CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

CloudCommand GmbH chr.schumacher@gmx.tm

Incident Response Fallbeispiel

Vorbereitungsphase

Schritt 1: Identifizierung der Incident-Response-Teammitglieder

- Der Sicherheitsbeauftragte, John, identifiziert und benennt die Mitglieder des Incident-Response-Teams. Dies umfasst Sicherheitsexperten, IT-Administratoren, Rechtsberater und Kommunikationsexperten.

Vorbereitungsphase

Schritt 2: Erstellung eines Incident-Response-Plans

- John und das Team erstellen einen Incident-Response-Plan, der die Verfahren und Verantwortlichkeiten für den Umgang mit Sicherheitsvorfällen festlegt. Dieser Plan wird regelmäßig überprüft und aktualisiert.

Vorbereitungsphase

Schritt 3: Definition von Incident-Kategorien und Schweregraden

- Das Team definiert die verschiedenen Arten von Sicherheitsvorfällen, die auftreten könnten, und weist ihnen Schweregrade zu. Dies hilft bei der Priorisierung und Reaktion

Vorbereitungsphase

Schritt 4: Einführung von Sicherheitsmaßnahmen

- Das Unternehmen implementiert präventive Sicherheitsmaßnahmen wie Firewalls, Intrusion Detection Systeme (IDS) und regelmäßige Software-Updates sowie Monitoring Tools, um Sicherheitslücken zu minimieren.

Vorbereitungsphase

Schritt 5: Schulung der Mitarbeiter

- Alle Mitarbeiter erhalten regelmäßige Schulungen zur Informationssicherheit, um das Bewusstsein für Sicherheitsrisiken und die Meldung von Vorfällen zu erhöhen.

Vorbereitungsphase

Schritt 6: Testen der Incident-Response-Verfahren

- Das Incident-Response-Team führt regelmäßige Übungen und Simulationen von Sicherheitsvorfällen durch, um sicherzustellen, dass alle Mitarbeiter mit den Verfahren vertraut sind und diese effektiv umgesetzt werden können.

Vorbereitungsphase

Schritt 7: Partnerschaften mit externen Experten

- Das Unternehmen identifiziert und knüpft Beziehungen zu externen Cybersecurity-Experten, Forensik-Unternehmen und rechtlichen Beratern, die im Falle eines Sicherheitsvorfalls hinzugezogen werden können.

Vorbereitungsphase

Schritt 8: Dokumentation und Protokollierung (übergreifend)

- Das Team erstellt und pflegt eine umfassende Dokumentation aller Incident-Response-Aktivitäten, einschließlich der ergriffenen Maßnahmen und der Kommunikation.

Vorbereitungsphase

Schritt 9: Kontinuierliche Verbesserung

- Das Unternehmen führt regelmäßige Überprüfungen und Audits der Incident-Response-Verfahren durch, um Schwachstellen zu identifizieren und Verbesserungen vorzunehmen.

Detection und Analysis

Schritt 1: Erkennung

- Das Security Operations Center verwendet ein SIEM-System und erhält Alarme über ungewöhnliche Netzwerkaktivitäten, die auf einen möglichen Sicherheitsvorfall hinweisen. Die Alarme umfassen ungewöhnlichen Datenverkehr auf einem internen Server und verdächtige Authentifizierungsversuche.

Detection und Analysis

Schritt 2: Alarmüberprüfung

- Das SOC-Team beginnt sofort mit der Überprüfung der Alarme. Sie überprüfen die Protokolle, um den Ursprung und die Art der verdächtigen Aktivität zu ermitteln.

Detection und Analysis

Schritt 3: Schweregradbewertung

- Das Team bewertet den Schweregrad des Vorfalls basierend auf der Art der Aktivität, ihrer möglichen Auswirkungen auf das Unternehmen und anderen relevanten Faktoren.

Detection und Analysis

Schritt 4: Verifizierung der Aktivität

- Das SOC-Team überprüft, ob die verdächtige Aktivität tatsächlich auf einen Angriff hinweist, indem sie sowohl technische als auch forensische Analysen durchführen. Dies kann das Untersuchen von Netzwerkprotokollen, Dateisystemen und Anwendungslogs umfassen.

Detection und Analysis

Schritt 5: Identifizierung von Angriffszielen

- Das Team identifiziert potenzielle Angriffsziele oder betroffene Systeme und Anwendungen, um den Umfang des Vorfalls besser zu verstehen.

Containment, Eradication, Recovery

Schritt 1: Incident-Response-Teamaktivierung

- Das Incident-Response-Team wird umgehend aktiviert, nachdem das IT-Sicherheitsteam verdächtige Aktivitäten auf mehreren Unternehmenssystemen bemerkt hat. Es besteht der Verdacht auf einen Ransomware-Angriff.

Containment, Eradication, Recovery

Schritt 2: Erstmaßnahmen

- Sofortige Trennung der betroffenen Systeme vom Netzwerk, um eine weitere Ausbreitung der Ransomware zu verhindern. Dies umfasst das Isolieren von infizierten Computern und das Abschalten von Netzwerkzugängen.

Containment, Eradication, Recovery

Schritt 3: Ransomware-Analyse

- Das Incident-Response-Team analysiert die Ransomware-Dateien und -Nachrichten, um den Angriffstyp, die Verbreitungsmethode und die Forderungen der Angreifer zu verstehen.

Containment, Eradication, Recovery

Schritt 4: Identifizierung der betroffenen Systeme

- Das Team ermittelt alle betroffenen Systeme und Anwendungen und erstellt eine Liste der kompromittierten Geräte und Daten.

Containment, Eradication, Recovery

Schritt 5: Datenwiederherstellung

- Das Unternehmen hat Backups seiner Daten und beginnt mit der Wiederherstellung von Daten von sicheren und unversehrten Quellen.

Containment, Eradication, Recovery

Schritt 6: Ransomware-Eradikation

- Das Team analysiert die Ursachen des Angriffs und sucht nach Schwachstellen, die vom Angreifer ausgenutzt wurden. Diese Schwachstellen werden behoben, um zukünftige Angriffe zu verhindern.

Containment, Eradication, Recovery

Schritt 7: System-Neuaufbau

- Betroffene Systeme werden von Grund auf neu aufgebaut und mit aktualisierter Sicherheitssoftware ausgestattet, um sicherzustellen, dass keine Ransomware-Rückstände verbleiben.

Containment, Eradication, Recovery

Schritt 8: Überwachung und Validierung

- Das Incident-Response-Team überwacht die Systeme weiterhin auf verdächtige Aktivitäten, um sicherzustellen, dass der Angriff vollständig eingedämmt und beseitigt wurde. Alle wiederhergestellten Daten werden ebenfalls auf Integrität und Vollständigkeit überprüft.

Post-Incident Activity

Schritt 1: Überprüfung der Sicherheitsmaßnahmen

- Das Unternehmen führt eine umfassende Überprüfung seiner Sicherheitsmaßnahmen durch, um Schwachstellen zu identifizieren und zu schließen, die zum Ransomware-Angriff geführt haben könnten.

Post-Incident Activity

Schritt 2: Kommunikation mit Kunden und Partnern

- Das Unternehmen informiert alle betroffenen Kunden und Geschäftspartner über den Vorfall und teilt ihnen mit, welche Maßnahmen ergriffen wurden, um ihre Daten zu schützen und den Geschäftsbetrieb wiederherzustellen.

Post-Incident Activity

Schritt 3: Datenschutzprüfung und Compliance

- Das Unternehmen arbeitet eng mit Datenschutzbehörden zusammen, um sicherzustellen, dass alle geltenden Datenschutzvorschriften eingehalten werden. Es werden auch zusätzliche Schritte unternommen, um die Compliance mit branchenspezifischen Standards zu gewährleisten.

Post-Incident Activity

Schritt 4: Incident-Response-Bericht

- Ein detaillierter Incident-Response-Bericht wird erstellt, der die gesamte Reaktion auf den Ransomware-Vorfall dokumentiert. Dieser Bericht enthält eine Zusammenfassung des Vorfalls, die ergriffenen Maßnahmen, die Lessons Learned und Empfehlungen zur Verbesserung der Sicherheit.

Post-Incident Activity

Schritt 5: Schulungen und Sensibilisierung

- Das Unternehmen investiert in Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiter, um das Bewusstsein für Sicherheitsrisiken zu schärfen und sicherzustellen, dass alle Mitarbeiter wissen, wie sie auf verdächtige Aktivitäten reagieren können.

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm