b. Validierung

c. Beispiele von Techniken, Technologien, Lösungen

- Backup - aber richtig
- Lücken minimieren - Security Updates
- Ins Netz gehen - der Router und nicht nur
- Vertraulichkeit mit Verschlüsselung
- Vertraulichkeit über öffentliche Netze => VPN
- Heterogenität und Isolation
- Analyse und Überwachung
- Problem: Trusted Computing!

3. Allgemeine Empfehlungen zur Vorgehensweise, Strategien

a. Konzepte

b. Technische Zuverlässigkeit

c. Prinzip *keep it simple*

d. Softwaremodelle: *open source* vs. *closed source*

e. Absicherung vs. Resilienz

H. Übungsszenarien

1. Szenario 1: Erschwindelte Überweisung

Das Unternehmen K in Oberfranken produziert Kompressoren. Das Besondere an den Produkten ist ihre zentrale Steuerung über IP-Netze, die mit den eingebauten Sensoren besonders effizient zusammenarbeitet. Chinesische Hersteller können technisch vergleichbare Systeme günstiger anbieten. Die cloudbasierte Steuerung über IP-Netze ist aber eine Besonderheit, bei der K einen beachtlichen Wettbewerbsvorsprung besitzt. Die Kundenserver sind - dank Verbindungen zur Cloud von K - für Kunden wartungsfrei (automatische Updates etc.), Geräte laufen länger, effizienter und Störungen sind seltener.

Um einen Geschäftsabschluss zu einem Projekt im Nahen Osten vorzubereiten, reist die Unternehmensleitung, insbesondere die beiden Geschäftsführer G und H, nach Dubai. Einer der teilnehmenden Mitarbeiter M postet privat auf Instagram Bilder und Informationen über die Reise, twittert auch in Absprache mit der PR-Abteilung einige Hintergründe der erfolgreichen Reise.

Darauf hin - am zweiten Tag der Reise - erhält die Assistentin A der Geschäftsführung eine E-Mail mit der Information der durch die Geschäftsleitung genutzten Fluglinie, dass der Rückflug womöglich nicht wie geplant stattfinden kann. Die A folgt dem Link in der Nachricht, der sie zu einer Webseite der Fluglinie lotst, allerdings scheinen die meisten Funktionen der Webseite nicht korrekt zu funktionieren. Per Telefon kann die A direkt mit der Fluggesellschaft klären, dass es sich wahrscheinlich um einen Irrtum handelt.

Am Folgetag erhält A eine weitere Nachricht - diesmal von einem der Geschäftsführer G - dass die Zahlung der Kosten für Hotelübernachtungen sowie regionale Reisen von Dubai aus zum Kunden nicht mit Kreditkarten beglichen werden konnten. Er bittet um eine Blitzüberweisung auf ein von ihm genanntes Konto des angeblichen Reiseveranstalters vor Ort. Da A sich noch eine Bestätigung von Mitarbeitern des Rechnungswesens holen will, wird sie darauf aufmerksam gemacht, dass womöglich etwas nicht stimmt. Als sie ungeduldig auf einen Rückruf des G wartet (weil dieser vorerst nicht erreichbar ist) erhält sie von der Nummer seines Mobiltelefon einen Anruf. Die Sprachqualität ist zwar sehr schlecht, aber A versteht, dass sie eine schnelle Überweisung tätigen soll. Im Nachgang erhält A eine weitere Bestätigung per E-Mail von G, in der sie auch auf die Dringlichkeit der Angelegenheit im schroffen Ton zum unverzüglichen Handeln aufgefordert wird. Da die Mitarbeiterin aus dem Rechnungswesen den G auch nicht erreichen kann, entscheiden beide, die geforderten 23.314,- EUR in Landeswährung zu überweisen.

Während sich die Delegation auf Rückreise befindet, meldet G der A, dass die SIM-Karte seines Telefons nicht funktioniert und bittet um Bestellung einer neuen. Im Kontakt mit dem Mobilfunkanbieter stellt sich heraus, dass eine e-SIM gerade neu aktiviert wurde. A meldet den Vorfall dem G und fragt zugleich, ob die Überweisung helfen konnte. G bestreitet, die Überweisung verlangt zu haben. Es stellt sich heraus, dass das Unternehmen Opfer eines Betruges geworden ist. Die ersten Erkenntnisse deuten darauf hin, dass die von A besuchte Webseite der Fluggesellschaft ein Fake war, ebenso, wie die Nachricht, der A folgte. Auf der Webseite konnte die Möglichkeit identifiziert werden, Schadsoftware herunterzuladen.

Der vom Rechner der A installierte Trojaner hat die Netzwerkfreigaben in K infiziert, durchsucht, weitere Systeme infiziert und ca. 8 GB an Daten an ein Botnetz gesendet. Die Mitarbeiter von K stellen fest, dass zumindest theoretisch auch die Rechner des Cloud-Systems zur Versorgung der Kundenserver infiltriert sein könnten.

Wie sollte der Zwischenfall aufgearbeitet werden?

2. Szenario 2: Ransomware-Angriff

A ist Inhaber eines erfolgreichen Architekturbüros, das er in Form einer GmbH (A-GmbH) betreibt. Als A zur Baustelle eines Kunden verreist, meldet sich seine Assistentin B am Nachmittag des 18. 9. (Freitag) mit der Frage, ob A Wartungsarbeiten an der IT-Infrastruktur angeordnet hat, weil die Systeme nicht richtig arbeiten würden. A bittet B, mit dem betreuenden EDV-Unternehmen E Kontakt aufzunehmen und es mit diesem zu klären.

Nach kurzem Einsatz eines Mitarbeiters von E kann B weiter arbeiten.

Am Montag, 21. 9., melden weitere Mitarbeiter der A-GmbH Probleme mit ihren Arbeitsrechnern. Die Programme, die auf interne Netzwerkressourcen zugreifen (Dateiserver), funktionieren nicht. Als A an seinem Arbeitsplatz ankommt, kann er seinen Rechner zwar starten, aber auf dem Desktop befinden sich gar nicht die gewohnten Symbole, sondern Dateien mit unbekannten Namenserweiterungen (Endungen), wie ".odveta" oder ".Lazarus+" und vielen weiteren Zeichen. Überall sind kleine Textdateien mit (unter anderem) folgendem Inhalt gespeichert:

```
Your Files Have Been Encrypted (...)
   (…) Send us following ID: qTCkjsdl+= (...)
Attention: Using 3rd Party Applications or Recovery Tools May
```