Microsoft Security

Swiss Security Week
16 – 18 November 2021

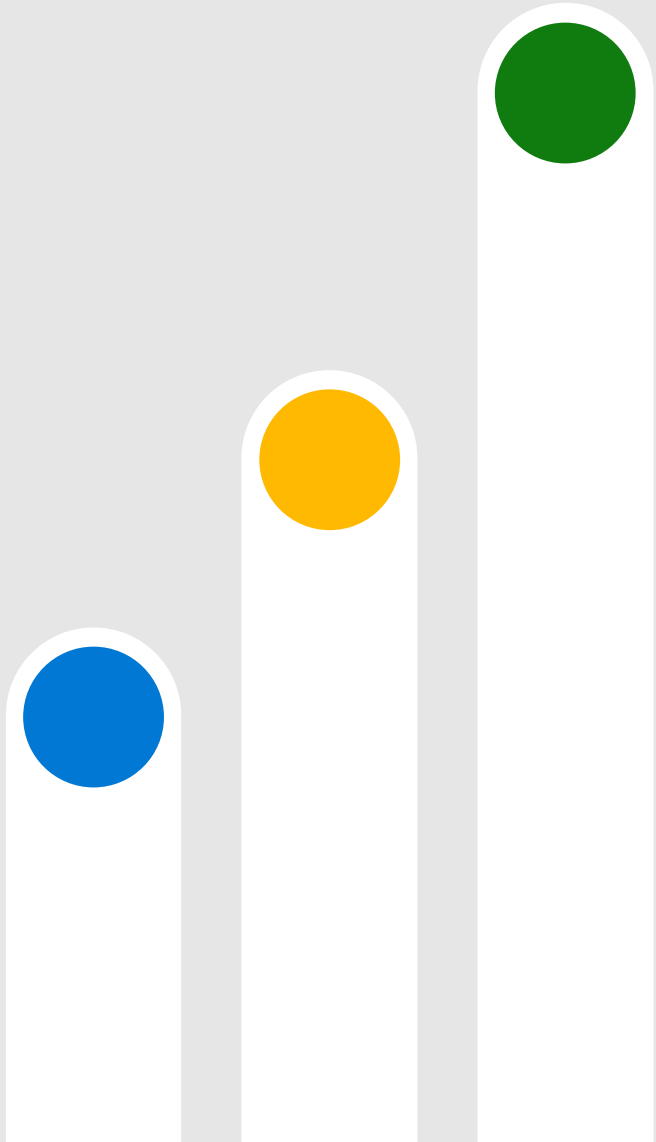
We've been hacked!

Nicola Guglielmo
Head of IT Operation

Kyle Krüsi
Senior MSM Customer Engineer

Agenda

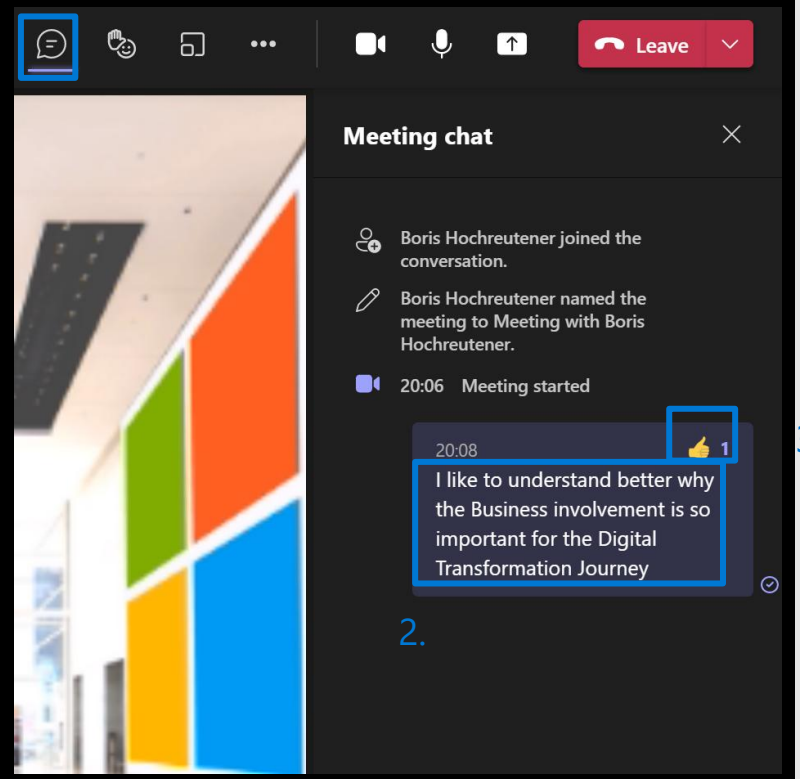
- Aktuelle Cyberangriffe in der Schweiz
- Was ist Cyber Security
- Theorie wie läuft ein Hack ab
- Erfahrungsbericht einer Cyberattacke bei Griesser
  - Zeitablauf
  - Wie lief der Hack technisch ab
  - Lessons Learned
- Summary
- Roundtable



Welcome to our #virtual Roundtable

We start with a Road to the Cloud to ensure a common End2End understanding and wording. This session will be followed by more interactive conversation based on your questions in the 2nd Roundtable Session.
Please continuously race your questions and ideas in our Chat.

HOW



1. Press the "Chat" icon in Teams
2. Ongoing Ask your questions in the Chat
3. Continuously vote questions –then more thumbs up then higher the priority in the 2nd Roundtable Session

Aktuelle Cyberangriffe in der Schweiz

Cyberangriff auf Industriegruppe Bucher

SECURITY, ATTACKE, INDUSTRIE, BUCHER INDUSTRIES, SCHWEIZ,

Von Keystone-sda/paz, 10. November 2021 17:28 — Letzte Aktualisierung: 11. November 2021 17:31

Foto: Bucher Municipal

Betroffen ist die Gemeindefahrzeugsparte Bucher Municipal. Die Produktion wurde vorsorglich gestoppt.

Erpresser stellen Schweizer Steuererklärungen ins Internet

Hochvertrauliche Daten von Privatpersonen und Firmen aus den Kantonen Zürich, Zug und Schwyz sind online zugänglich. Damit erreicht die Cyberkriminalität eine neue Dimension.

Opfer von Erpressern

Media-Markt ist auch in der Schweiz von Cyberangriff betroffen

Erpresser verlangten 240 Millionen Dollar und legten einen Grossteil der Systeme lahm. Für die Kundinnen und Kunden bedeutet das erhebliche Einschränkungen.

Beim Cyberangriff auf MCH sind wohl Kundendaten abgeflossen

MCH GROUP, SECURITY, SCHWEIZ, BREACH, CYBERCRIME

Von Katharina Jochum, 28. Oktober 2021 16:53 — Letzte Aktualisierung: 28. Oktober 2021 17:45

Die Gruppe betreibt unter anderem die Art Basel. Foto: G. Sighele unter CC 2.0.

Laut dem Messeveranstalter haben Analysen ergeben, dass beim Cyberangriff auch Daten von Kunden und Partnern erbeutet worden sind.

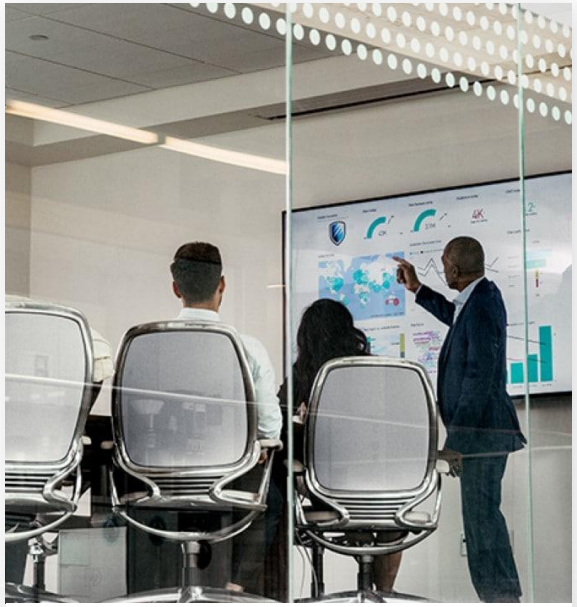
SRF Rundschau Sendung vom 13.10

Was ist Cyber Security?

- Cybersicherheit ist die Praxis, Computer, Server, mobile Geräte, elektronische Systeme, Netzwerke und Daten vor böswilligen Angriffen zu schützen.
- Es ist auch als Informationstechnologiesicherheit oder elektronische Informationssicherheit bekannt.
- Der Begriff gilt in einer Vielzahl von Kontexten, von Business bis Mobile Computing, und kann in einige gängige Kategorien unterteilt werden.

Identity and access management

Ihre universelle Plattform zur Verwaltung und Sicherung von Identitäten.



Threat protection

Stoppen Sie Angriffe mit integrierter und automatisierter Sicherheit.

Information protection

Schützen Sie Ihre sensiblen Daten – wo auch immer sie sich befinden oder reisen.

Cloud security (Security management)

Schützen Sie Ihre Cloud-übergreifenden Ressourcen.

Kosten für Sicherheitsverletzungen steigen

$4.3M

durchschnittliche Kosten für Sicherheitsverletzungen

+1 Woche

Der Lebenszyklus von Datenschutzverletzungen dauerte 2021 eine Woche länger als 2020 [1]

Insider-Datenschutzverletzungen können Kosten verursachen

bis 20%

des Jahresumsatzes eines Unternehmens [2]

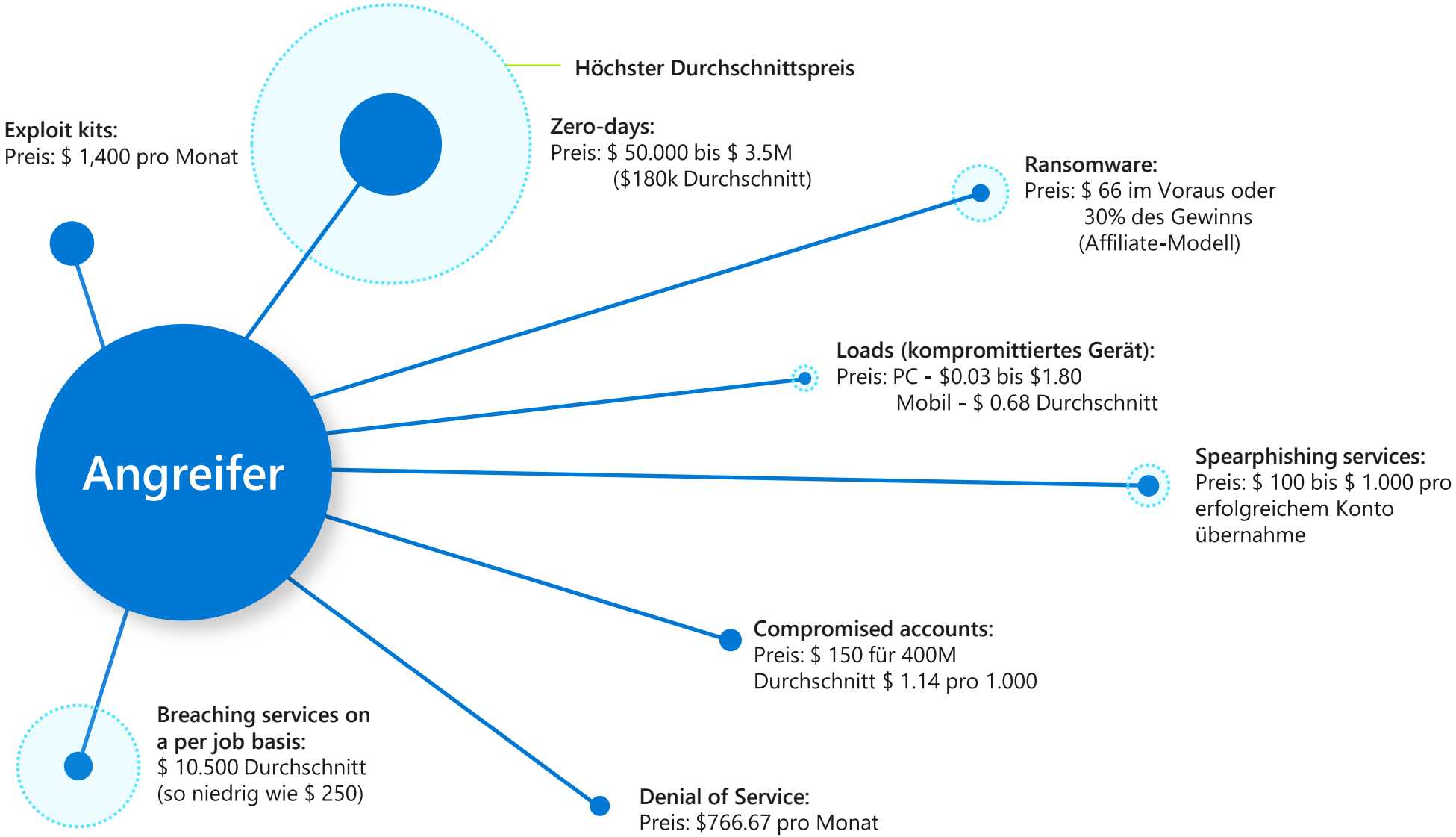
10%

Erhöhung der durchschnittlichen Gesamtkosten eines Verstoßes 2020-2021. Dies ist der größte kostenanstieg in einem Jahr in den letzten sieben Jahren. [1]

[1] Poneman Institute Cost of Breach Data, 2021

[2] Poneman Institute Cost of Insider Risk, 2020

Angriffsdienste sind billig



Traditionelle Verteidigungen sind den heutigen Herausforderungen nicht gewachsen

Cloud Changes Security

DIFFERENT SECURITY MODEL

SECURITY BENEFITS

- *Secure/consistent platform*
- *Better visibility, control, and threat detection*
- *Less direct responsibility*
- *Automated routine hygiene functions*
- *Easier compliance management/reporting*

REQUIRES

- *Learn New Platform and Controls*
- *Learn shared responsibility model*
- *Increase Identity & Access hygiene*

BIG CHANGES

IDENTITY & ACCESS IS THE FRONT LINE

- Primary security perimeter for all workloads
- Firewalls/network still required for legacy workloads

NO PERMANENT PRIVILEGES

- Just in Time access for all resources
- Used to secure cloud platform and your tenant

Security challenges

Managing an ever-changing modern workplace and enterprise security with:

- Employee's **work expectations**;
- **Securing** Remote Work is a continuum
- An **evolving threat landscape** that outpace conventional security tools;
- **Regulatory requirements** driving increasing costs;
- **Zero trust:** effectively adapting security to the complexity of the modern environment.
- **Re-Assess** Remote Work e.g. enablement during COVID-19
- Use Microsoft recommended practices to "**never trust, always verify**".

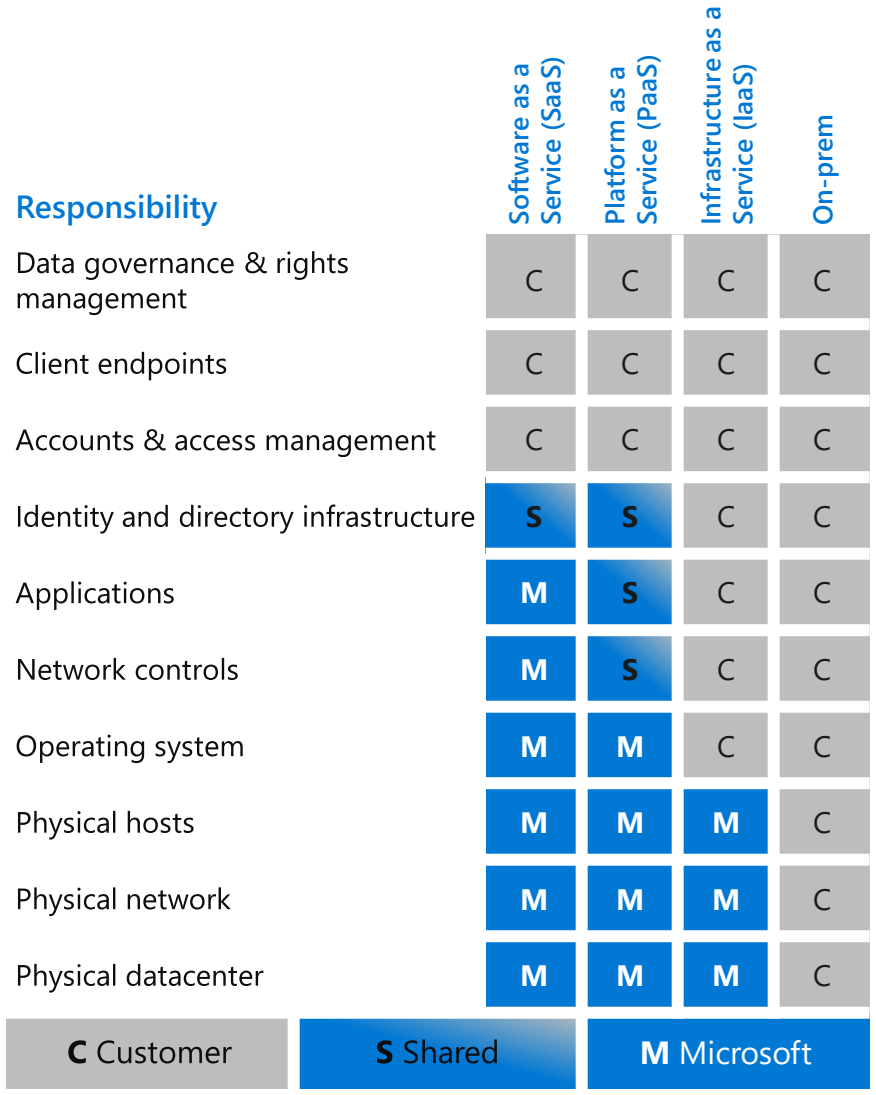
Security in a cloud-enabled world

Your organization's responsibility for security is based on the type of cloud service selected.

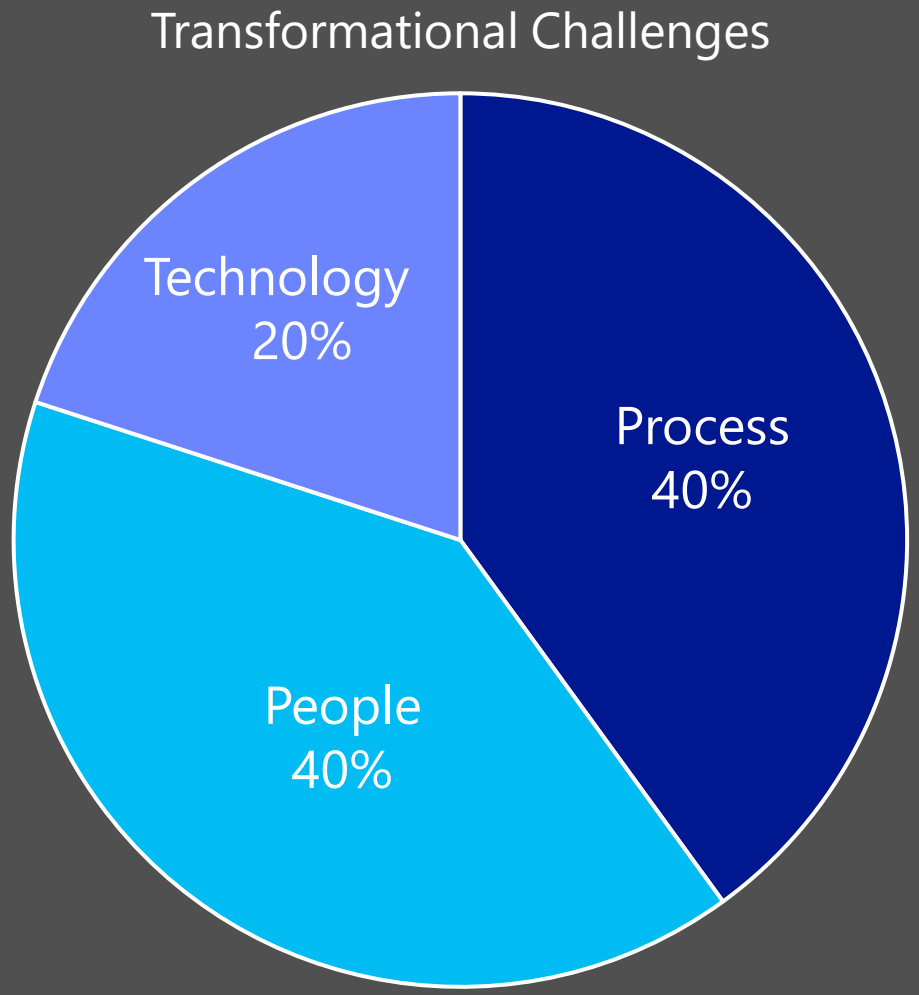
Cybersecurity threats make security more challenging—*however*, the public cloud makes it easier for you to manage as the security load shifts to the service provider.

Your organization's security focus ***must*** shift to data, identity, and application layers.

For a poster that maps this updated world, visit https://aka.ms/cloudsecurityposter

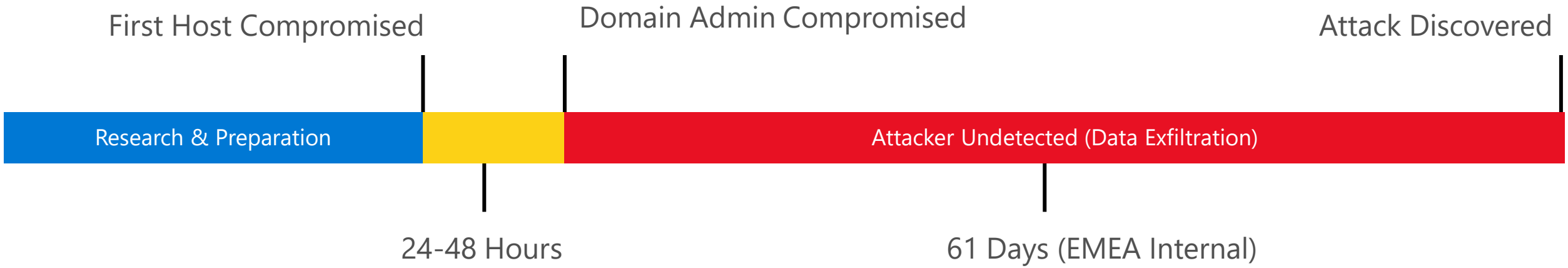


Heute bietet Security neue Möglichkeiten, um Ihr Unternehmen zu schützen, aber auch Herausforderungen



THEORIE
Typical Attack Timeline & Observations

Typical Attack Timeline & Observations



Attack Sophistication

Attack operators exploit any weakness

Target information on any device or service

Target AD & Identities

Active Directory controls access to business assets

Attackers commonly target AD and IT Admins

Attacks not detected

Current detection tools miss most attacks

You may be under attack (or compromised)

Response and Recovery

Response requires advanced expertise and tools

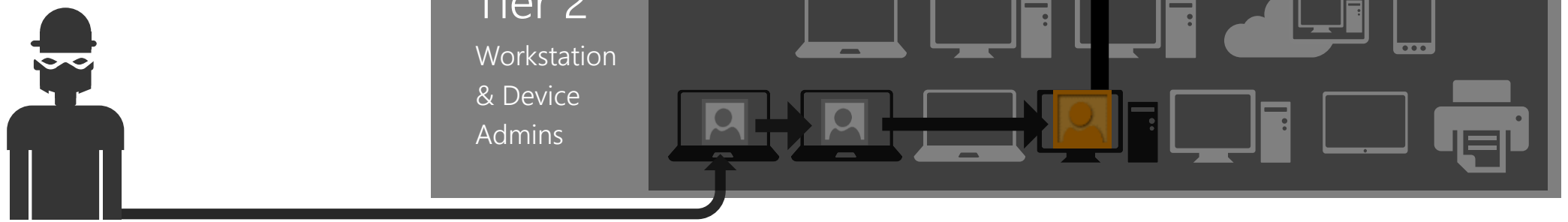
Expensive and challenging to successfully recover

Typical Attack Chain

Compromises privileged access

24-48 Hours

1. Beachhead (Phishing Attack, etc.)
2. Lateral Movement
   a. Steal Credentials
   b. Compromise more hosts & credentials
3. Privilege Escalation
   a. Get Domain Admin credentials
4. Execute Attacker Mission
   a. Steal data, destroy systems, etc.
   b. Persist Presence



Cyberattacke @Griesser

Griesser 1899
Anton Griesser with his team –
company founder and the first pioneer.
Anton Griesser und sein Team –
Unternehmensgründer und erster Pionier.
Anton Griesser et son équipe –
Fondateur de l'entreprise et premier pionnier.
Anton Griesser e il suo team –
fondatore dell'azienda e primo pioniere.

31'856t CO^2

Compensated with myClimate (as of October 2020).
Kompensiert mit myClimate (Stand Oktober 2020).
Compensées avec myClimate (état de octobre 2020).
Compensate con myClimate (aggiornato a ottobre 2020).

1'294'800 m^2

that's how many square meters of material Griesser processed in 2019.
so viele Quadratmeter an Material hat Griesser in 2019 verarbeitet.
la superficie de matière traitée par Griesser en 2019.
di materiale lavorato da Griesser nel 2019.

Griesser has an active presence in over 20 countries across Europe.
Griesser ist aktiv in mehr als 20 Ländern Europas.
Griesser déploie son activité dans plus de 20 pays en Europe.
Griesser è rappresentato in oltre 20 Paesi europei.

1'300

Employees.
Mitarbeiter.
Collaborateurs.
Collaboratori.

6

Production sites.
Produktionsstandorte.
Sites de production.
Siti di produzione.

1882*

Year of foundation.
Das Gründungsjahr.
Année de fondation.
Anno di fondazione.

over
über
plus de
oltre

30

different nationalities are represented at Griesser.
verschiedene Nationalitäten arbeiten bei Griesser.
nationalités différentes travaillent chez Griesser.
diverse nazionalità lavorano presso Griesser.

Tuesday
13.04.2021

TAGBLATT

Anmelden | Meine Gemeinde

Hacker greifen Aadorfer Griesser AG an

Die Griesser AG wurde Opfer einer gezielten Cyberattacke und ist aktuell nur telefonisch sowie per E-Mail erreichbar.

Stefan Borkert
14.04.2021, 17.18 Uhr

Hören | Merken | Drucken | Teilen

Die Griesser AG in Aadorf ist Opfer einer Cyberattacke geworden. PD

Computerworld

Business | Social | Mobile | Technik | Software | Security | Te

Fachkräfte | Business-IT | Homeoffice | Fintech | Start-ups | Interview | Swisscom Bu

Best Practice | Whitepapers | Pressemeldungen | ICT Analytics | Breakfast Sessions

Home › Security › Hacking › Schweizer Storenfirma Griesser von Hackern angegriffen

Sicherheitsvorfall 14.04.2021, 17:44 Uhr

Schweizer Storenfirma Griesser von Hackern angegriffen

Die Schweizer Storenfirma Griesser wurde von Hackern ins Visier genommen. Ob auch Daten von Mitarbeitenden, Kunden und Partnern betroffen sind, ist derzeit noch unklar.

PRESSEPORTAL

14.04.2021 – 16:03

Griesser AG

Griesser von Cyber-Angriff betroffen

Aadorf (ots)

Griesser wurde Opfer einer gezielten Cyber-Attacke und ist aktuell nur telefonisch sowie per Mail erreichbar. Ein oder mehrere unbekannte Täter haben mit einer Ransomeware, einem sogenannten Erpressungstrojaner, die Server in der Schweiz attackiert. Davon betroffen sind auch die Produktionsstätten in Aadorf (TG), Österreich und Frankreich.

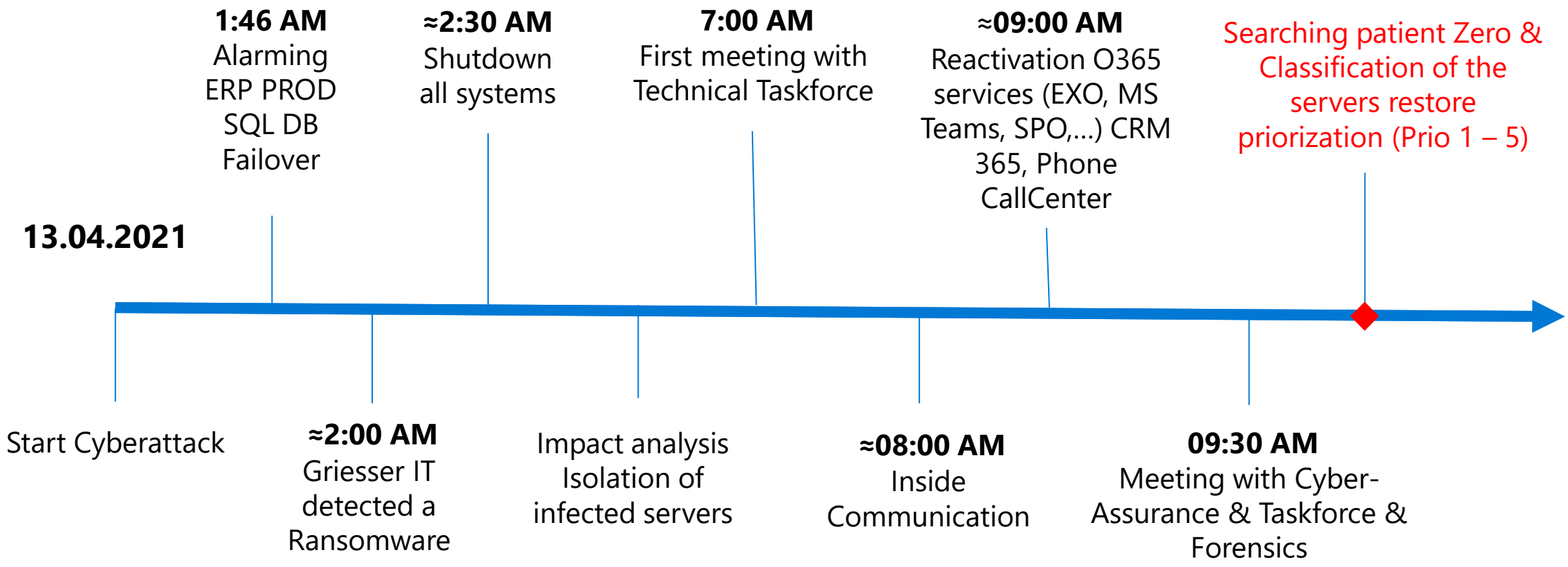
Um eine mögliche Ausbreitung des Angriffs im Unternehmen zu verhindern, fuhr die Griesser IT-Taskforce unverzüglich verschiedene IT-Systeme herunter. Parallel leitete ein Krisenstab mit Hochdruck weitere Schritte ein, um der Cyberattacke mit zielgerechten Massnahmen zu begegnen und den Normalbetrieb schrittweise wiederherzustellen. Ein eventueller Datenabfluss wird geprüft.

Abo Cyber-Erpressung in Aadorf

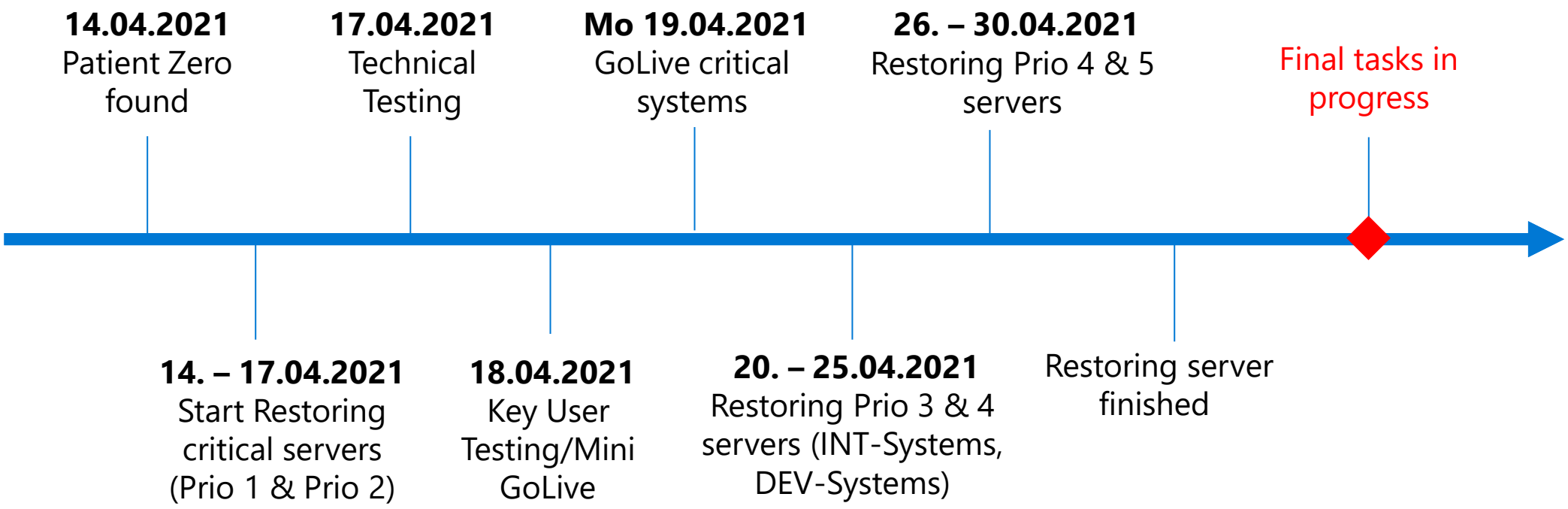
Hacker attackieren regionales KMU

Der Sonnenstoren-Hersteller Griesser ist Opfer einer Cyberattacke geworden. Es handelt sich um die Ransomeware Conti, wie das Unternehmen aus Aadorf mitteilt.

Cyberangriff Marke Griesser

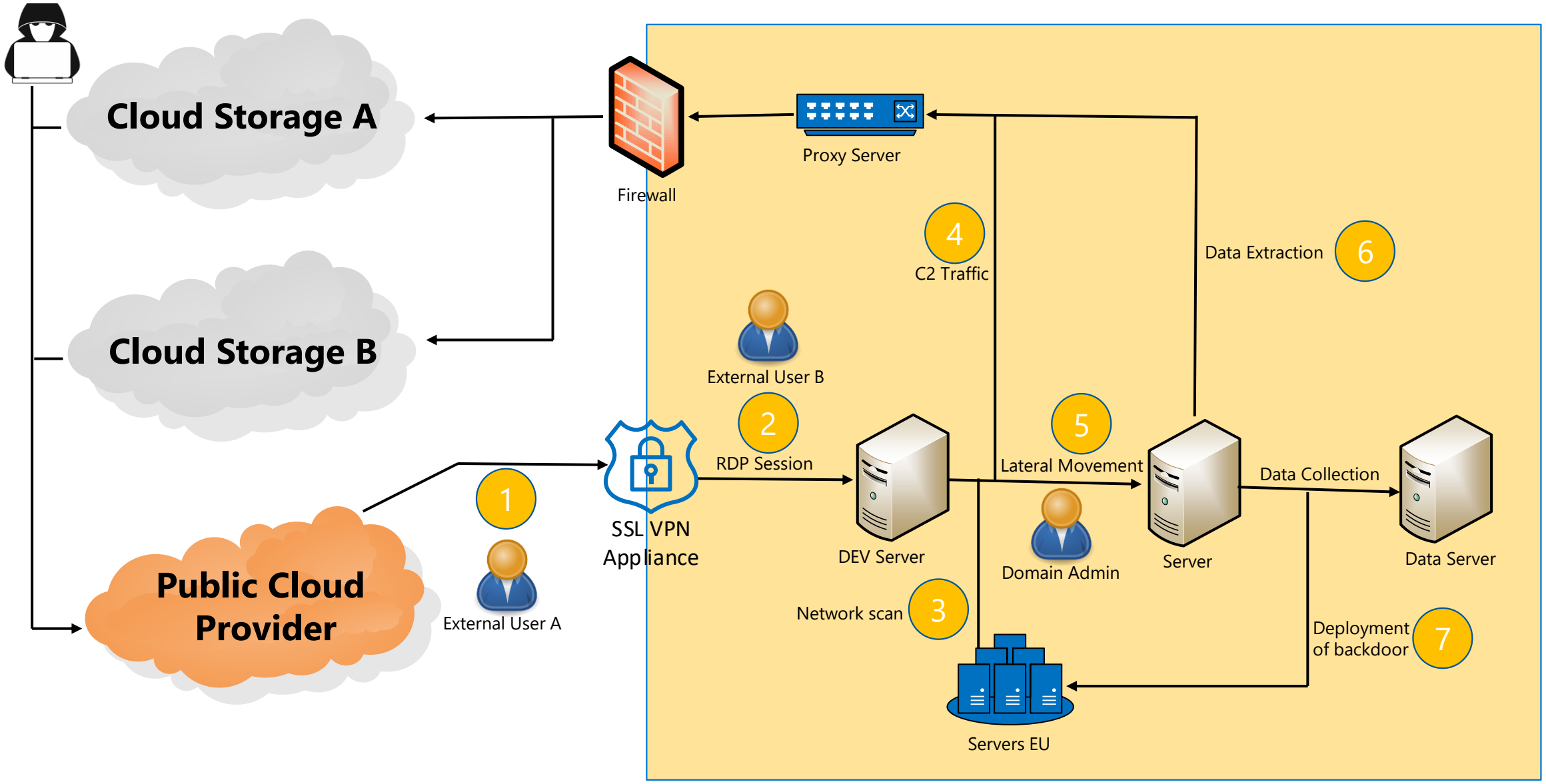


Cyberangriff Marke Griesser



Wie lief der Hack technisch ab?

Cyberattack Griesser



Kommunikation mit den Hackern

Kommunikationsverlauf

Hacker platzierte Kommunikations-Datei auf allen Server

README.txt

```
All of your files are currently encrypted by CONTI strain.

As you know (if you don't - just "google it"), all of the data that has been encrypted by our
software cannot be recovered by any means without contacting our team directly.
If you try to use any additional recovery software - the files might be damaged, so if you are
willing to try - try it on the data of the lowest value.

To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files
completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://contirecj4[redacted]/

HTTPS VERSION :
https://contirecovery.icu/

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are
ready to publish it on out news website if you do not respond. So it will be better for both
sides if you contact us as soon as possible.


---BEGIN ID---
SWk0YMC0ji4u[redacted]
---END ID---
```

Techniker

CIO

Cybersecurity Versicherung

Hallo, es sieht so aus, als hätten Sie unsere Umgebung verschlüsselt. Was sind die nächsten Schritte?

Guten Tag, wir lassen es Ihnen so schnell wie möglich wissen.

Wie sie ja Wissen haben wir (CONTI Team), ihre Daten verschlüsselt. Wir haben grosse Mengen von internen Daten heruntergeladen. Sollten Sie nicht auf unsere Forderungen eingehen, dann werden diese Daten veröffentlicht. Der Preis dafür beträgt $ XY in Bitcoin.

Wenn wir zu einer Einigung kommen, geben wir Ihnen die Daten zurück und erteilen Ihnen einige Security Vorschläge, um zukünftige Hacks zu verhindern.

.

Wir sind über die höhe des Geldbetrages überrascht, da normalweise in solchen Fällen einen kleinen Prozentsatz des Umsatzes verlangt wird.

Wir sind nicht am Umsatz Ihrer Firma interessiert, sondern am Wert der Daten. Wenn wir diese Woche eine Einigung erzielen könnten, gewähren wir Ihnen einen Rabatt.

Danke, können Sie uns einen Beweis geben ob sie die Daten wirklich haben?

Gerne senden wir Ihnen eine Datei zur Überprüfung.

Lessons learned

Technisch:

Operativ:

Prozess:

Technisch:

- Aktivierung MFA für alle
- Keine Internetzugriffsrechte für die Admins
- O365 Dienste waren nicht betroffen
- Virenscanner hatte nicht reagiert!
- Offline Backup unvollständig

Operativ:

- Priorisierung Security Themen (Reactive Operation)
- Einführung CISO@a Service
- Regelmässige Pentesting von extern durchführen
- Sich challengen lassen und reflektieren
- Positives aus dieser Erfahrung extrahieren
- Disaster Recovery Tests haben gefruchtet
- Backup Konzept / Backup Recovery Tests

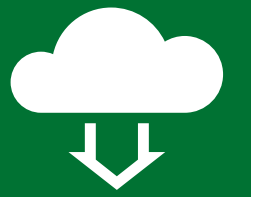
Prozess:

- Interne/externe Kommunikation sehr wichtig (Transparenz)
- Notfallpläne erarbeiten/regelmässig testen
- Cyberversicherung war sinnvoll (Fachleute umgehend am Tisch)
- Einführung eines SOC (Security Operations Center)

Summary

ZERO Trust - You're responsible for your data, verify and secure everything and audit your environment continuously

60% of data are stolen in just a few hours and 33% of organizations take 2+ years to discover a breach



Security awareness is a important risk-reduction strategy but does not replace new security technologies

Behind every stupid user is a stupider security professional - Ensure a clear Governance and control with automated processes

Culture is the best awareness tool, focus on People and process and technology is the natural outcome

Let’s have a 15min break

Roundtable and Q/A starts at 14:45

Bitte geben Sie Feedback zum Roundtable

References

- NIST Zero Trust - https://csrc.nist.gov/publications/detail/sp/800-207/draft
- Microsoft
  - MWT313W Integration Workshop: Zero Trust and the Modern SOC https://myready.microsoft.com/sessions/details/MWT313W?catalogMode=ondemand
  - https://myready.microsoft.com/winter2020/page/DownloadDocument?documentid=21d10e17-26b4-43c5-8729-0013296c7d04
  - https://www.microsoft.com/security/blog/2018/08/30/building-the-security-operations-center-of-tomorrow-harnessing-the-law-of-data-gravity/
  - Microsoft Zero Trust Maturity Model
  - Zero Trust web page
  - Microsoft Security blog post
  - CISO Zero Trust workshop series
  - Zero Trust e-book
  - 10 tips for enabling Zero Trust security
  - Securing privileged access overview | Microsoft Docs
  - Azure Active Directory security operations guide | Microsoft Docs

Microsoft

Thank you

The following slides contain preliminary information that may be changed substantially prior to final commercial release of the software described herein. The information contained represents the current view of Microsoft Corporation on the issues discussed as of the date of the presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of the presentation.

This presentation is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THE ROADMAP PORTION OF THIS PRESENTATION.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this presentation. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this information does not give you any license to these patents, trademarks, copyrights, or other intellectual property.