Penetrationstestbericht

Payment Gateway

der Dubius Payment Ltd.

EXAMPLE

14. Januar 2025

v1.1

Inhaltsverzeichnis

i Änderungsverzeichnis **3**

1 Ansprechpartner **4**
1.1 Ansprechpartner Dubius Payment Ltd. . . . 4
1.2 Ansprechpartner binsec GmbH . . . 4
1.3 Über den Pentester . . . 4

2 Projektübersicht **5**
2.1 Einführung . . . 5
2.2 Rahmenbedingungen . . . 5
2.3 Scope . . . 6
2.4 Durchgeführte Prüfungen . . . 7

3 Managementübersicht **8**
3.1 Zusammenfassung . . . 8
3.2 Liste der Findings . . . 9

4 Technischer Bericht **10**
4.1 Fehlerhafte Autorisierung . . . 10
4.2 SQL-Injection . . . 11
4.3 Keine Deaktivierung der Zugriffstoken nach einem Benutzerlogout . . . 12
4.4 Verwendung des veralteten OAuth 2.0 „Password Grant“ . . . 13
4.5 Unterstützung von TLS 1.0 und TLS 1.1 und nicht kryptographisch starken Cipher-Suites . . . 14

5 Anhang A **15**
5.1 Klassifizierung-Details . . . 15
5.2 Vorgehensweise bei Web-Anwendungen und APIs . . . 16
5.3 Risikobewertung . . . 17
5.4 Über die binsec GmbH . . . 19

i Änderungsverzeichnis

Version	Beschreibung	Autor	Datum
1.0	Reporterstellung	Dominik Sauer	14. Januar 2025
1.1	Qualitätssicherung	QA-Team	14. Januar 2025

1 Ansprechpartner

1.1 Ansprechpartner Dubius Payment Ltd.

Clyde Simmons
Chief Information Security Officer

☎ +19 99568719999
✉ csimmons@dubius-payment.com.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.betreibt eine Zahlungsapplikation, die Kreditkarteninformationen speichert, verarbeitet und weiterleitet. Das Unternehmen unterliegt somit dem Sicherheitsstandard der Kreditkartenindustrie, dem PCI DSS (Payment Card Industry Data Security Standard). Der PCI DSS verlangt in der Anforderungskategorie 11 die Durchführung von Penetrationstests auf Anwendungsebene und Netzwerkebene. Der Penetrationstest der Netzwerkebene umfasst in diesem Zusammenhang einen Test von außerhalb und einen von innerhalb des Netzwerks. Diese Tests müssen jährlich bzw. nach signifikanten Änderungen durchgeführt werden.

Aufgrund der PCI-DSS-Compliance der Dubius Payment Ltd. wurde für die folgende Applikation ein Penetrationstest durchgeführt:

- Payment-Gateway API

2.2 Rahmenbedingungen

Der Penetrationstest wurde zwischen dem 8. Januar 2025 und 10. Januar 2025 als externer 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. Alle Tests wurden von den folgenden IP-Adressen ausgeführt:

IPv4

- 185.156.254.128/25
- 217.111.127.122/32
- 162.55.59.194/32

IPv6

- 2a07:a1c1:1:600::/63
- 2001:920:1914:3464::/64

2.3 Scope

Zur Überprüfung der Mehrmandantenfähigkeit wurden mehrere Testaccounts angelegt. Diese und die zu testende Anwendung sind im Nachfolgenden aufgelistet:

Webanwendung	Benutzerkonto	Kommentar
https://api.dubius-payment.com/	pentest	Das Benutzerkonto war dem Händler mit der ID '1' zugewiesen.
https://api.dubius-payment.com/	pentest2	Das Benutzerkonto war dem Händler mit der ID '1' zugewiesen.
https://api.dubius-payment.com/	pentestAdmin	Dem Benutzerkonto war die Administratorrolle zugewiesen.

Empfehlung

Alle Benutzerkonten, die für den Penetrationstest erstellt worden sind, sollten nach dem vereinbarten Durchführungszeitraum gelöscht oder zumindest deaktiviert werden.

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 → HTTPS: Payment Gateway

Ergebnis	Task: HTTPS Check	Findings
✔	Informationssammlung (passiv, externe Ressourcen)	-
✔	Prüfung der zugrunde liegenden IT-Systeme als Angriffsvektor	-
✔	Informationssammlung (aktiv, Prüfobjekte)	-
✔	Konfigurationsmanagement Webserver & Webanwendung	-
✔	Prüfung der Zugriffskontrollen bei Benutzerauthentifikation	-
✔	Identitätsmanagement & Registrierungsprozess	-
✔	Prüfung der Handhabung von Benutzerkennwörtern	-
✘	Sichere Datenübertragung	Seite 14
✘	Sitzungsverwaltung	Seiten 13, 12
✘	Vertikale Berechtigungsprüfung (Privilegienausweitung)	Seite 10
✔	Horizontale Berechtigungsprüfung (Mehrmandantenfähigkeit)	-
✘	Eingabevalidierung (z.B. Injection, XSS)	Seite 11
✔	Überprüfung der Dateiuploadmöglichkeiten	-
✔	Low and Slow Denial of Service	-
✔	Fehlerbehandlung und Benutzerbenachrichtigungen	-

3 Managementübersicht

3.1 Zusammenfassung

Der Penetrationstest wurde zwischen dem 8. Januar 2025 und 10. Januar 2025 durchgeführt. Dabei konnten 5 Schwachstellen identifiziert werden, die jeweils als Finding einer initialen Risikobewertung unterzogen wurden. Insgesamt wurden 2 Findings mit unmittelbarem Handlungsbedarf und ein Finding mit Handlungsbedarf bewertet. Die 2 Findings mit der Bewertung Hinweis sind als Vorschlag zur Erhöhung des Sicherheitsniveaus zu verstehen.

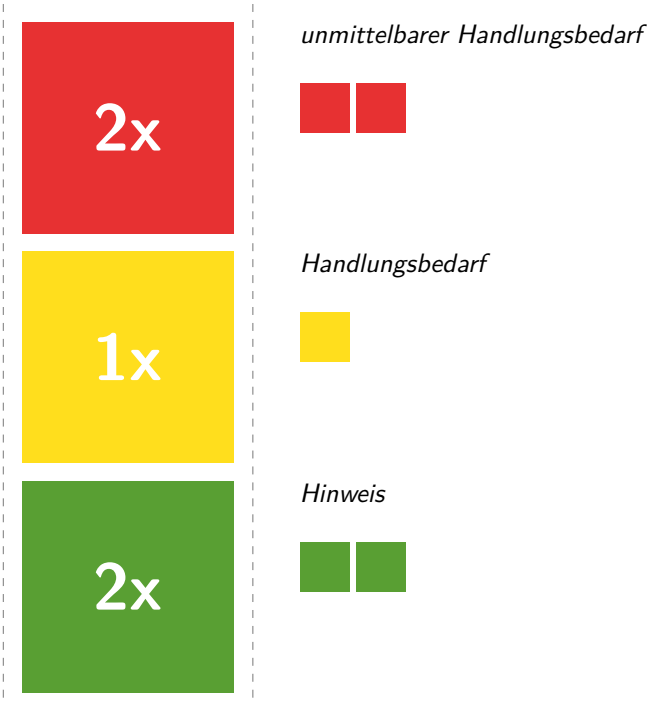


Abb. Risikoverteilung der Findings

Die untersuchte Anwendung weist Sicherheitsmängel in verschiedenen Kategorien auf, wie z.B. einem fehlerhaften Berechtigungsmanagement und fehlerhafter Eingabevalidierung. Sie entspricht nicht dem Sicherheitsniveau typischer Zahlungsapplikationen. Neben der Behebung der identifizierten Schwachstellen empfehlen wir den Softwareentwicklungsprozess zu verbessern und zum Beispiel Code Reviews bei zentralen Änderungen vorzunehmen.

3.2 Liste der Findings

1

Nicht behoben: *Berechtigungsmanagement*

Merchants können die im System hinterlegten Benutzerkonten löschen. Siehe Seite 10.

System: Payment Gateway

2

Nicht behoben: *Eingabevalidierung*

Aufgrund fehlender Eingabevalidierung können Datenbankinhalte über einen Parameter ausgelesen werden. Siehe Seite 11.

System: Payment Gateway

3

Nicht behoben: *Sitzungsverwaltung*

Die Zugriffstoken sind nach einer Benutzerabmeldung weiterhin gültig. Siehe Seite 12.

System: Payment Gateway

4

Nicht behoben: *Sitzungsverwaltung*

Die API verwendet eine veraltete Methode zum Ausstellen von Zugriffstoken. Siehe Seite 13.

System: OAuth2 Authorization Server

5

Nicht behoben: *Datenübertragung*

Beim Aufbau einer verschlüsselten Verbindung zwischen Client und Server werden veraltete Protokolle sowie schwache Kryptoalgorithmen unterstützt. Siehe Seite 14.

System: Payment Gateway

4 Technischer Bericht

4.1 Fehlerhafte Autorisierung

unmittelbarer Handlungsbedarf
Schaden: Hoch
Eintrittswahrscheinlichkeit: Hoch

Finding #1 **Nicht behoben**

Das Payment-Gateway unterscheidet zwischen den beiden Benutzerrollen 'Administrator' und 'Merchant'. Während Administratoren die Benutzer verwalten, können Merchants Kreditkartenzahlungen über die API abwickeln. Aufgrund einer fehlerhaften Autorisierung sind Merchants in der Lage, die in der Anwendung hinterlegten Benutzerkonten zu löschen:

Anfrage eines Zugriffstokens als Merchant

Erfolgreiche Löschung eines Benutzerkontos

Empfehlung

Merchants sollten keine Benutzer löschen dürfen.

4.2 SQL-Injection

unmittelbarer Handlungsbedarf
Schaden: Hoch
Eintrittswahrscheinlichkeit: Hoch

Finding #2 **Nicht behoben**

Bei einer SQL-Injection wird die fehlende Überprüfung von Benutzereingaben ausgenutzt, um Datenbankbefehle einzuschleusen. Wie über die folgende URL beobachtet werden kann, kann die MySQL-Sleep-Funktion über den 'paymentToken' im HTTP-Request zur Auflistung von konkreten Zahlungsinformationen ausgeführt werden (GET /payments/{paymentToken}):

- `https://api.dubius-payment.com/payments/'%20or%20sleep(5);--`

Unter Verwendung von Zeitverzögerungen können Datenbankinhalte extrahiert werden, wie nachfolgendes Listing zeigt. Bei diesem Verfahren werden alle Zeichen von einem Datenbankeintrag einzeln durchiteriert, wobei eine Zeitverzögerung einsetzt, wenn der korrekte Buchstabe an der Reihe ist.

```
Database: dubius
  Table: payments
  [1531 entries]
  +--------------------------------------+-------------+---------------------------------+
  |payment_token                         | merchant_id | subject                         |
  +--------------------------------------+-------------+---------------------------------+
  |387d55db-36fd-4ff5-859b-07ef971d3c12 | 8           | Vulnus Health Order #28390      |
  +--------------------------------------+-------------+---------------------------------+
  |41f0cd66-0b1d-45ca-92ee-a45e45b2947a | 5           | Oblivius Education Order #3201 |
  +--------------------------------------+-------------+---------------------------------+
  (...)
```

Empfehlung

Zur Vermeidung von SQL-Injections sollten Prepared Statements verwendet werden.

4.3 Keine Deaktivierung der Zugriffstoken nach einem Benutzerlogout

- Handlungsbedarf
- Schaden: Mittel
- Eintrittswahrscheinlichkeit: Mittel

Finding #3 **Nicht behoben**

Das Payment Gateway verwendet Zugriffstoken, um HTTP-Requests einem Benutzerkonto zuzuordnen:

Die Zugangstoken bleiben jedoch nach einer Benutzerabmeldung weiterhin gültig (GET /user/logout). Sofern ein Angreifer in den Besitz eines Tokens von seinem Opfer gelangt, könnte er trotz einer Benutzerabmeldung Aktionen in dessen Namen ausführen.

Empfehlung

Der Zugriffstoken eines Benutzers sollte nach einem Benutzerlogout serverseitig deaktiviert werden.

4.4 Verwendung des veralteten OAuth 2.0 „Password Grant“

Hinweis
Schaden: Warnung
Eintrittswahrscheinlichkeit: Gering

Finding #4 **Nicht behoben**

Wie aus dem folgenden Screenshot entnommen werden kann, wurde OAuth2 als Benutzerauthentifizierung beim Payment Gateway implementiert:

Der „Password Grant“ von OAuth2 erlaubt es einem Benutzer Zugangstoken unter Verwendung seiner Zugangsdaten zu beziehen. Nach Security Best Practices[1] sollte dieser Grant-Typ nicht mehr unterstützt werden, da er die Zugangsdaten des Ressourcenbesitzers dem Client offenlegt. Stattdessen sollte der Grant-Type „Client Credentials“ verwendet werden.

Empfehlung

Es sollte evaluiert werden, ob der Grant-Typ „Client Credentials“ implementiert werden kann, um den unsicheren „Password Grant“ zu ersetzen.

[1] https://datatracker.ietf.org/doc/html/draft-ietf-oauth-security-topics

4.5 Unterstützung von TLS 1.0 und TLS 1.1 und nicht kryptographisch starken Cipher-Suites

Hinweis
Schaden: Warnung
Eintrittswahrscheinlichkeit: Gering

Finding #5 **Nicht behoben**

Beim Aufbau einer verschlüsselten Verbindung zwischen Client und Server werden vom Payment Gateway ältere Protokolle wie TLS 1.0 und TLS 1.1 unterstützt. Diese gelten als unsicher, wie in der technischen Richtlinie vom Bundesamt für Sicherheit in der Informationstechnik (*BSI TR-02102-2*[2]) nachgelesen werden kann. Das folgende Listing zeigt exemplarisch die unterstützten Protokolle des Webservers `https://api.dubius-payment.com/`:

```
Supported Server Cipher(s):
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve 25519 DHE 253
Preferred TLSv1.1  256 bits  ECDHE-RSA-AES256-SHA          Curve 25519 DHE 253
Preferred TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA          Curve 25519 DHE 253
```

Zudem unterstützt der Webserver die Cipher-Suite 'ECDHE-RSA-AES256-SHA' über TLS 1.2, welche vom BSI nicht mehr empfohlen wird.

Empfehlung

Die Protokolle TLS 1.0 und TLS 1.1 sowie die schwache Cipher Suite sollten nicht mehr unterstützt werden.

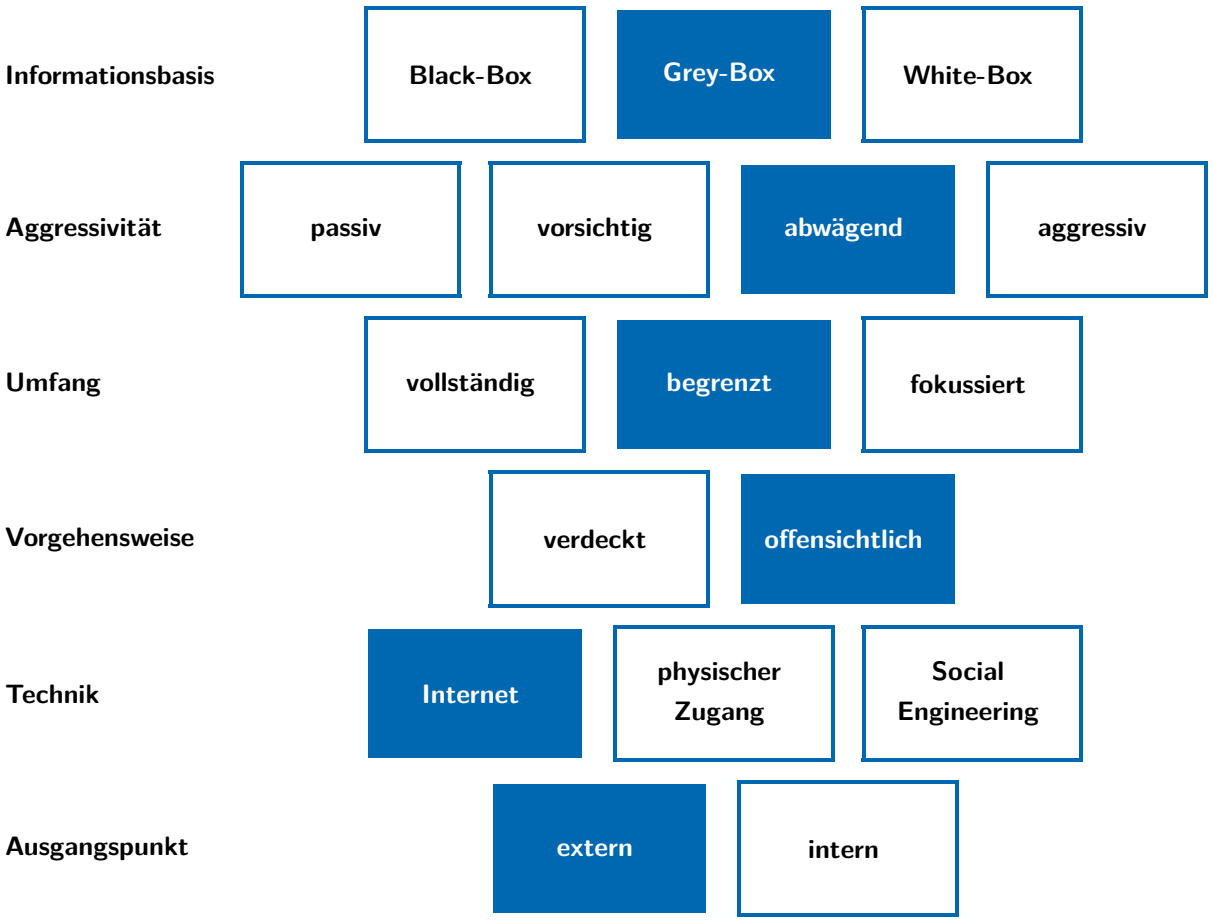
[2] `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.html`

5 Anhang A

5.1 Klassifizierung-Details

Als Vorgehensweise wurde in Kooperation mit der Dubius Payment Ltd. folgende Klassifizierungsvariante ausgewählt: Der Penetrationstest wurde als externer 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 Web-Anwendungen und APIs

Die Untersuchungsmethode der binsec GmbH bei Webanwendungen orientiert sich am OWASP Testing Guide und an den OWASP TOP 10. Das Open Web Application Security Project (OWASP) ist derzeit die weltweit größte Non-Profit-Organisation mit dem Ziel, die Sicherheit von Anwendungen zu erhöhen. Die OWASP Top 10 beinhalten die zehn kritischsten Schwachstellen bei Webanwendungen. Nach der aktuellen Veröffentlichung von 2021 sind beispielsweise die meisten Schwachstellen bei Webanwendungen auf Fehler im Berechtigungsmanagement zurückzuführen. Ebenfalls werden die OWASP API Security Top 10 beim Penetrationstest einbezogen, wenn Application Programming Interfaces (APIs) zum Untersuchungsgegenstand gehören.

Prüfpunkte

Der methodische Prüfungsansatz von der binsec GmbH unterteilt sich grob in die 16 folgenden Prüfphasen. Innerhalb der Prüfphasen wird die Webanwendung auf die Schwachstellen der OWASP TOP 10 untersucht. Während des Penetrationstests werden verschiedene Tools zur Analyse eingesetzt sowie intensive manuelle Prüfungen vorgenommen. Der genaue Verlauf des Penetrationstests ist stark von der Charakteristik der jeweiligen Anwendung abhängig und orientiert sich an der Vorgehensweise eines realen Angreifers:

1. Informationssammlung (passiv, externe Ressourcen)
2. Prüfung der zugrunde liegenden IT-Systeme als Angriffsvektor
3. Informationssammlung (aktiv, Prüfobjekte)
4. Konfigurationsmanagement Webserver & Webanwendung
5. Prüfung der Zugriffskontrollen bei Benutzerauthentifikation
6. Identitätsmanagement & Registrierungsprozess
7. Prüfung der Handhabung von Benutzerkennwörtern
8. Sichere Datenübertragung
9. Sitzungsverwaltung
10. Berechtigungsprüfung
11. Berechtigungsprüfung der Mehrmandantenfähigkeit
12. Eingabevalidierung (z.B. Injection, XSS)
13. Überprüfung der Dateiuploadmöglichkeiten
14. Low and Slow Denial of Service
15. Fehlerbehandlung
16. Erfolgreiche Schwachstellenausnutzung

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:

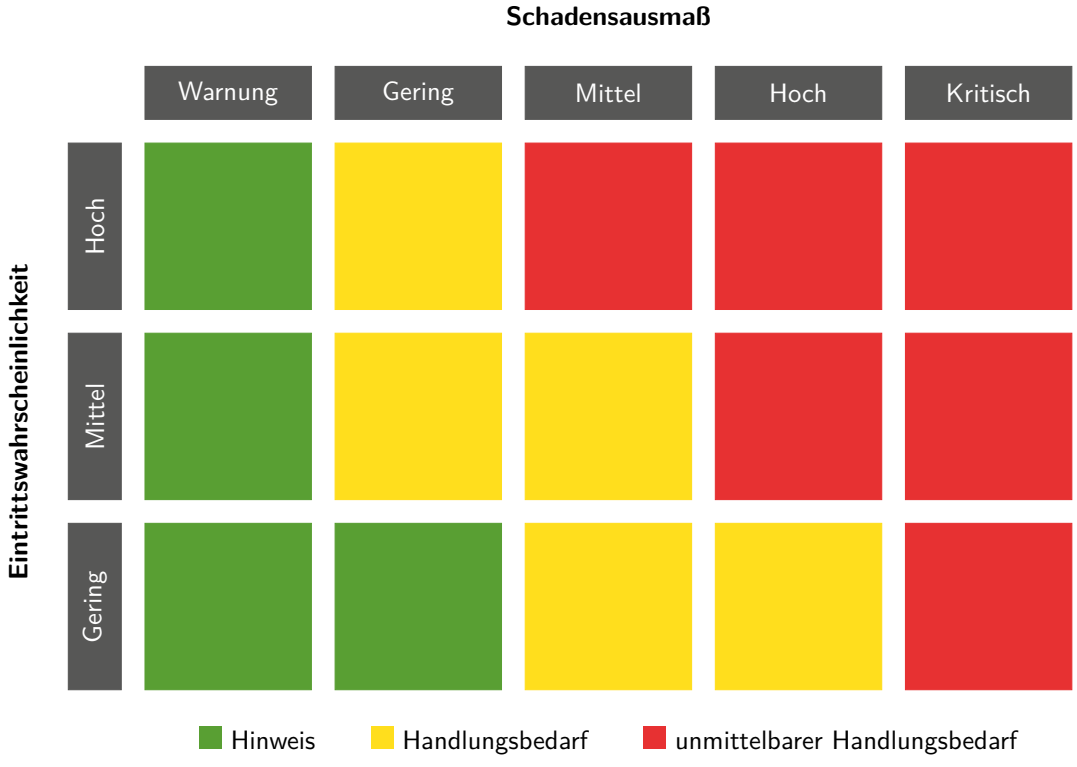
Eintrittswahrscheinlichkeit

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