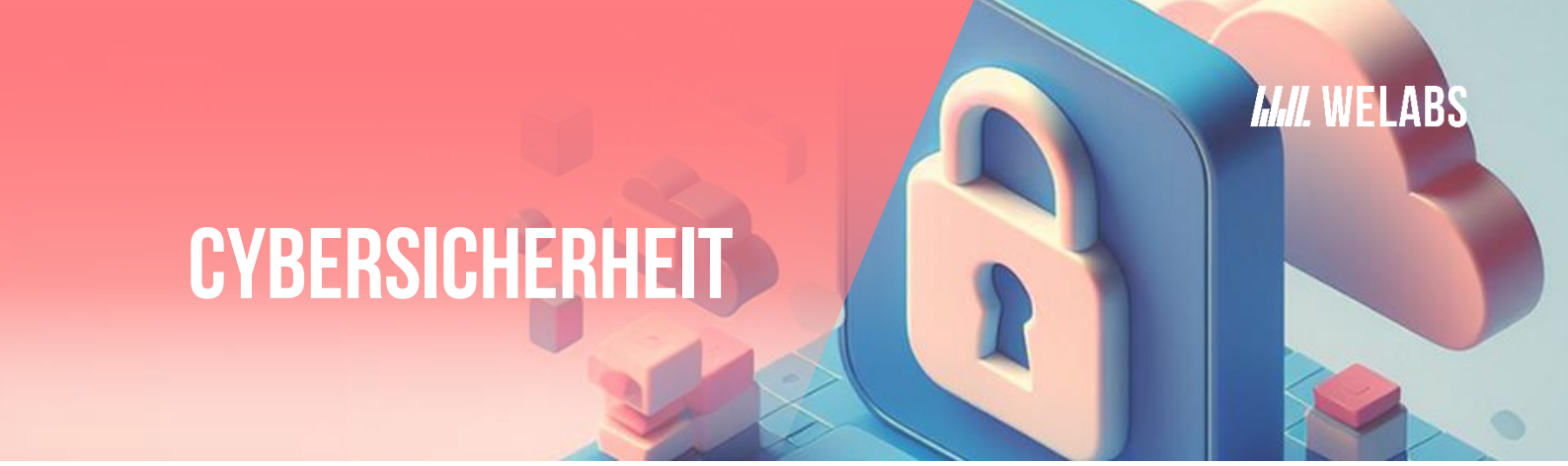
WELABS

CYBERSICHERHEIT



Auswirkungen für Unternehmen

Cyberangriffe bedrohen Unternehmen in vielfältiger Weise, vor allem durch den **Diebstahl sensibler Daten** wie Kundeninformationen und **geistigem Eigentum**. Die finanziellen Konsequenzen umfassen direkte **Kosten für Systemwiederherstellung, Geldbußen und Umsatzeinbußen durch Betriebsunterbrechungen**. Der Verlust von Kundendaten verstärkt diese Auswirkungen und kann zu einem **erheblichen Reputationsverlust** führen, der langfristige Umsatz- und Marktanteilsbeeinträchtigungen nach sich zieht. Um sich zu schützen, müssen Unternehmen erhebliche **Ressourcen in Cybersicherheit investieren**, einschließlich Schulungen, fortschrittlicher Sicherheitstechnologien und kontinuierlicher Überwachung. Eine **ganzheitliche Strategie** ist erforderlich, um effektiv Daten, Reputation und finanzielle Stabilität zu bewahren.

Welche Arten von Cyberangriffen gibt es?

MALWARE-ANGRIFFE

Viren, Trojaner und **Würmer**
sind Schadprogramme, die sich an Dateien anhängen oder als vermeintlich nützliche Software tarnen, um sich zu verbreiten. Dabei können sie schädliche Funktionen ausführen oder sich selbständig replizieren.

Ransomware
Daten werden verschlüsselt und Cyberkriminelle verlangt von Opfern eine Lösegeldzahlung für die Freigabe der Daten.

PHISHING-ANGRIFFE

E-Mail-Phishing
Täuschende E-Mails, die versuchen, vertrauliche Informationen wie Benutzernamen und Passwörter zu stehlen.

Spear Phishing
Gezielte Phishing-Angriffe, bei denen die Angreifer Informationen über das potenzielle Opfer verwenden, um ihre Chancen auf Erfolg zu erhöhen.

NETZWERKANGRIFFE & UNSICHER ENDGERÄTE

Denial-of-Service (DoS) / Distributed Denial-of-Service (DDoS) Angriffe

Überlastung eines Systems, Netzwerks oder Dienstes, um es für legitime Benutzer unzugänglich zu machen. Angriffe aus mehreren Quellen werden als DDoS-Angriffe bezeichnet.

Unsere Endgeräte

resultieren aus Faktoren wie veralteten Betriebssystemen, fehlender Sicherheitssoftware, schwachen Passwörtern und unsicheren Konfigurationen.

SICHERHEITSLÜCKEN

Datenlecks

sind unbefugte Freigabe sensibler Informationen, verursacht durch versehentliches Versenden, Speichern oder Sicherheitslücken. Dies kann dazu führen, dass vertrauliche Daten in die Hände Unbefugter gelangen.

Datenschutzverletzungen

sind unerlaubte Offenlegungen oder Zugriffe auf personenbezogene Daten z.B. Mitarbeiter- oder Kundendaten, die die Privatsphäre von Einzelpersonen gefährden können.

Diese und viele weitere Bedrohungen stellen komplexe Herausforderung dar, gerade das Thema Phishingmails gewinnt immer mehr an Bedeutung und kann mit einer geschulten Anti-Phishing Kampagne für Mitarbeiter: innen effektiv sensibilisiert und bekämpft werden. Wir von Welabs können Euch bei der Implementierung und Umsetzung einer optimalen Cybersicherheits-maßnahme unterstützen und den Einstieg in diesen Bereich ermöglichen. Besucht uns dafür gerne auf unsere Webseite und erfahrt mehr.