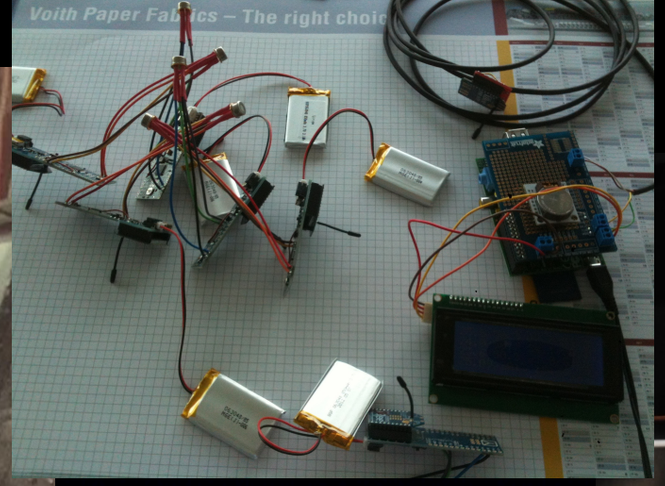
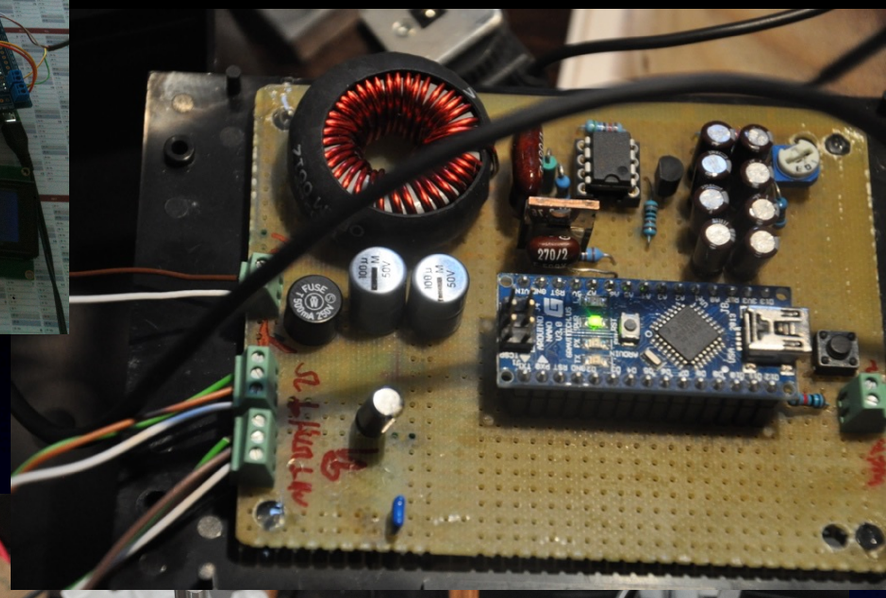
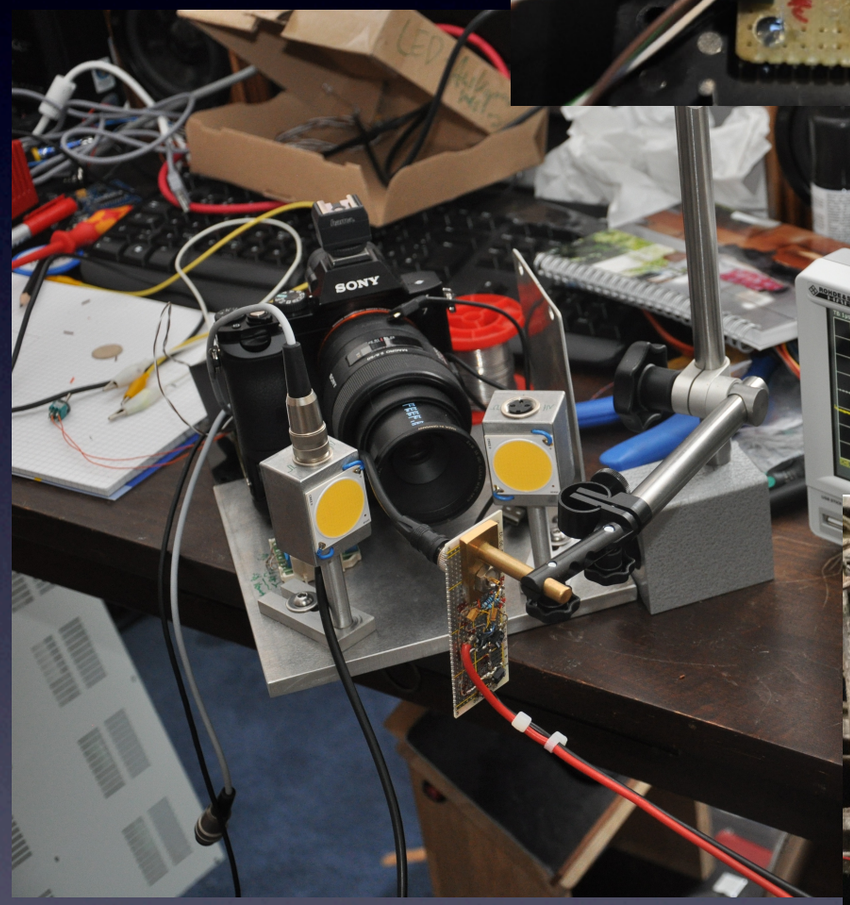
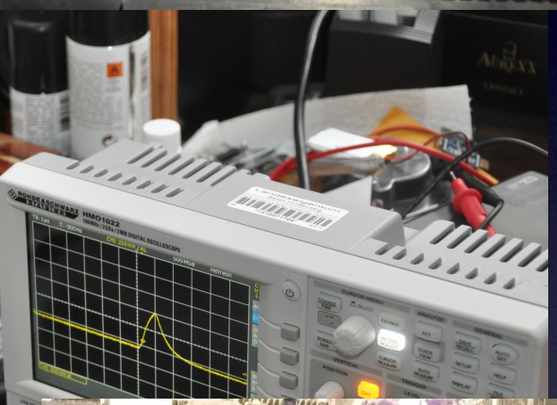
Best practises für die Produktions-IT

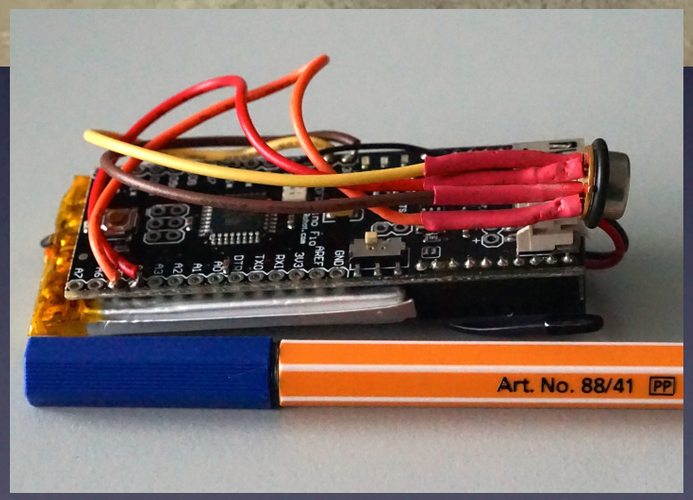
Till Hänisch, Duale Hochschule Baden Württemberg, Heidenheim, www.tillh.de

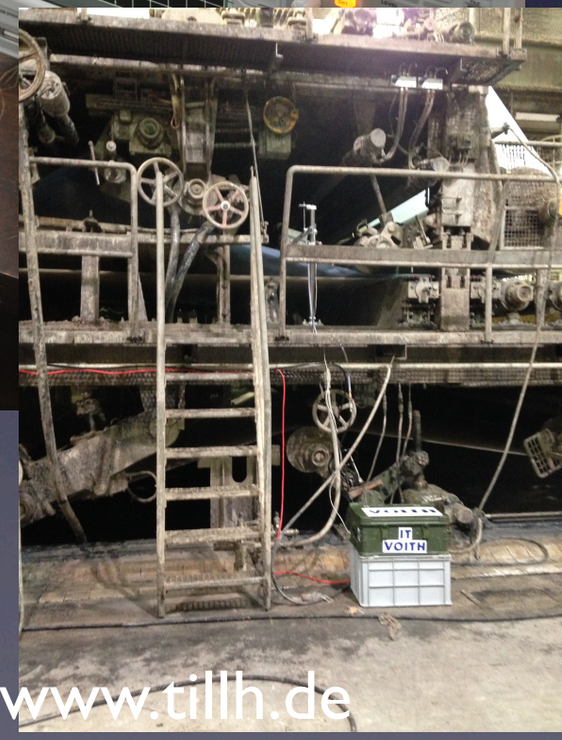












Best practises für die Produktions-IT

Till Hänisch, Duale Hochschule Baden Württemberg, Heidenheim, www.tillh.de

IT-Silos

IT in der Produktion

IT-Sicherheit ?

Never touch a running System

Verfügbarkeit

Enterprise IT

ITIL

Integrität

Consumer IT und Produktion finden zusammen

Virtuelle Fabrik

http://ubisense.net/en/blog/manufacturing/ubisense-smart-factory-delivering-never-possible-visibility-manufacturers-worldwide

Risiken

Übliche Maßnahmen funktionieren hier nur schlecht:

- Patch management
- Host basierte Virenscanner/IDS
- ITIL-ähnliche Prozesse
- Standardisierte Hardware/Software Plattform
- Portbasierte Authentisierung

Vorgehen

- Umfrage
- Best practises
- Übertragung
- Handreichung

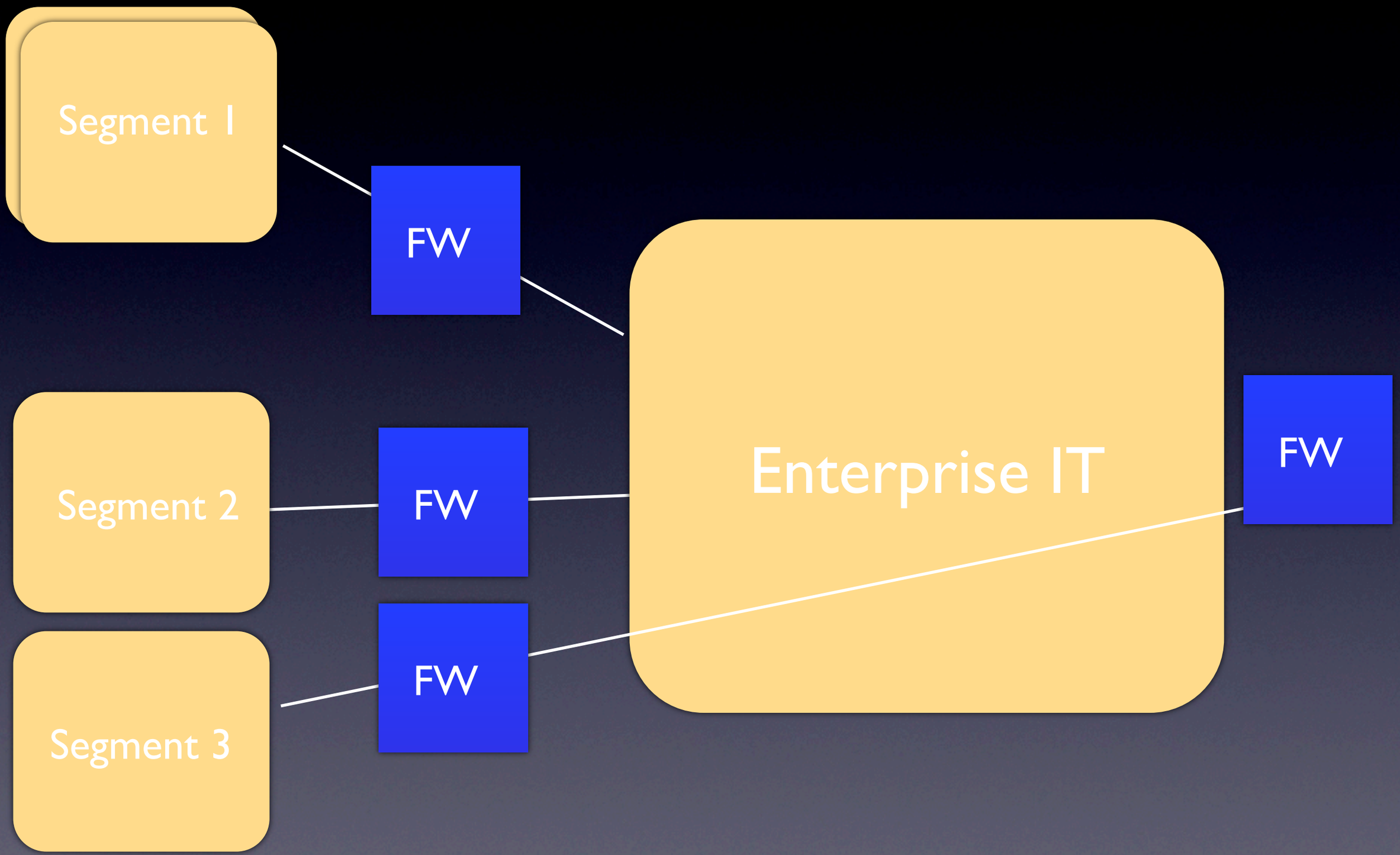
Lösungsmuster

Primärer Maßnahmen Typ	Primäre Ausrichtung	Maßnahme	U1	U2	U3	U4	U5
1. Organisatorisch	1.1 Präventiv	1.1.1 Methodische, wiederkehrende Risikoanalyse	■	●	●	▲	●
		1.1.2 Vorlage für einmalige Risikoeinschätzung	●	■	■	■	●
		1.1.3 Patch-Level-Management Prozess (soweit integrierbar)	■	●	●	●	■
		1.1.4 Richtlinienkatalog für Industrie 4.0 Anwendungsfälle	■	▲	●	▲	■
		1.1.5 Standardisierung von (Netz-)Infrastruktur	■	■	■	■	●
		1.1.6 Standardisierung von Software	■	▲	▲	▲	▲
		1.1.7 Standardisierung von System-Hardware	■	▲	▲	▲	▲
		1.1.8 Standardisierung der Fernzugriffe	▲	▲	●	●	▲
		1.1.11 Awareness der Produktionsverantwortlichen für IT-Sicherheitsziele	■	■	●	●	●
	1.2 Reaktiv	1.2.1 Prozess Security Information Event	▲	▲	■	●	■
2. Technisch	2.1 Präventiv	2.1.1 Netzwerksegmentierung an Hand der ursprünglichen Inselsysteme	●	●	●	■	■
		2.1.2 Netzwerksegmentierung an Hand von Systemklassen	■	●	■	■	●
		2.1.3 Logische Zugangskontrolle der Ports (IEEE 802.1X)	▲	▲	▲	■	▲
		2.1.5 Kommunikationsflüsse End-to-End verschlüsselt	●	■	■	■	▲
		2.1.6 Firewall-System, L3/L4	●	●	●	■	●
		2.1.8 Regelmäßige, automatisierte Verwundbarkeitsprüfung	●	●	●	■	▲
		2.1.9 Logische Limitierung von Mobilen Speichermedien	■	●	■	■	■
		2.1.10 Mechanismen zur Detektion von Schadsoftware von Mobilen Medien	■	●	■	■	■
		2.1.11 Authentifizierung durch Benutzerkennung und (inkl. schwaches) Passwort	●	●	●	●	●
		2.1.12 Authentifizierung der Endpunkte durch digitale Zertifikate (X509)	▲	■	■	■	■
	2.2 Reaktive	2.2.1 Host und/oder Netzwerkbasierendes IDS	▲	■	■	■	■
		2.2.2 HoneyPot (low/mid/high Interaktion)	■	●	■	▲	■

Legende: ● vollständig ▲ teilweise ■ nicht vorhanden

5 Unternehmen, im Mittel 3.000 Mio Umsatz, 15.000 Mitarbeiter

Segmentierung



Best practises

- Sicherheit auf Netzwerkebene, statt auf Host
- Segmentierung der Netzbereiche durch L3/L4 Firewalls (lokal oder in Schutzklassen/zonen)
- Default Deny bei Kommunikation
- Standardisierung von Fernzugriffen
- Überwachung durch IDS/Honeypot
- Verifizierte mobile Medien
- Awareness für IT-Sicherheit bei Produktions-verantwortlichen
- Wissen über Verwundbarkeiten (Vulnerability scan, Configuration Management)
- Methodische Risikoanalyse

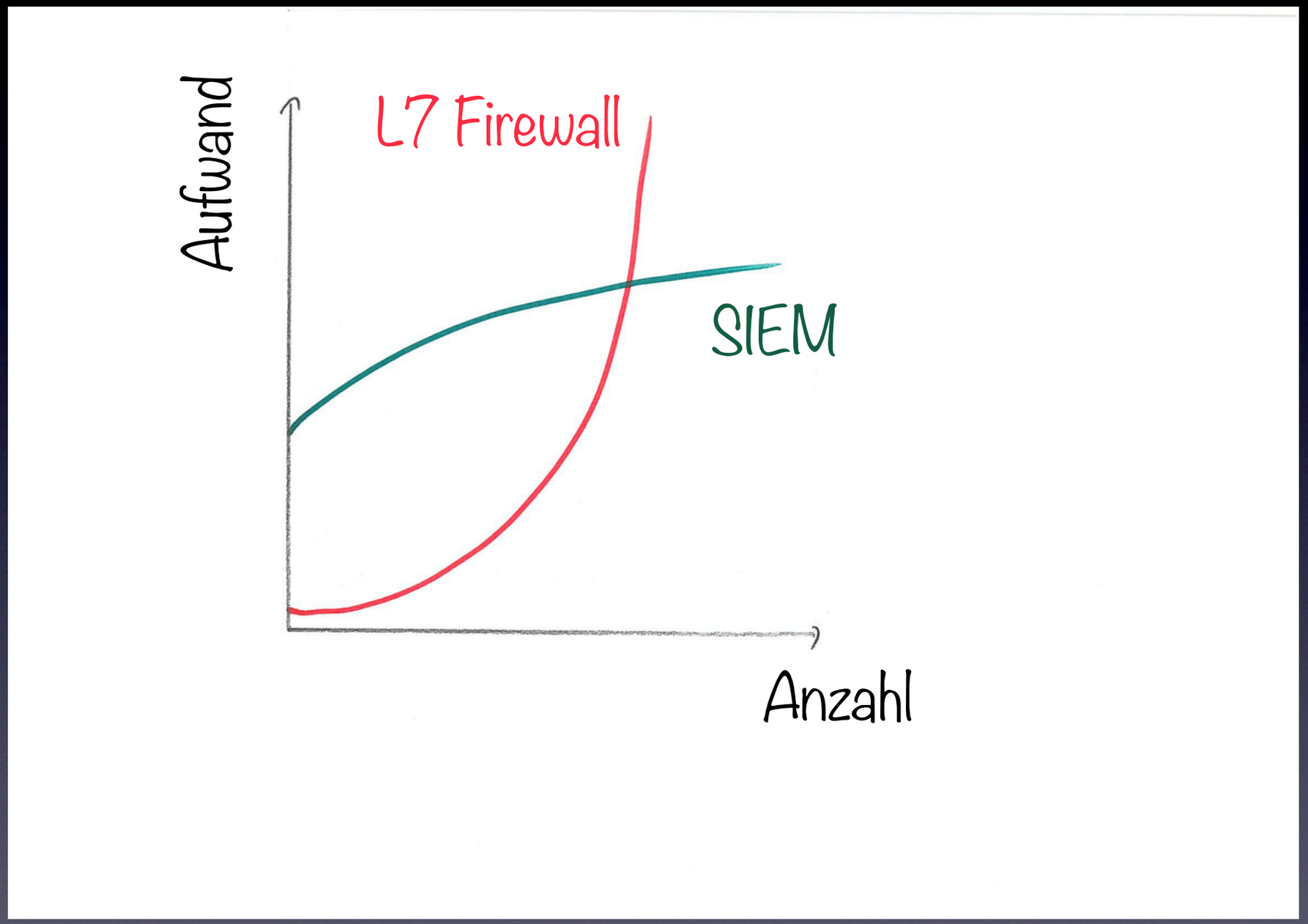
Best practises

- Sicherheit auf Netzwerkebene, statt auf Host
- Segmentierung der Netzbereiche durch L3 Firewalls (lokal oder in Schutzklassen/zonen)
- Default Deny bei Kommunikation
- Standardisierung von Fernzugriffen
- Überwachung durch IDS/Honeypot
- Verifizierte mobile Medien
- Awareness für IT-Sicherheit bei Produktions-verantwortlichen
- Wissen über Verwundbarkeiten (Vulnerability scan, Configuration Management)
- Methodische Risikoanalyse

Für Mittelständische Unternehmen umsetzbar

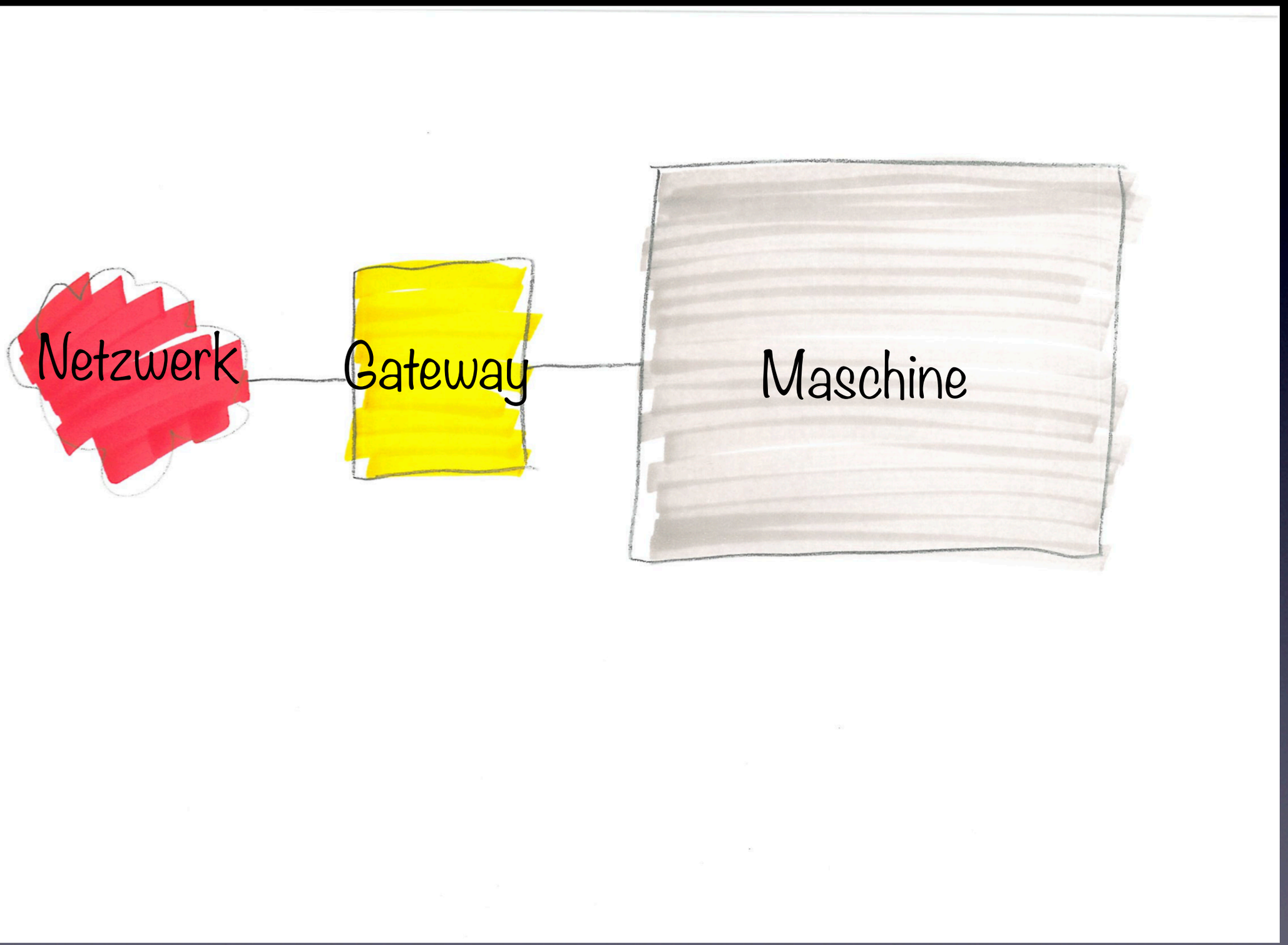
Nur teilweise übertragbar

Zusätzliche Maßnahmen für mittelständische Unternehmen

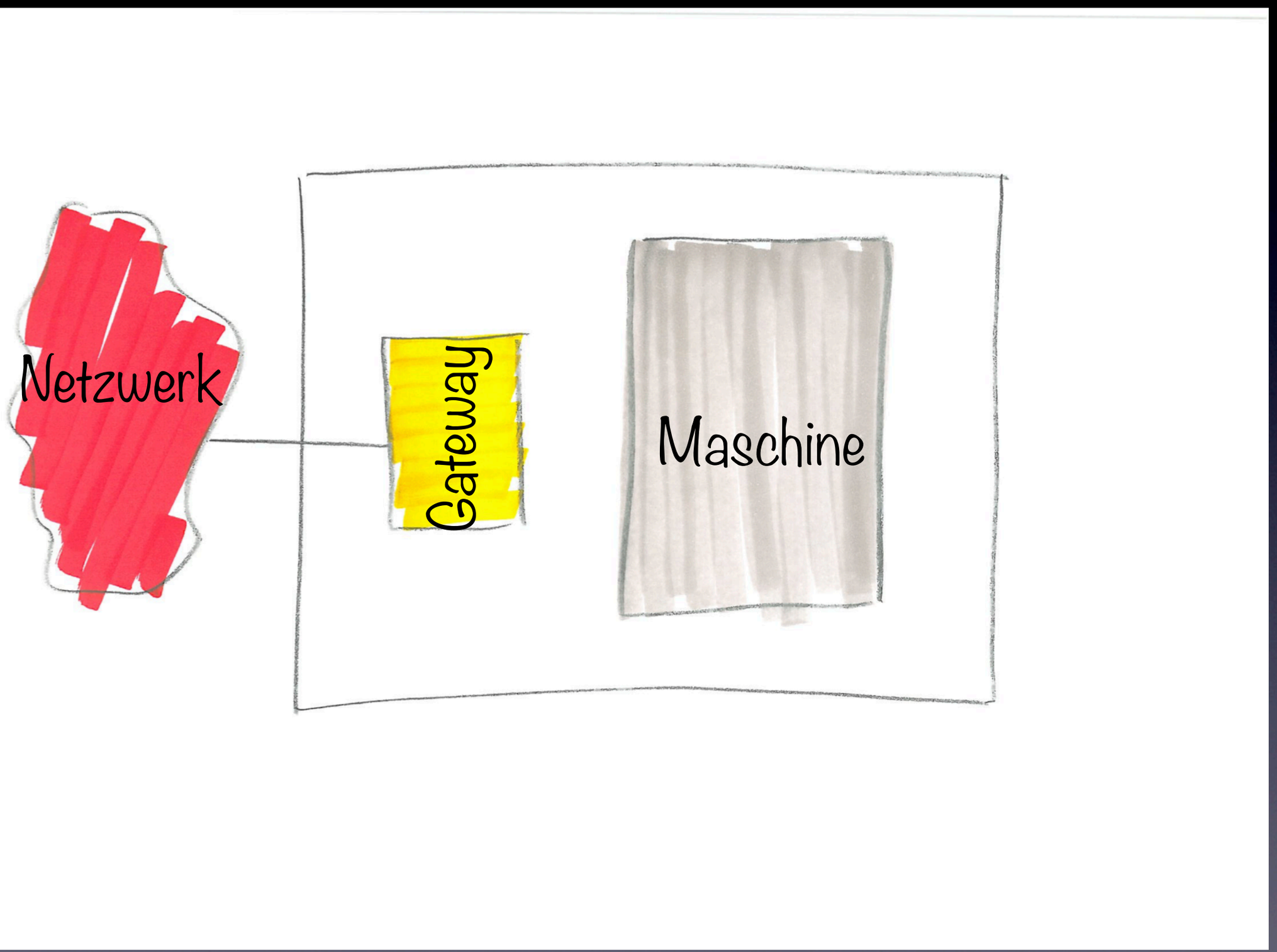


Maschinen durch Application Layer Firewalls isolieren

Aber wer konfiguriert die ?



Aber wer konfiguriert die ?



Danke für Ihre Aufmerksamkeit !

haenisch@dhbw-heidenheim.de