Cyber Security Incident Response Plan für kleine und mittlere Unternehmen

Cyber Security Incident Response Plan (CSIRP) für kleine und mittlere Unternehmen (KMU).

Dieser Plan ist als Leitfaden gedacht und sollte entsprechend den spezifischen Bedürfnissen und Gegebenheiten deines Unternehmens angepasst werden.

1. Einleitung:

Der Cyber Security Incident Response Plan (CSIRP) dient dazu, sicherzustellen, dass dein Unternehmen angemessen auf Cyber-Sicherheitsvorfälle reagieren kann, um Schäden zu minimieren und den Betrieb so schnell wie möglich wiederherzustellen.

Du musst kein Unternehmen mit 20 Mitarbeitern sein, um Opfer einer Cyberattacke zu werden. Im Zweifel ist Hackern dein Unternehmen, Größe oder Umsatz vollkommen egal. Die Angriffe von Hackern laufen heute automatisiert ab. Im dümmsten Fall bist du oder dein Unternehmen einfach nur Beifang einer größeren Attacke.

Alle hier beschriebenen Maßnahmen lassen sich auch in kleinen Betrieben umsetzen.

2. Ziele:

- Früherkennung und schnelle Reaktion auf Sicherheitsvorfälle.
- Minimierung von Schäden und Datenverlust.
- Sicherstellung der Geschäftskontinuität.
- Schutz von Unternehmensdaten, Kundeninformationen und geistigem Eigentum.

3. Verantwortlichkeiten:

- Benennung eines **Incident Response Teams (IRT)** mit klaren Rollen und Verantwortlichkeiten.
- Ernennung eines **Incident Response Managers (IRM)** zur Koordinierung der Reaktion.

4. Vorbeugende Maßnahmen:

- Implementierung von Firewalls, Intrusion Detection/Prevention Systemen (IDS/IPS) und Antivirensoftware.
- Regelmäßige Aktualisierung von Betriebssystemen und Anwendungen.
- Schulung der Mitarbeiter in Bezug auf Cyber-Sicherheit.

5. Erkennung und Meldung:

- Überwachung von Netzwerk- und Systemaktivitäten.
- Nutzung von SIEM (Security Information and Event Management)-Tools zur Erkennung von Anomalien.
- Einrichtung eines Meldeverfahrens für Mitarbeiter, um Verdachtsfälle zu melden.

6. Klassifizierung und Eskalation:

- Klassifizierung von Vorfällen nach Schweregrad und potenziellen Einfluss.
- Definition von Eskalationsstufen und Kontaktinformationen für die Meldung an das IRT.

7. Reaktion:

- Sofortige Trennung des betroffenen Systems vom Netzwerk (Isolierung).
- Sammeln von Beweisen, Protokollen und Informationen zum Vorfall.
- Analyse des Vorfalls, um den Angriffstyp und den Umfang zu verstehen.

8. Eindämmung und Wiederherstellung:

- Wiederherstellung betroffener Systeme aus verifizierten Backups.
- Überprüfung und Aktualisierung der Sicherheitsmaßnahmen.
- Schließen von Sicherheitslücken und Schwachstellen.

9. Kommunikation:

- Kommunikation mit internen und externen Stakeholdern, darunter Mitarbeiter, Kunden, Partner und Behörden.
- Erstellung von Kommunikationsvorlagen für verschiedene Szenarien.
- Stelle sicher, die Kontaktdaten aller Ansprechpartner verfügbar zu machen.
- Beachte Erreichbarkeiten während Urlaub, Feiertagen und bei Krankheit.
- Stelle alle Kontaktdaten außerhalb deines Netzwerkes zur Verfügung.

10. Berichterstattung und Dokumentation:

- Erstellung eines detaillierten Vorfallberichts, der die Ursachen, Auswirkungen, durchgeführten Maßnahmen und Empfehlungen umfasst.
- Erfassung und Aufbewahrung aller relevanten Informationen und Protokolle.

11. Nachbereitung und Lernen:

- Evaluierung der Reaktion des IRT und Identifizierung von Verbesserungsmöglichkeiten.
- Schulung der Mitarbeiter anhand des Vorfalls, um zukünftige Vorfälle zu verhindern.
- Aktualisierung des CSIRP entsprechend den gewonnenen Erkenntnissen.

12. Wiederherstellung des Normalbetriebs:

- Überwachung der Systeme nach der Wiederherstellung, um sicherzustellen, dass keine weiteren Angriffe stattfinden.
- Rückkehr zum Normalbetrieb nach Abschluss der Reaktion und Eindämmung.

Es ist ratsam, den Plan regelmäßig zu überprüfen und zu aktualisieren, um sicherzustellen, dass er immer auf dem neuesten Stand ist und den aktuellen Bedrohungen und Gegebenheiten entspricht.

Du kannst mit all den Buzzwords nichts anfangen?
Du benötigst weitere Informationen zu Zero Trust?

Kontakt: R.Henrici henrici@jkaref.com
Telefon: ++49 (0)30-555797650

Wen kann ich im Notfall kontaktieren?
Dieses Dokument ausdrucken, den Raum für Deine Notizen nutzen, z.B. Telefonnummern und andere analoge Kontaktmöglichkeiten hier eintragen: