Sicherheitsauditreport

Dieser Bericht ergänzt die vorhandene Netzwerkinfrastruktur-Dokumentation und führt weitere Punkte auf, die bisher nur unzureichend oder gar nicht behandelt wurden.

Testing

Interner Netzwerkscan

- Tools: Nmap
- Zweck: Erkennen offener Ports und Dienste im internen Netz, Identifizierung möglicher Schwachstellen und Fehlkonfigurationen.
- Ergebnis: Aufzeigen unbeabsichtigter Freigaben, Dienste und Ports, die das Risiko erhöhen können.

Social-Engineering-/Phishing-Tests

- Tools: Security Awareness Program (Securepoint, kommerziell)
- Zweck: Überprüfung der „Human Firewall“ – wie sensibel reagieren Mitarbeitende auf gefälschte E-Mails oder Links.
- Ergebnis: Erkennen, ob Schulungen wirken oder ob noch Lücken im Bewusstsein für IT-Sicherheit bestehen.

Log-Review & SIEM-Check

- Tools: Graylog
- Zweck: Zentrale Analyse, Korrelation und Alarmierung bei sicherheitsrelevanten Ereignissen.
- Ergebnis: Frühzeitige Erkennung von verdächtigen Aktivitäten, automatisierte Meldungen bei Anomalien.

Backup- und Restore-Tests

- Tools: Je nach eingesetzter Backup-Software (z. B. Veeam, Bacula, Acronis) oder manuelle Tests
- Zweck: Überprüfung, ob Daten tatsächlich vollständig und konsistent wiederhergestellt werden können.
- Ergebnis: Sicherstellung, dass das Backup-Konzept in der Praxis funktioniert (Zeitaufwand, Integrität, Vollständigkeit).

Fehlende Informationen

1. **Berechtigungsmatrix**
    - Die Gruppenstruktur ist grob beschrieben, jedoch fehlt eine genaue Übersicht, welche Abteilungen bzw. Rollen Zugriff auf welche Ressourcen (Dateien, Anwendungen) haben.
2. **BYOD-Richtlinie**

- Die Dokumentation enthält keine Policy zum Umgang mit privaten Geräten (Smartphones, Tablets etc.), die ggf. im Unternehmensnetzwerk verwendet werden.

3. **Virtualisierungs- und Applikationsserver-Konzept**
    - Es wird nicht erwähnt, welche Virtualisierungsplattform im Einsatz ist (z. B. Proxmox, Microsoft Hyper-V Cluster) und ob dedizierte Applikationsserver existieren.
4. **Detaillierte Backup-Prozesse**
    - Der grobe Ablauf (ZFS-Snapshots, externe Festplatten, Offsite) ist bekannt, doch Tools, Zeitpläne und Verantwortlichkeiten sind unklar.
5. **Dokumentation von Recovery-Tests**
    - Es ist nicht festgehalten, ob und wie regelmässig Wiederherstellungstests durchgeführt werden.
6. **Switches und Router**
    - Es fehlen Informationen zu Marke, Modell, Portanzahl, Kapazitäten und möglicher Redundanz am zweiten Standort.
7. **VLAN- und IP-Adressierung**
    - VLANs sind zwar benannt, jedoch fehlen konkrete IP-Bereiche.
8. **Wartungsfenster und Patch-Strategie**
    - Eine Wartung für die Server, Clients und aktiven Komponenten bezüglich OS- und Firmware-Updates (Server, Firewall, Switches, Router) ist nicht festgehalten.

Optional

9. **USV-Kommunikation und Standort Basel**
    - Keine Information, ob in Basel überhaupt eine USV vorhanden ist und ob dort eine Absicherung gewünscht ist.
10. **Fehlender Failover-Router in Basel**

- Die Dokumentation sagt nichts darüber aus, warum am Standort Basel kein redundanter Router (Failover) vorhanden ist.

11. **IPsec-Konfiguration**

- Es ist nicht ersichtlich, welchen SHA-Wert bzw. IPsec-Modus (z. B. IKEv1 oder IKEv2, Phase1/Phase2-Parameter) die VPN-Verbindung nutzt.

12. **Bandbreiten im LAN**

- In der Dokumentation fehlt eine konkrete Angabe zu den verfügbaren Bandbreiten innerhalb des LAN (z. B. 1 Gbit/s, 10 Gbit/s).
- Auch das Netzwerkdiagramm gibt keinen Aufschluss, ob z. B. zwischen Servern und Switches 10 Gbit/s-Verbindungen bestehen.

13. **Badge-Ausgabe und On-/Offboarding**

- Es ist nicht beschrieben, wie Badges beim Eintritt und Austritt von Mitarbeitenden verwaltet werden (z. B. Ausgabe, Sperrung).

14. **Auswertung von Zutritts- und Kameraprotokollen**

- Es gibt keine klaren Vorgaben, wie Zutritte oder Kameraaufzeichnungen analysiert werden, wer dies tut und in welchen Abständen.
- Fehlende Angaben zum Anbiter der Badges, wie und wo diese administriert werden.

15. **Spezifikationen zu Server-Hardware und Performance**

- Weder Anzahl der CPU-Kerne und -Modelle noch die Art der Überwachung (Performance-Monitoring) sind aufgeführt.

16. **Firewall-Hardware**

    - Die Dokumentation nennt keine Marke, kein Modell und keine Angabe zur Leistung (z. B. Durchsatz).

17. **WLAN**

    - Eine klare Vorgehensweise zur möglichen Einführung von (Gast-)WLAN oder der Umgang mit Smartphones ist nicht dokumentiert.

18. **VPN-Konfiguration**

    - Ob Full-Tunnel oder Split-Tunneling eingesetzt wird, wie Schlüssel verwaltet und rotiert werden und ob Zertifikate zum Einsatz kommen, ist offen.
    - Details zum IPsec-Hashing (SHA-Wert) und Modus (Phase1/2) sind ebenfalls nicht vorhanden.

19. **Passwortmanager**

    - Es wird zwar ein Passwortmanager erwähnt, aber nicht, welcher Anbieter genutzt wird, ob er On-Premise oder in der Cloud betrieben wird und ob eine 2FA-Absicherung existiert.

Konkrete Schwachstellen und Massnahmen

1. **Fehlende Firewall-Regeltabelle**
    - Schwachstelle: Unvollständig dokumentierte Paketfilterregeln können dazu führen, dass der Überblick nicht mehr gewährleistet ist und sich dadurch Fehler einschleichen können.
    - Massnahme: Einführung einer ausführlichen Firewall-Regeltabelle mit Angaben zu Quelle, Ziel, Port, Aktion (Allow/Deny/Drop) und verpflichtendes Logging bei kritischen Regeln. Zusätzlich Dokumentation von Hersteller, Modell und Leistungsdaten.
2. **Fehlende BYOD-Richtlinie**
    - Schwachstelle: Private Geräte könnten ohne Sicherheitsmassnahmen (z. B. MDM) ins Netzwerk eingebunden werden und Malware oder Datenlecks verursachen.
    - Massnahme: Ausarbeitung eines BYOD-Konzepts, das sowohl Sicherheitsanforderungen (Verschlüsselung, Virenschutz) als auch Nutzungsbedingungen (Netzwerksegmentierung, Zugriffsrechte) regelt.
3. **Keine Planung für Gast-WLAN oder Smartphone-Zugänge**

- Schwachstelle: Da kein WLAN vorhanden ist, ist unklar wie Gäste und deren Geräte, sowie die Smartphones oder Tablets der Mitarbeiter behandelt werden.
- Massnahme: Erstellung eines WLAN-Konzepts, um auch ein sicherer Umgang mit Mobilgeräten von Mitarbeiter und Gastgeräten zu gewährleisten oder eine Begründung dokumentieren, weshalb keine Wireless Lösung realisiert wird, damit nicht versehntlich doch eines aus Unwissenheit erstellt wird.

4. **Fehlende Berechtigungsmatrix**
    - Schwachstelle: Ohne konkrete Zuordnung von Abteilungen zu Ressourcen können sich “zu weitgehende” oder “zu eingeschränkte” Berechtigungen einschleichen.
    - Massnahme: Erstellung einer Tabelle, in der jede Abteilung/Rolle den jeweiligen Freigaben (Lese-, Schreibrechte etc.) zugeordnet ist. In regelmässigen Abständen reviewen.
5. **Unrealistische SSD-Kapazitäten und fehlende ZFS-Redundanz**
    - Schwachstelle: Mit je einer Festplatte pro Z-Pool ist keine Ausfallsicherheit garantiert.
    - Massnahme: Überprüfung der tatsächlichen Speichermedien. Einführung eines redundanten ZFS-Konzepts (Mirror oder RAID-Z), um Ausfallsicherheit zu gewährleisten.

    HINWEIS:
    40TB oder 60TB SSD sind sehr unrealistisch.

6. **Backup-Lagerung auf separatem Host**
    - Schwachstelle: Backups werden zwar nicht auf demselben Medium gelagert, jedoch fehlt ggf. ein eigener Host für Sicherungen. Monats-/Jahressicherungen nur auf externen Medien zu haben, ist riskant.
    - Massnahme: Einrichtung eines dedizierten Backup-Servers (ggf. an einem externen Standort) und häufigere Offsite-Sicherungen, um Daten bei einem Brand oder Diebstahl am Hauptstandort zu schützen.
7. **Unvollständige oder unklare USV-Abdeckung**
    - Schwachstelle: Der Standort Basel scheint ohne USV-Schutz zu sein, was bei Stromausfällen zum Systemausfall führen kann.
    - Massnahme: Evaluierung, ob eine USV in Basel implementiert werden sollte. Zudem klären, ob die USV in Zug über SNMP/Netzwerkschnittstelle überwacht und ggf. gesteuert werden kann.
8. **Fehlende Wartungs- und Patch-Strategie**
    - Schwachstelle: Netzwerktechnik und Server können ungepatcht bleiben und dadurch bekannte Sicherheitslücken aufweisen.
    - Massnahme: Einrichtung fester Wartungsfenster (z. B. monatliche Server-Patches, quartalsweise Firmware-Updates), klare Kommunikation an alle Betroffenen im Unternehmen.

Optional

9. **Fehlender Failover-Router in Basel**

- Schwachstelle: Bei einem Routerausfall (oder Ausfall des Internetanschlusses) ist der Standort Basel abgeschnitten.
- Massnahme: Anschaffung oder Konfiguration eines zweiten Routers als Failover-Lösung, um eine Failoverleitung zu schaffen.

10. **Fehlende IPsec-Parameter (SHA-Wert, Modus)**

- Schwachstelle: Ohne klar definierte und dokumentierte Crypto-Parameter für IPsec kann es zu schwächeren Sicherheitseinstellungen oder Inkompatibilitäten kommen.
- Massnahme: Festlegung der genauen IPsec-Einstellungen (z. B. SHA256, AES-256-GCM) und Dokumentation, damit die VPN-Sicherheit transparent und überprüfbar ist.

11. **Unbekannte LAN-Bandbreiten**

- Schwachstelle: Mögliche Performance-Engpässe oder Fehlplanungen, da unklar ist, ob 100 Mbit/s, 500 Mbit/s, 1 Gbit/s oder 10 Gbit/s genutzt wird.
- Massnahme: Erfassung des physischen Aufbaus (Switches, Kabel, Ports), Dokumentation der tatsächlichen Netzwerkbandbreite zwischen Hosts, Servern und Switches. Zumindest im Netzwerkdiagramm sollten diese Informationen ersichtlich sein.

12. **Mangelnde Protokollierung und Auswertung von Kamera- und Zutrittsdaten**
    - Schwachstelle: Ein Vorfall lässt sich nicht lückenlos nachvollziehen, wenn nicht klar ist, wer und wann Zutritte oder Kameraaufnahmen überprüft.
    - Massnahme: Festlegen von Verantwortlichkeiten und Intervallen für die Auswertung von Protokollen sowie das Definieren von Löschfristen und Datenschutzrichtlinien.

13. **Unklare oder fehlende Aktivkomponenten-Redundanz**

- Schwachstelle: Schlecht dokumentierte Switches und Router erleichtern unbefugte Zugriffe (z. B. offene Ports, fehlende Redundanz). Am Standort Basel fehlen failover-fähige Komponenten.
- Massnahme: Detaillierte Erfassung aller Switches (Marke, Modell, Firmware-Version), Port-Übersichten und Einrichtung eines Router-Failoversystems in Basel.

14. **Unklarer VPN-Betrieb**

- Schwachstelle: Unzureichende Dokumentierung der Authentifizierungs- und Verschlüsselungsmethoden erhöhen das Risiko einer Fehlkonfiguration.
- Massnahme: Dokumentation der VPN-Settings (Full-Tunnel oder Split-Tunnel, AES-256, SHA256 etc.) und ein Prozess für regelmässige Schlüsselrotation. Hierbei ggf. auf Bridge-Mode (PPPoE) setzen, um doppelte Firewalls zu vermeiden, sofern das Konzept es erlaubt.

15. **RAM-Anforderungen für ZFS**

- Schwachstelle: ZFS kann bei grossen Speichermengen (z. B. 120 TB) sehr RAM-intensiv sein (mindestens 1 GB pro TB, ggf. 1,5 GB pro TB). Es bleibt möglicherweise nicht genug RAM für VMs.
- Massnahme: Prüfen, ob die physischen Hosts über genügend RAM für den ZFS-Cache verfügen, oder die Storage-Kapazität anpassen bzw. aufteilen.