CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

CloudCommand GmbH chr.schumacher@gmx.tm

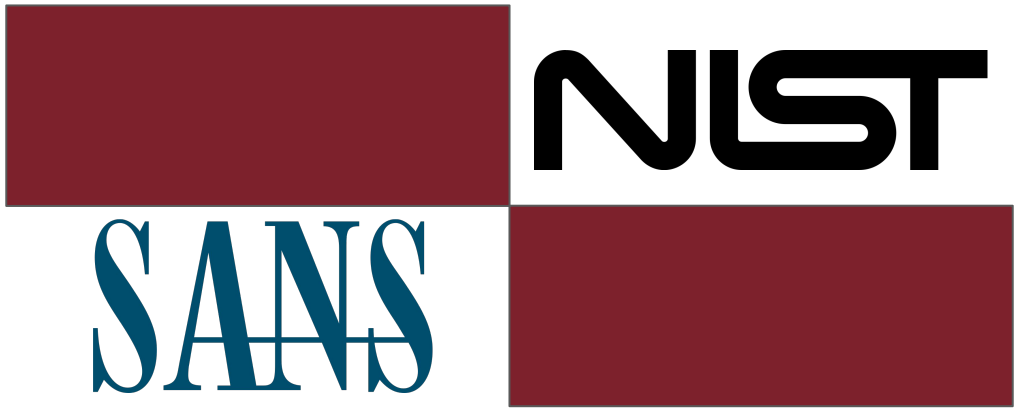
Grundlagen und Frameworks

Definition Incident Response

Incident Response (manchmal auch als Reaktion auf Cybersicherheitsvorfälle bezeichnet) bezieht sich auf die **Prozesse** und **Technologien** eines Unternehmens zur **Erkennung von** und **Reaktion auf Cyberbedrohungen, Sicherheitsverletzungen oder Cyberangriffe**. Das Ziel der Incident Response ist es, **Cyberangriffe zu verhindern**, bevor sie stattfinden, und die Kosten und die **Unterbrechung des Geschäftsbetriebs**, die sich aus einem Cyberangriff ergeben, zu **minimieren**.

Frameworks

NIST Incident Response Framework und SANS Incident Response Framework als globale Standards:



Frameworks

“Ein IT-Sicherheits-Framework ist eine **Serie dokumentierter Prozesse**, die benutzt werden, um **Richtlinien und Prozeduren** zu definieren, die sich mit der **Implementierung** und dem weitergehenden Management von Kontrollen der **Informations-Sicherheit** im Unternehmensumfeld beschäftigen.”

Frameworks

NIST Incident Response Framework:

- 1901 gegründet als Teil des US-Handelsministeriums
- Eines der ältesten Labore für Naturwissenschaften in den USA
- Entwicklung eines Incident Response Frameworks im Rahmen der Cybersicherheitsinitiativen (Beliebte Lösung für Organisationen weltweit)
- Bietet detaillierte Schritte zur Erstellung eines Incident Response Plans
- Enthält Anleitungen zur Bildung eines Incident Response Teams
- Legt Kommunikationsverfahren für den Umgang mit Sicherheitsvorfällen fest
- Bietet auch Schulungsszenarien für Mitarbeiter an

Der NIST Incident Response Lifecycle

1. Preparation
2. Detection and Analysis
3. Containment, Eradication, and Recovery
4. Post-incident activity

Der NIST Incident Response Lifecycle

Phase I: Vorbereitung

- Die Vorbereitungsphase umfasst die Aktivitäten, die eine Organisation durchführt, um sich auf die Reaktion auf Zwischenfälle vorzubereiten. Dies schließt die Bereitstellung geeigneter Werkzeuge und Ressourcen sowie die Schulung des Teams ein. In dieser Phase wird auch die Arbeit berücksichtigt, die unternommen wurde, um Zwischenfälle zu verhindern.

Der NIST Incident Response Lifecycle

Phase II: Detektion und Analyse

- Nach den Richtlinien des National Institute of Standards and Technology (NIST) stellt die präzise Identifikation und Bewertung von Zwischenfällen oft die größte Herausforderung für viele Organisationen bei der Bewältigung von Vorfällen dar.

Der NIST Incident Response Lifecycle

Phase III: Eindämmung, Ausrottung und Erholung

- Der Schwerpunkt dieser Phase liegt darauf, die Auswirkungen eines Vorfalls so gering wie möglich zu halten und Serviceunterbrechungen zu minimieren.

Der NIST Incident Response Lifecycle

Phase IV: Tätigkeit nach dem Ereignis

- Das Lernen und die Verbesserung nach einem Vorfall stellen einen der wichtigsten Aspekte der Reaktion auf Zwischenfälle dar, der jedoch häufig vernachlässigt wird. In dieser Phase erfolgt eine Analyse der Vor- und Reaktionsbemühungen. Die Ziele hierbei sind, die Auswirkungen des Vorfalls zu begrenzen und Möglichkeiten zu identifizieren, um künftige Reaktionsaktivitäten zu optimieren.

Frameworks

SANS Incident Response Framework:

- SANS Institute = privates, gewinnorientiertes Unternehmen in den USA, das 1989 gegründet wurde
- Spezialisiert auf Informationssicherheit, Cybersecurity-Schulungen und den Verkauf von Zertifikaten
- Framework erhielt weltweit Anerkennung für seine Vollständigkeit und Wirksamkeit
- Veröffentlichung eines 20-seitigen Handbuchs, das einen strukturierten 6-Schritte-Plan für das Incident Response-Verfahren enthält

Der SANS Incident Response Lifecycle

1. Preparation
2. Identification
3. Containment
4. Recovery
5. Lessons Learned

Der SANS Incident Response Lifecycle

Phase I: Preparation

- In der Vorbereitungsphase legt das Unternehmen die Grundlagen für ein effektives Incident Response-Verfahren. Dies umfasst die Entwicklung von Richtlinien und Verfahren, die Auswahl und Schulung von Teammitgliedern, die Bereitstellung von Ressourcen und die Schaffung von Kommunikationswegen. Eine gründliche Vorbereitung ist entscheidend, um schnell und effizient auf Sicherheitsvorfälle reagieren zu können.

Der SANS Incident Response Lifecycle

Phase II: Identification

- In dieser Phase werden Sicherheitsvorfälle erkannt und analysiert. Das Incident Response Team überwacht kontinuierlich Netzwerke und Systeme, um verdächtige Aktivitäten zu identifizieren. Die gesammelten Daten werden analysiert, um die Art und Schwere des Vorfalls festzustellen. Eine schnelle Erkennung und Analyse sind entscheidend, um Gegenmaßnahmen rechtzeitig einzuleiten.

Der SANS Incident Response Lifecycle

Phase III: Containment

- Die Eindämmungsphase konzentriert sich darauf, den Vorfall zu stoppen und weitere Schäden zu verhindern. Das Incident Response Team isoliert betroffene Systeme, deaktiviert Angriffe und entfernt schädlichen Code. Die schnelle und effektive Eindämmung ist entscheidend, um die Ausbreitung des Vorfalls einzuschränken.

Der SANS Incident Response Lifecycle

Phase IV: Recovery

- Nach erfolgreicher Eindämmung beginnt die Erholungsphase. Hier werden betroffene Systeme und Dienste wiederhergestellt. Sicherheitsverbesserungen werden implementiert, um zukünftige Vorfälle zu verhindern. Die Erholung zielt darauf ab, den normalen Betrieb wiederherzustellen und die Geschäftskontinuität sicherzustellen.

Der SANS Incident Response Lifecycle

Phase V: Lessons Learned

- Die Phase "Lessons Learned" dient der Reflexion und Verbesserung. Das Unternehmen bewertet den gesamten Vorfall, identifiziert Schwachstellen und Lerneffekte. Die gewonnenen Erkenntnisse werden genutzt, um Schulungen durchzuführen, Incident Response-Verfahren zu aktualisieren und die Sicherheitspraktiken zu verbessern. Dies trägt dazu bei, zukünftige Vorfälle effektiver zu bewältigen.

Das Prinzip Command, Control, Communication

Command:

- Angemessene Führung und Anleitung zur Überwachung der Reaktion.

Control:

- Verwaltung technischer Aspekte während des Incident Response, wie die Koordination von Ressourcen und die Zuweisung von Aufgaben.

Communication:

- Informierung von Behörden & Stakeholder

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm