COMPUTERSYSTEME

Member of ACP Group

Angriffsfläche verringern

Security Tag mit SWS & Sophos

Hans-Martin Kuhn

IT Security Consultant T.I.S.P.

IT for innovators.

Member of ACP Group

Die SWS ist ein herstellerunabhängiger IT-Provider, der End-to-End-Lösungen für Unternehmen, Behörden und Organisationen jeder Größe realisiert. Sie bietet Consulting, Beschaffung und Integration, Managed Services, Datacenter Services für das gesamte IT-Sortiment.

Um den Anforderungen im Thema Information Security gerecht zu werden, unterhält die SWS Computersysteme AG eine eigene Fachabteilung **Security Operations Center SOC**, welches sich ausschließlich mit dem Thema IT- und Cyber Security befasst. Diese Abteilung zeigt sich auch für die Aufrechterhaltung der definierten Security Operations sowohl für die SWS interne IT als auch nach außen, zu Kunden der SWS/ACP Deutschland zuständig. Das Team verfügt über Experten der Informationssicherheit mit mehrjähriger Erfahrung im Bereich der Technik, des Information Security Managements und des Information Security Consultings.

Das SWS SOC ist die zentrale Sicherheitsleitstelle zum Schutz der IT-Infrastruktur und deren Daten vor sämtlichen Cyber Bedrohungen. Um täglich wachsende Herausforderungen meistern zu können, überwacht das SOC die definierte (gesamte) IT-Infrastruktur beim Kunden, sammelt und korreliert Daten, sucht nach Angriffsmustern und steuert wichtige Gegenmaßnahmen. Zentralen Mehrwert stellen dabei die folgenden Punkte dar:

- Erkennung und Analyse von Anomalien innerhalb der überwachten Infrastruktur
- Erteilung von konkreten Handlungs- und Abwehrempfehlungen
- Transparenz der betreuten IT-Infrastruktur
- Bewertung der Sicherheitslage der IT-Infrastruktur
- Compliance durch Dokumentation von Ereignissen und Maßnahmen
- Laufendes Reporting als Grundlage für weiterführende Security Entscheidungen

SWS COMPUTERSYSTEME
Member of ACP Group

Themengebiete

Offensive Operations

- Managed Vulnerability Scan
- Penetration Test
- Phishing Simulation

Defensive Operations

- DNS Security
- Endpoint Protection
- Managed SIEM
- Incident Response/Forensik

Security Management

- Awareness Training
- Vulnerability Management (CVE Check)
- Incident Response Plan

Security Analytics

- IoC Analyse
- Schwachstellenanalyse
- Security Assessment

SWS COMPUTERSYSTEME
Member of ACP Group

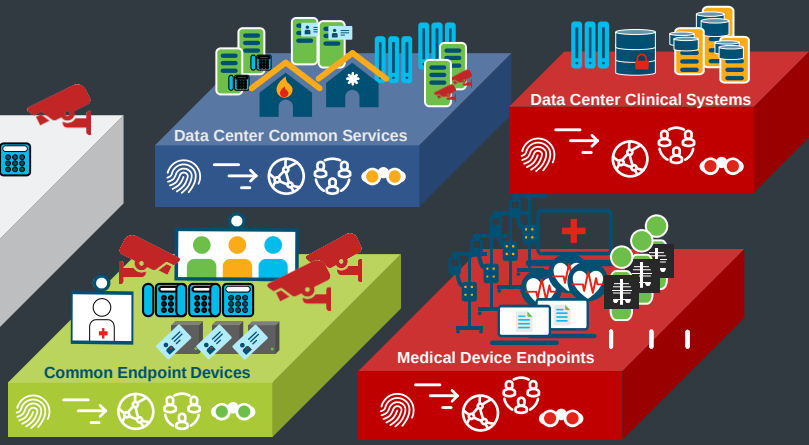
Angriffsfläche verringern – Trends in der IT Security

Flach → Segmentiert

Wie?

Fehlende Visibilität

Flaches Netzwerk

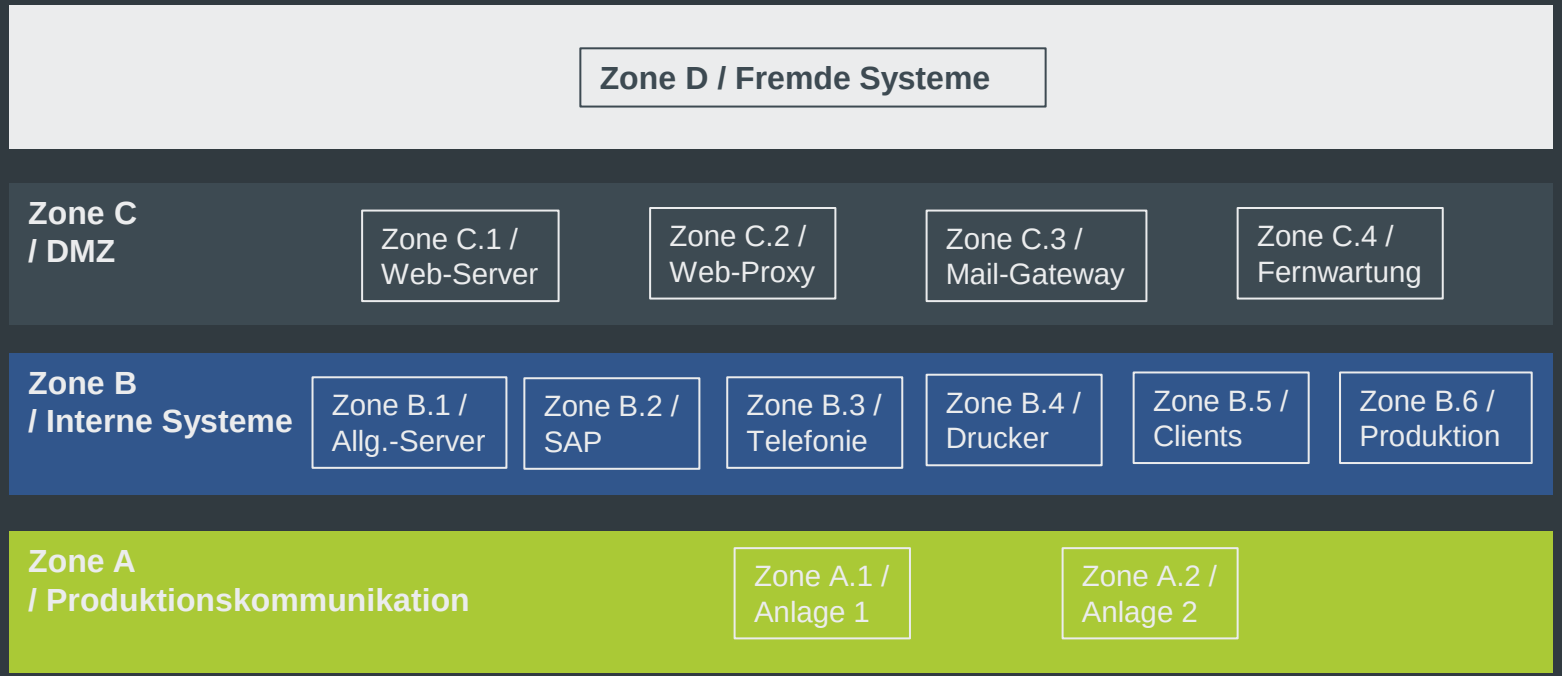


Segmentiertes Netzwerk mit Enklaven

Identity & Vertrauen | Policy Enforcement | Isolation | Verfügbarkeit | Visibilität

Angriffsfläche verkleinern!

Wie?


Zone D / Fremde Systeme
Zone C / DMZ
Zone C.1 / Web-Server
Zone C.2 / Web-Proxy
Zone C.3 / Mail-Gateway
Zone C.4 / Fernwartung
Zone B / Interne Systeme
Zone B.1 / Allg.-Server
Zone B.2 / SAP
Zone B.3 / Telefonie
Zone B.4 / Drucker
Zone B.5 / Clients
Zone B.6 / Produktion
Zone A / Produktionskommunikation
Zone A.1 / Anlage 1
Zone A.2 / Anlage 2

Netzwerkinfrastruktur

Traditionell

VS

Software-Defined

Traditionell vs Software-Defined

Traditionell

- Pilot muss wissen WIE ein Flugzeug gesteuert wird, damit er zum Ziel kommt.

➢ Admin ist beim traditionellen Ansatz Fluglotse und Pilot gleichzeitig.

Software-Defined

- Fluglotse muss nur wissen, was die richtige Route für das Flugzeug ist, er muss nicht wissen wie ein Flugzeug funktioniert.

➢ Beim software-defined Ansatz ist der Admin lediglich Fluglotse.

Segmentierung und Sicherheit

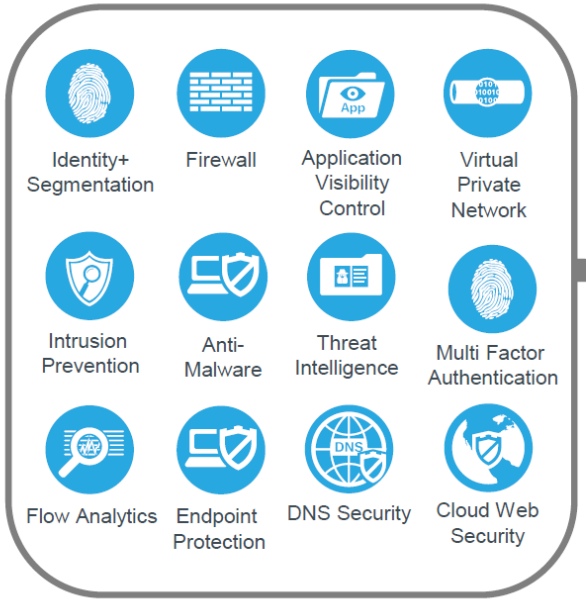
Ist Segmentierung alleine schon ausreichend um sich umfassend zu schützen?

Nein - Kombinieren Sie Netzwerksegmentierung immer zumindest mit regelmäßigen Systemupdates, regelmäßigen Backups, schwer zu erratenden Zugangsdaten (MFA) sowie mit Systemen zur Erkennung von Angriffen.

Aber auch Endpointsecurity (EDR/XDR), Netzwerkzugangskontrolle (NAC), Berechtigungsmanagement,…

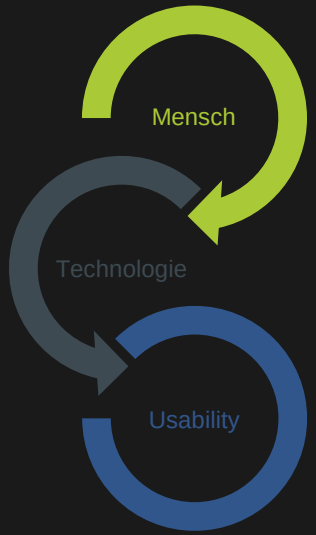
und…

Transparenz schaffen



Log-Daten!

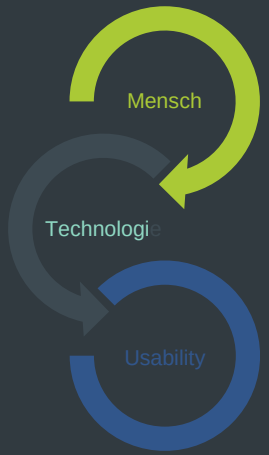
„menschliche Firewall“



Der Mensch als Sicherheitsrisiko?

„Technik vs. Mensch:
Was nutzt ein hoher technischer Standard,
Wenn die Schwachstelle Mensch umgangen wird?”

Quelle: 15. Deutscher IT-Sicherheitskongress, Andreas Rieb, Universität der Bundeswehr München



SWS COMPUTERSYSTEME
Member of ACP Group

Der Entwicklungspfad

Cloud ready!

Zero – Trust Implementierung

Unternehmens-Richtlinien & Compliance

Security-Integrationen

Segmentierung

BYOD

Vollständige Sichtbarkeit

Asset Sichtbarkeit

Gäste & WLAN

Geräte Administration

Agentless Posture

Strategische Reiseroute

Zitatsammlung zum Umgang mit Bürokratie, Krise

- Bei der Eroberung des Weltraums sind zwei Probleme zu lösen: die Schwerkraft und der Papierkrieg. Mit der Schwerkraft wären wir fertig geworden.
  Wehrner von Braun, deutsch-amerikanischer Wissenschaftler

- Bürokratie ist ein Versuch, den Fluss der Information zu rationalisieren und ihre Nutzung so effizient wie möglich zu gestalten, indem jede Information ausgesondert wird, die von einem akuten Problem ablenkt.
  Max Weber, deutscher Soziologe, Jurist und Ökonom

- Wenn einem das Wasser bis zum Hals steht, darf man den Kopf nicht hängen lassen.
  Ingrid Matthäus-Maier, deutsche Politikerin

- Krisen meistert man am besten, indem man ihnen zuvorkommt.
  Walt Whitman Rostow, US-amerikanischer Ökonom

- Wer zu lange ein Auge zugedrückt hat, wird erstaunt sein, wenn ihm plötzlich beide aufgehen.
  Søren Kierkegaard, dänischer Schriftsteller, Theologe und Philosoph

- Selbst dann, wenn man eine rosarote Brille aufsetzt, werden Eisbären nicht zu Himbeeren.
  Franz Josef Strauß, deutscher Politiker

- Widerstehe im Anfang, zu spät wird sonst das Heilmittel bereitet.
  Ovid, römischer Dichter

https://www.haushaltssteuerung.de/zitate-haushaltsreden-sonstiges.html#buerokratie

Vielen Dank für eure Aufmerksamkeit.

Fragen?

IT for innovators.

Member of ACP Group