MOORE Deutschland

Cyber Security – die verbindlichen Standards von Moore Global

Carol Haßelmans

MOORE Deutschland

Warum ist Cyber Security wichtig?

1. Schutz vor gängigen Bedrohungen
2. Risiko-Minimierung
3. Compliance-Anforderungen
4. Vertrauen der Stakeholder
5. Bereitschaft zur Meldung von Vorfällen
6. Wettbewerbsvorteil
7. Datenschutz

MOORE Deutschland

- **Schutz vor gängigen Bedrohungen**
  - Abwehr von Malware, Phishing, Ransomware, Social Engineering
  - Reduzierung von Ausfallzeiten und finanziellen Schäden

- **Risiko-Minimierung**
  - Identifikation und Priorisierung von Schwachstellen
  - Proaktives Management von Cyber-Risiken

MOORE Deutschland

- **Compliance Anforderungen**
  - Erfüllung gesetzlicher Vorgaben (z. B. DSGVO, ISO 27001)
  - Vermeidung von Bußgeldern und Reputationsschäden

- **Vertrauen der Stakeholder**
  - Kunden und Partner erwarten sichere Prozesse
  - Stärkung der Markenreputation durch IT-Sicherheit

MOORE Deutschland

- **Bereitschaft zur Meldung von Vorfällen**
  - Klare Prozesse zur Incident Response
  - Förderung einer Sicherheitskultur im Unternehmen
  - Minderung der Auswirkung von Vorfällen durch klar definierte Abläufe

- **Wettbewerbsvorteil**
  - Cyber Security als Differenzierungsmerkmal
  - Kundenbindung durch transparente Sicherheitsstandards

MOORE Deutschland

➢ Datenschutz

- Sicherstellung der Vertraulichkeit personenbezogener Daten
- Einhaltung von Datenschutzgesetzen

MOORE Deutschland

Modelle von MGNL zur Umsetzung von Cyber Security

Modell 1: Cybercore – empfohlene Best Practice

Modell 2: Cyberplus – mittlere Compliance

Modell 3: Cyberelite – erhöhte Compliance

MOORE Deutschland

Modell 1 – Cybercore

- Cyber Risk Assessment, mindestens aber ein Cyber Risk Register
- Komplexitätsanforderungen für Passwörter (mindestens 12 Zeichen, Groß- & Kleinbuchstaben, Ziffer, Sonderzeichen), optimal regelmäßige Passwortänderungen
- Datenverschlüsselung bei Übertragung (zB SSL)
- Grundlegende Sicherheitsmaßnahmen (Firewall, Antivirus)
- Access control management (need-to-know basis, 2FA)
- Mitarbeiterschulungen und Awareness-Programme
- Vulnerability Management (laufende Überwachung und ggf. Patching)
- Notfallwiederherstellungsplan

MOORE Deutschland

Modell 2 – Cyberplus

- Alle Maßnahmen von Modell 1
- Erweitertes Cyber Risk Assessment (basierend auf entsprechenden Standards) incl. Asset & Threat Identification
- Vulnerability assessment & remediation (ISO 27001 oder COBIT)
- Penetration testing
- Netzwerk Segmentierung
- I(ntrusion)P(revention)S(ystem) zur Erkennung und Abwehr von Angriffen
- Dokumentierte Sicherheitsrichtlinien und Notfallpläne

MOORE Deutschland

Modell 3 – Cyberelite

- Alle Anforderung der Modelle 1 und 2
- Strenge Compliance-Standards (ISO 27001, TISAX, NIST)
- Planung & regelmäßiger Test von Sicherheitsvorfällen
- Mindestens jährliche Überprüfung des Notfallwiederherstellungsplans und des Geschäftsfortführungsplans
- Vollständig integriertes Cyber Security Management System
- Einrichtung eines Security Operations Center (SOC)

MOORE Deutschland

Fragen? Kommentare? Erfahrungen? Meinungen?

MOORE Deutschland

Danke für Eure Aufmerksamkeit!

Und viel Spaß bei der Umsetzung der Standards... ;)

MOORE Deutschland

WANDEL ERFOLGREICH GESTALTEN