
ACP
ACP – Offizieller Ausrüster
Ihrer Cloud.
Offizieller Ausrüster
Ihrer Cloud.

Smart Factoy of the Future?

Aber wie weit sind unsere C(F,I,E)O‘s

Disclaimer

Die nun folgenden Ausführungen und Erzählungen basieren auf wahrer Begebenheit beziehen sich jedoch **NICHT** auf die Teilnehmer dieses Auditoriums oder auf Teilnehmer, welche in parallelen Vortragsreihen anwesend sind oder auf Teilnehmer, welche die Absicht hatten heute teilzunehmen, jedoch noch im Stau stehen oder auf Teilnehmer, welche zu Hause vor dem Fernseher sitzen und stattdessen die nächste Staffel von „Wanted“ oder „Mr. Robot“ verfolgen.

Department Information Security

ACP IT SOLUTIONS GMBH

DI RIEGLER Markus
Head of Department, CISO
Member of Austrian Security Hub
markus.riegler@acp.at
Security-ao@acp.at

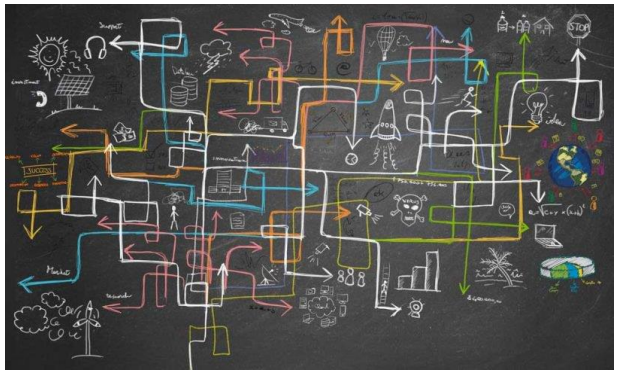
ACP Security Operation Center

Incident Response („Post Mortem Analysen“)

Bewusstseins-Bildung und IT Security Kompetenz

Beratungsleistung und Auditierung

Themenkomplexität



IT-SA Nürnberg 2018
Über 750 Aussteller
122 Themengebiete
3 Hallen, 24 Länder

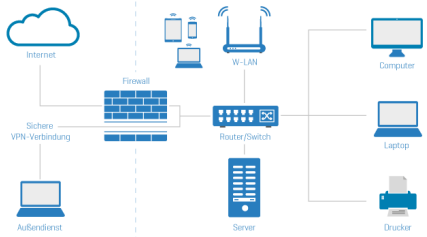
IT Security…?

Zitat: „Wie sicher sind wir eigentlich?“

Welcher Standpunkt - Betrachtungsweise

- ✓ Global
- ✓ Regional - Länder
- ✓ Branchenspezifisch

- ✓ Oder einfach nur „Wie gut ist meine „IT“ sicherheitstechnisch aufgestellt?“



IT Security…?

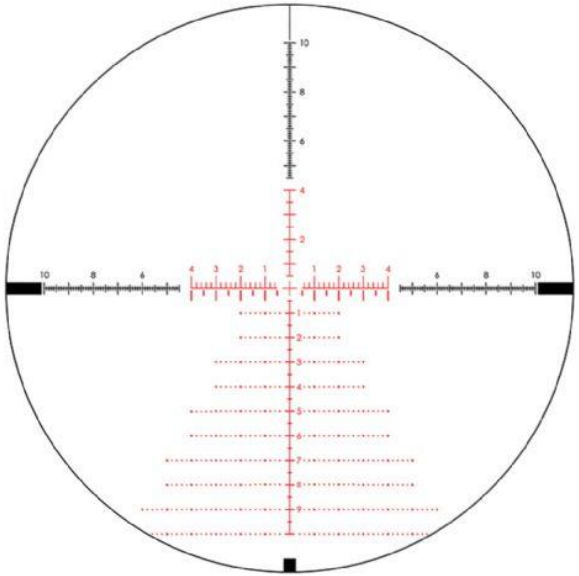
Zitat: „Wer interessiert sich denn für uns? – Wer soll uns schon angreifen?“

Im Fadenkreuz

Gezielter Angriff

Branch
(kritische Infrastruktur, öffentliche Einrichtung, Technologie)

Verhalten
(Statements, politische Meinungen, Soziale Medien)



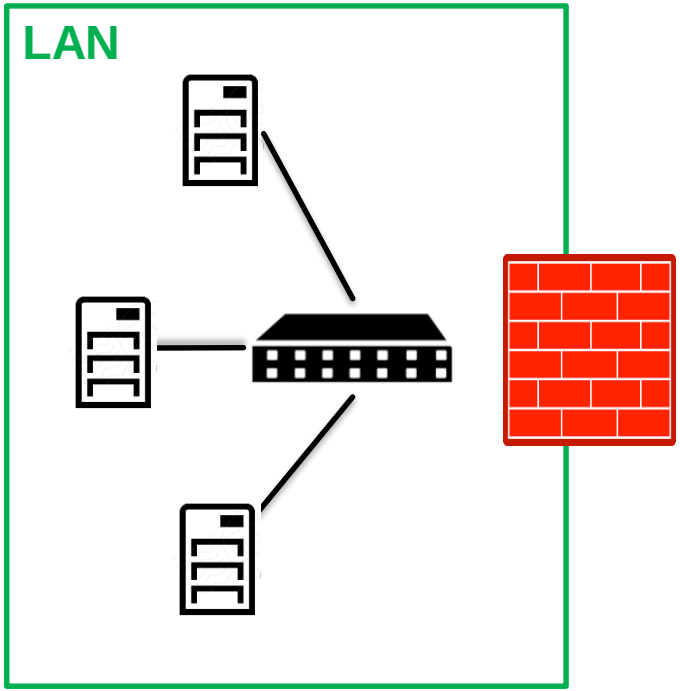
Zufallsprinzip

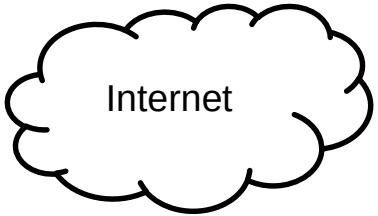
Schwachstellen-Scan
(Portscans, Vulnerability Scans, Shodan.io)

(Spear)-Phishing
(Telefonanruf, E-Mail)

Das RDP Problem…
und das Darknet

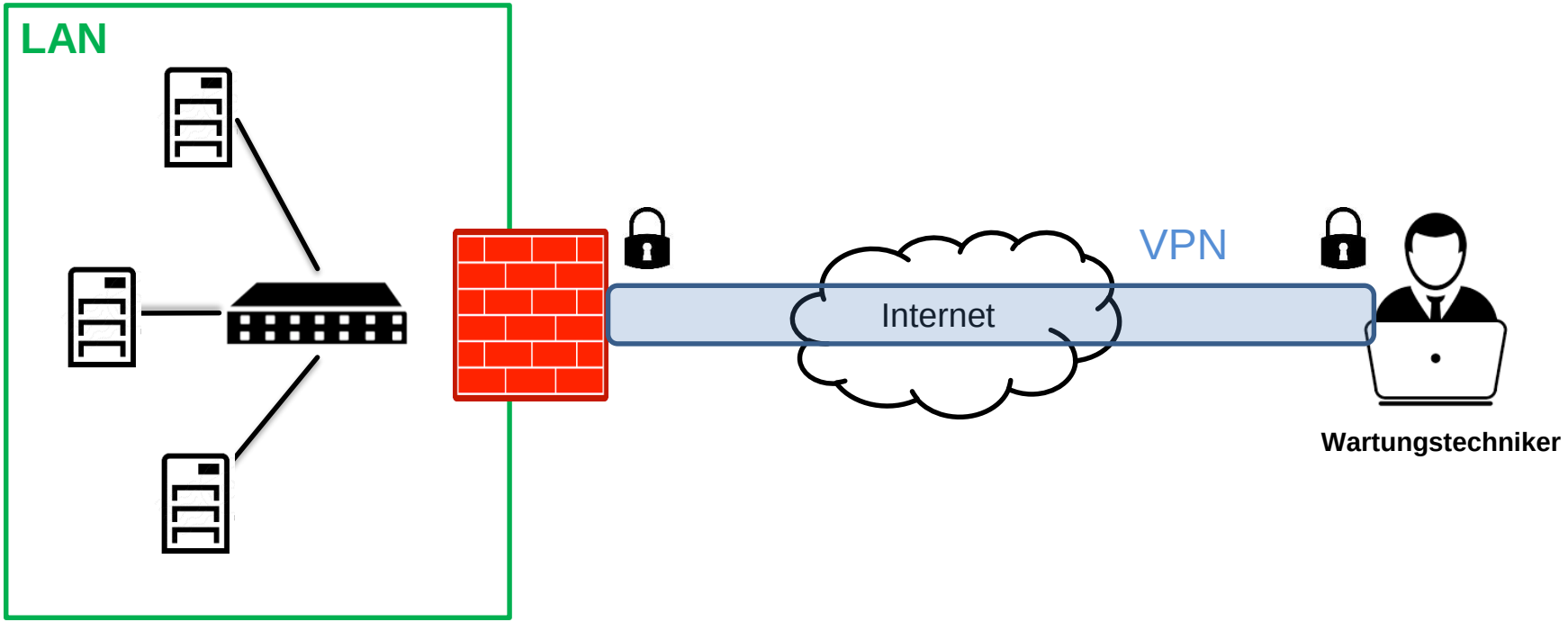
Problemstellung:



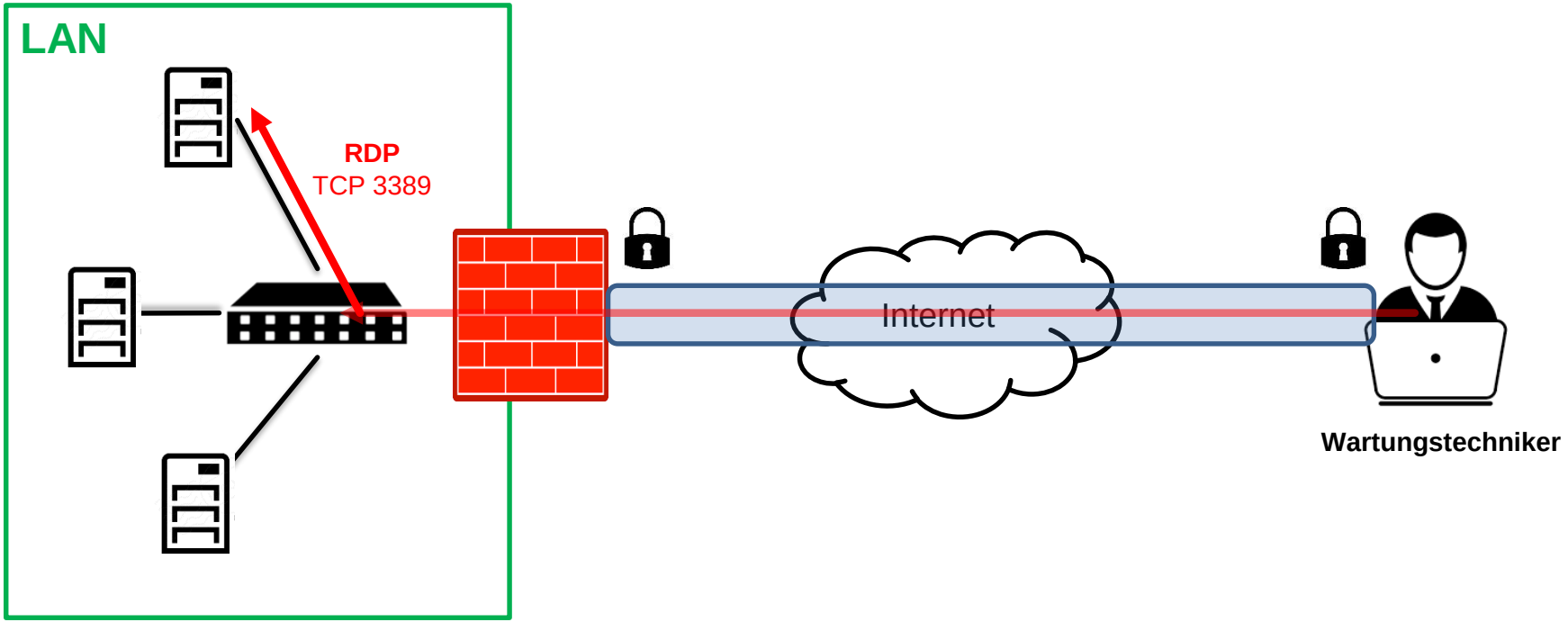


Wartungstechniker

Lösung 1:

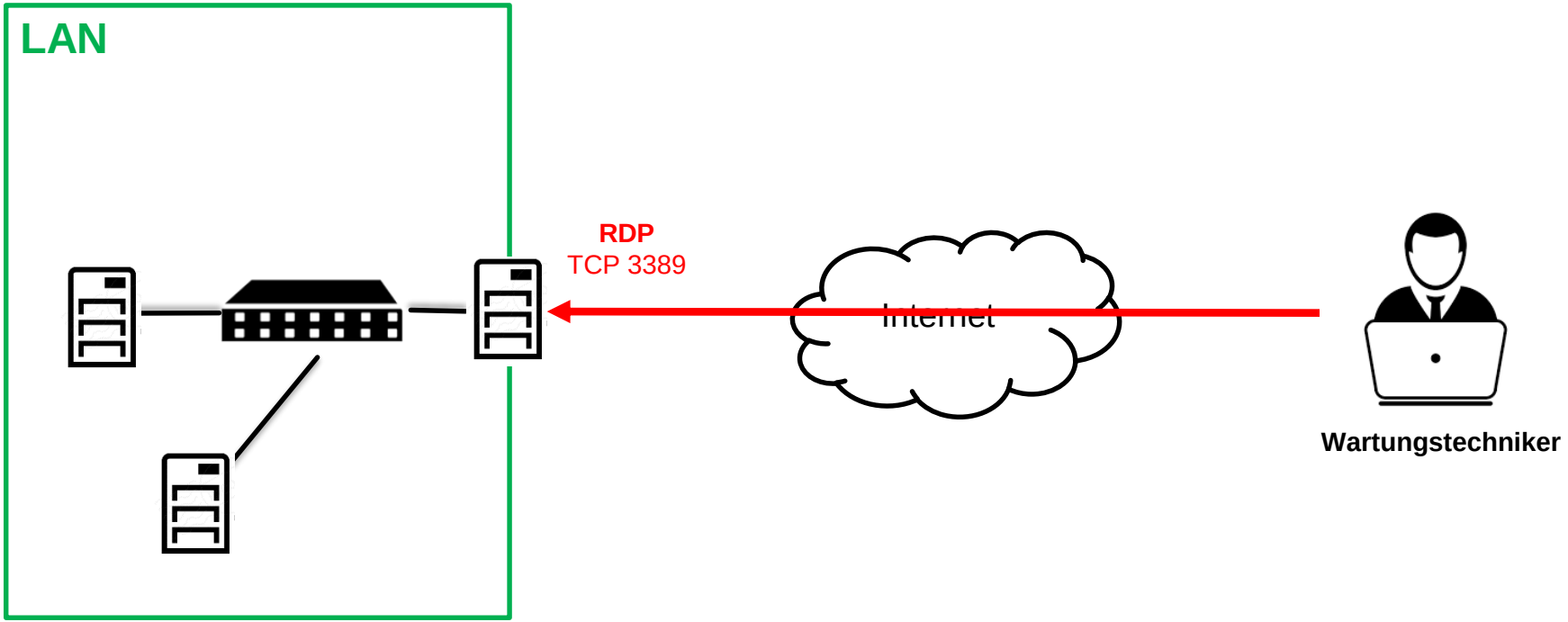


Lösungsvorschlag:



Die Realität:

Die Realität:

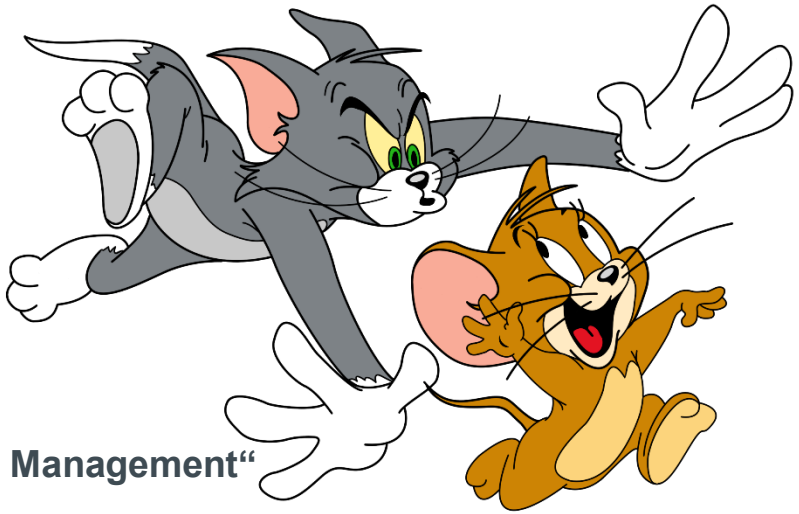


IT Security…?

Zitat: „Wir haben ja eine Firewall und einen Virenschutz!“

Was braucht es zum Schutz?

DAS KATZ- UND MAUSSPIEL



✓ **Vom „Virenschutz“ zur Endpoint Protection**

Signatur Basierte Erkennung
Heuristische Methoden
Verhaltensbasierte Methoden

✓ **Von der Firewall zur „Next Gen“ oder „Unified Threat Management“**

Packet Filter
Stateful Filter
Application Layer (Web Application Firewall)
NIDS, IPS, Cloud Services

Wo liegt das Problem?

DIE BLINDEN FLECKEN

Was braucht es dazu?

DAS SECURITY OPERATION CENTER

IT Security…?

Zitat: „Und was soll ich jetzt tun? – Wo soll ich anfangen? Und was kostet das?“

ACP Information Security Portfolio			
	MENSCH	**ORGANISATION**	**TECHNIK**
Identifizierung / Analyse	Personen, Profile, Rollen	Schutzbedarf und Gefährdungslage	Inventarisierung
Erkennung / Bewertung	Mitarbeiterbefragung /Sicherheitsprüfung	Risikomanagement	Frühwarnsysteme
Schutzmaßnahmen	Bewusstseinsbildung	Managementsystem für Informationssicherheit	Sicherheitsprodukte- und Services
Wiederherstellung	Mitarbeiter-Ein-/Austritt	Notfallvorsorge und Geschäftsfortführung	Daten- /Systemwiederherstellung
Auditierung / Test	Penetration Tests Menschliche Sicherheitsprüfung	Standards und Normen	Penetration Tests Technische Sicherheitsprüfung

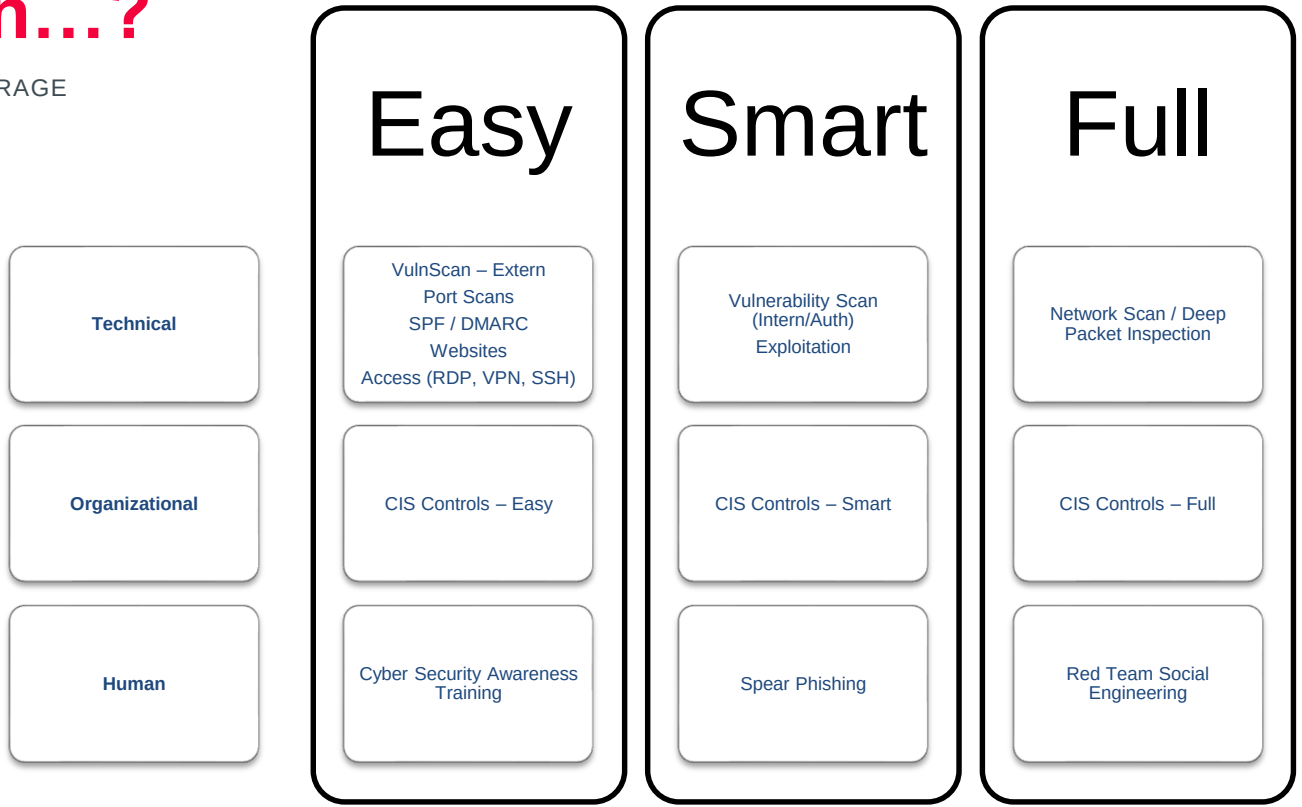
Risikobasierter Ansatz

EIN KRANKENHAUS IST KEIN MALERBETRIEB
EINE BANK IST KEIN SÄGEWERK

- ✓ „Safari Prinzip“ – Besser sein als die Anderen !
- ✓ Die offensichtlichen Schwächen finden und schließen !
- ✓ Die gleichen einfachen Werkzeuge nutzen !

Kosten…?

DIE GRÄTCHENFRAGE




ACP
ACP – Offizieller Ausrüster
Ihrer Cloud.
Offizieller Ausrüster
Ihrer Cloud.