IT-Infrastruktur Dokumentation

Einleitung

Diese Dokumentation gibt einen umfassenden Überblick über die IT-Infrastruktur eines Unternehmens mit zwei Standorten und insgesamt 25 Mitarbeitenden. Sie beschreibt die eingesetzte Technik, die Systemkonfiguration sowie die organisatorischen und sicherheitstechnischen Richtlinien. Darüber hinaus dient sie als Nachschlagewerk für Administratoren, Auditoren und Entscheidungsträger. Im Rahmen eines Sicherheitsaudits wurden bestehende Schwachstellen analysiert, fehlende Punkte identifiziert und entsprechende Massnahmen berücksichtigt oder ergänzt.

1. Zusammenfassung

Die IT-Infrastruktur des Unternehmens ist durch den Aufbau zweier Standorte (Bern und Biel), einer umfassenden Cloud-Integration (TERRA Cloud), sowie klar definierten Sicherheits- und Organisationsrichtlinien auf einem hohen Niveau. Im Folgenden werden die wichtigsten Aspekte und Neuerungen zusammengefasst:

1.1 Infrastruktur & Hardware

- Zwei Standorte (Bern und Biel) plus Cloud-Anbindung**: Standortübergreifende Hochgeschwindigkeits-Vernetzung (10 Gbit/s) mit Backup-Leitung (1 Gbit/s), um Ausfälle abzufedern.
- Redundante Komponenten: Zugangsbeschränkte EDV-Räume, USV-Systeme zur Überbrückung kurzzeitiger Stromausfälle und strukturierte Server-Räume mit Racks.
- Zentrale Cloud-Umgebung: Virtuelle Server in der TERRA Cloud mit eigenem Backup-Brandabschnitt und zusätzlicher Sicherung in der Hetzner-Cloud.

siehe Kapitel: Infrastrukturübersicht; Server; Backup

1.2 Server, Virtualisierung & Backup

- Aktuelle Betriebssysteme: Windows Server 2022 Standard für Domänen-Controller, Datei- und Applikationsserver; Exchange Server 2019 für E-Mails.
- Mehrstufiges Backup-Konzept nach dem 3-2-1-Prinzip:
    1. TERRA Cloud (Primär-Backup)
    2. NAS in Bern (Lokale Kopie)
    3. Veeam-Backup bei Hetzner (Geografische Redundanz)
- Regelmässige Tests & DR-Plan: Die Wiederherstellung wird jährlich geübt, und der Desaster Recovery Plan (DRP) definiert konkrete Massnahmen für Priorisierung, RTO (4 Stunden für kritische Systeme) und RPO (maximal 12 Stunden Datenverlust).

siehe Kapitel: Server; Backup

1.3 Netzwerk & Sicherheit

- OPNSense-Firewalls an jedem Standort mit restriktiven Regeln und Failover-Logik für die Internetanbindung. In der Cloud-Umgebung wird eine virtuelle Securepoint-Firewall eingesetzt.
- WireGuard-VPN: Site-to-Site- und End-to-Site-Verbindungen (Roadwarrior) für einen sicheren Zugriff auf interne Ressourcen.
- Managed Unifi Switches und Access Points: Zentrales Management über Unifi-Controller, deaktivierte ungenutzte Ports, geplante Einführung von VLAN-Segmentierung (feingranular) und 802.1X für Port-Sicherheit.
- Passwort-Management: Self-hosted Bitwarden für alle Mitarbeitenden, um Zugriffsberechtigungen zentral zu steuern und Passwörter sicher zu verwalten.

siehe Kapitel: Netzwerk und aktive Komponenten; Organisatorische Richtlinien

1.4 Clients & Benutzerverwaltung

- Keine BYOD: Jeder Mitarbeitende erhält ein firmeneigenes, persönlich zugewiesenes Notebook, strikt von privaten Geräten getrennt.
- Active Directory: Zentrale Verwaltung von Benutzern, Gruppen und Policies. Feingranulare Rechte- und Freigaben auf dem Fileserver.
- Regelmässige Schulungen (Security Awareness): Schulungen zu Phishing-Erkennung, Passwort- und Datenumgang; ergänzend laufende Phishing-Simulationen mit Securepoint zum Testen der Mitarbeiter-Sensibilität.

siehe Kapitel: Benutzerverwaltung; Benutzermatrix und Berechtigungsmatrix

1.5 Prozesse, Compliance & Monitoring

- Change Management: Änderungen an Firewall-Regeln, Serverkonfigurationen oder Nutzerberechtigungen werden in einem Änderungsprotokoll dokumentiert und einem Freigabeprozess (4-Augen-Prinzip) unterzogen.
- Monitoring mit Zabbix: Zentrale Überwachung von Servern, Netzwerken und Firewalls mit Alarmierung bei kritischen Zuständen.
- ISMS in Vorbereitung: Aufbau eines Information Security Management Systems nach ISO 27001-Standards ist in Planung. Regelmässige Penetrationstests und Sicherheitsaudits sollen fortlaufend stattfinden.

siehe Kapitel: Organisatorische Richtlinien

2. Infrastrukturübersicht

2.1 Standorte

- **Bern** (Hauptsitz)
- **Biel** (Zweigstelle)
- **TERRA Cloud**
- **Hetzner Cloud**

Alle Standorte (ausgenommen Hetzner Cloud) sind mittels eines Site-to-Site VPN (WireGuard) miteinander verbunden und verfügen jeweils über eine 10 Gbit/s Internetanbindung.

2.2 EDV Raum und Rack

- An jedem Standort befindet sich ein RFID-Badge zugangsbeschränkter EDV Raum.
- Zugriffskontrolle erfolgt über Unifi Access Door und Unifi Controller auf dem APP-Server.
- Es steht jeweils ein Racks zur Verfügung, in dem sich der Router, Firewall und Core Switch befinden.
- Um einen Unterbruch durch kurze Stromausfälle zu verhindern, ist eine kleine USV mit Netzkarte im Rack verbaut.
- Am Standort Bern steht zusätzlich ein NAS für Backups.

Anpassung nach Sicherheitsaudit

Rauchmelder, Feuerlöscher und Löschdecken werden installiert bzw. zu Verfügung gestellt. Es werden jährliche Brandschutzinspektionen durchgeführt. Es werden alle Mitarbeitende über die neuen Massnahmen informiert.

2.3 ISP (Internet Service Provider)

Jeder Standort ist mit einem 10 Gbit/s Init7-Internetzugang angebunden, um eine zuverlässige und performante Verbindung zu gewährleisten. Als Backup-Leitung dient ein 1 Gbit/s Internetzugang von Solnet, der automatisch umschaltet, falls die Hauptleitung ausfällt. Die Konfiguration der Failover-Logik wird von den OPNSense-Firewalls übernommen, sodass ein unterbrechungsfreier Betrieb sichergestellt ist.

Die Solnet-Leitung bietet ausreichende Kapazität für alle kritischen Dienste und wird regelmässig getestet, um die Funktion des Failover-Mechanismus sicherzustellen.

2.4 Client-Device / BYOD

Im Geschäftsbetrieb kommen ausschliesslich firmeneigene Notebooks zum Einsatz, die jedem Mitarbeitenden persönlich zugewiesen werden. Die Nutzung privater Geräte (BYOD) ist aus Sicherheits- und Compliance-Gründen nicht gestattet.

3. Netzwerk und aktive Komponenten

3.1 Netzwerkarchitektur

- Das Netzwerk ist sternförmig aufgebaut, wobei möglichst alle Geräte über zentrale Switches im Serverraum miteinander verbunden sind.

3.2 Firewall

- An jedem Standort wird eine OPNSense-Firewall eingesetzt.
- In der TERRA Cloud Umgebung wird eine virtuelle Appliance von Securepoint genutzt.
- Die Konfiguration ist sehr restriktiv, es werden nur die wirklich benötigten Ports freigegeben.
- Eine Tabelle mit den wichtigsten Firewall-Regeln:

Firewall-Regeln für den Standort Bern

Regel-ID	Quelle	Ziel	Port/ Protokoll	Erlaubt/ Verweigert	Kommentar
FW-001	Internal-Network Bern	VPN-Net-Terra-Cloud	53 (UDP/TCP)	Erlaubt	DNS-Anfragen an die Domain Controller in der Cloud
FW-002	Internal-Network Bern	VPN-Net-Terra-Cloud	67-68 (UDP)	Erlaubt	DHCP-Anfragen an die Domain Controller in der Cloud
FW-003	Internal-Network Bern	VPN-Net-Terra-Cloud	445 (TCP)	Erlaubt	SMB-Verbindungen von Bern zur Cloud
FW-004	Internal-Network Bern	VPN-Net-Terra-Cloud	853 (TCP)	Erlaubt	DNS-Anfragen über DNS-over-TLS an die Cloud-DCs
FW-005	Internal-Network Bern	VPN-Net-Terra-Cloud	5514, 8080, 3478 (TCP/UDP)	Erlaubt	Unifi-Kommunikation von Bern zur Cloud
FW-006	VPN-Net-Terra-Cloud	Internal-Network Bern	22 (TCP)	Erlaubt	SSH-Verbindungen von der Cloud zu Bern
FW-007	VPN-Net-Terra-Cloud	Internal-Network Bern	51821 (UDP)	Erlaubt	WireGuard S2S VPN von der Cloud zu Bern
FW-008	VPN-Net-Terra-Cloud	Internal-Network Bern	8 (ICMP)	Erlaubt	ICMP Echo-Request von VPN-Net-Terra-Cloud zu Bern
FW-009	VPN-Net-Terra-Cloud	Internal-Network Bern	5514, 8080, 3478 (TCP/UDP)	Erlaubt	Unifi-Kommunikation von der Cloud nach Bern
FW-010	Internal-Network Bern	VPN-Net-Biel	51821 (UDP)	Erlaubt	Site-to-Site WireGuard VPN zu VPN-Net-Biel
FW-011	Internal-Network Bern	VPN-Net-Biel	8 (ICMP)	Erlaubt	ICMP Echo-Request von Bern zu VPN-Net-Biel
FW-012	VPN-Net-Biel	Internal-Network Bern	8 (ICMP)	Erlaubt	ICMP Echo-Request von VPN-Net-Biel zu Bern
FW-013	Internal-Network Bern	Internet	443 (TCP)	Erlaubt	HTTPS-Verbindungen zum Internet
FW-014	Internal-Network Bern	Vpn-Net-Terra-Cloud	25, 587, 993 (TCP)	Erlaubt	SMTP, IMAP und Authentifizierung am Mailserver
FW-015	Internet	Internal-Network Bern	123 (UDP)	Erlaubt	NTP-Verbindungen vom Internet zu Bern
FW-016	Internet	Internal-Network Bern	51822 (UDP)	Erlaubt	End-to-Site WireGuard VPN

Regel-ID	Quelle	Ziel	Port/ Protokoll	Erlaubt/ Verweigert	Kommentar
FW-017	Internet	Internal-Network Bern	80 (TCP)	Verweigert	Default-Deny-Regel
FW-C018	Any	Any	Any	Verweigert	Default-Deny-Regel

Kommentar: Evtl. Port 88 (Kerberos) für die Domain Controller freigeben.
Diese Tabelle bildet die Paketfilterregeln der Firewall in Bern ab. In Biel werden genau die gleichen Regeln angelegt, jedoch werden jeweils Ziel oder Quelle äquivalent angepasst.

Hinweis

Diese Tabelle ist nicht abschliessend und stellt den aktuellen Stand der Firewall-Regeln für den Standort Bern dar. Die Konfiguration der Firewall wird regelmässig überprüft, gesichert und optimiert, um den Anforderungen an Sicherheit und Performance gerecht zu werden. Änderungen werden dokumentiert und einem Freigabeprozess unterzogen, um sicherzustellen, dass keine sicherheitskritischen Lücken entstehen.

Firewall-Regeln für die TERRA Cloud (VPN-Net-Terra-Cloud)

Regel-ID	Quelle	Ziel	Port/ Protokoll	Erlaubt/ Verweigert	Kommentar
FW-C001	VPN-Net-Bern	Internal-Network (Cloud)	53 (UDP/TCP)	Erlaubt	DNS-Anfragen von Bern an die Domain Controller in der Cloud
FW-C002	VPN-Net-Bern	Internal-Network (Cloud)	67-68 (UDP)	Erlaubt	DHCP-Anfragen von Bern an die Cloud
FW-C003	VPN-Net-Bern	Internal-Network (Cloud)	445 (TCP)	Erlaubt	SMB-Verbindungen von Bern zur Cloud
FW-C004	VPN-Net-Bern	Internal-Network (Cloud)	853 (TCP)	Erlaubt	DNS-Anfragen über DNS-over-TLS von Bern zur Cloud
FW-C005	VPN-Net-Bern	Internal-Network (Cloud)	5514, 8080, 3478 (TCP/UDP)	Erlaubt	Unifi-Kommunikation von Bern zur Cloud
FW-C006	VPN-Net-Biel	Internal-Network (Cloud)	53 (UDP/TCP)	Erlaubt	DNS-Anfragen von Biel an die Domain Controller in der Cloud
FW-C007	VPN-Net-Biel	Internal-Network (Cloud)	67-68 (UDP)	Erlaubt	DHCP-Anfragen von Biel an die Cloud
FW-C008	VPN-Net-Biel	Internal-Network (Cloud)	445 (TCP)	Erlaubt	SMB-Verbindungen von Biel zur Cloud
FW-C009	VPN-Net-Biel	Internal-Network (Cloud)	853 (TCP)	Erlaubt	DNS-Anfragen über DNS-over-TLS von Biel zur Cloud
FW-C010	VPN-Net-Biel	Internal-Network (Cloud)	5514, 8080, 3478 (TCP/UDP)	Erlaubt	Unifi-Kommunikation von Biel zur Cloud
FW-C011	Internal-Network (Cloud)	VPN-Net-Bern	22 (TCP)	Erlaubt	SSH-Verbindungen von der Cloud nach Bern

Regel-ID	Quelle	Ziel	Port/ Protokoll	Erlaubt/ Verweigert	Kommentar
FW-C012	Internal-Network (Cloud)	VPN-Net-Biel	22 (TCP)	Erlaubt	SSH-Verbindungen von der Cloud nach Biel
FW-C013	Internal-Network (Cloud)	VPN-Net-Bern	51821 (UDP)	Erlaubt	WireGuard S2S VPN von der Cloud nach Bern
FW-C014	Internal-Network (Cloud)	VPN-Net-Biel	51821 (UDP)	Erlaubt	WireGuard S2S VPN von der Cloud nach Biel
FW-C015	Internal-Network (Cloud)	VPN-Net-Bern	8 (ICMP)	Erlaubt	ICMP Echo-Request von der Cloud nach Bern
FW-C016	Internal-Network (Cloud)	VPN-Net-Biel	8 (ICMP)	Erlaubt	ICMP Echo-Request von der Cloud nach Biel
FW-C017	VPN-Net-Bern	Internal-Network (Cloud)	8 (ICMP)	Erlaubt	ICMP Echo-Request von Bern zur Cloud
FW-C018	VPN-Net-Biel	Internal-Network (Cloud)	8 (ICMP)	Erlaubt	ICMP Echo-Request von Biel zur Cloud
FW-C019	Internal-Network (Cloud)	Internet	443 (TCP)	Erlaubt	HTTPS-Verbindungen von der Cloud zum Internet
FW-C020	Internal-Network (Cloud)	Internet	25, 587, 993 (TCP)	Erlaubt	SMTP, IMAP und Authentifizierung vom Mailserver
FW-C021	Internet	Internal-Network (Cloud)	123 (UDP)	Erlaubt	NTP-Verbindungen vom Internet zur Cloud
FW-C022	Internet	Internal-Network (Cloud)	51822 (UDP)	Erlaubt	End-to-Site WireGuard VPN
FW-C023	Internet	Internal-Network (Cloud)	80 (TCP)	Verweigert	HTTP aus Sicherheitsgründen unterbunden
FW-C024	Any	Any	Any	Verweigert	Default-Deny-Regel

Kommentar: Evtl. Port 88 (Kerberos) für die Domain Controller freigeben.

Hinweis

Diese Tabelle ist nicht abschliessend und zeigt den aktuellen Stand der Firewall-Regeln für die Cloud (VPN-Net-Terra-Cloud). Die Konfiguration wird regelmässig überprüft, gesichert und optimiert, um eine sichere Kommunikation zwischen der Cloud, den Standorten (Bern und Biel) und dem Internet zu gewährleisten. Änderungen werden dokumentiert und einem Freigabeprozess unterzogen.

3.3 Switches

- Managed Unifi Switches mittels Unifi-Controller verwaltet.
- Nicht verwendete Ports werden deaktiviert.
- Die Standardpasswörter der Switches werden ersetzt und ordnungsgemäss dokumentiert.

In Planung

- Die Netzwerk-Segmentierung (VLAN) wird in einem zukünftigen Projekt weiter ausgebaut.
- Port-Security und 802.1X sind in Planung und teilweise bereits implementiert.

3.4 Access Points

- Unifi Access Points an beiden Standorten.
- Zentrales Management erfolgt über den Unifi-Controller.
- Getrennte SSIDs für das interne Netz (EDU-intern; WPA3-Enterprise) und Gästenetz (EDU-Guest; Captive Portal).
- Das Captive Portal ermöglicht die Anmeldung im Gästenetz für persönliche sowie für Gästegeräte.
- Die Standardpasswörter der Access Points werden ersetzt und ordnungsgemäss dokumentiert.

3.5 Router

- Pro Standort ein Router mit genügend Kapazität im Bridge-Modus.
- Die OPNSense-Firewalls übernehmen das Routing und NAT.

3.6 VPN-Verbindungen

- WireGuard wird für die VPN-Verbindungen eingesetzt.

S2S VPN (Standort-zu-Standort und Cloud)

- Die Standorte Bern und Biel sowie das Cloud-LAN in der TERRA Cloud sind über Site-to-Site WireGuard VPNs miteinander verbunden.
- Konfigurationsparameter:
    - **Tunnel-Adressen:**
        - Bern: 10.1.0.0/24
        - Biel: 10.1.1.0/24
        - Cloud: 10.1.2.0/24
    - **Gateways:**
        - Bern: 10.1.0.254
        - Biel: 10.1.1.254
        - Cloud: 10.1.2.254
    - **MTU:** 1420
    - **Verschlüsselung:** Curve25519, ChaCha20-Poly1305
    - **Keepalive:** 25 Sekunden

Anpassung nach Sicherheitsaudit:

- Es wird ein PSK (Pre-shared-Key) eingesetzt.

E2S VPN (Roadwarriors)

- Benutzer können sich von extern per WireGuard-Client verbinden. Der Zugriff erfolgt über die zentrale Firewall in der TERRA Cloud.
- Konfigurationsparameter:
    - **Tunnel-Adressen:** 10.2.0.0/24
    - **Gateway:** 10.2.0.254
    - **MTU:** 1420
    - **Verschlüsselung:** Curve25519, ChaCha20-Poly1305

- **Keepalive:** 25 Sekunden
- **Zugriffsrechte:** Über AD-Gruppen gesteuert, Zugriff auf interne und Cloud-Ressourcen nur bei Bedarf.

Anpassung nach Sicherheitsaudit:

- Es wird ein PSK (Pre-shared-Key) eingesetzt.

- Benutzer erhalten nur Zugriff auf die Ressourcen, die für ihre Arbeit erforderlich sind. Logs werden auf dem zentralen Syslog-Server gesammelt.

4. Server

4.1 Übersicht

Die Server werden vollständig in der TERRA Cloud gehostet. Die Backupserver befinden sich zur zusätzlichen Absicherung in einem separaten Rechenzentrum bzw. Brandabschnitt von TERRA. Dank der flexiblen Cloud-Architektur können die Server jederzeit problemlos skaliert werden, um den aktuellen Anforderungen gerecht zu werden.

Server	Betriebssystem	Aufgaben	Performance	Diskaufteilung	Standort
TERRA-DC01	Windows Server 2022 Standard	Active Directory, DNS, DHCP, Gruppenrichtlinien	CPU: 4 Kerne, RAM: 16 GB	C: OS (100 GB), D: Daten (200 GB)	TERRA Cloud
TERRA-DC02	Windows Server 2022 Standard	Active Directory, DNS, DHCP, Gruppenrichtlinien (Backup)	CPU: 4 Kerne, RAM: 16 GB	C: OS (100 GB), D: Daten (200 GB)	TERRA Cloud
TERRA-FS01	Windows Server 2022 Standard	Zentrale Dateiablage mit Freigaben	CPU: 8 Kerne, RAM: 32 GB	C: OS (100 GB), D: Freigaben (2 TB)	TERRA Cloud
TERRA-APP01	Windows Server 2022 Standard	ERP, CRM, Unifi Controller, Bitwarden	CPU: 8 Kerne, RAM: 32 GB	C: OS (100 GB), D: Apps (600 GB)	TERRA Cloud
TERRA-EX01	Exchange Server 2019	E-Mail-Verwaltung (SMTP, IMAP, Outlook-Integration)	CPU: 8 Kerne, RAM: 64 GB	C: OS (100 GB), D: Exchange-Daten (1 TB)	TERRA Cloud
TERRA-SL01	Ubuntu Server 24.04 LTS	Zentralisierung der Logs von Firewalls, Switches, Servern und Clients	CPU: 4 Kerne, RAM: 8 GB	/: OS (50 GB), /var/log (2 TB)	TERRA Cloud
HETZNER-BK01	Ubuntu Server 24.04 LTS	Speicherung von Veeam-Backups für geografische Redundanz	CPU: 4 Kerne, RAM: 16 GB	/: OS (50 GB), /backup (10 TB)	Hetzner

4.2 Berechtigungen

- Active Directory wird als zentrales Benutzer- und Berechtigungsverwaltungssystem genutzt.

- Domänen-Admins haben volle Berechtigungen auf den DCs und den Servern.
- Auf dem Fileserver wird eine feingranulare Rechtevergabe über Freigaben und NTFS-Berechtigungen umgesetzt. (Siehe Berechtigungs-Matrix in Kapitel 8)
- Die Anmeldung beim ERP, beim CRM und bei Bitwarden über LDAP geregelt.

5. IP-Konzept

Die folgende Tabelle beschreibt das IP-Konzept der Firma:

Bereich	Subnetz	Gateway	Verwendung
Cloud LAN	192.168.1.0/24	192.168.1.254	Server und Dienste in der TERRA Cloud
Biel LAN	192.168.2.0/24	192.168.2.254	Interne Geräte, Server, Clients
Bern LAN	192.168.3.0/24	192.168.3.254	Interne Geräte, Server, Clients
Site-to-Site VPN	10.1.0.0/24	10.1.0.254	Tunnel-Adresse Bern
	10.1.1.0/24	10.1.1.254	Tunnel-Adresse Biel
	10.1.2.0/24	10.1.2.254	Tunnel-Adresse Cloud LAN
End-to-Site VPN	10.2.0.0/24	10.2.0.254	Tunnel für Homeoffice-Benutzer
Management VLAN	192.168.10.0/24	192.168.10.254	Netzwerkgeräte (Switches, APs)
Gastnetz VLAN	192.168.20.0/24	192.168.20.254	Gäste-WLAN, persönliche Geräte

Das IP-Konzept gewährleistet eine klare Trennung der verschiedenen Netzwerkbereiche und erleichtert die Verwaltung sowie die Sicherheitskonfigurationen. DHCP wird an beiden Standorten durch die Domain Controller bereitgestellt, wobei statische IP-Adressen oder IP Reservierungen im DHCP für kritische Systeme (Server, Netzwerkgeräte) verwendet werden.

6. Benutzerverwaltung

6.1 Allgemeines

- **Active Directory (AD)** dient der zentralen Verwaltung von Benutzern, Gruppen und Computern.
- Jeder Benutzer erhält ein persönliches Benutzerkonto (UPN: `vorname.nachname@firma.local` / `DOMAIN\vorname.nachname`).
- Jeder Benutzer erhält ein Userhome welches automatisch als Laufwerk H: eingebunden wird: `\\Fileserver\Userhomes$\%USERNAME%`.

6.2 Benutzer

Vorname	Name	Abteilung
Andreas	Maier	IT
Benjamin	Schuster	Accounting
Carla	Weber	Logistics
David	Roth	Logistics
Elisabeth	Hoffmann	Marketing
Franziska	Vogel	Marketing
Georg	Schäfer	Accounting
Hanna	Becker	Logistics

Vorname	Name	Abteilung
Ingo	Klein	Logistics
Julia	Lehmann	Logistics
Karl	Braun	Management
Leonie	Richter	Logistics
Maria	Schulz	Accounting
Niklas	Winter	Logistics
Olivia	Kaiser	Marketing
Paul	Becker	HR
Quentin	Lorenz	Marketing
Rebecca	Neumann	Logistics
Stefan	Möller	Accounting
Tanja	Bachmann	Logistics
Ulrich	Dietz	Logistics
Valerie	Sommer	Management
Walter	Weiss	IT
Xaver	Huber	HR
Yvonne	König	HR

6.3 Benutzermanagement

- Neue Benutzer werden durch die IT-Abteilung in Absprache mit der Personalabteilung erstellt.
- Standardmässig treten die Benutzer in vordefinierte Gruppen (z.B. Abteilungsgruppen wie `Logistics`, `Marketing`, `HR`, `Accounting`, `Management`, `IT`) ein.
- Benutzerkonten werden bei Ausscheiden aus dem Unternehmen deaktiviert und nach definiertem Zeitraum gelöscht oder archiviert.

6.4 Passwort-Richtlinie

- **Passwortlänge**: mindestens 12 Zeichen
- **Komplexität**: Kombination aus Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen
- **Änderungsintervall**: alle 365 Tage und bei Bedarf (bzw. Verdacht auf Phishing)
- **Passworthistorie**: die letzten 5 Passwörter dürfen nicht wiederverwendet werden
- **Konto-Sperrung** nach 5 ungültigen Anmeldeversuchen

6.5 Schulung

- Alle Benutzer erhalten eine IT-Sicherheitsschulung “Security Awareness” (Einsteiger und jährliche Auffrischung).
- Inhalte der Schulung:
    - Sicherer Umgang mit Passwörtern
    - Erkennen von Phishing-Mails
    - Umgang mit sensiblen Daten
    - Richtlinien für den Internet- und E-Mail-Gebrauch

- Bei vermehrtem Auftreten von Phishing-Angriffen oder anderen Malware-Aktivitäten werden die Mitarbeitenden durch gezielte Informationsrundmails und Inputs in Meetings sensibilisiert und auf potenzielle Gefahren aufmerksam gemacht.
- Zur Steigerung des Sicherheitsbewusstseins setzen wir das Security Awareness Program von Securepoint ein. Dieses versendet regelmässig “Phishing”-Testmails mit unterschiedlichen Inhalten und Themen an die Mitarbeitenden. Die daraus gewonnenen Statistiken liefern wertvolle Einblicke in die Aufmerksamkeit und Reaktionsfähigkeit der Belegschaft.

7. Benutzermatrix und Berechtigungsmatrix

7.1 Benutzermatrix

Vorname	Name	Abteilung	Gruppe(n)
Andreas	Maier	IT	Domain Admins
Benjamin	Schuster	Accounting	gg_Accounting
Carla	Weber	Logistics	gg_Logistics
David	Roth	Logistics	gg_Logistics
Elisabeth	Hoffmann	Marketing	gg_Marketing
Franziska	Vogel	Marketing	gg_Marketing
Georg	Schäfer	Accounting	gg_Accounting
Hanna	Becker	Logistics	gg_Logistics
Ingo	Klein	Logistics	gg_Logistics
Julia	Lehmann	Logistics	gg_Logistics
Karl	Braun	Management	gg_Management
Leonie	Richter	Logistics	gg_Logistics
Maria	Schulz	Accounting	gg_Accounting
Niklas	Winter	Logistics	gg_Logistics
Olivia	Kaiser	Marketing	gg_Marketing
Paul	Becker	HR	gg_HR
Quentin	Lorenz	Marketing	gg_Marketing
Rebecca	Neumann	Logistics	gg_Logistics
Stefan	Möller	Accounting	gg_Accounting
Tanja	Bachmann	Logistics	gg_Logistics
Ulrich	Dietz	Logistics	gg_Logistics
Valerie	Sommer	Management	gg_Management
Walter	Weiss	IT	Domain Admins
Xaver	Huber	HR	gg_HR
Yvonne	König	HR	gg_HR

7.2 Berechtigungsmatrix

Abteilungsressource	Logistics	Marketing	HR	Accounting	Management	IT
Logistics	Vollzugriff	Kein Zugriff	Kein Zugriff	Kein Zugriff	Lesen (R)	Lesen (R)
Marketing	Kein	Vollzugriff	Kein	Kein Zugriff	Lesen (R)	Lesen (R)

Abteilungsressource	Logistics	Marketing	HR	Accounting	Management	IT
	Zugriff		Zugriff			
HR	Kein Zugriff	Kein Zugriff	Vollzugriff	Kein Zugriff	Lesen (R)	Lesen (R)
Accounting	Kein Zugriff	Kein Zugriff	Kein Zugriff	Vollzugriff	Lesen (R)	Lesen (R)
Management	Lesen (R)	Lesen (R)	Lesen (R)	Lesen (R)	Vollzugriff	Lesen (R)
IT	Kein Zugriff	Kein Zugriff	Kein Zugriff	Kein Zugriff	Lesen (R)	Vollzugriff
Gemeinsame Datenablage (D:)	Vollzugriff	Vollzugriff	Vollzugriff	Vollzugriff	Vollzugriff	Vollzugriff

Hinweise zur Matrix

- Jede Abteilung hat Vollzugriff auf ihre spezifischen Daten innerhalb der Datenablage (D:).
- Abteilungsübergreifende Zugriffe sind stark eingeschränkt, um Datensicherheit und Vertraulichkeit zu gewährleisten.
- Management und IT haben zusätzliche Leserechte oder administrativen Zugriff auf verschiedene Ressourcen.

Diese Matrix stellt sicher, dass die Zugriffsrechte klar definiert sind und den Datenschutz- sowie Sicherheitsrichtlinien entsprechen.

8. Backup-Konzept

Für die Sicherung der Unternehmensdaten wird ein dreistufiges Backup-Konzept eingesetzt, das sowohl lokale als auch externe Sicherungen umfasst. Dieses Konzept gewährleistet maximale Datensicherheit und Redundanz:

1. **TERRA Cloud Backup**
    - Die primäre Backuplösung wird von der TERRA Cloud bereitgestellt.
    - Alle Daten werden in einem separaten Brandabschnitt innerhalb des TERRA Cloud Rechenzentrums gesichert.
    - Die Backups erfolgen täglich und beinhalten System-State-, Daten- und Applikationssicherungen.
2. **Lokales Backup auf NAS**
    - Zusätzlich werden die Daten auf einem zentralen NAS im Standort Bern gesichert.
    - Diese Sicherung bietet schnellen Zugriff für Wiederherstellungen vor Ort und dient als zusätzliche Absicherung.
    - Das NAS wird regelmässig gewartet und ist in das lokale Netzwerk integriert.
3. **Veeam Backup bei Hetzner**
    - Ein weiteres Backup wird über Veeam zu einem dedizierten Backupserver bei Hetzner erstellt.
    - Diese externe Sicherung gewährleistet geografische Redundanz und Schutz vor lokalen Ausfällen, wie Naturkatastrophen oder Bränden.
    - Die Verbindung zur Hetzner-Infrastruktur erfolgt verschlüsselt, und die Backups werden in regelmässigen Intervallen auf Integrität geprüft.

Zusammenfassung:
Das dreistufige Backup-Konzept (TERRA Cloud, NAS in Bern, Veeam bei Hetzner) stellt sicher, dass die Unternehmensdaten jederzeit verfügbar und geschützt sind. Die Kombination aus lokaler, regionaler und externer Datensicherung minimiert das Risiko von Datenverlusten und ermöglicht eine flexible Wiederherstellung bei Bedarf. Alle Backups unterliegen einer regelmässigen Überprüfung und werden gemäss dem 3-2-1-Prinzip umgesetzt:

- **3 Kopien** der Daten (Produktion und zwei Backups)
- **2 verschiedene Speichermedien**
- **1 Backup an einem externen Standort**

8.1 Desaster Recovery Plan

Der Desaster Recovery Plan (DRP) legt Massnahmen zur Wiederherstellung der IT-Infrastruktur im Falle eines grösseren Ausfalls (z. B. Brand, Ransomware) fest.

1. Notfall-Dokumentation

- Zentrale Dokumentation kritischer Systeme, Konfigurationen und Ansprechpartner.
- Regelmässige Updates und Verfügbarkeit in verschlüsselter digitaler sowie physischer Form.

2. Wiederanlaufplan

- Priorisierte Wiederherstellung:
    1. Netzwerk (Firewall, VPN, Switches).
    2. Domain Controller (AD, DNS).
    3. Fileserver (Unternehmensdaten).
    4. Applikationsserver (ERP, CRM).
    5. Mailserver (E-Mail-Kommunikation).
- RTO: 4 Stunden für kritische, 24 Stunden für sekundäre Systeme.
- RPO: Maximaler Datenverlust: 12 Stunden.

4. Test und Simulation

- Jährliche Tests des DRP zur Sicherstellung der Funktionsfähigkeit.
- Dokumentation von Tests und Behebung erkannter Schwachstellen.

9. Organisatorische Richtlinien

9.1 Change Management

- Alle Änderungen (Firewall-Regeln, Server-Konfigurationen, etc.) werden in einem Änderungsprotokoll festgehalten.
- Geplante Changes werden vorab durch IT-Leitung oder Geschäftsleitung freigegeben, gemäss dem 4-Augen-Prinzip.

9.2 IT-Sicherheit und Compliance

- Einhalten des Daten Schutz Gesetzes.
- Aufbau eines ISMS (Information Security Management System) gemäss ISO 27001 (in Planung).

- Regelmässige Penetrationstests oder Sicherheitsaudits durch externe Dienstleister.

9.3 Monitoring und Alarmierung

- Monitoring aller zentralen Komponenten (Server, Netzwerk, Firewall) über das Tool “Zabbix”.
- Alarmierung via E-Mail und SMS/Push-Benachrichtigung bei kritischen Zuständen (z.B. hoher Speicherverbrauch, Netzausfall, CPU-Spitzenlast).

9.4 Passwort-Management

Alle Passwörter werden im self-hosted Bitwarden gespeichert, um mehreren Personen gleichzeitig ein korruptionsfreies Arbeiten zu ermöglichen. Die Passwörter werden zentral verwaltet, und Passwortfreigaben können benutzerbezogen vergeben werden.

Zusätzlich erhält jede:r Mitarbeiter:in ein persönliches Login für persönliche Passwörter. Alle Logins sind individuell; Gruppen-Logins werden nicht verwendet.

9.5 IT-Verantwortlichkeit

Die IT-Verantwortlichkeiten innerhalb der Organisation werden gemäss dem RACI-Modell (Responsible, Accountable, Consulted, Informed) klar definiert und auf die beteiligten Personen verteilt. Die Verteilung der Rollen ist wie folgt:

Rollenbeschreibung gemäss Organisation

- **CISO (Chief Information Security Officer):** Valerie Sommer
    - Hauptverantwortliche Person für die IT-Sicherheitsstrategie der Organisation und alle sicherheitsbezogenen Entscheidungen.
    - Entscheidungsbefugnis und letztendliche Verantwortung für Sicherheitsmassnahmen (Accountable).
- **IT-Leiter:** Andreas Maier
    - Operative Führung und Umsetzung aller IT-Prozesse und Projekte.
    - Hauptverantwortlicher für die Ausführung (Responsible), in Sicherheitsfragen jedoch dem CISO untergeordnet.
- **IT-Mitarbeiter (Stellvertretung):** Walter Weiss
    - Unterstützt den IT-Leiter und übernimmt in definierten Fällen die Rolle des Verantwortlichen (Responsible) oder der Stellvertretung (Accountable), insbesondere in Abwesenheit des IT-Leiters.

9.6 Prozessabläufe

- Die Prozessabläufe werden aktuell erarbeitet und zu einem späteren Zeitpunkt bereitgestellt.

10. Ausblick

- VLAN-Segmentierung & 802.1X: Die geplante Erweiterung der Netzwerksegmentierung wird die IT-Sicherheit weiter erhöhen und den Überblick über Zugriffe erleichtern.

- Port-Security: Die bereits teilweise implementierte Port-Security soll umfassender ausgerollt werden, um unautorisierte Geräteverbindungen zu verhindern.
- ISMS & Zertifizierungen: Die Einführung eines strukturierten ISMS (gemäss ISO 27001) ist der nächste Schritt, um die Sicherheitsprozesse zu standardisieren und zu zertifizieren.
- Erweiterte Cloud-Strategie: Weitere Dienste könnten in die TERRA Cloud oder zusätzliche Cloud-Anbieter (z. B. Azure, AWS) integriert werden, um Flexibilität und Skalierbarkeit zu steigern.
- Regelmässige Sicherheitsaudits: Externe Auditoren und Penetrationstests werden in kürzeren Intervallen eingeplant, um Schwachstellen frühzeitig zu erkennen.

Massnahmen des Sicherheitsaudits

Audit von Flamur Shehi und Julian Matt am 31.01.2025 durchgeführt.

Fehlende Punkte

1. **Unzureichende Dokumentation von USV-Wattzahlen**
    - **Risiko**: Ausfall im Notfall
    - **Empfohlene Massnahme**:
      Führen Sie eine Lastberechnung durch, um sicherzustellen, dass die USV alle kritischen Komponenten im Notfall versorgen kann. Dokumentieren Sie die Ergebnisse in der Netzwerkinfrastruktur-Dokumentation & im Netzwerkplan.

   Wird in der IT-Dokumentation erfasst, sobald die genutzten Produkte sowie deren Spezifikationen bekannt sind.

2. **Brandschutzmassnahmen in den EDV-Räumen fehlen oder sind unklar**
    - **Risiko**: Unzureichender Schutz vor Bränden
    - **Empfohlene Massnahme**:
      Überprüfen Sie die bestehenden Brandschutzvorrichtungen (z.B. Rauchmelder, Feuerlöscher) & führen Sie gegebenenfalls eine Brandschutzinspektion durch. Stellen Sie sicher, dass alle Mitarbeitenden über die Brandschutzmassnahmen informiert sind.

   Wird implementiert, siehe Abschnitt 2.2 EDV Raum und Rack

3. **Unklare ISMS-Planung**
    - **Risiko**: Keine klare Abgrenzung, welche Netzwerkteile abgesichert werden
    - **Empfohlene Massnahme**:
      Definieren Sie den Umfang des ISMS & identifizieren Sie die spezifischen Teile des Netzwerks, die abgedeckt werden sollen. Dokumentieren Sie dies in einem ISMS-Plan.

   Wie in Kapitel “9.2 IT-Sicherheit und Compliance” bereits angedeutet ist, ist dies bereits in Planung.

4. **Kein Backup für Firewalls**
    - **Risiko**: Netzwerkausfall bei Störung

- **Empfohlene Massnahme**:
  Implementieren Sie eine Hochverfügbarkeitslösung (HA) für Firewalls, einschliesslich automatischer Failover-Mechanismen. Erstellen Sie regelmässige Backups der Firewall-Konfiguration & dokumentieren Sie diese Verfahren.

Es wurde der Geschäftsleitung vorgeschlagen, diese hat sich jedoch bewusst dagegen entschieden, da sie nicht als geschäftskritisch angesehen wird. Falls eine Firewall an einem Standort ausfällt, stehen immer noch die E2S-Roadwarrior-VPN-Verbindungen zu den anderen Standorten zur Verfügung. Sollten in Zukunft schwerwiegende Probleme diesbezüglich auftreten, wird dieser Punkt noch einmal mit der Geschäftsleitung hinsichtlich der Notwendigkeit dieser Lösung diskutiert.

5. **Nicht dokumentierte VPN-Verschlüsselung**
   - **Risiko**: Gefahr veralteter oder unsicherer Verschlüsselung
   - **Empfohlene Massnahme**:
     Überprüfen Sie die implementierte Verschlüsselung (z.B. AES-256) für die VPN-Verbindungen & stellen Sie sicher, dass sie den aktuellen Sicherheitsstandards entspricht. Dokumentieren Sie die verwendeten Protokolle & Verschlüsselungsmethoden.

Ist bereits in der Dokumentation unter Abschnitt “3.6 VPN-Verbindungen” beschrieben. Die zusätzliche Sicherung des PSK wurde nach dem Audit implementiert.

6. **Fehlende Antivirus-Strategie für Clients**
   - **Risiko**: Malware-Infektionen
   - **Empfohlene Massnahme**:
     Erstellen & dokumentieren Sie eine umfassende Antivirus-Strategie, die regelmässige Updates, Scans & Schulungen für Benutzer umfasst. Halten Sie diese Informationen in einer zentralen Sicherheitsdokumentation fest.

Es wird keine zusätzliche Antivirenlösung implementiert, da nach Absprache mit der Geschäftsleitung, der Microsoft Defender als genügend angesehen wird. Daher keine Massnahme nötig.

7. **Fehlende Dokumentation der Softwareverwaltung**
   - **Risiko**: Gefahr unsicherer oder nicht autorisierter Software
   - **Empfohlene Massnahme**:
     Implementieren Sie ein Softwaremanagement-System, das alle Installationen dokumentiert & genehmigt. Führen Sie regelmässige Audits durch, um sicherzustellen, dass nur autorisierte Software installiert ist.

Wie bereits in Abschnitt “9.2 IT-Sicherheit und Compliance” beschrieben, werden Softwares nur von den Sysadmins genehmigt und installiert. Die Benutzer sind über Gruppenrichtlinien daran gehindert, selbstständig Software zu installieren. Als zukünftiges Projekt ist die Implementierung einer Software-Management-Lösung wie Microsoft Intune bereits geplant.

8. **Unklarheiten bei der Videoüberwachung**
   - **Risiko**: Kein dokumentiertes VLAN/Subnetz für Überwachungssysteme

- **Empfohlene Massnahme (Teil 1)**:
  Überprüfen Sie das bestehende Videoüberwachungssystem auf Funktionalität & Abdeckung der kritischen Bereiche. Stellen Sie sicher, dass alle Aufzeichnungen gemäss den Datenschutzrichtlinien behandelt werden.
- **Empfohlene Massnahme (Teil 2)**:
  Dokumentieren Sie das VLAN & Subnetz, in dem sich das Videoüberwachungssystem befindet, um sicherzustellen, dass es von anderen Netzwerksegmenten getrennt ist & Sicherheitsrichtlinien eingehalten werden.

Eine Videoüberwachung ist nicht erwünscht, da dies überdimensioniert wäre. Im EDV-Raum befinden sich lediglich eine Firewall, ein Router und ein Core-Switch, sowie in Bern ein NAS. Die Geschäftsleitung stimmt mit uns überein, dass die eingeschränkte Zugriffskontrolle mit den RFID-Badges völlig ausreichend ist.

Tests

Interner Netzwerkscan

- **Ziel**: Überprüfen der Sicherheit und Erreichbarkeit aller Geräte innerhalb des internen Netzwerks.
- **Tools**:
  - **Nmap**: Ein leistungsstarkes Tool zum Scannen von Netzwerken, das Informationen über aktive Hosts, offene Ports und Dienste liefert.
  - **Angry IP Scanner**: Ein einfaches Tool zur schnellen Erkennung aktiver IP-Adressen im Netzwerk.

Sehr gute Idee, werden wir so eins zu eins umsetzen/testen. Da wir den Angry IPscanner nicht kennen und Javaruntime dafür nötig wäre, haben wir entschieden, dass wir Nmap nutzen werden. Es werden auch die sinnvollen Tools aus der Kali Toolbox verwendet.

Externer Netzwerkscan

- **Ziel**: Überprüfen der Sicherheitskonfigurationen von externen Zugriffspunkten (z.B. Firewalls, Router).
- **Tools**:
  - **Nessus**: Ein umfassendes Vulnerability-Scanning-Tool, das Schwachstellen im externen Netzwerk identifizieren kann.
  - **OpenVAS**: Eine Open-Source-Alternative zu Nessus, die ebenfalls Schwachstellen im Netzwerk aufdecken kann.

Scans von aussen werden in Betracht gezogen, hier werden jedoch die selben Tools verwendet wie im Abschnitt “Interner Netzwerkscan” beschreiben.

Backup-Wiederherstellungstest

- **Ziel**: Überprüfen der Funktionsfähigkeit des Backup-Systems und der Wiederherstellungsprozesse.
- **Tools**:
  - **Veeam Backup & Replication**: Ein Tool zur Verwaltung und Durchführung von Backup-Wiederherstellungen.

    - **TERRA Cloud Management Console**: Zum Testen der Wiederherstellung von Backups aus der Cloud.

  Hier werden wir die bereits von TERRA Cloud integrierten Backup und Replication Funktionen nutzen, da wir mit diesen bereits eigene Erfahrungen sammeln konnten. Umfassende Recoverytest werden halbjährlich mit explizit dafür gedachten Recovery VMs von TERRA Cloud durchgeführt.

Firewall-Konfigurationstest

- **Ziel**: Überprüfen der Firewall-Regeln und deren Wirksamkeit.
- **Tools**:
    - **GFI Languard**: Ein Tool zur Überprüfung von Firewall-Regeln und zur Durchführung von Sicherheitsüberprüfungen.
    - **Netcat**: Ein einfaches Tool zur Durchführung von Portscans und zum Testen der Erreichbarkeit bestimmter Ports.

  siehe Abschnitt “Externer Netzwerkscan”

Anhang

- **Netzplan** (vereinfacht)

Erfasst von Timon Bachmann und Ruben Notaro am 26.01.2025