Incident Response – Checkliste für KMU

Ein Incident Response Plan definiert das Vorgehen und die Zuständigkeiten im Fall einer (vermuteten) IT-Sicherheitsverletzung.

Bearbeiten und definieren Sie die folgenden Punkte und halten Sie die Ergebnisse schriftlich fest. Ihr so entstehender Incident Response Plan sollte von allen beteiligten Personen jederzeit abrufbar sein – auch wenn kein sicherer Zugriff auf Ihre IT-Systeme möglich ist.

1.	**Vorbereitung**	
	Verantwortlichkeiten für IT und IT-Sicherheit festlegen	
	Kontaktliste mit Zuständigkeiten, Befugnissen und Erreichbarkeit erstellen	
	Bei Bedarf externe Unterstützung für Sicherheitsvorfälle sicherstellen	
	Bestandsaufnahme der IT-Systeme und -Ressourcen	
	Geschäftskritische Assets und Prozesse identifizieren	
	Bedrohungsmodellierung: Risiken und Schwachstellen priorisieren	
	Erstellen und Veröffentlichen von Erstmaßnahmen bei IT-Sicherheitsvorfällen	
	Kommunikationsabläufe nach innen und außen (z.B. Presse) definieren	
	Externe Meldewege für Sicherheitsvorfälle vorbereiten	
	Alternativen Kommunikationskanal etablieren	

2.	**Bewältigung**	
	Alle definierten Ansprechpartner kontaktieren und informieren	
	Betroffene User befragen (was, wann, wo, wie?)	
	Relevante Sachverhalte dokumentieren	
	Systemprotokolle, Logdateien sammeln und sichern	
	Betroffene Personen informieren (Mitarbeitenden, ggf. Kunden/Partner)	
	Meldepflichten befolgen	

Blechturmgasse 11 | 1050 Wien | Österreich | Tel.: +43 1 589 95-0 | E-Mail: office@ikarus.at | www.IKARUSsecurity.com

3.	**Nachbereitung**	
	Aufgedeckte Sicherheitslücken oder Schwachstellen schließen	
	Netzwerk und IT-Systeme besonders gründlich beobachten	
	bestehende Regelungen, Prozesse und Maßnahmen überprüfen und optimieren	
	Dokumentationen zum Notfallmanagement aktualisieren	
	IT-Sicherheitsarchitektur weiterentwickeln	

Diese Checkliste kann kleineren Unternehmen als Ausgangspunkt für die Erstellung eines effektiven Incident Response Plans dienen. Die aufgeführten Maßnahmen tragen nicht nur dazu bei, die Abwehr zu stärken und potenzielle Sicherheitsvorfälle frühzeitig zu erkennen. Sie ermöglichen auch eine effektive Reaktion im Ernstfall, um potenzielle Schäden zu minimieren, die Geschäftsfähigkeit schnell wieder herzustellen und die Cyber-Resilienz langfristig zu stärken.

Links:

Bedrohungsmodellierung: ein praxisnaher Leitfaden

Incident Response: Leitfaden zur Bewältigung von IT-Sicherheitsvorfällen

Über IKARUS Security Software GmbH

Seit 1986 entwickelt und betreibt das österreichische Privatunternehmen IKARUS Security Software führende Cyber Security Technologien. Mit effizienten Cloud-Lösungen, Incident Response Services, einer modularen Threat Intelligence Plattform und Services zur Absicherung kritischer Infrastrukturen schützt IKARUS Unternehmen jeder Größe.

Die eigene Malware Scan Engine und das österreichische Rechenzentrum sorgen für volle Transparenz und Sicherheit bei der Datenverarbeitung. Kunden schätzen zudem den persönlichen technischen Support direkt vom Hersteller.

Blechturmgasse 11 | 1050 Wien | Österreich | Tel.: +43 1 589 95-0 | E-Mail: office@ikarus.at | www.IKARUSsecurity.com