Aus dem Nähkästchen:
Wie steht es um die Informationssicherheit in KMU?

18. Security Forum – Informationssicherheit in KMU

Vortragende:
Sebastian Harrand
Geschäftsführer Harrand Consulting GmbH

Bernd Schulz
Geschäftsführer F1 GmbH

Referent

harrand consulting gmbh

Sebastian Harrand

- Senior Consultant
- Geprüfter Datenschutzauditor
- Geprüfter ISMS-Auditor / 27001
- Auditleiter der DQS für ISO 27001 und TISAX
- Sicherheitsgutachter der TI der eGK
- Prüfverfahrenskompetenz nach § 8a III BSIG bei KRITIS-Betreibern

Tätigkeiten: Beratung

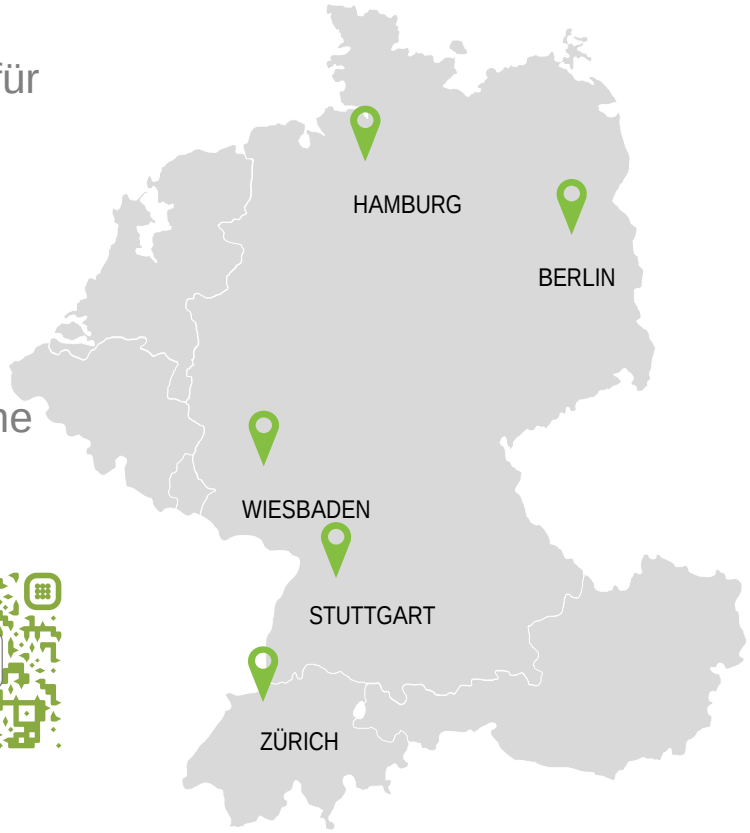
- Datenschutzmanagement
- externer Datenschutzbeauftragter
- Durchführung von Datenschutzaudits
- Informationssicherheitsmanagement
- Implementierung
- Auditierung
- Hinweisgeberschutz

Unternehmensvorstellung

Die harrand consulting gmbh ist Ihr Partner für

- Datenschutz
- Informationssicherheit
- Auditierungen
- Hinweisgeberschutz

Bundesweite und internationale Beratung mittelständischer Unternehmen und Konzerne zum Datenschutz- und Informationssicherheitsmanagement.



Kontakt:

www.harrand-consulting.de

18. Security Forum – Informationssicherheit in KMU

Bernd Schulz

- Senior Consultant
- Zertifizierter Sachverständiger nach DIN EN ISO/IEC 17024
- Consultant zur Vorbereitung von Unternehmen auf die DIN EN ISO/IEC 27001
- Gutachter für FuE Projekte im IT-Bereich

Tätigkeiten: Beratung

- externer Datenschutzbeauftragter
- externer Informationssicherheitsbeauftragter
- Beratung/Vorbereitung auf die Auditierung zur DIN EN ISO/IEC 27001
- Hinweisgeberschutz

KMU

18. Security Forum – Informationssicherheit in KMU

Klein- und Mittelständische Unternehmen (KMU)

Ein Unternehmen gilt als KMU, wenn es nicht mehrheitlich (unter 25 %) einem nicht-KMU gehört.

Obergrenze:
Es darf nicht mehr als 249 Beschäftigte haben.

Finanzielle Schwellenwerte:
Es darf einen Jahresumsatz von höchstens 50 Mio. € ODER eine Bilanzsumme von höchstens 43 Mio. € aufweisen.

Unterteilung nach Größenklassen
Mikrounternehmen: 1 bis 9 Beschäftigte.
Kleine Unternehmen: 10 bis 49 Beschäftigte.
Mittlere Unternehmen: 50 bis 249 Beschäftigte

Informationssicherheit

Informations- und IT-Sicherheit

harrand consulting gmbh

Übersicht Regulatorik

Gesetzliche Anforderungen

- DSGVO BDSG
- PDSG SGB X
- CSA Cyber Security Act
- AIA Artificial Intelligence Act
- EU-RL 2026/1148 KRITIS-V IT-Sicherheitsgesetz
- CRA Cyber Resilience Act
- NIS2 NIS2UmsuCG
- §§ 391, 393 SGB V
- DORA Digital Operational Resilience Act

Normative Anforderungen

- ISO/IEC 27001:2022 ISMS
- ISO/IEC 27799:2016 **ISMS Gesundheit**
- ISO/IEC 42001:2023 AIMS
- BSI IT-Grundschutz
- IEC TR 60601-4-5 SECURITY features of MEDICAL DEVICES
- ISA-62443 Security of industrial automation and control systems
- ISO/IEC 81001-1 Health Software & Health IT-Systems
- ISO 14971 Risikomanagement Für Medizinprodukte
- ISO/IEC 22301:2019 BCM

Bereichsspezifische Anforderungen

- B3S Finanzen Versicherungen
- B3S Gesundheit
- B3S IT und TK
- B3S Wasser
- B3S Transport Verkehr
- B3S Energie

18. Security Forum – Informationssicherheit in KMU

Informationssicherheit

... dabei handelt es sich um ein umfassendes Konzept zum Schutz von Daten und Informationssystemen vor Bedrohungen wie Missbrauch, unbefugtem Zugriff, Verlust oder Zerstörung, basierend auf den drei Grundpfeilern Vertraulichkeit (nur Befugte sehen Daten), Integrität (Daten sind unverändert und korrekt) und Verfügbarkeit (Daten sind jederzeit zugänglich). Sie umfasst technische (z.B. Firewalls, Verschlüsselung) und organisatorische Maßnahmen (z.B. Schulungen, Prozesse), um die Informationswerte eines Unternehmens langfristig zu sichern!

Gefahren im Bereich der Informationssicherheit

18. Security Forum – Informationssicherheit in KMU

Ransomware

Eines der größten aktuellen Risiken ist die Cyberkriminalität, vor allem in Form von Ransomware-Angriffen.
Deutschland gehört zu den Ländern mit hoher Ransomware-Gefährdung, betroffen sind insbesondere kleine und mittelständische Unternehmen (KMU) sowie öffentliche Einrichtungen.

Beispiele und Anmerkungen zu Ransomware

18. Security Forum – Informationssicherheit in KMU

Phishing und Social Engineering

Ein zentrales Einfallstor für Angriffe sind Phishing-E-Mails und andere Formen des Social Engineering. Dabei werden Menschen gezielt manipuliert, um Passwörter, Zugangsdaten oder vertrauliche Informationen preiszugeben.

Moderne Phishing-Mails sind oft äußerst täuschend gestaltet, nicht zuletzt durch den Einsatz von künstlicher Intelligenz (KI), die Mail-Texte personalisiert und realistisch gestaltet.

Beispiele und Anmerkungen zu Phishing und Social Engineering

18. Security Forum – Informationssicherheit in KMU

Bedrohung durch staatliche Akteure und Spionage

Neben klassischen Kriminellen *sehen Sicherheitsbehörden auch staatliche Akteure als wachsende Gefahr*:
Hackergruppen mit politisch motivierten Zielen oder im Auftrag ausländischer Nachrichtendienste zielen auf *Regierungsbehörden, kritische Infrastruktur oder strategisch wichtige Unternehmen.*

Beispiele und Anmerkungen zur Bedrohung durch staatliche Akteure und Spionage

18. Security Forum – Informationssicherheit in KMU

Angriffe auf kritische Infrastruktur

Kritische Infrastrukturen – etwa Energie-, Wasser- oder Telekommunikationsnetze – sind essenziell für das Funktionieren des öffentlichen Lebens.

Experten warnen, dass deren Schutz oft unzureichend ist und dass *technische Details leicht online zugänglich sind*, was das Risiko von Sabotage, Spionage oder gezielten Cyberangriffen erhöht.

Beispiele und Anmerkungen zu Angriffen auf kritische Infrastrukturen

Schwachstellen in Lieferketten und Software

Ein weiteres großes Risiko sind Lieferkettenangriffe. Dabei schleusen Angreifer Schadsoftware über Drittanbieter-Software, Bibliotheken oder vernetzte Systeme in eigentlich sichere Netzwerke ein.

Gerade die deutsche Industrie – von Maschinenbau bis Automotive – *nutzt viele Drittsoftware-Komponenten.* Wenn diese nicht ausreichend geprüft werden, kann ein einziger Schwachpunkt ganze Produktionsketten lahmlegen.

Beispiele und Anmerkungen zu Schwachstellen in Lieferketten und Software

18. Security Forum – Informationssicherheit in KMU

Künstliche Intelligenz als doppelte Klinge

Künstliche Intelligenz verändert die Informationssicherheit auf zweierlei Weise:

Für Verteidiger: KI kann helfen, Anomalien schneller zu erkennen, Angriffe zu analysieren und Abwehrsysteme zu verbessern.

Für Angreifer: Sie wird dazu verwendet, personalisierte Phishing-Kampagnen zu erstellen, Malware dynamisch anzupassen oder Deepfakes für Betrug einzusetzen. Beispielsweise kann KI reale Stimmen oder Gesichter klonen und so Mitarbeiter täuschen, Anweisungen auszuführen, die sie sonst nicht geben würden.

Beispiele und Anmerkungen zu Künstlicher Intelligenz als doppelte Klinge

Mangel an Fachkräften und Sicherheitskultur

Ein oft unterschätzter Risikofaktor ist der Fachkräftemangel im Bereich IT-Sicherheit. Es fehlen in Deutschland zehntausende Spezialisten, was die effektive Absicherung von Unternehmen und Behörden erschwert.

Ebenso ist die Sicherheitskultur – also das Bewusstsein und Grundverständnis für Risiken bei Mitarbeitern – entscheidend. Viele Angriffe beginnen mit einem menschlichen Fehler, nicht mit einem technischen Versagen.

Beispiele und Anmerkungen zu Mangel an Fachkräften und Sicherheitskultur

SCHLUSSFOLGERUNGEN

18. Security Forum – Informationssicherheit in KMU

Die Gefahren im Bereich der Informationssicherheit sind vielschichtig und entwickeln sich ständig weiter. Technische, organisatorische und menschliche Faktoren spielen zusammen. Um diesen Bedrohungen zu begegnen, braucht Deutschland:

- stärkere Umsetzung von Sicherheitsstandards in öffentlichen und privaten Institutionen,
- internationale Zusammenarbeit,
- Entwicklung des Bewusstseins dafür, dass Informationssicherheit ein gesamtgesellschaftliches Thema ist!

Danke für die Aufmerksamkeit!

Sebastian Harrand / Bernd Schulz

harrand consulting gmbh

harrand-consulting.de

tercenum.de

www.f1-gmbh.de
+49 (30) 565862610
info@f1-gmbh.de