

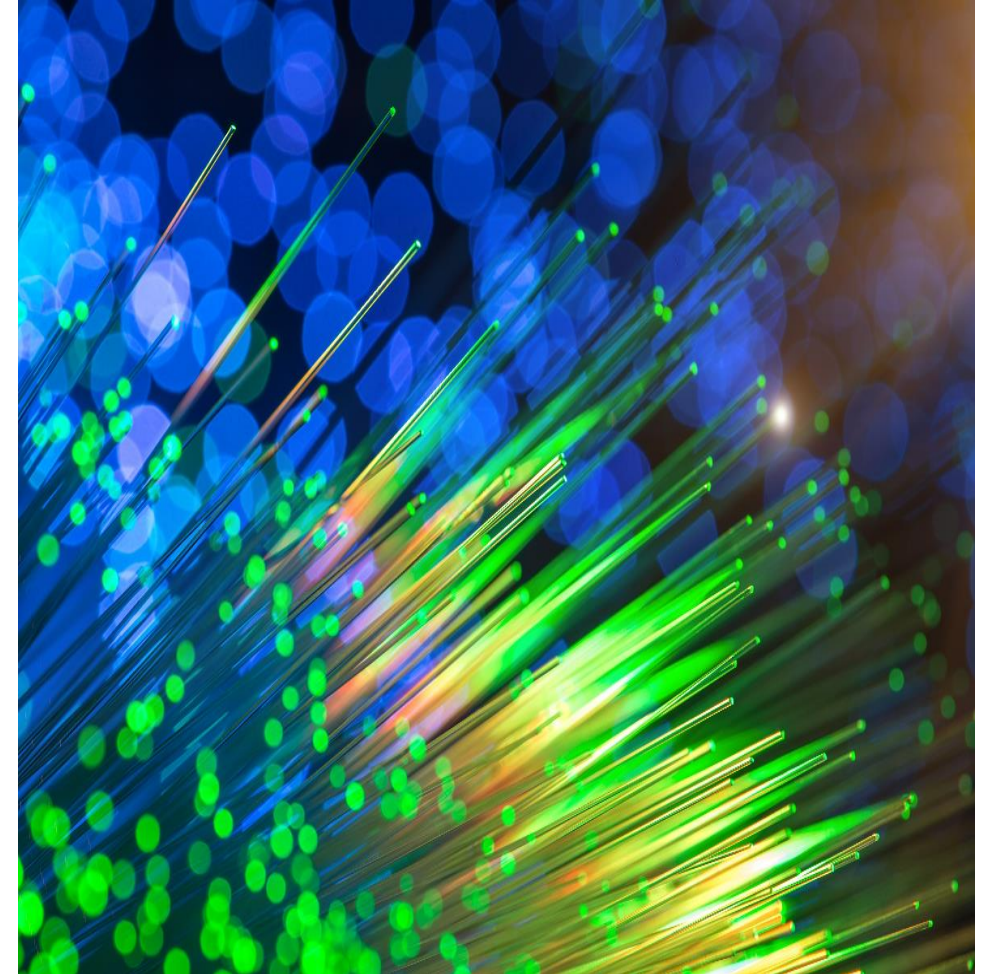
# Cyber Security Management in Private Equity Portfoliogesellschaften

15. September 2021

# Agenda

---

- 1 /** Einführung
- 2 /** Cyber Report 2021
- 3 /** Aktuelle Cyber-Threats und deren Schadensausmaß
- 4 /** Cyber Security Management in der Praxis
- 5 /** Virtuelle Diskussionsrunde inkl. Q&A



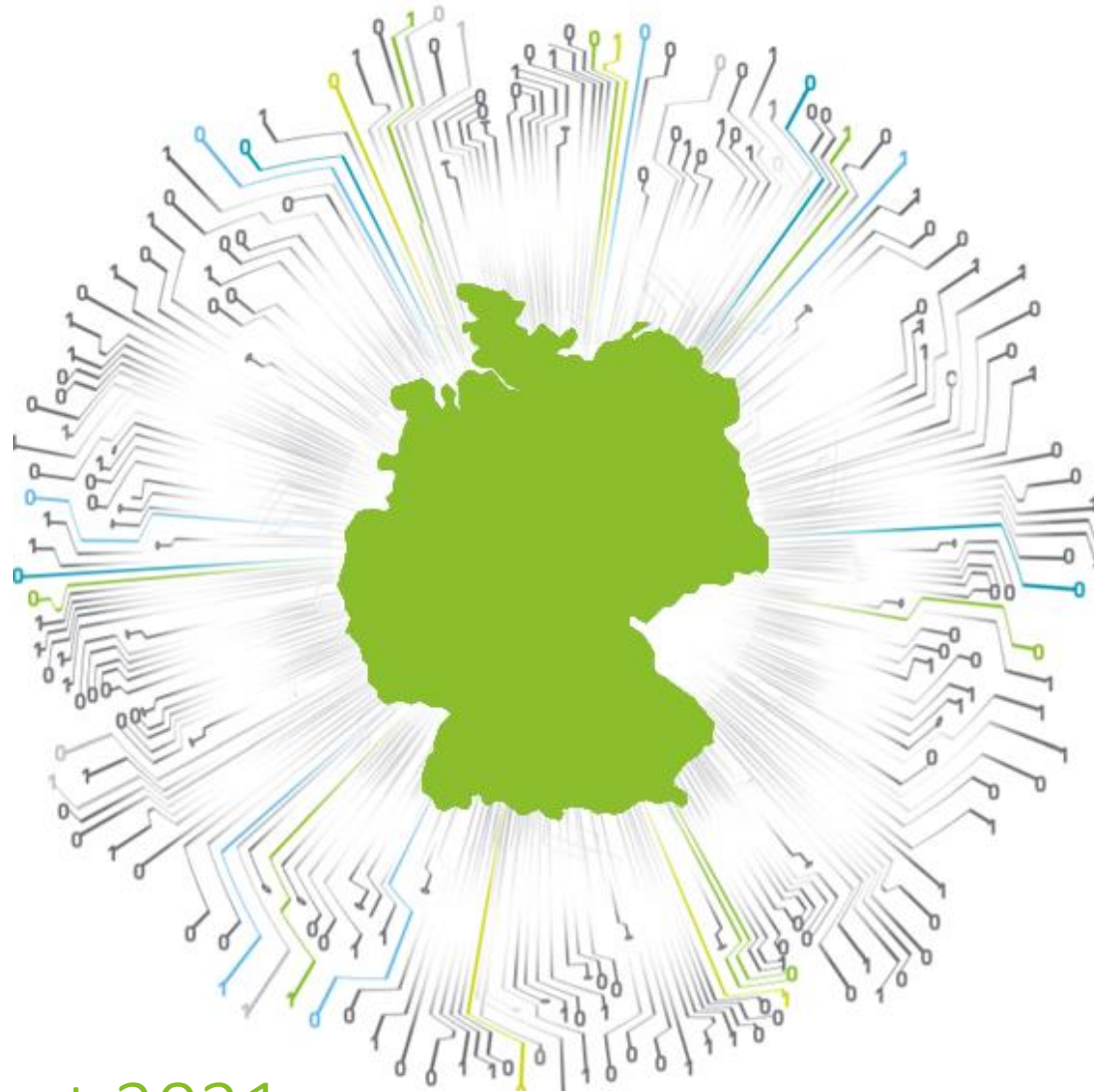
# Einführung

Judith Gorenflos (Senior Advisor Deloitte CFO Forum)

# Cyber Security Report 2021

Peter Wirnsperger

(Partner, Risk Advisory, Cyber and Strategic Risk)



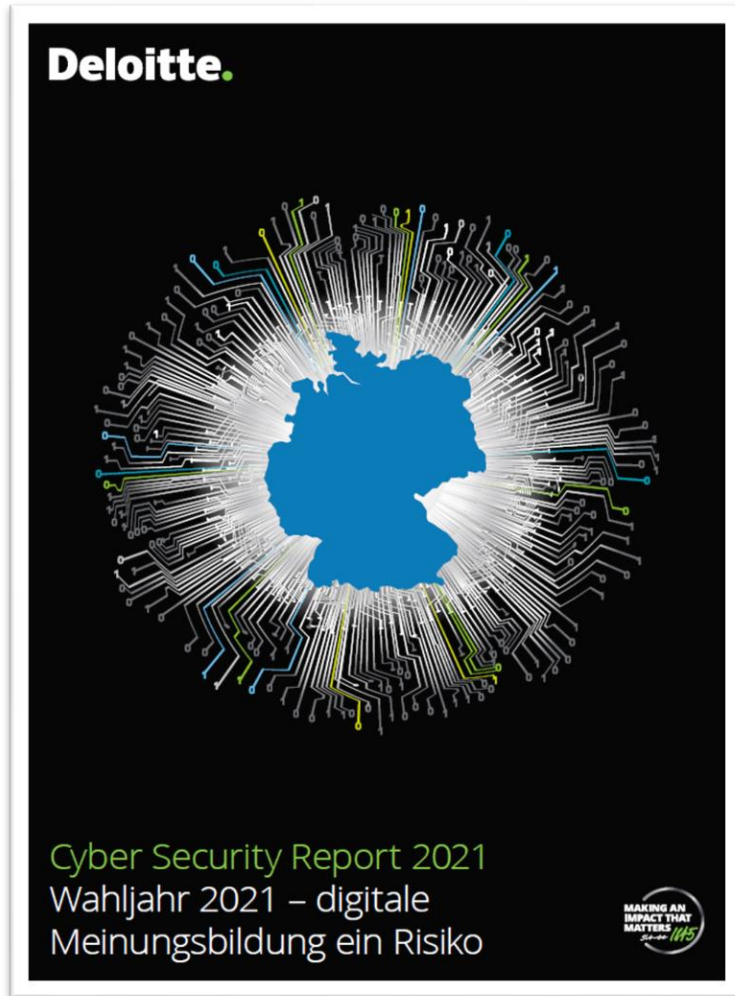
## Cyber Security Report 2021

Wahljahr 2021 – digitale Meinungsbildung ein Risiko

September 2021

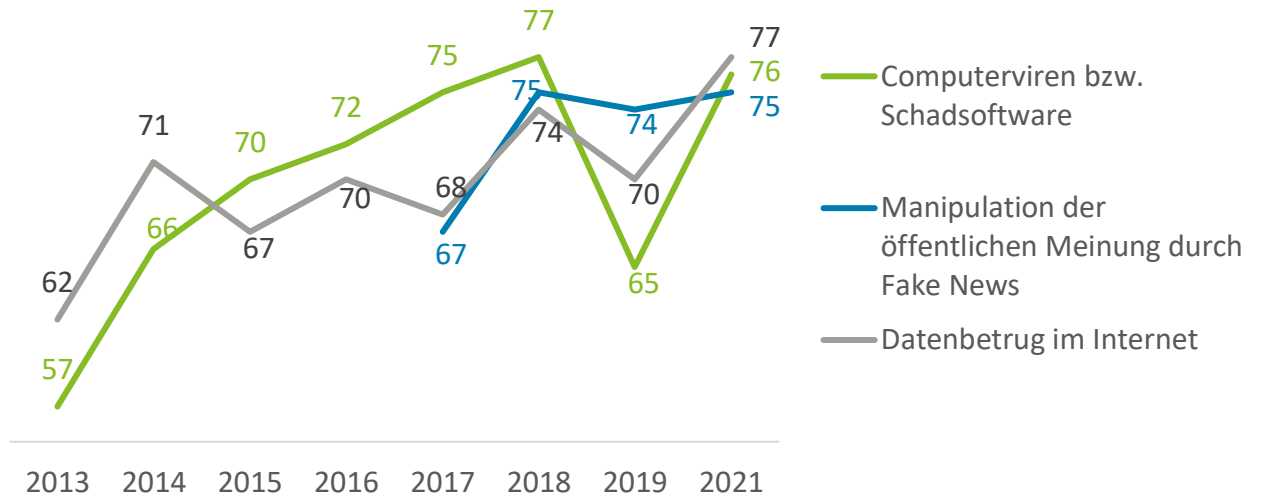
# Cyber Security Report 2021

## Beispiel Ergebnisse



### Bedrohungen durch Cyber-Risiken

Die **Bedrohung** durch einige der genannten Cyber-Risiken hat aus Sicht der Top-Entscheider aus Politik und Wirtschaft **in den vergangenen Jahren zugenommen**.



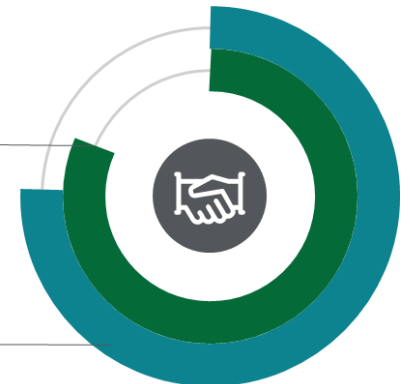
Es müsste **einen stärkeren Austausch** zwischen **staatlichen Stellen** und **Privatwirtschaft** zum Thema Cyber-Sicherheit geben.

**79 %**

der Wirtschaftsführer geben das an.

**76 %**

der Abgeordneten geben das an.



# Cyber Security Report 2021

## Kernaussagen

### Einschätzung der Gefährdung

Im Vergleich zu vorherigen Erhebungen verbleiben die Einschätzungen vieler Cyber-Risiken auf hohem Niveau. Datenbetrug im Internet wird vor den Gefahren durch Schadsoftware und Fake News als größtes Cyber-Risiko für die Menschen in Deutschland in diesem Jahr angesehen. Mit dieser Risikoeinstufung liegt die Gefahr durch Datenbetrug seit 2013 konstant unter den Top-3-Risiken aus Sicht der Entscheidungsträger.

### Ausbaufähige Zusammenarbeit von Politik und Wirtschaft

Auch wenn eine gute Zusammenarbeit zwischen Politik und Wirtschaft essenziell für das Cyber-Sicherheitsniveau in Deutschland und Europa ist, wird der Austausch zwischen beiden Seiten von knapp 80 Prozent der Wirtschaftsführer als nicht ausreichend empfunden. Bedingt wird diese Wahrnehmung durch die Auffassung beider Seiten, dass Abgeordnete nicht gut über die Bedürfnisse der Wirtschaft informiert sind.

### Schlüsseltechnologien „Made in EU“

Die große Mehrheit der Abgeordneten und der Wirtschaftsführer erachten es für die Cyber-Sicherheit in Deutschland als notwendig, dass wichtige Schlüsseltechnologien für die Digitalisierung und Vernetzung von deutschen oder europäischen Unternehmen hergestellt werden. Die Abhängigkeit von anderen Ländern im Bereich von Schlüsseltechnologien wird kritisch gesehen.

### Zentralisierung

Fast drei Viertel der Wirtschaftsführer wünschen sich eine stärkere Zentralisierung staatlicher Stellen beim Thema Cyber-Sicherheit, um einen einheitlichen Ansprechpartner für ihre Belange zu haben. Zum einen würde dadurch die Verteilung der Zuständigkeiten klarer strukturiert. Zum anderen würde es Vertrauen in die zuständigen Behörden schaffen.

### Cyber-Risiken in der Corona-Pandemie

Durch die Corona-Pandemie ist die Bedeutung der Cyber-Sicherheit verstärkt in den Fokus der Öffentlichkeit gelangt. Die Verbreitung der Home-Office-Arbeit und die starke Vernetzung erhöhen die Angriffsfläche für Cyber-Kriminelle. Um dieser Herausforderung zu begegnen, hat ein Großteil der Entscheidungsträger spezielle IT-Sicherheitsmaßnahmen getroffen. Auch wenn das Risiko, das von Mitarbeitenden im Home-Office ausgeht insgesamt als eher gering eingeschätzt wird, bestehen bei einem Teil der Befragten Zweifel am Risikobewusstsein ihrer Mitarbeiter.

# Cyber Security Report 2021

## Mögliche Handlungsfelder und deren Bedeutung für die Wirtschaft

### 01 Zusammenarbeit mit der Wirtschaft vertiefen

- Austausch zwischen Politik und Wirtschaft fördern
- Akteure aus der Wirtschaft und Gesellschaft müssen ihre Belange aktiv in die Politik bringen

### 02 Internet- und Medienkompetenz fördern

- Meinungsmanipulationen aktiv entgegenwirken
- Sensibilisierung im Bereich Cyber-Sicherheit
- Gefahren in Social Media gezielt adressieren

### 03 Technologische Unabhängigkeit fördern

- Forschungs- und Entwicklungsaktivitäten gezielt fördern
- Schaffung eines europäischen Rechtsrahmens

### 04 Verhältnismäßige und ausbalancierte Regulierung

- Balance in der Regulierung von Cyber-Sicherheitsmaßnahmen finden
- Qualität in der Umsetzung von Cyber-Sicherheitsmaßnahmen verbessern

#### Bedeutung für die Wirtschaft:



Investitionen in Prävention notwendig



Unternehmerisches Potential in der Entwicklung von Schlüsseltechnologien



Viele Unternehmen sind noch nicht ausreichend resilient und benötigen weitere Optimierung



Kontinuierliche Sensibilisierung



# Cyber Security Report 2021 – Ansprechpartner & Team



**Peter J. Wirnsperger**

Lead Civil Government

Tel: +49 (0)40 32080 4675

[pwirnsperger@deloitte.de](mailto:pwirnsperger@deloitte.de)



**Marius von Spreti**

Cyber Risk Leader

Tel: +49 (89) 29036 5999

[mvonspreti@deloitte.de](mailto:mvonspreti@deloitte.de)



**André Roosen**

Senior Manager

Cyber | Public Sector



**Cornelis Raeber**

Manager

Cyber | Public Sector



**Sabrina Zimmermann**

Senior Consultant

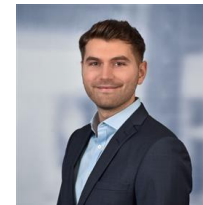
Cyber | Public Sector



**Nicolas Inzelmann**

Senior Consultant

Cyber Strategy



**Maximilian Lobbes**

Consultant

Cyber Strategy



**Markus Göttemann**

Consultant

Cyber | Public Sector



**Franziska Hörth**

Consultant

Cyber | Public Sector

# Aktuelle Cyber-Threats und deren Schadensausmaß

Thomas Wendrich (Director, Risk Advisory, Cyber and Strategic Risk)



## Wargaming und Red Teaming – der Weg zur besseren Cyber Resilience

Thomas Wendrich - Deloitte Cyber Risk

**Warum gewinnt das Thema *Cyber*  
für alle Geschäftsbereiche und Stabs-funktionen  
zunehmend an Relevanz?**

# Warum ist das Thema “**Cyber Security**” für alle Bereiche von wachsender Bedeutung?



Zunahme **bargeldloser Zahlungsverkehr** und digitalen Zahlungsmitteln



**Kundenerwartung** in die Online-Präsenz und Services



Optimierung **interner Prozesse**, z. B. Logistik, KRITIS-Verordnung



Optimierung des **Einkaufs**

Parallel zu den wachsenden Anforderungen an die Digitalisierung nehmen die **illegalen Gewinne aus der Cyber-Kriminalität** zu



**Anatomie der Angriffen**, die unmittelbar auf illegale Gewinne zielen (CEO fraud, Ransomware) **ändert sich**

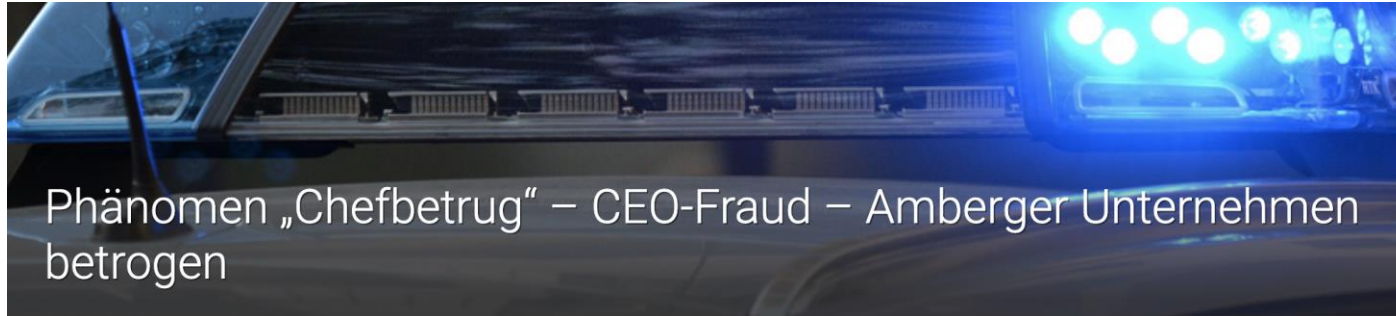


**Das Risiko**, Opfer von direkten Angriffen zu werden, ist **unverändert hoch**



**Das Risiko**, Opfer von ungezielten Angriffen (Kollateralschäden) zu werden, **ist gestiegen**

# Vorfälle



## Phänomen „Chefbetrug“ – CEO-Fraud – Amberger Unternehmen betrogen

📅 6. Juli 2021

Bereits am 1. Juli 2021 wurde ein Unternehmen aus Amberg Opfer einer Betrugsmasche – dem CEO-Fraud. Dabei erlitt die Firma einen finanziellen Schaden in Höhe eines höheren fünfstelligen Eurobetrages.

SPECIALTY CHEMICALS

## Siegfried, Brenntag, and Symrise hit by cyberattacks

Companies say hacker activity caused temporary production shutdowns

by Melody M. Bomgardner

May 27, 2021 | A version of this story appeared in **Volume 99, Issue 20**

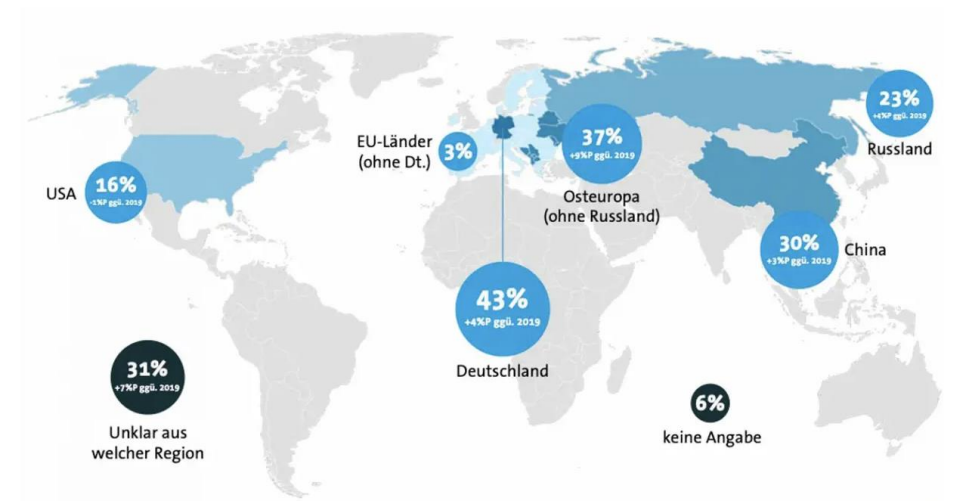
Das Bundeskriminalamt zählte in drei Jahren 250 Betrugsfälle, die bekanntesten waren 2016 der bayerische Autozulieferer Leoni AG (40 Mio. Euro) und der österreichisch-chinesische Luftfahrtzulieferer FACC (50 Mio. Euro). In der Regel verzichten die betroffenen Firmen aus Imagegründen darauf, darüber zu berichten.

## 220 Milliarden Euro Schaden durch Ransomware und andere Cyber-Angriffe

Deutsche Unternehmen beklagen zunehmende kostspielige Cyber-Angriffe. Dabei spielt Ransomware eine gewichtige Rolle.

Lesezeit: 3 Min. In Pocket speichern

71



Ursprungsregionen von Cyber-Angriffen, sofern sie die Geschädigten ausmachen konnten. (Bild: Bitkom)

## Leoni AG: 40 Mio. EUR-Betrug durch Social Engineering

Der Autozulieferer Leoni ist einem sog. „CEO-Fraud“ zum Opfer gefallen. Der Schaden beläuft sich auf ca. 40 Millionen EUR.

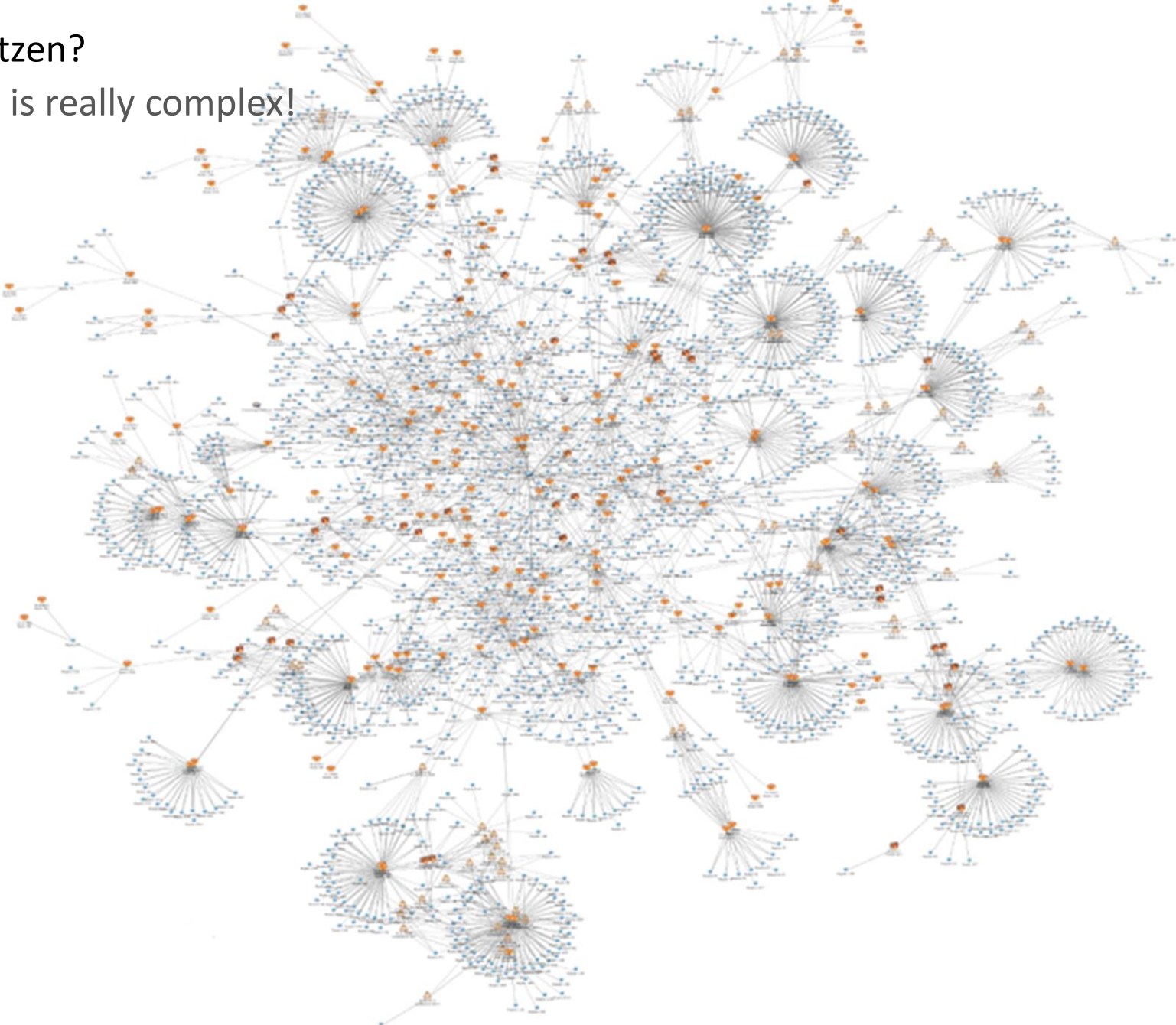
Die **internen Strukturen** und **Verantwortlichkeiten** erschweren häufig die Umsetzung einer effizienten Cyber-Sicherheitsorganisation



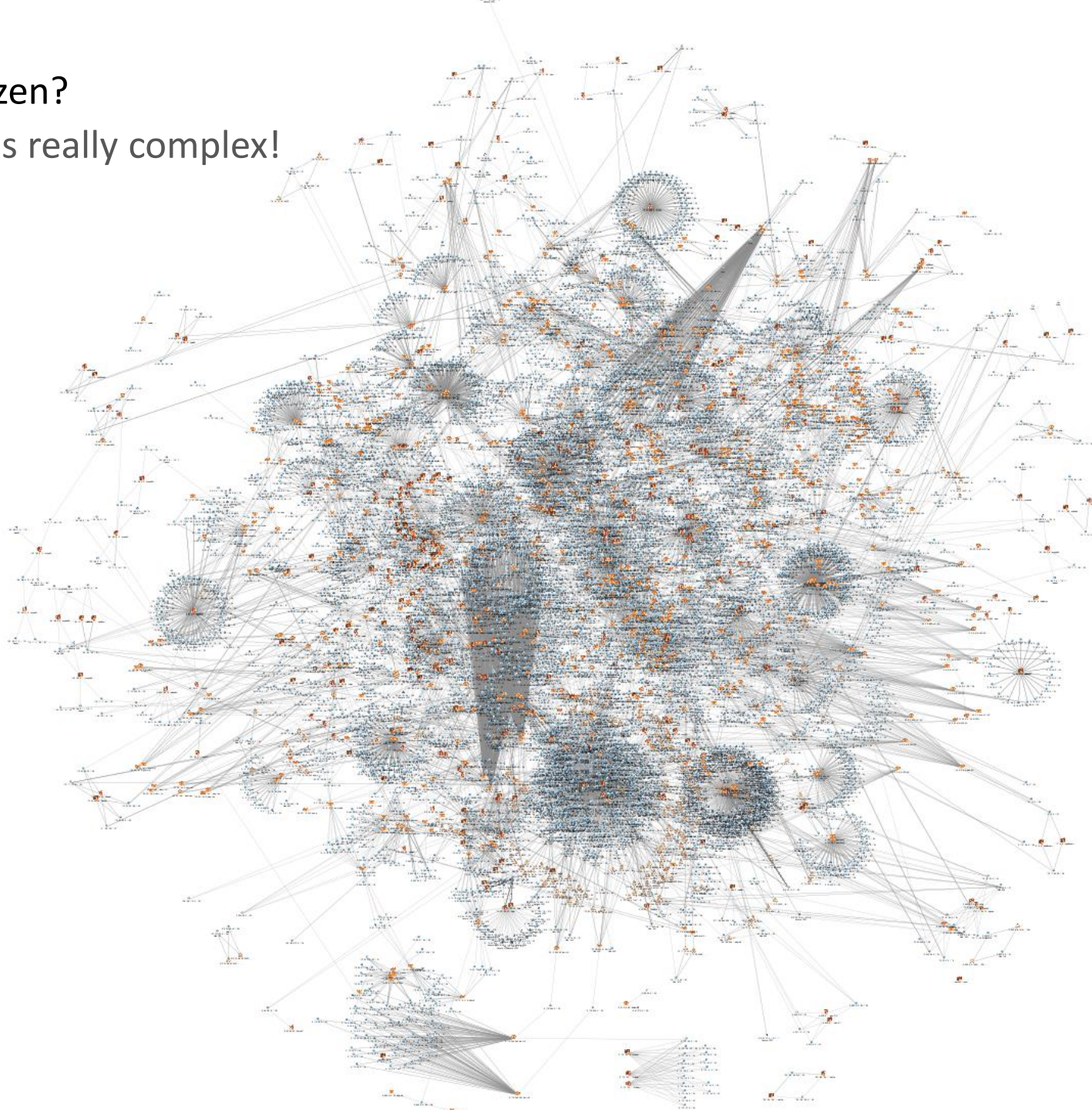


Was muss ich schützen?

OUR infrastructure is really complex!

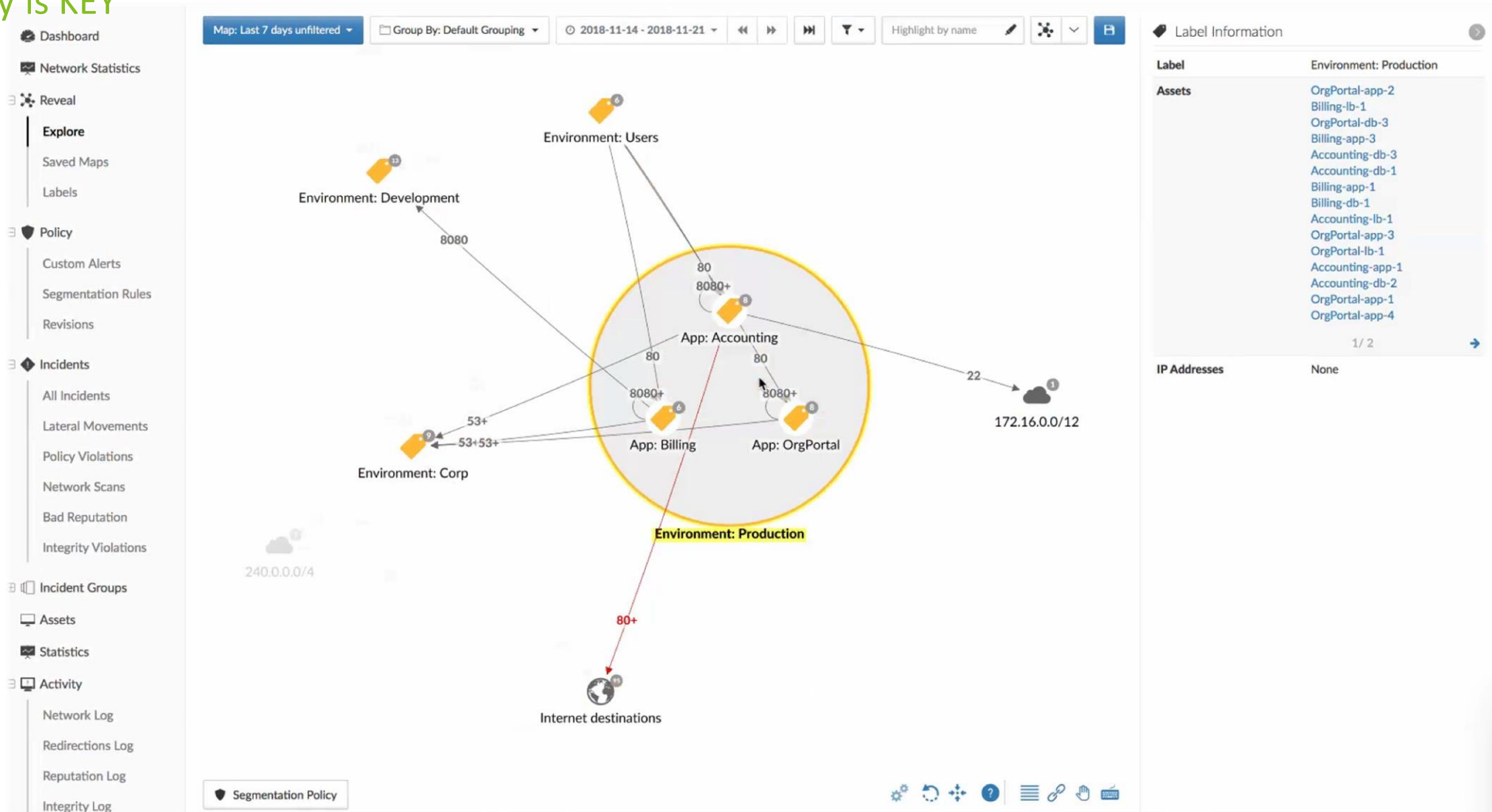


Was muss ich schützen?  
OUR infrastructure is really complex!



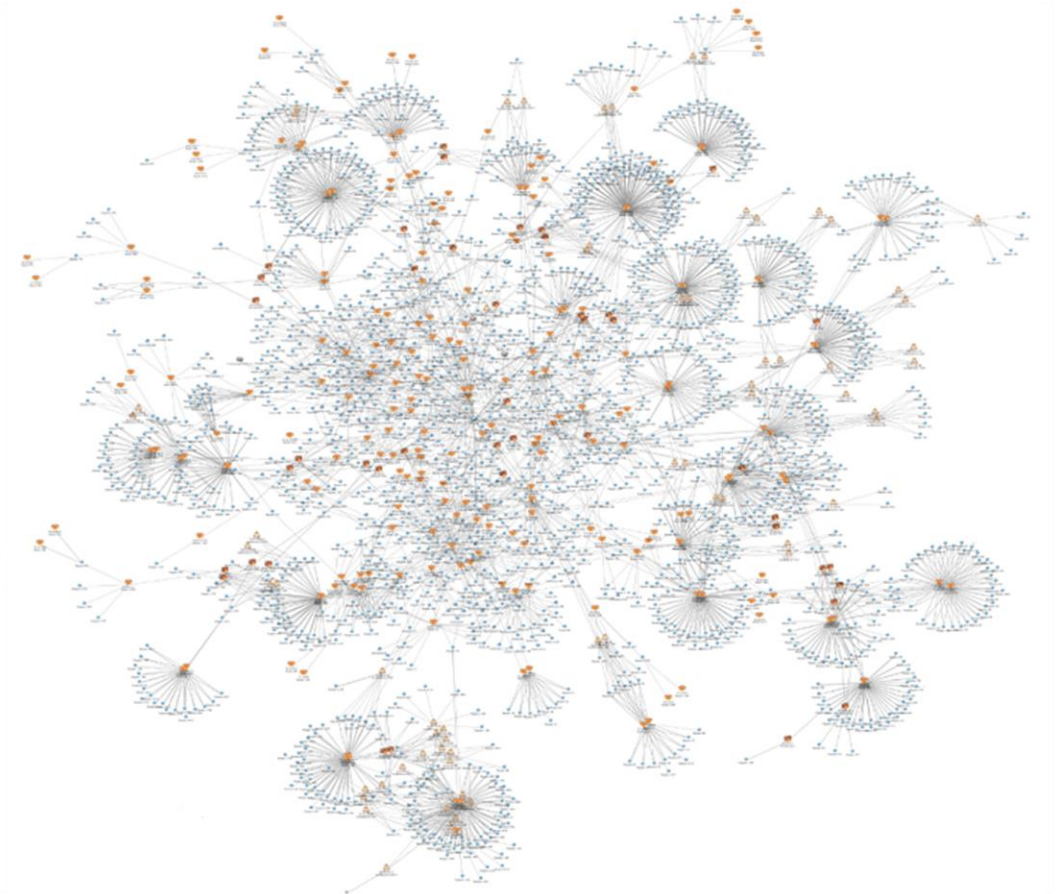
# Was muss ich schützen?

Visibility is KEY



# WAS ich schützen möchte MUSS ich kennen!

OUR Infrastructure is really complex



Visibility is KEY

Dashboard

Network Statistics

Reveal

Explore

- Saved Maps
- Labels

Policy

- Custom Alerts
- Segmentation Rules
- Revisions

Incidents

- All Incidents
- Lateral Movements
- Policy Violations
- Network Scans
- Bad Reputation
- Integrity Violations

Incident Groups

Assets

Statistics

Activity

- Network Log
- Redirections Log
- Reputation Log
- Integrity Log

Segmentation Policy

Map: Last 7 days unfiltered

Group By: Default Grouping

2018-11-14 - 2018-11-21

Highlight by name

Label Information

| Label  | Environment: Production |
|--------|-------------------------|
| Assets | OrgPortal-app-2         |
|        | Billing-db-1            |
|        | OrgPortal-db-3          |
|        | Billing-app-3           |
|        | Accounting-db-3         |
|        | Accounting-db-1         |
|        | Billing-app-1           |
|        | Accounting-ib-1         |
|        | OrgPortal-app-3         |
|        | OrgPortal-ib-1          |
|        | Accounting-app-1        |
|        | Accounting-db-2         |
|        | OrgPortal-app-1         |
|        | OrgPortal-app-4         |

IP Addresses

None

1 / 2

**Wie kann *eine Organisation* sich präventiv und reaktiv auf Schadensfälle vorbereiten?**

# Resilienz – ein Schlüssel zu mehr Sicherheit

Wie können Organisationen Bedrohungen und Risiken antizipieren, sich vorbereiten, effizient reagieren und sich kontinuierlich anpassen?

**Ziel:**

**Nachhaltige Stärkung der Resilienz von Organisationen gegen feindliche Angriffe und Missbrauch**

**Ansatz:**

**Red Teaming** – wir agieren aus der Perspektive des Angreifers, um digitale, physische und soziale Schwachstellen aufzudecken und die Reaktionsfähigkeit von Führungskräften und Mitarbeitern unter realen Bedingungen zu testen

## Resilienz



**Red Teaming** wurde im 19. Jahrhundert im Militär entwickelt und ist heute ein integraler Bestandteil des Planungsprozesses



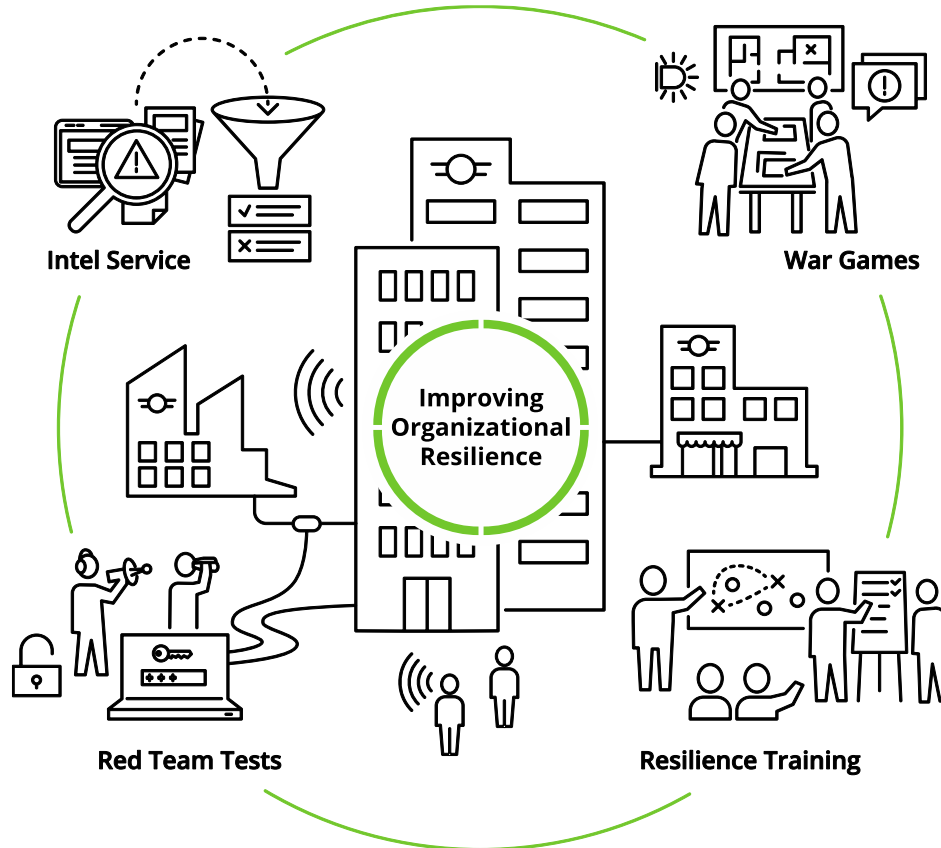
**2018** hat die **EZB** mit dem TIBER-EU Framework erst-mals einen regulatorischen Rahmen für Red Teaming vorgegeben



**Unser Service** versteht sich als kontinuierliches Angebot mit dem Ziel die organisatorische Resilienz nachhaltig zu erhöhen

# Red Teaming Übungen sind ein umfassendes Konzept, bestehend aus vier zusammenhängenden und sich ergänzenden Elementen

**Regelmäßige Berichte** mit 360°-Blick auf gegenwärtige, aufkommende und potentielle Bedrohungen



**Feindselige Angriffe**, mit dem Ziel Verwundbarkeiten aufzu-decken und darzustellen, wie das Kerngeschäft bei Ausnutzung dieser betroffen sein könnte

**Simulation** von fortlaufenden, variablen Szenarien zum Test der Reaktionsfähigkeit einer Organisation

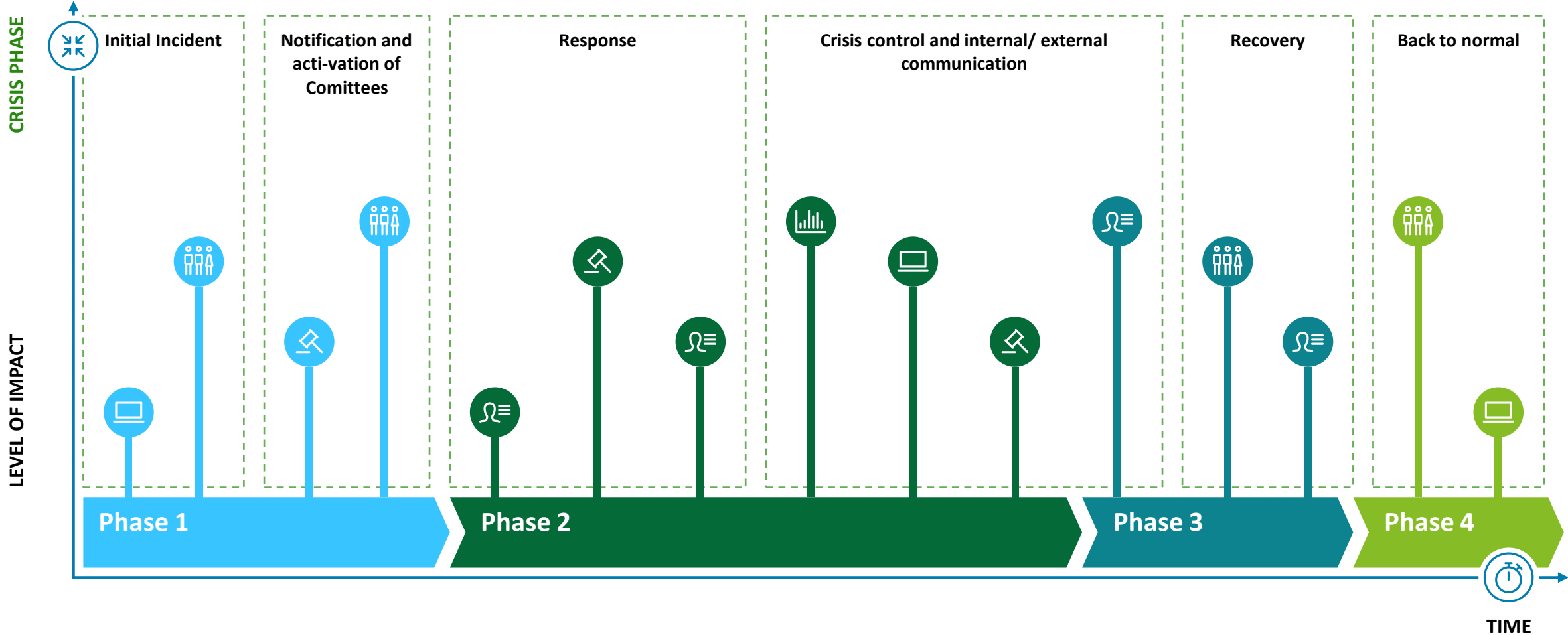
**Trainingsprogramm**, das alle relevanten Akteure einbindet und im Ergebnis die Resilienz des Unternehmens steigert

**Wie sind *Übungen zur Krisenbewältigung* strukturiert und wie laufen sie ab?**

Cyber War Games



# Lageeinspielungen (exemplarisch)

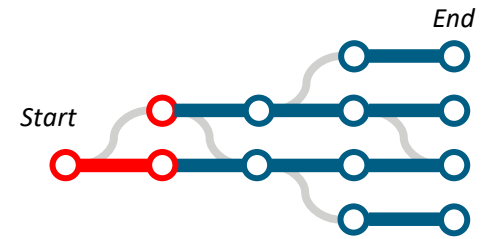


**Welche *Auswirkungen* könnte ein Cyber-Angriff auf die “CFO-FORUM AG” haben?**

Ein “Cyber-War-Game-Intermezzo”

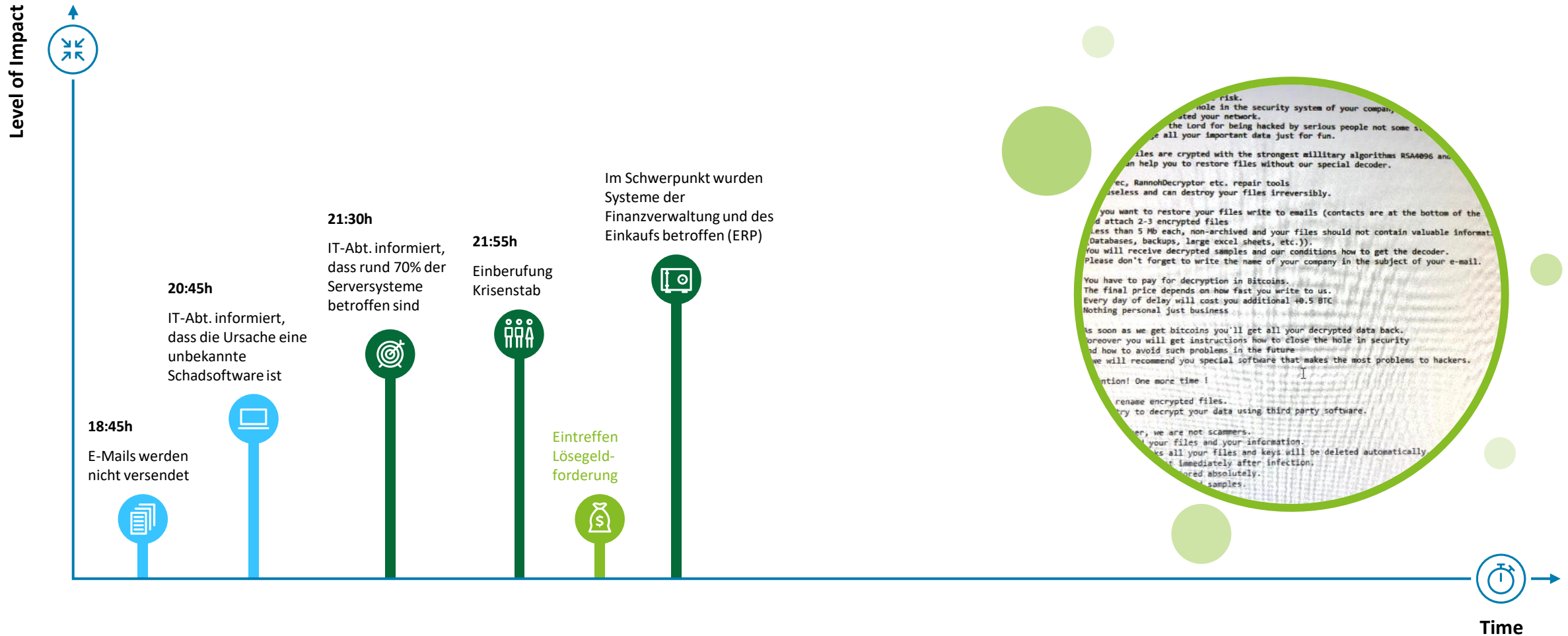
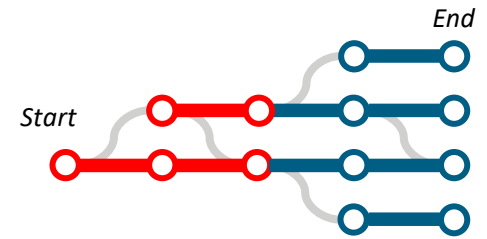
# Lageeinspielungen

Simulationen sind dynamisch – Szenarien entwickeln sich auf Grundlage der Entscheidungen und Handlungen des Krisenteams



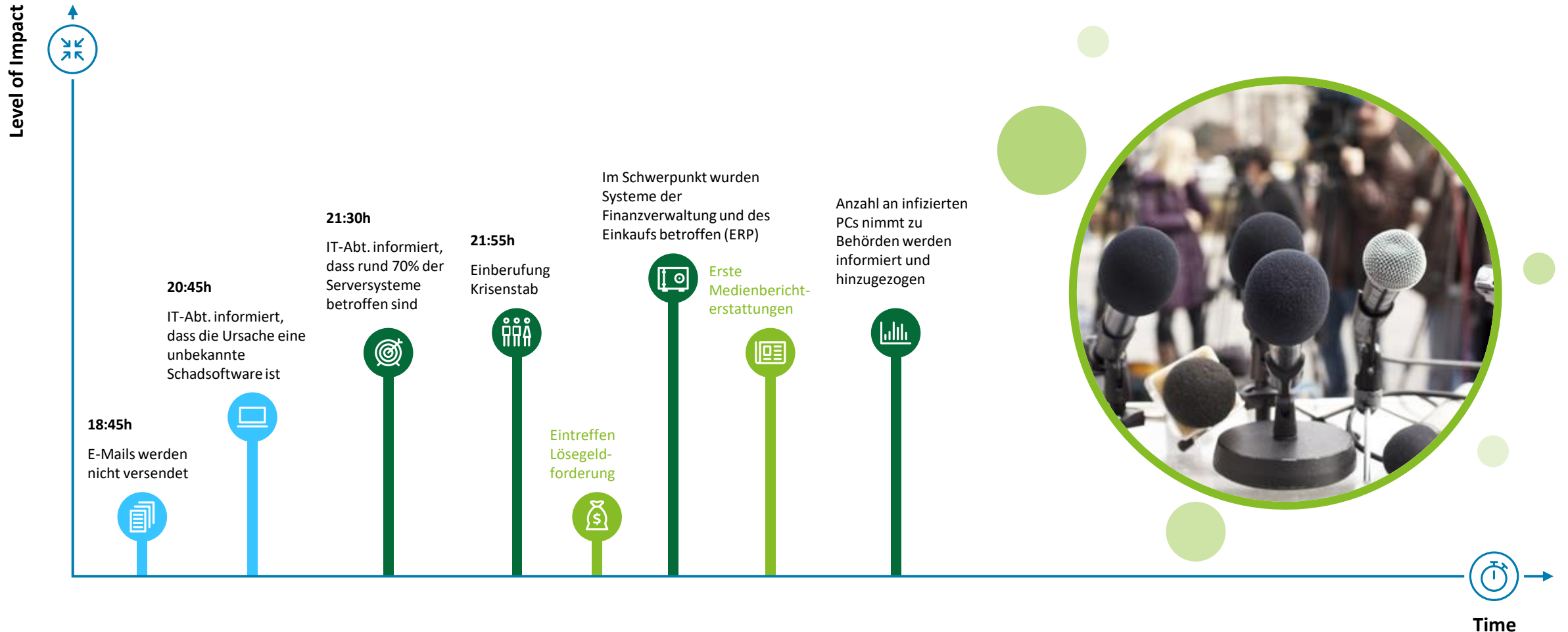
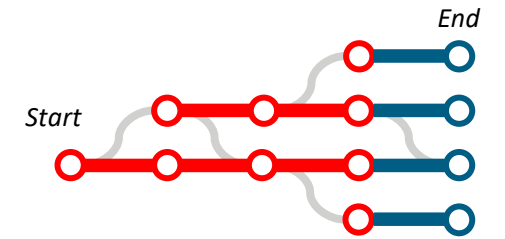
# Lageeinspielungen

Simulationen sind dynamisch – Szenarien entwickeln sich auf Grundlage der Entscheidungen und Handlungen des Krisenteams

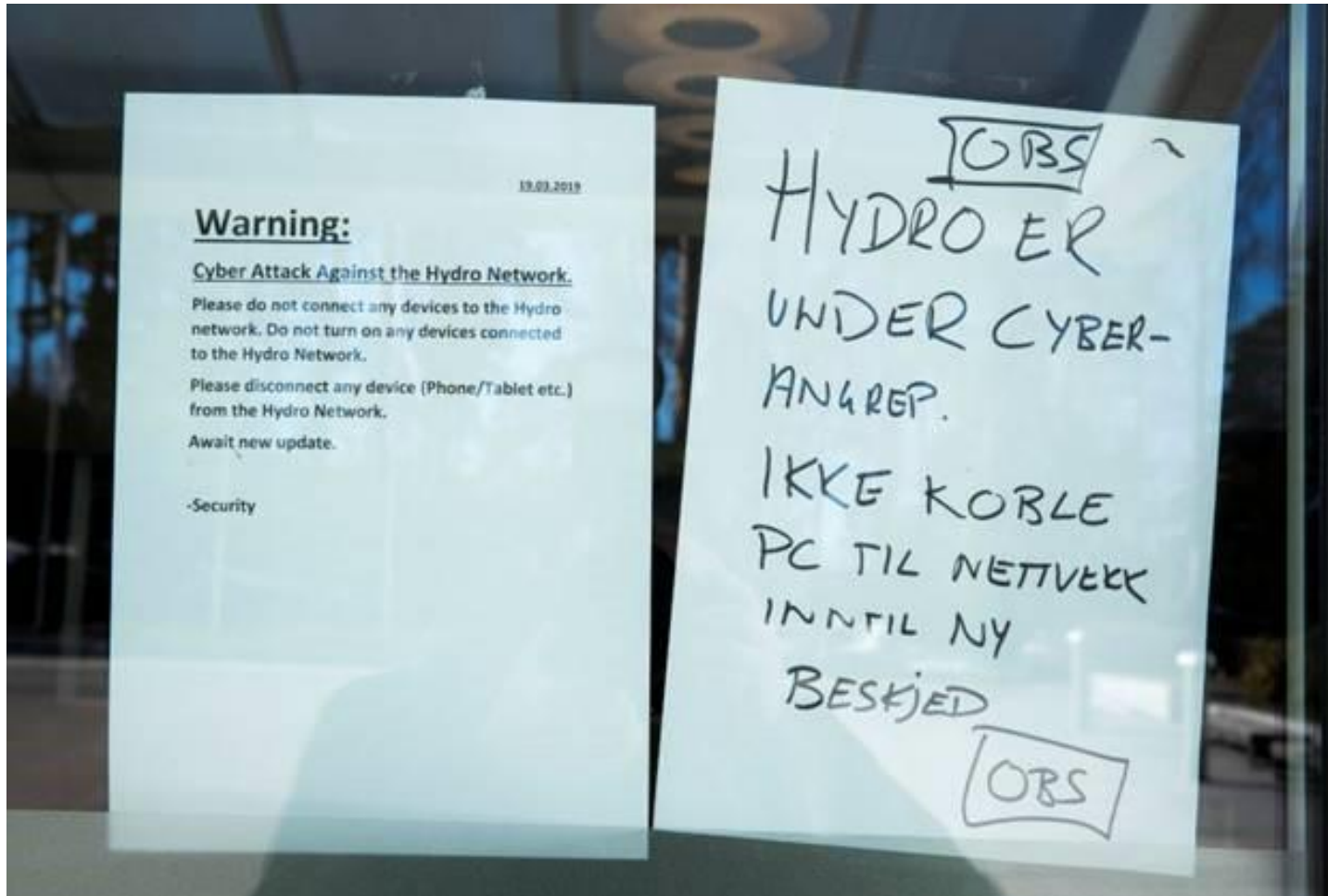


# Lageeinspielungen

Simulationen sind dynamisch – Szenarien entwickeln sich auf Grundlage der Entscheidungen und Handlungen des Krisenteams



## Kommunikation bei Norsk Hydro



Ein Hacker-Angriff auf den Aluminiumhersteller Norsk Hydro hat Furcht vor einem Versorgungsengpass ausgelöst. Der Preis für das unter anderem im Automobil- und Flugzeugbau benötigte Industriemetall stieg am Dienstag um bis zu 1,2 Prozent auf ein Drei-Monats-Hoch von 1944 Dollar je Tonne.

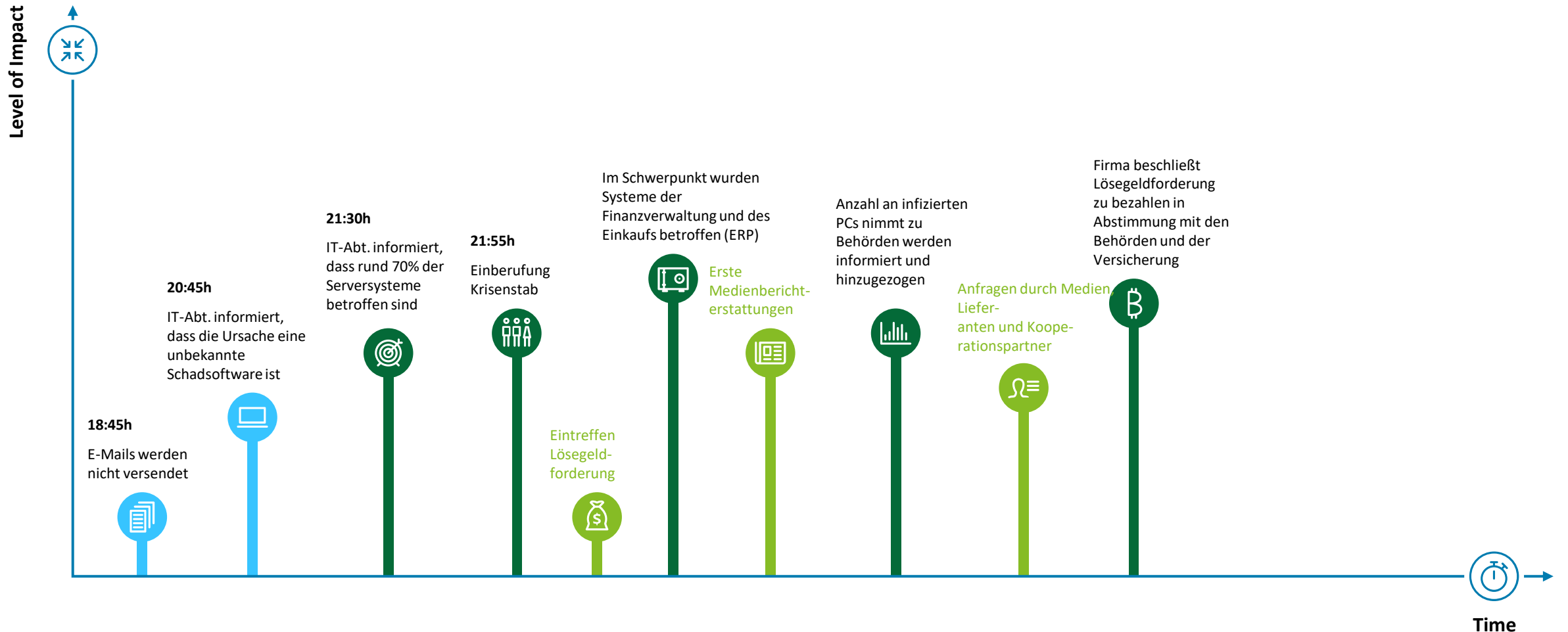
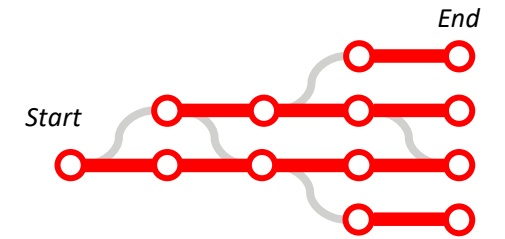
Die Aktien von Norsk Hydro verloren bis zu 3,4 Prozent.

Youtube Video:

<https://youtu.be/S-ZIVuM0we0>

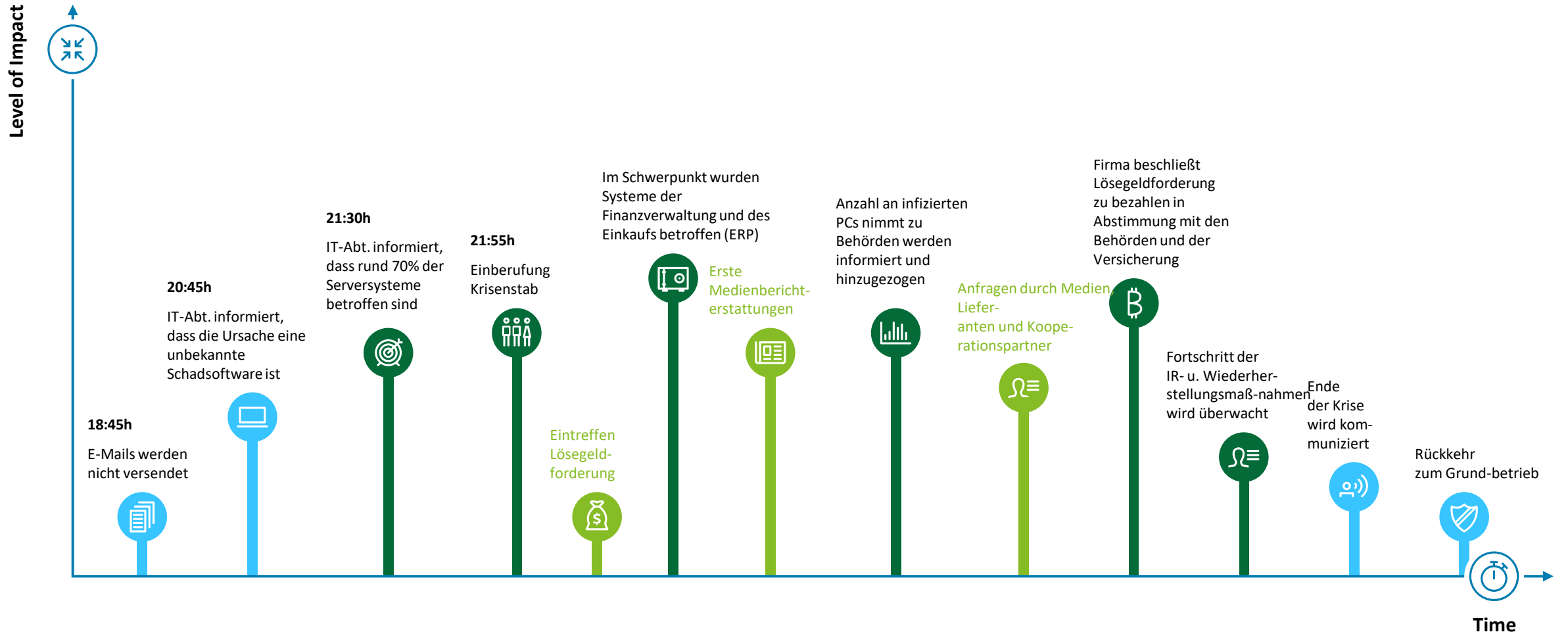
# Lageeinspielungen

Simulationen sind dynamisch – Szenarien entwickeln sich auf Grundlage der Entscheidungen und Handlungen des Krisenteams



# Lageeinspielungen

Simulationen sind dynamisch – Szenarien entwickeln sich auf Grundlage der Entscheidungen und Handlungen des Krisenteams



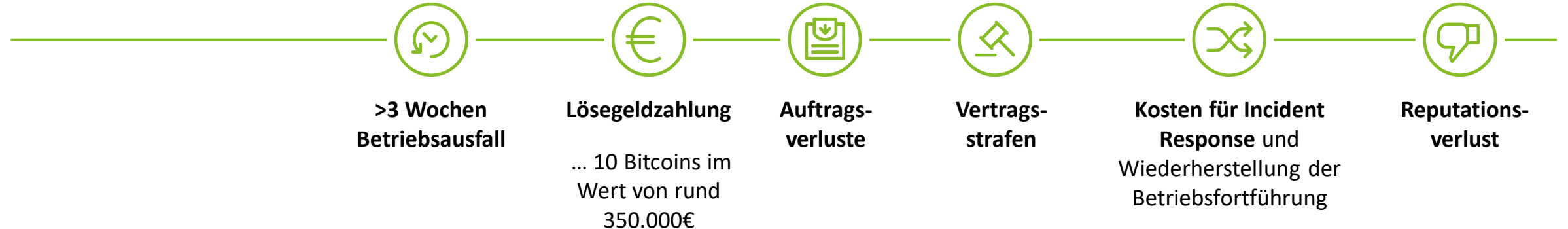


# Resumé

# Nachträgliche Betrachtung der Schäden aus dem Ransomware-Angriff

Die aus Ransomware-Angriffen resultierenden Schäden variieren sehr stark je Unternehmen.

Bei einem vergleichbaren Angriff sind folgenden Schäden entstanden



# Lessons Learnd



**Leistungen**  
der verschiedenen externen  
Anbieter (Cloud-Dienste, Forensic,  
etc.)



**Abgeschlossenen Versicherungen**  
auf Umfang und Inhalte  
überprüfen



**Krisenszenarien**  
auf Aktualität und Relevanz  
untersuchen



Folgende Maßnahmen  
zur schnellen  
Krisenbewältigung  
**sollten überprüft  
werden**



**Gesamtnotfallkonzept**  
für Backups im Zusammen-spiel  
mit den wichtigsten  
Krisenszenarien



**Operative Prozesse** im internen  
und externen Umfeld prüfen




**IT- und Prozesskonzepte** auf  
Tauglichkeit für das eigene Geschäft  
überprüfen

---

## Thomas Wendrich

**Director - Cyber & Strategic Risk**

 [twendrich@deloitte.de](mailto:twendrich@deloitte.de)

 +49 1515 8072334

Dammtorstraße 12  
20354 Hamburg  
Deutschland



Diese Präsentation enthält ausschließlich allgemeine Informationen und weder die Deloitte GmbH Wirtschaftsprüfungsgesellschaft noch Deloitte Touche Tohmatsu Limited, noch ihre Mitgliedsunternehmen oder deren verbundene Unternehmen (insgesamt das „Deloitte Netzwerk“) erbringen mittels dieser Präsentation professionelle Beratungs- oder Dienstleistungen. Diese Präsentation ist insbesondere nicht geeignet, eine persönliche Beratung zu ersetzen. Keines der Mitgliedsunternehmen des Deloitte Netzwerks ist verantwortlich für Verluste jedweder Art, die irgendjemand im Vertrauen auf diese Präsentation erlitten hat. Diese Präsentation ist vertraulich zu behandeln. Eine Weitergabe an Dritte – auch in Auszügen – bedarf unserer vorherigen schriftlichen Zustimmung.

Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited („DTTL“), eine „private company limited by guarantee“ (Gesellschaft mit beschränkter Haftung nach britischem Recht), ihr Netzwerk von Mitgliedsunternehmen und ihre verbundenen Unternehmen. DTTL und jedes ihrer Mitgliedsunternehmen sind rechtlich selbstständig und unabhängig. DTTL (auch „Deloitte Global“ genannt) erbringt selbst keine Leistungen gegenüber Mandanten. Eine detailliertere Beschreibung von DTTL und ihren Mitgliedsunternehmen finden Sie auf [www.deloitte.com/de/UeberUns](http://www.deloitte.com/de/UeberUns).

Deloitte erbringt Dienstleistungen in den Bereichen Wirtschaftsprüfung, Risk Advisory, Steuerberatung, Financial Advisory und Consulting für Unternehmen und Institutionen aus allen Wirtschaftszweigen; Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Mit einem weltweiten Netzwerk von Mitgliedsgesellschaften in mehr als 150 Ländern verbindet Deloitte herausragende Kompetenz mit erstklassigen Leistungen und unterstützt Kunden bei der Lösung ihrer komplexen unternehmerischen Herausforderungen. Making an impact that matters – für rund 286.000 Mitarbeiter von Deloitte ist dies gemeinsames Leitbild und individueller Anspruch zugleich.

**Haben Sie Fragen?**





Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited („DTTL“), ihr weltweites Netzwerk von Mitgliedsunternehmen und ihre verbundenen Unternehmen (zusammen die „Deloitte-Organisation“). DTTL (auch „Deloitte Global“ genannt) und jedes ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen, die sich gegenüber Dritten nicht gegenseitig verpflichten oder binden können. DTTL, jedes DTTL-Mitgliedsunternehmen und verbundene Unternehmen haften nur für ihre eigenen Handlungen und Unterlassungen und nicht für die der anderen. DTTL erbringt selbst keine Leistungen gegenüber Mandanten. Weitere Informationen finden Sie unter [www.deloitte.com/de/UeberUns](http://www.deloitte.com/de/UeberUns).

Deloitte ist ein weltweit führender Dienstleister in den Bereichen Audit und Assurance, Risk Advisory, Steuerberatung, Financial Advisory und Consulting und damit verbundenen Dienstleistungen; Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Unser weltweites Netzwerk von Mitgliedsgesellschaften und verbundenen Unternehmen in mehr als 150 Ländern (zusammen die „Deloitte-Organisation“) erbringt Leistungen für vier von fünf Fortune Global 500®-Unternehmen. Erfahren Sie mehr darüber, wie rund 330.000 Mitarbeiter von Deloitte das Leitbild „making an impact that matters“ täglich leben: [www.deloitte.com/de](http://www.deloitte.com/de).

Diese Veröffentlichung enthält ausschließlich allgemeine Informationen. Weder die Deloitte GmbH Wirtschaftsprüfungsgesellschaft noch Deloitte Touche Tohmatsu Limited („DTTL“), ihr weltweites Netzwerk von Mitgliedsunternehmen noch deren verbundene Unternehmen (zusammen die „Deloitte-Organisation“) erbringen mit dieser Veröffentlichung eine professionelle Dienstleistung. Diese Veröffentlichung ist nicht geeignet, um geschäftliche oder finanzielle Entscheidungen zu treffen oder Handlungen vorzunehmen. Hierzu sollten Sie sich von einem qualifizierten Berater in Bezug auf den Einzelfall beraten lassen.

Es werden keine (ausdrücklichen oder stillschweigenden) Aussagen, Garantien oder Zusicherungen hinsichtlich der Richtigkeit oder Vollständigkeit der Informationen in dieser Veröffentlichung gemacht, und weder DTTL noch ihre Mitgliedsunternehmen, verbundene Unternehmen, Mitarbeiter oder Bevollmächtigten haften oder sind verantwortlich für Verluste oder Schäden jeglicher Art, die direkt oder indirekt im Zusammenhang mit Personen entstehen, die sich auf diese Veröffentlichung verlassen. DTTL und jede ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen.