techem

Übersicht der Sicherheitsorganisation und -architektur

1 Einführung

Die Sicherheitsarchitektur der Techem Gruppe erfolgt nach einer Defense-in-Depth-Strategie und erstreckt sich nach Best-Practice-Ansätzen über die verschiedenen Sicherheitsebenen. Die verwendeten Frameworks für die Sicherheitsorganisation sowie -architektur sind primär die Normenreihe der ISO 27000, des National Institute of Standards and Technology (NIST) sowie des Bundesamts für Sicherheit in der Informationstechnik (BSI).

2 Organisatorische Sicherheit

2.1. Zertifizierung nach ISO 27001 und ISMS

Das Informationssicherheitsmanagementsystem (ISMS) der Techem Gruppe ist in bestimmten Bereichen nach ISO 27001 zertifiziert. Der Geltungsbereich der Zertifizierung ergibt sich aus dem jeweiligen Zertifikat (aktuell: IT-Kernsysteme und dazugehörige Support-Prozesse inkl. der Techem Solutions). Die Erstzertifizierung erfolgte 2022 nach der DIN EN ISO 27001:2017. Die Rezertifizierung erfolgte 2025, wobei die Transition auf die neue Normversion DIN EN ISO 27001:2022, sowie die Erweiterung des Anwendungsbereiches auf die Techem Solutions durchgeführt wurde.
Das ISMS beinhaltet die Leitlinie zur Informationssicherheit, die Richtlinie zum Informationssicherheitsmanagement, das Informationssicherheitsmanagementhandbuch sowie die darunterliegenden einschlägigen Richtlinien. Das Risikomanagement ist Kernbestandteil des ISMS und wird durch die Sicherheitsorganisation überwacht.

2.2. Sicherheitsorganisation

Die Sicherheitsorganisation der Techem ist eine Gruppenfunktion und zuständig für alle Gesellschaften der Techem. Sie setzt sich aus dem Head of Information Security einschließlich seines Teams sowie dem Head of IT Security einschließlich seines Teams zusammen. Der Head of Information Security ist gesamtheitlich verantwortlich für alle sicherheitsrelevanten Belange und hat ein jederzeitiges, direktes Vortragsrecht bei Geschäftsführung und Advisory Board. Sind Sicherheitsbelange betroffen ist die Abteilung Information Security weisungsbefugt. Das IT-Security Team ist durch Rufbereitschaft 24/7 erreichbar.

2.3. Audits

Die Teams führen regelmäßig Audits durch, welche die ausländischen Teilgesellschaften der Techem sowie strategisch kritische Dienstleister betreffen. Die Audits finden gewöhnlich in einem geregelten Rhythmus statt und werden von den Teams jedes Geschäftsjahr neu geplant. Abseits dessen sind jederzeit anlassbezogene Audits möglich.

2.4. Schulungen, Trainings und Sensibilisierungen

Es finden regelmäßig Schulungen, Trainings und Sensibilisierungsmaßnahmen in unterschiedlichen Formaten statt. Das primäre E-Learning zur Informationssicherheit wird jährlich an alle Mitarbeiter über das zentrale Human Resources (HR)-System ausgerollt, die Teilnahme ist verpflichtend und wird durch HR bis zur Geschäftsführerebene hin nachverfolgt. Dieses ist ebenfalls für Externe und Subunternehmer verpflichtend. Es finden regelmäßige Live-Phishing-Simulationen statt, die durch einen spezialisierten Dienstleister durchgeführt werden. Daneben finden regelmäßig Schulungen zu speziellen Themen statt, welche anlassbezogen ausgewählt und durchgeführt werden. Dies gilt ebenfalls für die Security Teams selbst im Hinblick auf fachspezifische Fortbildungen.

2.5. Beratung der Fachbereiche

Die Sicherheitsorganisation der Techem berät die Fachbereiche, Mitarbeiter*innen sowie Projekte und stellt somit sicher, dass die Prinzipien von security-by-design eingehalten werden.

Techem Energy Services GmbH · Hauptstraße 89 · D-65760 Eschborn.

techem

2.6. Outsourcing und Dienstleister

Im Bereich Security werden Dienstleister für verschiedene Bereiche eingesetzt, diese umfassen u. a.:

- Managed Security Services
- Incident management und Security Operations
- Penetrationstests, Red Teaming sowie Beratung
- Phishing Simulationen, E-Learnings sowie spezialisierte Trainings

3 Physische Sicherheit

Die Gebäude und Büroflächen sind durch Kartenlesegeräte und Firmenausweise zutrittsbeschränkt. Gäste müssen sich anmelden, bekommen Besucherausweise und dürfen sich in den internen Büroflächen nicht unbeaufsichtigt bewegen. Besonders sensible Bereiche verfügen über spezielle Zutrittsberechtigungen, die erst nach einem mehrstufigen Genehmigungsverfahren vergeben werden. Die Gebäude werden teilweise per Video und von Bewegungsmeldern überwacht.

Die IT der Techem ist vollständig outsourced, so dass sich keine Serverräume, Rechenzentren o. ä. in den Gebäuden der Techem befinden.

4 Technische Sicherheit

4.1. User

Die Benutzerverwaltung erfolgt zentral und erstreckt sich auf on-premise Systeme sowie Cloud-Anwendungen. Flächendeckend ist Multifaktor-Authentifizierung (MFA) im Einsatz, Authentifizierung über single sign-on (SSO) wird präferiert. Administratorrechte werden auf eigene Userkonten ausgelagert mit denen nicht alltäglich gearbeitet werden kann und nur nach einem festgelegten Prozess mit mehreren Genehmigungsinstanzen vergeben. Diese sind grundsätzlich zeitlich beschränkt und werden regelmäßig auditiert. Die Passwortrichtlinie sieht lange und komplexe Passwörter vor, die nicht periodisch geändert werden müssen. Userkonten von externen Usern sind grundsätzlich zeitlich beschränkt. Alle Benutzerrechte werden nach dem Minimalprinzip vergeben. Die Rechte und Rollen werden in der Benutzerverwaltung zentral verwaltet, die Rechte und Rollen innerhalb von Fachanwendungen liegen im Verantwortungsbereich des jeweiligen Systemverantwortlichen.

4.2. Endgeräte

Es werden durchgehend zentral gemanagte Laptops eingesetzt. Zusätzlich ist ein Zugang zur Techem-IT-Umgebung über virtuelle Anwendungen möglich. Das Laptop stellt nach erfolgreicher Authentifizierung automatisch einen VPN-Tunnel her. Ohne diesen kann das Laptop nur offline verwendet werden und es gibt keinen Zugriff auf interne oder cloudbasierte Systeme. Die VPN-Verbindung prüft beim Aufbau den Status des Geräts, nur wenn dieser als compliant eingestuft wird erfolgt der Verbindungsaufbau. Das Patchmanagement wird zentral durch den IT-Dienstleister sichergestellt.

Zugriff über mobile Geräte (Smartphones, Tablets) kann ausschließlich durch verwaltete Geräte erfolgen. Dazu wird ein Mobile Device Management (MDM) verwendet. Der Appstore ist stark limitiert und nur vorher geprüfte und freigegebene Apps können verwendet werden. Bring-your-own-device (BYOD) ist nur für Smartphones oder Tablets möglich und erfolgt ebenso ausschließlich durch MDM. Die Festplatten der Endgeräte sind verschlüsselt.

4.3. Netzwerk und Internet

Das interne Netzwerk ist in mehrere logische Netzwerkzonen unterteilt, die durch Firewalls voneinander getrennt sind. Die Produktionsumgebung sowie nicht produktive Systeme sind in verschiedene Umgebungen segmentiert. Ein Zugriff von außen kann nur über eine Demilitarisierte Zone (DMZ) oder per Site-to-Site VPN erfolgen, der Zugriff über Clients ist ausschließlich per Virtual Private Network (VPN) möglich. Die Netzwerke in den Standorten sind durch Network Access Control (NAC) gesichert.

Die zentrale Cloud-Umgebung befindet sich in der EU und ist redundant aufgebaut, die Sicherheitspolicies werden zentral durch die Sicherheitsorganisation verwaltet.

Jeglicher Internetzugriff erfolgt über einen zentralen Cloud-Proxy der u. a. per SSL-Inspection, Black-/Whitelists und Sandboxing die Sicherheit beim

Browsen sicherstellt. Ein Cloud Access Security Broker (CASB) stellt sicher, dass keine unbekannten Cloud-Applikationen verwendet werden können, dieser verhindert zusätzlich unkontrollierten Datenabfluss.

4.4. Server und Datenbanken

Server und Datenbanken sind nahezu vollständig virtualisiert und auf zwei Rechenzentren verteilt, von dem jedes die Arbeit des anderen übernehmen kann (Active/Passive-Konfiguration). Sie befinden sich in unterschiedlichen Netzwerkzonen und können mit Ausnahme von Entwicklungsmaschinen nur durch Sprungserver im internen Netz erreicht werden. Alle Server verwenden gehärtete Standard-Images und unterliegen standardisierten Patchgruppen. Änderungen an Systemen werden nur durch einen Change-Prozess freigegeben, in den die Sicherheitsorganisation eingebunden ist.

4.5. Storage, Backup und Archiv

Storage findet maßgeblich auf Cloud-Speichern statt. Backups und das Archiv werden in einem dedizierten dritten Rechenzentrum aufbewahrt, ein zusätzliches Backup in der Cloud findet regelmäßig statt.

4.6. Kommunikation

Primäre Kommunikationsmittel sind E-Mail und Instant Messaging. Die Schutzmechanismen für E-Mails beinhalten u. a. Spam- und Phishing-Schutz, Link- und Anhang-Protection sowie Sandboxing. Verschlüsselung per TLS 1.2 wird erzwungen, die Nutzung von S/MIME ist möglich.

4.7. Anwendungen

Standard-Software wird über die zentrale Softwareverteilung ausgerollt und aktuell gehalten. Individuelle Software muss über einen Request beantragt werden und wird durch mehrere Instanzen vor Freigabe geprüft, auch diese Anwendungen werden paketiert und ausgerollt. Eigene Installationen mittels lokaler Adminrechte sind die Ausnahme und maßgeblich auf Benutzer mit IT-Kenntnissen beschränkt, die diese Rechte für ihre tägliche Arbeit benötigen.

Unternehmensweite Anwendungen werden vor Einführung im Rahmen der Einkaufsprozesse geprüft und freigegeben, dies gilt auch für reine SaaS-Anwendungen.

4.8. Zertifikatsverwaltung

Techem nutzt eine eigene Public Key Infrastructure (PKI) zur Erstellung von Zertifikaten für verschiedene Einsatzzwecke. Es existieren zwei Stränge (RSA und ECC), die Zertifizierungsrichtlinie sowie die Zertifikatsrückruflisten werden veröffentlicht unter ca-rsa.techem.de, bzw. ca-ecc.techem.de.

4.9. Penetrationstests und Sicherheitsüberprüfungen

Die Sicherheitsorganisation der Techem führt regelmäßig Penetrationstests und Sicherheitsüberprüfungen durch. Diese werden analog zum Auditplan festgelegt und geplant. Penetrationstests werden größtenteils durch externe, spezialisierte Dienstleister durchgeführt. Projekte mit erheblichen Auswirkungen auf das Tagesgeschäft (z. B. neue Kundenportale, Schnittstellen zum automatisierten Datenaustausch, Fernableseinfrastruktur, etc.) werden nach einer erfolgten Risikobeurteilung vor Inbetriebnahme ebenfalls geprüft, ein go-live erfolgt erst nach bestandenen Überprüfungen durch einen externen Dienstleister.

4.10. Data Leak Prevention (DLP) und Informationsklassifizierung

Techem hat eine Informationsklassifizierung eingeführt, die Kennzeichnung von Dokumenten ist vor elektronischer Speicherung in Office-Anwendungen verpflichtend. Auch E-Mails müssen klassifiziert werden. Öffentlich verfügbare KI-Systeme wurden gesperrt, um einen Abfluss von sensiblen Daten zu verhindern.
Außerhalb der gesicherten Techem-Umgebung können Dateien nicht heruntergeladen und gespeichert werden, um unkontrollierten Informationsabfluss zu vermeiden.

5 Security Operations

5.1. Security Operations Center

Die Techem nutzt ein externes Security Operations Center (SOC) welches als managed security service 24/7 betrieben wird. Als Basis dient das Security

Information and Event Management (SIEM), in dem die Protokolldateien der Systeme gesammelt und analysiert werden.
Für Incident Response und Forensik steht bei Bedarf ein Team zur Unterstützung auf Abruf bereit.

5.2. Vulnerability Management

Alle Systeme werden regelmäßig im Rahmen des Vulnerability Managements auf Schwachstellen überprüft. Die internen Netzwerkbereiche werden regelmäßig gescannt, Endgeräte übertragen ihre Daten per installiertem Agent. Die Sicherheitsorganisation analysiert und bewertet die eingehenden Daten und legt in Abstimmung mit den IT-Abteilungen Maßnahmen zur Risikominimierung fest.

5.3. Threat Intelligence

Es kommt ein spezialisiertes System zum Sammeln von Informationen in Form von threat Intelligence zum Einsatz. Dieses beinhaltet Clear sowie Dark Web Scans, Aufzeigen von Angriffstrends oder das Aufspüren von potentiellen Phishing Domains oder Social Media Profilen zur Vorbereitung von Social Engineering Angriffen.

5.4. Incident Management

Das Security Incident Management wird durch die Sicherheitsorganisation durchgeführt und sichergestellt. Hierfür besteht ein Incident Response Plan, der die strukturierte Reaktion auf Sicherheitsvorfälle regelt.

Im Falle eines kritischen Vorfalls kann der Krisenstab der Techem aktiviert werden, die Entscheidung hierüber trifft der Head of Information Security.

Eschborn, 14.07.2026

Ansprechpartner:

Information Security
Techem Energy Services GmbH
Hauptstr. 89
65760 Eschborn

Web: www.techem.de