NetUSE AG

Cyberkriminelle vs. User

Welches Rüstzeug brauche ich als Unternehmen

1. Forum Wirtschaftsschutz SH 30.8.2023

Agenda

- Motivation von Cyberkriminellen
- Ein paar Worte zum Microsoft Key-Loss/Hack
- Cybersecurity im Unternehmen
- Angriffsvektoren – Einstiegspunkte
- Ablauf eines Angriffs
- Die Versicherung: Backup

Motivation von Cyberkriminellen

1. **Organisierte Cyberkriminalität**
   ➡ **Geld**

2. **Politisch motivierte Cyberkriminelle**
   ➡ **Aufmerksamkeit, Desinformation etc.**
3. **Staatliche Angreifer**
   ➡ **Spionage, Sabotage, politischer Einfluss**
4. **Einzeltäter & Trittbrettfahrer**
   ➡ **meistens Geld**

Microsoft Key Loss – Cloud Hack

- **Angriff durch „Storm-0588“**
- **mutmaßliche staatlich gestützte chinesische Hackergruppe**

Empfehlungen:

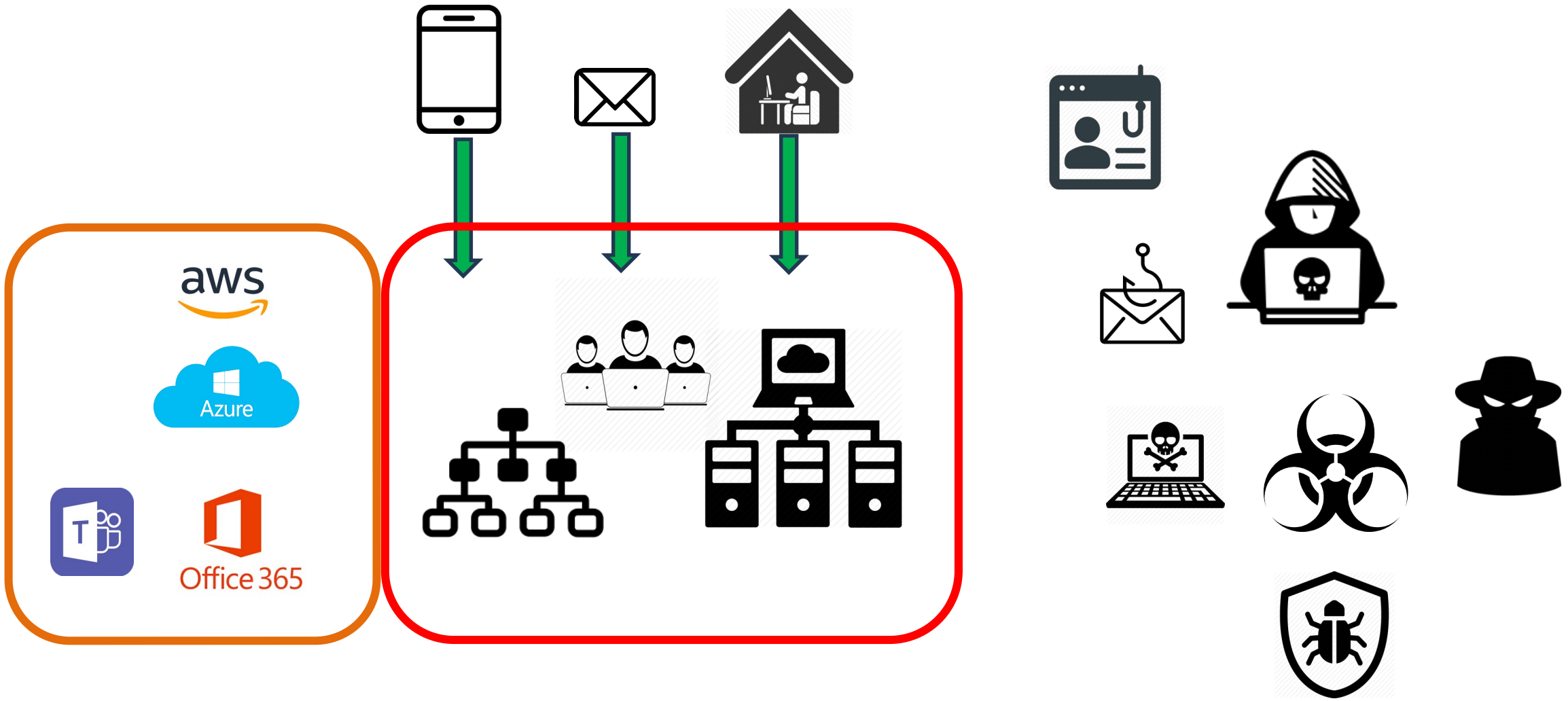
- **Zusätzliche 3.rd Party Cloud Security Lösungen einsetzen.**
- **Azure Security tiefer beschäftigen**

Cybersecurity im Unternehmen

Verantwortlich: Geschäftsführer / Vorstand

Cybersecurity muss „von oben gelebt werden“

- Offenes Mindset
- Vertrauensvolles Klima
- Awareness – Schulungen und Übungen
- Budget


aws
Azure
Office 365

Einstiegspunkte für Angriffe

1. **Email**

2. **Exponierte Intranet-Systeme (z.B. Exchange, Sharepoint, NAS)**
3. **Verlust von bzw. kompromittierte Zugangsdaten**
4. **Schlecht gesicherte Endgeräte**
5. **Spätes Patchen**

Im Kommen: Mangelhaft gesicherte Cloud-Ressourcen

Email

- Anti-Spam
- Anti-Phishing
- Awareness – ChatGPT/generative KI's sind ein Problem
- Firewall – Anti Bot Gateway auch für Mobile & PC/MAC
- Attachments: Emulation, Konvertierung, Block by Type
- Microsoft Office 365 – Teams – Exchange Online
  => zusätzliche Security Lösung (!= Microsoft)

Exponierte Intranet-Systeme

- **Exchange o.ä. (auch Open Source)**
- **Sharepoint**
- **NAS**
- **Wiki, Intranet-Portale**
- **…**

Gehören hinter eine Firewall und nur per VPN erreichbar!

Ein KMU kann diese nicht "sicher" betreiben (lassen)!

Exponierte Intranet-Systeme

Beispiel:

- **Externer IT-Dienstleister betreut KMU Exchange**
- **Annahme: DL hat 1 Admin für 50 Kunden**
- **Exchange Patch steht an, z.B. 2 Stunden Arbeitszeit**

- **1 Admin – 40 Stundenwoche**
- **50 Systeme = 100 Stunden Arbeit**
- **Das "letzte" System ist nach 2,5 Wochen dran.**

Ups.....

Verlust von Zugangsdaten

Credo: Jeder Zugriff aus dem Internet auf Unternehmens-informationen und Anwendungen muss mit 2FA/MFA gesichert sein!

- Passwordmanager
- Kein Password-Reuse
- Nur vertrauensvolle Endgeräte verwenden
- Trennung Privat – Dienst

Ungesicherte Endgeräte

Mobiles Arbeiten → Höhere Sicherheit auf Endgeräten notwendig.

- **PC / Notebook / MAC**
- **Datenträger verschlüsselt?**

- **Smartphone ?**
- **Tablet ?**

Spätes Patchen

Wieviel "Zeit" haben sie, nach dem der Hersteller / Anbieter den Patch veröffentlicht hat?

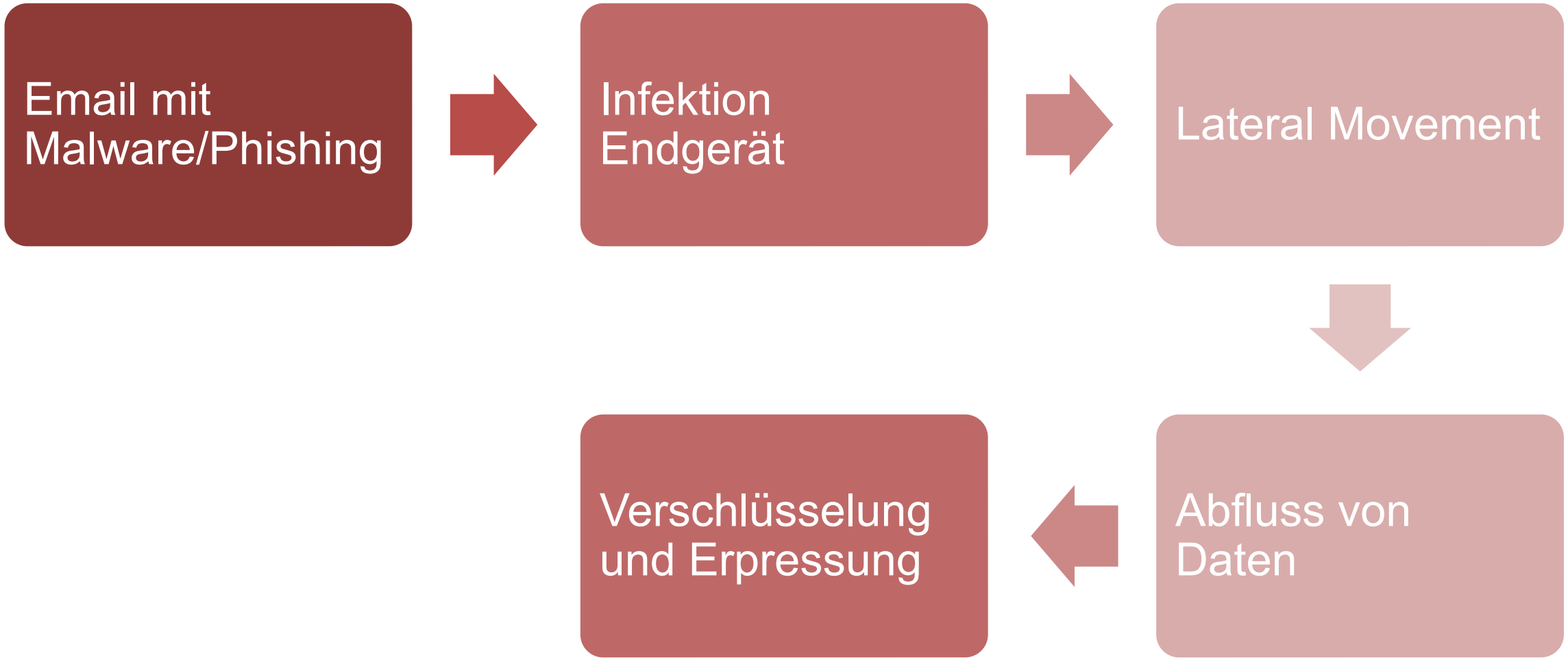
A. **Stunden?**
B. **Tage?**
C. **Wochen?**
D. **Einen Monat?**
E. **Länger?**

Spätes Patchen

Wieviel "Zeit" haben sie, nach dem der Hersteller / Anbieter den Patch veröffentlicht hat?

A. Stunden
B. Tage
C. Wochen
D. Einen Monat
E. Länger

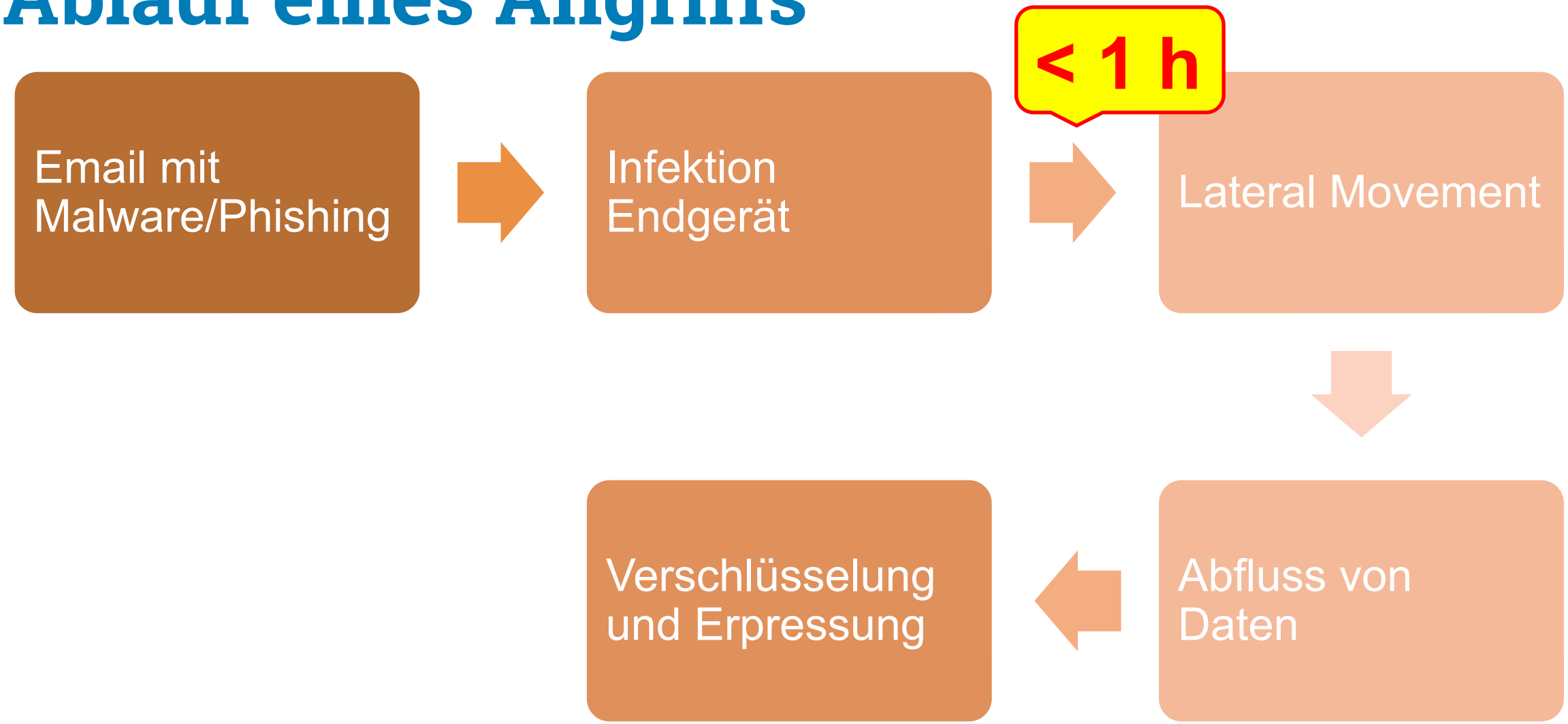
Ablauf eines Angriffs



Ausbreitung - "Lateral Movement"

Wann beginnt im Mittel die Ausbreitung eines Hackers im Netz?

Ablauf eines Angriffs



Was begünstigt "Lateral Movement"?

1. **Fehlende Patches (Spätes Patchen)**
2. Normale Useraccounts mit administrativen Rechten
3. Schlechte Konfiguration (u.a. AD)
4. Keine Netzsegmentierung
5. Kein MFA für privilegierte Accounts
6. Keine zusätzliche Sensorik im Netzwerk (IPS)
7. Detect statt Prevent in der Policy
8. Firewall-Policy zu lasch
9. Späte Reaktion

Die Versicherung: Backup

1. Restore regelmäßig Testen
2. Speicherdauer ?
3. Cloud nach "on premise" Backup
4. Tape (!) - Offsite Backup

Orientierungshilfe

- Wie sicher ist mein Unternehmen?
- Testen lassen?
- „Brand“-Übungen machen?

- Technische Sicherheit vs. Organisatorische Sicherheit?

- BSI Grundschutz ?
- ISO 27001 ff

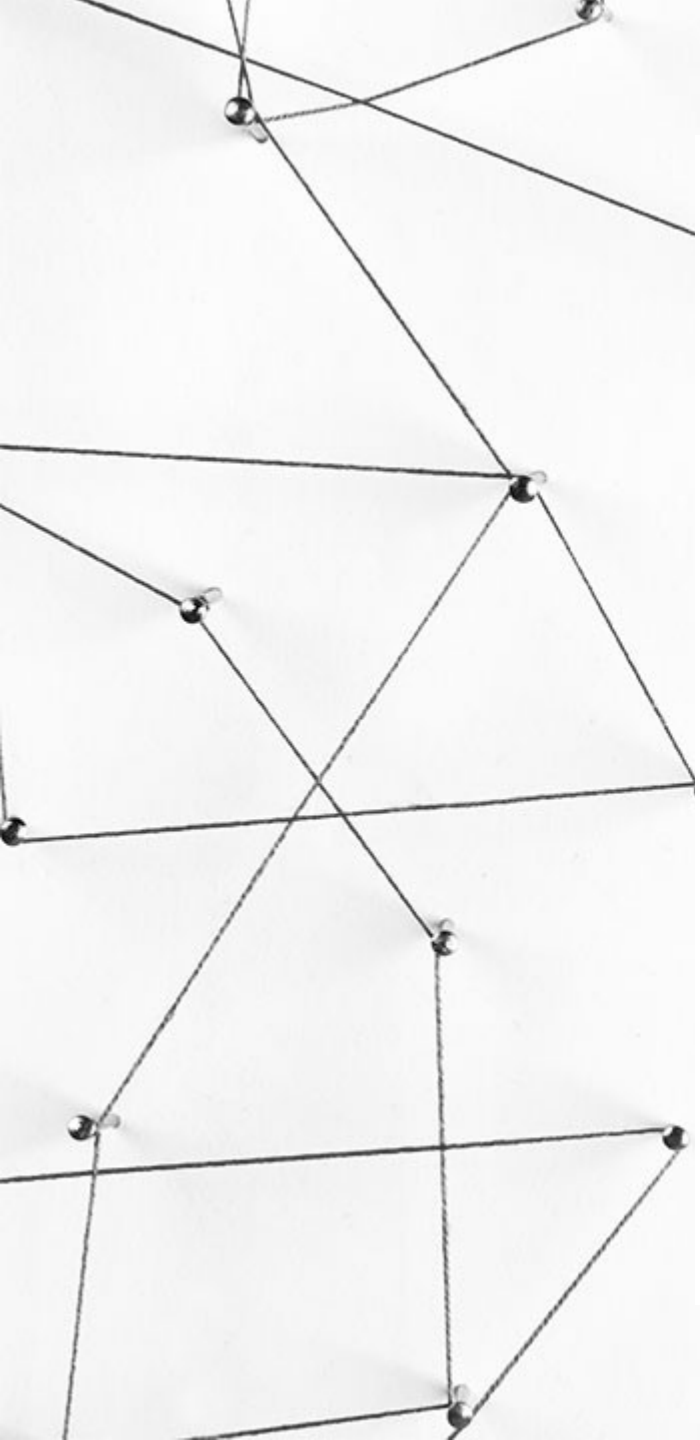
Orientierungshilfe

Jährlich Kosten für Cybersecurity-Lösungen (Software, Lizenzen, Hardware) ohne Personalkosten/Dienstleistungen

< **400** EUR je Mitarbeiter (Kopf, nicht FTE)

Þ **Vermutlich liegt da was im Argen**

MSP: Kosten sind höher, da dort Personalkosten des DL enthalten sind.



Fragen?