SWS COMPUTERSYSTEME
Member of ACP Group

BRAIN SHARE
SWS COMPUTERSYSTEME AG

Modern Datacenter

AGILE, SECURE, COMPLIANT

IT for innovators.
Member of ACP Group

Ihr SWS Trio für die nächsten 60 Minuten

Florian Fröhlich

Senior Consultant Datacenter

Cloud & Modern Datacenter

seit 2018 bei der SWS, Regensburg

10+ Jahre Erfahrung Enterprise IT

Sascha Feig

Senior Consultant Datacenter

Workspace & VDI

seit 2016 bei der SWS, Hauzenberg

20+ Jahre Erfahrung Enterprise IT

Andreas Karl

Senior Consultant Datacenter

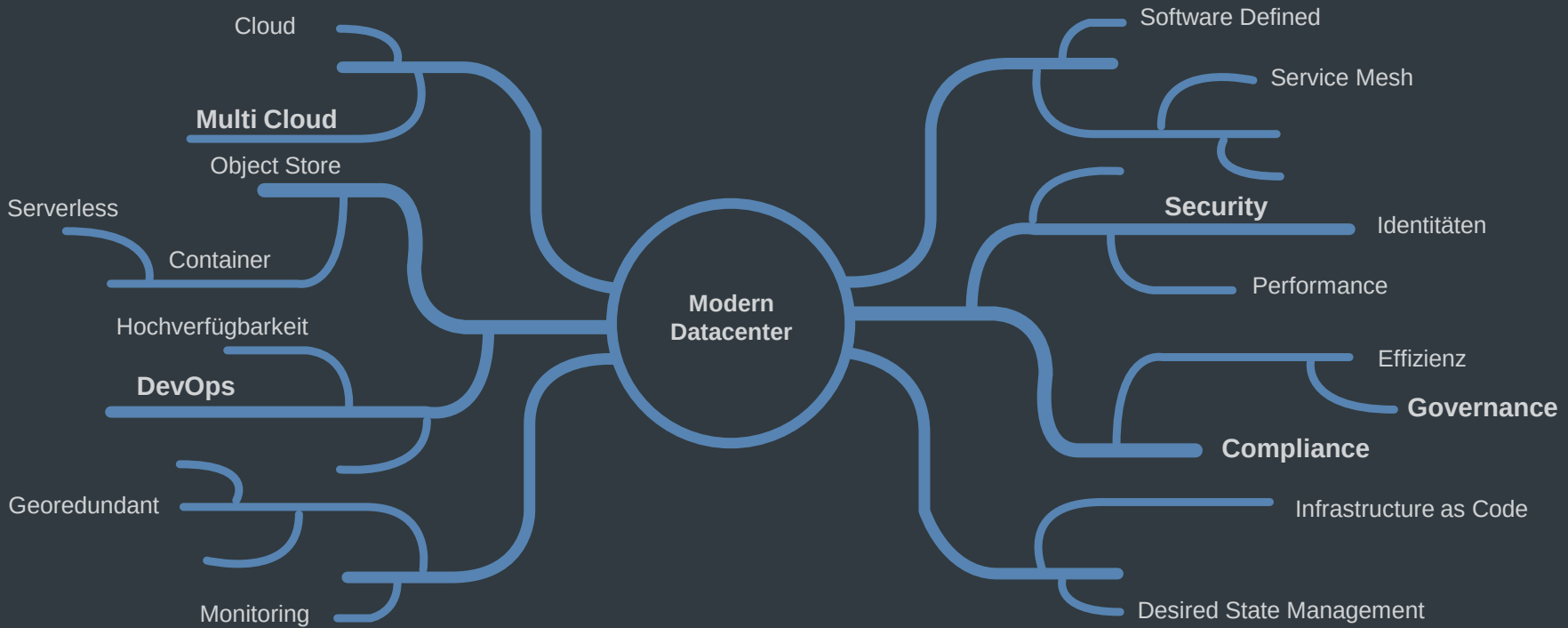
Infrastructure & Backup

seit 2018 bei der SWS, Regensburg

10+ Jahre Erfahrung Enterprise IT


DISRUPTIVE IT

Klassische IT	Aspekt	Disruptive IT
IT-orientiert	Fokus	Kundenzentriert mit Ergebnisfokus
Iterativ, inkrementell, fette Prozesse	Prozesse	Design Thinking, Kanban, Scrum, schlanke Prozesse
starr	Mindset	agil


Modern Datacenter
Cloud
Multi Cloud
Object Store
Serverless
Container
Hochverfügbarkeit
DevOps
Georedundant
Monitoring
Software Defined
Service Mesh
Security
Identitäten
Performance
Effizienz
Governance
Compliance
Infrastructure as Code
Desired State Management

Was Sie brauchen?

- Mindset
- Vision
- Einen starken und vertrauensvollen Partner

Komplexe Herausforderungen

- Security ist überall gefordert, jedoch oft schwierig in der Umsetzung
- Durchdachte Lösungen werden immer wichtiger, um Anforderungen bewältigen zu können
- IT wandert immer stärker in die Fachabteilungen und wird immer stärker zum Werkzeug
- Bei richtiger Positionierung kann die IT eine starke und geschätzte Rolle innerhalb der Organisation einnehmen

Die SWS kann helfen!

- Consulting
  - Lösungen finden
  - Verbesserung bestehender Prozesse
  - Integrative Gesamtkonzepte
  - Bewältigen von Sicherheits- und Complianceanforderungen
- Technologie
  - Klassisch
  - Modern
  - Nextgen
- Training
  - Agile Methoden
  - Mindset und Kultur
  - Technologie

Cloud Management

Neue Wege in der Verwaltung ihres Datacenter mit Cloudtechnologie zur Bewältigung aktueller und zukünftiger Herausforderungen

SWS COMPUTERSYSTEME
Member of ACP Group

Es gibt keine Cloud, nur Computer die anderen gehören? **Das ist falsch!**

- Beim Begriff Cloud geht es mittlerweile viel mehr um Bereitstellungsmodelle und Management
- Cloudtechnologien ermöglichen es trotz immer komplexerer Herausforderungen Lösungen bereitzustellen
- Synonym für Effizienz, Geschwindigkeit, Abstraktion komplexer Zusammenhänge

Use Case: Verteilte Datacenter standardisieren

- Vereinfachte Bereitstellung neuer Systeme
- Definierte Zustände an jedem Standort
- Verlässliche Qualität
- Compliance Anforderungen schneller und einfacher umsetzen

Use Case: Außenstelle

- Umfängliche Lösung ohne hohen Hard- und Softwareinvest für Management
- Management der Serverinfrastruktur auch als SaaS Angebot verfügbar
- Nutzung erprobter Betriebskonzepte
- It just works!

Use Case: Performance & Effizienz

- Ohne Unterstützung von Software nicht mehr möglich
- Kontinuierlich proaktiv oder anlassbezogen bei Problemen
- Als Vorbereitung für Migrationen in die Cloud
- Als SaaS, Managed Service und On-Prem verfügbar

SWS COMPUTERSYSTEME
Member of ACP Group

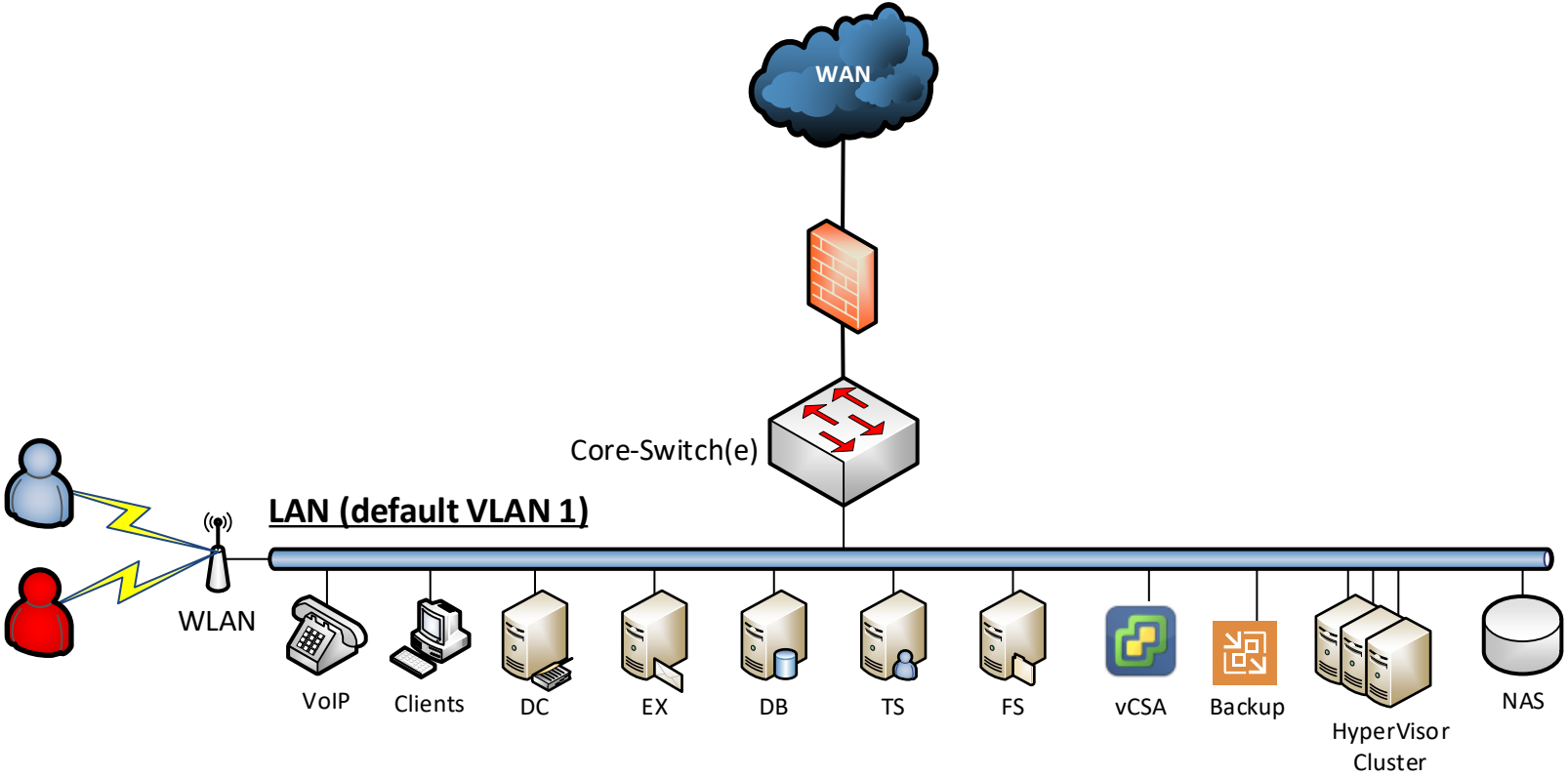
BRAIN SHARE
SWS COMPUTERSYSTEME AG

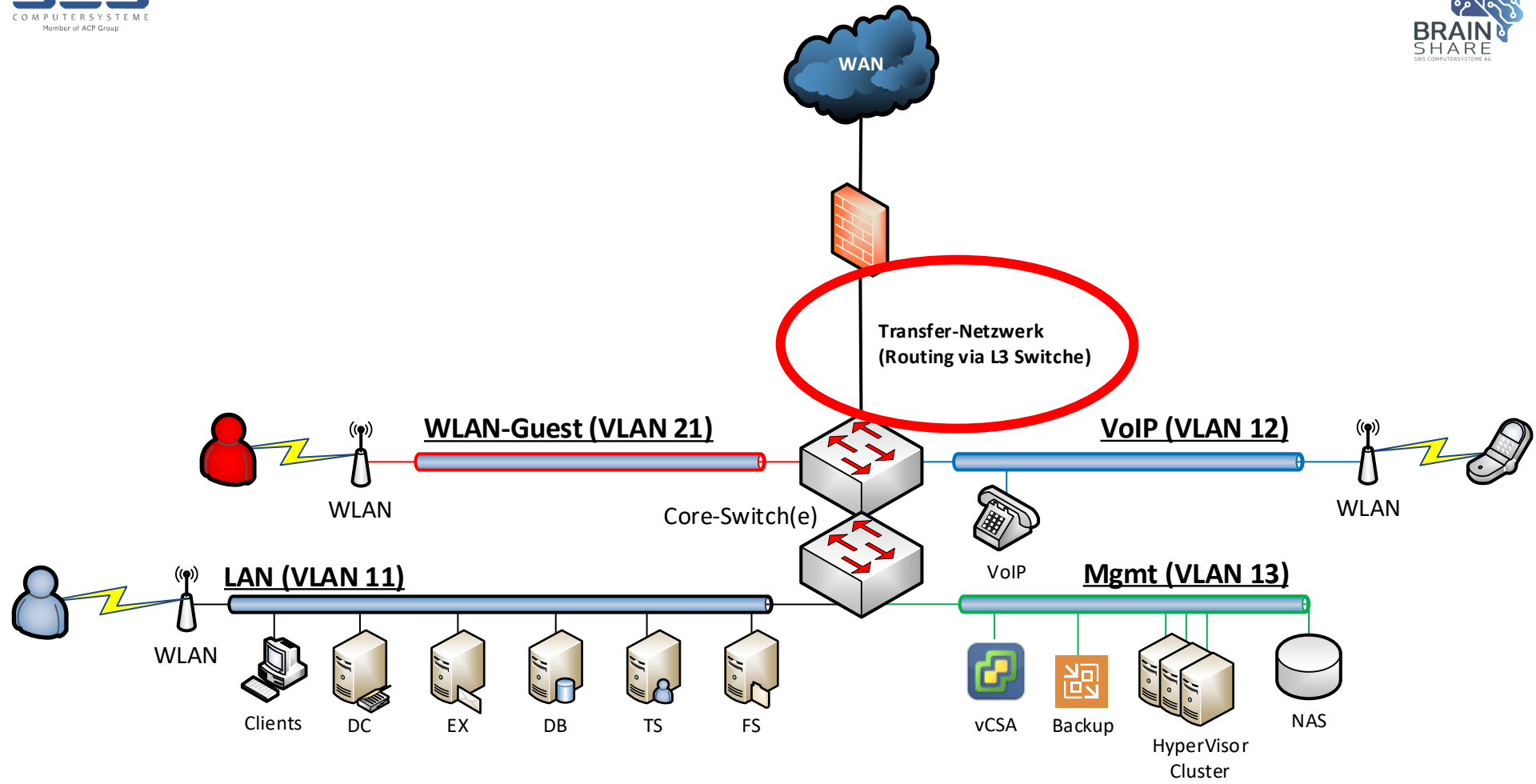
Netzwerksegmentierung und Flowanalyse

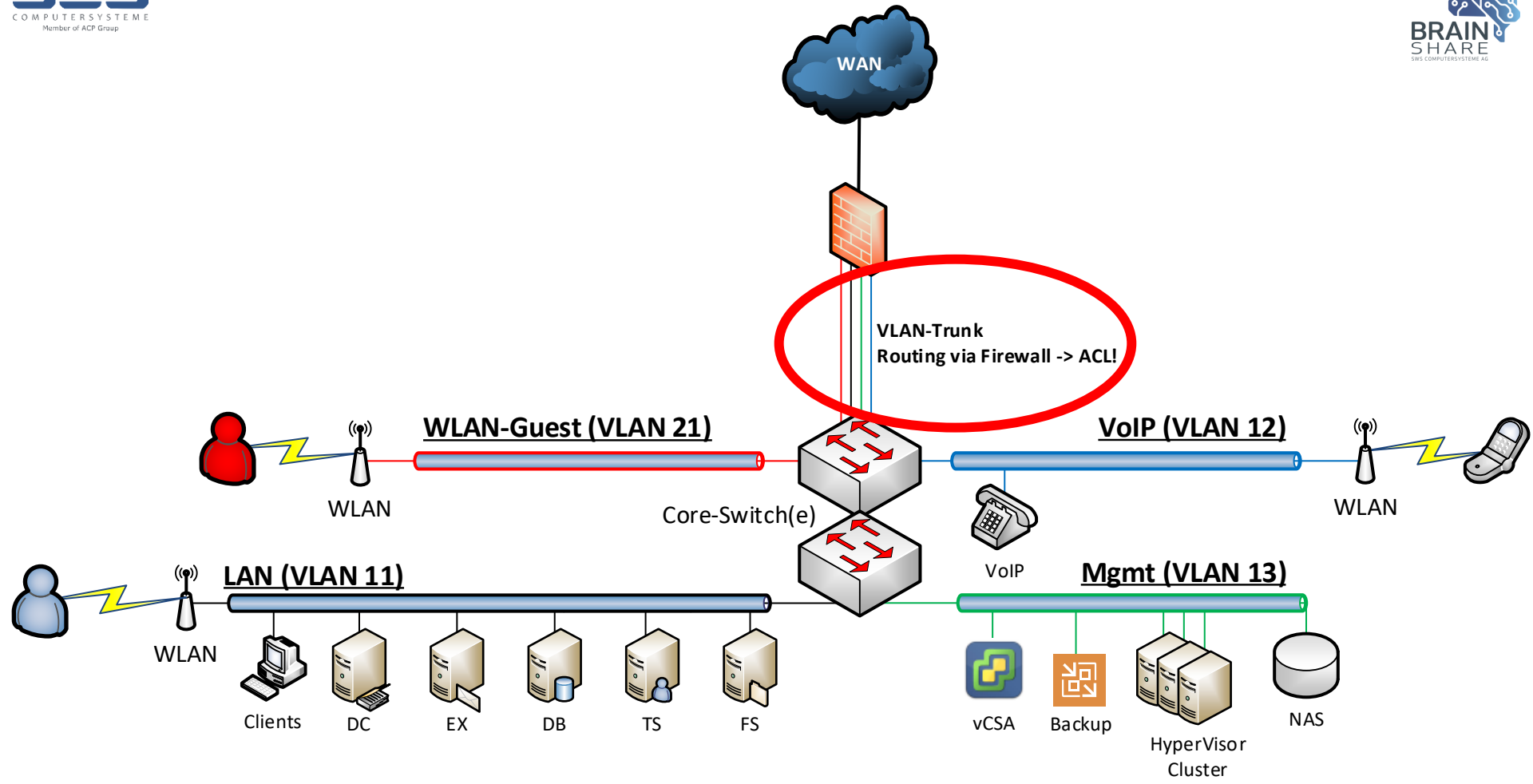
IT for innovators.
Member of ACP Group

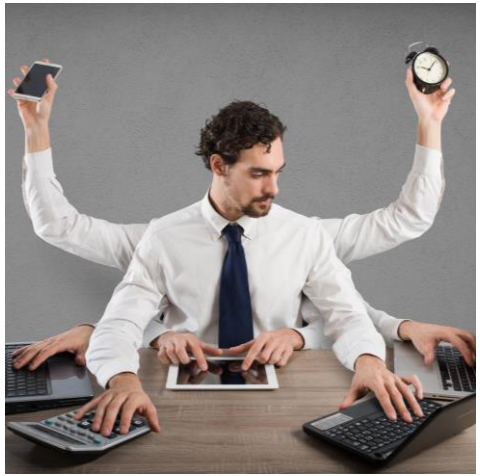
SWS COMPUTERSYSTEME
Member of ACP Group

Alles im großen Teich
oder
segmentieren Sie schon?


WAN
Core-Switch(e)
LAN (default VLAN 1)
WLAN
VoIP
Clients
DC
EX
DB
TS
FS
vCSA
Backup
HyperVisor Cluster
NAS


WAN
Transfer-Netzwerk
(Routing via L3 Switche)
WLAN-Guest (VLAN 21)
VoIP (VLAN 12)
WLAN
WLAN
Core-Switch(e)
VoIP
LAN (VLAN 11)
Mgmt (VLAN 13)
WLAN
Clients
DC
EX
DB
TS
FS
vCSA
Backup
HyperVisor
Cluster
NAS


WAN
VLAN-Trunk
Routing via Firewall -> ACL!
WLAN-Guest (VLAN 21)
VoIP (VLAN 12)
WLAN
WLAN
Core-Switch(e)
VoIP
LAN (VLAN 11)
Mgmt (VLAN 13)
WLAN
Clients
DC
EX
DB
TS
FS
vCSA
Backup
HyperVisor Cluster
NAS



What`s next?

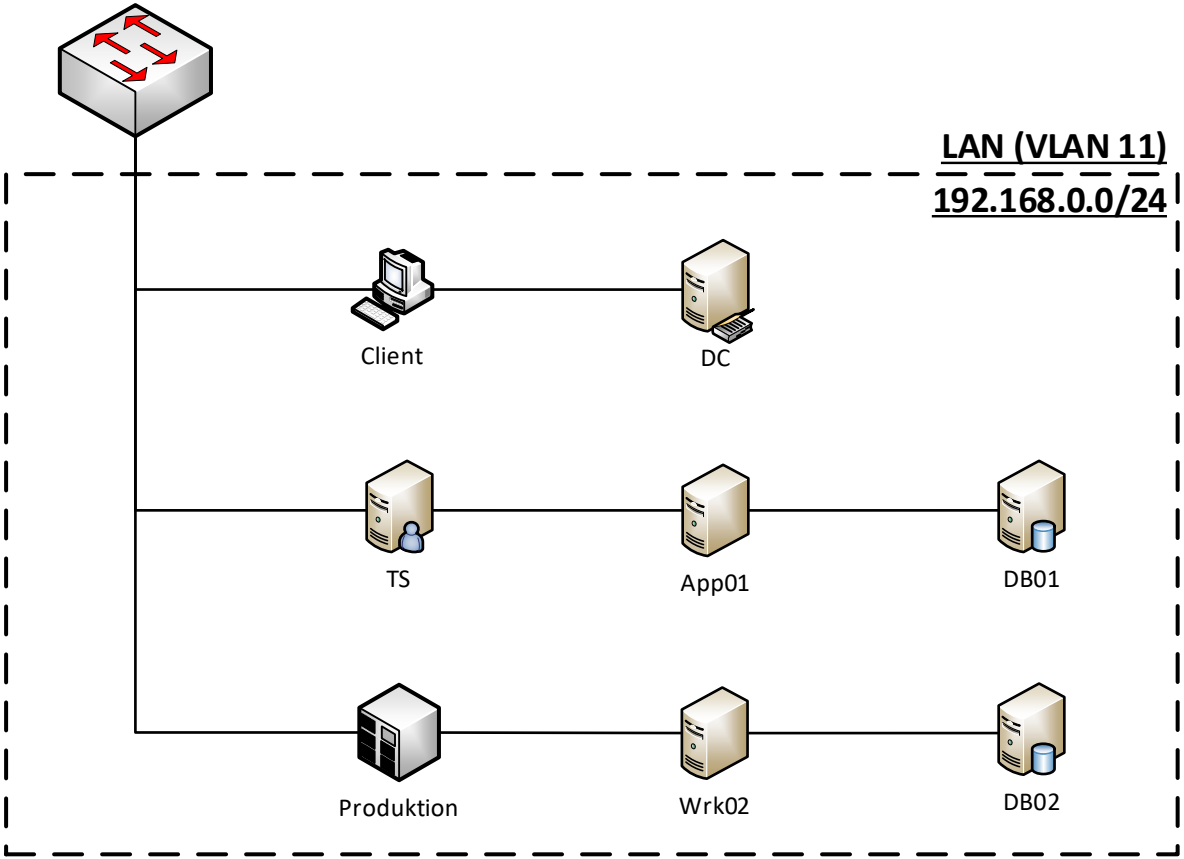
- Für jede Anwendung ein VLAN?
- Wer verwaltet das?
- Wer pflegt Zugriffsrechte?
- Wer dokumentiert und wo?

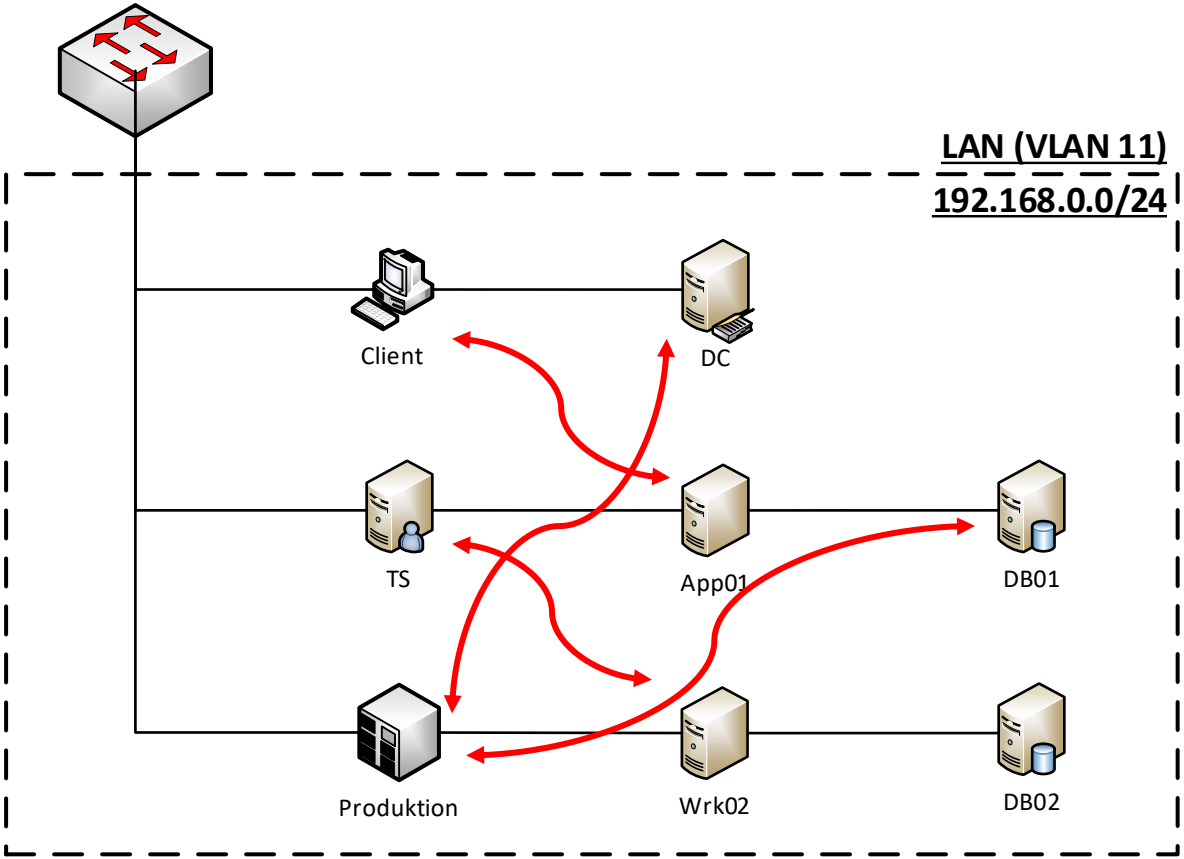
Wer behält den Überblick?

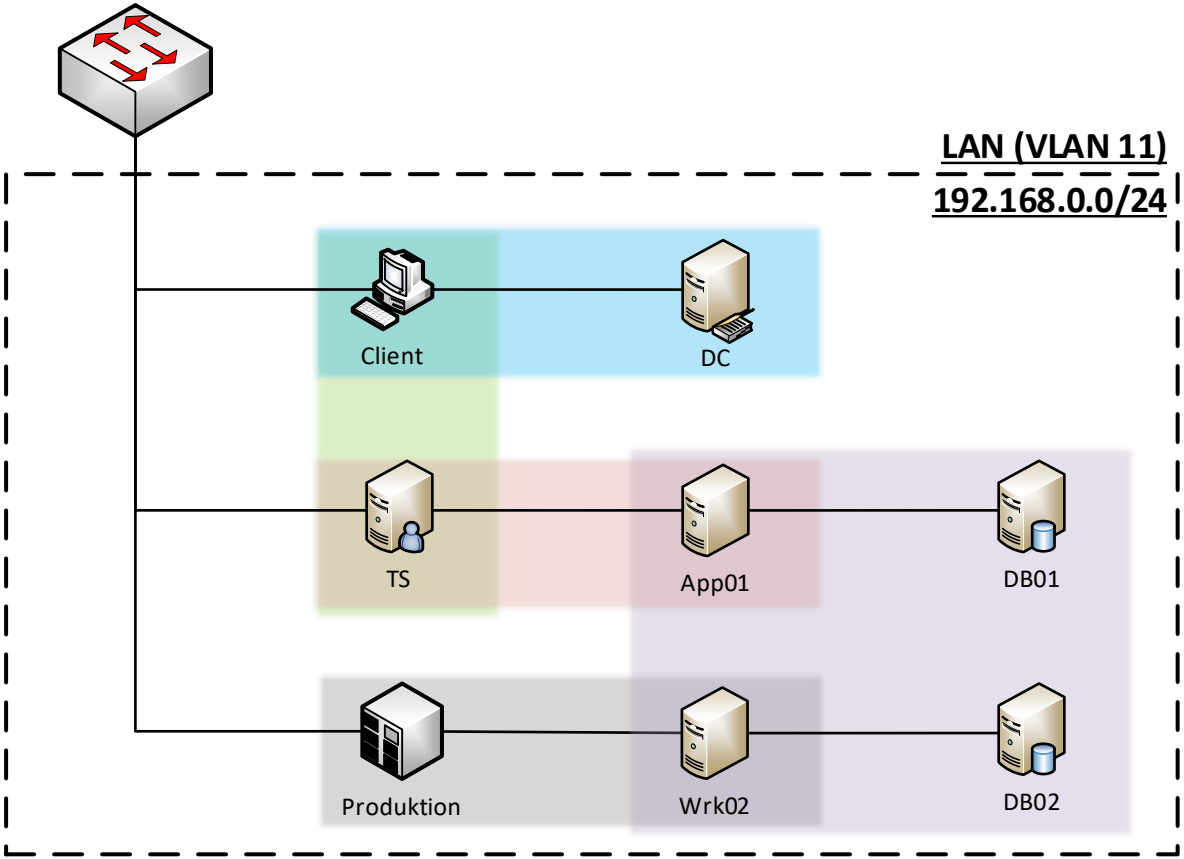
Die Lösung: Mikrosegmentierung

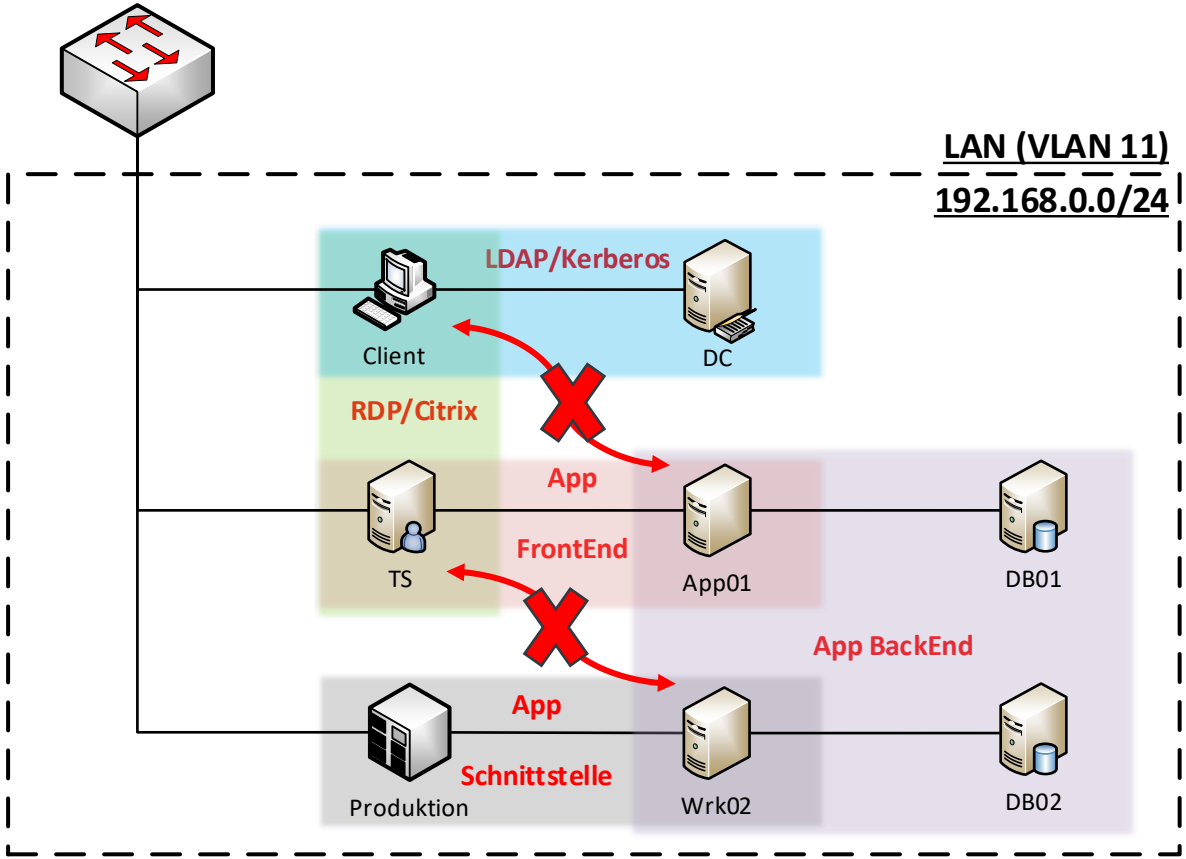
- Weg von klassischen VLANs
- Hin zu einem verwalteten Netzwerk
- (Teil-)Verlagerung der Security von der Firewall auf Netzwerkkomponenten
- Virtualisierung des Netzwerkes

Kurzum: Software defined Network (SdN)


LAN (VLAN 11)
192.168.0.0/24
Client
DC
TS
App01
DB01
Produktion
Wrk02
DB02


LAN (VLAN 11)
192.168.0.0/24
Client
DC
TS
App01
DB01
Produktion
Wrk02
DB02


LAN (VLAN 11)
192.168.0.0/24
Client
DC
TS
App01
DB01
Produktion
Wrk02
DB02


LAN (VLAN 11)
192.168.0.0/24
LDAP/Kerberos
Client
DC
RDP/Citrix
App
FrontEnd
TS
App01
DB01
App BackEnd
App
Schnittstelle
Produktion
Wrk02
DB02

Weitere Vorteile:

- Transparenz im Netzwerk
- „Einfaches“ Management in einer GUI
- Kein Kopfzerbrechen über IP-Netze, VLANs, ACLs
- Skalierung in die Cloud (Public/Private)
- Flowanalyse (Wer mit wem?)
- Transformation von „Nord-Süd“ zur „Ost-West“ Traffic

Fazit: Die Security wächst linear mit den Workloads

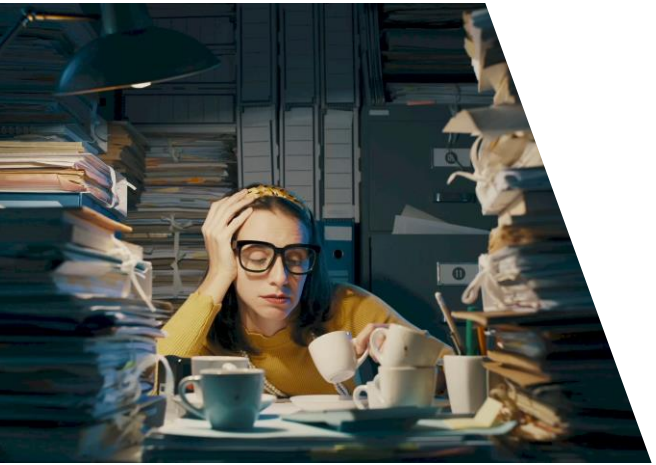
Monitoring & Analytics …
… verbindet ?!

- Klassisches Monitoring kennt man …
  - Hardware (Server Hardware, SAN, NAS, …)
  - Betriebssysteme (Windows, Linux, VMware, …)
  - Anwendungen (AD, SQL, Exchange, …)
  - Geschäftsprozesse

Was ist mit den „Insel“-Daten aus …

- DataCenter Management (SaaS)
- Orchestrierung und Konfiguration-Management
- Firewall Logging / Flowanalyse
- Patchmanagement
- Schwachstellen Scan / CVE Informationen
- Backup

Mögliche Herausforderungen



- Benachrichtigungen aus „Inseln“ sind passiv
- Mehrere Monitoring Lösungen parallel - unterschiedliche Benachrichtigungsschwellen
- Kein Gesamtstatus

Wer behält den Überblick?

Unsere Ziele

- Gesamtstatus erlangen
- Nachvollziehbare Weitergabe an den „Menschen“ (Ticket, Mail, Telefon, …)
- Kontinuierliche und automatische Nachprüfung von gemeldeten Abweichungen und Fehlern

```
Starting Nmap 7.01 ( ht
Nmap scan report for met
Host is up (0.00014s lat
PORT     STATE SERVICE VE
8080/tcp open  http    Or
| http-methods:
|_  Potentially risky meth
|_http-open-proxy: Proxy mi
|_http-server-header: Glass
|_http-title: GlassFish Serv
| vulscan: scip VulDB - http
| [103593] Oracle GlassFish S
| [100159] Oracle Solaris Clu
| [100132] Oracle Retail Open
| [82677] Oracle Solaris Cluste
| [80575] Oracle VM VirtualBox
| [80536] Oracle Retail 4.0/4.1
| [78622] Oracle Communications
| [74879] Oracle iPlanet Web Prox
| [67060] Oracle iPlanet Web Prox
| [11830] Oracle iPlanet Web Proxy
| [11826] Oracle iPlanet Web Proxy
| [5172] Oracle Database 4.0/4.1 Ap
| [59134] Oracle Virtualization 4.0
| [59122] Oracle Database Server 4.0
| [56150] Oracle SunMC 4.0 Web Conso
| [54071] Oracle Sun Java System Web
| [19795] Oracle Application Server 4
| [16934] Oracle Application Server 4.
| [15737] Oracle Web Listener 4.0.7.0.
| [15392] Oracle Application Server 4.0
| [103980] Oracle Hospitality e7 4.2.1
| [103977] Oracle Hospitality Guest Acce
| [103976] Oracle Hospitality Guest Acce
| [103914] Oracle Communications Network
```

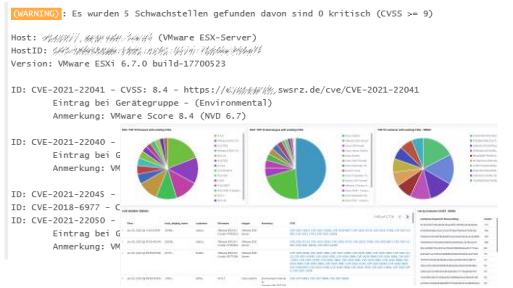
Ansatz: Schwachstellen

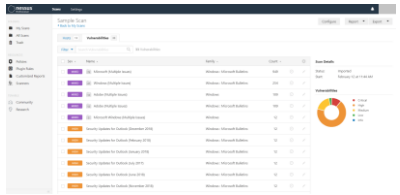
Software
Firmware

VMware ESXi 6.7.0
build-17700523

Vulnerability
Database

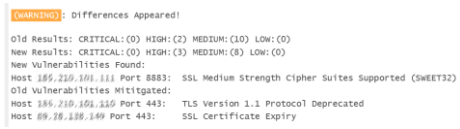
Monitoring Ergebnis



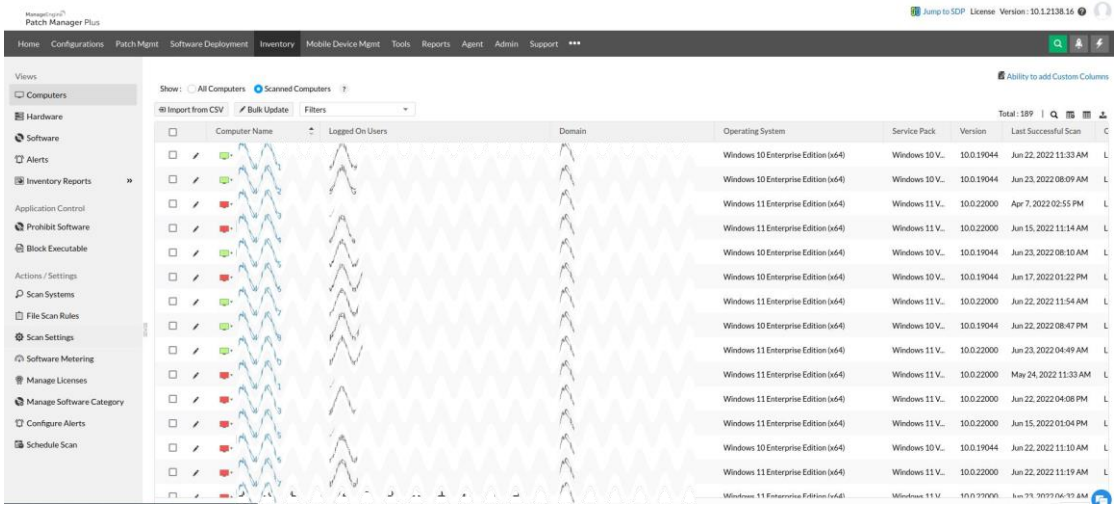


Schwachstellen Scan

Monitoring Ergebnis



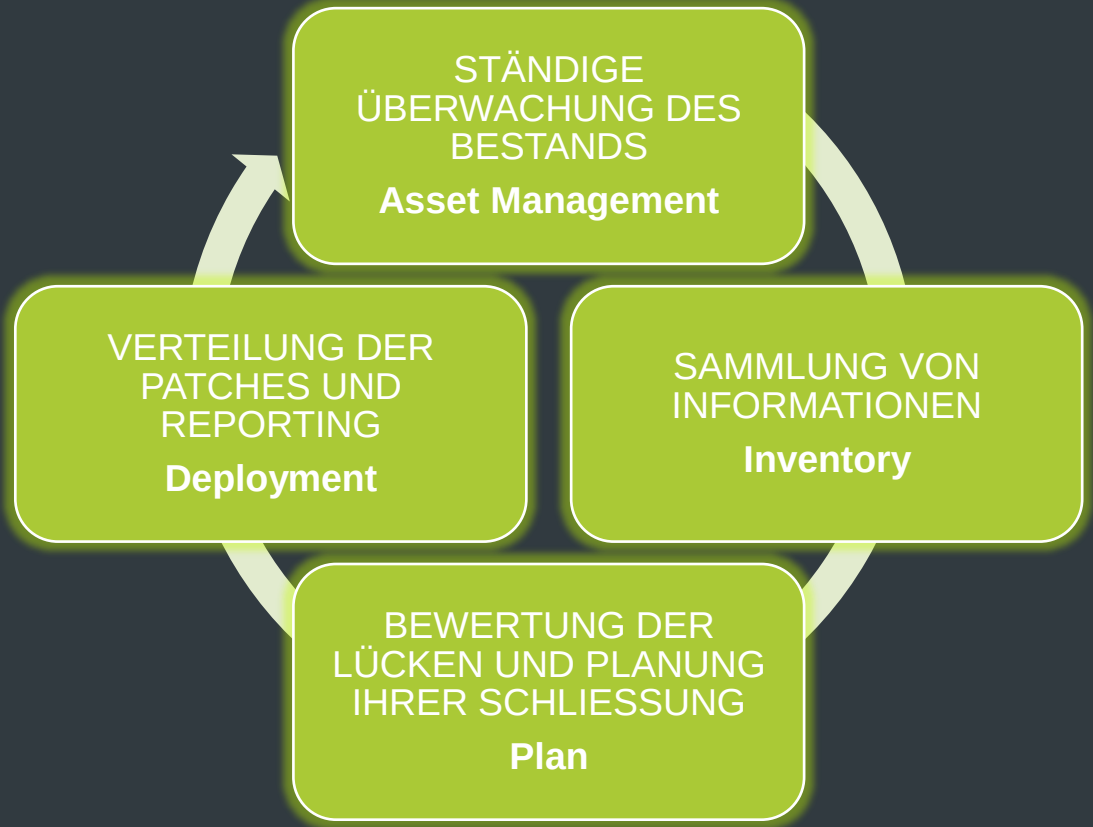
Ansatz: Patch-Management



Was ist Patchmanagement

- Kontrolle über Updates von Betriebssystemen oder Anwendungen
- Eine wichtige Säule in der IT-Sicherheit und des Lifecycle-Managements von IT-Systemen
- Es sollte ein definierter und standardisierter Prozess zur Sicherung der Compliance eines Unternehmens sein
- Es ist ein wichtiger Bestandteil eines jeden Schwachstellenmanagement-Programms (Vulnerability Management)

Schritte Patch-Management



Warum patchen?

Warum patchen Unternehmen nicht oder nur unzureichend…

- Berüchtigte Legacy-Systeme
- Angst vor Ausfällen, die mit der Aktualisierung der Plattform einhergehen könnten
- Keine geeignete Softwarelösung die zur Entlastung beiträgt (viele manuelle Tätigkeiten / WSUS)
- Abhängigkeiten von anderen Systemen

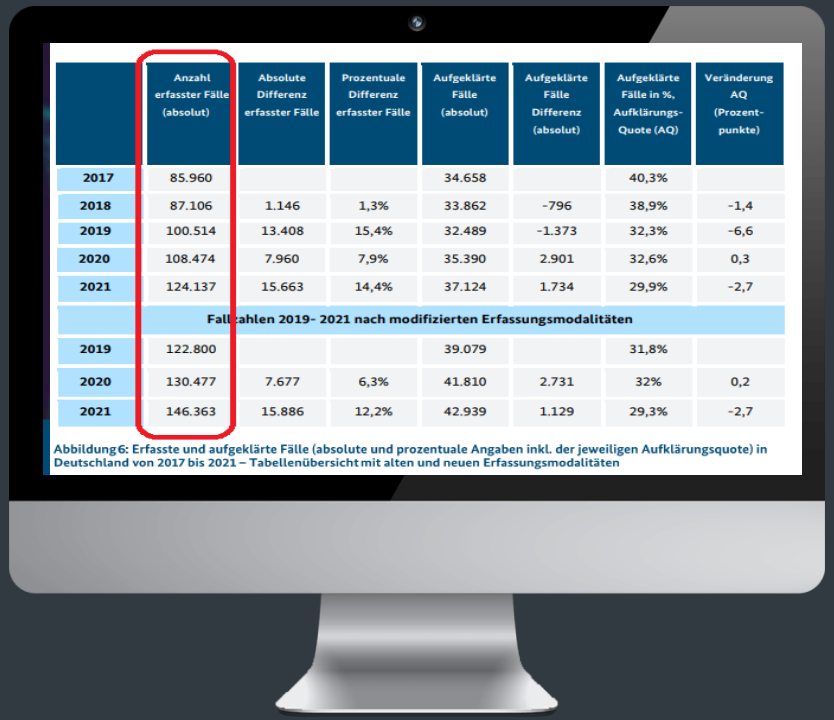
Warum sollte man patchen…

- Sicherheit
- Systemverfügbarkeit
- Compliance (z.B. Versicherungsschutz Cybercrime Versicherungen)
- Funktionsverbesserungen

Es gibt heutzutage **fast** keinen Grund mehr **nicht** zu Patchen

Warum ist *regelmäßiges* patchen wichtiger denn je, jedoch mit Bedacht

- Cybercrimefälle haben sich seit 2015 in Summe mehr als verdreifacht (2015 ~45.000 Fälle | BSI CyberCrime Bundeslagebild 2021)
- Unterschiedliche Plattformen und Anwendungen bieten ein Einfallstor wenn nicht gepatcht
- WannaCry, Exchange Lücke, MSDT Zero-Day-Lücke (Follina), Log4j, ThirdParty Anwendungen uvm…
- Nicht allem muss ein Patch verpasst werden, hier gilt es abzuwägen
- Jedes Unternehmen muss selbst entscheiden, welche der Optionen Situationsbedingt am besten passt, patchen sollte aber die angestrebte Lösung sein.

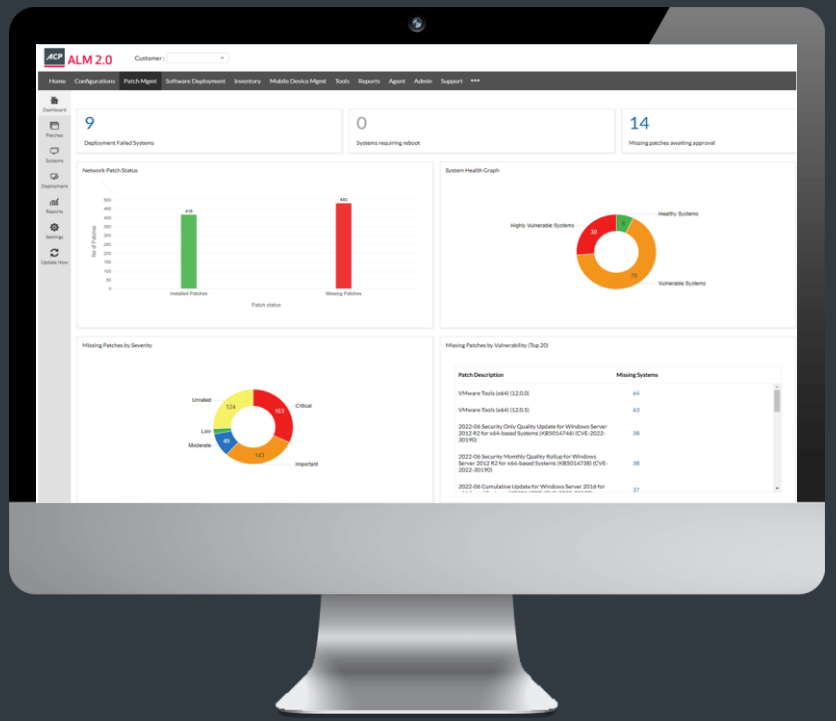


	Anzahl erfasster Fälle (absolut)	Absolute Differenz erfasster Fälle	Prozentuale Differenz erfasster Fälle	Aufgeklärte Fälle (absolut)	Aufgeklärte Fälle Differenz (absolut)	Aufgeklärte Fälle in %, Aufklärungs-Quote (AQ)	Veränderung AQ (Prozent-punkte)
2017	85.960			34.658		40,3%	
2018	87.106	1.146	1,3%	33.862	-796	38,9%	-1,4
2019	100.514	13.408	15,4%	32.489	-1.373	32,3%	-6,6
2020	108.474	7.960	7,9%	35.390	2.901	32,6%	0,3
2021	124.137	15.663	14,4%	37.124	1.734	29,9%	-2,7
	Fallzahlen 2019- 2021 nach modifizierten Erfassungsmodalitäten						
2019	122.800			39.079		31,8%	
2020	130.477	7.677	6,3%	41.810	2.731	32%	0,2
2021	146.363	15.886	12,2%	42.939	1.129	29,3%	-2,7

Abbildung 6: Erfasste und aufgeklärte Fälle (absolute und prozentuale Angaben inkl. der jeweiligen Aufklärungsquote) in Deutschland von 2017 bis 2021 – Tabellenübersicht mit alten und neuen Erfassungsmodalitäten

Patch-Management und Schwachstellenmanagement

- Patch-Management“ und „Schwachstellenmanagement“ werden manchmal als synonym verwendet, es gibt jedoch Unterschiede
- beide Strategien zielen darauf ab, Risiken zu mindern
- Mit Schwachstellenmanagement werden Lücken erkannt, priorisiert und gemeldet
- Mit einem Patch-Management werden diese Lücken zielgerichtet beseitigt
- Beide Systeme zusammen ermöglichen es fundierte und wirksame Entscheidungen zu treffen, Lücken zu schließen und Systeme frühzeitig abzusichern



Automatisieren von Patch-Management

- **WELCHE VORTEILE BRINGT DIE AUTOMATISIERUNG VON PATCH MANAGEMENT?**
  - Erhöhung des IT-Sicherheitsniveaus und der Kosteneffizienz der Unternehmens-IT
  - Mit Automatisierung können Sie häufige Aufgaben vereinheitlichen, manuelle Fehler reduzieren und dafür sorgen, dass sich Ihre Mitarbeiter vermehrt neuen und innovativen Ideen widmen können.
  - Sicherstellen der IT-Compliance und Reporting (Visibilität der Systeme und Anwendungen sowie Reports)
  - Einhalten der Richtlinien, wie empfohlen durch **BSI-Grundschutz** oder die internationale Norm **ISO/IEC 27001** (zeitnahes Einspielen sicherheitsrelevanter Patches und Updates)

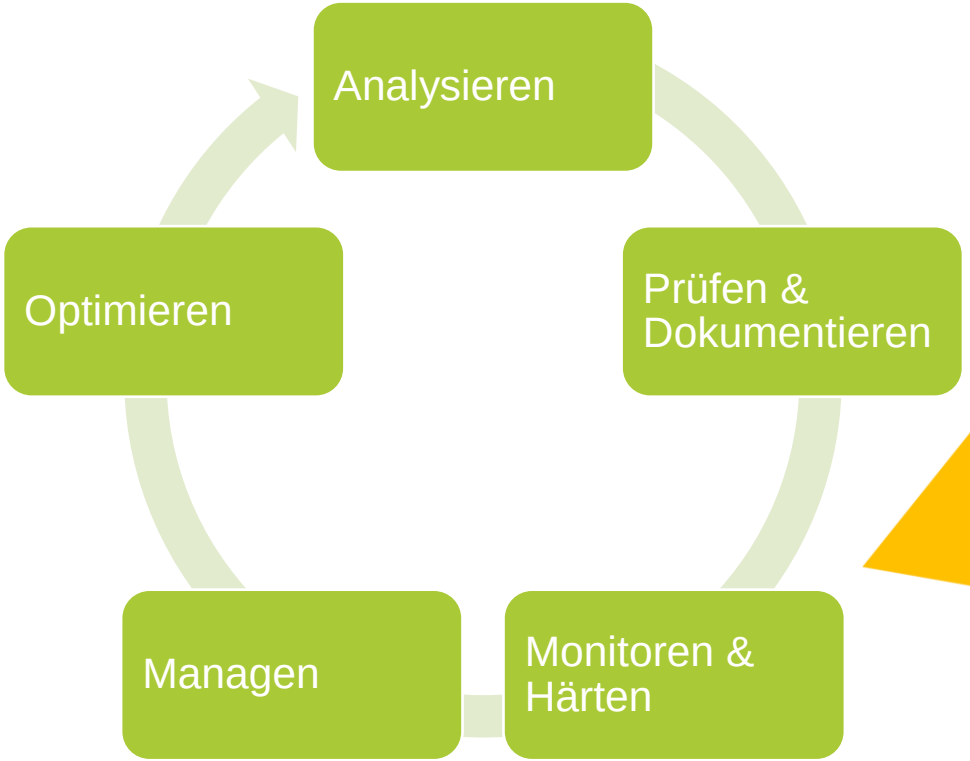
Darüber hinaus ist es nie eine schlechte Idee, ein Drittunternehmen hinzuzuziehen, das Ihnen hilft, Ihr Unternehmen mit einem Patch- und Update-Zeitplan zu unterstützen, der mit Ihrem Geschäftsbetrieb synchronisiert ist.

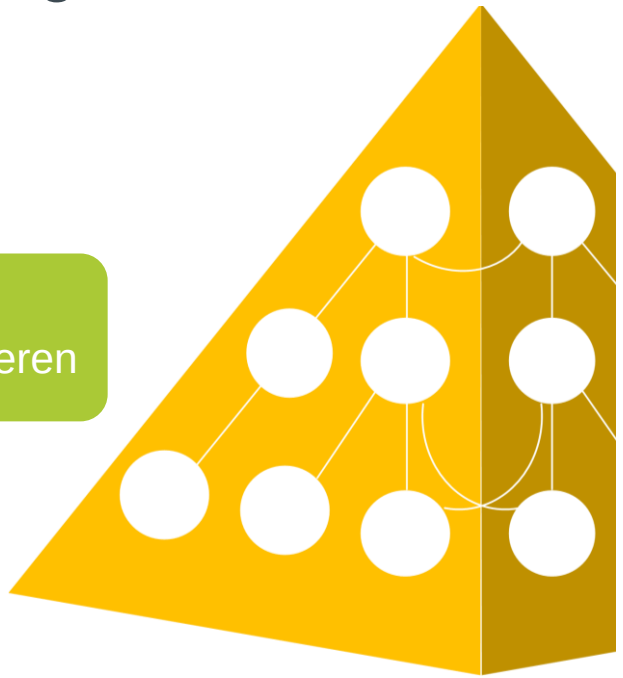
„Wir können Ihnen dabei helfen!“

Besuchen Sie uns am Managed Service Stand und gewinnen Sie eine Teststellung unseres Patch-Managements aus unserem Service-Katalog

Active Directory und Berechtigungsmanagement

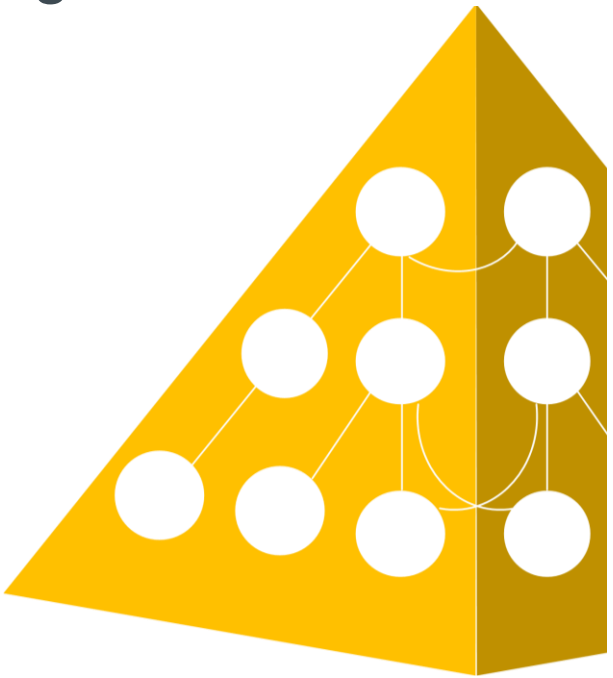
Active Directory und Berechtigungsmanagement





Active Directory und Berechtigungsmanagement

- AD Sicherheit in den Blick rücken – Verantwortlichkeit auch Rechtlich!
  "Know your Backyard" - Kenne Deinen Hinterhof
- Wiederkehrende Prüfungen
  "Perform Security Controls periodically"
- Monitoring und Härten - Berichte für Chef und Prüfer
  "Prove to the management and auditors you are doing something"
- Managen - Wie Effektiv sind meine Maßnahmen
  "Follow the effectiveness of your controls"
- Optimierung – Schritthalten mit aktuellen Bedrohungen
  "Be at the tail of hackers"



Analysieren

Active Directory:

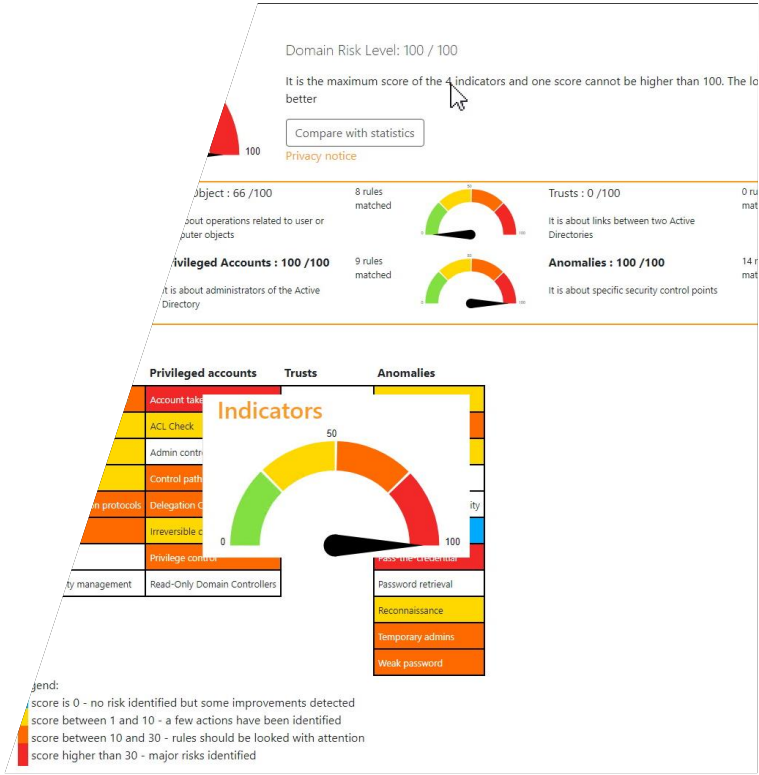
- Design
- Verantwortlichkeiten
- Risikobewertung

Berechtigungsmanagement:

- Ist-Situation dokumentieren
- Berichte zu direkten Berechtigungen, verwaiste Benutzer, verschachtelte Gruppen etc.
- interaktive Suche

Analysetool Active Directory

- Rund 200 Prüfungen gegen das AD
- Bewertung
- Handlungsempfehlungen
- Regelmäßiges Update des Regelsets (2022-06-25)
- Vergleich mit anderen AD
- Vergleich mit früheren Checks - Regelmäßigkeit!



>>> Braucht jeder, der ein AD betreibt – allerwenigstens einmal

Beispiel einer Prüfung mit Handlungsempfehlung

Check the process of registration of computers to the domain

Rule ID:
S-ADRegistration

Description:
The purpose is to ensure that basic users cannot register extra computers in the domain

Technical explanation:
By default, a basic user can register up to 10 computers within the domain. This default configuration represents a security issue as basic users shouldn't be able to create such accounts and this task should be handled by administrators.

Advised solution:
To solve the issue, limit the number of extra computers that can be registered by a basic user. It can be reduced by modifying the value of *ms-DS-MachineAccountQuota* to zero (0). Another solution can be to remove altogether the authenticated users group in the domain controllers policy. Do note that if you need to set delegation to an account so it can add computers to the domain, it can be done through 2 methods: Delegation in the OU or by assigning the *SeMachineAccountPrivilege* to a special group

Points:
10 points if present

Documentation:
https://docs.microsoft.com/troubleshoot/windows-server/identity/default-workstation-numbers-join-domain
http://prajwaldesai.com/allow-domain-user-to-add-computer-to-domain/
http://blog.backslasher.net/preventing-users-from-adding-computers-to-a-domain.html
[MITRE]Mitre Att&ck - Mitigation - User Account Management

The subnet declaration is incomplete [4 IP of DC not found in declared subnets]	*+ 5 Point(s)*
Presence of non-supported version of Windows 10 = 3	*+ 5 Point(s)*
Number of accounts which has never-expiring passwords: 31	*+ 1 Point(s)*

Regelmäßig prüfen und dokumentieren

Active Directory:

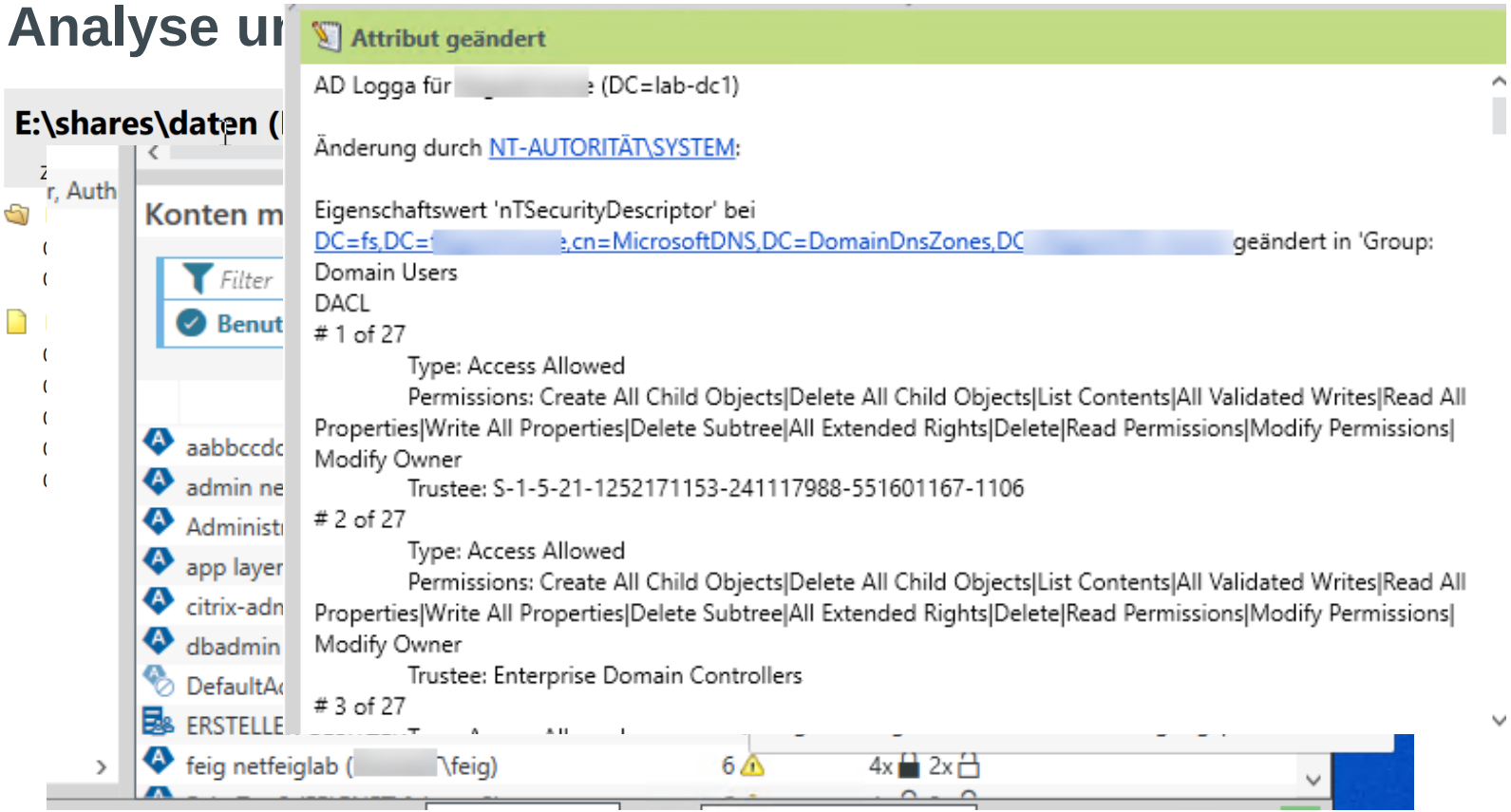
- Leichen im Keller
- AD Verbindungen oder
- bekannte Schwachstellen und Sicherheitsstandards

mit Empfehlungen

Berechtigungsmanagement:

- Erstellung und Löschung von AD Elementen
- privilegiertes Accountmanagement
- Zugriff auf vertrauliche Daten
- aktive Nachfrage beim Datenverantwortlichen

Analyse ur


Attribut geändert
AD Logga für [redacted] (DC=lab-dc1)
Änderung durch NT-AUTORITÄT\SYSTEM:
Eigenschaftswert 'nTSecurityDescriptor' bei
DC=fs,DC=[redacted],cn=MicrosoftDNS,DC=DomainDnsZones,DC[redacted] geändert in 'Group:
Domain Users
DACL
1 of 27
Type: Access Allowed
Permissions: Create All Child Objects|Delete All Child Objects|List Contents|All Validated Writes|Read All Properties|Write All Properties|Delete Subtree|All Extended Rights|Delete|Read Permissions|Modify Permissions|Modify Owner
Trustee: S-1-5-21-1252171153-241117988-551601167-1106
2 of 27
Type: Access Allowed
Permissions: Create All Child Objects|Delete All Child Objects|List Contents|All Validated Writes|Read All Properties|Write All Properties|Delete Subtree|All Extended Rights|Delete|Read Permissions|Modify Permissions|Modify Owner
Trustee: Enterprise Domain Controllers
3 of 27
E:\shares\daten
Konten m
Filter
Benut
aabbccdc
admin ne
Administ
app layer
citrix-adn
dbadmin
DefaultAc
ERSTELLE
feig netfeiglab ([redacted]\feig)
6
4x
2x

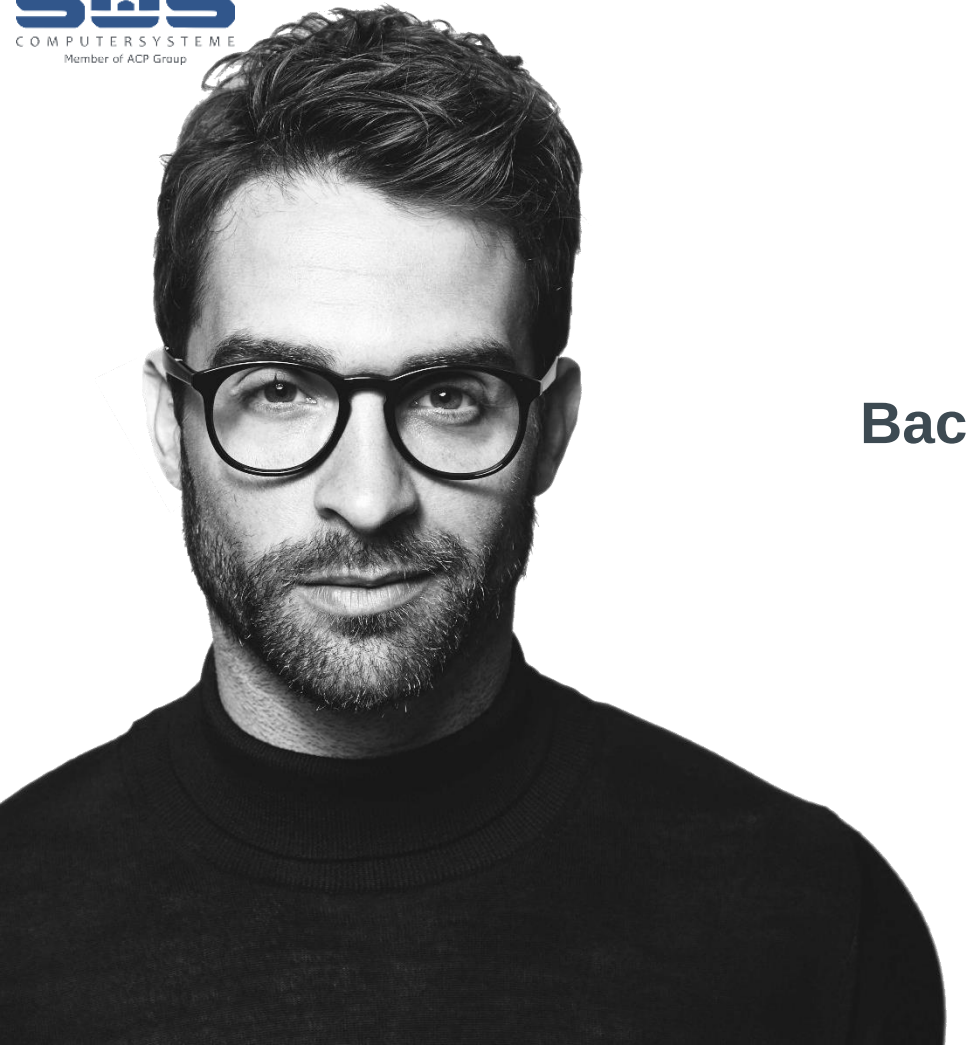
Zusammenfassung

- AD analysieren > Handlungsempfehlungen bewerten und umsetzen - regelmäßige Prüfung

- Berechtigungskonzept mit Rechte- und Rollenkonzept Nachvollziehbarkeit, Berichte und Vereinfachung der Umsetzung mit Tools,
  regelmäßige Prüfung und Monitoring

- Wir bieten Workshops für Umsetzung

SWS COMPUTERSYSTEME
Member of ACP Group



BRAIN SHARE
SWS COMPUTERSYSTEME AG

Backup – Sicher vor Ransomware

IT for innovators.
Member of ACP Group

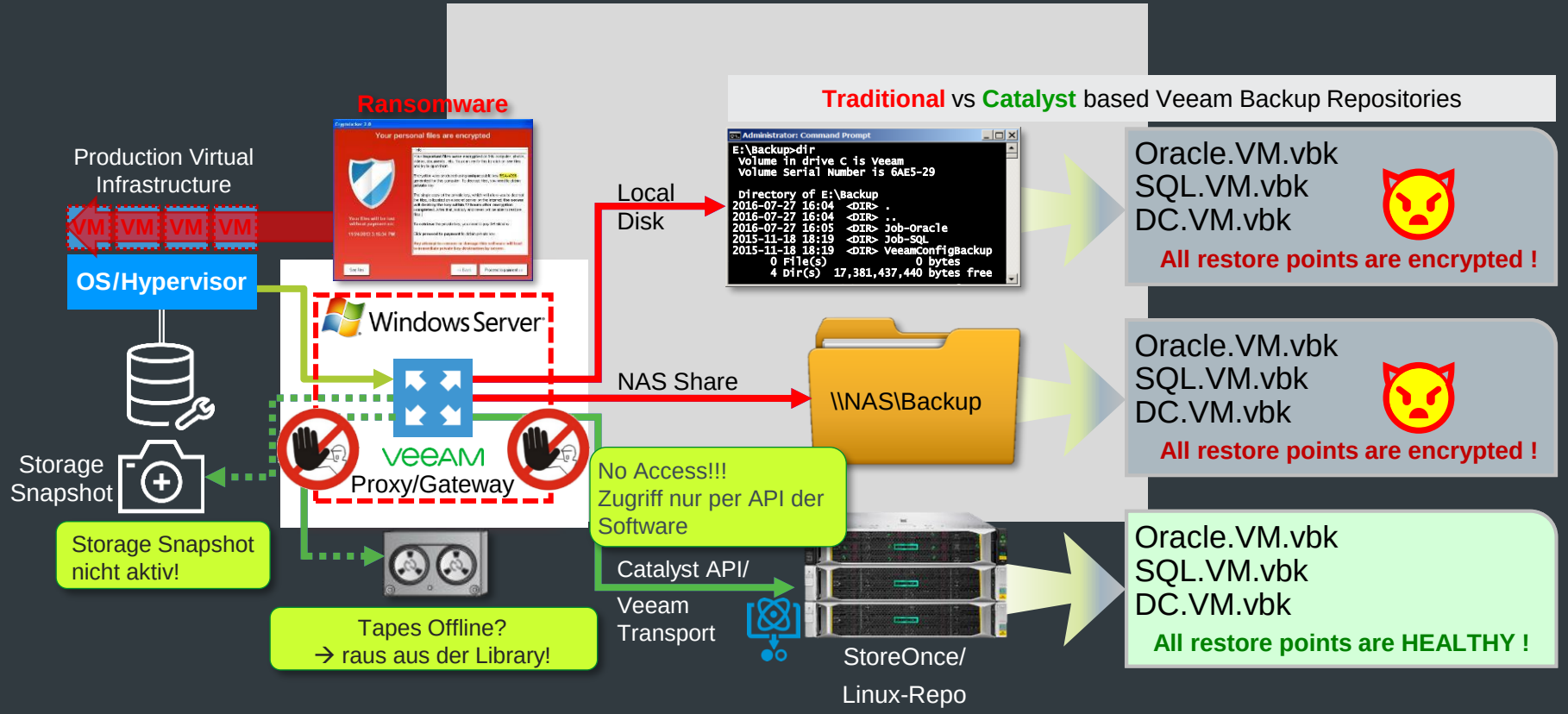
Ja logisch backupen wir!

Aber:
Ist die Umgebung sicher implementiert?

- Vor Datenverlust?
- Vor Angriffen?
- Vor dem eigenen Personal?

Das Backup Repository gegen Angriffe schützen

Das beste Backup nützt nichts, wenn Ransomware das Backup Repository löscht!



Mal nachgedacht:

- Wo steht meine Backupumgebung physikalisch?
- Wie ist meine Umgebung implementiert (IP/VLAN)?
- Wer kommt bis zum Login bzw. der GUI?
- Wer hat darauf Zugriff (Authentifizierung) mit welchen Rechten?
- Wie ist mein Datenfluss?
- Compliance?

Golden-Rule erfüllt: 3-2-1(-1-0)?

3 Kopien – 2 Medien – 1 Medienbruch (– 1 Offline – 0 Fehler)

Wo steht meine Backupumgebung physikalisch?

- Im Serverraum am Standort?
- In einem zweiten Brandabschnitt?
- In einer anderen Filiale/Außenstelle?
- Wer hat Zugang zu den Räumen/Systemen?
- Auslagerung in die Cloud/Tape → Offline?

Wie ist meine Umgebung implementiert (IP/VLAN)?

- Welche Bandbreiten sind vorhanden (Line-Speed)?
- NIC-Teaming möglich/sinnvoll?
- In welchen IP-Netz bzw. VLAN?
- Wo ist dies geroutet (default Gateway)?
- Welche ACLs (Firewall) sind konfiguriert?
- Wann wurden diese das letzte mal geprüft?
- Wo/Wie sind die remote Management-Cards (iLO, CIMC, IPMI, iDRAC, etc.) implementiert?

Wer hat welche Berechtigungen?

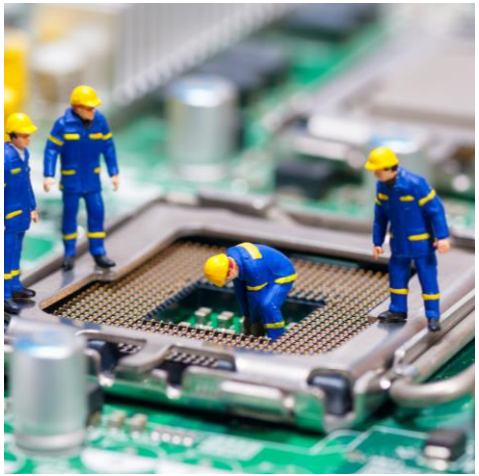
- Wer kommt bis zur GUI, soll er das auch?
- Wer kommt an die Logindaten?
- Wo sind die Logindaten gespeichert (Keylogger)?
- Wogegen wird Authentifiziert (AD/Workgroup)?
- Direkter oder indirekter Zugriff (Jumphost)?
- Gibt es ein (mehrstufiges) Berechtigungskonzept?
- Vieraugenprinzip beim Restore?

Wie ist mein Datenfluss?

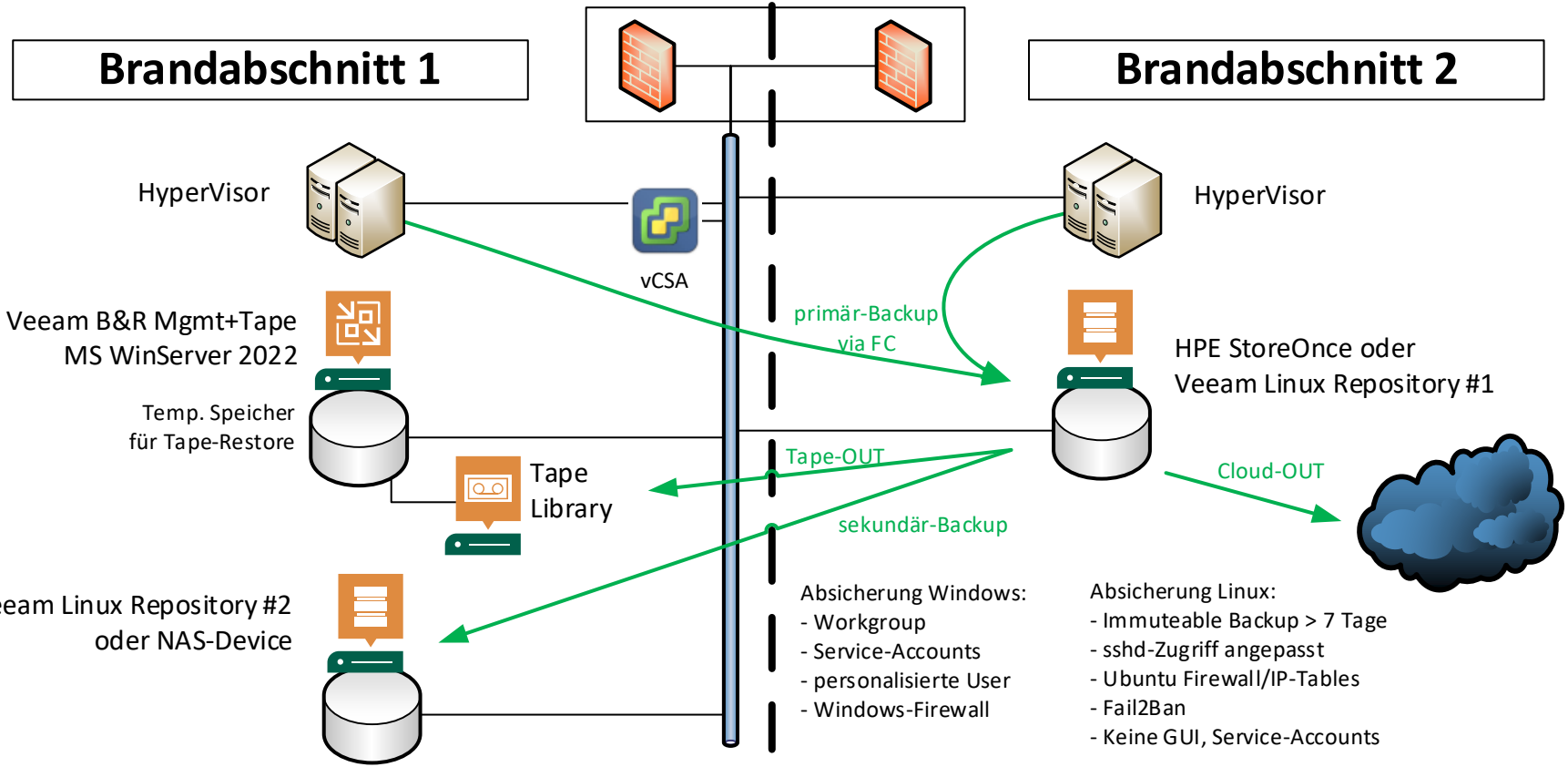
- Läuft dieser optimal?
- Ist die physikalische Anbindung redundant?
- Welche Backupmethode wird verwendet (SAN/HotAdd/NBD)?
- Wie ist der Datenfluss beim Restore?
- Gibt es Bottlenecks wegen der Implementierung (Routing)?
- Wie ist die Infrastruktur eingebunden (DNS bei DR)?
- Welche Bandbreiten sind Richtung Cloud vorhanden?

Compliance – oder die Orga drum herum:

- Prüfung der Backups, DR-Test automatisieren?
- Wer dokumentiert bzw. protokoliert die Ergebnisse?
- Gibt es einen Wiederanlaufplan für den DR-Fall?
- Gibt es rechtliche Vorgaben für Backup/Restore (Versicherung)?
- SLAs für Vorhaltezeiten (GFS)?
- „Plan-B“ für verschlüsselte Backups (wo ist das Passwort)?
- Automatische Alarmierung bei Anomalien (Ransomware)?
- Einhaltung des Backupfensters (RPO) und Wiederherstellungszeiten (RTO)?



So kann eine (Veeam-) Umgebung am Ende aussehen:



Coming soon: SWS BackupVault

Der Ransomeware-Sichere Backuptresor der SWS

- Mehrstufiges Security-Konzept
- ManagedService
- Laufzeit 60 Monate
- Kapazität von 16 TB bis 128 TB Netto-Kapazität
- Anbindung per 1 Gbit/sec oder 10 Gbit/sec
- geschlossene BlackBox incl. Monitoring

Die SWS kann helfen!

- Disruptive IT
- Cloud Management
- Netzwerksegmentierung und Flowanalyse
- Berechtigungsmanagement
- Patchmanagement
- Monitoring und Analytics
- Backup – sicher vor Ransomware