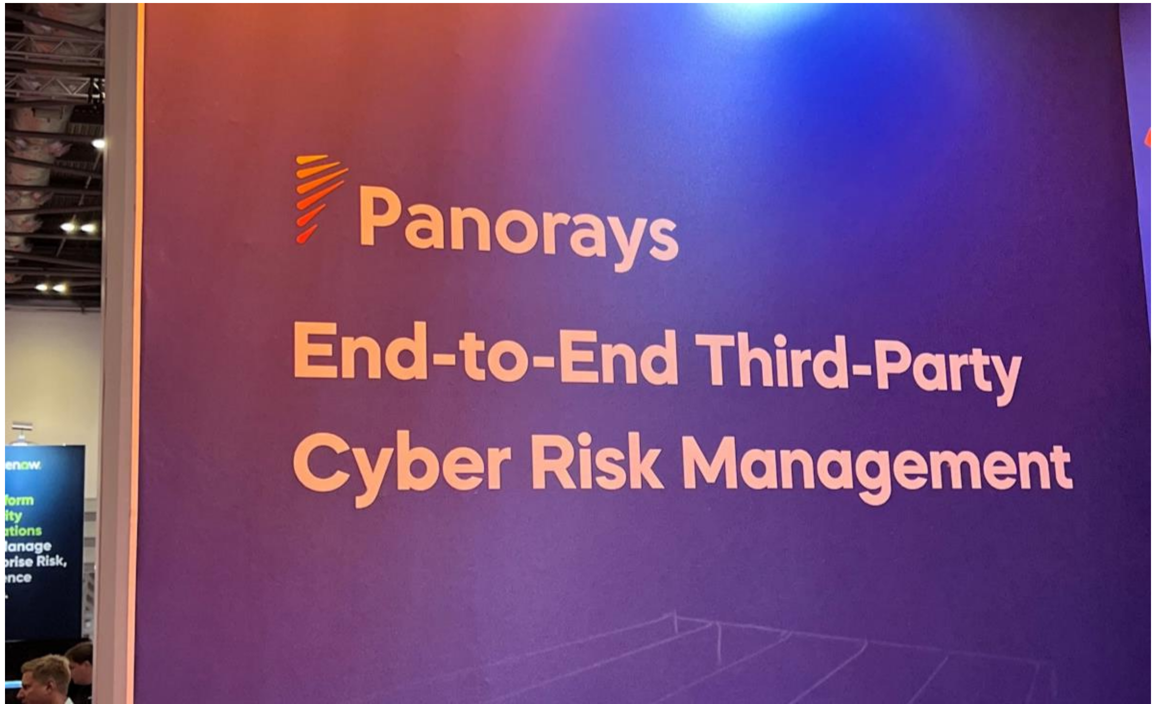
Digital Supply Chain Attack

Mit der zunehmenden Vernetzung mit Geschäftspartnern und Systeme

- Netzwerk
- API Zugriff
- VPN-Zugriff
- OT /IoT

stellt diese eine weitere Herausforderung für Ihre IT Sicherheit dar.



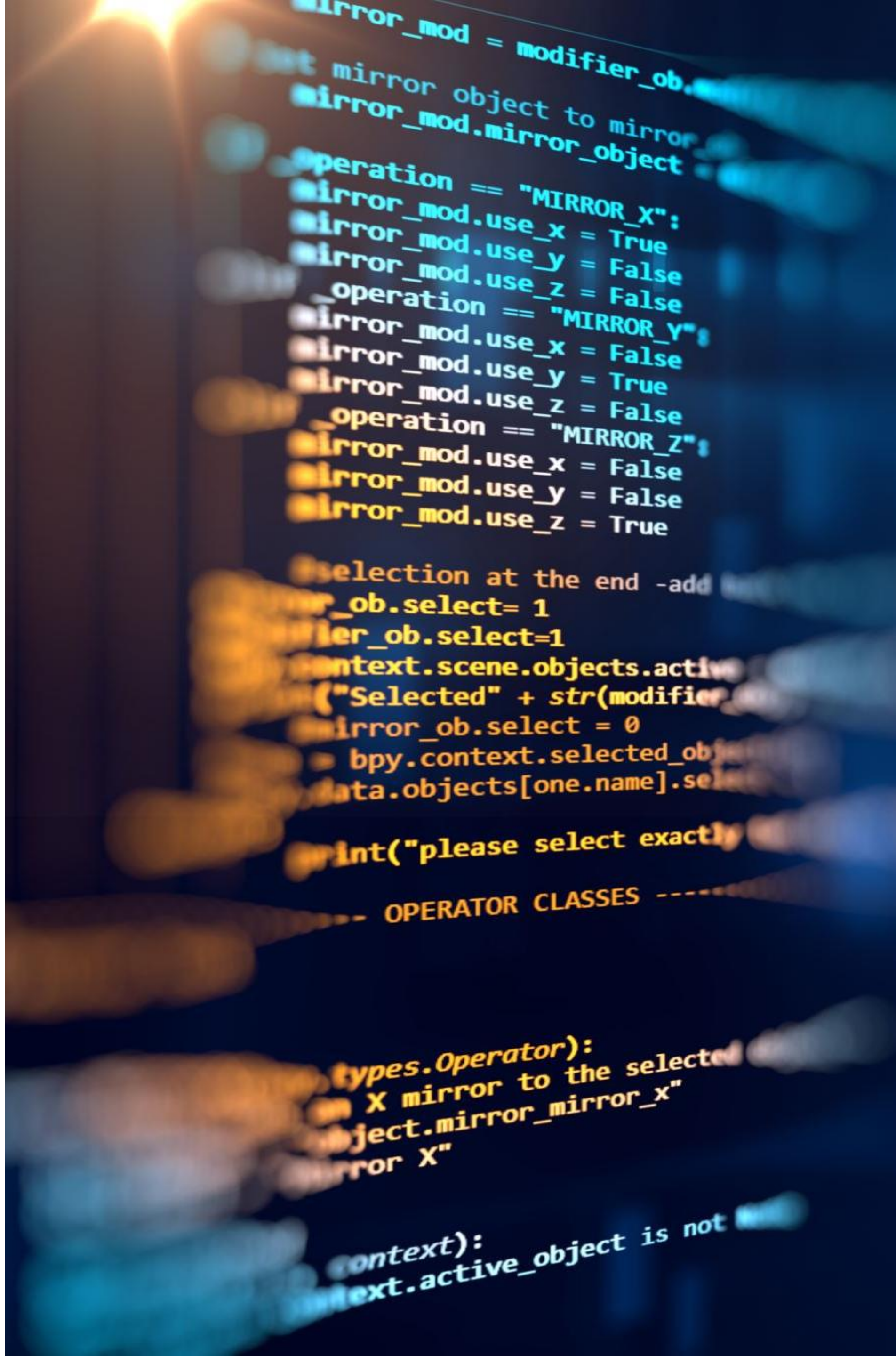


tems
security

Multi Channel Phishing

Multi Channel Phishing

- Linkedin (Fake Accounts invite)
- Slack (Username / Password)
- Tik Tok (blur picture, Download software)
- Whats App (Fake co-worker, Excel, Winword)
- Vom Mobile to Desktop (incompatible Browser)
- Microsoft Teams (Chat Funktion, Datentransfer)

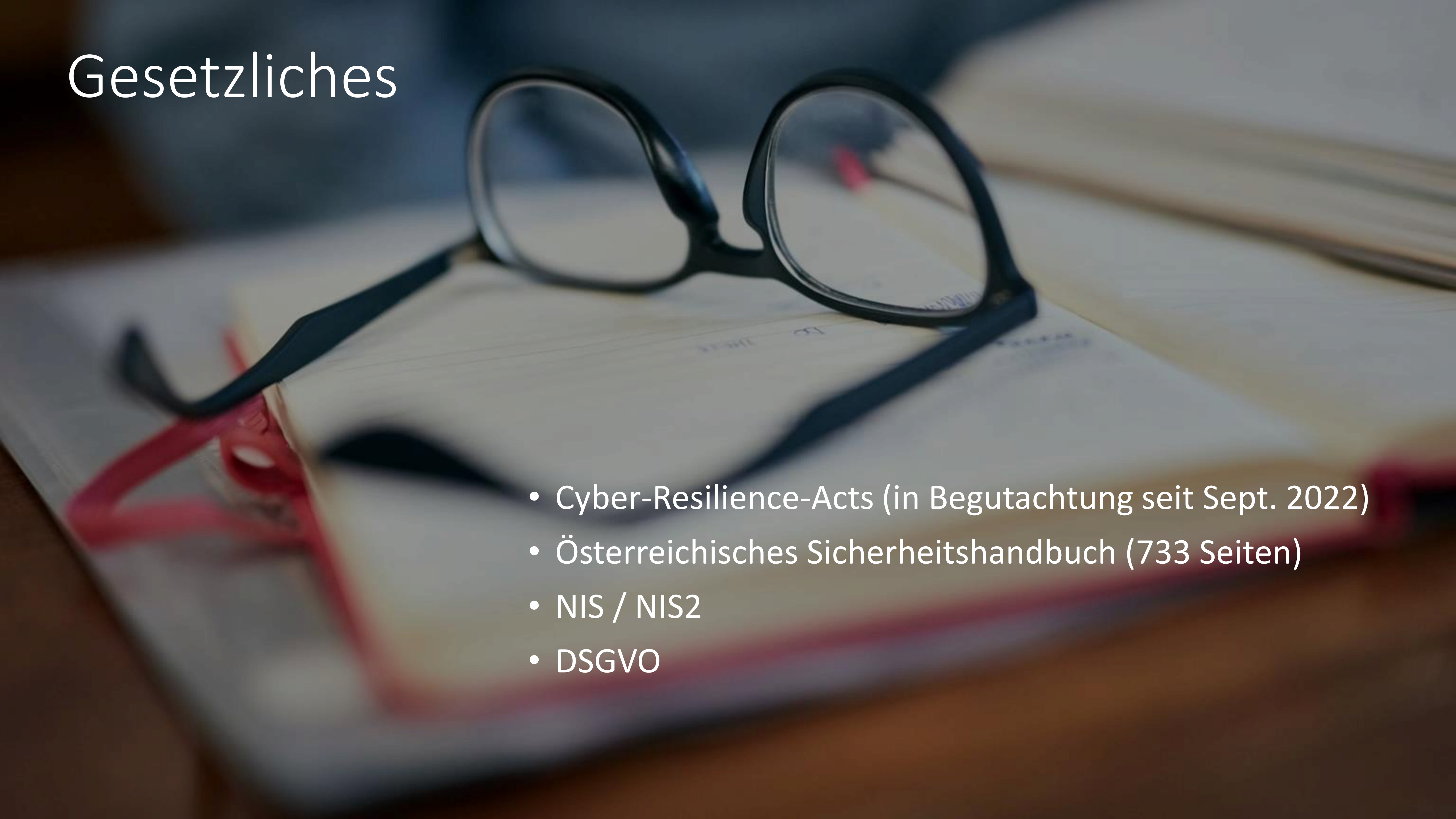


```
irror_mod = modifier_ob
mirror object to mirror
irror_mod.mirror_object
peration == "MIRROR_X":
irror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
 operation == "MIRROR_Y"
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
 operation == "MIRROR_Z"
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True

selection at the end -add
_ob.select= 1
er_ob.select=1
ntext.scene.objects.active
("Selected" + str(modifier
irror_ob.select = 0
 bpy.context.selected_ob
ata.objects[one.name].sel

int("please select exactly

 OPERATOR CLASSES ----

types.Operator):
 X mirror to the selected
ject.mirror_mirror_x"
rror X"

ontext):
ext.active_object is not
```

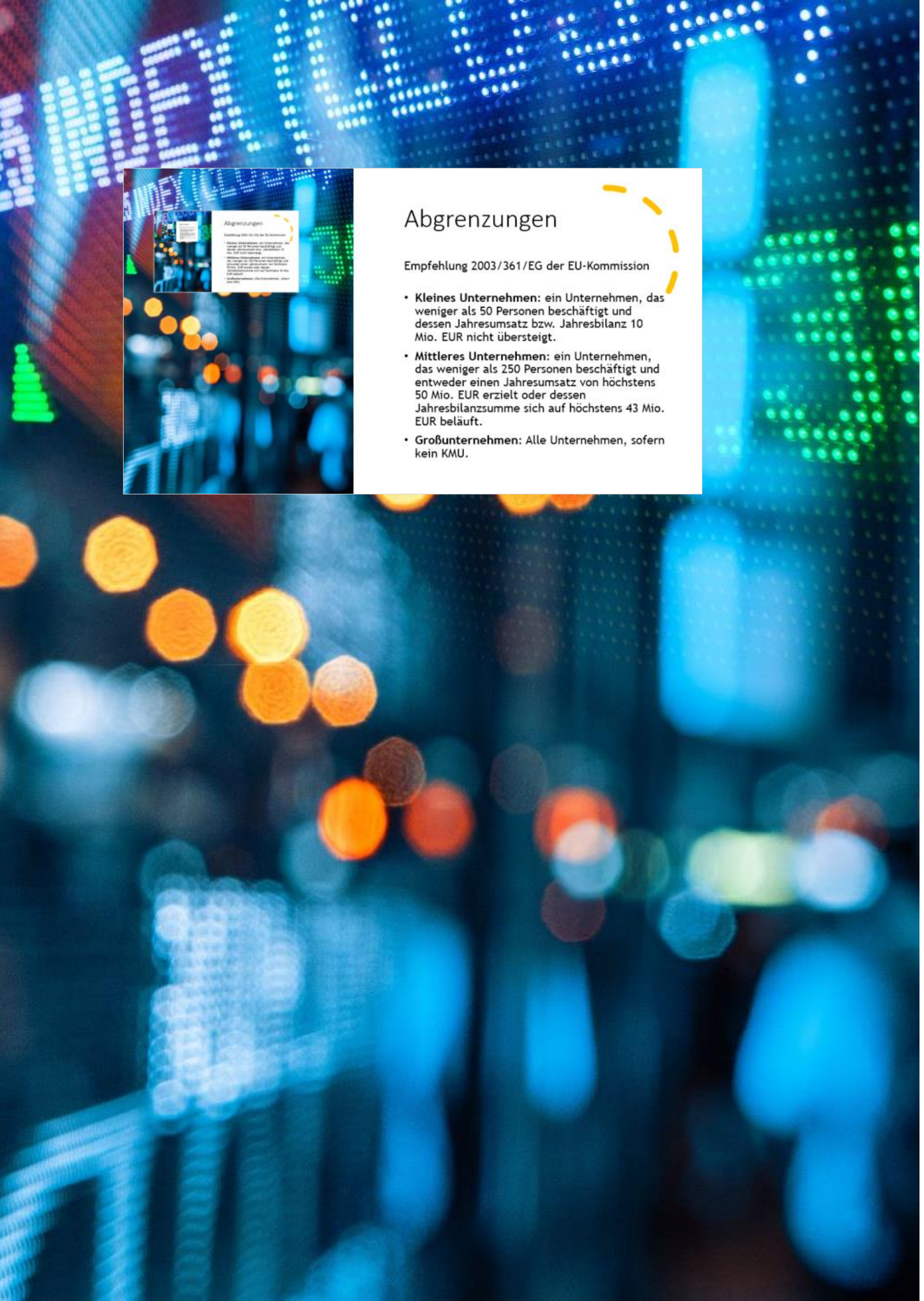
Gesetzliche Vorgaben / Richtlinien

tems security

Gesetzliches



- Cyber-Resilience-Acts (in Begutachtung seit Sept. 2022)
- Österreichisches Sicherheitshandbuch (733 Seiten)
- NIS / NIS2
- DSGVO



Abgrenzungen

Empfehlung 2003/361/EG der EU-Kommission

- **Kleines Unternehmen**: ein Unternehmen, das weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 10 Mio. EUR nicht übersteigt.
- **Mittleres Unternehmen**: ein Unternehmen, das weniger als 250 Personen beschäftigt und entweder einen Jahresumsatz von höchstens 50 Mio. EUR erzielt oder dessen Jahresbilanzsumme sich auf höchstens 43 Mio. EUR beläuft.
- **Großunternehmen**: Alle Unternehmen, sofern kein KMU.

Abgrenzungen

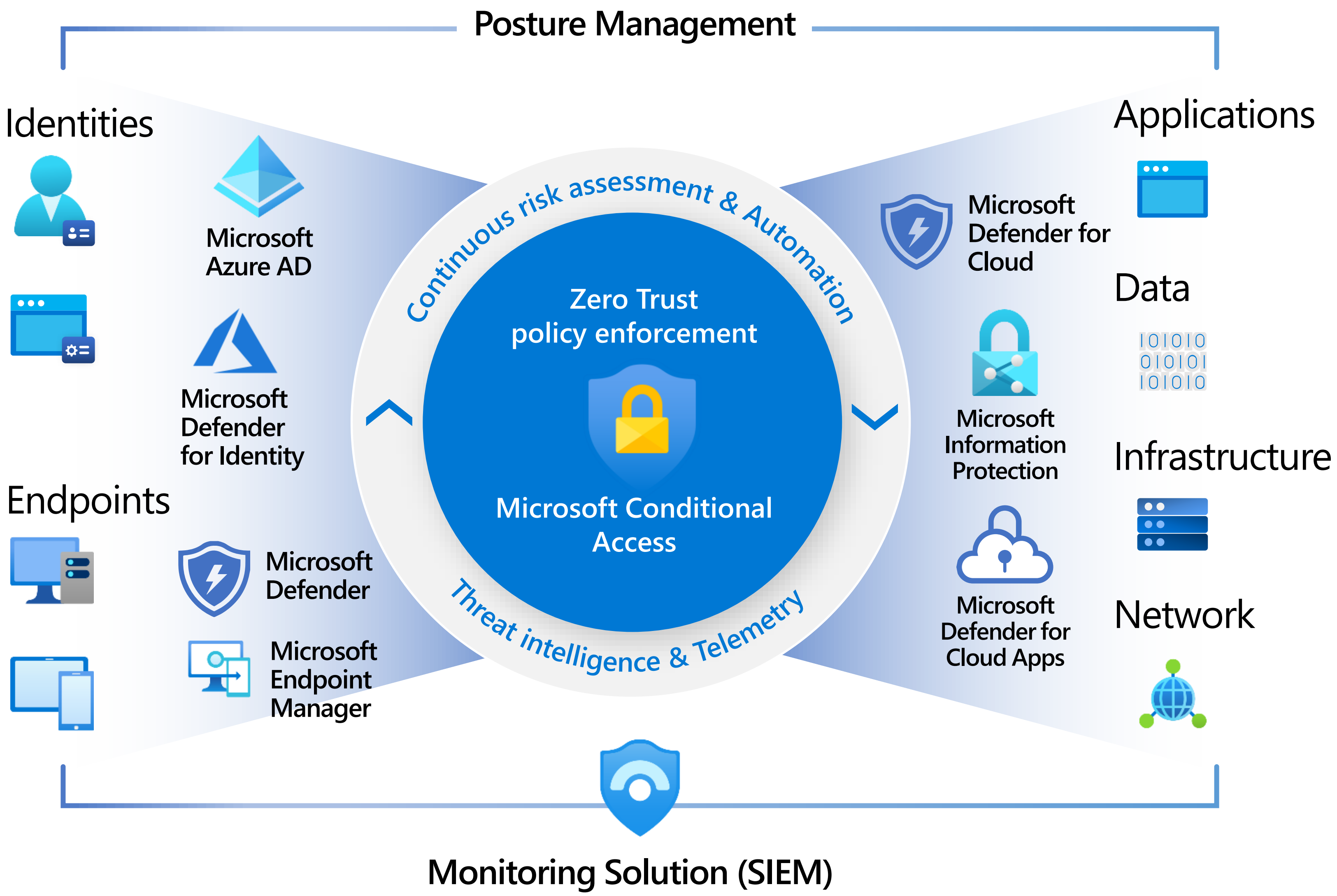
Empfehlung 2003/361/EG der EU-Kommission

- **Kleines Unternehmen**: ein Unternehmen, das weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 10 Mio. EUR nicht übersteigt.
- **Mittleres Unternehmen**: ein Unternehmen, das weniger als 250 Personen beschäftigt und entweder einen Jahresumsatz von höchstens 50 Mio. EUR erzielt oder dessen Jahresbilanzsumme sich auf höchstens 43 Mio. EUR beläuft.
- **Großunternehmen**: Alle Unternehmen, sofern kein KMU.

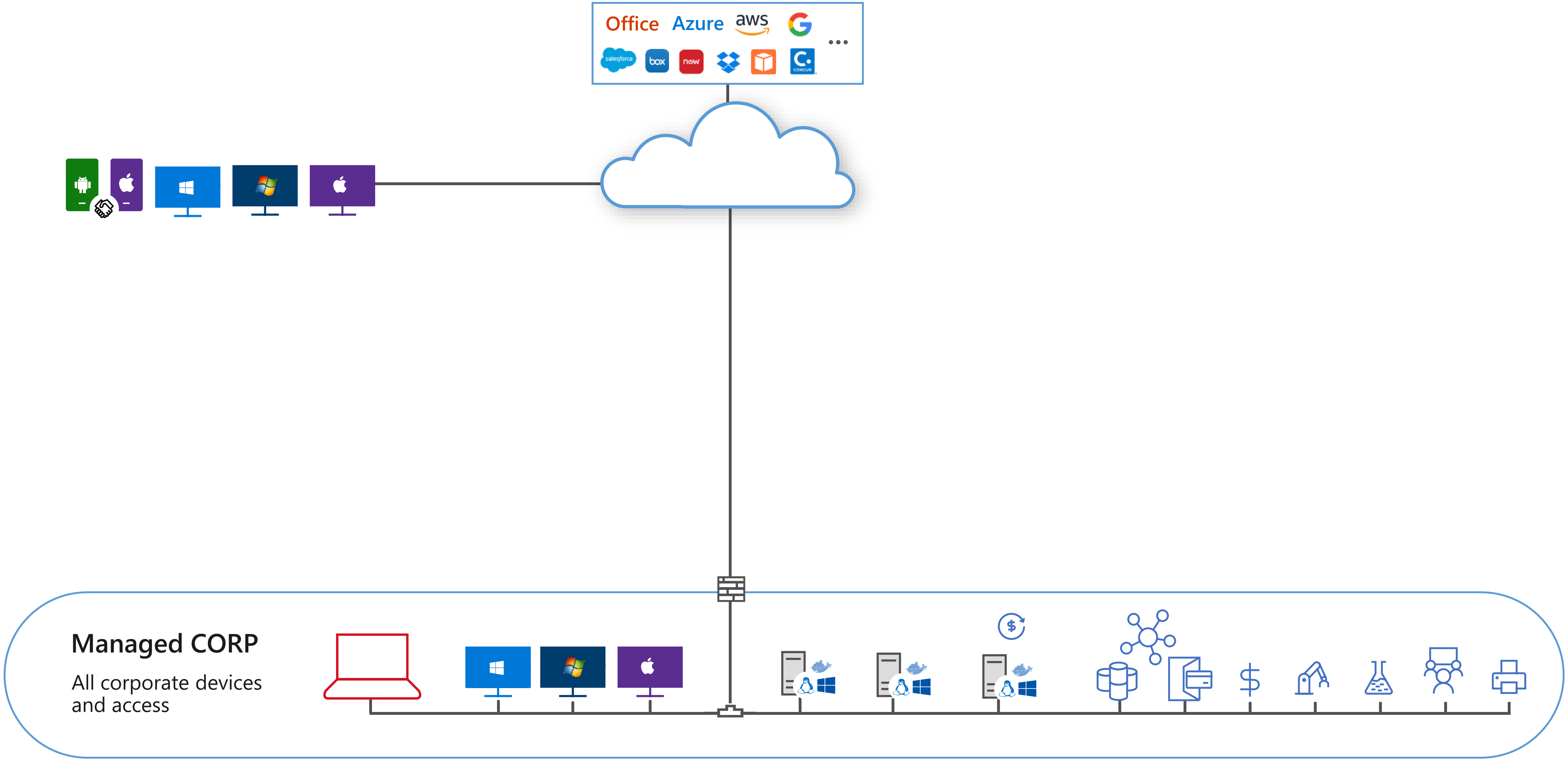
Zero Trust Model

tems security

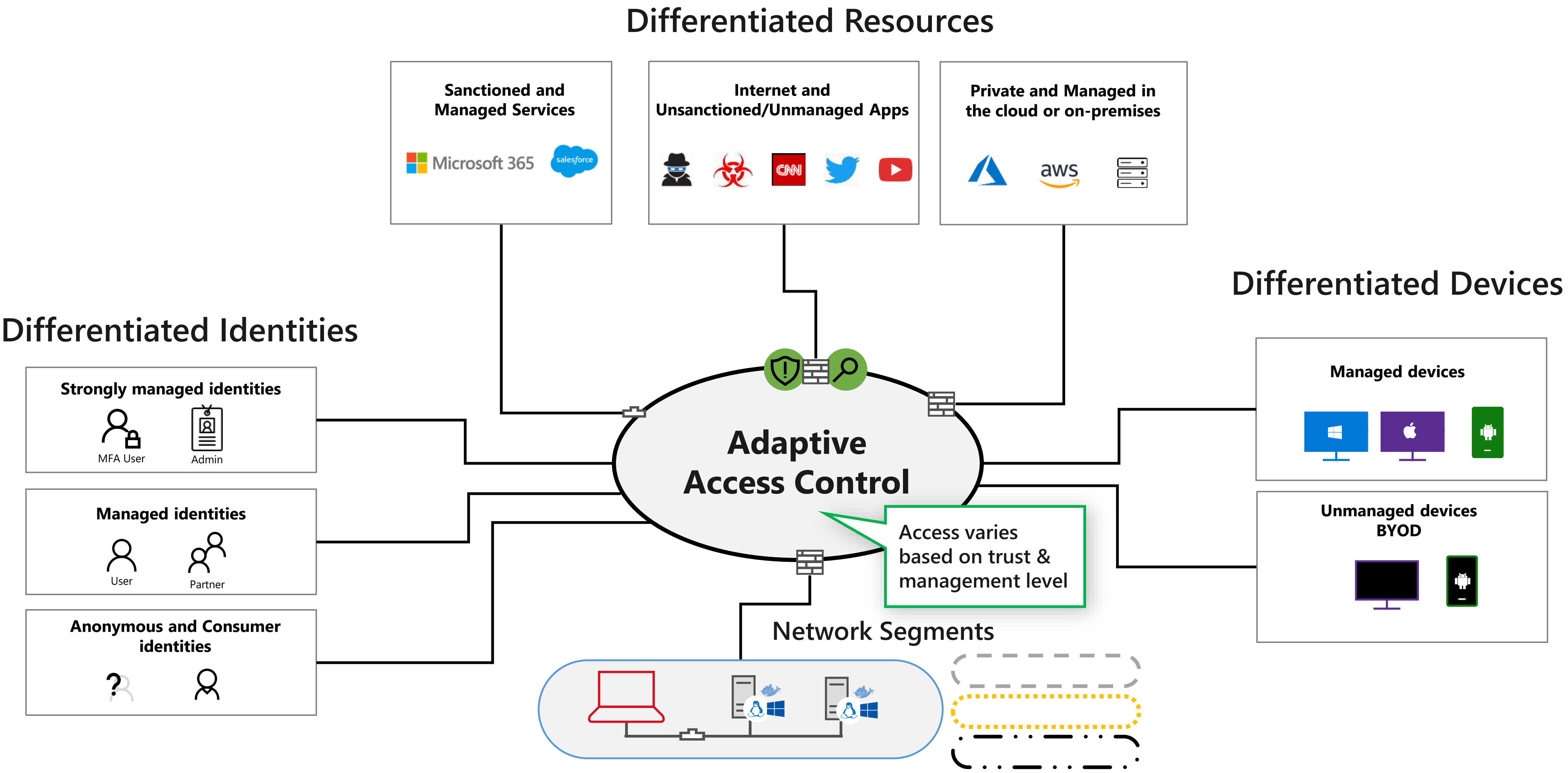
Microsoft Zero Trust Concept


Posture Management
Identities
Microsoft Azure AD
Microsoft Defender for Identity
Endpoints
Microsoft Defender
Microsoft Endpoint Manager
Continuous risk assessment & Automation
Zero Trust policy enforcement
Microsoft Conditional Access
Threat intelligence & Telemetry
Applications
Microsoft Defender for Cloud
Data
10101
01010
10101
Microsoft Information Protection
Infrastructure
Microsoft Defender for Cloud Apps
Network
Monitoring Solution (SIEM)

Typical 'Flat' Network



Full Zero Trust End State



Differentiated Resources

Sanctioned and Managed Services

Internet and Unsanctioned/Unmanaged Apps

Private and Managed in the cloud or on-premises

Differentiated Identities

Strongly managed identities

Managed identities

Anonymous and Consumer identities

Adaptive Access Control

Access varies based on trust & management level

Differentiated Devices

Managed devices

Unmanaged devices BYOD

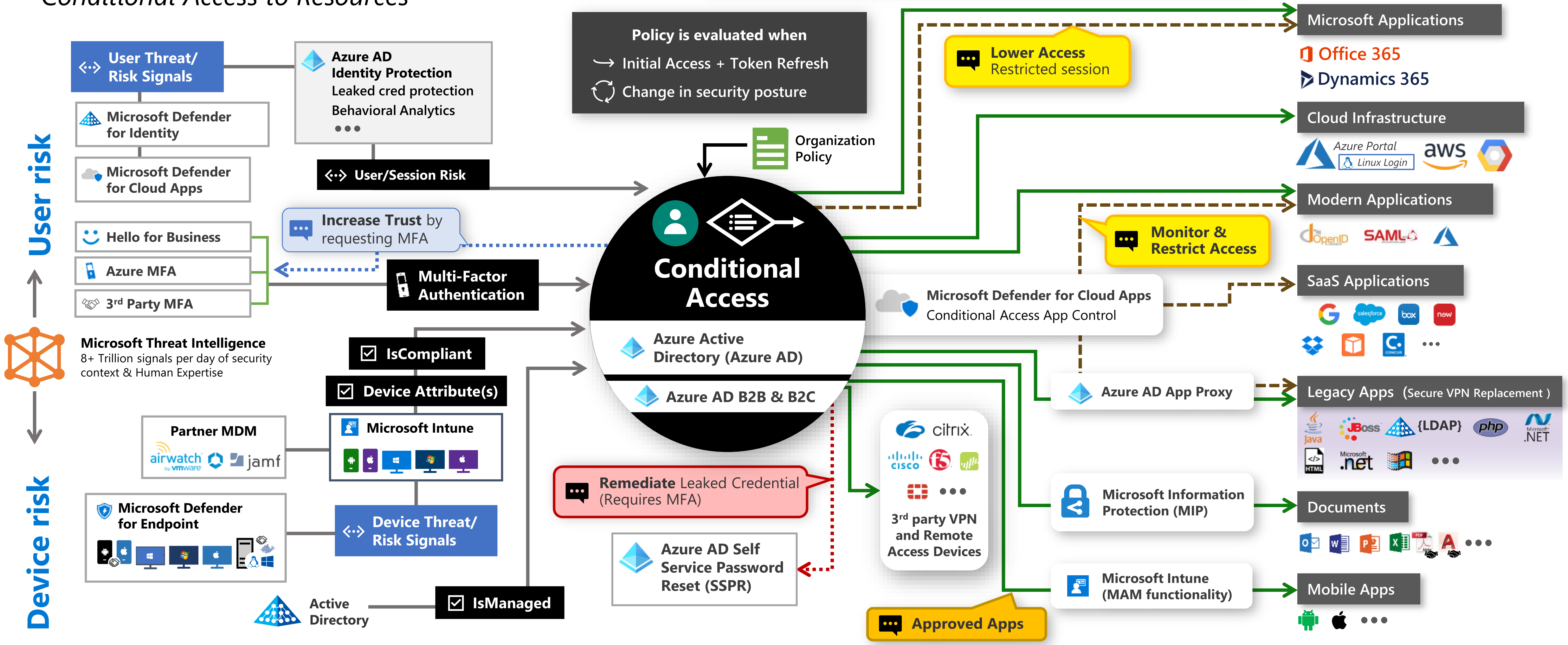
Network Segments

Zero Trust User Access

Conditional Access to Resources

Legend

Full access	Limited access
Risk Mitigation	Remediation Path



User risk

User Threat/ Risk Signals

Azure AD Identity Protection
Leaked cred protection
Behavioral Analytics
•••

Microsoft Defender for Identity

Microsoft Defender for Cloud Apps

User/Session Risk

Policy is evaluated when
Initial Access + Token Refresh
Change in security posture

Organization Policy

Increase Trust by requesting MFA

Hello for Business

Azure MFA

3rd Party MFA

Multi-Factor Authentication

Microsoft Threat Intelligence
8+ Trillion signals per day of security context & Human Expertise

Conditional Access

Azure Active Directory (Azure AD)

Azure AD B2B & B2C

IsCompliant

Device Attribute(s)

Partner MDM
airwatch by vmware
jamf

Microsoft Intune

Device risk

Microsoft Defender for Endpoint

Device Threat/ Risk Signals

Active Directory

IsManaged

Remediate Leaked Credential (Requires MFA)

Azure AD Self Service Password Reset (SSPR)

citrix
cisco
•••
3rd party VPN and Remote Access Devices

Approved Apps

Lower Access
Restricted session

Microsoft Applications
Office 365
Dynamics 365

Cloud Infrastructure
Azure Portal
Linux Login
aws

Modern Applications
OpenID
SAML

Monitor & Restrict Access

Microsoft Defender for Cloud Apps
Conditional Access App Control

SaaS Applications
salesforce
box
now
•••

Azure AD App Proxy

Legacy Apps (Secure VPN Replacement)
Java
JBoss
{LDAP}
php
.NET
HTML
.net
•••

Microsoft Information Protection (MIP)

Documents
•••

Microsoft Intune (MAM functionality)

Mobile Apps
•••

Signal
to make an informed decision

Decision
based on organizational policy

Enforcement
of policy across resources

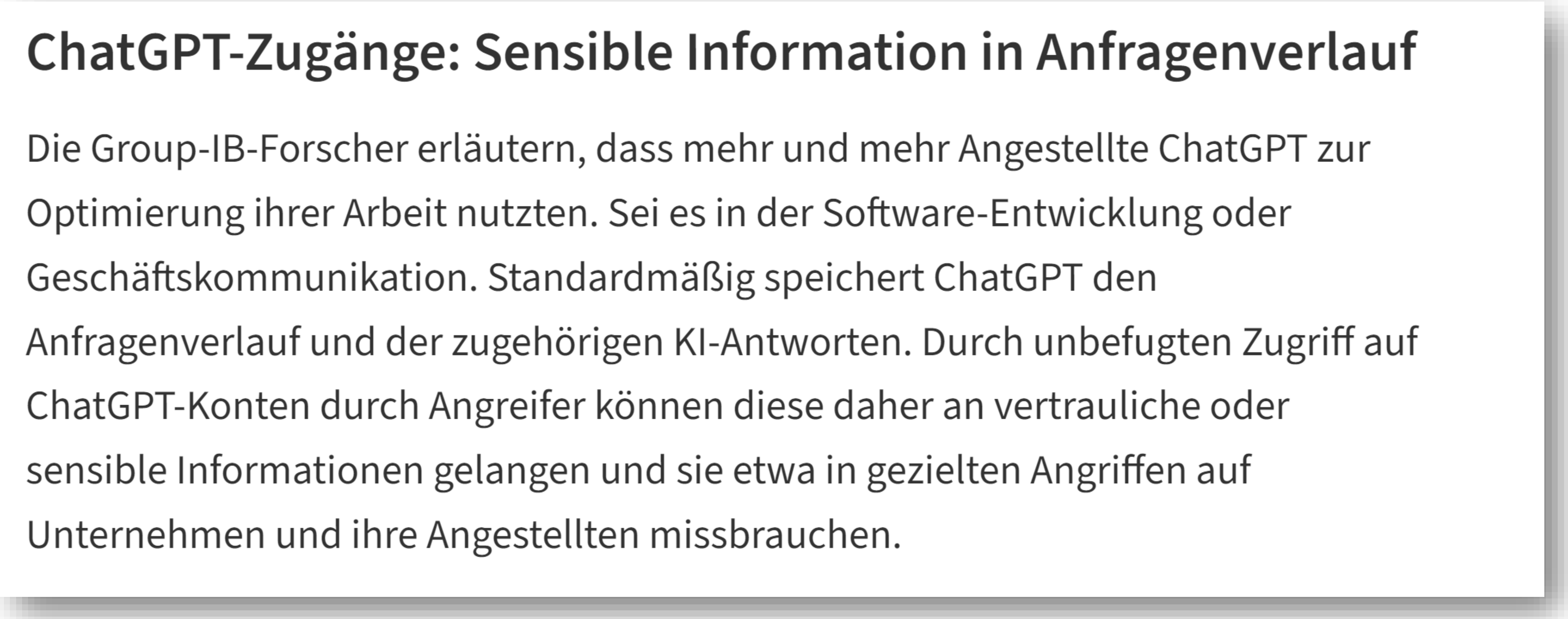
Hype oder kein Hype von AI / KI

tems security

AI / KI

- AI wird immer schneller Schwachstellen in bestehenden Systemen finden, und Hacker werden diese in naher Zukunft noch schneller aktiv ausnutzen.
- Chat GPT kennt die User schon jetzt um ein Vielfaches besser, als Google dies jemals schaffen könnte.
- Ein Datenparadies für jeden Polizei-Profiler.

ChatGPT Zugänge im Darknet (101.134)



ChatGPT-Zugänge: Sensible Information in Anfragenverlauf

Die Group-IB-Forscher erläutern, dass mehr und mehr Angestellte ChatGPT zur Optimierung ihrer Arbeit nutzten. Sei es in der Software-Entwicklung oder Geschäftskommunikation. Standardmäßig speichert ChatGPT den Anfragenverlauf und der zugehörigen KI-Antworten. Durch unbefugten Zugriff auf ChatGPT-Konten durch Angreifer können diese daher an vertrauliche oder sensible Informationen gelangen und sie etwa in gezielten Angriffen auf Unternehmen und ihre Angestellten missbrauchen.

Die falsche IT-Sicherheit

tems security

Software Hersteller:

Microsoft, Google, AV Hersteller

Hardware Hersteller:

Drucker, IoT, Storageüberwachung
Serverüberwachung

IT-Security-Lösungen:

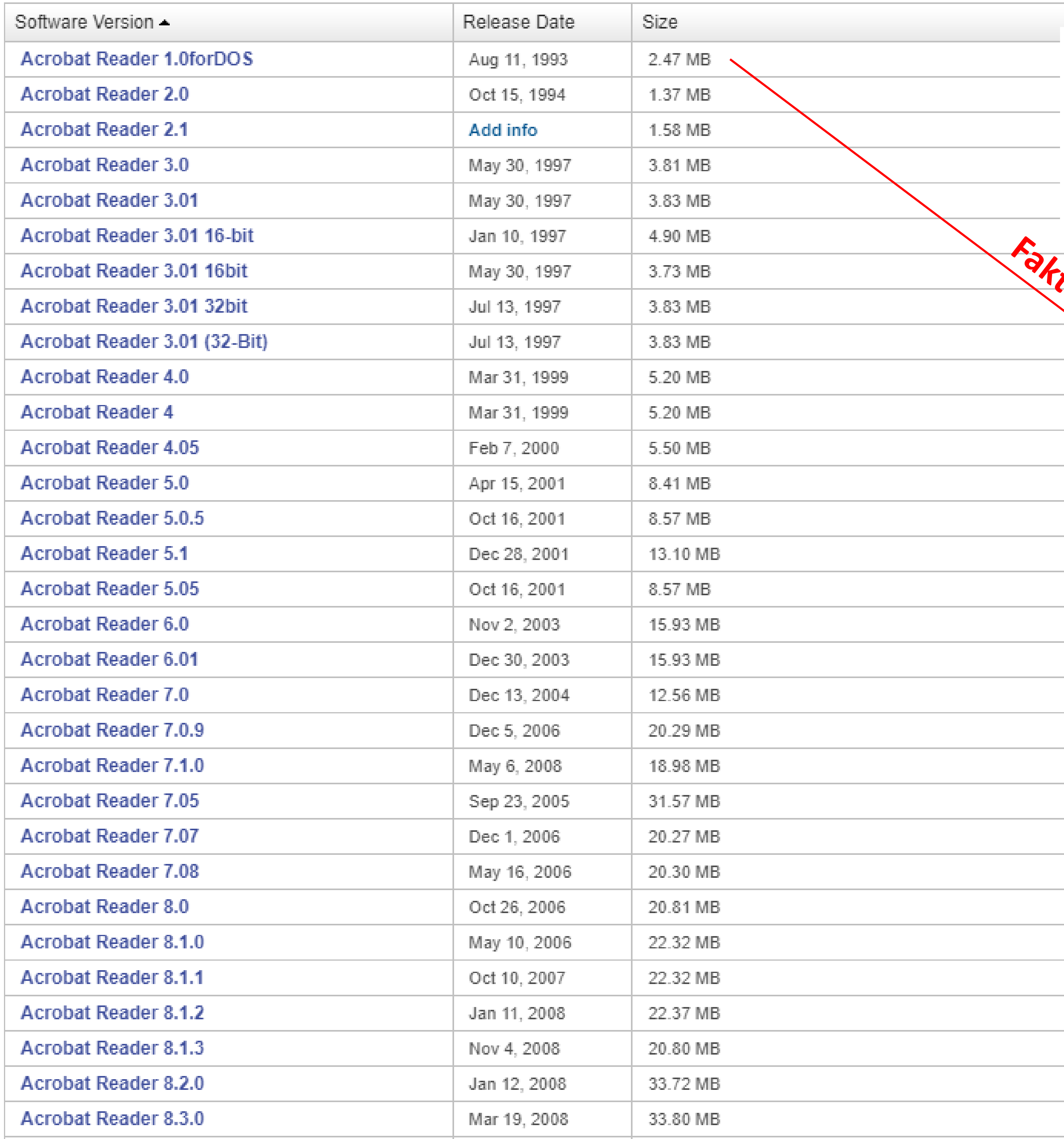
“Alles mit Cloudanbindung”

Externe Dienstleister:

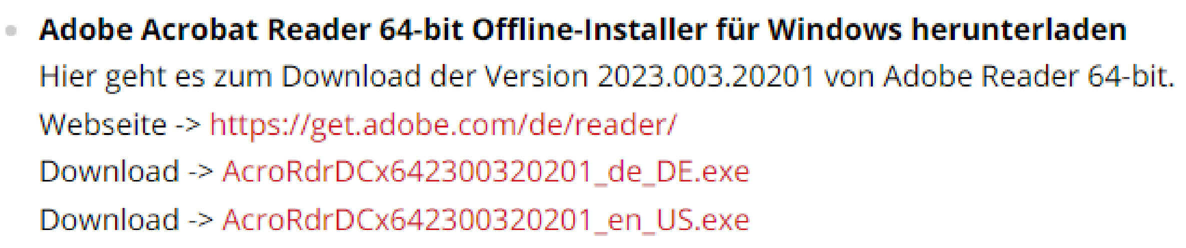
IT-Support, Applikationssupport

Bildquelle: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Software

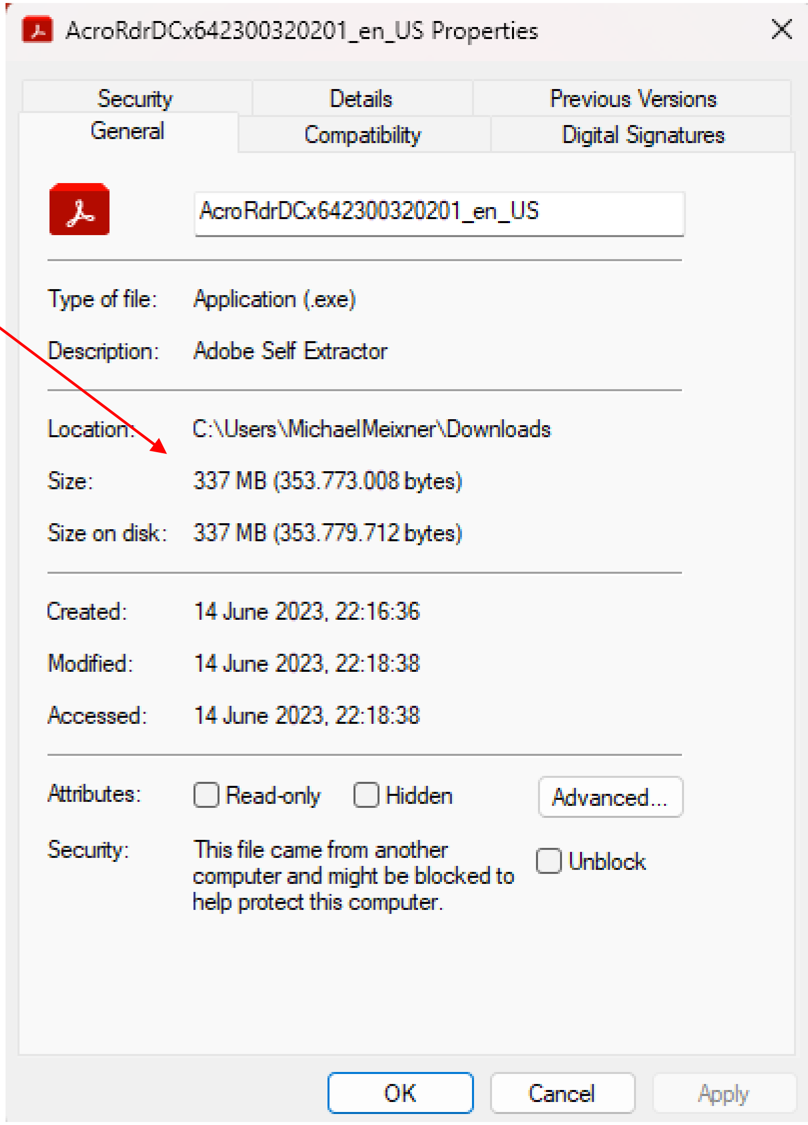


Software Version ▲	Release Date	Size
Acrobat Reader 1.0forDOS	Aug 11, 1993	2.47 MB
Acrobat Reader 2.0	Oct 15, 1994	1.37 MB
Acrobat Reader 2.1	Add info	1.58 MB
Acrobat Reader 3.0	May 30, 1997	3.81 MB
Acrobat Reader 3.01	May 30, 1997	3.83 MB
Acrobat Reader 3.01 16-bit	Jan 10, 1997	4.90 MB
Acrobat Reader 3.01 16bit	May 30, 1997	3.73 MB
Acrobat Reader 3.01 32bit	Jul 13, 1997	3.83 MB
Acrobat Reader 3.01 (32-Bit)	Jul 13, 1997	3.83 MB
Acrobat Reader 4.0	Mar 31, 1999	5.20 MB
Acrobat Reader 4	Mar 31, 1999	5.20 MB
Acrobat Reader 4.05	Feb 7, 2000	5.50 MB
Acrobat Reader 5.0	Apr 15, 2001	8.41 MB
Acrobat Reader 5.0.5	Oct 16, 2001	8.57 MB
Acrobat Reader 5.1	Dec 28, 2001	13.10 MB
Acrobat Reader 5.05	Oct 16, 2001	8.57 MB
Acrobat Reader 6.0	Nov 2, 2003	15.93 MB
Acrobat Reader 6.01	Dec 30, 2003	15.93 MB
Acrobat Reader 7.0	Dec 13, 2004	12.56 MB
Acrobat Reader 7.0.9	Dec 5, 2006	20.29 MB
Acrobat Reader 7.1.0	May 6, 2008	18.98 MB
Acrobat Reader 7.05	Sep 23, 2005	31.57 MB
Acrobat Reader 7.07	Dec 1, 2006	20.27 MB
Acrobat Reader 7.08	May 16, 2006	20.30 MB
Acrobat Reader 8.0	Oct 26, 2006	20.81 MB
Acrobat Reader 8.1.0	May 10, 2006	22.32 MB
Acrobat Reader 8.1.1	Oct 10, 2007	22.32 MB
Acrobat Reader 8.1.2	Jan 11, 2008	22.37 MB
Acrobat Reader 8.1.3	Nov 4, 2008	20.80 MB
Acrobat Reader 8.2.0	Jan 12, 2008	33.72 MB
Acrobat Reader 8.3.0	Mar 19, 2008	33.80 MB



- **Adobe Acrobat Reader 64-bit Offline-Installer für Windows herunterladen**
  Hier geht es zum Download der Version 2023.003.20201 von Adobe Reader 64-bit.
  Webseite -> https://get.adobe.com/de/reader/
  Download -> AcroRdrDCx642300320201_de_DE.exe
  Download -> AcroRdrDCx642300320201_en_US.exe

Faktor x135



AcroRdrDCx642300320201_en_US Properties

AcroRdrDCx642300320201_en_US

Type of file: Application (.exe)

Description: Adobe Self Extractor

Location: C:\Users\MichaelMeixner\Downloads

Size: 337 MB (353.773.008 bytes)

Size on disk: 337 MB (353.779.712 bytes)

Created: 14 June 2023, 22:16:36

Modified: 14 June 2023, 22:18:38

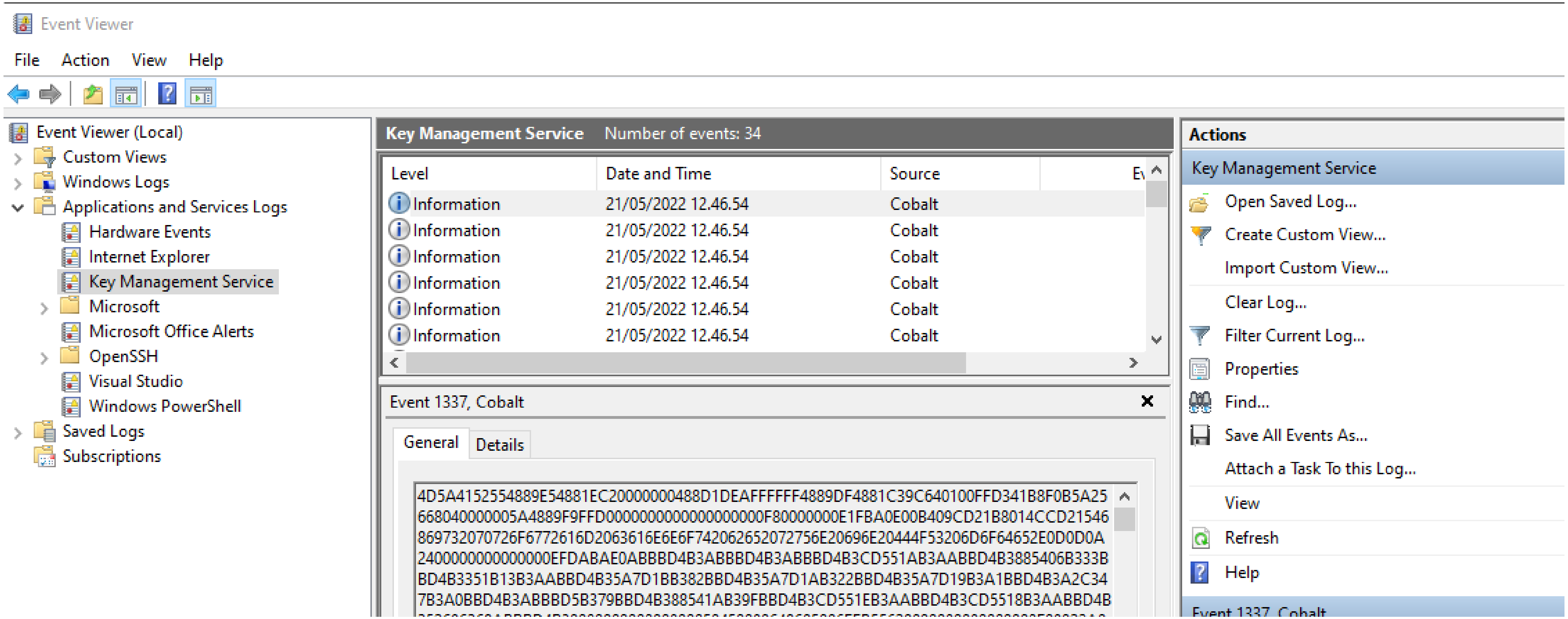
Accessed: 14 June 2023, 22:18:38

Attributes: □ Read-only □ Hidden

Security: This file came from another computer and might be blocked to help protect this computer. □ Unblock

Fileless Malware

Eine Möglichkeit einer Fileless Malware



Key Management Service Number of events: 34

Level	Date and Time	Source	Ev
Information	21/05/2022 12.46.54	Cobalt	
Information	21/05/2022 12.46.54	Cobalt	
Information	21/05/2022 12.46.54	Cobalt	
Information	21/05/2022 12.46.54	Cobalt	
Information	21/05/2022 12.46.54	Cobalt	
Information	21/05/2022 12.46.54	Cobalt	

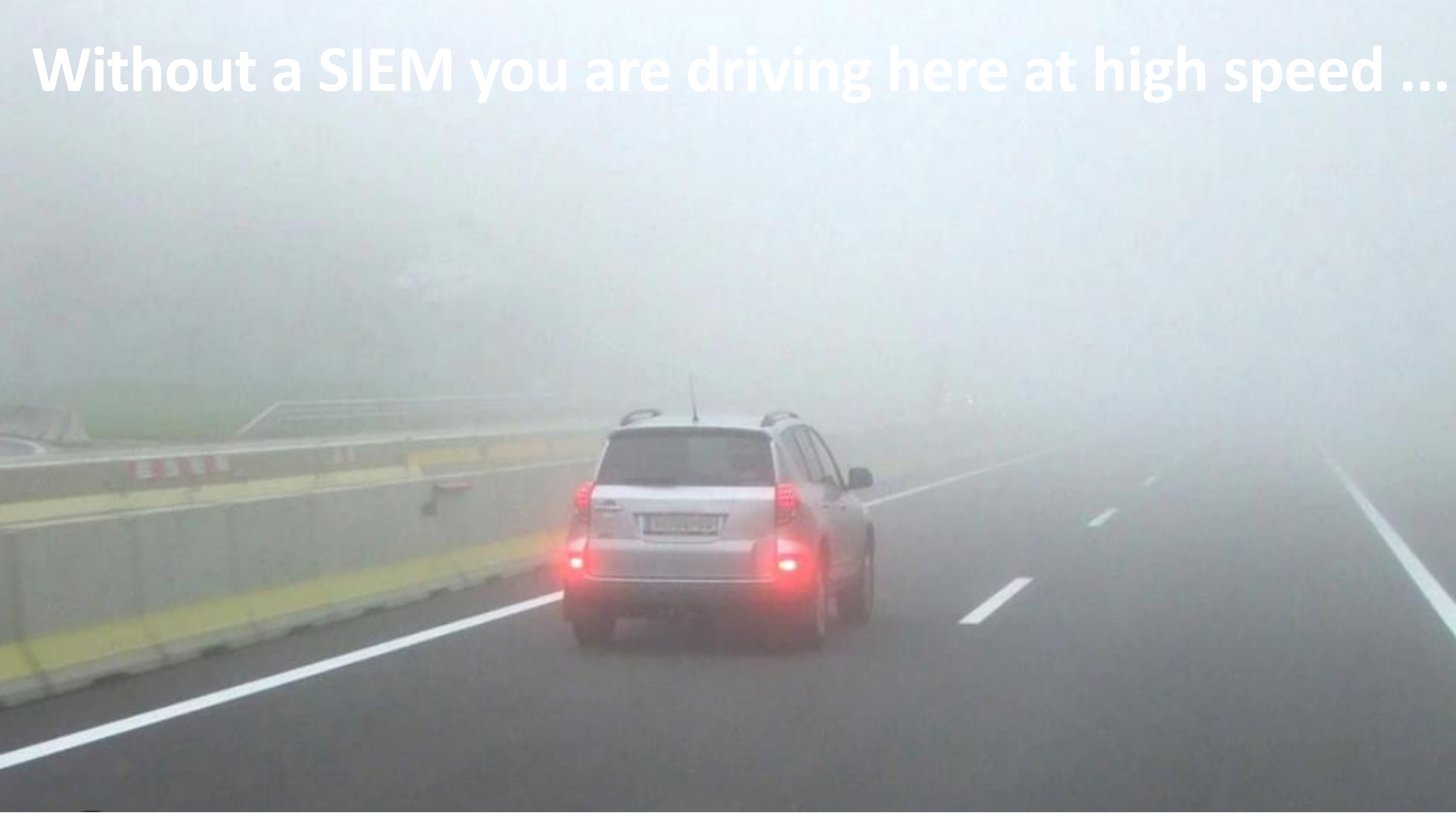
Event 1337, Cobalt

```
4D5A4152554889E54881EC20000000488D1DEAFFFFFF4889DF4881C39C640100FFD341B8F0B5A25
668040000005A4889F9FFD0000000000000000000F80000000E1FBA0E00B409CD21B8014CCD21546
869732070726F6772616D2063616E6E6F742062652072756E20696E20444F53206D6F64652E0D0D0A
2400000000000000EFDABAE0ABBBD4B3ABBBD4B3ABBBD4B3CD551AB3AABBD4B3885406B333B
BD4B3351B13B3AABBD4B35A7D1BB382BBD4B35A7D1AB322BBD4B35A7D19B3A1BBD4B3A2C34
7B3A0BBD4B3ABBBD5B379BBD4B388541AB39FBBD4B3CD551EB3AABBD4B3CD5518B3AABBD4B
```

IT-Security
Log-Management

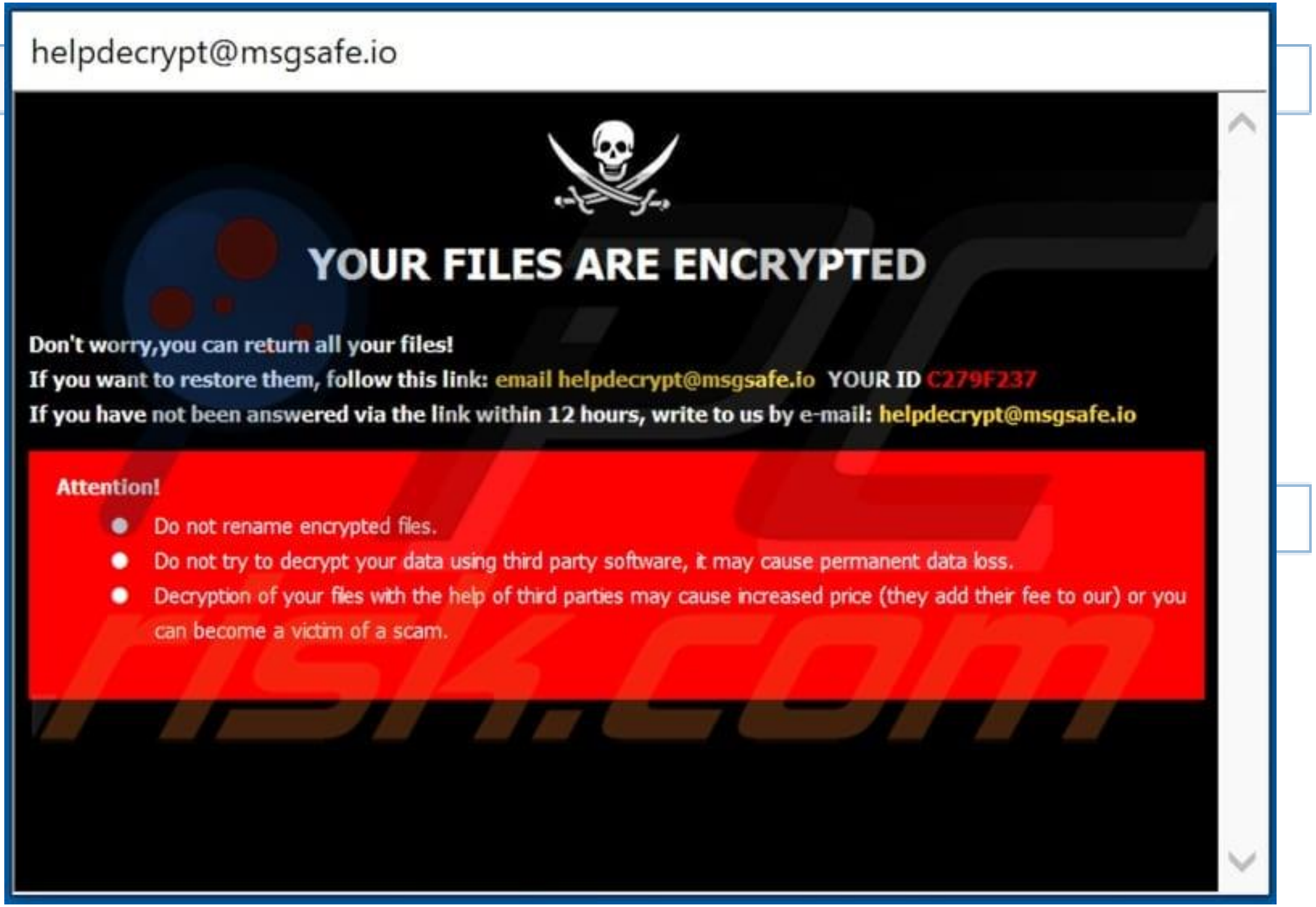
tems security

Without a SIEM you are driving here at high speed …



With and without Log Management

System or network activity (packets, program execution, ...)



helpdecrypt@msgsafe.io

YOUR FILES ARE ENCRYPTED

Don't worry,you can return all your files!
If you want to restore them, follow this link: email helpdecrypt@msgsafe.io YOUR ID C279F237
If you have not been answered via the link within 12 hours, write to us by e-mail: helpdecrypt@msgsafe.io

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

OR

Source: Cybok.org

Zusammenfassung

Tokensicherheit
API Sicherheit

Fileless Malware

Monitoring
Monitoring
Monitoring

Training für
IT-Mitarbeiter

IT-Topics von vor
20 Jahre umsetzen

Durchführung von
Cyber Security
Assessments

IT Security ist kein
Produkt

Für jedes IT-Security
Tool braucht es
Mitarbeiter

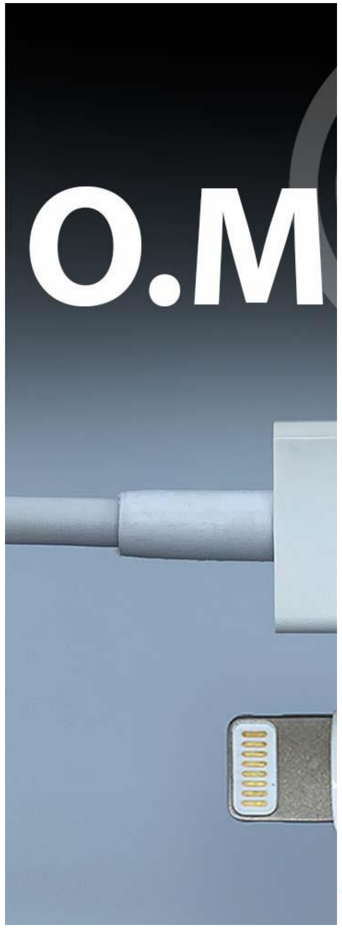
Vorhandene IT-Security Produkte
richtig konfigurieren

Wir werden nicht
mehr alle Daten
jeden Tag sichern
können

OMG
Cables

tems security

OMG Cables



MALICIOUS CABLE
DETECTOR

BY

Know your limit

Work smarter
Not harder

Source: Internet

tems security

Get in contact with us

Philip Berger
Managing Director

☎ +43(664) 343 8644

✉ Philip.berger@tems-security.at

Michael Meixner, CISSP
Managing Director

☎ +43(664) 1453328

✉ Michael.meixner@tems-security.at