INFOSHEET ➜ CYBERSECURITY ASSESSMENT

Die Cybersicherheit hat für Unternehmen heute oberste Priorität. Cyberangriffe stören die betrieblichen Abläufe und führen zu Imageschäden und finanziellen Strafen. Die Geschäftsleitung muss den Stand der Cybersicherheit in ihrem Unternehmen kennen und eine Strategie zur effizienten Risikominderung umsetzen.

VORTEILE

Ein 360° Cybersecurity Assessment schärft Ihr Bewusstsein für potenzielle Risiken, identifiziert Lücken und Schwachstellen und schützt letztlich den Ruf und das finanzielle Wohlergehen Ihres Unternehmens. Indem Sie Risiken proaktiv angehen und mindern, schützen Sie nicht nur sensible Daten, sondern fördern auch das Vertrauen Ihrer Kunden und sorgen für langfristige Stabilität in der digitalen Landschaft. Im Grunde handelt es sich um eine strategische Investition in die Sicherheit und den nachhaltigen Erfolg Ihres Unternehmens.

ASSESSMENT-PROZESS

Je nach Wahl des Pakets umfasst der Assessment Prozess folgendes:

1. Fragebogen für Sie und Fragebogen für Ihre Mitarbeiter
2. Überprüfung der Dokumentation
3. Interviews mit IT und Unternehmen
4. Schwachstellentests
5. Berichte für die Führungsebene mit Zusammenfassung, Reifegrad, Testergebnissen, Probleme und Empfehlungen mit Aktionsplänen zur Risikominimierung.

Mit drei Packages bewertet das SPIE 360° Cyber Risk Assessment den Reifegrad Ihres Kontrollrahmens und gibt Ihnen Empfehlungen, wie Sie Ihre Sicherheitslage auf effiziente Weise verbessern können:

EVALUATE

Einsteiger-Check-up

Mit dem **Evaluate-Paket** wird der Zustand Ihres Kontrollrahmens anhand von Interviews und Schnellprüfungen überprüft und es wird ermittelt, ob Ihre Kontrollen den besten Praktiken und Standards entsprechen.

ENABLE

Bewertung der Wirksamkeit

Im Rahmen des **Enable-Pakets** wird ausserdem überprüft, ob die Kontrollen wirksam sind, indem umfassende Tests mit Tools durchgeführt werden.

EMPOWER

Individuelle und umfassende Tests

Das **Empower-Paket** stellt sicher, dass Ihre Cybersicherheitskontrollen die Anforderungen Ihres Unternehmens erfüllen, indem es auf der Grundlage jahrelanger Erfahrung massgeschneiderte, gründliche Tests durchführt.

ÜBER SPIE ICS

Unsere Werte (Leistung, Kundennähe und Verantwortung) und unser umfassendes Lösungsportfolio machen uns zum idealen Partner für kleine, mittlere und grosse Unternehmen.

Unsere Dienstleistungen basieren auf branchenweiten Best Practices, aktuellen Zertifizierungen und modernen, prozessorientierten Methoden.

swiss safety center – ISO 9001 ISO 14001 ISO 45001 – certified system
swiss safety center – ISO 27001 – certified system
swiss safety center – ISO 20000 – certified system

IPMA Hermes PRINCE2 ITIL

KONTAKTIEREN SIE UNS

SPIE ICS AG
Freiburgstrasse 251
CH-3018 Bern

Telefon +41 58 301 11 11
info.ch@spie.com
www.spie.ch

DOMAIN	SERVICES	EVALUATE	ENABLE	EMPOWER
Governance	Information System Landscape	✓	✓	✓
	Sicherheitsorganisation und Governance	✓	✓	✓
	Grundlegende Datenschutzanforderungen (GDPR, FADP)	✓	✓	✓
	Verwaltung der IT-Partner (Sicherheitsanforderungen, KPI und SLA)	*Optional*	*Optional*	✓
	TrustMetric-Risikobewertung und Peer-Vergleich	✓	✓	✓
Processes	Identitäts- und Zugangsverwaltungsprozess (inkl. Zugangskontrollen, Authentifizierung, Autorisierung, Joiner-Mover-Leaver und Überprüfung)	✓	✓	✓
	IT-Betriebsprozess (Infrastruktur und Anwendungsinventar, Patching, Protokollierung und Überwachung, Sicherung und Wiederherstellung)	✓	✓	✓
	Reaktion auf einen Vorfall mit Incident Response, zur Aufrechterhaltung des Geschäftsbetriebs und zur Wiederherstellung	✓	✓	✓
Technology	Wichtige Sicherheitskontrollen für Endgeräte und Netzwerke	✓	✓	✓
	TrustMetric – Erkennung externer Schwachstellen	✓	✓	✓
	Schwachstellentests für Windows-Endpunkte	✗	✓	✓
	Netzsicherheit (Firewall, Switches, Netzsegmentierung, Bewertung)	✗	✓	✓
	Active-Directory-Sicherheitsstatus	✓	✓	✓
	Überprüfung der Benutzer- und Passwortrichtlinien sowie der Computer, die der Domäne bekannt sind	✗	✓	✓
	MS 365 Best Practices für Benutzer und Administrator	*Optional*	*Optional*	✓
	Azure-Best-Practices	*Optional*	*Optional*	✓
	E-Mail-Sicherheit	✓	✓	✓
	Prüfung der Vollständigkeit und Genauigkeit des Inventars	✗	✗	✓
People	Bewertung des Reifegrads der Mitarbeiter (Online-Fragebogen)	✓	✓	✓
	Durchführung eines Phising-Angriffs per E-Mail	*Optional*	*Optional*	*Optional*
	REPORTING-SERVICE	**EVALUATE**	**ENABLE**	**EMPOWER**
	Standardberichte mit Schlüsselnachweisen und Schlüsselkontrollen (PowerPoint-Format)	✓	✓	✓
	Detaillierte Testergebnisse mit Nachweisen	✓	✓	✓
	Detaillierter Bericht mit erkannten Problemen und Empfehlungen	✗	*Optional*	✓
	Zusammenfassung	✗	*Optional*	✓
	Präsentation und Massnahmenplan	✓	✓	✓