Bedrohungsmodell - OTT Auth

Owner: Team 22
Reviewer: Dimov & Tadjiev & Sacha Hack
Contributors: Georg Neugebauer, DevSecOps Kursteilnehmer, Hristomir Dimov, Nodirjon Tadjiev
Date Generated: Fri Nov 10 2023

Executive Summary

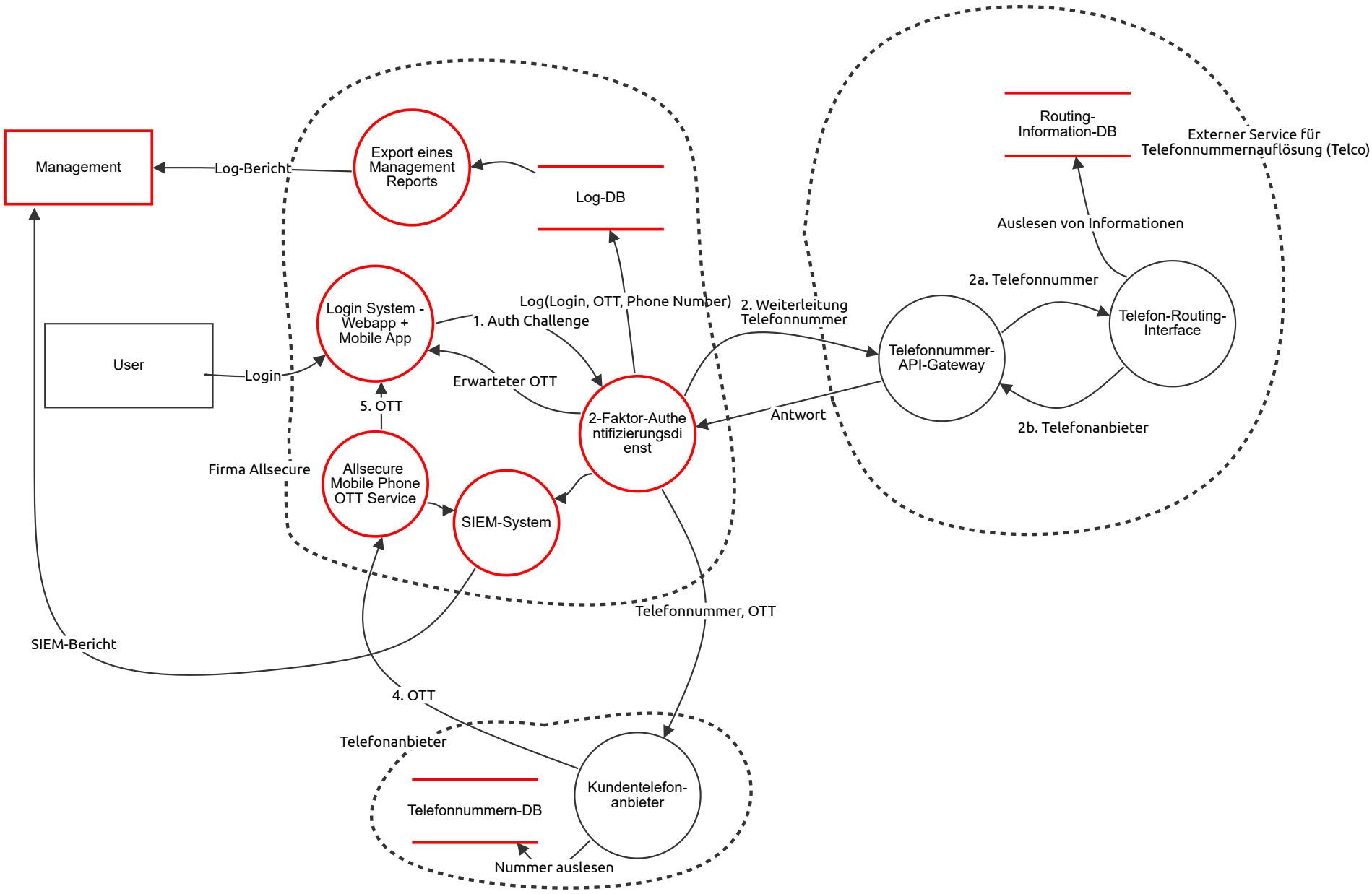
High level system description

Die Firma Allsecure betreibt unterschiedliche Anwendungen mit Hilfe einer 2-Faktorauthentifizierung via One-time token, der an das entsprechende Smartphone des Nutzers geschickt wird.

Summary

Total Threats	13
Total Mitigated	0
Not Mitigated	13
Open / High Priority	4
Open / Medium Priority	2
Open / Low Priority	7
Open / Unknown Priority	0

Architekturdiagramm



Architekturdiagramm

User (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Login System - Webapp + Mobile App (Process)

Vergleicht eingegebenen OTT-Wert auf Telefon mit erwartetem OTT seitens 2-Faktor-Dienst.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
103	Zero-Day Schwachstelle der Standard-SW für Kryptographie	Information disclosure	Low	Open		Leak von Kundendaten ist möglich anhand einer Schwachstelle in der Krypto-Software 117 TA0100 8.3.7 MASVS-CODE-4	* FH Style verschlüsseln: VPN mit anderem Verschlüsselungssoftware * Regelmäßige Sicherheitsprüfungen und Aktualisierung der Krypto-Software Um das Risiko eines Kundendatenlecks aufgrund von Schwachstellen in der Krypto-Software zu minimieren, ist es entscheidend, regelmäßige Sicherheitsprüfungen durchzuführen und sicherzustellen, dass die verwendete Krypto-Software auf dem neuesten Stand ist. Durch regelmäßige Sicherheitsprüfungen können Schwachstellen in der Krypto-Software identifiziert und behoben werden, bevor sie von Angreifern ausgenutzt werden können. * Technische/organisatorische Umsetzung der Maßnahme: Implementierung von automatisierten und manuellen Sicherheitsprüfungen, um Schwachstellen in der Krypto-Software zu identifizieren. Einführung eines effektiven Patch-Management-Systems, um sicherzustellen, dass die Krypto-Software stets auf dem neuesten Stand ist. * Durch regelmäßige Sicherheitsprüfungen und die Aktualisierung der Krypto-Software wird das Risiko von Schwachstellen und einem daraus resultierenden Datenleck erheblich reduziert. Wiederbewertung des Risikos: Nach Implementierung der Maßnahmen sollte eine regelmäßige Überprüfung erfolgen, um sicherzustellen, dass die Sicherheitsvorkehrungen wirksam sind und den aktuellen Bedrohungen standhalten können.

2-Faktor-Authentifizierungsdienst (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
119	Zero-Day Schwachstelle der Standard-SW für Kryptographie	Information disclosure	Low	Open		Leak von Kundendaten ist möglich anhand einer Schwachstelle in der Krypto-Software 117 TA0100 D 2 R 0 E 6 A 10 D 1 Relativ unwahrscheinlich Kann aber alle Benutzer betreffen 6.2.4 MASVS-CODE-4	* Krypto-Software-Sicherheitsbewertung und Aktualisierung: Um das Risiko eines Kundendatenlecks aufgrund von Schwachstellen in der Krypto-Software zu minimieren, ist es wichtig, die Sicherheit der verwendeten Krypto-Software zu bewerten und regelmäßige Aktualisierungen sicherzustellen. Durchführen einer umfassenden Sicherheitsbewertung der Krypto-Software, um potenzielle Schwachstellen zu identifizieren. * Technische/organisatorische Umsetzung der Maßnahme: Beauftragen von Sicherheitsfachleuten oder Sicherheitsunternehmen, um eine umfassende Sicherheitsbewertung der Krypto-Software durchzuführen. Patch-Management: Einrichten eines effektiven Patch-Management-Systems, um sicherzustellen, dass die Krypto-Software stets auf dem neuesten Stand ist. * Bewertung der Risikoreduktion und Wiederbewertung des Risikos: Die Sicherheitsbewertung und regelmäßige Aktualisierung der Krypto-Software tragen dazu bei, bekannte Schwachstellen zu beheben und das Risiko eines Kundendatenlecks zu minimieren. D3-DLIC
120	API Gateway Schlüssel werden ausgelesen	Information disclosure	Medium	Open		Mit dem Schlüssel kann man Benutzerdaten auslesen, obwohl robuster Verschlüsselungsalgorithmus angewendet wird. 94 TA0100 D 7 R 2 E 8 A 2 D 7 Nur Telefonnummern werden damit ausgelesen Mittlere Wahrscheinlichkeit, da man schon Zugriff auf den Service gehabt haben muss... 4.2.2 MASVS-NETWORK-2	* Verbessertes Schlüsselmanagement und Datenzugriffskontrolle: Um sicherzustellen, dass selbst bei einem robusten Verschlüsselungsalgorithmus der Zugriff auf Benutzerdaten nur autorisierten Personen möglich ist, sind verbessertes Schlüsselmanagement und eine effektive Datenzugriffskontrolle erforderlich. * Technische/organisatorische Umsetzung der Maßnahme: Hardware-Sicherheitsmodule (HSM): Integration von HSMs zur sicheren Verwahrung von Verschlüsselungsschlüsseln, um den physischen Schutz der Schlüssel zu gewährleisten. Schlüsselrotation: Implementierung von regelmäßiger Schlüsselrotation, um im Falle eines Kompromisses den Schaden zu begrenzen. Audit-Logging: Einführung von Audit-Logging-Mechanismen, um alle Zugriffe auf verschlüsselte Daten zu protokollieren und eine lückenlose Aufzeichnung von Aktivitäten zu gewährleisten. * Bewertung der Risikoreduktion und Wiederbewertung des Risikos: Durch verbessertes Schlüsselmanagement und präzise Datenzugriffskontrollen wird das Risiko eines unautorisierten Zugriffs auf Benutzerdaten trotz robuster Verschlüsselung minimiert. D3-FE

Telefonnummer-API-Gateway (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Kundentelefon-anbieter (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Telefon-Routing-Interface (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Erwarteter OTT (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

2b. Telefonanbieter (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Alternative A (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Log(Login, OTT, Phone Number) (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Nummer auslesen (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Auslesen von Informationen (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Antwort (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Telefonnummer, OTT (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

1. Auth Challenge (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

OTT (Descriptive text)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

4. OTT (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

2. Weiterleitung Telefonnummer (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

5. OTT (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Log-Bericht (Data Flow)

monatlich

Number	Title	Type	Priority	Status	Score	Description	Mitigations

SIEM-Bericht (Data Flow)

wochentlich

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Log-DB (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
104	interne Änderung von Log Dateien	Tampering	High	Open		Angreifer spooft die Identität eines Mitarbeiters und greift direkt auf die Log-DB, die nicht vom SIEM überwacht wird. 176 TA0102 D 9 R 7 E 10 A 10 D 8 Relativ Wahrscheinlich Schweregrad ist hoch, da das Management "So viele Daten wie möglich" haben möchte 7.3.3 MASVS-RESILIENCE-2	* Erweiterte Überwachung und Zugriffskontrolle für Log-Datenbanken: Um das Risiko eines Angriffs, bei dem ein Angreifer die Identität eines Mitarbeiters spooft und direkt auf die Log-Datenbank zugreift, zu minimieren, sind erweiterte Überwachungsmechanismen und Zugriffskontrollen erforderlich. Implementierung von Logging für Zugriffe auf die Log-Datenbank, um alle Aktivitäten zu protokollieren. Einführung von strengen Zugriffskontrollen für die Log-Datenbank, die sicherstellen, dass nur autorisierte Benutzer mit den notwendigen Rechten auf die Daten zugreifen können. * Technische/organisatorische Umsetzung der Maßnahme: Konfiguration von Datenbank-Logging-Mechanismen, um alle Zugriffe auf die Log-Datenbank aufzuzeichnen, einschließlich Benutzeridentität und durchgeführter Aktionen. Intrusion Detection- und Prevention-System (IDPS): Implementierung von IDPS, um verdächtige Aktivitäten in Echtzeit zu erkennen und darauf zu reagieren, um unautorisierte Zugriffe zu blockieren. * Bewertung der Risikoreduktion und Wiederbewertung des Risikos: Durch erweiterte Überwachung und Zugriffskontrollen wird das Risiko eines erfolgreichen Angriffs auf die Log-Datenbank erheblich minimiert. Nach Implementierung der Maßnahmen sollte eine regelmäßige Überprüfung erfolgen, um sicherzustellen, dass die Sicherheitsvorkehrungen wirksam sind und den aktuellen Bedrohungen standhalten können. D3-DQSA

Telefonnummern-DB (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
156	Angreifer gibt sich als 2FA Dienst aus	Spoofing	Low	Open		Angreifer im lokalen Netz betreibt ARP Spoofing und fängt alle Daten ab die an das 2FA System gehen würden. 97 TA0100 D 3 R 7 E 5 A 5 D 3 2.5.3 MASVS-NETWORK-2	* Schutz vor ARP Spoofing und Sicherung des 2FA-Systems: Um das Risiko eines ARP Spoofing-Angriffs zu minimieren, bei dem ein Angreifer im lokalen Netzwerk alle Daten abfängt, die an das 2FA-System gehen würden, sind sowohl technische als auch organisatorische Maßnahmen erforderlich. Netzwerksicherheit. Verschlüsselung des Datenverkehrs. Zwei-Faktor-Authentifizierung (2FA) Stärkung. * Technische/organisatorische Umsetzung der Maßnahme: Implementierung von Netzwerküberwachungstools, die auf ARP Spoofing hinweisen und bei Verdacht Alarme auslösen. Verschlüsselung des Datenverkehrs: Implementierung von Ende-zu-Ende-Verschlüsselung für alle Kommunikationen zwischen Clients und dem 2FA-System. Stärkung der 2FA-Mechanismen: Auswahl von robusten 2FA-Methoden, die schwer zu kompromittieren sind, selbst wenn ein Angreifer den Datenverkehr abfängt. * Bewertung der Risikoreduktion und Wiederbewertung des Risikos: Durch die Implementierung von Maßnahmen gegen ARP Spoofing und die Verschlüsselung des Datenverkehrs wird das Risiko eines erfolgreichen Angriffs erheblich minimiert. Nach Implementierung der Maßnahmen sollte eine regelmäßige Überprüfung erfolgen, um sicherzustellen, dass die Sicherheitsvorkehrungen wirksam sind und den aktuellen Bedrohungen standhalten können. D3-MAC

Routing-Information-DB (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
107	Angreifer ändert Informationen für die Telefonnumerauflösung	Tampering	High	Open		Angreifer hat Schreibrechte auf die DB des Telefonanbieters und/oder verschlüsselt die Informationen in der DB. 161 TA0105 D 9 R 7 E 10 A 10 D 6 Relativ Wahrscheinlich Man soll auch damit rechnen, dass externe Services einen schlechteren Sicherheitsstandard haben können. 5.2.5 MASVS-AUTH-3	* Datenbankzugriffskontrollen und Verschlüsselung: Um das Risiko eines Angriffs zu minimieren, bei dem ein Angreifer Schreibrechte auf die Datenbank des Telefonanbieters erlangt oder Informationen in der Datenbank verschlüsselt, sind robuste Zugriffskontrollen und Verschlüsselung erforderlich. * Technische/organisatorische Umsetzung der Maßnahme: Festlegung von klaren Zugriffsrichtlinien für die Datenbank und sicherstellen, dass nur autorisierte Benutzer entsprechende Berechtigungen haben. Transparente Datenbankverschlüsselung: Implementierung von Technologien, die eine transparente Datenbankverschlüsselung ermöglichen, ohne die Anwendungslogik zu beeinträchtigen. Hardware Security Modules (HSM): Integration von HSMs zur sicheren Aufbewahrung von Verschlüsselungsschlüsseln, um den physischen Schutz der Schlüssel zu gewährleisten. * Bewertung der Risikoreduktion und Wiederbewertung des Risikos: Durch die Implementierung von Zugriffskontrollen und Datenbankverschlüsselung wird das Risiko eines erfolgreichen Angriffs auf die Datenbank erheblich minimiert. Nach Implementierung der Maßnahmen sollte eine regelmäßige Überprüfung erfolgen, um sicherzustellen, dass die Sicherheitsvorkehrungen wirksam sind und den aktuellen Bedrohungen standhalten können. D3-DENCR

Allsecure Mobile Phone OTT Service (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
154	Mitarbeiter kann sich selber als Manager eintragen	Elevation of privilege	High	Open		Wenn ein Angreifer schon Rechte eines Mitarbeiters hat, kann er sich selber als Manager eintragen und kriegt dann alle sensible Daten. 117 TA0111 D 9 R 3 E 10 A 7 D 8 Relativ schwierig zu machen Hohe Wahrscheinlichkeit, dass dieses versucht wird 2.2.1 MASVS-AUTH-3	* Identitäts- und Berechtigungsmanagement mit Zwei-Faktor-Authentifizierung (2FA): Um das Risiko einer Erhöhung von Privilegien zu minimieren, sollte ein robustes Identitäts- und Berechtigungsmanagement implementiert werden. Die 2FA stellt sicher, dass der Angreifer nicht nur Zugriff auf Benutzeranmeldeinformationen benötigt, sondern auch einen zweiten Authentifizierungsfaktor, um sich erfolgreich als Manager einzutragen. * Technische/organisatorische Umsetzung der Maßnahme: Implementierung von 2FA für alle Benutzerkonten, insbesondere für privilegierte Konten wie Manager. Überprüfung und Aktualisierung von Berechtigungen basierend auf dem Prinzip der geringsten Rechte. * Bewertung der Risikoreduktion und Wiederbewertung des Risikos: Die Implementierung von 2FA und PoLP minimiert das Risiko einer Erhöhung von Privilegien erheblich, da sie den Zugang zu sensiblen Daten erschweren und unnötige Berechtigungen begrenzen. Nach Implementierung der Maßnahmen sollte eine regelmäßige Überprüfung erfolgen, um sicherzustellen, dass die Sicherheitsvorkehrungen effektiv sind und den aktuellen Bedrohungen standhalten können. D3-MAC

Export eines Management Reports (Data Flow)

monatlicher Management-Report

Number	Title	Type	Priority	Status	Score	Description	Mitigations
114	Email wird abgefangen	Information disclosure	Medium	Open		Email wird über ein öffentliches Server gesendet und kann damit abgefangen werden. Kann aber nicht geändert werden, da diese signiert wurde. 117 TA0100 D 8 R 3 E 7 A 7 D 2 Sehr viele Daten gehen ans Management und können gelesen werden. Eher Unwahrscheinlich (Nur wenige Angreifer können einfach Mails abfangen) Aber Anzahl der Betroffenen hoch 9.2.1 MASVS-NETWORK-1	* Transport Layer Security (TLS) für sichere E-Mail-Kommunikation: Die Implementierung von Transport Layer Security (TLS) für die E-Mail-Kommunikation stellt sicher, dass die Daten während der Übertragung zwischen Servern verschlüsselt sind. TLS verschlüsselt den Datenverkehr zwischen E-Mail-Servern, was die Wahrscheinlichkeit eines Abfangens und Mitlesens durch Dritte erheblich reduziert. * Digitale Signatur: Einsatz von digitalen Signaturen für E-Mails, um die Authentizität der Absenderadresse zu überprüfen. TLS-Implementierung: Konfiguration der E-Mail-Server, um TLS für die Verschlüsselung des Datenverkehrs zwischen Servern zu aktivieren. Überwachung und Logging: Einführung von Überwachungsmechanismen und Protokollierung, um verdächtige Aktivitäten zu erkennen und darauf reagieren zu können. * Bewertung der Risikoreduktion und Wiederbewertung des Risikos: Die Implementierung von TLS und digitalen Signaturen reduziert erheblich das Risiko des Abfangens von E-Mails und schützt vor möglichen Manipulationen während der Übertragung. Nach der Umsetzung der Maßnahmen sollte eine regelmäßige Überprüfung erfolgen, um sicherzustellen, dass die Sicherheitsvorkehrungen wirksam sind und den aktuellen Bedrohungen standhalten können. D3-CTS

Number	Title	Type	Priority	Status	Score	Description	Mitigations
153	Mitarbeiter kann sich als Manager eintragen	Elevation of privilege	High	Open		Wenn ein Angreifer schon Rechte von einem Mitarbeiter hat, kann er sich selber als Manager eintragen und kriegt dann alle sensible Daten. 151 TA0111 D 8 R 3 E 10 A 8 D 6 2.2.1 MASVS-AUTH-3	* Prinzip der geringsten Rechte (Principle of Least Privilege, PoLP): Das Prinzip der geringsten Rechte (PoLP) beinhaltet die Vergabe von minimal notwendigen Zugriffsrechten für Benutzer, um ihre Aufgaben zu erfüllen. Die Anwendung des Prinzips der geringsten Rechte reduziert die Angriffsfläche, indem nur die notwendigen Berechtigungen für die jeweiligen Aufgaben vergeben werden. * Konsequente Anwendung von PoLP bei der Zuweisung von Berechtigungen für Benutzer und Systeme. Regelmäßige Überprüfungen der Benutzerberechtigungen sowie Sicherheitsaudits, um sicherzustellen, dass die Rechte angemessen vergeben und keine unnötigen Privilegien vorhanden sind. Implementierung von Tools und Systemen zur Überwachung von Benutzeraktivitäten. * Die Anwendung des Prinzips der geringsten Rechte und die kontinuierliche Überwachung von Benutzeraktivitäten tragen dazu bei, das Risiko einer Privilegieneskalation erheblich zu reduzieren. D3-MAC

Management (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
149	Daten von Server wird getraut	Repudiation	Low	Open		Angreifer könnten eigene Daten einspielen. Damit kann man andere Angriffe auf andere Leute schieben mit gefälschten Informationen. 148 TA0101 D 3 R 4 E 7 A 7 D 1 Schaden ist relativ niedrig, da dies weitere Spuren hinterlassen könnte Wahrscheinlichkeit auch niedrig, da andere Angriffe vorausgehen müssen und SIEM Systeme nicht öffentlich sind. 5.1.1 MASVS-AUTH-3	* Digitale Signaturimplementierung: Die Implementierung einer digitalen Signatur ermöglicht es, die Authentizität und Integrität von Daten zu gewährleisten. Digitale Signaturen bieten eine zuverlässige Methode zur Identifizierung und Überprüfung von Absendern. * Technische/organisatorische Umsetzung der Maßnahme: Implementierung eines sicheren Systems zur Generierung, Speicherung und Verwaltung von digitalen Schlüsseln, um die Integrität der Signaturen zu gewährleisten. Verschlüsselung. Protokollierung und Überwachung. * Bewertung der Risikoreduktion und Wiederbewertung des Risikos: Die Einführung von digitalen Signaturen reduziert das Risiko der Repudiation erheblich, da die Authentizität der Daten überprüft werden kann. Nach Implementierung der Maßnahme sollte eine regelmäßige Überprüfung erfolgen, um sicherzustellen, dass die Sicherheitsmaßnahmen immer noch wirksam sind und den sich ändernden Bedrohungen standhalten können. D3-SRA
152	Angreifer gibt sich als SIEM aus	Spoofing	Low	Open		Angreifer im lokalen Netz betreibt ARP Spoofing und fängt alle Daten ab die an das SIEM System gehen würden. 151 TA0101 D 3 R 2 E 7 A 6 D 4 2.5.3 MASVS-NETWORK-2	* Netzwerksegmentierung und Überwachung: Netzwerksegmentierung ist eine Maßnahme, bei der das Netzwerk in isolierte Segmente unterteilt wird. In diesem Fall könnte man das Netzwerk so strukturieren, dass das SIEM-System in einem eigenen Segment platziert ist. Durch die Segmentierung des Netzwerks wird die Angriffsfläche für ARP Spoofing reduziert, da ein Angreifer, der sich im lokalen Netz befindet, Schwierigkeiten hat, auf das Segment des SIEM-Systems zuzugreifen. * Technische/organisatorische Umsetzung der Maßnahme: Implementierung von Firewalls und Netzwerkrichtlinien, um das Netzwerk in Segmente zu unterteilen. * Bewertung der Risikoreduktion und Wiederbewertung des Risikos: Die Netzwerksegmentierung und Überwachung tragen dazu bei, das Risiko von Spoofing-Angriffen zu minimieren, indem der Angriffsvektor begrenzt wird und Anomalien frühzeitig erkannt werden. Nach Implementierung der Maßnahmen sollte eine regelmäßige Überprüfung erfolgen, um sicherzustellen, dass die Sicherheitsvorkehrungen effektiv sind und den aktuellen Bedrohungen standhalten können. D3-PCSV

SIEM-System (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
117	Angreifer gibt sich im lokalen Netz als 2FA dienst aus	Denial of service	Low	Open		Angreifer gibt sich im Lokalem Netzwerk über VPN als 2FA aus und sendet viele Daten an das SIEM welches intern nichts Wesentliches tun kann, außer die Anwesenheit eines Angriffs anzukündigen. 607 TA0109 D 3 R 2 E 6 A 4 D 1 Nicht schwer, aber SIEM weiss trotzdem, dass es einen Angriff gibt. Wahrscheinlichkeit - mittel, da das Netz innerlich nicht gesichert ist. 2.5.3 MASVS-NETWORK-2	* Erhöhte Sicherheit für VPN-Zugriff und Verbesserung des SIEM-Systems: Um die beschriebene Bedrohung zu minimieren, sind verstärkte Sicherheitsmaßnahmen für den VPN-Zugriff erforderlich, insbesondere in Bezug auf die Authentifizierung und Überwachung. Verbesserte VPN-Sicherheit: Durch eine stärkere Authentifizierung für den VPN-Zugriff wird es für einen Angreifer schwieriger, sich als legitimer Benutzer auszugeben. * Technische/organisatorische Umsetzung der Maßnahme: Implementierung von MFA für den VPN-Zugriff, um sicherzustellen, dass der Angreifer nicht nur Benutzeranmeldeinformationen, sondern auch einen zweiten Authentifizierungsfaktor benötigt. Regelmäßige Überprüfungen von VPN-Logs. Erweiterte Analysefähigkeiten im SIEM. Automatisierte Reaktionen im SIEM. * Bewertung der Risikoreduktion und Wiederbewertung des Risikos: Die verbesserte VPN-Sicherheit durch MFA und regelmäßige Überprüfungen, kombiniert mit einem leistungsfähigen SIEM-System, reduziert das Risiko eines erfolgreichen Angriffs erheblich. D3-MAC
155	keine Überprüfung von Serverdaten	Repudiation	Low	Open		Angreifern wird erlaubt, eigene Daten einzuspielen. Damit lassen sich Angriffe auf andere Leute schieben. 173 TA0104 D 2 R 2 E 5 A 4 D 1 Schaden ist relativ niedrig, da dies weitere Spuren hinterlassen könnte Wahrscheinlichkeit auch niedrig, da andere Angriffe vorausgehen müssen und SIEM Systeme nicht öffentlich sind. 14.5.1 MASVS-AUTH-3	* Logging und digitale Signaturen zur Überprüfung der Datenintegrität: Um das Risiko der Repudiation zu minimieren, bei dem Angreifer versuchen könnten, gefälschte Daten einzuspielen und Angriffe auf andere Personen zu schieben, ist es wichtig, umfassendes Logging und digitale Signaturen zu implementieren. Logging: Protokollierung aller Transaktionen und Aktionen, um eine lückenlose Aufzeichnung von Aktivitäten zu gewährleisten. Digitale Signaturen: Anwendung digitaler Signaturen auf kritische Daten und Transaktionen. * Technische/organisatorische Umsetzung der Maßnahme: Implementierung von robusten Logging-Mechanismen, die relevante Informationen über Transaktionen, Benutzeraktionen und Systemaktivitäten erfassen. Digitale Signaturen: Einführung von digitalen Signaturen für kritische Daten und Transaktionen. * Bewertung der Risikoreduktion und Wiederbewertung des Risikos: Die Implementierung von Logging und digitalen Signaturen minimiert das Risiko der Repudiation, indem sie eine nachvollziehbare Aufzeichnung von Aktivitäten schafft und die Integrität von Daten gewährleistet. D3-FIM