Redefining Hosting – Reinventing Security

kyberio.

Sicherheitskonzept der kyberio GmbH

Sicherheit auf allen Ebenen:
physisch, digital und organisatorisch

kyberio.

Sicherheit
bei kyberio

3 gelebtes ISMS: ISO 27001

4 Perfekte Ergänzung: PCI-Zertifizierung

5 5-Zonen-Sicherheitskonzept

6 Auszug aus unserem ISMS

8 Business and Service Continuity

Zertifizierte Sicherheit:
Unser gelebtes ISMS

Die Basis unserer ISO 27001-Zertifizierung nach IT-Grundschutz vom Bundesamt für Sicherheit in der Informationstechnik bildet eine Vielzahl klarer und gelebter Vorgaben und Prozesse.

Die Zertifizierung nach **BSI ISO 27001** betrachtet den Verbund des Rechenzentrums in Hannover und dessen Management. Hier sind alle Systeme und Prozesse enthalten, die zum Betrieb der Rechenzentrums-Infrastruktur, der Kundenverwaltung sowie der Leistungserbringung für die Co-Location notwendig sind.

Die Anwendung von ISO 27001 auf der Basis des IT Grundschutzes vom Bundesamt für Sicherheit in der Informationstechnik (BSI) umfasst die Maßnahmenziele und Maßnahmen aus Annex A von ISO 27001 und die damit verbundenen Ratschläge zur Umsetzung und Anleitung für allgemein anerkannte Verfahren aus ISO/IEC 27002.

Als Voraussetzung für die Zertifizierung hat Kyberio verbunden mit dem Rechenzentrum und die damit verbundenen Organistationsabläufe ein mehrstufiges Prüfverfahren durchlaufen. Dieser wird in einem regelmäßigen Zyklus widerholt.

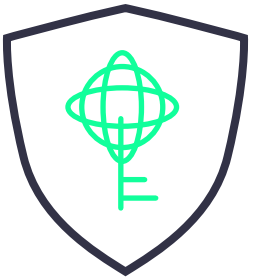
Im Wesentlichen umfasst die Prüfung die Bereiche:

- Die geschäftlichen Anforderungen des Unternehmens
- Technische Infrastruktur
- Die Verantwortung des Managements
- Organisatorische Abläufe
- Risikomanagement
- Datenschutz

Mit Kyberio setzen unsere Kunden auch bezüglich der IT-Sicherheitsgesetzgebung auf ihre eigene Sicherheit. Die Anforderungen bezüglich Datenschutz und die damit verbundenen Haftungsrisiken haben sich seit Mai 2018 durch die Datenschutzgrundverordnung der EU weiter verschärft. Diese sieht bei Verstößen gegen Datenschutzrecht noch drastischere Strafen vor als das vorherige Bundesdatenschutzgesetz.

Tatsächlich ist es so, dass die Zertifizierung nicht nur eine rechtliche Absicherung darstellt, sondern verbunden mit einer Verbesserung der Sicherheit auch viele unternehmerische Vorteile bietet. Zusammengefasst sind das:

- Verbesserte Sicherheit der IT Infrastruktur
- Verschärftes Sicherheitsbewusstsein vom Management bis zur Belegschaft.
- Rechtliche Absicherung und Senkung des Haftungsrisikos
- Verbesserung der Wettbewerbsfähigkeit
- Kosteneinsparung durch Outsourcing sicherheitsrelevanter Dienstleistungen die im Unternehmen nur mit hohem Aufwand abgebildet werden können.
- Schaffung von Vertrauen bei Kunden und bei der Öffentlichkeit
- Möglichkeit der eigenen Zertifizierung von Applikationen auf Basis der vorhandenen Zertifizierung von Kyberio.



PCI-DSS v3.2 –
Die perfekte Ergänzung

PCI-DSS Standard steht für „Payment Card Industry Data Security Standard". Der PCI Standard entspricht einem Regelwerk, dass die Sicherheitsanforderungen an den Zahlungsverkehr mit Kreditkarten abbildet. Dieser Standard ist für alle Firmen, Einrichtungen und Organisationen bindend, die Kreditkarteninhaberdaten verarbeiten.

Unternehmen und Organisationen, die Kreditkarteninhaberdaten (CHD – „Cardholder Data") elektronisch auf einer Kreditkarteninhaber-Umgeber (CDE –„Cardholder Environment") verarbeiten, müssen diese Umgebung entsprechend der PCI-Richtlinien vor Datenmissbrauch und unberechtigtem Zugriff absichern und deren fortlaufenden Betrieb schützen. Des Weiteren sieht der Standard eine eindeutige Verantwortlichkeitszuordnung für die unterschiedlichen Bereiche und Aufgaben innerhalb der CDE vor. Sämtliche Zugriffe und Arbeitsschritte müssen nachverfolgt werden können. Ein wichtiger Teil beim Betrieb einer solchen Umgebung, ist die physikalische Sicherheit und die damit verbundenen Prozesse, um diese im Rechenzentrumsbetrieb zu gewährleisten.

Diese Anforderungen decken 12 Bereiche ab:

- Firewall-Konzept
- Sicherheitseinstellungen für Passwörter
- Schutz der Daten von Kreditkarteninhabern
- Verschlüsselung von Daten
- Virenschutz
- Pflege der Systeme und Anwendungen
- Einschränkungen von Zugriffen
- Benutzerbezogene Zugangskontrolle
- Beschränkung und Sicherheit vom physikalischen Zugang zum Server
- Protokollierung der Zugriffe auf Daten
- Regelmäßige Überprüfung der Systeme
- Einhaltung von Richtlinien der Informationssicherheit

Die Nachvollziehbarkeit von Zutritt und Zugang zur Umgebung wird durch professionelle Zutrittskontrollen und Abläufe, durch eine nahtlose Videoüberwachung rund um die Uhr und durch die Protokollierung und eindeutige Zuordnung der sich im Rechenzentrum befindenden Personen und dem Datenabgleich und dessen Plausibilitätsprüfung sichergestellt.

Als Co-Location-Kunde in unserem Rechenzentrum, profitieren Sie von einer bereits von einem qualifizierten Auditor („QSA") nach PCI zertifizierten Dienstleistung, die bis zum eigenen Rack reicht. Somit können Sie sich auf die Compliance Ihrer im Rack betriebenen Infrastruktur konzentrieren und die physikalische Sicherheit Ihres Racks (wesentliche Bestandteile der Anforderungen 9 und 12 des PCI-Anforderungskataloges, sowie Anforderung 11.1 bzgl. drahtlose Zugangspunkte) durch unsere Zertifizierung attestieren. Diese Punkte fallen für Ihr eigenes Audit weg, da Sie Ihre Zertifizierung auf der zertifizierten PCI-Compliance des Rechenzentrumbetreibers aufbauen.

E-Commerce-Anbieter, Content-Provider, Einrichtungen und Organisationen unterschiedlicher Art, die im Netz per Kreditkarte Leistungen oder Produkte anbieten oder Spenden annehmen, haben somit die Möglichkeit dies in einer PCI-Zertifizierten Rechenzentrumsumgebung in einem eigenen, individuell verschließbaren 19" Rack (mit 21 oder 42 Höheneinheiten) umzusetzen. Gern stellen wir Ihnen zu diesem Zweck unsere Attestation of Compliance („AOC") zur Verfügung.

5-ZONEN-SICHERHEITSKONZEPT

Sicherheitszone 1: Grundstück

- Zufahrts- und Zutrittskontrolle
- Zaunanlage mit Rolltoren
- Kameraüberwachung (Aussenbereich und Dach)

Sicherheitszone 2: Gebäudehülle

- Zugangskontrolle
- Kameraüberwachung
- Alarmanlage

Sicherheitszone 3: Innenräume

- Zugangskontrolle
- Kameraüberwachung
- Alarmanlage

Hochsicherheitszone 4: Rechenzentrum

- Multi-Faktor-Zugangskontrolle
- Videoüberwachung
- Alarmanlagen

Sicherheitszone 5: Gitter-Cage

MADE IN GERMANY
ISO 27001
nach IT-Grundschutz

MEHR ALS SICHER

5-Zonen-Sicherheit

Menschen, Technik, Prozesse

Im Rahmen unserer ISMS adressieren wir eine Vielzahl von Themen, um den dauerhaft sicheren Betrieb unserer Rechenzentren und der Kundensysteme zu gewährleisten.

Hierzu gehören unter anderem:

- **24/7/365 Personal vor Ort:** Durch unser durchgehend besetztes Operation Center vor Ort können wir schnell auf jegliches Ereignis reagieren und den reibungslosen Betrieb der Rechenzentren sicher stellen.
- **Perimeterschutz:** Der Gewerbepark auf dem sich das Rechenzentrum befindet, wird durch Gittertore geschützt, das Rechenzentrum selbst verfügt über einen zusätzlichen Perimeterschutz. Das Gittertor zum Kundenparkplatz und zum Gebäude werden durch das Operation Center gesteuert und überwacht und bleibt für Unbefugte rund um die Uhr verschlossen.
- **24h Videoüberwachung:** Der Außenbereich, alle Gebäudezugänge, sowie die Rechenzentrumsfläche werden rund um die Uhr von Kameras mit Bewegungsserkennung überwacht. Die Live-Videosequenzen werden dabei ins Openration Center übertragen, dort kontrolliert und zusätzlich zur späteren Prüfung gespeichert.
- **Zutrittskontrolle:** Der Zutritt erfolgt ausschließlich nach vorheriger Anmeldung und in Begleitung von autorisierten Mitarbeitern und entsprechend des Sicherheitskonzeptes mit Zwei-Faktor-Authentifikation (2FA). Die Authentifikation erfolgt mit einem personalisierten RFID-Transponder des Mitarbeiters („Besitz“) in Kombination mit erfolgreicher Eingabe der persönlichen PIN („Wissen“).

MEHR ALS SICHER

5-Zonen-Sicherheit

→ **Überwachung und Alarmierung:** Die Gebäudeleittechnik ist vollständig in unsere zentrale Überwachungslösung und Alarmierungsprozesse integriert. Die Einhaltung definierter Betriebsparameter und/oder Störungsmeldungen werden hierbei sowohl dem Personal vor Ort, als auch unseren über redundante Kommunikationskanäle angebundenen Sicherheitsdienstleistern umgehend signalisiert. Je nach Art der Meldung, informiert der Sicherheitsdienstleister bei Bedarf selbstständig die Polizei, Feuerwehr und Haustechnik oder hält zunächst Rücksprache mit dem Personal vor Ort.

→ **Brandschutzkonzept:** Zur frühzeitgen Identifikation und Vermeidung von Bränden kommen hochsensible Rauchmelder zur Brandfrühsterkennung (VESDA) zum Einsatz. Sollten ergänzend weitere Brandmelder (2-Linien-Abhängigkeit) einen potenziellen Brand detektieren, wird nach einer Vorwarnung zum Schutz etwaiger Personen auf der Technikfläche eine automatische Stickstoff-Löschung (N^2-Löschung) ausgelöst. Parallel werden die Feuerwehr, das Operation Center und die Haustechnik informiert und ein Notfallplan aktiviert.

→ **Redundante Stromversorgung:** Eine batteriegestützte Unterbrechungsfreie Stromversorgung (USV) verbunden mit einer Diesel-Netzersatzanlage (NEA), sichern den Betrieb bei Ausfall des öffentlichen Energienetzes. Diese sind so dimensioniert, dass alle Komponenten inklusive Klimatisierung ohne Einschränkungen weiter betrieben werden können.

→ **Mehrschichtiger Schutz vor Cyberangriffen:** Der Schutz von Netzwerken und IT-Systemen vor Cyberangriffe ist für uns essentiell und wird permanent von uns an aktuelle Bedrohungslagen angepasst. Sowohl für Kunden, als auch für unsere eigenen Systeme haben wir ein mehrschichtiges Sicherheitskonzept, unter anderem basierend auf D/DOS-Protection, Threat-Detection (IDS/IPS), Next Generation Firewalls, Malware-Protection und manipulationssicheren Backups entwickelt.

Business and Service Continuity

Im Rahmen des ISMS wurden umfangreiche Notfallpläne, Strategien und Eskalationspfade definiert, um selbst in Krisenzenarien (z.B. im Brandfall, bei Stromausfällen oder Cyberangriffen) einen möglichst unterbrechnungsfreien Betrieb essentieller Systeme bzw. deren möglichst schnelle Wiederherstellung zu gewährleisten.

Neben der regelmäßigen Überprüfung der hierfür notwendigen Dokumentationen, Prozesse und Systeme, führen wir wiederkehrend Notfallübungen und Schulungen mit allen Mitarbeitern und externen Diensleistern (z. B. Wartungsfirmen) durch. Für den Betrieb notwendige kritische Systeme (wie etwa unser Monitoring) sind redundant ausgelegt und auf unsere zwei unabhängigen Rechenzentren verteilt.

Sämtliche Systeme werden kontinuierlich gewartet und regelmäßigen Fuktionstests (inklusive Lastübernahme der NEA) unterzogen. Durch vertraglich vereinbarte Bereitschaftsdienste mit unseren Wartungsfirmen, stellen wir zudem die schnelle Reaktion im Störungsfall sicher.

Redefining Hosting – Reinventing Security

kyberio.

Fragen
und Kontakt:

Kyberio
Am Mittelfelde 29
30519 Hannover
Telefon: 0511 - 71 260 0
Telefax: 0511 - 71 260 199
E-Mail: vertrieb@kyberio.de
www.kyberio.de

Design by Agentur für Markenschärfung Hannover, Icons: Freepik