Penetrationstestbericht

Externe IT

der Dubius Payment Ltd.

EXAMPLE

13. Januar 2025

v1.1

Inhaltsverzeichnis

i Änderungsverzeichnis

Version	Beschreibung	Autor	Datum
1.0	Reporterstellung	Dominik Sauer	13. Januar 2025
1.1	Qualitätssicherung	QA-Team	13. Januar 2025

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. 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.

2.2 Rahmenbedingungen

Der Penetrationstest wurde zwischen dem 6. 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

Im Detail sollten die IT-Systeme im Netzbereich 185.156.252.0/27 auf Schwachstellen hin untersucht 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 → Network: 185.156.252.0/27

Ergebnis	Task: Informationssammlung	Findings
✔	Identifikation des verantwortlichen Unternehmens für den IP-Adressbereich	-
✔	Identifikation von Domain-Namen	-
Ergebnis	**Task: Diensterkennung**	**Findings**
✔	Identifikation von aktiven IT-Systemen und Diensten	-

Prüfobjekt → Network: 185.156.252.0/27 · IP: 185.156.252.12 (sslvpn.dubius-payment.com) · HTTPS: 443/tcp

Ergebnis	Task: HTTPS Check	Findings
✔	Informationssammlung (passiv, externe Ressourcen)	-
✔	Informationssammlung (aktiv, Prüfobjekte)	-
✔	Konfigurationsmanagement Webserver & Webanwendung	-
✘	Prüfung der Zugriffskontrollen bei Benutzerauthentifikation	Seite 10
✔	Sichere Datenübertragung	-
✔	Eingabevalidierung (z.B. Injection, XSS)	-

Prüfobjekt → Network: 185.156.252.0/27 · IP: 185.156.252.19 (exchange.dubius-payment.com) · SMTP: 25/tcp und 465/tcp

Ergebnis	Task: Informationssammlung	Findings
✔	Überprüfung, ob SMTP-Befehle zur Informationsgewinnung deaktiviert wurden	-
Ergebnis	**Task: Konfigurationsmanagement**	**Findings**
✔	Überprüfung, ob E-Mails an externe Personen mit einer unternehmensinternen E-Mail-Adresse versendet werden können (Open-Relay)	-
✘	Überprüfung, ob gefälschte E-Mails mit unternehmensinterner Absender-Adresse an Mitarbeiterinnen und Mitarbeiter versendet werden können	Seite 13
Ergebnis	**Task: Sichere Datenübertragung**	**Findings**
✔	Überprüfung der verwendeten SSL/TLS-Protokolle und Cipher-Suites	-

Ergebnis	Task: Identifikation von Schwachstellen	Findings
✔	Überprüfung, ob Schwachstellen für die eingesetzte Softwareversion bekannt sind	-

Prüfobjekt → Network: 185.156.252.0/27 · IP: 185.156.252.19 (exchange.dubius-payment.com) · HTTPS: 443/tcp

Ergebnis	Task: HTTPS Check	Findings
✔	Informationssammlung (passiv, externe Ressourcen)	-
✔	Informationssammlung (aktiv, Prüfobjekte)	-
✘	Konfigurationsmanagement Webserver & Webanwendung	Seite 12
✔	Prüfung der Zugriffskontrollen bei Benutzerauthentifikation	-
✘	Sichere Datenübertragung	Seite 14
✔	Eingabevalidierung (z.B. Injection, XSS)	-

3 Managementübersicht

3.1 Zusammenfassung

Der Penetrationstest wurde zwischen dem 6. Januar 2025 und 10. Januar 2025 durchgeführt. Dabei konnten 5 Schwachstellen identifiziert werden, die zu 4 Findings zusammengefasst und einer initialen Risikobewertung unterzogen wurden. Insgesamt wurden 2 Findings mit unmittelbarem Handlungsbedarf und ein Finding mit Handlungsbedarf bewertet. Das Finding mit der Bewertung Hinweis ist als Vorschlag zur Erhöhung des Sicherheitsniveaus zu verstehen.

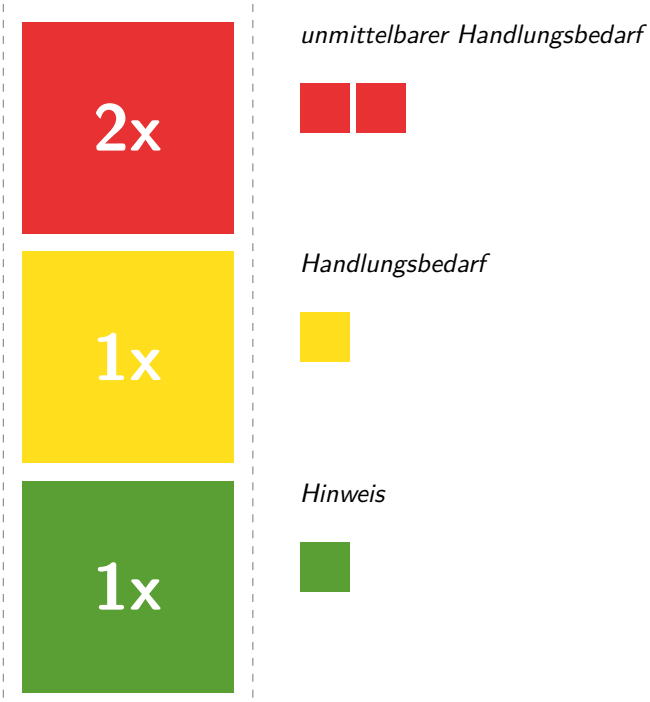


Abb. Risikoverteilung der Findings

Während des Penetrationstests konnten kritische Schwachstellen identifiziert werden, welche auf eine schwache Passwortrichtlinie und veraltete Softwarelösungen zurückzuführen sind. So können beispielsweise die Zugangsdaten von Mitarbeitern und Mitarbeiterinnen der Dubius Payment Ltd. erraten werden, wodurch unbefugt auf interne IT-Systeme von extern zugegriffen werden kann. Alle kritischen Schwachstellen sollten umgehend behoben werden.

3.2 Liste der Findings

1 

Nicht behoben: *Zugangskontrolle*

Die Passwörter von Active-Directory-Nutzern können erraten werden. Siehe Seite 10.

System: 185.156.252.12

2 

Nicht behoben: *Patch-Management*

Es werden veraltete Softwarekomponenten eingesetzt, für die bereits Schwachstellen bekannt sind. Siehe Seite 12.

System: 185.156.252.19

3 

Nicht behoben: *Fehlkonfiguration*

Sicherheitsmaßnamen gegen das Versenden von Mails mit gefälschter unternehmensinterner Absenderadresse fehlen. Siehe Seite 13.

System: 185.156.252.19

4 

Nicht behoben: *Datenübertragung*

Beim Aufbau einer verschlüsselten Verbindung zwischen Client und Server werden kryptographisch nicht starke Protokolle sowie schwache Cipher-Suiten unterstützt. Siehe Seite 14.

System: 185.156.252.12, 185.156.252.19

4 Technischer Bericht

4.1 Schwache Active-Directory-Passwörter

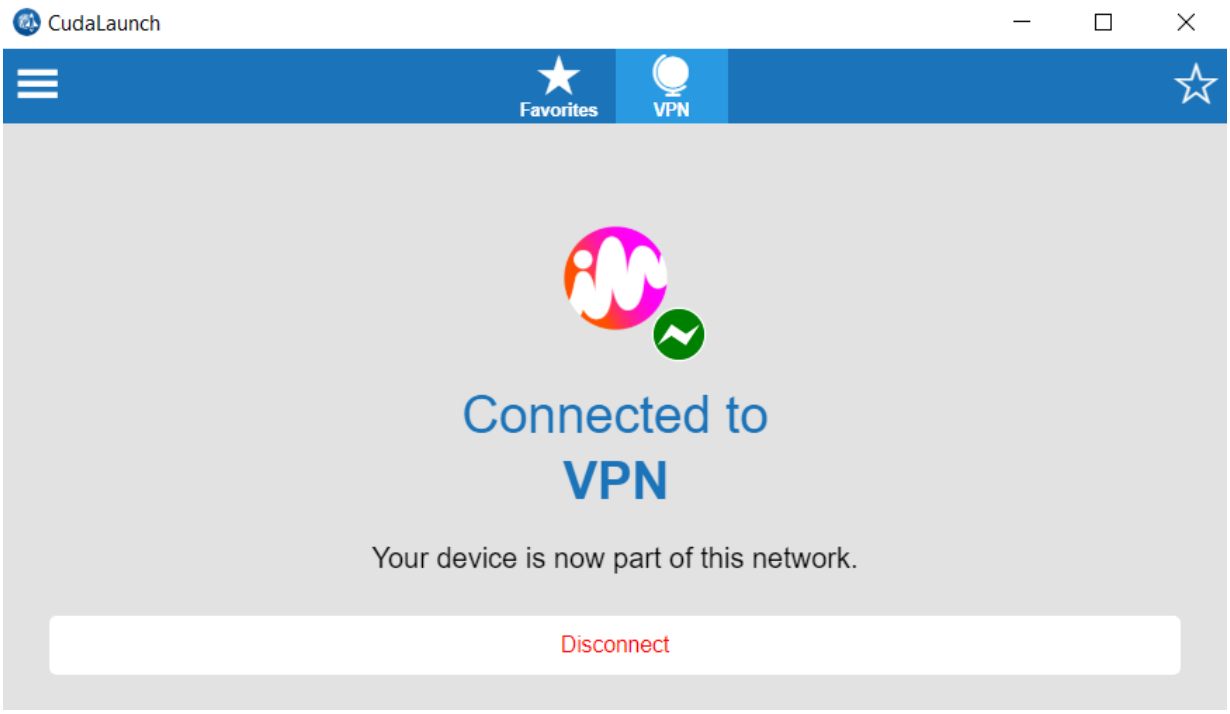
unmittelbarer Handlungsbedarf
Schaden: Kritisch
Eintrittswahrscheinlichkeit: Mittel

Finding #1 **Nicht behoben**

Mittels Password Spraying konnten im Zuge des Penetrationstests die Kennwörter mehrerer Benutzer erraten werden. Wie nachfolgend zu sehen ist, neigen Benutzer dazu, Passwörter nach einem vorhersehbarem Schema zu vergeben. Die kompromittierten Benutzerkonten verwenden beispielsweise Abwandlungen des Firmennamens als Passwort:

- csimmons:Dubius2021!
- pbaker:Dubius1+

Mit Hilfe der oben genannten Zugangsdaten konnte sich erfolgreich zum internen Unternehmensnetzwerk via SSL-VPN verbunden werden:



In Rücksprache mit der Dubius Payment Ltd. sollte das interne Netzwerk nicht weiter auf Schwachstellen hin untersucht werden.

Empfehlung

Alle Benutzerpasswörter sollten umgehend geändert werden. Grundsätzlich sollte ein starkes Passwort mindestens 12 Zeichen lang sein und eine Kombination aus Klein- und Großbuchstaben, Zahlen und Sonderzeichen beinhalten.

Ergänzend zur Passwortrichtlinie könnte mit Hilfe einer Password Policy Enforcement Lösung bei der Vergabe von Kennwörtern auf Wörterbucheinträge, Namen sowie auf das Vorhandensein in vergangenen Passwort Leaks geprüft werden. Grundsätzlich reduzieren Wörter wie der Firmenname im Passwort die Entropie eines Passworts.

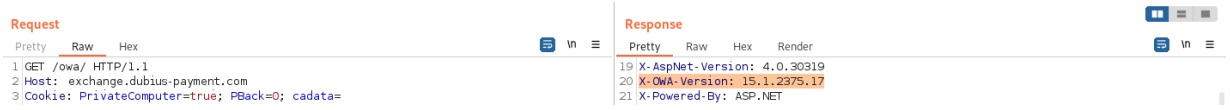
4.2 Einsatz von veralteter Software

unmittelbarer Handlungsbedarf
Schaden: Kritisch
Eintrittswahrscheinlichkeit: Mittel

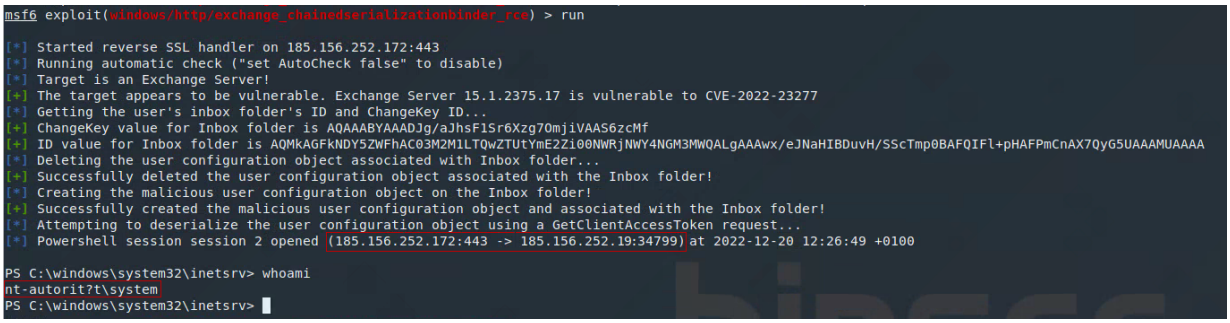
Finding #2

Nicht behoben

Während des Penetrationstests konnte eine veraltete Softwarelösung identifiziert werden, wofür bereits Schwachstellen bekannt sind. Wie aus dem folgenden Screenshot entnommen werden kann, setzt die Dubius Payment Ltd. einen Microsoft Exchange ein, dessen Version (15.1.2375.17) als veraltet gilt[1]:



Zum Beispiel ist die o.g. Exchange-Version anfällig gegenüber eine Remote Code Execution (RCE), welche aber zur Ausnutzung ein valides Benutezrkonto erfordert[2]. In Rücksprache mit der Dubius Payment Ltd. und unter Verwendung der kompromittierten Benutzerkonten aus dem Finding auf Seite 10 konnte die Schwachstelle erfolgreich verifiziert werden:



Empfehlung

Die o.g. Softwarelösungen sollten umgehend aktualisiert werden.

[1] https://learn.microsoft.com/en-us/exchange/new-features/build-numbers-and-release-dates?view=exchserver-2019
[2] https://nvd.nist.gov/vuln/detail/CVE-2022-23277

4.3 Kein Schutz vor E-Mails mit gefälschter unternehmensinterner Absenderadresse

- Handlungsbedarf
- Schaden: Mittel
- Eintrittswahrscheinlichkeit: Mittel

Finding #3 **Nicht behoben**

Über den SMTP-Server 185.156.252.19:25 können Mails mit gefälschter unternehmensinterner Absenderadresse an die Mitarbeiterinnen und Mitarbeiter der Dubius Payment Ltd. versendet werden. So wurde beispielsweise mit dem nachfolgenden Linux-Befehl eine Mail von csimmons@dubius-payment.com an das Postfach dwestcott@dubius-payment.com während des Penetrationstests erfolgreich zugestellt:

```
sendEmail \
-f csimmons@dubius-payment.com \
-t dwestcott@dubius-payment.com \
-s 185.156.252.19:25 \
-u Mail Spoofing Test -vv -o tls=no \
-m "[ English version below ]\n\nDies ist eine Testmail im Rahmen einer technischen
    Sicherheitsanalyse von der binsec GmbH. Falls Sie diese E-Mail erhalten, wuerden wir Sie
    bitten diese Mail an Herrn Dominik Sauer - ds@binsec.com - weiterzuleiten.\n\n\nVielen lieben
     Dank.\n\n###############\n\nThis is a test email as part of a technical security analysis by
    binsec GmbH. If you receive this email, we would ask you to forward this email to Mr. Sauer (
    ds@binsec.com).\n\nThank you very much."
```

Infolgedessen kann sich als ein beliebiger Angestellter der Dubius Payment Ltd. ausgegeben werden und in dessen Namen versucht werden, z.B. Zahlungen in Auftrag zu geben.

Empfehlung

Grundsätzlich kann eine vertrauenswürdige E-Mail-Kommunikation nur durch digitale Signaturen bzw. Kryptographie erreicht werden. Nichtsdestotrotz empfehlen wir die Umsetzung von üblichen Security-Best-Practices. Darunter fällt beispielsweise der Eintrag korrekter SPF-Records (Sender Policy Framework) für die Domain 'dubius-payment.com', das Aktivieren von DKIM-Signaturen und spezifizieren einer DMARC-Richtlinie sowie die Einführung von angemessenen SPAM-Filtern. So könnten eingehende E-Mails mit einer gefälschten Absenderadresse @dubius-payment.com erkannt werden, wenn diese nicht von einem validen System verschickt wurden.

4.4 Unterstützung und TLS 1.1 und nicht kryptographisch starken Cipher-Suites

Hinweis
Schaden: Gering
Eintrittswahrscheinlichkeit: Gering

Finding #4 **Nicht behoben**

Beim Aufbau einer verschlüsselten Verbindung zwischen Client und Server werden von den folgenden Webservern ältere Protokolle wie TLS 1.1 unterstützt:

- 185.156.252.12
- 185.156.252.19

Diese gelten als unsicher, wie in der technischen Richtlinie vom Bundesamt für Sicherheit in der Informationstechnik (BSI TR-02102-2[3]) nachgelesen werden kann. Das folgende Listing zeigt exemplarisch die unterstützten Protokolle des Webservers `https://185.156.252.19`:

```
SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   disabled
TLSv1.1   enabled
TLSv1.2   enabled
TLSv1.3   enabled
```

Zudem werden Cipher Suiten von den o.g. IT-Systemen über TLS 1.2 unterstützt, welche vom BSI nicht mehr empfohlen werden:

- ECDHE-RSA-AES256-SHA
- ECDHE-RSA-AES128-SHA
- AES128-SHA
- AES256-SHA
- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA

Empfehlung

Die veralteten Protokolle sowie die schwachen Cipher Suiten sollten nicht mehr unterstützt werden.

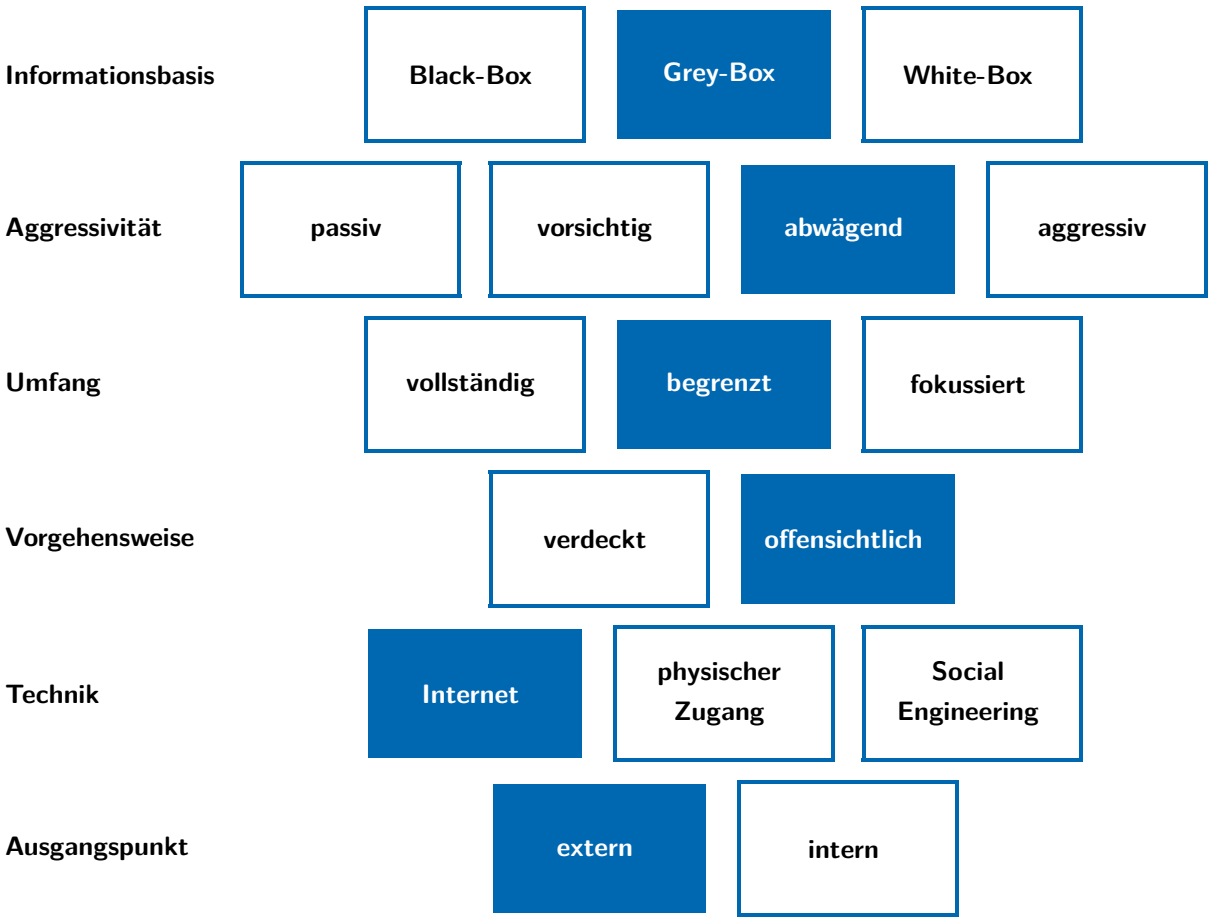
[3] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.html

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 IT-Infrastrukturen

Der genaue Verlauf eines Penetrationstests hängt stark von den spezifischen Diensten in einer IT-Infrastruktur ab. Dennoch lässt sich die Vorgehensweise eines realen Angreifers verallgemeinern. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) listet in seinem Durchführungskonzept für Penetrationstests beispielsweise Modulbeschreibungen für aktive Eindringsversuche auf. In Anlehnung an den Angaben vom BSI unterteilt sich der methodische Prüfungsansatz der binsec GmbH grob in die 3 folgenden Prüfphasen:

Identifikation der Angriffsfläche

- Auswertung öffentlich zugänglicher Daten
- Identifikation der erreichbaren Dienste anhand offenen Ports über TCP und UDP
- Überprüfung, ob Zugangskontrollen wie Firewalls oder Netzwerksegmentierung vorhanden sind

Prüfung auf Sicherheitslücken

- Überprüfung der Patchstände und der eingesetzten Softwareversionen nach Aktualität
- Überprüfung der Zugangsbeschränkungen von Diensten
- Überprüfung der Absicherung von Diensten nach Security Best Practices

Exploitation

- Entwicklung von Proof-of-Concepts zur Ausnutzung von identifizierten Schwachstellen
- Rechteausweitung anhand der Verkettung von Schwachstellen

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:

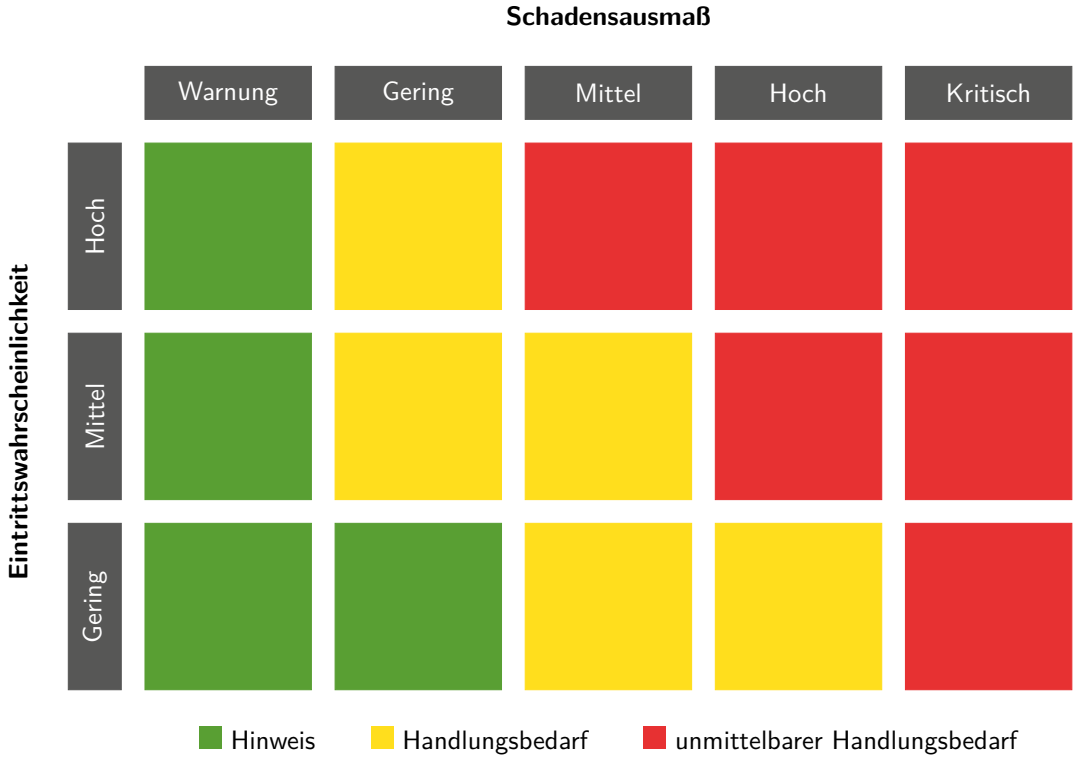
Eintrittswahrscheinlichkeit

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