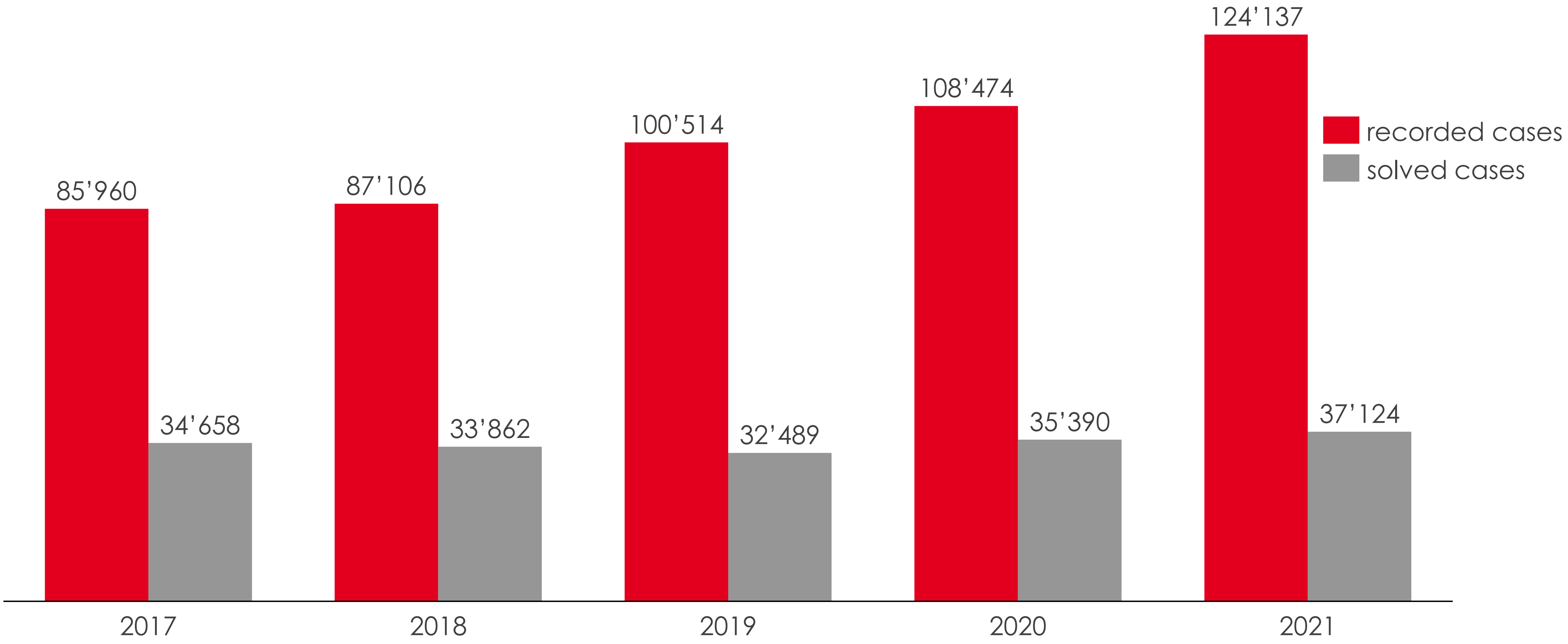
In the crosshairs of cybercriminals - A field report from Marabu

27th of June 2022, SWISS FEA Event

(York Boeder, CEO, und Stefan Würtemberger, Vice President Information Technology, Marabu GmbH & Co. KG)

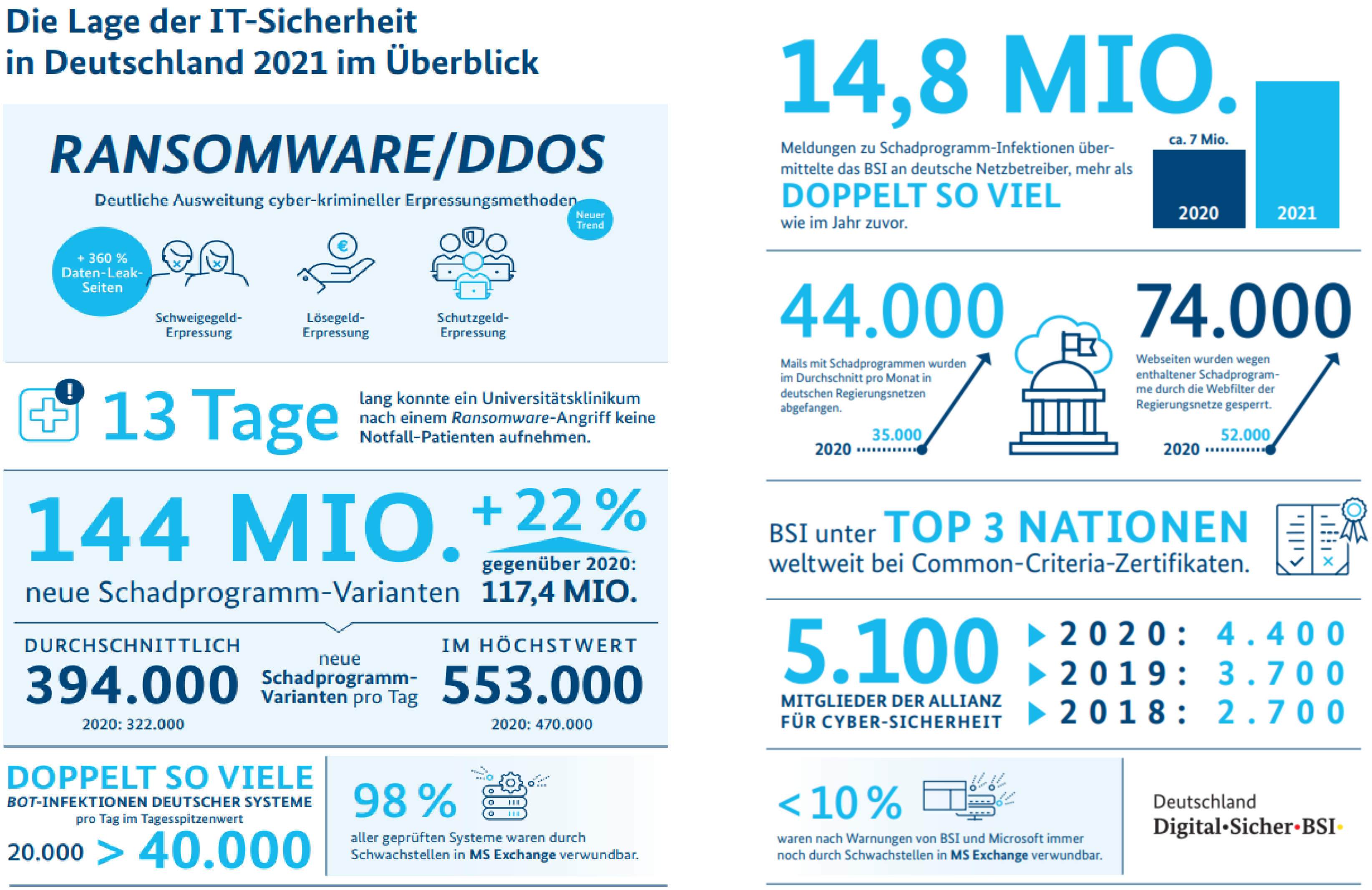
Cases of cybercrime in the narrower sense (2021)

In 2021, there was a renewed increase in cybercrime offenses in the narrower sense in Germany. The BKA reported a total of 39,823 cases. This represents an increase of 12.2% compared to the previous year.



Source: Cybercrime | Bundeslagebild 2020

Cases of cybercrime in the narrower sense (2021)



Die Lage der IT-Sicherheit in Deutschland 2021 im Überblick

RANSOMWARE/DDOS

Deutliche Ausweitung cyber-krimineller Erpressungsmethoden

Neuer Trend

+ 360 % Daten-Leak-Seiten

Schweigegeld-Erpressung

Lösegeld-Erpressung

Schutzgeld-Erpressung

13 Tage lang konnte ein Universitätsklinikum nach einem *Ransomware*-Angriff keine Notfall-Patienten aufnehmen.

144 MIO. neue Schadprogramm-Varianten

+22 % gegenüber 2020: **117,4 MIO.**

DURCHSCHNITTLICH		IM HÖCHSTWERT
394.000	neue **Schadprogramm-Varianten** pro Tag	**553.000**
2020: 322.000		2020: 470.000

DOPPELT SO VIELE
***BOT*-INFEKTIONEN DEUTSCHER SYSTEME**
pro Tag im Tagesspitzenwert
20.000 > **40.000**

98 % aller geprüften Systeme waren durch Schwachstellen in **MS Exchange** verwundbar.

14,8 MIO. Meldungen zu Schadprogramm-Infektionen übermittelte das BSI an deutsche Netzbetreiber, mehr als **DOPPELT SO VIEL** wie im Jahr zuvor.

44.000 Mails mit Schadprogrammen wurden im Durchschnitt pro Monat in deutschen Regierungsnetzen abgefangen.
2020 35.000

74.000 Webseiten wurden wegen enthaltener Schadprogramme durch die Webfilter der Regierungsnetze gesperrt.
2020 52.000

BSI unter **TOP 3 NATIONEN** weltweit bei Common-Criteria-Zertifikaten.

5.100 MITGLIEDER DER ALLIANZ FÜR CYBER-SICHERHEIT

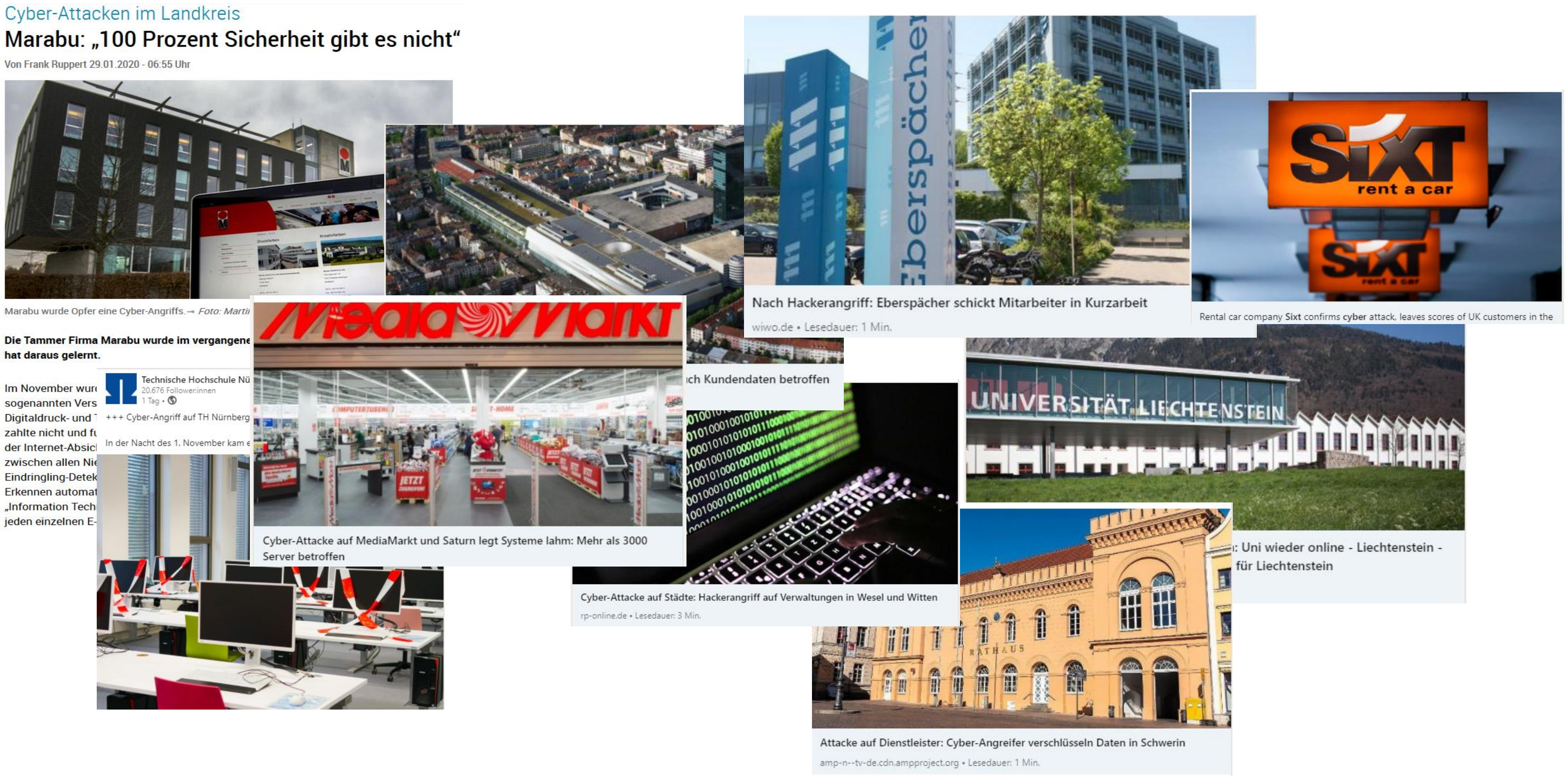
2020:	4.400
2019:	3.700
2018:	2.700

< 10 % waren nach Warnungen von BSI und Microsoft immer noch durch Schwachstellen in **MS Exchange** verwundbar.

Deutschland
Digital•Sicher•BSI•

Source: Cybercrime | Bundeslagebild 2021

Victims of Cyber Attacks



Cyber-Attacken im Landkreis

Marabu: „100 Prozent Sicherheit gibt es nicht“

Von Frank Ruppert 29.01.2020 - 06:55 Uhr

Marabu wurde Opfer eine Cyber-Angriffs. Foto: Marti

Die Tammer Firma Marabu wurde im vergangene hat daraus gelernt.

Im November wur sogenannten Vers Digitaldruck- und zahlte nicht und fu der Internet-Absic zwischen allen Nie Eindringling-Detek Erkennen automat „Information Tech jeden einzelnen E-

Technische Hochschule Nü
20.676 Follower:innen
1 Tag •

+++ Cyber-Angriff auf TH Nürnberg

In der Nacht des 1. November kam e

Cyber-Attacke auf MediaMarkt und Saturn legt Systeme lahm: Mehr als 3000 Server betroffen

ch Kundendaten betroffen

Nach Hackerangriff: Eberspächer schickt Mitarbeiter in Kurzarbeit

wiwo.de • Lesedauer: 1 Min.

Rental car company **Sixt** confirms **cyber** attack, leaves scores of UK customers in the

Cyber-Attacke auf Städte: Hackerangriff auf Verwaltungen in Wesel und Witten

rp-online.de • Lesedauer: 3 Min.

: Uni wieder online - Liechtenstein - für Liechtenstein

Attacke auf Dienstleister: Cyber-Angreifer verschlüsseln Daten in Schwerin

amp-n--tv-de.cdn.ampproject.org • Lesedauer: 1 Min.

The Marabu Case

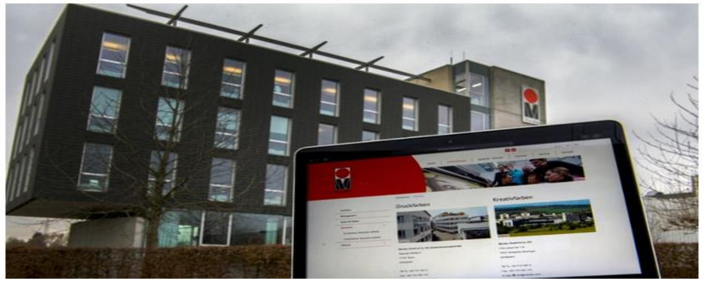
Everybody in the world

The Marabu Case

Cyber-Attacken im Landkreis

Marabu: „100 Prozent Sicherheit gibt es nicht“

Von Frank Ruppert 29.01.2020 - 06:55 Uhr



Marabu wurde Opfer eine Cyber-Angriffs.→ *Foto: Martin Kalb*

Die Tammer Firma Marabu wurde im vergangenen Jahr Opfer einer Cyber-Attacke und hat daraus gelernt.

Im November wurde die Tammer Firma Marabu Opfer ei
sogenannten Verschlüsselungstrojaners sollte Geld von
Digitaldruck- und Tampondruckfarben sowie Kreativfarb
zahlte nicht und fuhr alle seine Server herunter. Danach
der Internet-Absicherung erfolgen. „Wir haben Firewalls
zwischen allen Niederlassungen aktiviert und verbessert
Eindringling-Detektion- und Prävention-Filter, die den Ne
Erkennen automatisch stoppen“, erklärt Stefan Würtemb
„Information Technology“ bei dem Unternehmen. Außer
jeden einzelnen E-Mail-Anhang auf Schadsoftware teste

Hacker-Attacke auf Marabu

Nach dem Cyberangriff

Von Claudia Mocek 26.11.2020 - 11:40 Uhr

Marabu aus Tamm hat seine Mitarbeiter für das Thema IT-Sicherheit sensibilisiert.→ *Foto: Martin Kalb*

Ein Jahr nach der Attacke: Das Ermittlungsverfahren ist eingestellt, der Wettlauf „Gut gegen Böse“ bei der Sicherheitstechnik geht weiter.

Morgens um vier Uhr begann der Verschlüsselungstrojaner damit, sämtliche Daten der Firma Marabu zu verschlüsseln. Der Hersteller von Druckfarben aus Tamm fuhr alle Rechner herunter und war sechs Tage lang von der Außenwelt abgeschnitten. Mit den Erpressern hat Marabu nicht verhandelt, um wieder an seine Daten zu kommen. Anders als andere Firmen hat sich das Unternehmen an die Öffentlichkeit gewendet, um über den Vorgang zu informieren. Was sich wie ein Krimi anhört, jährt sich am 29. November zu ersten Mal. Die BZ hat nachgefragt, wie es nach dem Angriff weiterging.

Millionen-Schaden

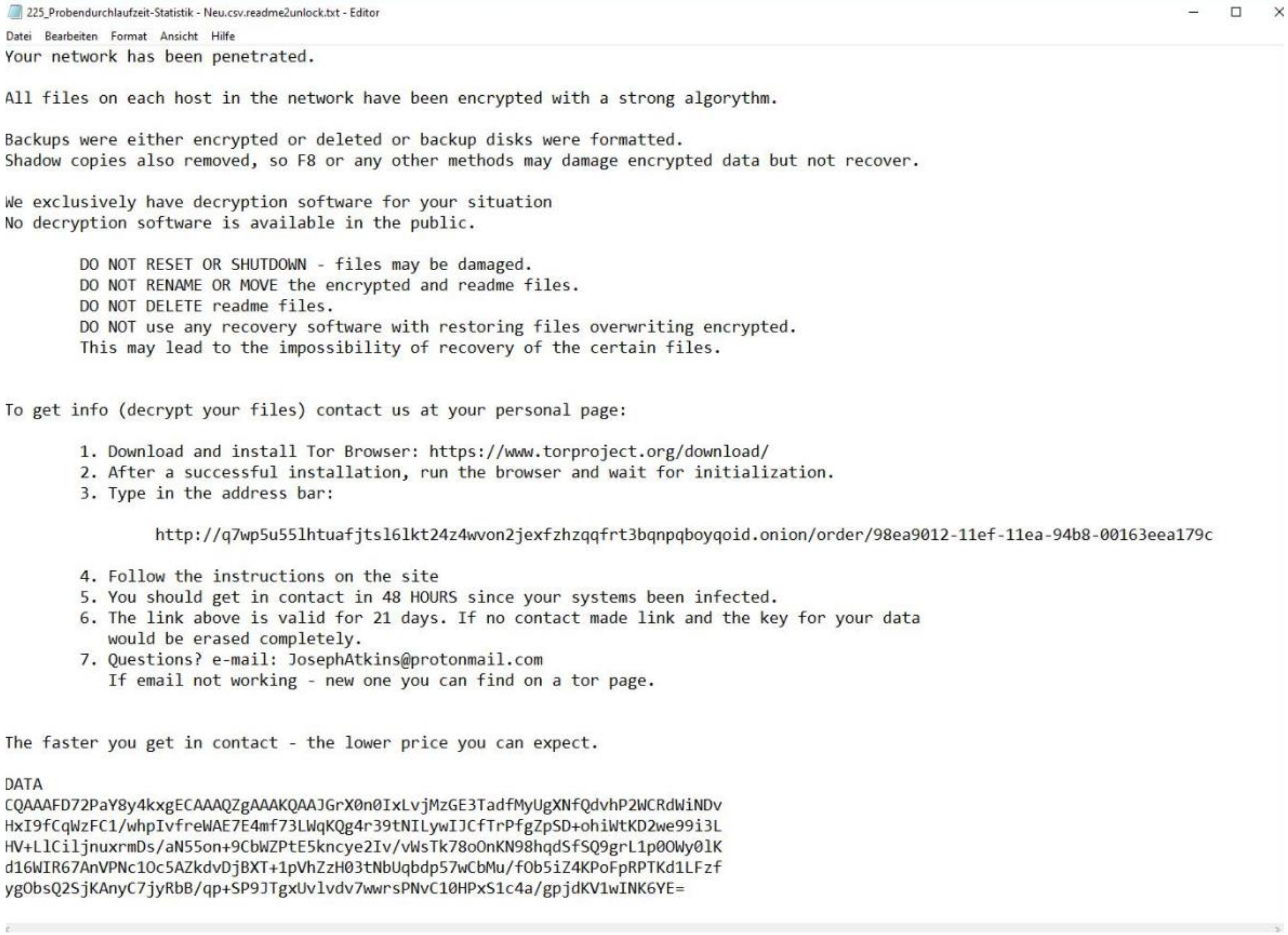
StZ Plus

Hacker legen Traditionsfirma Marabu lahm

en weltweit führenden Herstellern von Sieb-, Digital- und Tampondruckfarben.
nville, Marabu

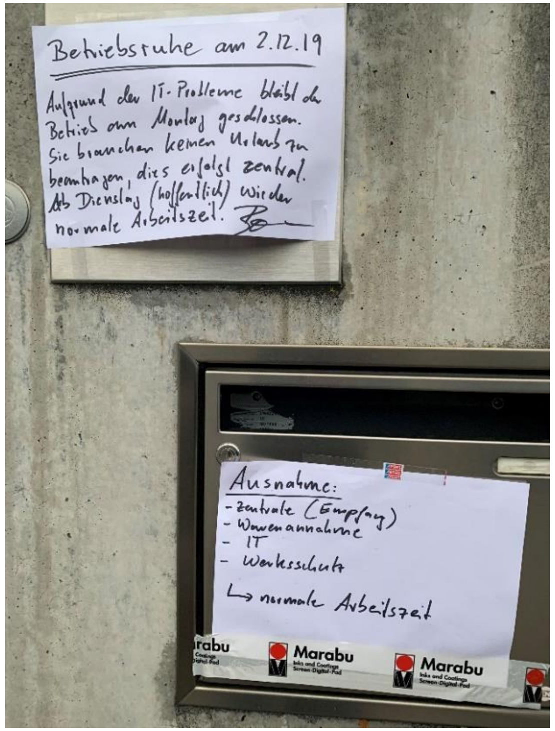
ar nichts mehr: Nach einer gezielten Hackerattacke laufen die Geschäfte
ler an. Die Attacke könnte auch für Autobauer Folgen haben. Und ein
er könnte jede Firma treffen.

Black Friday – 29. November 2019


225_Probendurchlaufzeit-Statistik - Neu.csv.readme2unlock.txt - Editor
Datei
Bearbeiten
Format
Ansicht
Hilfe

```
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorythm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

        DO NOT RESET OR SHUTDOWN - files may be damaged.
        DO NOT RENAME OR MOVE the encrypted and readme files.
        DO NOT DELETE readme files.
        DO NOT use any recovery software with restoring files overwriting encrypted.
        This may lead to the impossibility of recovery of the certain files.


To get info (decrypt your files) contact us at your personal page:

        1. Download and install Tor Browser: https://www.torproject.org/download/
        2. After a successful installation, run the browser and wait for initialization.
        3. Type in the address bar:

                http://q7wp5u55lhtuafjtsl6lkt24z4wvon2jexfzhzqqfrt3bqnpqboyqoid.onion/order/98ea9012-11ef-11ea-94b8-00163eea179c

        4. Follow the instructions on the site
        5. You should get in contact in 48 HOURS since your systems been infected.
        6. The link above is valid for 21 days. If no contact made link and the key for your data
           would be erased completely.
        7. Questions? e-mail: JosephAtkins@protonmail.com
           If email not working - new one you can find on a tor page.


The faster you get in contact - the lower price you can expect.

DATA
```

CQAAAFD72PaY8y4kxgECAAAQZgAAAKQAAJGrX0n0IxLvjMzGE3TadfMyUgXNfQdvhP2WCRdWiNDv
HxI9fCqWzFC1/whpIvfreWAE7E4mf73LWqKQg4r39tNILywIJCfTrPfgZpSD+ohiWtKD2we99i3L
HV+LlCiljnuxrmDs/aN55on+9CbWZPtE5kncye2Iv/vWsTk78oOnKN98hqdSfSQ9grL1p0OWy0lK
d16WIR67AnVPNc1Oc5AZkdvDjBXT+1pVhZzH03tNbUqbdp57wCbMu/fOb5iZ4KPoFpRPTKd1LFzf
ygObsQ2SjKAnyC7jyRbB/qp+SP9JTgxUvlvdv7wwrsPNvC10HPxS1c4a/gpjdKV1wINK6YE=



Betriebsruhe am 2.12.19

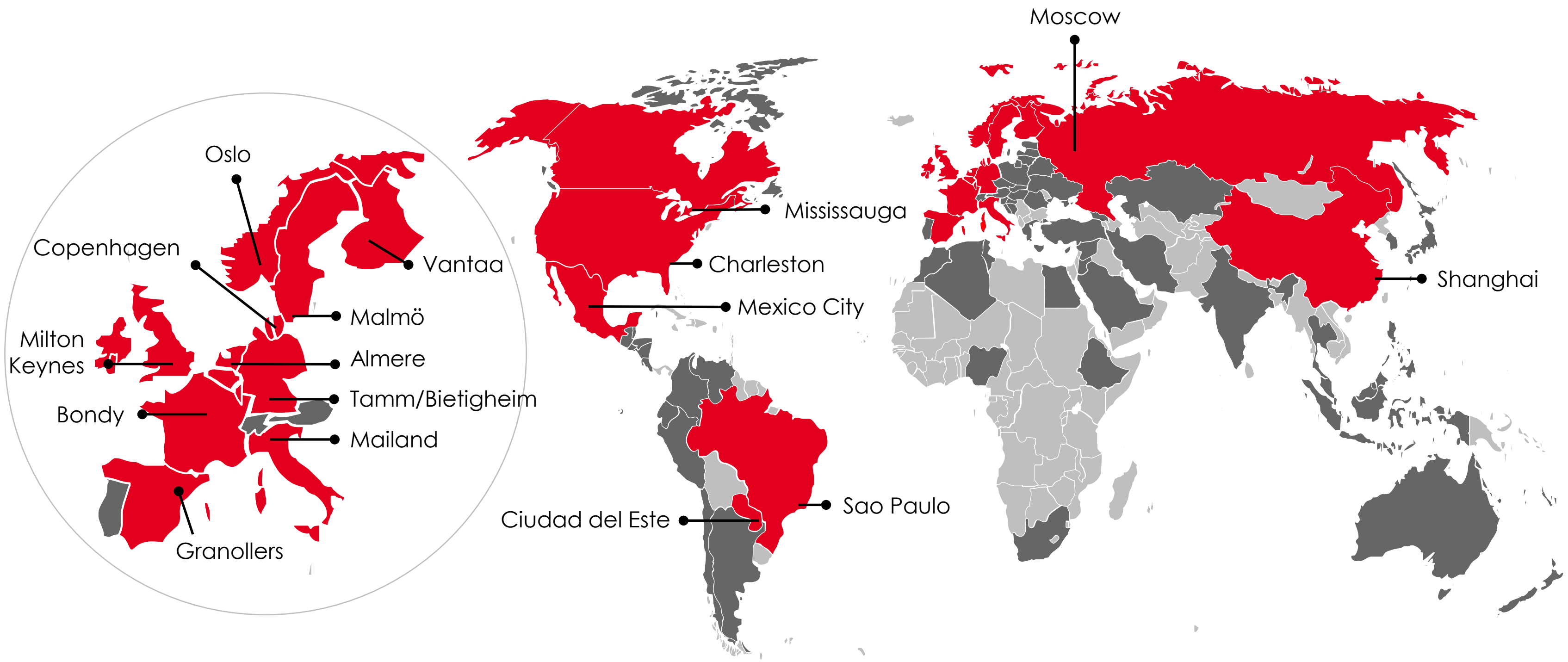
Aufgrund der IT-Probleme bleibt der
Betrieb am Montag geschlossen.
Sie brauchen keinen Urlaub zu
beantragen, dies erfolgt zentral.
Ab Dienstag (hoffentlich) wieder
normale Arbeitszeit.

Ausnahme:

- Zentrale (Empfang)
- Warenannahme
- IT
- Werksschutz

↳ normale Arbeitszeit

Global Presence



🟥 Marabu Group: Subsidiaries

⬛ Distribution Partner over 90 countries

First Steps

Involve the police

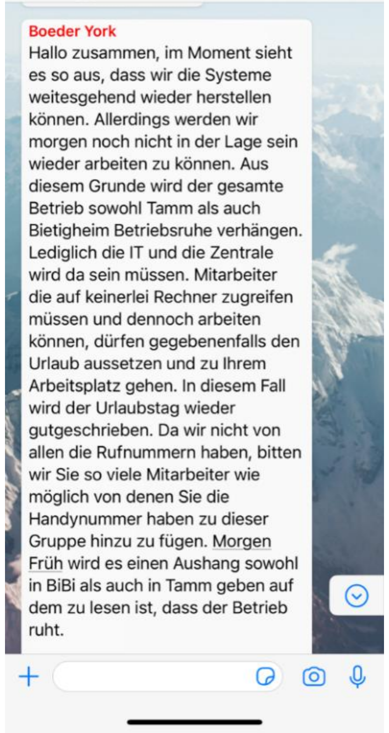
- After receiving the extortion letter – involve the police

Communication Channels

- Who must be informed in the company?
- How is information passed on?

Core Team / Crisis Unit

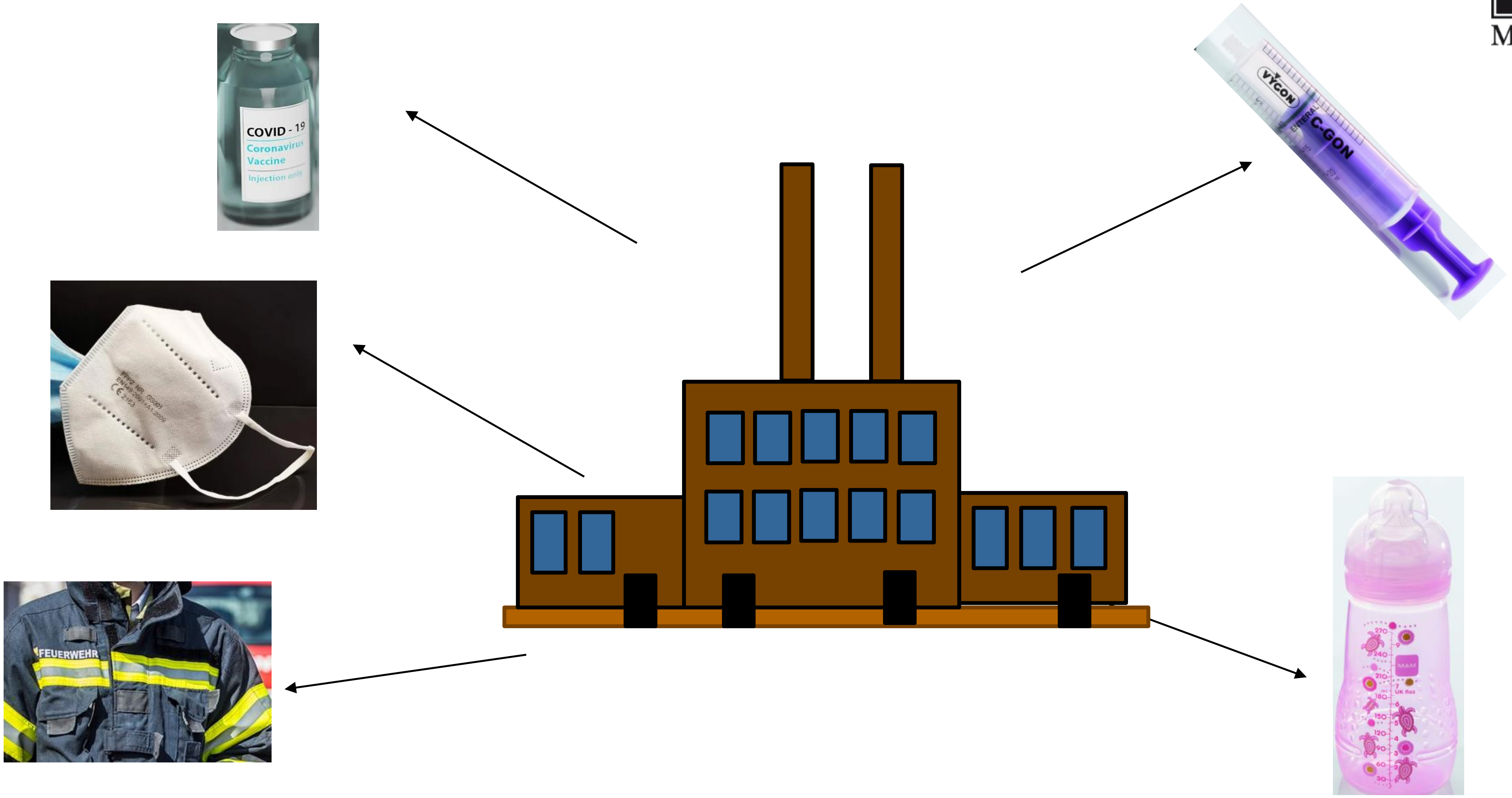
- Define Core Team (Management, IT, HR, Finance)
- Form a Crisis Management Team
- Set up (analog) emergency operation



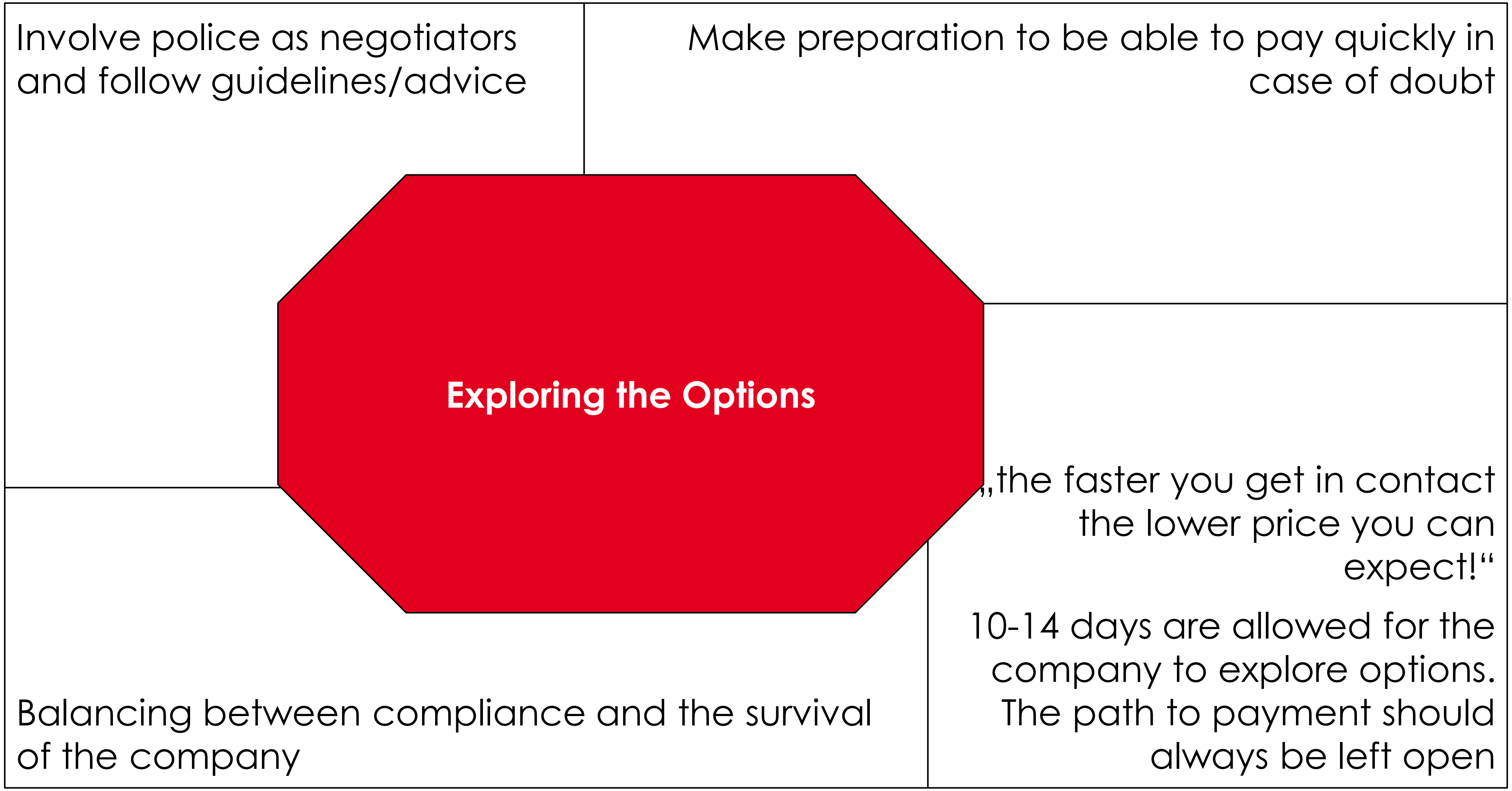
Boeder York

Hallo zusammen, im Moment sieht es so aus, dass wir die Systeme weitesgehend wieder herstellen können. Allerdings werden wir morgen noch nicht in der Lage sein wieder arbeiten zu können. Aus diesem Grunde wird der gesamte Betrieb sowohl Tamm als auch Bietigheim Betriebsruhe verhängen. Lediglich die IT und die Zentrale wird da sein müssen. Mitarbeiter die auf keinerlei Rechner zugreifen müssen und dennoch arbeiten können, dürfen gegebenenfalls den Urlaub aussetzen und zu Ihrem Arbeitsplatz gehen. In diesem Fall wird der Urlaubstag wieder gutgeschrieben. Da wir nicht von allen die Rufnummern haben, bitten wir Sie so viele Mitarbeiter wie möglich von denen Sie die Handynummer haben zu dieser Gruppe hinzu zu fügen. Morgen Früh wird es einen Aushang sowohl in BiBi als auch in Tamm geben auf dem zu lesen ist, dass der Betrieb ruht.

Supply Chains – set up emergency operation



Exploring the Options



Involve police as negotiators and follow guidelines/advice

Make preparation to be able to pay quickly in case of doubt

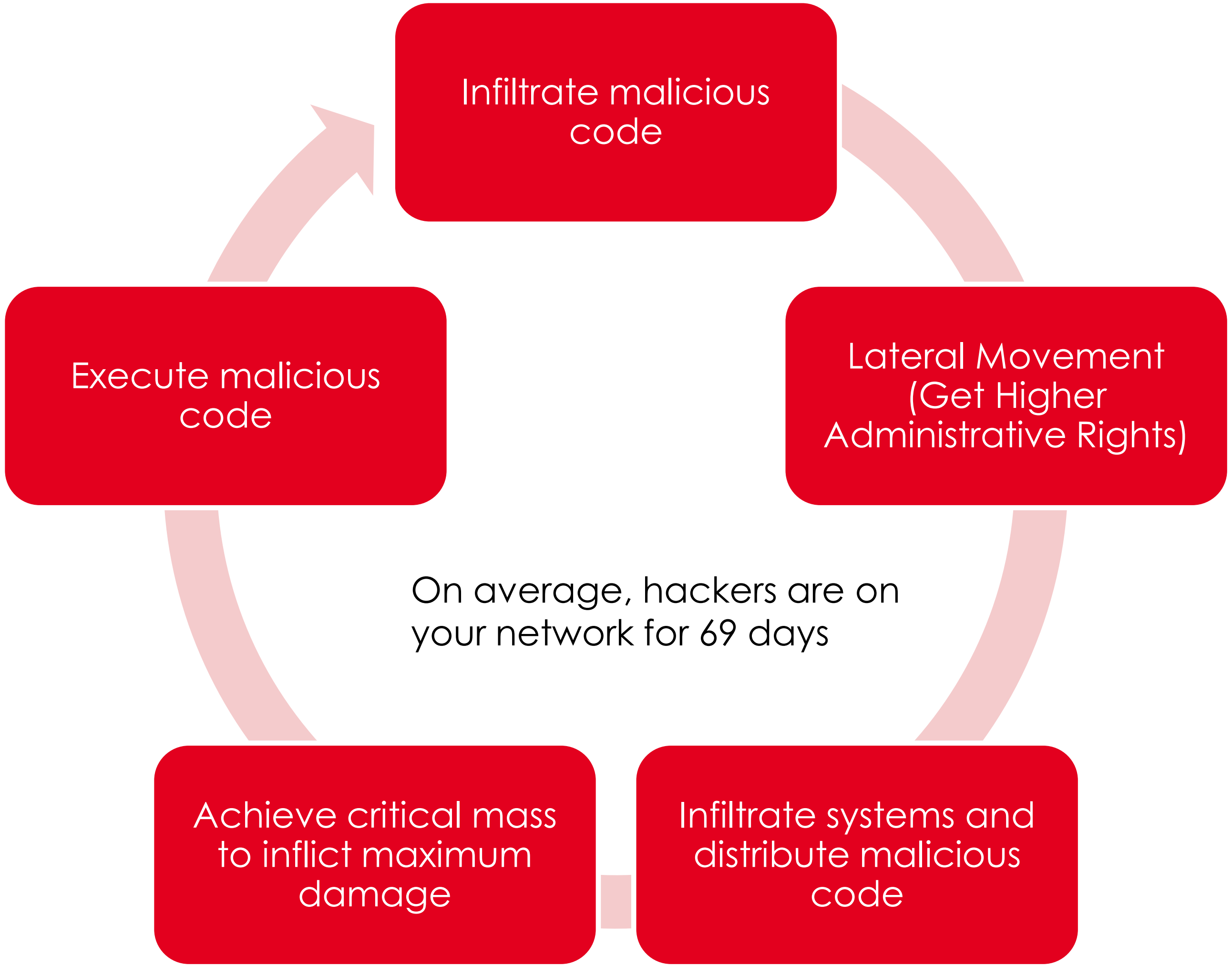
Exploring the Options

„the faster you get in contact the lower price you can expect!“

10-14 days are allowed for the company to explore options. The path to payment should always be left open

Balancing between compliance and the survival of the company

Procedure of the Cyber Attack



Infiltrate malicious code

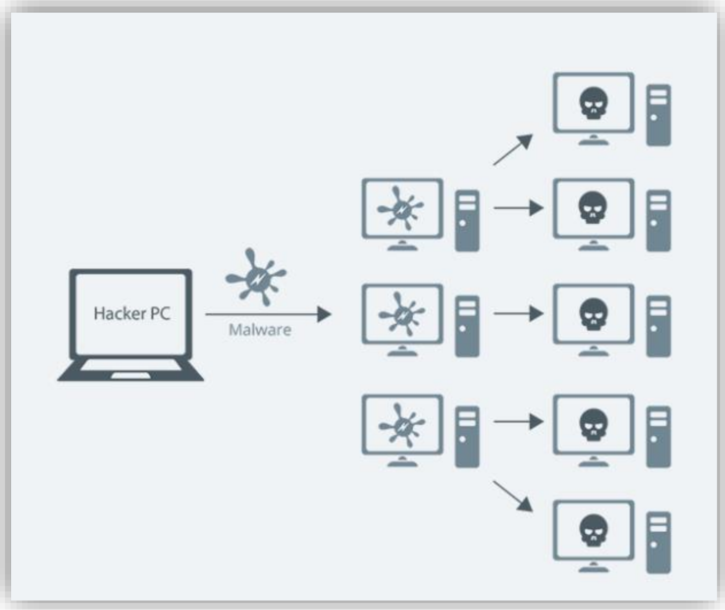
Lateral Movement (Get Higher Administrative Rights)

Infiltrate systems and distribute malicious code

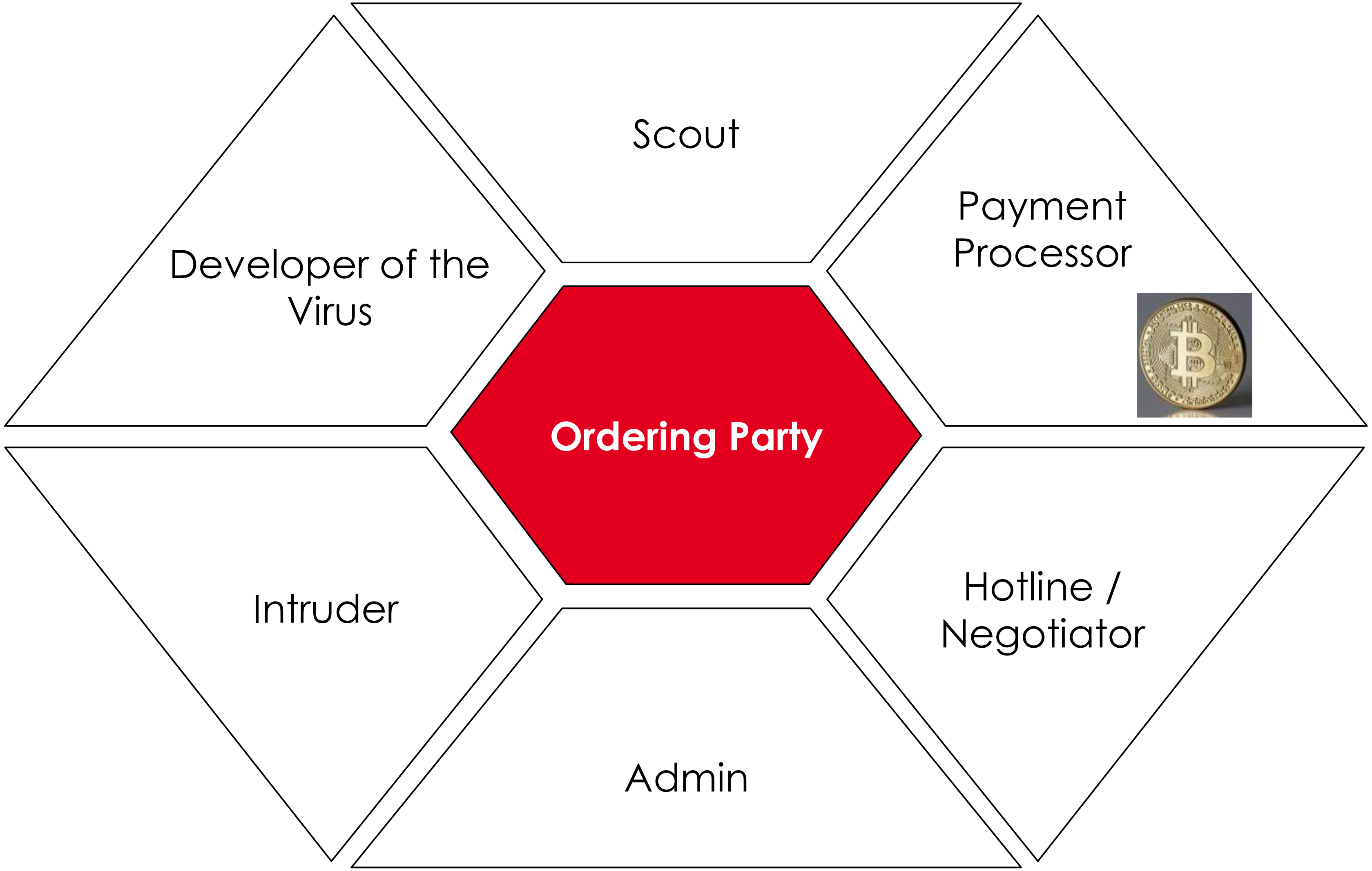
Achieve critical mass to inflict maximum damage

Execute malicious code

On average, hackers are on your network for 69 days



The Darknet in the Background



Scout

Developer of the Virus

Payment Processor

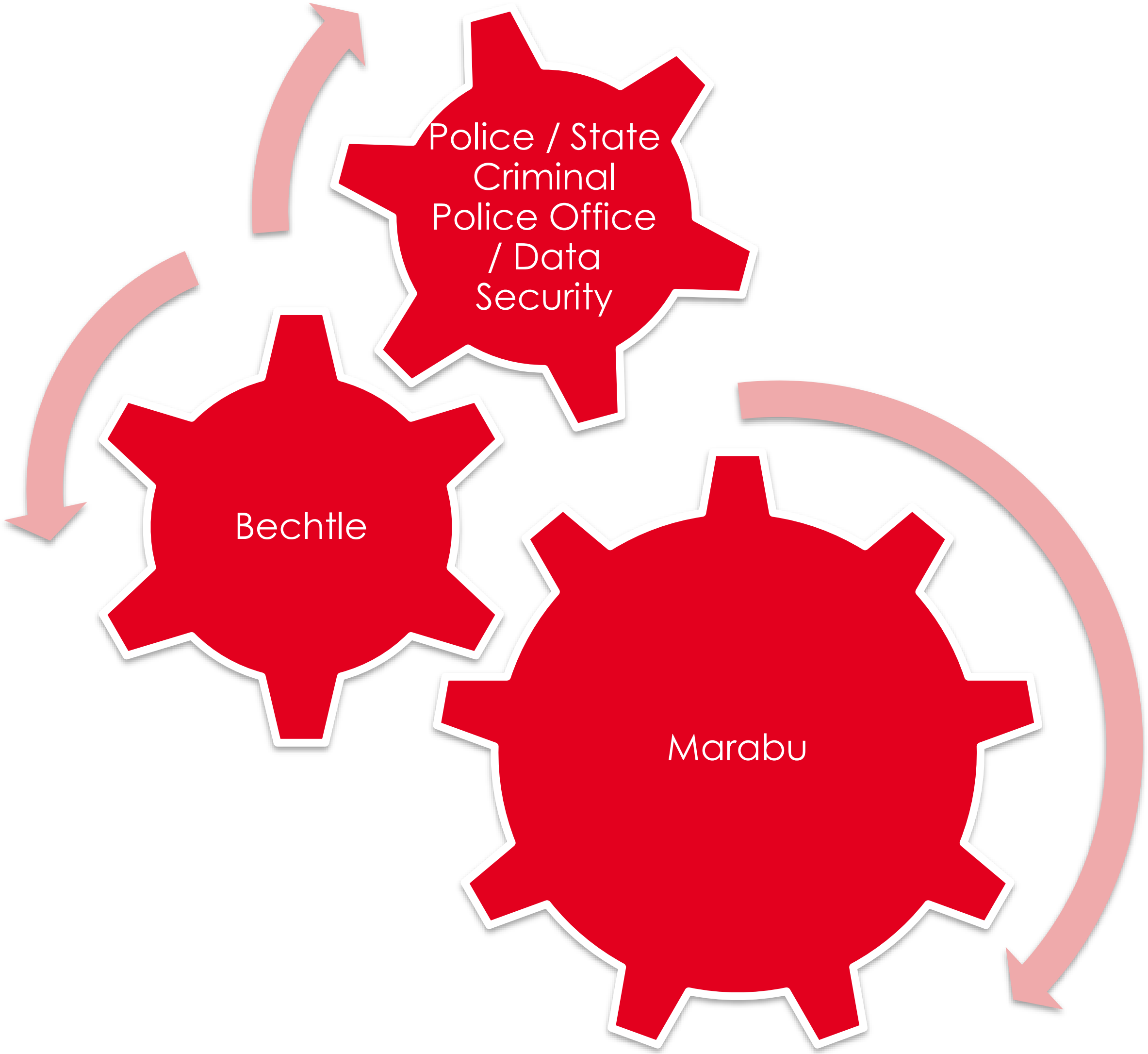
Ordering Party

Intruder

Hotline / Negotiator

Admin

External Service Provider



BECHTLE

- Forensic analysis of malware
- Network and security specialists
- Project and emergency managers

Police Department K5 (Cybercrime)

- Investigator
- Negotiation officer & psychologist

Baden-Württemberg
LANDESKRIMINALAMT

State Criminal Police Office

- Forensic analysis of the malware
- Tactical investigation

Data Protection Authority BW

- Data protection breach detection and procedure

Software used

NUIX Carving

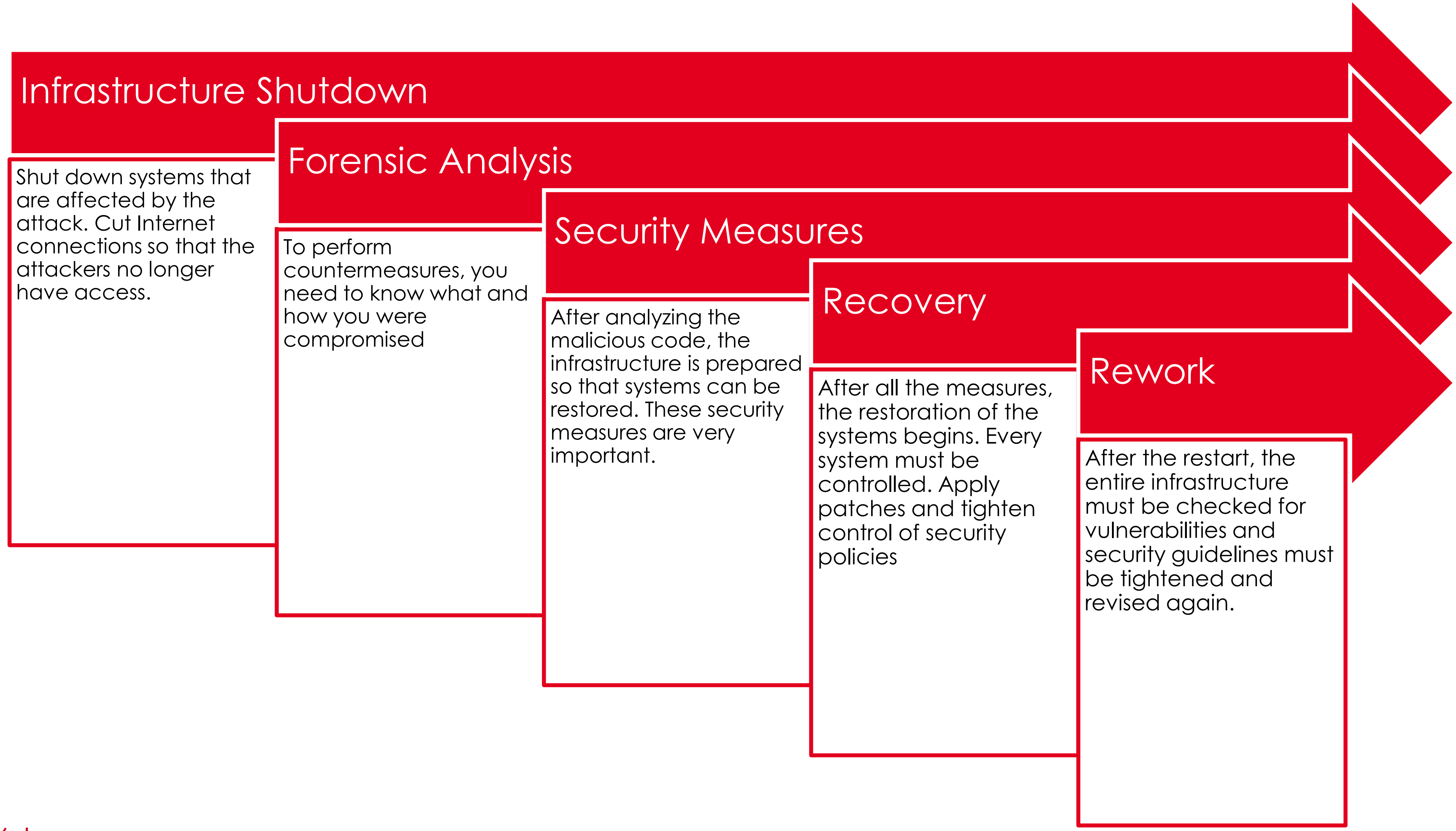
Israeli software to recover and outsource fully or partially deleted files and memory

OnTrack EasyRecovery

Recovering hard disk fragments

By using these software products, we were able to recover approximately 3.8 TB of data.

Recovery Procedure



Infrastructure Shutdown

Shut down systems that are affected by the attack. Cut Internet connections so that the attackers no longer have access.

Forensic Analysis

To perform countermeasures, you need to know what and how you were compromised

Security Measures

After analyzing the malicious code, the infrastructure is prepared so that systems can be restored. These security measures are very important.

Recovery

After all the measures, the restoration of the systems begins. Every system must be controlled. Apply patches and tighten control of security policies

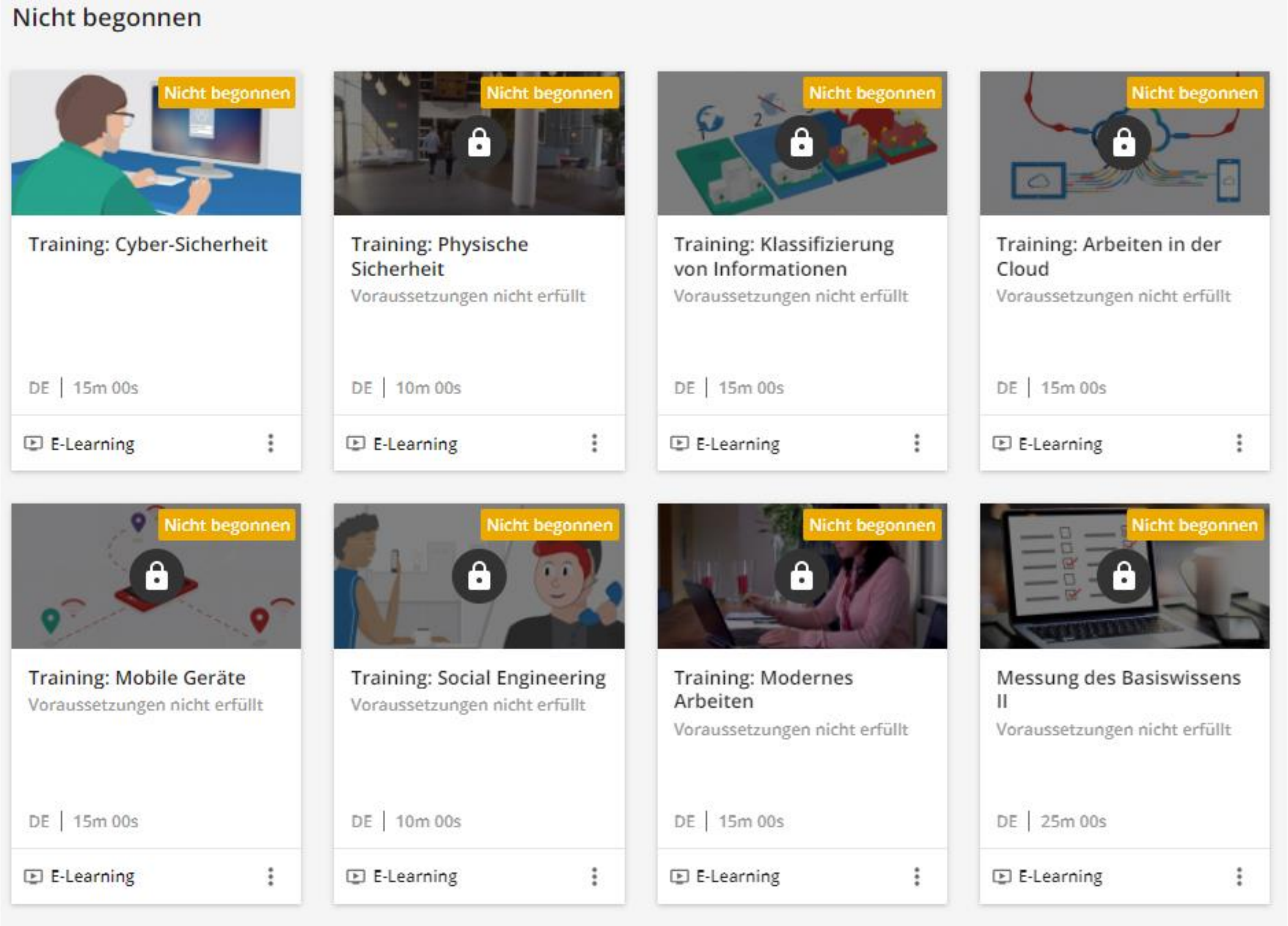
Rework

After the restart, the entire infrastructure must be checked for vulnerabilities and security guidelines must be tightened and revised again.

Lessons Learned

- External cyber specialists
- Notification to the police
- Documented infrastructure helps external specialists
- Good network specialists are the backbone
- Update contingency plans regularly
- Store backups without tying them to infrastructure (paper, etc..)
- Do not underestimate the effort for internal communication
- Take out cyber insurance, you never know when you might need it
- The better the cybersecurity strategy & crisis management, the better prepared you will be
- Cybersecurity strategy is now the responsibility of management / CEO
- Put cybersecurity to the test on a regular basis.
- Don't stop talking about cyberattacks and their impact

Cyber Security Trainings



Nicht begonnen

Nicht begonnen
Training: Cyber-Sicherheit
DE | 15m 00s
E-Learning

Nicht begonnen
Training: Physische Sicherheit
Voraussetzungen nicht erfüllt
DE | 10m 00s
E-Learning

Nicht begonnen
Training: Klassifizierung von Informationen
Voraussetzungen nicht erfüllt
DE | 15m 00s
E-Learning

Nicht begonnen
Training: Arbeiten in der Cloud
Voraussetzungen nicht erfüllt
DE | 15m 00s
E-Learning

Nicht begonnen
Training: Mobile Geräte
Voraussetzungen nicht erfüllt
DE | 15m 00s
E-Learning

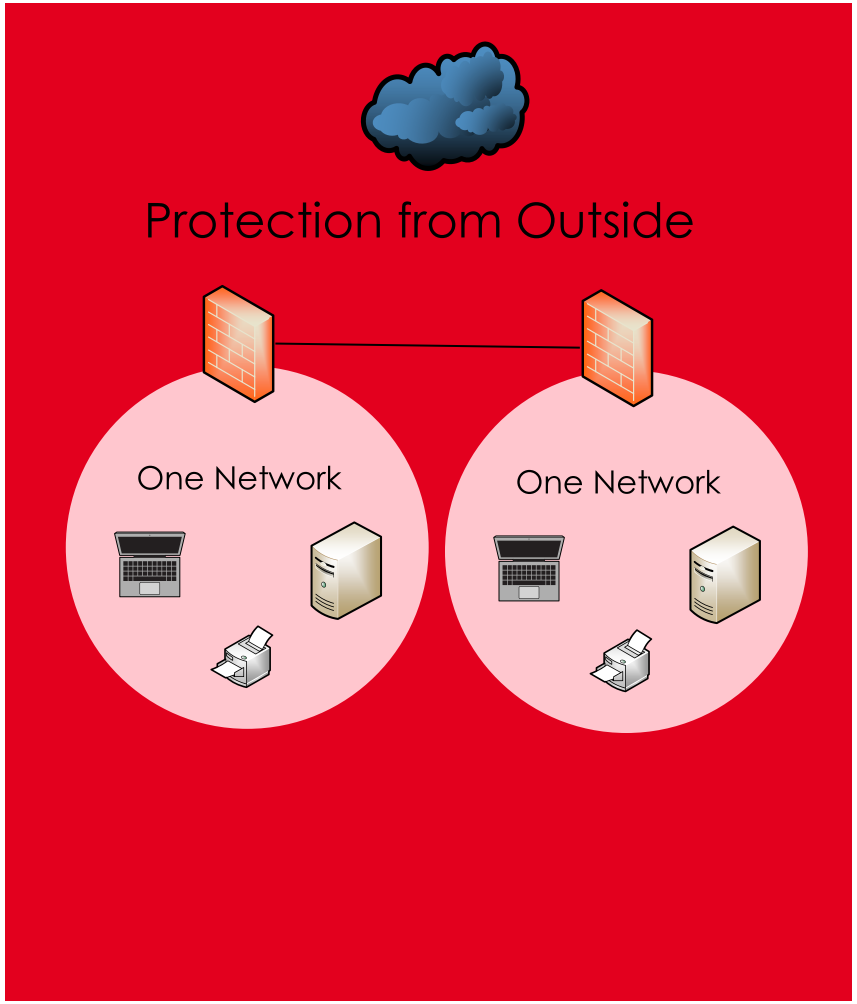
Nicht begonnen
Training: Social Engineering
Voraussetzungen nicht erfüllt
DE | 10m 00s
E-Learning

Nicht begonnen
Training: Modernes Arbeiten
Voraussetzungen nicht erfüllt
DE | 15m 00s
E-Learning

Nicht begonnen
Messung des Basiswissens II
Voraussetzungen nicht erfüllt
DE | 25m 00s
E-Learning

IT Security

Former

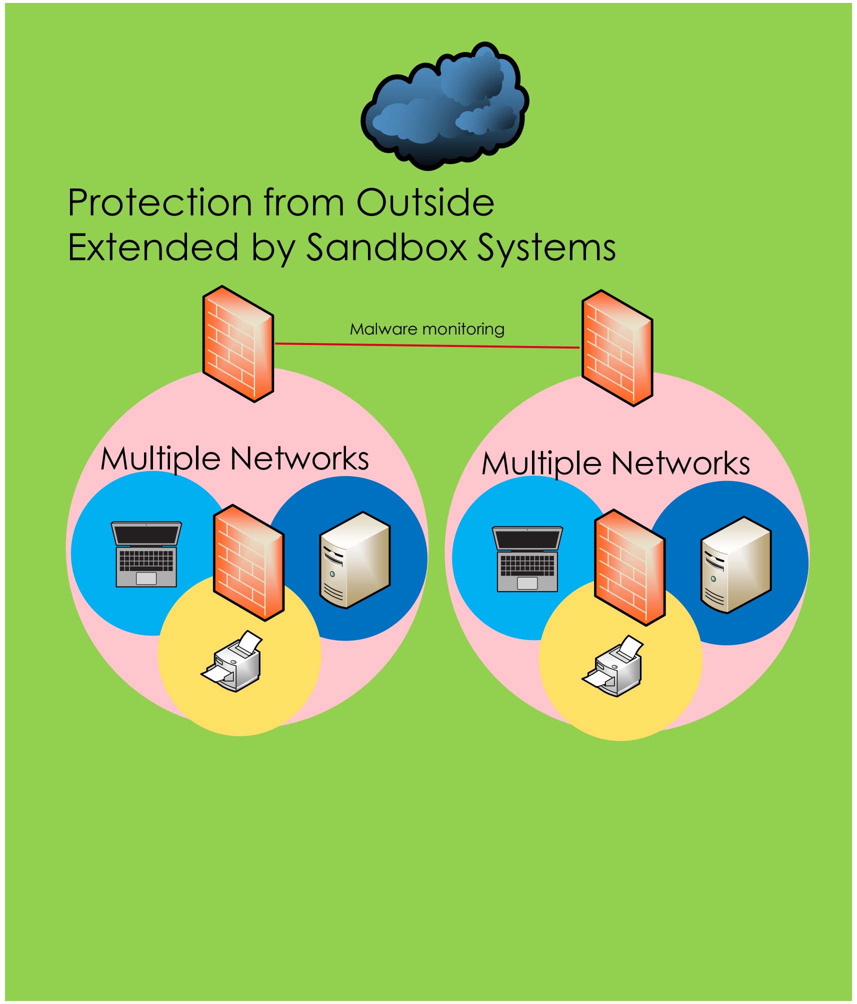


Protection from Outside

One Network

One Network

Today – Status 2021

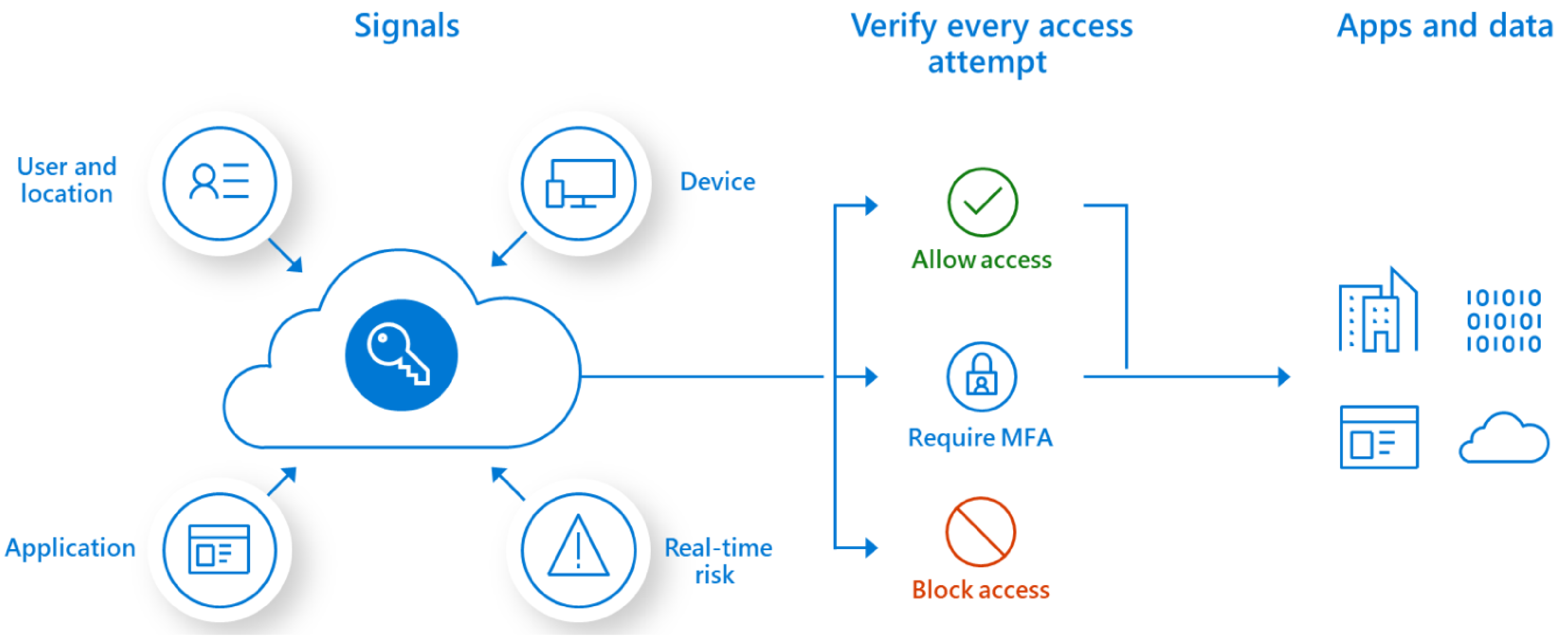


Protection from Outside
Extended by Sandbox Systems

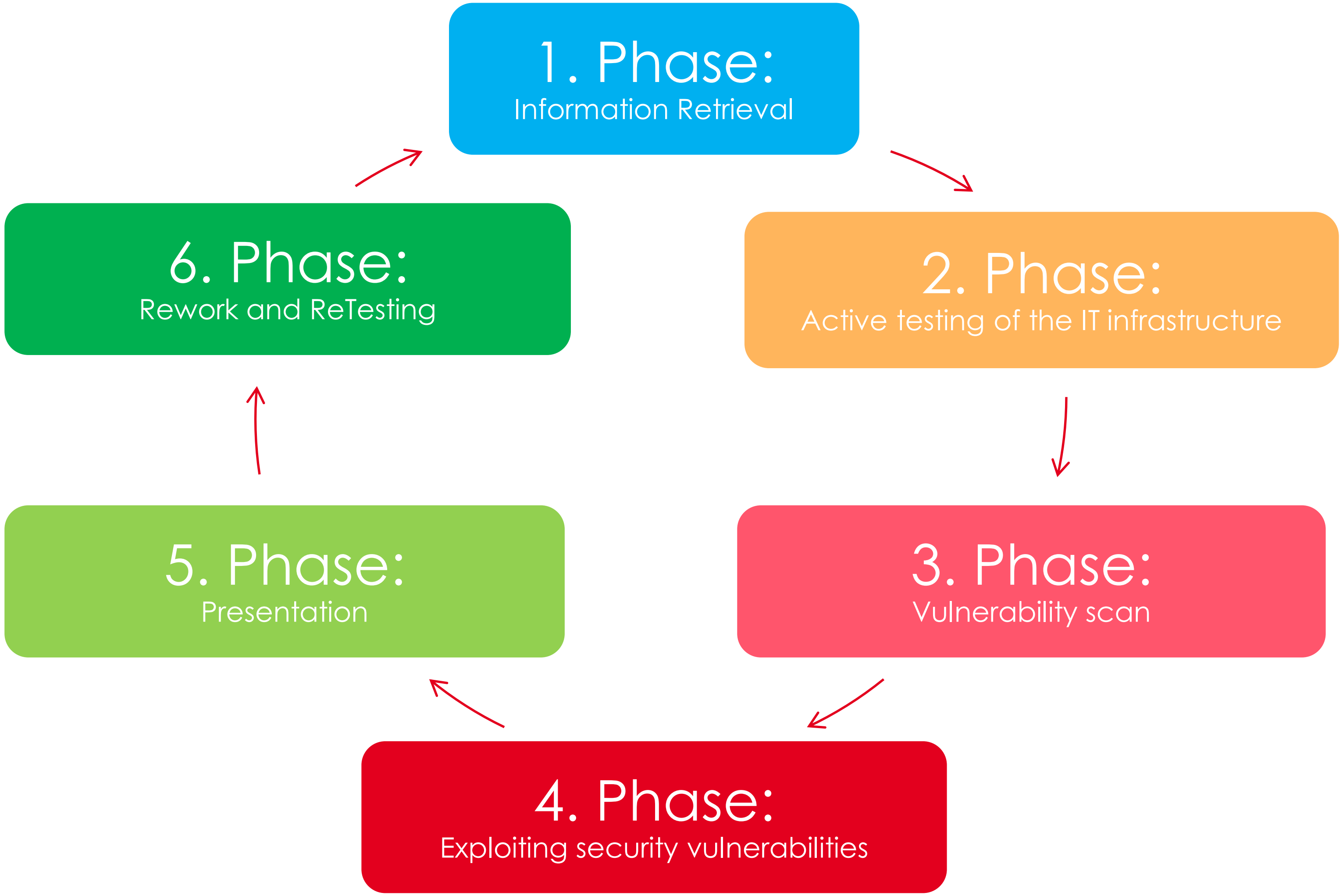
Multiple Networks

Multiple Networks

IT Security ZERO-Trust Environment



Scope of a safety inspection(PenTest)



1. Phase:
Information Retrieval

2. Phase:
Active testing of the IT infrastructure

3. Phase:
Vulnerability scan

4. Phase:
Exploiting security vulnerabilities

5. Phase:
Presentation

6. Phase:
Rework and ReTesting

What does it look like when it happens twice?

- The first time:

- In the beginning we knew nothing
- We had no clear plan
- No experience and exact procedures

- But the second time:

- Knew that an attack was underway
- Clear planning and strategy
- Experience in process and strategy

This means:
For the first attack it took us 9 weeks, for the second 48 hours.

Thank you

Marabu GmbH & Co.KG

www.marabu.de