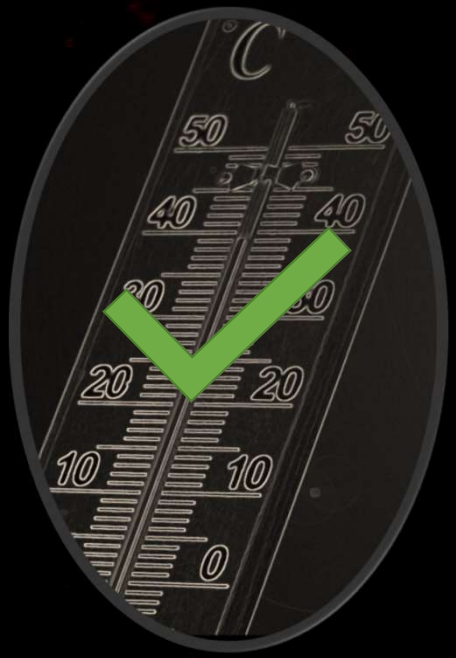
Mayday aus dem SOC

Ein Cybercrime Vorfall – wenn der Ernstfall eintritt! –

Geschichten aus dem Antares SOC und
der Incident Response Group Austria (IRGA) – www.irga.at

DI Alexander Graf | CEO
Antares Netlogix Netzwerkberatung GmbH

Klassische Szenarios



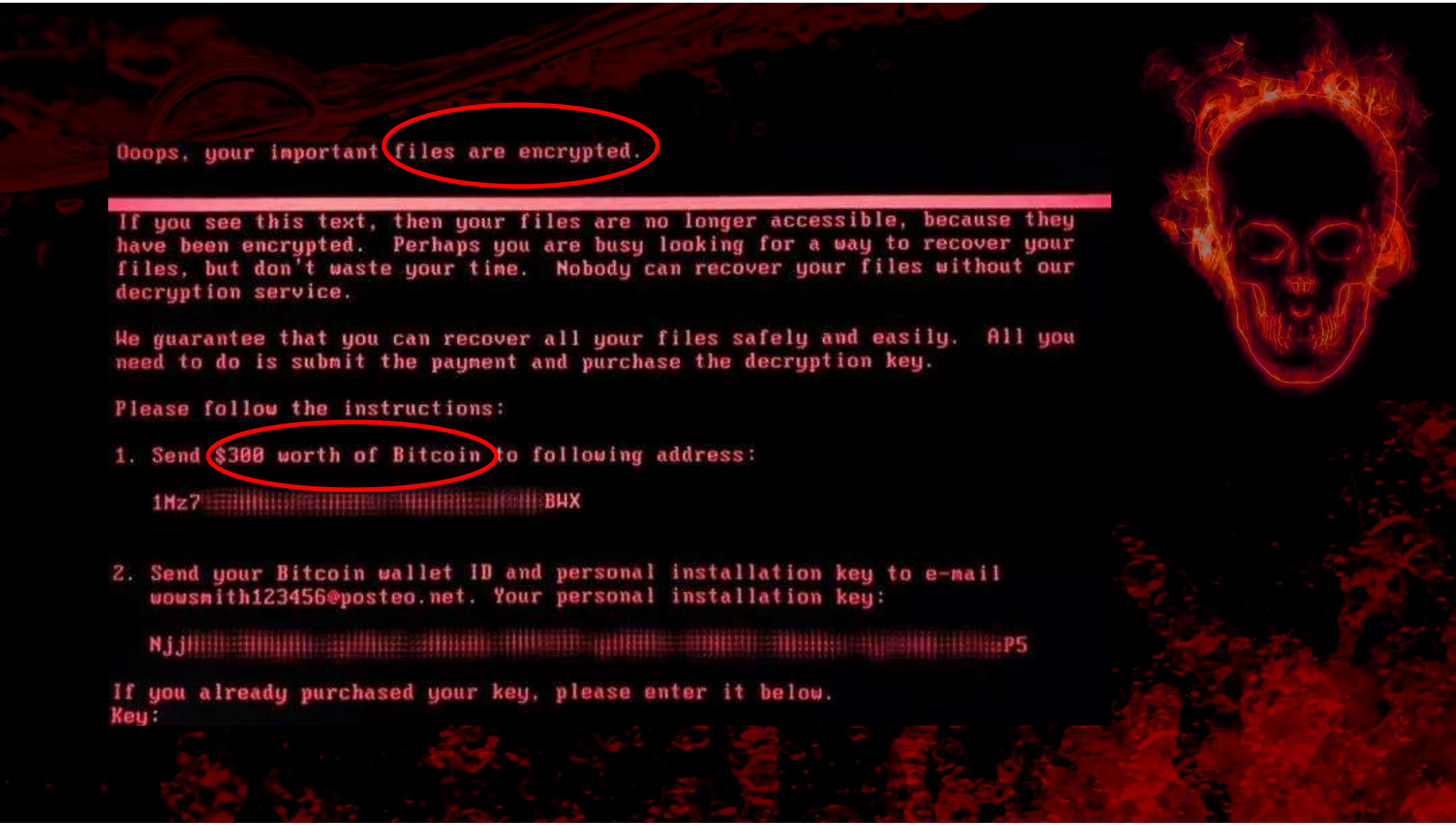
Datacenter
Strom/Klima

Feuer

Flut

Blackout


… und im Fall einer Cyber Attacke?
Mayday = Emergency Operations


Ooops, your important files are encrypted.
If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.
We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1. Send $300 worth of Bitcoin to following address:
1Mz7 BWX
2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:
Njj P5
If you already purchased your key, please enter it below.
Key:

Wie werde ich die Angreifer wieder los?

(IT) Rollen

Internet „abdrehen“?

Forensik

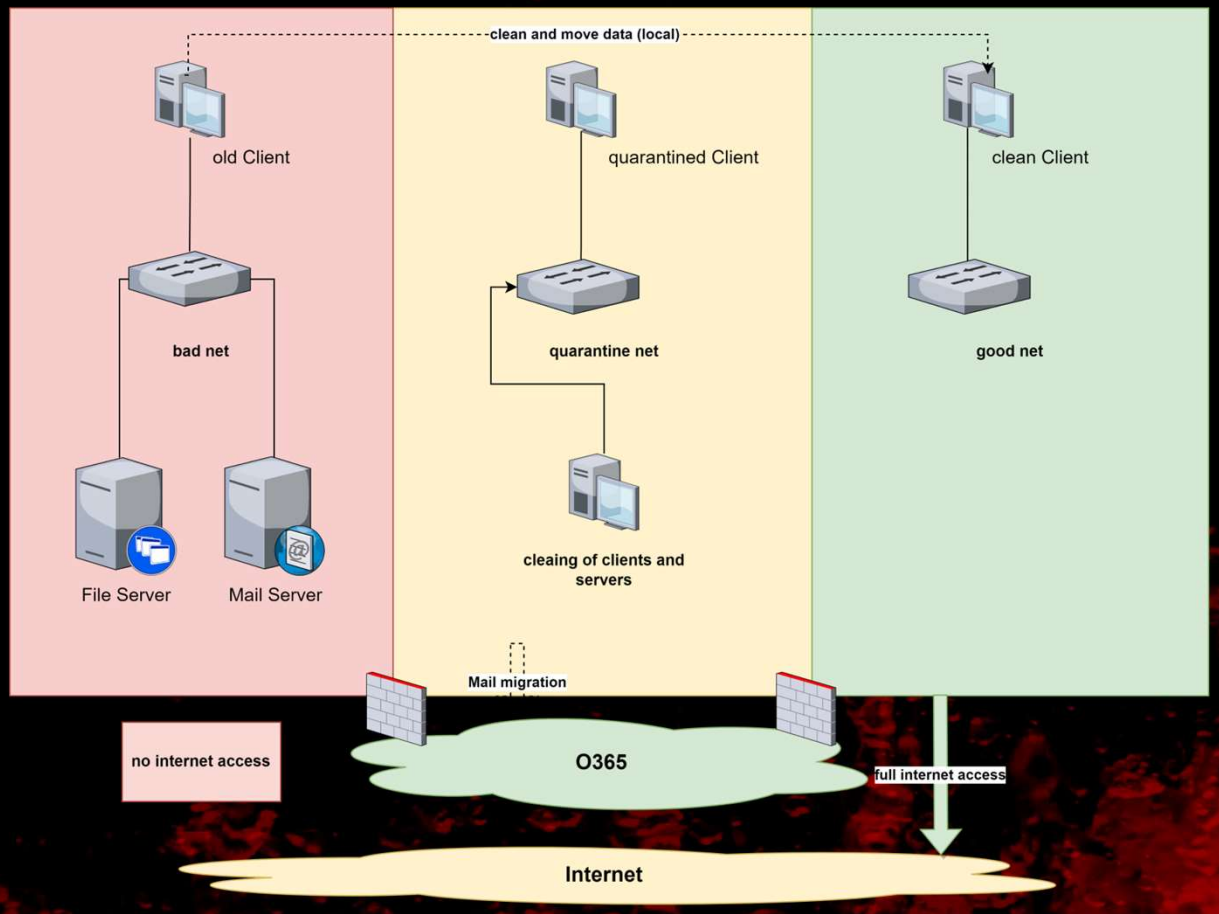
IT Infrastruktur Wiederherstellung

Business Continuity Management

Finanz	**Löhne, Steuern, Rechnungen, …**
Produktion	**Wartungsarbeiten, Reinigungsarbeiten, Ersatzteilversorgung, …**
HR	**Manuelle Zeiterfassung Mitarbeiter in Urlaub/Zeitausgleich?**
Logistik	**Lagerlogistik, Lieferscheine, Ersatzteile,…**

Recovery Team

Goodnet/Badnet Concept



Notfall Budget

Wer verhandelt mit den Erpressern?

Wie erreiche ich meine Mitarbeiter/Kunden?

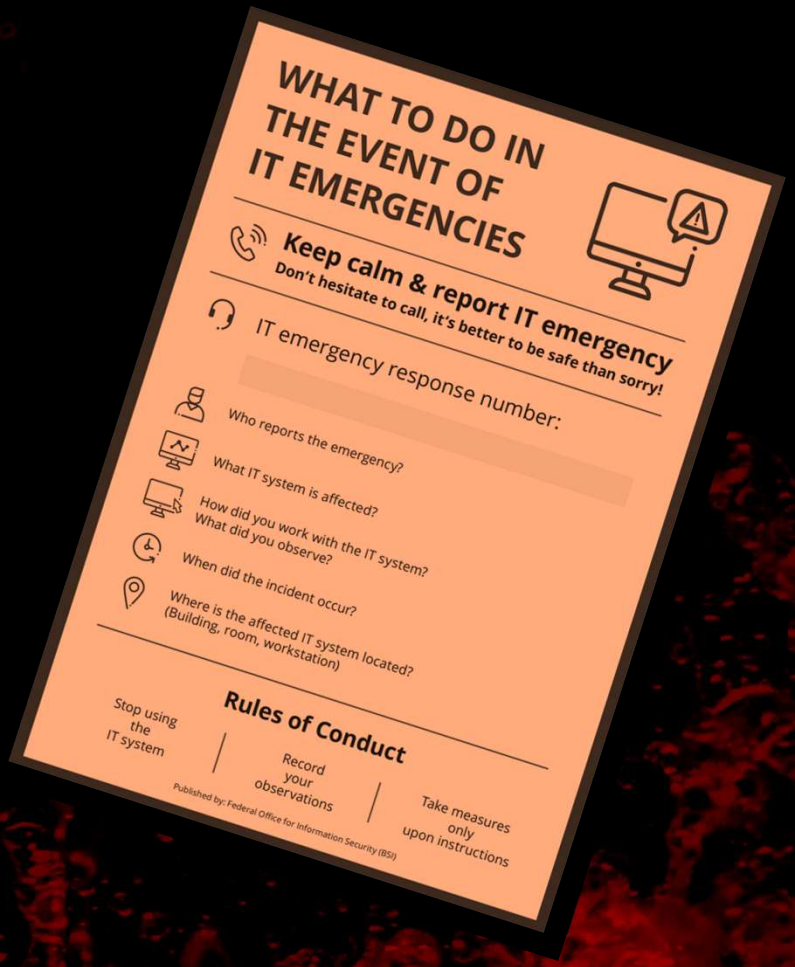
IT Notfallhandbuch

Rollen

Prozesse

Beispiel

- **Fehler in der Produktionssteuerung**
- **Info von der Fachabteilung**
- **Abarbeitung laut Notfallhandbuch**
- **Ransomware wurde erkannt**
- **Notfall wird ausgerufen**



Strategie

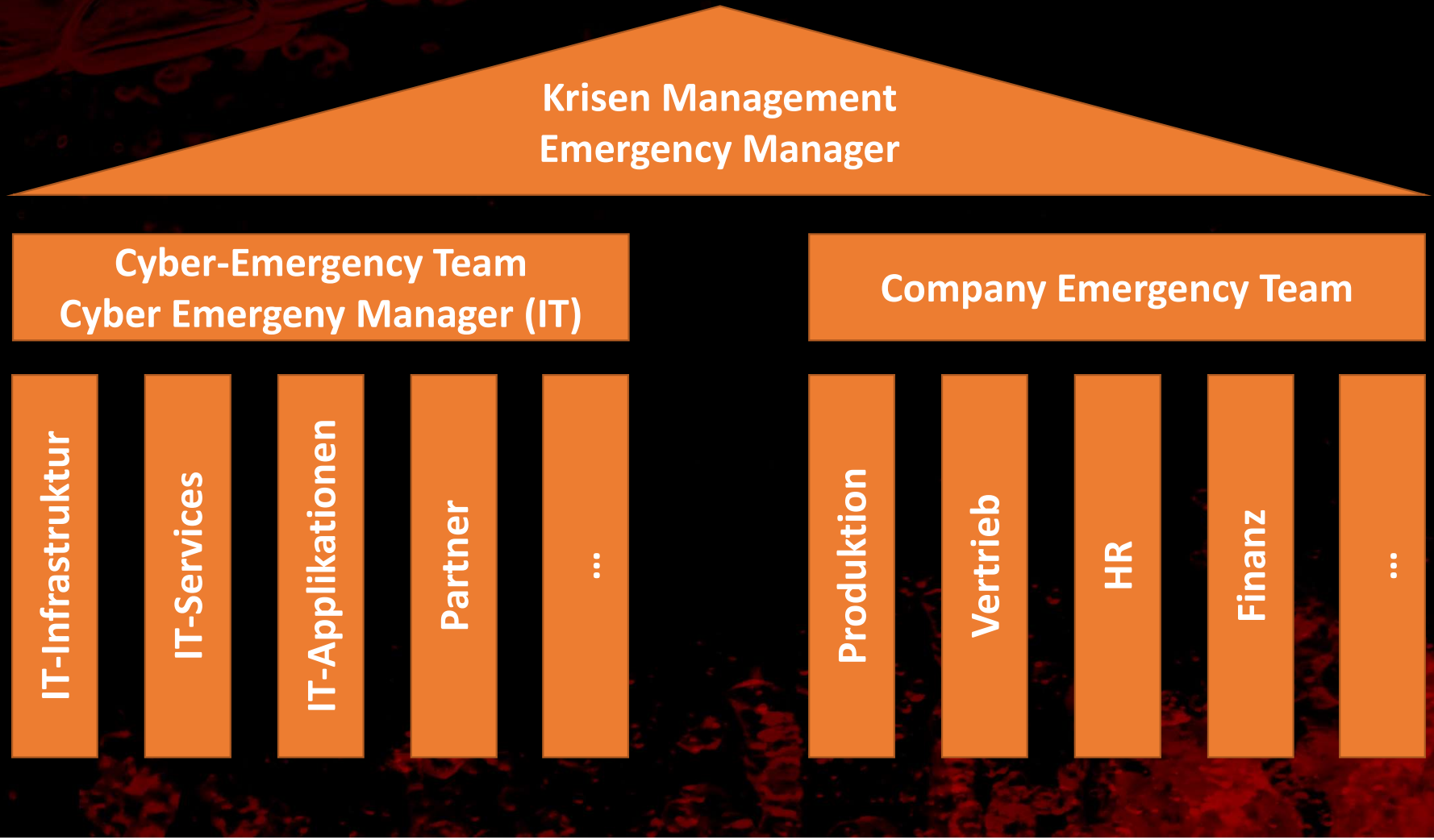
- **Zugeben oder abstreiten?**
- **Wer macht die Pressearbeit?**
- **Verhandeln wir mit den Erpressern?**
- **Zahlen wir zur Not Lösegeld?**
- **Erfahrung mit Kryptowährungen vorhanden?**
- **Cyber Versicherung?**
- **Notfall Budget?**

Notfallplan (Beispiel)

- Alarmierung des Notfallteams
- IT: Identifikation -> Eindämmung (Playbook)
- Interne Kommunikation
- Produktion, Maschinen in sicheren Zustand bringen
- IT: Ransomware entfernen (Playbook)
- PR
- IT: Wiederherstellung (Playbook)
- Lessons Learned

Maßnahmen abhängig von der Strategie!

Notfall Organisation



Durchbrechen der Cyber Kill Chain – aber wie?

Z.B. mit IAM

Cyber Kill Chain

- ablaufbezogene Sicht eines Angriffs
- mit festen aufeinander folgenden Abschnitten für einen erfolgreichen Angriff

- Aber
  - Der oder die Angreifer (aber vielleicht auch der Pentester) „puzzeln“ sich quasi von einer Chance zur nächsten an ihr Ziel.
  - Das MITRE ATT&CK Mapping berücksichtigt diese Tatsache.

Mitre ATT@CK Matrix – 14 Taktiken

• Reconnaissance	- Daten/Informationen sammeln
• Ressourcenentwicklung	- Tool Installation
• Erstzugang	- Eintritt in die Infrastruktur
• Ausführung	- Code Ausführung
• Persistenz	- Tarnen und warten
• Erweiterung der Zugriffsrechte	- Rechte erhöhen
• Umgehung – Schutzmaßnahmen	- Tarnen und täuschen

Mitre ATT@CK Matrix – 14 Taktiken

• Anmeldedatenzugriff	- Accounts stehlen
• Erkundung	- Umgebung analysieren
• Laterale Bewegungen	- Bewegung in der IT
• Erfassung	- Daten sammeln
• Command and Control	- Kontrollübernahme
• Exfiltration	- Abzug der Daten
• Folgen für die Firma	- Epressung (Geld, Image, …)

Wieso ist IAM wichtig für Ihr Unternehmen?

Der frühere FBI-Direktor Robert Mueller hat es auf den Punkt gebracht:

- „I am convinced that there are two types of companies:
- **Those that have been hacked and those that will be.”**

Übertreibt Mueller?

Keineswegs, wenn man sich die Zahlen aus Deutschland ansieht:

So hat eine Umfrage unter deutschen Unternehmen ergeben, dass in 2021 Cyberangriffe bei fast 9 von 10 Unternehmen Schäden verursacht haben – Schäden, die sich auf horrende 223,3 Milliarden EUR beliefen.

WAS BEDEUTET IDENTITY & ACCESS MANAGEMENT (IAM)?

- IAM gehört zu den Bereichen IT-Sicherheit und Datenmanagement.
- Es ist der Schlüssel dazu, dass nur die richtigen Personen in Ihrem Unternehmen Zugriffe (Access) auf benötigte technische Ressourcen haben (Zugriffsberechtigungen).
- Dabei sind nicht nur Ihr eigenes Personalmanagement und die IT Partner sondern auch das Customer Identity Management zu berücksichtigen.

WAS BEDEUTET IDENTITY & ACCESS MANAGEMENT (IAM)?

- Ziel von IAM ist es, Ihre Daten von beiden Seiten zu schützen.
- IAM sorgt dafür, dass Unternehmen Berechtigungen und Benutzer in sämtlichen Systemen und Anwendungen zentral managen können.
- Wesentlich hierfür ist eine automatisierte Benutzerverwaltung und eine Standardisierung von Prozessen und Workflows.

Bequemlichkeit – des hauma glei!

- Ihre Mitarbeiter sollen so schnell wie möglich ihrer Arbeit nachgehen können.
- Wenn sie eine Berechtigung oder einen Zugang benötigen, werden Anfragen oft möglichst schnell abgearbeitet, ohne eine Kontrollinstanz zu befragen.

Historie – Culture eats strategy for breakfast!

- Gefestigte Prozesse sind oft nur schwierig aufzubrechen.
- Wenn Accounts und Berechtigungen „schon immer“ in den Zuständigkeitsbereich der IT gefallen sind, ist eine Änderung ein anstrengender Prozess, vor dem viele zurückschrecken werden.

Komplexität von IT/ Schatten IT

- Oftmals fehlt eine ausreichende Dokumentation in der eigenen IT-Abteilung.
- Accounts werden lieber nicht gelöscht, da nicht ganz sicher ist, ob diese noch benötigt werden.

Fehlende Ressourcen

- Wie hoch wird Identity Management in Ihrem Unternehmen priorisiert?
- Oft bereits auf der Roadmap
- Die Einführung entsprechender Prozesse wird immer wieder vertagt.

Falsche Sicherheit

- Es ist oft ein Fehlschluss zu denken, das eigene Unternehmen sei schon sicher genug.
- Oder zu klein für einen Angriff.
- Oder dass wirklich bekannt ist, wer welche Zugänge besitzt.

Hoher Administrativer Aufwand

- Auch wenn Ihr Unternehmen diese Schwachstellen nicht besitzt, kann eine manuelle Identitätsverwaltung ohne Governance trotzdem Schwachstellen aufzeigen.
- Nehmen wir an, eine Zurückverfolgung wird notwendig:
- Hat ein Personalchef die Verantwortung für Zugänge ausschließlich der IT-Abteilung übertragen, entsteht ein hoher administrativer Aufwand.

Wie gut fuktioniert EVA bei Ihnen?

Business Continuity Management mit IAM

Goodnet

- Automatisierte Ausbringung der Rechte in der Goodnet Instruktur via IAM Workflows
  - Abteilungsressourcen
  - Projektressourcen
- Der Workflow dokumentiert den Prozess!

WIR UNTERSTÜTZEN UNTERNEHMEN

SECURITY

Individuelle Konzepte & Lösungen!

SICHERHEIT

INFRASTRUKTUR

Optimierung & Steigerung der Verfügbarkeit!

NETZWERKE

BCM

Vom Notfallhand-buch bis zum Wiederanlauf!

NOTFÄLLE

COMPLIANCE

Tools & IT-Prozesse sind unsere Leidenschaft!

DATENSCHUTZ

NIS-2 | EU-DSGVO | ISO 27001 | PCI DSS


ANTARES NETLOGIX
www.netlogix.at
Fragen?
tenfold
Partner