Incident Response Plan LDAP-Server

Version: 1.0
Erstellt am: 09.10.2024
Erstellt von: Michael Herz, David Westmeyer, Andy Salewski

Inhaltsverzeichnis

1. Präambel

Dieser **Incident Response Plan (IRP)** definiert alle Maßnahmen zur Identifikation, Reduktion und der Wiederherstellung bei Sicherheitsvorfällen, welche den LDAP-Dienst auf dem Ubuntu-Biotic Server (**IP: 192.168.56.100)** betreffen.

Der LDAP-Server ist die Admin-Domäne des Unternehmens **Smooth Beans** uns damit entscheidend für die Verwaltung der Benutzer- und Berechtigungsdaten des Unternehmens.

Dieser Incident Response Plan stellt sicher, dass die **Integrität**, **Vertraulichkeit** und **Verfügbarkeit** der LDAP-Datenbank jederzeit gewährleistet ist.

2. Zielsetzung

- **Ziel:** Schutz der **Vertraulichkeit, Integrität** und **Verfügbarkeit** der **LDAP-Datenbank** und der darauf basierenden Dienste.
- **Umfang:** Fokus auf den LDAP-Server sowie dessen Sicherheitsinfrastruktur, einschließlich der laufenden Dienste (SSH, ClamAV, Fail2Ban, Suricata, Snort, rkhunter, UFW Firewall, AppArmor).

3. Vorbereitung

- **3.1 Incident Response Team:**
  - Bestimmung der Mitglieder des IRT durch die Geschäftsleitung, einschließlich IT-Sicherheits- und Systemadministrationsexperten und Kommunikationsexperten.
  - Regelmäßige Schulungen und Übungen zur Stärkung der Reaktionsfähigkeit sowie des Sicherheitsbewusstseins des Personals.
- **3.2 Ressourcen:**
  - Einsatz von Überwachugstools wie Suricata und Snort zur Detektion von Intusion und Anomalien im Netzwerkverkehr oder Benutzerverhalten.
  - Einsatz von ClamAV und rkhunter zur Maleware und Rootkit detektion sowie Fail2Ban zur Sperrung verdächtiger IP-Adressen.
  - Gewährleistung einer funktionierenden UFW-Firewall und AppAmor-Profilen zur Eindämmung unautorisierter Zugriffe.

- **3.3 Dokumentation:**

  - Erstellung und Pflege umfassender Sicherheitsdokumenationen, einschließlich der Benutzer- und Berechtigungsstrukturen sowie des Netzwerkplans.

  - Vorhalten von **Incident Reports**, welche folgende Kategorien abdecken:
    - *Standard Incident Reports*
    - *Datenschutzverletzungsberichte*
    - *Systemfehlerberichte*

  - Bereitstellung von E-Mail-Vorlagen zur schnellen Kommunikation mit der Belegschaft und den Stakeholdern.

4. Identifikation:

- **4,1 Monitoring:**
  - *Einrichtung/Angliederung an Log-Management-Lösungen wie **Wazuh,** zur Überwachung, Protokollierung und Auswertung von ergeinissen im Zusammenhang mit LADP, SSH, ClamAV und anderen relevanten Diensten.*

  - *Anwendung von Anomalieerkennung durch Snort und Suricata zur Identifikation von verdächtigen Aktivitäten, wie etwa unübliche Login-Versuche oder erhöhte Serverlast.*

- **4.2 Warnsystem:**
  - *Implementierung von Benachrichtigungen zur sofortigen Alarmierung des IRT bei identifizierten Sicherheitsvorfällen, einschließlich mehrerer fehlgeschlagener Anmeldeversuche oder ungewöhnlicher Zugriffsmuster.*
  -

5. Einschätzung:

- **5.1 Kategorisierung des Vorfalls:**
  - *Analyse des Vorfalls zur bestimmung des Typs (z.B. unerlaubter Zugriff, Datenverlust, Maleware-Infektion) und der Schwere des Vorfalls (kritsch, hoch, mittel, niedrig).*

- **5.2 Erfassen von Beweisen:**
  - *Umfassende Dokumentation sämtlicher relevanten Log-Dateien und Systemzustände zum Zeitpunkt des Vorfalls.*
  - *Erstellen eines foresischen Abbilds der betroffenen Systeme, wenn dies als Notwendig erachtet wird.*

6. Reaktion

- **6.1 Isolation:**
  - *Sofortige Trennung des LADP-Servers vom restlichen Netzwerk, um eine weitere Verbreitung von Angriffen oder Datenverlusten zu verhindern.*

- **6.2 Behebung:**
  - *Durchführen von Maleware-Scnas mit ClamAV und rkhunter und Implementation von Bereinigungsschriften zur Eliminierung von Bedrohungen*

  - *Überprüfung und Anpassung der Benutzerkonten und Berechtigungen bei Verdacht auf unbefugten Zugriff.*

- **6.3 Kommunikation:**
  - *Verwenden der Bereitgestellten E-Mail-Vorlagen zur schnellen Information des Managements, der Belegschadt und der Stakeholder über den Vorfall, die Auswirkungen, die eingeleiteten Maßnahmen sowie Anweisungen bezüglich des Verhaltens während des Vorfalls.*

7. Erholung

- **7.1 Wiederherstellung:**
  - *Wiederherstellung des LDAP-Servers anhand eines vorherigem, vertrauenswürdigen Backups (Borg-Backup).*
  - *Gründliche Überprüfung aller Systeme und Dienste auf ihre ordnungsmäßige Funktionalität.*

- **7.2 Validierung:**
  - *Durchführung umfassender Tests und Überprüfungen, im die **Integrität, Verfügbarkeit** und **Vertraulichkeit** aller Systeme nach dem Sicherheitsvorfall sicherzustellen.*

8. Nacharbeitung:

- **8.1 Auswertung:**
  - *Durchführung einer Nachbesprechung zur Analyse des Vorfalls, der Reaktionsmaßnahmen und der gewonnenen Erkenntnisse sowie ggf. Überarbeitung und Anpassung/Aktualisierung des vorhandenen Sicherheitskonzeptes und dem Implementieren weiterer Schutzmechanismen.*

- **8.2 Dokumentation:**
  - *Erfassung aller Schritte, Entscheidungen und Ergebnisse des Vorfalls, in einem detaillierten Bericht, einschließlich der Nutzung von Incident Reports.*

- **8.3 Schulung:**
  - *Organisation und Durchführung regelmäßiger und Schulungen und Zielgerichteten Übungen des IT-Teams sowie aller relevanten Beschäftigten, um das Bewusstsein für Sicherheitspraktiken zu erhöhen und die Reaktionsfähigkeiten zu verbessern.*

9. Prävention:

- **9.1 Sicherheitsrichtlinien:**
  - *Regelmäßige Überprüfung und Aktualisierung der Sicherheitsrichtlinien und -verfahren, zum Zwecke der kontinuierlichen Verbesserung der Sicherheit.*

- **9.2 Systemupdates:**
  - *Sicherstellung der Aktualität aller Software-lösungen und Sicherheitsanwendungen (z.B. ClamAV, Fail2Ban) durch regelmäßige Patch-Managemt-Prozesse.*

- **9.3 Penetrationstests:**
  - *Durchführung regelmäßiger Penetrationstests zur Identifikation und Behebung potentieller Schwachstellen in der Systemkonfiguration.*

- **9.4 Red Team Engagements:**
  - *Durchführung von Red Team Engagements, um die Sicherheitsmaßnahmen aus der Perspektive eines realistischen Angreifers zu testen.*
  - *Identifizierung von Schwachstellen und Angriffspunkten, gefolgt von Empfehlungen zur Verbesserung der Sicherheitsstrategie.*
  - *Durchführen von Nachbesprechungen zur Analyse der Ergebnisse und zur entwicklung vin Maßnahmen zur Risikominderung.*

- **9.5 Backup-Strategie:**
  - *Regelmäßige Erstellung volständiger und inkrementiellen Backups der LDAP-Datenbank.*
  - *Überprüfung und Dokumentation der Backup-Prozesse, um die Integrität und Wiederherstellbarkeit der Backups zu gewährleisten.*
  - *Speicherung von Backups an einem sicheren, physisch getrennten Ort sowie in der Cloud, um im Katastrophenfall die Wiederherstellung zu ermöglichen.*

- **9.6 Schulungen des gesamten Personals:**
  - *Durchführung regelmäßiger Sicherheitsschulungen für die gesamte Belegschaft, um das Bewusstsein für die Cyber-Sicherheitsrisiken zu schärfen und **Best Practices** zu vermitteln.*
  - *Spezifische für das IT-Team zu aktuellen Bedrohungen, Incident Response-Prozessen und Tools, welche im Unternehmen eingesetzt werden.*
  - *Durchführung von Übungen und Simulationen, um das Wissen über Notfallmaßnahmen und Reaktionspläne zu festigen.*

10. Schlussfolgerung

Ein effektiver Incident Response Plan ist entscheidend für die Sicherheit des LDAP-Servers der **Smooth Beans GmbH**. Durch die systematische Vorbereitung, Identifikation, Reaktion, Erholung und Nacharbeitung von Sicherheitsvorfällen kann die **Integrität** der Systeme gewahrt werden, die Auswirkungen von Vorfällen minimiert und die Risiken für das Unternehmen erheblich minimiert werden. Durch die Bereitstellung von Incident Report Vorlagen und E-Mail-Templets zur Informationsweitergabe an die Belegschaft wird eine transparente Kommunikation während und nach eines Vorfalles gewährleistet. Regelmäßige Schulungen, die Implementation einer Backup-Strategie sowie die Anpassung des Incident Response Plans an neue Bedrohungen sind unerlässlich zur Gewährleistung einer nachhaltigen Sicherheitsstrategie.