Checkliste

Themen für Ihren Incident-Response-Plan für Cybersicherheit

Vor einem Vorfall

- [ ] Liste wichtiger Daten und Systeme erstellen
- [ ] Backups Ihrer Daten erstellen
- [ ] Antivirus, Firewall und andere Sicherheitstools implementieren
- [ ] Standardisierte Sicherheitsprotokolle erstellen
- [ ] Mitarbeiter zu Best Practices für Cybersicherheit schulen
- [ ] Reaktionsplan erstellen und Rollen zuweisen
- [ ] Interne und externe Kommunikationspläne entwickeln
- [ ] Pläne testen und üben (Tabletop-Übungen, Simulationen)
- [ ] Auf Bedrohungen überwachen, etwa ungewöhnliche Netzwerkaktivitäten, veränderte Dateien, verdächtige Logins

Während eines Vorfalls

- [ ] Reaktionsplan einleiten
- [ ] Betroffene Systeme isolieren
- [ ] Malware und Backdoors entfernen
- [ ] Sicherheitslücken patchen
- [ ] Systeme auf einwandfreie Versionen zurücksetzen
- [ ] Beweismittel (Protokolle, Dateien, Datenträger-Images) aufbewahren

Nach einem Vorfall

- [ ] Protokolle analysieren, um die Ursache des Lecks zu diagnostizieren
- [ ] Umfang des Lecks ermitteln
- [ ] Kunden, Stakeholder und Behörden gemäß gesetzlichen Vorschriften benachrichtigen
- [ ] Externe Zulieferer und Strafverfolgungsbehörden einbeziehen
- [ ] Nachträgliche Prüfung durchführen
- [ ] Pläne und Sicherheitsprotokolle, Richtlinien und Training entsprechend Ergebnissen aktualisieren