Penetrationstestbericht

Interne IT

der Dubius Payment Ltd.

EXAMPLE

6. Juni 2024

v1.1

Inhaltsverzeichnis

i Änderungsverzeichnis

Version	Beschreibung	Autor	Datum
1.0	Reporterstellung	Dominik Sauer	5. Juni 2024
1.1	Qualitätssicherung	QA-Team	6. Juni 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. 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 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

Im Detail wurden die IT-Systeme der Domäne 'dubius-payment.com' auf Schwachstellen hin überprüft, welche sich in den folgenden privaten IPv4-Netzbereichen befanden:

- 10.250.53.0/24 (DMZ)
- 10.247.97.0/24 (Management)
- 10.250.229.0/24 (Client)

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 → Active Directory: Dubius

Ergebnis	Task: Konfigurationsmanagement	Findings
✘	Verifikation ob SMB-Signing aktiviert wurde	Seite 13
Ergebnis	**Task: Identifikation von Schwachstellen**	**Findings**
✔	Überprüfung, ob der Domain-Controller anfällig gegenüber bereits veröffentlichten Schwachstellen ist	-
Ergebnis	**Task: Identifikation von Schwachstellen (ohne Zugangsdaten)**	**Findings**
✔	Manuelle und automatische AD Enumerierung	-
✔	NTLM-Relay zu LDAP(S) (LDAP Signing und Channel Binding)	-
✔	Prüfen auf Zugangsdaten aus Credential Leaks	-
✔	Extrahieren von AD Zugangsdaten aus Netzwerkdruckern	-
✔	Abfangen von Benutzernamen und Hashes mittels Network Poisoning	-
✔	Prüfen, ob die Erstellung von Computerobjekten erzwungen werden kann, um einen ersten Zugang zu erhalten	-
✔	Prüfen, ob ein Computerobjekt erstellt und der Zugriff delegiert werden kann	-
✘	Prüfen, ob gültige Anmeldedaten via Passwort-Spraying bzw. Bruteforce erraten werden können	Seite 15
✔	Überprüfung ob WSUS Spoofing möglich ist	-
✔	Abfangen von Zugangsdaten aus unverschlüsseltem Netzwerkverkehr	-
Ergebnis	**Task: Identifikation von Schwachstellen (mit Zugangsdaten)**	**Findings**
✔	Überprüfung auf falsch konfigurierte ADCS-Templates	-
✔	Prüfung, ob Passwörter in Beschreibungsfeldern von AD-Benutzern zu finden sind	-
✘	Durchsuchen von Dateifreigaben nach Zugangsdaten	Seite 16
✔	Überprüfung, ob sensitive Daten in Gruppenrichtlinieneinstellungen offengelegt werden	-
✔	Extraktion von Passworthashes (Kerberoasting)	-
Ergebnis	**Task: Privilege Escalation**	**Findings**
✘	Auslesen lokaler Hashes und zwischengespeicherter Kennwörter	Seite 15

Prüfobjekt → Network: Internal IT · DNS: DNS (tcp/53)

Ergebnis	Task: Informationssammlung	Findings
✔	Identifikation der hinterlegten DNS-Einträge	-
Ergebnis	**Task: Konfigurationsmanagement**	**Findings**
✔	Überprüfung, ob ein Zonentransfer durchgeführt werden kann	-
Ergebnis	**Task: Identifikation von Schwachstellen**	**Findings**
✔	Überprüfung, ob Schwachstellen für die eingesetzte Softwareversion des DNS-Servers bekannt sind	-

Prüfobjekt → Network: Internal IT · FTP: FTP (tcp/21)

Ergebnis	Task: Konfigurationsmanagement	Findings
✔	Überprüfung, ob ein anonymer Login vom FTP-Server unterstützt wird	-
Ergebnis	**Task: Sichere Datenübertragung**	**Findings**
✔	Überprüfung, ob sensitive Daten im Klartext übertragen werden	-
Ergebnis	**Task: Identifikation von Schwachstellen**	**Findings**
✔	Überprüfung, ob Schwachstellen für die eingesetzte Softwareversion bekannt sind	-

Prüfobjekt → Network: Internal IT · HTTP: HTTP (tcp/80)

Ergebnis	Task: HTTP Check	Findings
✔	Informationssammlung (aktiv, Prüfobjekte)	-
✘	Sichere Datenübertragung	Seite 18

Prüfobjekt → Network: Internal IT · HTTPS: HTTPS (tcp/443)

Ergebnis	Task: HTTPS Check	Findings
✔	Informationssammlung (aktiv, Prüfobjekte)	-
✔	Prüfung der Zugriffskontrollen bei Benutzerauthentifikation	-
✔	Eingabevalidierung (z.B. Injection, XSS)	-

Prüfobjekt → Network: Internal IT · IPMI: IPMI (udp/623)

Ergebnis	Task: Konfigurationsmanagement	Findings
✔	Überprüfung, ob auf den Server über die IPMI-Schnittstelle ohne Benutzerauthentifikation zugegriffen werden kann	-
Ergebnis	**Task: Identifikation von Schwachstellen**	**Findings**

✔	Überprüfung, ob mit der Cipher Zero die Authentifikation umgangen werden kann	-
✔	Überprüfung, ob Passworthashes für die Systembenutzer von extern abgefragt werden können	-

Prüfobjekt → Network: Internal IT · LDAP: LDAP, LDAPS (tcp/389, tcp/636)

Ergebnis	Task: Informationssammlung	Findings
✔	Informationssammlung ohne Zugangsdaten	-
Ergebnis	**Task: Sichere Datenübertragung**	**Findings**
✔	Überprüfung, ob sensitive Daten im Klartext übertragen werden	-

Prüfobjekt → Network: Internal IT · MySQL / MariaDB: MYSQL (tcp/3306)

Ergebnis	Task: Konfigurationsmanagement	Findings
✔	Überprüfung, ob eine Verbindung zur Datenbank ohne Benutzerauthentifikation hergestellt werden kann	-
Ergebnis	**Task: Identifikation von Schwachstellen**	**Findings**
✔	Überprüfung, ob Schwachstellen für die eingesetzte Softwareversion bekannt sind	-

Prüfobjekt → Network: Internal IT · NTP: NTP (udp/123)

Ergebnis	Task: Informationssammlung	Findings
✔	Überprüfung, ob NTP-Befehle zur Informationsgewinnung deaktiviert wurden	-
Ergebnis	**Task: Konfigurationsmanagement**	**Findings**
✔	Überprüfung, ob der NTP-Server als Teil eines DDoS-Angriffs misstbraucht werden kann	-
Ergebnis	**Task: Identifikation von Schwachstellen**	**Findings**
✔	Überprüfung, ob Schwachstellen für die eingesetzte Softwareversion bekannt sind	-

Prüfobjekt → Network: Internal IT · RDP: RDP (tcp/3389)

Ergebnis	Task: Informationssammlung	Findings
✔	Identifikation des verwendeten Betriebssystems über eine RDP-Verbindung	-
Ergebnis	**Task: Identifikation von Schwachstellen**	**Findings**
✔	Überprüfung, ob der RDP-Server gegen bereits bekannte Schwachstellen gepatcht wurde	-

Prüfobjekt → Network: Internal IT · RPC: RPC (tcp/139)

Ergebnis	Task: Informationssammlung	Findings
✔	Überprüfung, ob Remote-Procedure-Calls ohne Benutzerauthentifikation ausgeführt werden können	-

Prüfobjekt → Network: Internal IT · SMB: SMB (tcp/445)

Ergebnis	Task: Informationssammlung	Findings
✘	Identifikation der erreichbaren Netzwerkverzeichnisse ohne Benutzerauthentifikation via SMB	Seite 16

Ergebnis	Task: Identifikation von Schwachstellen	Findings
✔	Überprüfung, ob der SMB-Server gegen bereits bekannte Schwachstellen gepatcht wurde	-

Prüfobjekt → Network: Internal IT · SMTP: SMTP (tcp/25)

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	-

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

Prüfobjekt → Network: Internal IT · SNMP: SNMP (udp/161)

Ergebnis	Task: Konfigurationsmanagement	Findings
✘	Überprüfung, ob Systeminformationen aufgrund der Unterstützung von veralteten SNMP-Protokollen extrahiert werden können	Seite 19

Prüfobjekt → Network: Internal IT · SSH: SSH (tcp/22)

Ergebnis	Task: Konfigurationsmanagement	Findings
✔	Überprüfung, ob eine veraltete SSH Protokollversion unterstützt wird	-

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

Prüfobjekt → Network: Internal IT · Telnet: TELNET (tcp/23)

Ergebnis	Task: Konfigurationsmanagement	Findings
✔	Überprüfung, ob auf das IT-System via Telnet zugegriffen werden kann	-

Ergebnis	Task: Identifikation von Schwachstellen	Findings
✔	Überprüfung, ob die Benutzerauthentifikation umgangen werden kann	-

3 Managementübersicht

3.1 Zusammenfassung

Der Penetrationstest wurde zwischen dem 5. Juni 2024 und 7. Juni 2024 durchgeführt. Dabei konnten 14 Schwachstellen identifiziert werden, die zu 5 Findings zusammengefasst und einer initialen Risikobewertung unterzogen wurden. Insgesamt wurden 3 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.

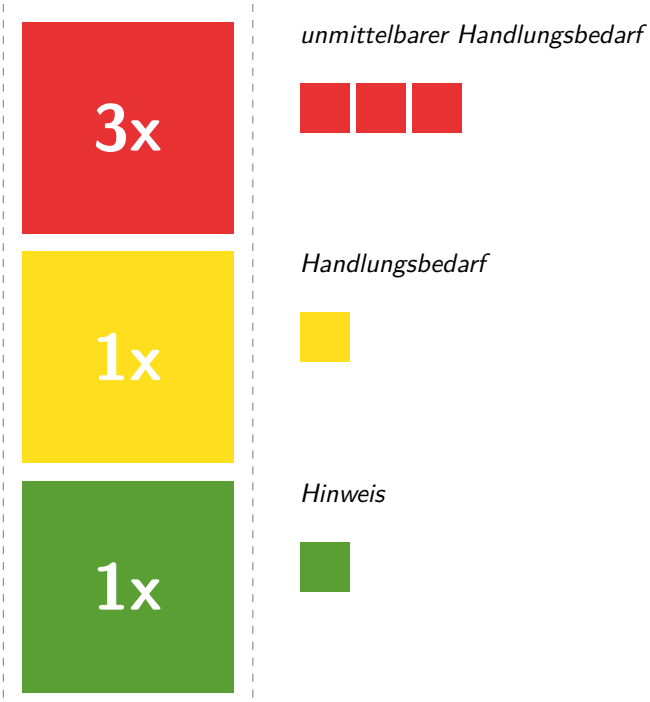


Abb. Risikoverteilung der Findings

Während des Penetrationstests konnten mehrere kritische Schwachstellen identifiziert werden, worüber alle internen IT-Systeme der Domäne 'Dubius' kompromittiert werden konnten. So kann beispielsweise aufgrund schwacher Benutzerpasswörter oder einer fehlenden Absicherung der Netzwerkverzeichnisse administrativer Zugriff erlangt werden. Alle kritischen Schwachstellen sollten umgehend behoben werden.

3.2 Liste der Findings

1

Nicht behoben: *Fehlkonfiguration*

Eine fehlende Sicherheitsvorkehrung bei den Netzwerkverzeichnissen ermöglicht die vollständige Kompromittierung aller IT-Systeme der internen Domäne. Siehe Seite 13.

System: SMB

2

Nicht behoben: *Zugangskontrolle*

Mehrere Domänenbenutzer verwenden schwache Benutzerpasswörter, wodurch unbefugt auf IT-Systeme zugegriffen werden kann. Siehe Seite 15.

System: Domain Controller

3

Nicht behoben: *Zugangskontrolle*

Aufgrund eines fehlerhaften Berechtigungsmanagement können über die Netzwerkverzeichnisse auf die Daten von fremden Domänenbenutzern zugegriffen werden. Siehe Seite 16.

System: 10.247.97.204, 10.247.97.210, 10.247.97.212

4

Nicht behoben: *Datenübertragung*

Die Zugangsdaten mehrerer Dienste und Anwendungen werden im Klartext übertragen. Siehe Seite 18.

System: z.B. 10.247.97.56, 10.247.97.57, 10.247.97.58 (insg. 5x)

5

Nicht behoben: *Fehlkonfiguration*

Systeminformationen wie die Netzwerkkonfiguration können aufgrund einer fehlenden Benutzerauthentifizierung extrahiert werden. Siehe Seite 19.

System: z.B. 10.247.97.174, 10.247.97.190, 10.247.97.201 (insg. 4x)

4 Technischer Bericht

4.1 Fehlendes SMB Signing

unmittelbarer Handlungsbedarf
Schaden: Kritisch
Eintrittswahrscheinlichkeit: Mittel

Finding #1 **Nicht behoben**

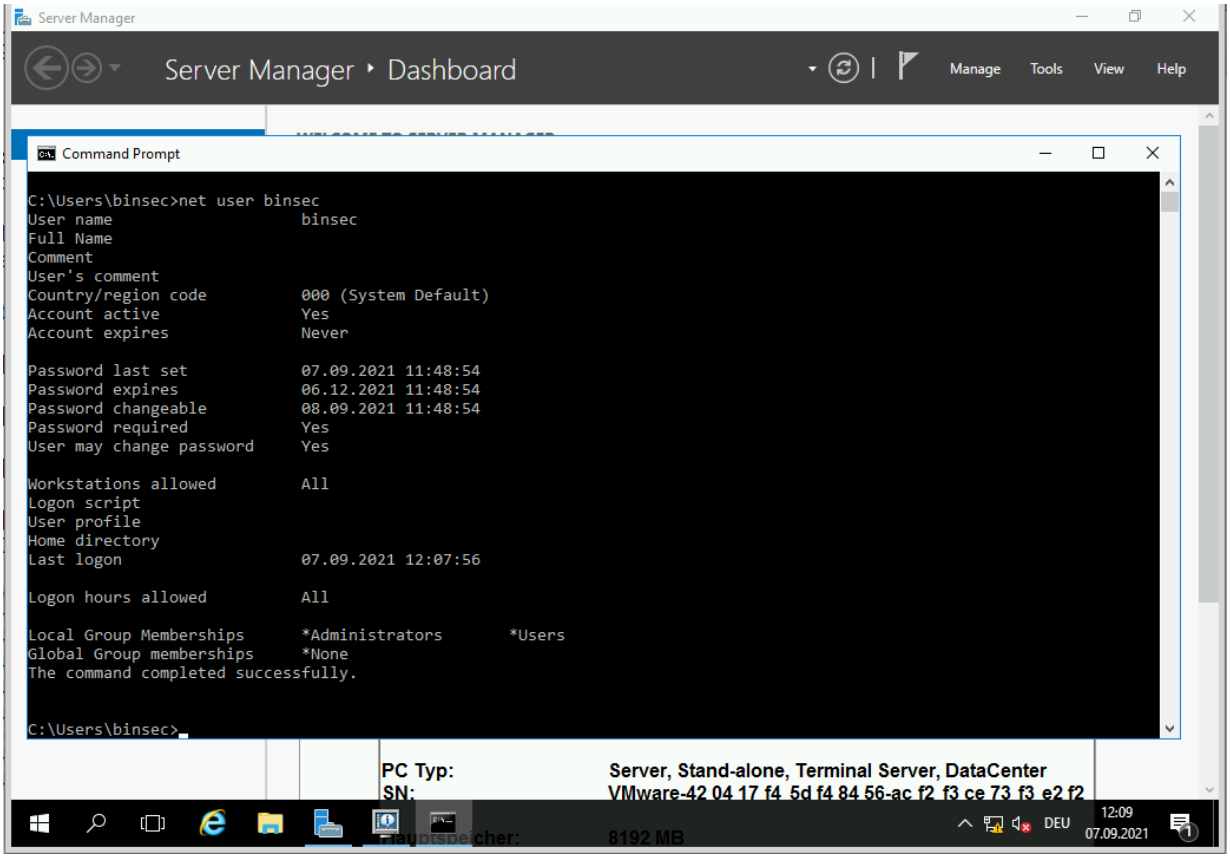
Für den Datenaustausch zwischen heterogenen Systemen verwendet die Dubius Payment Ltd. SMB, wie beispielsweise aus dem folgenden Portscan entnommen werden kann:

```
Nmap scan report for 10.247.97.142
Host is up (0.0013s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
Service Info: OS: Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
```

Als Benutzerauthentifikation an den Netzlaufwerken hat Windows ein Single-Sign-On-Verfahren implementiert, wobei Clients einen NTLM-Hash als Identitätsnachweis über das Netzwerk versenden. Wie aus dem folgenden Listing entnommen werden kann, können die NTLM-Hashes in einem lokalen Netzwerk abfangen werden.

```
[HTTP] NTLMv2 Username : Dubius\dpadmin
[HTTP] NTLMv2 Hash     : dpadmin::Dubius:4141414141414141414141414141414141:4
    e51fb6e7ae458c248879791706e1023:0101000000000000a79bd1ebad701815cd4bb325b[...]
```

Sofern der Besitzer eines abgefangenen Hashes privilegierte Berechtigungen auf einem beliebigen Zielsystem besitzt, kann ein Angreifer den Hash weiterleiten, um sich auf dem IT-System anzumelden und Systembefehle auszuführen. Infolgedessen war es während des Penetrationstests möglich, Befehle als administrativer Benutzer der internen Domäne 'Dubius' auszuführen. So zeigt beispielsweise der folgende Screenshot den neu angelegten Domänen-Administrator 'binsec':



Empfehlung

SMB-Signing sollte mittels Gruppenrichtlinie für alle IT-Systeme der Domäne aktiviert werden. Dabei werden die NTLM-Hashes von ihren Besitzern digital signiert, wodurch sie von einem Angreifer nicht länger zur Authentifikation an IT-Systemen weitergeleitet werden können. Zudem sollte der Domänen-Admin 'binsec' gelöscht werden.

4.2 Schwache Benutzerpasswörter

unmittelbarer Handlungsbedarf
Schaden: Kritisch
Eintrittswahrscheinlichkeit: Gering

Finding #2 **Nicht behoben**

Wie aus dem folgenden Screenshot entnommen werden kann, ist eine schwache Passwortrichtlinie für die Domäne 'Dubius' im Einsatz, wonach Benutzerpasswörter lediglich 7 Zeichen enthalten müssen:

```
Minimum password length: 7
Password history length: 5
Maximum password age: Not Set

Password Complexity Flags: 000000
    Domain Refuse Password Change: 0
    Domain Password Store Cleartext: 0
    Domain Password Lockout Admins: 0
    Domain Password No Clear Change: 0
    Domain Password No Anon Change: 0
    Domain Password Complex: 0

Minimum password age: None
Reset Account Lockout Counter: 30 minutes
Locked Account Duration: 30 minutes
Account Lockout Threshold: None
Forced Log off Time: Not Set
```

Zur Rekonstruktion von schwachen Passwörtern, wurden die Passworthashes aller Domänenaccounts am Domain Controller 10.247.97.31 als Administrator der Domäne 'Dubius' extrahiert. Die folgende Auflistung zeigt alle Benutzerpasswörter, die im zeitlichen Rahmen des Penetrationstests gebruteforced werden konnten:

Benutzername	Passwort	Anmerkung
Dubius\csimmons	Dubius2021!	Domänenadministrator
Dubius\pbaker	Chandler#1982	Domänenbenutzer
Dubius\rhobbes	Rylan_1234	Domänenbenutzer

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.

4.3 Unzureichendes Berechtigungsmanagement bei den Netzwerkverzeichnissen

unmittelbarer Handlungsbedarf
Schaden: Hoch
Eintrittswahrscheinlichkeit: Mittel

Finding #3 **Nicht behoben**

Die Benutzerkonten der Domäne 'Dubius' mit den Gruppenmitgliedschaften 'Domain Users' und 'dubius-payment' haben Lese- und Schreibzugriff auf die folgenden Netzwerkverzeichnisse:

```
[+] IP: 10.247.97.204:445      Name: ad.dubius-payment.com
        Disk                          Permissions     Comment
        ----                          -----------     -------
        c$                            READ ONLY
        home                          READ, WRITE

 [+] IP: 10.247.97.210:445      Name: unknown
        Disk                          Permissions     Comment
        ----                          -----------     -------
        Backup                        READ ONLY

[+] IP: 10.247.97.212:445      Name: srv01.dubius-payment.com
        Disk                          Permissions     Comment
        ----                          -----------     -------
        McAfee                        READ ONLY
        NETLOGON                      READ ONLY
        SYSVOL                        READ ONLY
```

Auf dem 'home'-Netzwerkverzeichnis von 10.247.97.204 konnten beispielsweise Zugangsdaten für den Domänenaccount 'Dubius\jpitts' aus zwischengespeicherten Firefoxprofilen extrahiert werden. Infolgedessen können unprivilegierte Domänenbenutzer nach dem aktuellen Stand ihre Benutzerrolle wechseln, indem sie sich als 'Dubius\jpitts' an den IT-Systemen und Diensten der Dubius Payment Ltd. anmelden:

```
ds@binsec ~/ $ssh jpitts@10.250.53.35
jpitts@10.250.53.35's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have mail.
Last login: Thu Jul 18 08:10:49 2019 from 10.20.1.74
jpitts@wiki:~$
```

Empfehlung

In Rücksprache mit Dubius Payment Ltd. sollten unprivilegierte Domänenbenutzer nur auf das Netzwerkverzeichnis '//10.247.97.204/home' zugreifen dürfen. Infolgedessen sollte das Berechtigungsmanagement intern überprüft und korrigiert werden.

Darüber hinaus fungiert das IT-System 10.247.97.204 als Fileserver aber auch als Domain Controller. Gemäß Security Best Practices sollte nur eine Funktion pro Server konfiguriert werden. Infolgedessen sollte der Fileserver auf einem dedizierten IT-System betrieben werden, um die Angriffsfläche am Domain Controller zu reduzieren.

4.4 Klartextübertragung von Authentifizierungsdaten

Handlungsbedarf
Schaden: Mittel
Eintrittswahrscheinlichkeit: Mittel

Finding #4 **Nicht behoben**

Die Benutzerdaten zur Authentifizierung werden bei den folgenden Diensten im Klartext übertragen, wodurch diese von einem Angreifer mitgeschnitten werden könnten:

Telnet (23/tcp)

- 10.247.97.56
- 10.247.97.57
- 10.247.97.58

HTTP (80/tcp)

- http://10.247.97.80
- http://10.247.97.81

Empfehlung

Die Webanwendungen sollten nur über HTTPS erreichbar sein und anstelle Telnet sollte ausschließlich SSH verwendet werden.

4.5 Informationssammlung über veraltete SNMP-Versionen

Hinweis
Schaden: Warnung
Eintrittswahrscheinlichkeit: Hoch

Finding #5 **Nicht behoben**

Über das Simple Network Management Protocol (SNMP) können Netzwerkelemente von einer zentralen Station aus überwacht und gesteuert werden. Jedoch sieht sowohl die SNMP-Version 'SNMPv1' als auch 'SNMPv2' keine Verschlüsselung der Daten vor. Weiterhin können über den Community-String 'public' via 'SNMPv1' und 'SNMPv2' Systeminformationen, wie z.B. IP-Adressen oder Routinginformationen, von folgenden IT-Systemen extrahiert werden:

- 10.247.97.174
- 10.247.97.201
- 10.247.97.190
- 10.247.97.235

Das nachfolgende Listing zeigt exemplarisch die Routingtabelle von 10.247.97.174:

```
[+] Try to connect to 10.247.97.174 using SNMPv1 and community 'public'


[*] Routing information:

  Destination           Next hop              Mask                  Metric
  0.0.0.0               10.247.97.1         0.0.0.0               1

[...]
```

Empfehlung

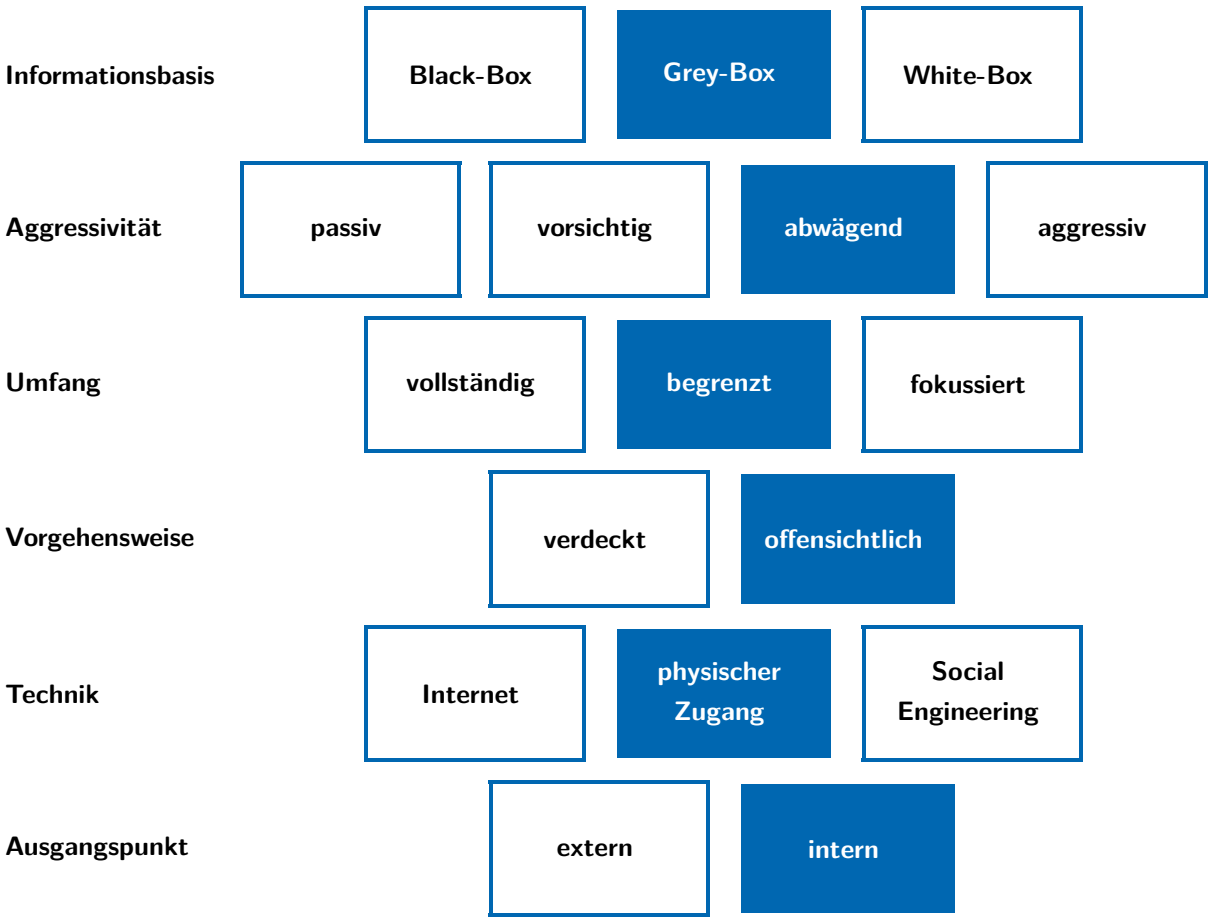
Die SNMP-Versionen 'SNMPv1' und 'SNMPv2' sollten deaktiviert und anstelle dessen 'SNMPv3' mit aktiver Verschlüsselung und Benutzerauthentifizierung eingesetzt werden.

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 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 Vorgehensweise bei einem Active Directory

Die Untersuchungsmethode der binsec GmbH orientiert sich bei einem Active Directory (AD) an den Bausteinen für IT-Grundschutz vom Bundesamt für Sicherheit in der Informationstechnik (BSI) und den CIS-Benchmarks (Center for Internet Security Benchmarks) zum Schutz von IT-Systemen und Daten vor Cyberangriffen. Üblicherweise erfolgt der Penetrationstest gegen ein AD vor Ort in den Räumlichkeiten des Auftraggebers, welcher einen physischen Anschluss ins lokale Netzwerk bereitstellt. Lediglich die Ausgangssituation bzw. die Angreifer-Perspektive für den Penetrationstest gegen ein AD kann variieren:

- Der Angreifer hat sich physischen Zugang zum Netzwerk verschafft und muss im ersten Schritt einen initialen Zugang zur Domäne erhalten. So können beispielsweise Angriffsvektoren wie Man-in-the-Middle-Angriffe, Password Spraying oder die Identifikation von Informationslücken genutzt werden, um Konten von Domänenbenutzern zu übernehmen.
- Der Angreifer konnte einen AD-Benutzer kompromittieren und initialen Zugriff auf das Active Directory erlangen (Assumed Breach). Diese Sichtweise ist vergleichbar mit einem unprivilegierten Domänenbenutzer, welcher seine Berechtigungen erweitern will. Hierzu dienen beispielsweise Schwachstellen wie die Ausnutzung von Fehlkonfigurationen sowie Berechtigungsfehler im AD und dessen Services, wie auch eine Datenanalyse von Netzwerkverzeichnissen.
- Der Angreifer hat Zugriff auf ein Administratorkonto der Domäne und verfügt über internes Wissen über die lokale IT-Infrastruktur (bspw. ehemaliger IT-Mitarbeiter). Als Domain-Admin können beispielsweise die Passwort Hashes sämtlicher Benutzer ausgelesen werden, um die Vergabe von schwachen Passwörtern zu identifizieren und die Wirksamkeit der Passwortrichtlinie zu überprüfen.

Zusammenfassend unterteilt sich der methodische Prüfungsansatz grob in die 3 folgenden Prüfphasen:

1. Identifikation von Schwachstellen (ohne Zugangsdaten)
   - OSINT-Analyse (Open Source Intelligence) wie die Abfrage von Zugangsdaten in Datenleaks
   - Manuelle und automatische AD-Enumerierung
   - Überprüfung auf den Einsatz veralteter Betriebssysteme und Software
   - Überprüfung ob Härtungsmaßnahmen zum Schutz vor Man-in-the-Middle-Angriffen vorhanden sind
   - Extraktion von Zugangsdaten und Passworthashes in Services
   - Kompromittierung von Benutzerkonten via Passwort-Spraying
2. Identifikation von Schwachstellen (mit Zugangsdaten)
   - Manuelle und automatische AD-Enumerierung
   - Extraktion von Zugangsdaten und Passworthashes in Services
   - Überprüfung des Berechtigungsmanagements beispielsweise bei Netzwerkverzeichnissen
   - Überprüfung der Härtungsmaßnahmen vom AD
3. Privilegienausweitung
   - Abhängigkeitsüberprüfung zu anderen Domänen
   - Auslesen lokaler Hashes und zwischengespeicherter Kennwörter

5.4 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:

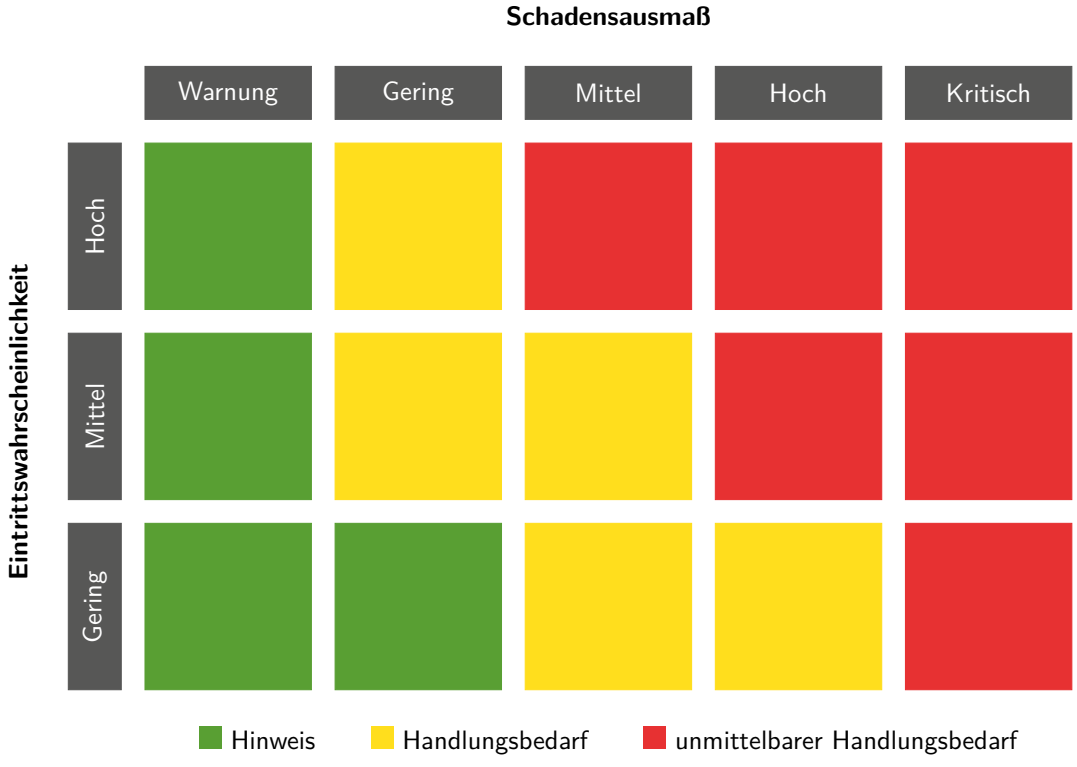
Eintrittswahrscheinlichkeit

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.



5.5 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