Incident-Klassifizierungsrichtlinien

Klassifizierungsrichtlinien ermöglichen es dem Incident-Response-Team, Vorfälle schnell zu bewerten, die richtigen Ressourcen zuzuweisen und angemessene Reaktionsstrategien zu entwickeln. Sie fördern eine einheitliche Kommunikation und Dokumentation innerhalb des Unternehmens.

1. Kategorisierung nach Schweregrad

Kritisch:

- Vorfälle, die zu einem vollständigen Systemausfall oder zu einem erheblichen Datenverlust führen.
- Beeinträchtigen die Geschäftskontinuität oder die Sicherheit von sensiblen Daten.
- Sofortige Maßnahmen sind erforderlich.

Hoch:

- Vorfälle, die ernsthafte Auswirkungen auf die Systeme oder Daten haben, jedoch nicht zu einem vollständigen Ausfall führen.
- Erfordern eine schnelle Reaktion, um die Auswirkungen zu minimieren.

Mittel:

- Vorfälle, die potenziell schädlich sind, aber keine unmittelbaren Bedrohungen für die Systeme oder Daten darstellen.
- Erfordern eine Untersuchung, jedoch keine sofortige Reaktion.

Niedrig:

- Vorfälle, die geringfügige Auswirkungen haben oder als geringes Risiko eingestuft werden.
- Können in der Regel in regulären Wartungs- oder Überprüfungsprozessen behandelt werden.

2. Kategorisierung nach Art des Vorfalls

Malware:

Definition: Schadsoftware, die Systeme infiziert und schädliche Aktivitäten ausführt.
Beispiele: Viren, Würmer, Trojaner, Ransomware.
Reaktion: Isolierung betroffener Systeme, Durchführung von Malware-Analysen und Bereinigung.

Phishing:

Definition: Versuche, sensible Informationen durch betrügerische Emails oder

Webseiten zu erlangen.
Beispiele: Emails, die vorgeben, von vertrauenswürdigen Quellen zu stammen, um Benutzer zur Eingabe von Anmeldedaten zu verleiten.
Reaktion: Sensibilisierung der Mitarbeiter, Blockierung der Phishing-URLs und Analyse der betroffenen Konten.

Datenverlust:

Definition: Verlust oder Diebstahl von Daten, sei es durch menschliches Versagen oder böswillige Angriffe.
Beispiele: Verlust von Laptops mit sensiblen Daten, unzureichende Datensicherung.
Reaktion: Sofortige Untersuchung des Vorfalls, Benachrichtigung betroffener Personen und Implementierung von Maßnahmen zur Verhinderung zukünftiger Vorfälle.

Systemausfall:

Definition: Unerwartete Ausfälle von Systemen oder Diensten, die den Betrieb beeinträchtigen.
Beispiele: Stromausfall, defekte Hardware
Reaktion: Vorsorgen, redundant aufgestellt sein, Backups parat haben

Unbefugter Zugriff:

Definition: Versuche oder erfolgreiche Zugriffe auf Systeme oder Daten durch nicht autorisierte Personen.
Beispiele: Physischer Zugriff auf ungesicherte, unbeaufsichtigte Geräte, Hackerangriffe
Reaktion: Sofortige Unterbindung des Zugriffs, Isolierung mit nachfolgender Untersuchung des eventuell entstanden Schadens bzw. Verlust von Daten

3. Kategorisierung nach betroffenen Ressourcen

Netzwerk:

- Vorfälle, die das Netzwerk betreffen, z. B. DDoS-Angriffe.

Anwendungen:

- Vorfälle, die spezifische Anwendungen oder Software betreffen.

Daten:

- Vorfälle, die sich auf Datenbanken oder Datenspeicher auswirken.

Hardware:

- Vorfälle, die physische Geräte oder Infrastruktur betreffen.

4. Kategorisierung nach Ursprung

Intern:

Vorfälle, die durch interne Mitarbeiter oder Systeme verursacht werden.

Extern:

Vorfälle, die von externen Angreifern oder Bedrohungen ausgehen.