Penetrationstestbericht

InsoCare

der Dubius Payment Ltd.

EXAMPLE

20. Dezember 2024

v1.1

Inhaltsverzeichnis

i Änderungsverzeichnis

Version	Beschreibung	Autor	Datum
1.0	Reporterstellung	Dominik Sauer	19. Dezember 2024
1.1	Qualitätssicherung	QA-Team	20. Dezember 2024

1 Ansprechpartner

1.1 Ansprechpartner Dubius Payment Ltd.

Damian Westcott
CEO

✉ d.westcott@dubius-payment.com

Dubius Payment Ltd.
71 Peachfield Road
SO53 4NE CHANDLER
United States

1.2 Ansprechpartner binsec GmbH

Dominik Sauer
Head of Penetration Testing

☎ +49 69247560713
✉ ds@binsec.com

binsec GmbH
Solmsstraße 41
60486 Frankfurt am Main
Germany

1.3 Über den Pentester

Seit 2013 obliegt Herrn Dominik Sauer die Leitung und Durchführung von Penetrationstests der binsec GmbH. Er startete seine Karriere bereits während seines Informatikstudiums an der Hochschule Darmstadt und beendete seine akademische Laufbahn mit einem sehr guten Masterabschluss in Informatik mit Vertiefungsrichtung IT-Sicherheit. Ebenfalls kann er die führenden Zertifikate im Bereich Penetration-Testing vorweisen und ist seit 2013 „Offensive Security Certified Professional (OSCP)“ sowie „Offensive Security Certified Expert (OSCE)“ seit 2015.

Darüber hinaus engagiert er sich seit 2017 als Dozent in Forschung und Lehre an der Hochschule Darmstadt (HDA) und an der Technischen Hochschule Mittelhessen (THM). So hält er beispielsweise Lehrveranstaltungen zu Penetration Testing oder zur digitalen Forensik und betreut wissenschaftliche Arbeiten.

2 Projektübersicht

2.1 Einführung

Die Dubius Payment Ltd. bietet unter dem Namen InsoCare eine Gesamtlösung für Menschen mit Diabetes an. InsoCare besteht hierbei aus den folgenden drei Komponenten:

- InsoPump
- InsoSense
- InsoApp

Sowohl InsoPump, der Insulin Pumpe, als auch InsoSense, dem zugehörigen Sensor, kommunizieren über Bluetooth Low Energy mit der InsoApp. InsoApp steht sowohl für Android als auch iOS zur Verfügung. InsoApp wurde gesondert einem Pentest unterzogen.

2.2 Rahmenbedingungen

Der Penetrationstest wurde zwischen dem 5. Juni 2024 und 7. Juni 2024 als interner Grey-Box-Test durchgeführt, ohne aggressive Angriffstechniken wie DDoS-Attacken zu verwenden. Die vollständige Klassifizierung ist in Kapitel 5.1 dargestellt. Die grundsätzliche Vorgehensweise ist in Kapitel 5.2 beschrieben.

2.3 Scope

Gegenstand dieses Pentests waren ausschließlich die InsoPump und InsoSense - lediglich zur Überprüfung der Bluetooth Kommunikation wurde dem Pentester darüber hinaus die InsoApp in der Version 1.2b zur Verfügung gestellt.

2.4 Durchgeführte Prüfungen

In dem zuvor genannten Scope wurden nachfolgende Prüfpunkte bei den einzelnen Zielsystemen bzw. -anwendungen untersucht. Diese Auflistung wird automatisiert aus dem Dokumentationswerkzeug der binsec GmbH erzeugt.

Prüfobjekt → Hardware: InsoPump

Ergebnis	Task: Informationssammlung (passiv, externe Ressourcen)	Findings
✔	Identifikation erreichbarer Schnittstellen	-

Prüfobjekt → Hardware: InsoPump · UART: Debug-Interface

Ergebnis	Task: Informationssammlung (aktiv, Prüfobjekte)	Findings
✔	UART-Anschlüsse identifizieren	-
✔	Überprüfung, ob es möglich ist, die Firmware zu dumpen	-

Prüfobjekt → Hardware: InsoPump · Bluetooth LE: InsoPump <--> InsoApp

Ergebnis	Task: Informationssammlung (passiv, externe Ressourcen)	Findings
✔	Identifikation der Bluetooth Version	-
✘	Überprüfung der Privacy Features	Seite 12
Ergebnis	Task: Informationssammlung (aktiv, Prüfobjekte)	Findings
✔	Analyse der Datenkommunikation	-
Ergebnis	Task: Kryptographie	Findings
✘	Analyse des Verbindungsaufbaus	Seite 10
Ergebnis	Task: Eingabevalidierung (z.B. Injection, XSS)	Findings
✔	Automatisierte Prüfung der Eingabevalidierung via Fuzzing	-
Ergebnis	Task: Identifikation von Schwachstellen	Findings
✔	Prüfung auf Low-Level-Angriffe, welche die Sicherheit der Verbindung beeinträchtigen	-
✘	Überprüfung auf Low-Level-Angriffe, die zum Absturz des Geräts führen	Seite 11
✔	Prüfung auf Low-Level-Angriffe, die zu einem Deadlock führen	-

Prüfobjekt → Hardware: InsoSense

Ergebnis	Task: Informationssammlung (passiv, externe Ressourcen)	Findings
✔	Identifikation erreichbarer Schnittstellen	-

Prüfobjekt → Hardware: InsoSense · Bluetooth LE: InsoSense <--> InsoApp

Ergebnis	Task: Informationssammlung (passiv, externe Ressourcen)	Findings
✔	Identifikation der Bluetooth Version	-
✘	Überprüfung der Privacy Features	Seite 12

Ergebnis	Task: Informationssammlung (aktiv, Prüfobjekte)	Findings
✔	Analyse der Datenkommunikation	-

Ergebnis	Task: Kryptographie	Findings
✘	Analyse des Verbindungsaufbaus	Seite 10

Ergebnis	Task: Eingabevalidierung (z.B. Injection, XSS)	Findings
✔	Automatisierte Prüfung der Eingabevalidierung via Fuzzing	-

Ergebnis	Task: Identifikation von Schwachstellen	Findings
✔	Prüfung auf Low-Level-Angriffe, welche die Sicherheit der Verbindung beeinträchtigen	-
✘	Überprüfung auf Low-Level-Angriffe, die zum Absturz des Geräts führen	Seite 11
✔	Prüfung auf Low-Level-Angriffe, die zu einem Deadlock führen	-

3 Managementübersicht

3.1 Zusammenfassung

Der Penetrationstest wurde zwischen dem 5. Juni 2024 und 7. Juni 2024 durchgeführt. Dabei konnten 4 Schwachstellen identifiziert werden, die zu 3 Findings zusammengefasst und einer initialen Risikobewertung unterzogen wurden. Insgesamt wurde kein Finding mit unmittelbarem Handlungsbedarf und 2 Findings mit Handlungsbedarf bewertet. Das Finding mit der Bewertung Hinweis ist als Vorschlag zur Erhöhung des Sicherheitsniveaus zu verstehen.

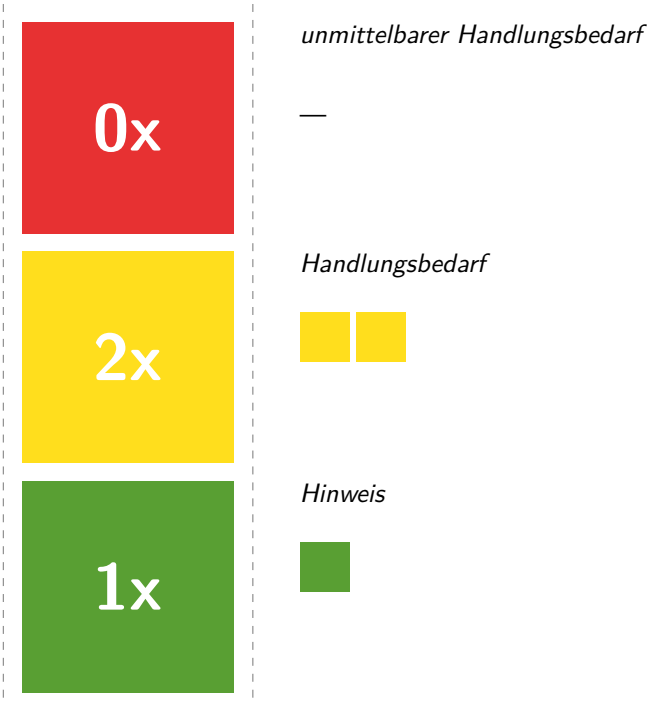


Abb. Risikoverteilung der Findings

Während des Penetrationstests konnten mehrere Schwachstellen mit Handlungsbedarf identifiziert werden, welche beide die Bluetooth LE Verbindung sowohl der InsoPump als auch des InsoSense betreffen. Zum einen basiert die Verbindung zwischen InsoPump und InsoSense auf veraltete Sicherheitsfeatures von Bluetooth LE und ist daher anfällig für Man-in-the-Middle-Angriffe. Zum anderen ist der verbaute Bluetooth LE Chip in der InsoPump anfällig für bereits bekannte Schwachstellen, wodurch die InsoPump durch einen Angreifer zum Absturz gebracht werden kann.

3.2 Liste der Findings

1

Nicht behoben: *Datenübertragung*

Es wird eine veraltete Bluetooth Pairing-Methode eingesetzt, für die bereits Schwachstellen bekannt sind. Siehe Seite 10.

System: InsoPump, InsoSense

2

Nicht behoben: *Datenübertragung*

Die InsoPump kann über einen manipulierten Bluetooth-Verbindungsaufbau zum Absturz gebracht werden. Siehe Seite 11.

System: InsoPump

3

Nicht behoben: *Fehlkonfiguration*

Im eingeschalteten Zustand sind Nutzer der Insulinpumpe trackbar. Siehe Seite 12.

System: InsoPump

4 Technischer Bericht

4.1 Einsatz von veralteter Bluetooth Pairing-Methoden

Handlungsbedarf
Schaden: Mittel
Eintrittswahrscheinlichkeit: Mittel

Finding #1 **Nicht behoben**

Der verschlüsselte Verbindungsaufbau in Bluetooth Low Energy wird über das sog. 'Pairing' realisiert. Die Pairing-Methoden der Versionen 4.0 und 4.1 werden seit der Veröffentlichung von Version 4.2 in 2014 unter 'legacy' zusammengefasst und sind anfällig für Brute-Force Angriffe[1]. Dies bedeutet im Detail, dass ein Angreifer, welcher dazu in der Lage ist den Verbindungsaufbau über Bluetooth LE mitzuschneiden, die Verschlüsselung der Verbindung umgehen kann und Zugriff auf die ggfs. sensitiven Daten hat.

Empfehlung

Statt der veralteten Pairing-Methode sollte auf ein 'Secure Connections'-Pairing gesetzt werden.

[1] https://www.sciencedirect.com/science/article/pii/S1389128621005697#sec4.5

4.2 InsoPump kann über BLE zum Absturz gebracht werden

Handlungsbedarf
Schaden: Mittel
Eintrittswahrscheinlichkeit: Mittel

Finding #2 **Nicht behoben**

Unter dem Namen 'SweynTooth' wurden 2020 insgesamt 14 Schwachstellen in diversen Bluetooth LE Implementierungen identifiziert[2]. Diese Schwachstellen wurden in drei Gruppen unterteilt: Crash, Deadlock und Security Bypass. Wie dem folgenden Listing entnommen werden kann, ist die Insulinpumpe anfällig für den 'Invalid Channel Map' Angriff, welcher zu einem Absturz des Gerätes führt:

```
$ python2.7 invalid_channel_map.py /dev/ttyACM0 **:**:**:**:**:**
Serial port: /dev/ttyACM0
Advertiser Address: **:**:**:**:**:**
TX ---> BTLE_ADV / BTLE_SCAN_REQ
Waiting advertisements from **:**:**:**:**:**
**:**:**:**:**:**: BTLE_ADV / BTLE_ADV_IND Detected
TX ---> BTLE_ADV / BTLE_CONNECT_REQ
Malformed connection request was sent
TX ---> BTLE_ADV / BTLE_SCAN_REQ
TX ---> BTLE_ADV / BTLE_SCAN_REQ
No advertisement from **:**:**:**:**:** received
The device may have crashed!!!
Capture saved in logs/invalid_channel_map.pcap
```

Der Wert der 'Channel Map' gibt bei einem BLE Verbindungsaufbau die zu benutzenden Kanäle an, wobei die Bluetooth Spezifikation eine Mindestanzahl von 2 Kanälen vorschreibt. Wird der Wert stattdessen auf 0 gesetzt, führt dies zu einem Absturz des Gerätes. Die Insulinpumpe ist auch ohne fremdes Eingreifen nach wenigen Sekunden wieder einsatzbereit.

Empfehlung

Sofern ein Update seitens des betroffenen BLE-SoC Herstellers verfügbar ist, sollte auf dieses zurückgegriffen werden.

[2] https://asset-group.github.io/disclosures/sweyntooth/

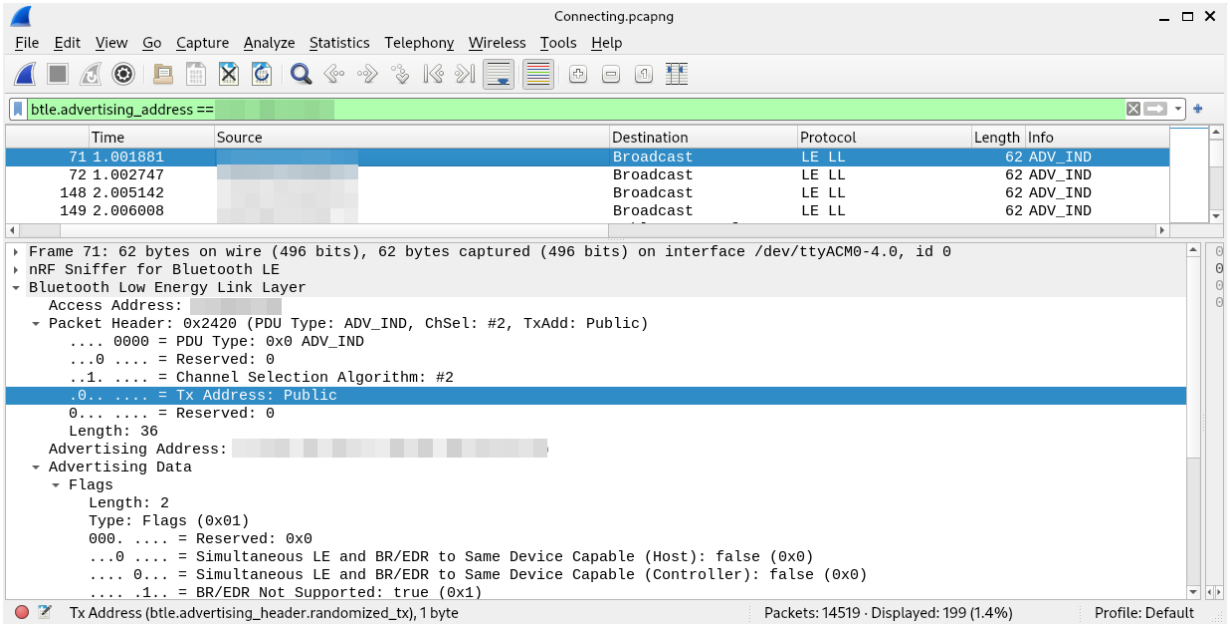
4.3 Fehlendes Privacy Feature

Hinweis
Schaden: Warnung
Eintrittswahrscheinlichkeit: Hoch

Finding #3 **Nicht behoben**

Bluetooth Low Energy (BLE) bietet verschiedene Datenschutzfunktionen, um die Sicherheit und Privatsphäre der Nutzer zu gewährleisten. Eine der zentralen Funktionen ist das Privacy-Feature, das darauf abzielt, die Identität von Geräten zu verschleiern, um die Nachverfolgbarkeit zu reduzieren.[3]

Bei den Advertisements der Insulinpumpe wird nicht auf dieses Feature zurückgegriffen. Wie der nachfolgende Screenshot zeigt, werden Advertisments mit einer sog. 'Public Address' verschickt:



Während das Gerät eingeschaltet ist und Advertisments verschickt, sind Nutzer des Geräts somit grundsätzlich trackbar.

Empfehlung

Das Privacy Feature[4] sollte bei der Insulinpumpe implementiert werden.

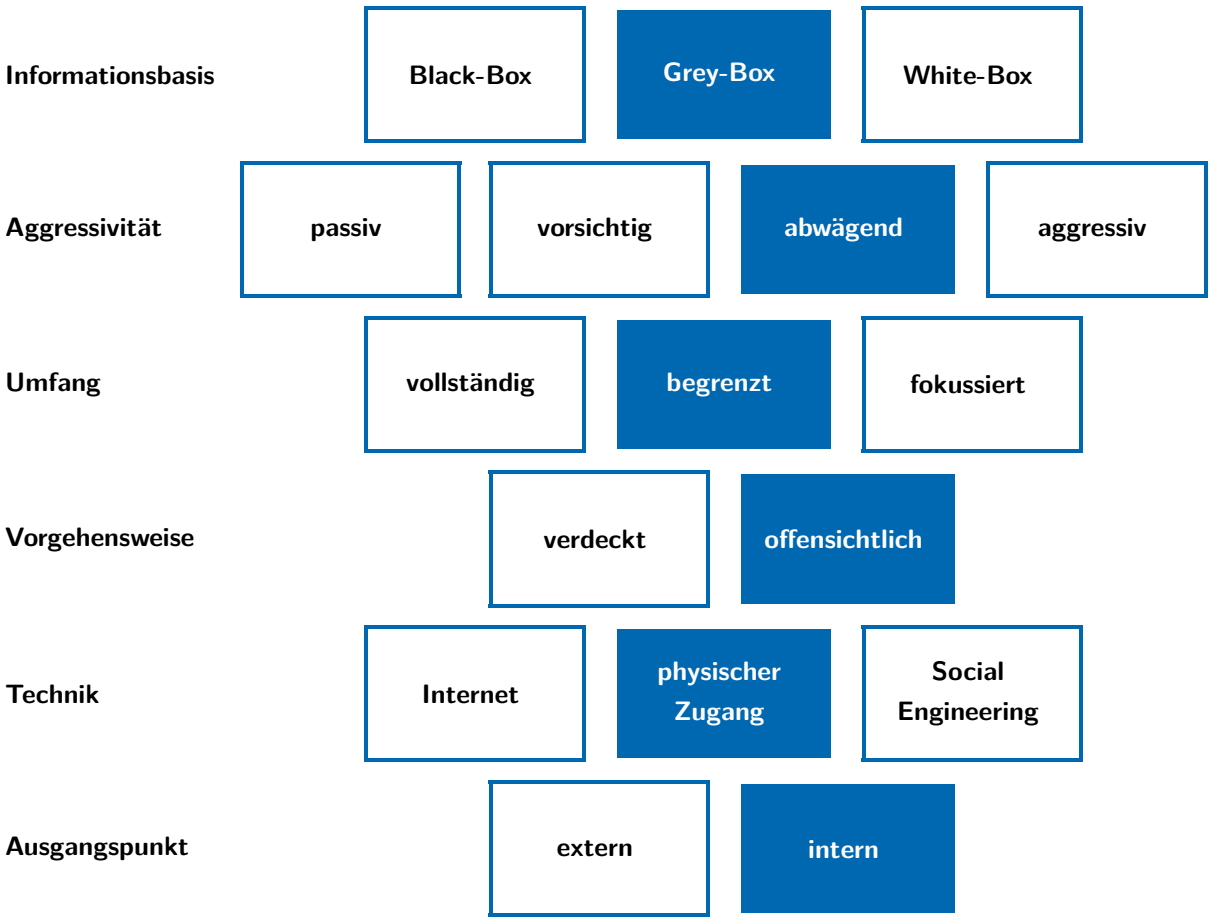
[3] 'A survey on Bluetooth Low Energy security and privacy', 3.1.5. Privacy features (https://doi.org/10.1016/j.comnet.2021.108712)
[4] Bluetooth Core Specification Version 6.0, Vol 1, Part A, 5.4.5 'Privacy Feature'

5 Anhang A

5.1 Klassifizierung-Details

Als Vorgehensweise wurde in Kooperation mit der Dubius Payment Ltd. folgende Klassifizierungsvariante ausgewählt: Der Penetrationstest wurde als interner Grey-Box-Test durchgeführt, ohne aggressive Angriffstechniken wie DDoS-Attacken zu verwenden.

Inhaltlich anlehnend an die Studie - „Durchführungskonzept für Penetrationstests“ - vom Bundesamt für Sicherheit in der Informationstechnik (BSI), ergibt sich folgendes Schema zur Klassifizierung des Penetrationstest:



5.2 Vorgehensweise bei Medical Devices

Die Medical Device Regulation (MDR) fordert die Verifizierung und Validierung der Sicherheit von Medizinprodukten und Software. Die Medical Device Coordination Group stellt in ihrem Leitfaden zur Cybersicherheit für Medizinprodukte fest, dass das primäre Mittel zur Sicherheitsüberprüfung und -validierung Tests sind.

Die Vorgehensweise eines Penetrationstest für ein Medizinprodukt, meist bestehend aus einem oder mehreren Hardwaregeräten und einer dazugehörigen Software, ist aufgrund der unterschiedlichen Anwendungsfällen dieser Medizingeräten und Funktionsweisen in der Regel jeweils ein Einzelfall. Die Kernfragen für einen Penetrationstest von einem Medizingerät sind meistens:

- Kann die Gesundheit des Patienten durch direkte Manipulation des Geräts negativ beeinträchtigt werden?
- Können Messdaten manipuliert werden, sodass aufgrund falscher oder ausbleibender Therapie ein Schaden für den Patienten entsteht?
- Sind die Gesundheitsdaten des Patienten in den verarbeitenden IT-Systemen angemessen nach Stand der Technik geschützt.

Oftmals bestehen Medizingeräte aus einem technischen Zusammenspiel von Sensoren/Messgeräten, einem Embedded Linux OS mit einer kabellosen Datenübertragung per Bluetooth/RFID/WIFI, während die Datenverarbeitung auf Windows-Computern, Smartphones und/oder in Cloud durchgeführt wird.

Die Vorgehensweise, bzw die konkreten sinnvollen zu testenden Angriffsvektoren werden daher gemeinsam mit dem Kunden initial besprochen und umfasst meist eine Prüfung der kabellosen Datenübertragung, einem Öffnen des Geräts zur Identifikation weiterer Angriffsvektoren sowie je nach Einzelfall auch das Testen von Web-Anwendungen und APIs.

5.3 Risikobewertung

Die binsec GmbH versteht unter dem Begriff „Risiko“ die Kombination aus der Eintrittswahrscheinlichkeit einer Schwachstelle (bzw. der Wahrscheinlichkeit ihrer Ausnutzung) und dem möglichen Schadensausmaß. Die Eintrittswahrscheinlichkeit bzw. die Wahrscheinlichkeit der Ausnutzung einer Sicherheitslücke in IT-Systemen hängt im Wesentlichen von diesen Faktoren ab:

- Wie einfach kann die Schwachstelle identifiziert werden? (Visibility)
- Existieren vorgefertigte Exploits für diese Schwachstelle oder muss der Angreifer einen entsprechenden Wissensstand mitbringen um sie auszunutzen? (Exploitability)
- Setzt die Ausnutzung besondere Rechte voraus? (Privilege Escalation)
- Ist eine Kombination mit anderen Sicherheitslücken erforderlich? (Vulnerability Chaining)
- Ist für die Schwachstelle menschliche Interaktion notwendig? (Social Engineering)

Bestimmend für das mögliche Schadensausmaß sind die folgenden Klassifikationen:

1. Finanzieller Schaden
2. Vollständige Kompromittierung des Systems
3. Verletzung der Sicherheitsziele in Bezug auf Daten oder Benutzerkonten:
    a) Vertraulichkeit (Confidentiality)
    b) Verfügbarkeit (Availability)
    c) Integrität (Integrity)
4. Umgehung von Schutzmechanismen
5. Informationslücke

Aus der Kombination von Eintrittswahrscheinlichkeit und möglichem Schadensausmaß trifft der Penetrationstester eine subjektive Einschätzung des Risikos für jede gefundene Sicherheitslücke. Wir empfehlen zusätzlich eine eigene Bewertung der ermittelten Schwachstellen durchzuführen.

Die Einschätzung wird folgender Einstufung unterzogen:

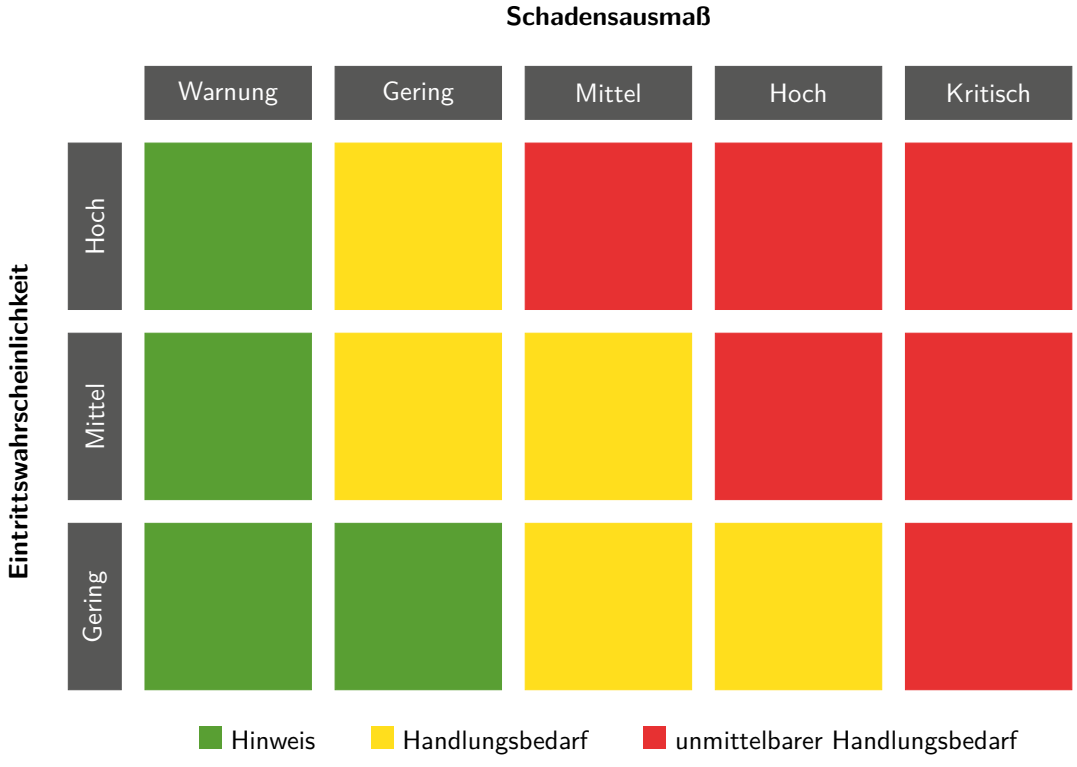
Eintrittswahrscheinlichkeit

Hoch	Die Schwachstelle ist offensichtlich oder Exploits sind frei verfügbar.
Mittel	Die Schwachstelle ist in angemessener Zeit zu entdecken, Exploits müssen eventuell angepasst werden.
Gering	Die Schwachstelle ist aufwendig zu finden und es werden eventuell Privilegien benötigt oder die Ausnutzung setzt weitere Schwachstellen voraus.

Schadensausmaß

Kritisch	Vollständige Kompromittierung des Systems.
Hoch	Verletzung der Sicherheitsziele in Bezug auf Informationen oder IT-Systeme.
Mittel	Umgehung von Schutzmechanismen.
Gering	Vorbereitung der Ausnutzung weiterer Schwachstellen als Teil einer Langzeitattacke.
Warnung	Informationslücke.

Aus der Einstufung des Risikos wird eine Handlungspriorität abgeleitet.



5.4 Über die binsec GmbH

Wir sind ein auf IT-Penetrationstests spezialisiertes Dienstleistungsunternehmen aus Frankfurt am Main. Seit 2013 ist die Durchführung technischer Sicherheitsanalysen von IT-Infrastrukturen, Web-Anwendungen, APIs, Mobilen APPs (Android / iOS) usw. der Kernbestandteil unserer täglichen Arbeit. Als inhabergeführtes Unternehmen legen wir hohen Wert auf die langfristige Zufriedenheit unserer Kunden. Die Zertifizierungen unserer Mitarbeiter, die Lehrtätigkeiten an Hochschulen sowie unsere Praxiserfahrung sprechen für sich.

binsec GmbH
Solmsstraße 41
60486 Frankfurt am Main
Germany

✉ info@binsec.com
☎ +49 69 2475607-0

Geschäftsführer: Patrick Sauer
Prokurist: Dominik Sauer, Florian Zavatzki

Handelsregister: Frankfurt a.M. HRB 97277
USt-IdNr.: DE290966808