Attracting Tomorrow

TDK

Die (Un-)Sicherheit der industriellen IT

Paul Blenderman, Manager Servers & Infrastructure

TDK-Micronas GmbH
Magnetic Sensors Business Group

IT Operations
Freiburg, Germany
10.06.2023

TDK-Micronas

Halbleiter: Magnetische Sensoren, Motorregelungen

Wir machen den gesamten Prozess selbst: von Entwicklung bis Versand.

Seit 1952. Hauptsitz in Freiburg.
Seit 2016 Teil des TDK-Konzerns.
Etwa 1000 Mitarbeiter.

Eigene Waferfab.

Industrie 4.0 als es den Begriff noch gar nicht gab

Halbleiterherstellung hat sehr früh mit Vernetzung der Produktion und Anbindung an zentraler IT angefangen.

MES/Automation/usw. in den 90ern gestartet - damals war die Sicherheit noch nicht das große Thema.

Micronas hat an die 2000 "Dinge" in der Produktion am Netz.

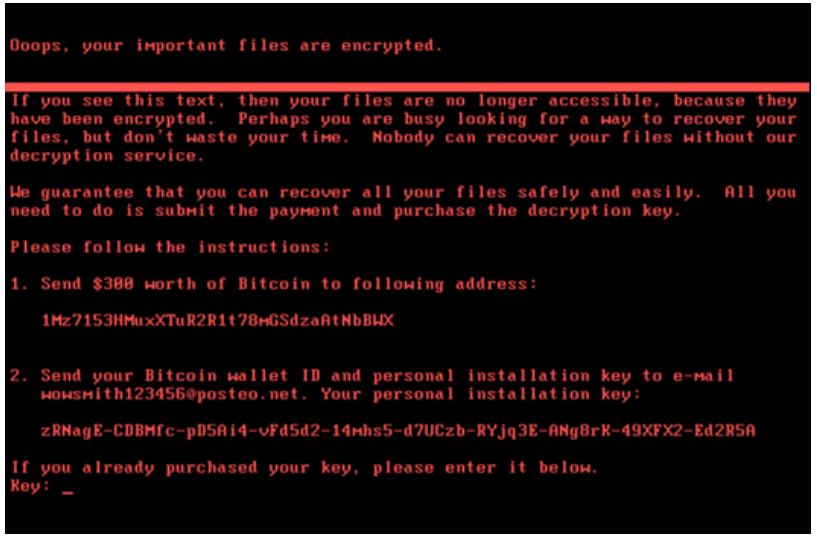
Und dann kamen WannaCry und NotPetya

2017 ist jetzt 6 Jahre her.

Erst WannaCry – griff Verwundbarkeit in Windows an.

Dann NotPetya –
griff zusätzlich **Verwundbarkeit in typischen Netzwerkkonfigurationen** an.

Startschuss für ganz viele Verbesserungen im IT-Sicherheitsbereich…

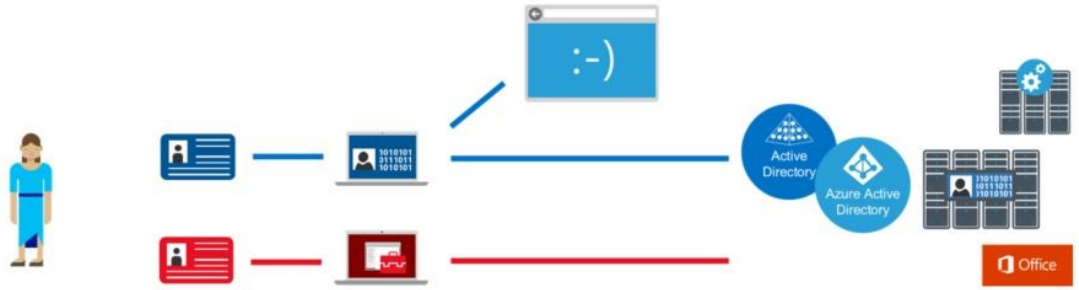


Maßnahmen auf allen Ebenen…

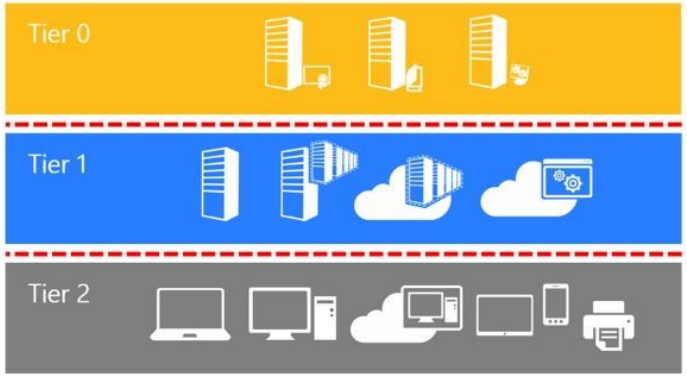
- Schnelles und verlässliches **Patchen** √
- Ausführung von **Office-Makros** einschränken √
- **Alte Office-Dateiformate** (.DOC, .XLS, …) und exotische Dateitypen (.SCR, ...) blockieren √
- **USB-**(Speicher-)Nutzung einschränken √
- Anwendern **lokale Adminrechte** wegnehmen √
- **Passwortqualität** verbessern √
- **Identische Passwörter verhindern**, LAPS √
- Keine identischen Accounts auf mehreren Rechnern verwenden …
- **Windows 10 Enterprise**: Device Guard, Credential Guard √
- Internetzugang von Servern einschränken …
- **Alte Protokolle/Verschlüsselungsverfahren** abschaffen: SMBv1, NTLM, unsigniertes SMB u. LDAP, RC4 …
- **EDR** statt klassischem Antimalwareschutz √

Und noch mehr…

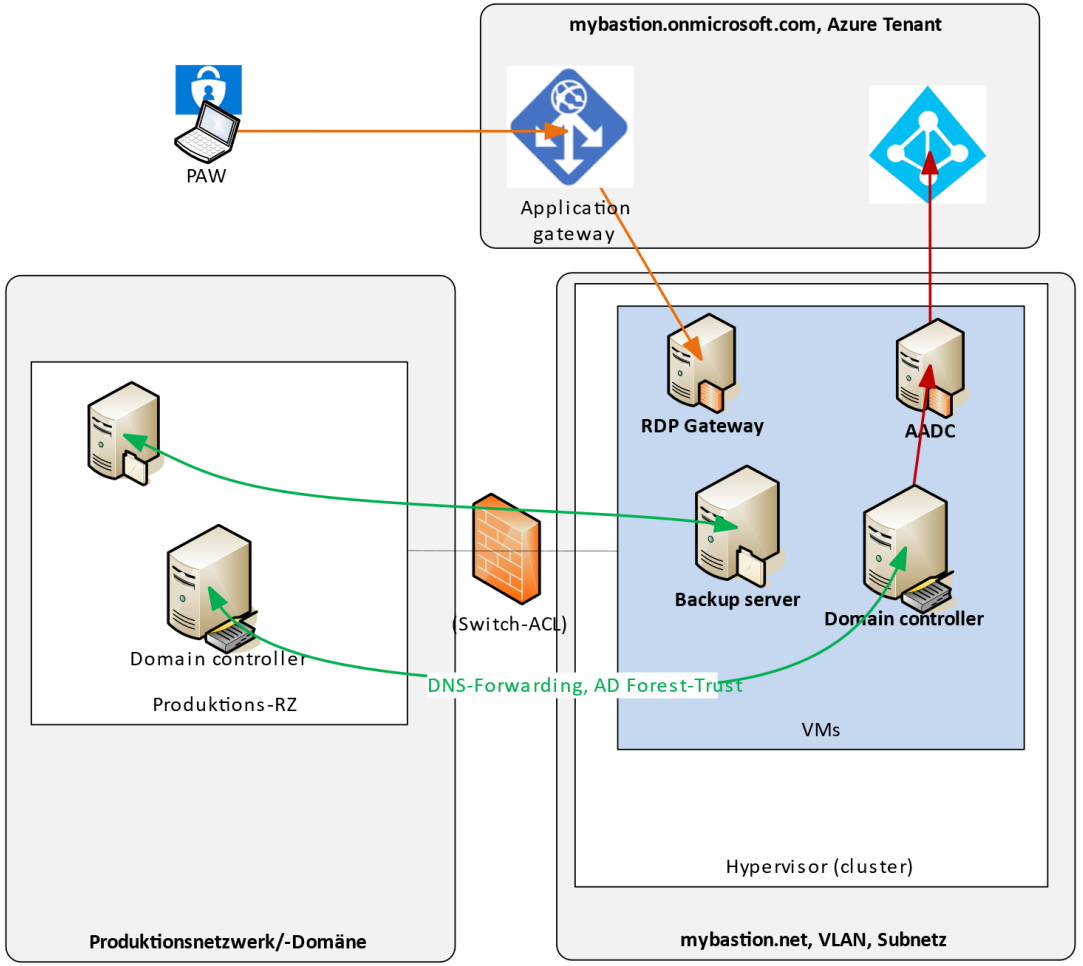
- **Privileged Access Workstations** für Admins



- **Adminaccounts reduzieren, Tiered Admins**

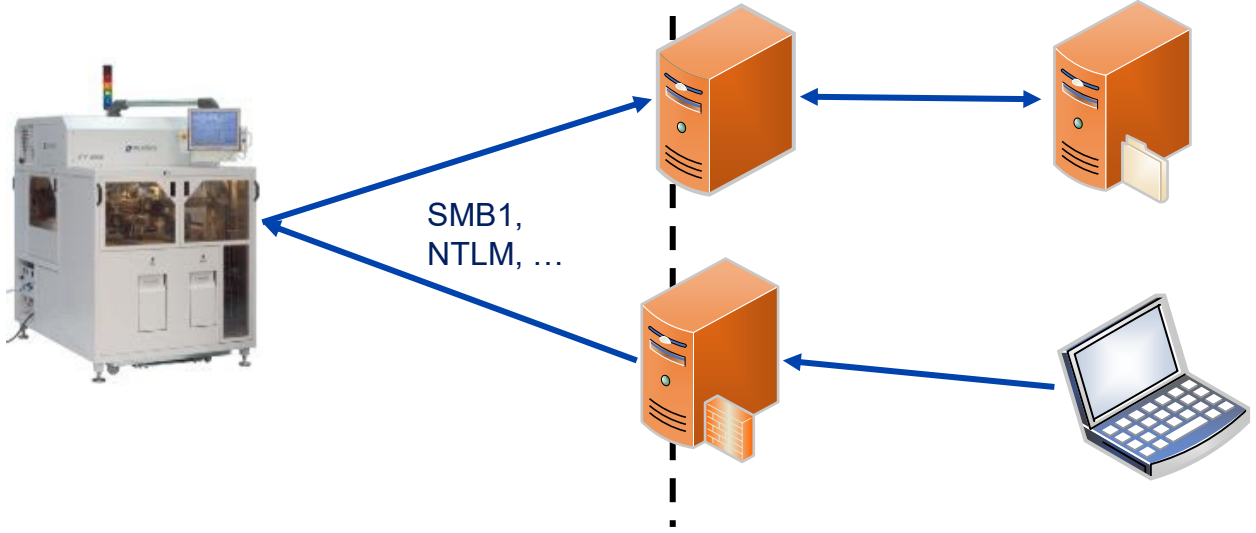


- **Bastion-Domäne/-Tenant/-Netz** für Backup, Monitoring, SIEM, …



Aber all das erreicht die Produktion nur bedingt...

- Veraltete Clients (noch heute 40+ Windows 2000, 100+ XP, 100+ Windows 7 und schon wieder 100+ veraltete Windows 10, alte Unix-/Linux-Versionen)
- Anlagen leben viel länger als die Software gepflegt wird
- Veraltete Server für zugehörige Anwendungen
- Rechner, die nicht von IT gepflegt werden
- Hersteller unterstützt Sicherheitsmaßnahmen nicht (*verbietet* sie)
- Oft sehr unsichere Konfigurationen



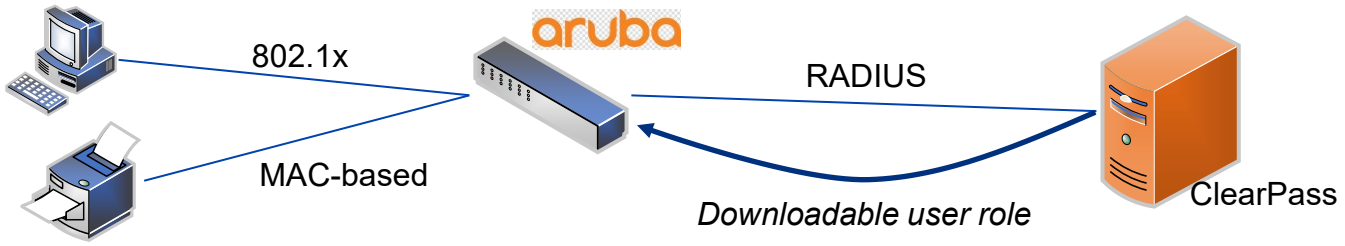
Zurückrudern!

- Domänenmitgliedschaft aufgeben
- Dedizierte *rückwärtskompatible* Server
- Jumphosts
- Aber vor allem: **Segmentierung**!

Netzwerksegmentierung

- Ganze Fertigung, oder einen ganzen Fertigungsbereich per Firewall abschotten?
  Dann immer noch freie Bahn zwischen den Produktionsrechnern…

- Unsere Lösung: portbasierte Policies (ACLs) mit HPE Aruba AOS(-CX) Switches und ClearPass



  - Endgeräte können noch mit Servern kommunizieren aber nicht mehr untereinander
    Mikrosegmentierung am *Edge*

Wie stehen wir heute da? Und Sie?