DEFENDERBOX
EINFACH.SCHNELL.CYBERSICHER.

XX.XX.2025

ERGEBNISBERICHT
PENTESTING

LOGO

Weitere Informationen erhalten Sie
unter: vertrieb@defenderbox.de
Telefon +49 2732 7652 088

Inhaltsverzeichnis

I. Kurze Zusammenfassung

A. Externe Angriffsfläche (Externe Schwachstellenanalyse)

Bei diesem externen Audit haben wir uns auf die Identifizierung von Schwachstellen in den externen Systemen des Kunden konzentriert, zu denen wichtige Domains und IP-Adressen gehören, die die Angriffsfläche des Unternehmens bilden. Diese Systeme wurden mit Nessus und NodeZero gründlich untersucht, um potenzielle Sicherheitsrisiken aufzudecken. Nachfolgend finden Sie eine Liste der Domains und IPs, die in die Bewertung einbezogen wurden. Die folgenden Ergebnisse basieren auf den Erkenntnissen aus diesen externen Systemen:

IP-Adresse	Domänenname
131.2.XXX.XXX	autodiscover.mustermann.de
	mail.mustermann.de
	mx.mustermann.de
181.69.XXX.XXX	prod.mustermann.de
	www.prod.mustermann.de
131.2.XXX.XXX	connect.mustermann.de
60.134.XXX.XX	mdm.mustermann.de
129.24.XXX.XXX	mustermann.de
131.2.XXX.XXX	transfer.mustermann.de
131.2.XXX.XXX	utm.mustermann.de

Die externe Prüfung ergab mehrere Möglichkeiten zur Verringerung der Anfälligkeit:

➢ **Kritisches Risiko:**

- **Erkennung der Protokolle SSL Version 2 und 3:** Der Remote-Dienst unterstützt SSL 2.0 und SSL 3.0, die beide kritische kryptografische Schwachstellen aufweisen, wie z. B. unsicheres Auffüllen mit CBC-Chiffren und anfällige Sitzungsneuaushandlung. Diese Schwachstellen ermöglichen es Angreifern, Man-in-the-Middle-Angriffe durchzuführen oder die Kommunikation zu entschlüsseln. Obwohl moderne SSL/TLS-Protokolle die Aushandlung stärkerer Versionen ermöglichen, sind viele Browser für Downgrade-Angriffe wie POODLE anfällig, so dass SSL 2.0 und 3.0 unbedingt vollständig deaktiviert werden sollten. Außerdem betrachten NIST und PCI DSS v3.1 SSL 3.0 oder eine andere SSL-Version nicht mehr als sicher für den Schutz sensibler Daten.
  Host: transfer.mustermann.de Port **990**

➢ **Hohes Risiko:**

- **Apache 2.4.x < 2.4.64 Mehrere Schwachstellen:** Der Remote-Apache-HTTP-Server ist veraltet (Version < 2.4.64) und von mehreren Schwachstellen betroffen, darunter Denial-of-Service (CVE-2025-49630), HTTP-Response-Splitting (CVE-2024-42516) und mehrere SSRF-bezogene Probleme (CVE-2024-43204, CVE-2024-43394) sowie eine Log-Injection-Schwachstelle in mod_ssl (CVE-2024-47252). Um diese Sicherheitsrisiken zu beheben, wird ein Upgrade auf Version 2.4.64 empfohlen.
  Host: prod.mustermann.de Port **443**

- **OpenSSL Heartbeat Informationsoffenlegung (Heartbleed):** Der entfernte Dienst ist anfällig für einen Out-of-bounds-Read-Fehler, der durch eine speziell gestaltete TLS-Heartbeat-Nachricht (RFC 6520) ausgelöst wird. Diese Schwachstelle könnte es einem Angreifer ermöglichen, auf bis zu 64 KB des Serverspeichers zuzugreifen und

möglicherweise vertrauliche Informationen wie Passwörter und private Schlüssel offenzulegen.
Host: transfer.mustermann.de Port **990**

➢ Mittleres Risiko:

- **SSL-Zertifikat nicht vertrauenswürdig:** Das X.509-Zertifikat des Servers ist aufgrund einer unterbrochenen Vertrauenskette nicht vertrauenswürdig. Dies kann durch ein nicht erkanntes oder selbstsigniertes Zertifikat, fehlende Zwischenzertifikate, abgelaufene oder noch nicht gültige Zertifikate oder nicht überprüfbare digitale Signaturen verursacht werden. Auf öffentlich zugänglichen Systemen untergraben solche Probleme die SSL/TLS-Sicherheit und erhöhen das Risiko von Man-in-the-Middle-Angriffen.
  Host: connect.mustermann.de Port **443**, **1194** und **80**

- **Selbstsigniertes SSL-Zertifikat:** Die X.509-Zertifikatskette für diesen Dienst ist nicht von einer vertrauenswürdigen Zertifizierungsstelle signiert. Bei öffentlich zugänglichen Systemen untergräbt dies die SSL-Sicherheit, da Angreifer potenziell Man-in-the-Middle-Angriffe durchführen können. Beachten Sie, dass diese Überprüfung Zertifikate ausschließt, die von unbekannten, aber nicht selbstsignierten Stellen signiert wurden.
  Host: connect.mustermann.de Port **443**, **1194** und **80**

- **HSTS fehlt auf HTTPS-Server (RFC 6797):** Der Remote-Webserver erzwingt nicht HTTP Strict Transport Security (HSTS) gemäß RFC 6797. HSTS ist ein optionaler Antwort-Header, der Browser anweist, für die Kommunikation ausschließlich HTTPS zu verwenden. Ohne HSTS ist der Server anfällig für Downgrade-Angriffe, SSL-Stripping-Man-in-the-Middle-Angriffe und einen verminderten Schutz vor Cookie-Hijacking.
  Hosts: mail.Mustermann.de, autodiscover.Mustermann.de und Mustermann.de Port **443** sowie prod.mustermann.de und www.prod.mustermann.de Ports **443** und **8443**

- **HTTP TRACE / TRACK-Methoden erlaubt:** Der Remote-Webserver unterstützt die TRACE- und/oder TRACK-Methoden, bei denen es sich um HTTP-Methoden handelt, die in erster Linie für die Fehlerbehebung bei Webserververbindungen vorgesehen sind. Die Aktivierung dieser Methoden kann jedoch Sicherheitsrisiken mit sich bringen und sollte deaktiviert werden, sofern sie nicht ausdrücklich erforderlich sind.
  Hosts: mx.mustermann.de, mail.mustermann.de und autodiscover.mustermann.de Port **443**

- **TLS-Version 1.0 Protokollerkennung:** Der Remote-Dienst akzeptiert Verbindungen mit TLS 1.0, einem veralteten Protokoll mit bekannten kryptografischen Schwachstellen. Moderne Browser und Anbieter unterstützen TLS 1.0 nicht mehr vollständig, und Compliance-Standards wie PCI DSS v3.2 verlangen, dass es deaktiviert wird. Es wird empfohlen, TLS 1.2 oder höher zu verwenden, um eine sichere und kompatible Kommunikation zu gewährleisten.
  Host: connect.mustermann.de Port **443**, **1194** und **80**

- **TLS-Version 1.1 Veraltetes Protokoll:** Der Remote-Dienst erlaubt Verbindungen mit TLS 1.1, das moderne und empfohlene Verschlüsselungssuiten, einschließlich authentifizierter Verschlüsselungsmodi wie GCM, nicht unterstützt. Es sollte TLS 1.2 oder höher verwendet werden, da ältere Versionen möglicherweise nicht mit aktuellen Browsern und Anbietern kompatibel sind.

Host: connect.mustermann.de Port **443**, **1194** und **80**

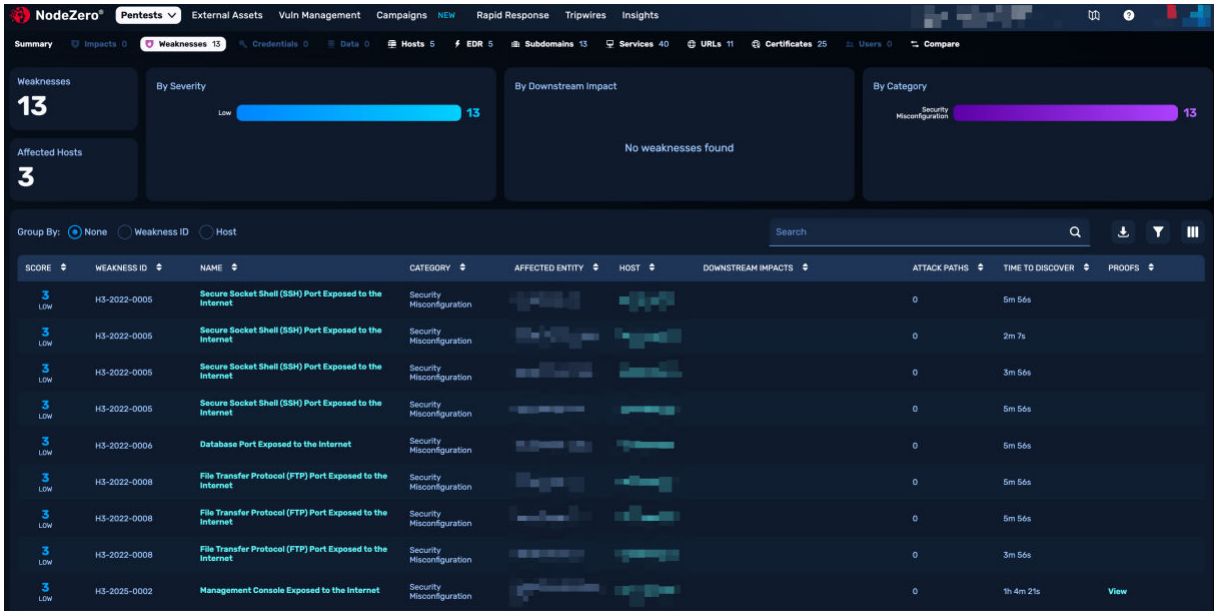
➢ Geringes Risiko:

- **ICMP-Zeitstempelanforderung Offenlegung des Remote-Datums:** Der Remote-Host antwortet auf ICMP-Zeitstempelanforderungen und gibt dabei sein Systemdatum preis. Diese Informationen können einem nicht authentifizierten Angreifer helfen, zeitbasierte Authentifizierungsmechanismen zu umgehen. Beachten Sie, dass Windows Vista, 7 und Server 2008 absichtlich ungenaue Zeitstempel zurückgeben, die in der Regel innerhalb von 1000 Sekunden von der tatsächlichen Zeit abweichen.
  Host: mustermann.de Port **0**

- **SSH-Algorithmen mit schwacher Schlüsselaustauschfunktion aktiviert:** Der Remote-SSH-Server erlaubt Schlüsselaustauschalgorithmen, die gemäß RFC9142 als schwach gelten, darunter verschiedene Diffie-Hellman- und SHA-1-basierte Methoden. Die Konfiguration des Servers lässt diese Algorithmen zwar zu, diese Überprüfung bewertet jedoch nicht die zugrunde liegende Softwareversion auf zusätzliche Schwachstellen.
  Hosts: prod.mustermann.de und www.prod.mustermann.de Port **22**

Externe Schwachstelle (externes Pentesting)

Der Scan identifizierte 13 Schwachstellen mit geringem Schweregrad auf 3 betroffenen Hosts, die alle mit einer falschen Sicherheitskonfiguration zusammenhängen. Zu den erkannten Problemen gehören exponierte SSH-Ports auf 131.2.XXX.XXX und 60.134.XXX.XXX (Port **22);** offene Datenbank- und FTP-Ports auf 131.2.XXX.XXX (Ports **3306** und **21)**, 60.134.XXX.XXX und 131.2.XXX.XXX (Port **21)**; über das Internet zugängliche Verwaltungskonsolen auf 181.69.XXX.XXX (Port **15672)** und 60.134.XXX.XXX (Port **8443)** sowie Probleme mit SSL/TLS-Zertifikaten auf 131.2.XXX.XXX und 60.134.XXX.XXX (Port **443)**. Diese Fehlkonfigurationen vergrößern die Angriffsfläche von außen und sollten durch Schließen unnötiger Ports, Begrenzung der Konsolenfreigabe und Erneuerung oder Austausch von Zertifikaten behoben werden.



B. Darknet-Recherche

Verschiedene Plattformen wurden verwendet, um exponierte E-Mail-Adressen und Zugangspunkte zu identifizieren, die online gefunden wurden. Es ist wichtig zu überprüfen, ob diese noch aktiv sind und verwendet werden.

Die folgenden geleakten E-Mails sowie die damit verbundenen Sicherheitsverletzungen und kompromittierten Daten wurden identifiziert:

E-Mail-Adresse	**Gefundene Sicherheitsverletzungen**	**Kompromittierte Daten**
max.mustermann@mustermann.de	2	E-Mail-Adressen, Berufsbezeichnungen, Namen, Telefonnummern, Anschriften und Social-Media-Profile
erika@mustermann.de	1	E-Mail-Adressen, Namen, Telefonnummern, Anschriften und Social-Media-Profile
info@mustermann.de	6	E-Mail-Adressen, Passwörter, Arbeitgeber, Bildungsniveau, Berufsbezeichnungen, Namen, Telefonnummern, Anschriften, geografische Standorte und Social-Media-Profile

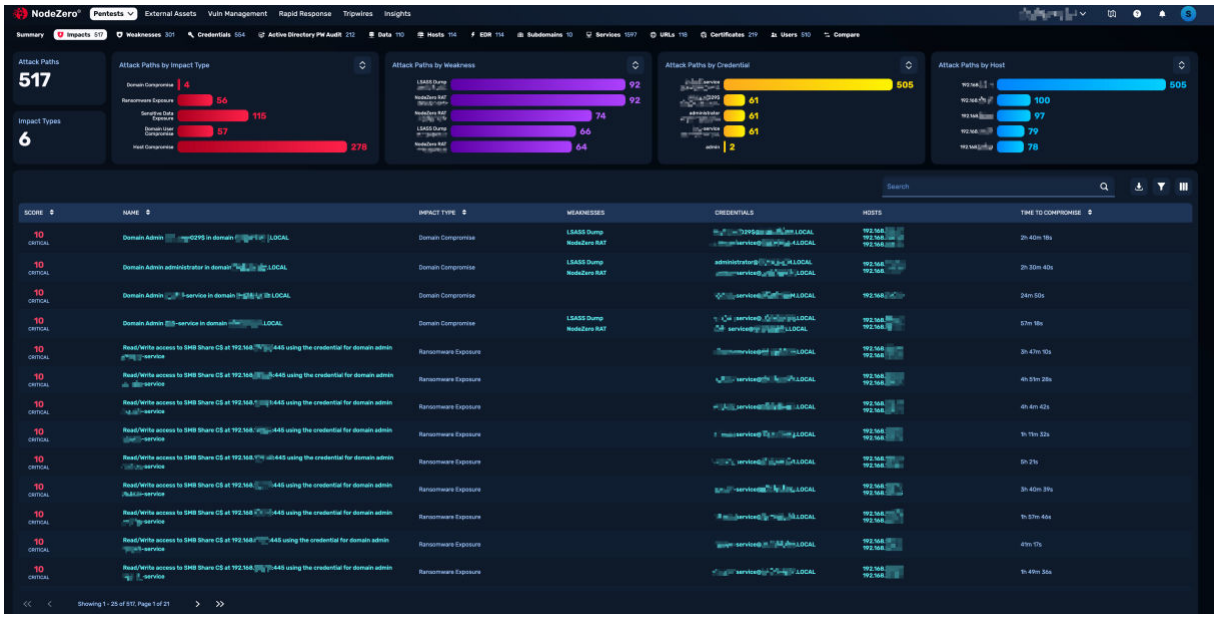
Weitere Details finden Sie im Anhang.

C. Interne Angreifbarkeit (internes Pentesting)

1. Automatischer Scan NodeZero – ohne Domain-Anmeldung

Ausgewählt nach Auswirkungen

Die aufgeführten Schwachstellen umfassen 214 kritische Schwachstellen (Schweregrad 10 und 9) und 3 Schwachstellen mit hohem Schweregrad (Schweregrad 8,4 und 7,5), was zu 517 unterschiedlichen Angriffspfaden führt. Diese Angriffspfade führen zu verschiedenen Arten von Auswirkungen, darunter 4 Fälle von **Domain-Kompromittierung,** 278 Fälle von **Host-Kompromittierung,** 56 Fälle von **Ransomware-Exposition,** 115 Fälle von **Exposition sensibler Daten** und 57 Fälle von **Domain-Benutzer-Kompromittierung.**



Diese Schwachstellen unterstreichen die dringende Notwendigkeit von Abhilfemaßnahmen, um schwerwiegende Auswirkungen im gesamten Netzwerk zu verhindern. Dazu gehören:
Mehrfacher Kompromittierung von Domänenadministratoren in der Domäne MUSTERMANN.LOCAL (5 Server):

- **Bewertung:** 10 (kritisch)
- **Art der Auswirkung:** Kompromittierung der Domäne
- **Hosts:** 192.168.XX.XX (mustermann037.mustermann.local), 192.168.XXX.XX (Mustermann038.mustermann.local), 192.168.XXX.XX (Mustermann029.mustermann.local), 192.168.XXX.XX (Mustermann050.mustermann.local) und 192.168.XXX.XX (Mustermann051.mustermann.local)
- **Kompromittierte Domain-Administratorkonten:** administrator, swtest-service, user-service und mustermann029$
- **Auswirkungen:**
  - ➢ Vollständige Kompromittierung der Domäne. Alle Hosts, Benutzerkonten, Infrastrukturen und Anwendungen, die mit MUSTERMANN.LOCAL verbunden sind, sollten als kompromittiert betrachtet werden. Die Angreifer haben sich über LSASS-Dumping und NodeZero RAT Domänenadministrator-Anmeldedaten verschafft und konnten so die vollständige Kontrolle über Active Directory, laterale Bewegungen,

Persistenz und Zugriff auf sensible Systeme und Daten erlangen.

Lese-/Schreibzugriff auf SMB-Freigabe C$ unter Verwendung der Anmeldedaten für den Domänenadministrator swtest-service (13 Server):

- **Bewertung:** 10 (kritisch)
- **Auswirkungstyp:** Ransomware-Exposition
- **Hosts:** 192.168.XXX.XX (Mustermann196.Mustermann.local), Domänencontroller 192.168.XXX.XX (Mustermann051.Mustermann.local), 192.168.XXX.XX6 (Mustermann057.Mustermann.local), 192.168.XXX.XX (Mustermann031.Mustermann.local), 192.168.XXX.XX (Mustermann191.Mustermann.local), 192.168.XXX.XX (Mustermann042.Mustermann.local), 192.168.XXX.XX (Mustermann195.Mustermann.local), 192.168.XXX.XX (Mustermann059.Mustermann.local), 192.168.XXX.XX (Mustermann005.Mustermann.local), 192.168.XXX.XX (Mustermann004.Mustermann.local), 192.168.XXX.XX (Mustermann041.Mustermann.local), 192.168.XXX.XX (Mustermann016.Mustermann.local) und 192.168.XXX.XX (Mustermann025.Mustermann.local) Port **445**
- **Kompromittierte Anmeldedaten:** Domänenadministrator **swtest-service** (beteiligt an über 500 Angriffspfaden).
- **Auswirkungen:**
  - Angreifer mit Domänenadministratorrechten und Schreibzugriff auf SMB-Verwaltungsfreigaben (C$) können Ransomware-Payloads auf mehreren kritischen Systemen bereitstellen und ausführen. Dies würde eine Massenverschlüsselung geschäftskritischer Daten ermöglichen, was zu weitreichenden Betriebsstörungen und potenziellen Lösegeldforderungen führen würde.

Lese-/Schreibzugriff auf SMB-Freigabe ADMIN$ unter Verwendung der Anmeldedaten für den Domänenadministrator swtest-service (17 Server):

- **Bewertung:** 10 (kritisch)
- **Art der Auswirkung:** Ransomware-Gefährdung
- **Hosts:** 192.168.XXX.XX (Mustermann004.Mustermann.local), 192.168.XXX.XX (Mustermann051.Mustermann.local), 192.168.XXX.XX (Mustermann059.Mustermann.local), 192.168.XXX.XX (Mustermann025.Mustermann.local), 192.168.XXX.XX (Mustermann189.Mustermann.local), 192.168.XXX.XX (Mustermann042.Mustermann.local), 192.168.XXX.XX (Mustermann196.Mustermann.local), 192.168.XXX.XX (Mustermann005.Mustermann.local), 192.168.XXX.XX (Mustermann028.Mustermann.local), 192.168.XXX.XX (Mustermann195.Mustermann.local), 192.168.XXX.XX (Mustermann003.Mustermann.local), 192.168.XXX.XX (Mustermann191.Mustermann.local), 192.168.XXX.XX (Mustermann057.Mustermann.local), 192.168.XXX.XX (Mustermann041.Mustermann.local), 192.168.XXX.XX (Mustermann031.Mustermann.local), 192.168.XXX.XX (Mustermann197.Mustermann.local), 192.168.XXX.XX

(Mustermann016.Mustermann.local) und 192.168.XXX.X (Mustermann008.Mustermann.local) Port **445**

- **Kompromittierte Anmeldedaten:** Domänenadministrator **swtest-service** (beteiligt an über 500 Angriffspfaden).
- **Auswirkungen:**
  - Angreifer mit Domänenadministratorrechten und Schreibzugriff auf SMB-Verwaltungsfreigaben (ADMIN$) können Ransomware-Payloads auf mehrere kritische Systeme remote übertragen und ausführen. Eine erfolgreiche Ausnutzung würde die Massenverschlüsselung geschäftskritischer Daten auf Servern und Domänencontrollern ermöglichen, was zu schwerwiegenden Betriebsstörungen und Lösegeldforderungen führen würde.

Sensible Dateien auf SMB-Freigabe C$, auf die mit den Anmeldedaten für den Domänenadministrator swtest-service (12 Server) zugegriffen werden kann:

- **Bewertung:** 10 (kritisch)
- **Art der Auswirkung:** Offenlegung sensibler Daten
- **Hosts:** 192.168.XXX.XX (Mustermann196.Mustermann.local), 192.168.XXX.XX (Mustermann057.Mustermann.local), 192.168.XXX.XX (Mustermann031.Mustermann.local), 192.168.XXX.XX (Mustermann191.Mustermann.local), 192.168.XXX.XX (Mustermann042.Mustermann.local), 192.168.XXX.XX (Mustermann195.Mustermann.local), 192.168.XXX.XX (Mustermann059.Mustermann.local), 192.168.XXX.XX (Mustermann005.Mustermann.local), 192.168.XXX.XX (Mustermann004.Mustermann.local), 192.168.XXX.XX (Mustermann041.Mustermann.local), 192.168.XXX.XX (Mustermann016.Mustermann.local) und 192.168.XXX.XX (Mustermann025.Mustermann.local) **Port 445**
- **Kompromittierte Anmeldedaten:** Domänenadministrator **swtest-service** (beteiligt an über 500 Angriffspfaden).
- **Auswirkungen:**
  - Angreifer mit Domänenadministratorrechten und Lesezugriff auf sensible Dateien auf SMB-Verwaltungsfreigaben (C$) können kritische Geschäftsdaten, darunter personenbezogene Daten, Finanzunterlagen und zwischengespeicherte Anmeldedaten, exfiltrieren. Diese Informationen können für weitere Kompromittierungen, Finanzbetrug, Verstöße gegen Vorschriften und langfristige Persistenz innerhalb der Umgebung genutzt werden.

Personenbezogene Daten/PCI auf SMB-Freigabe D$, auf die mit den Anmeldedaten für den Domänenadministrator swtest-service zugegriffen wird:

- **Bewertung:** 10 (kritisch)
- **Auswirkungstyp:** Offenlegung sensibler Daten
- **Hosts:** 192.168.XXX.XX (Mustermann005.Mustermann.local) und 192.168.XXX.XX (Mustermann051.Mustermann.local, Domänencontroller) **Port 445**
- **Kompromittierte Anmeldedaten:** Domänenadministrator **swtest-service** (beteiligt an über 500 Angriffspfaden).
- **Auswirkungen:**
  - Angreifer mit Domänenadministratorrechten und Zugriff auf sensible Dateien auf SMB-Verwaltungsfreigaben (D$) können personenbezogene Daten (PII), Finanzkontodaten (PCI), zwischengespeicherte Anmeldedaten und andere wichtige

Geschäftsinformationen exfiltrieren. Diese Gefährdung kann zu groß angelegten Identitätsdiebstählen, Finanzbetrug, Verstößen gegen gesetzliche Vorschriften (DSGVO/PCI-DSS) führen und weitere Kompromittierungen in der gesamten Umgebung ermöglichen.

Mehrere Domänenadministratoren in der Domäne MUSTERMANN.LOCAL (5 Server):

- **Bewertung:** 9,8 (kritisch)
- **Auswirkungstyp:** Kompromittierung von Domänenbenutzern
- **Hosts:** Domänencontroller 192.168.XXX.XX (Mustermann050.Mustermann.local) und 192.168.XXX.XX (Mustermann051.Mustermann.local), 192.168.XXX.XX (Mustermann029.Mustermann.local), 192.168.XXX.XX (Mustermann038.Mustermann.local) und 192.168.XXX.XX (Mustermann037.Mustermann.local)
- **Kompromittierte Anmeldedaten:** swtest-service, user-service, administrator und Mustermann029$
- **Auswirkungen:**
  - Mehrere Domänenadministratorkonten wurden kompromittiert, wodurch Angreifer uneingeschränkte Kontrolle über Active Directory und alle mit der Domäne verbundenen Systeme erhielten. Dies ermöglicht das Auslesen von Anmeldedaten, die Persistenz durch den Einsatz von RATs, laterale Bewegungen, die Ausweitung von Berechtigungen und die vollständige Übernahme der Umgebung. Die Kompromittierung mehrerer privilegierter Konten erhöht die Geschwindigkeit und Tiefe potenzieller Angreiferaktionen erheblich.

Mehrere kompromittierte Domänenbenutzer in MUSTERMANN.LOCAL (53 Server):

- **Bewertung:** 9 (kritisch)
- **Art der Auswirkung:** Kompromittierung von Domänenbenutzern
- **Hosts:** 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX usw.
- **Gefährdete Anmeldedaten:** Mustermann194, gMustermann, Mustermann022, jraulf, sdetzner, nhecker, jrinke, montage5, mhuster, mhanel, Mustermann010, mmichl, mberghoff, Mustermann189, tbielaszewski, ukanehl, fholthoff, Mustermann043, mheuwinkel, nrohe, montage7 usw.
- **Auswirkungen:**
  - Die Anmeldedaten mehrerer Domänenbenutzer wurden kompromittiert, wodurch Angreifer Zugriff auf sensible Systeme und Ressourcen erhielten. Dies ermöglicht laterale Bewegungen, die Ausweitung von Berechtigungen und die potenzielle Ausnutzung kritischer Geschäftsdaten auf mehreren Hosts.

SMB-Dienst, auf den mit den Anmeldedaten des Domänenadministrators Mustermann029$ zugegriffen wurde (46 Server):

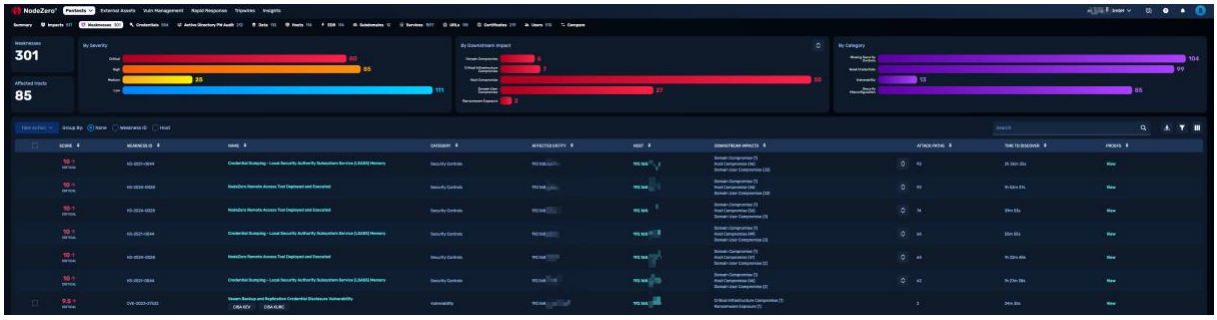
- **Bewertung:** 9,8 (kritisch)
- **Art der Auswirkung:** Kompromittierung des Hosts
- **Hosts:** 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX2, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX,

192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX, 192.168.XXX.XX usw. Port **445**

- **Gefährdete Anmeldedaten:** Mustermann029$ und swtest-service
- **Auswirkungen:**
  - ➢ Auf mehrere SMB-Hosts wurde mit zwei Domänenadministrator-Anmeldedaten zugegriffen, wodurch Angreifern die potenzielle vollständige Kontrolle über diese Systeme ermöglicht wurde und sie sich seitlich bewegen, ihre Berechtigungen erweitern und auf sensible Daten zugreifen konnten.

Ausgewählt aufgrund von Schwachstellen

Die Software NodeZero wurde auf der **DEFENDERBOX** ausgeführt und deckte 301 Schwachstellen auf, von denen 80 als kritisch, 85 als hoch, 25 als mittel und 111 als gering eingestuft wurden.



a) Lücken mit kritischen Auswirkungen

Credential Dumping – Local Security Authority Subsystem Service (LSASS) Speicher (6 Server):

- **Bewertung:** 10 - 9 (kritisch)
- **Sicherheitslücke:** Der Local Security Authority Subsystem Service (LSASS) speichert Anmeldedaten für aktive Windows-Sitzungen im Arbeitsspeicher. Angreifer mit Administratorrechten können Anmeldedaten mit Tools wie Mimikatz, procdump oder LaZagne aus dem LSASS-Speicher extrahieren.
- **Hosts:** 192.168.XXX.XX (Mustermann029.Mustermann.local), 192.168.XXX.XX (Mustermann037.Mustermann.local), 192.168.XXX.XX (Mustermann038.Mustermann.local), 192.168.XXX.XX (Mustermann040.Mustermann.local), 192.168.XXX.XX (Mustermann030.Mustermann.local) und 192.168.XXX.XX (Mustermann043.Mustermann.local)
- **Auswirkungen:**
  - ➢ Angreifer können Klartext-Anmeldedaten oder NTLM-Hashes abgreifen, wodurch sie sich als Benutzer anmelden, sich lateral über Active Directory bewegen und die Wiederverwendung von Passwörtern nutzen können, um weitere Hosts zu kompromittieren. Diese Schwachstelle trug zur Gefährdung durch Ransomware und zur Offenlegung sensibler Daten auf mehreren Hosts bei.

NodeZero-Fernzugriffstool bereitgestellt und ausgeführt (6 Server):

- **Bewertung:** 10 – 9,2 (kritisch)
- **Sicherheitslücke:** NodeZero RAT wurde auf Zielhosts entweder unter Ausnutzung von Sicherheitslücken oder mithilfe privilegierter Anmeldedaten bereitgestellt und ausgeführt. Dadurch können Angreifer Aktionen wie den Diebstahl von Anmeldedaten, die Kompromittierung von Hosts, laterale Bewegungen, die Bereitstellung von Ransomware und die Exfiltration von Daten durchführen.
- **Hosts:** 192.168.XXX.XX (Mustermann029.Mustermann.local), 192.168.XXX.XX (Mustermann037.Mustermann.local), 192.168.XXX.XX (Mustermann038.Mustermann.local), 192.168.XXX.XX (Mustermann040.Mustermann.local), 192.168.XXX.XX (Mustermann030.Mustermann.local) und 192.168.XXX.XX (Mustermann043.Mustermann.local)
- **Auswirkungen:**
  - Angreifer erlangten Fernzugriff auf 14 Hosts, wodurch sie Anmeldedaten stehlen, Domänen kompromittieren, Mandanten kompromittieren, Hosts übernehmen, Ransomware einsetzen und sich quer durch das Netzwerk bewegen konnten.

Sicherheitslücke bei der Offenlegung von Anmeldedaten in Swtest Backup and Replication:

- **Bewertung:** 9,5 (kritisch)
- **Sicherheitslücke:** Eine unsachgemäße Zugriffsprüfung in Swtest Backup and Replication (alle Versionen vor 11.0.1.1261 P20230227 und 12.0.0.1420 P20230223) ermöglicht es nicht authentifizierten Angreifern, auf Endpunkte des Backup-Servers zuzugreifen und Klartext-Anmeldedaten offenzulegen. Dies ist eine von der CISA bekannte, ausgenutzte Sicherheitslücke, die bekanntermaßen in Ransomware-Kampagnen verwendet wird.
- **Host:** 192.168.XXX.XX (Mustermann038.Mustermann.local) Port **9401**
- **Auswirkungen:**
  - Gefährdung kritischer Infrastrukturen mit Auswirkungen auf den MC-NMF-Dienst
  - Ransomware-Exposition mit Auswirkungen auf den MC-NMF-Dienst
  - Angreifer können sich unbefugten Zugriff auf die Remote-Backup-Infrastruktur von Swtest verschaffen, was möglicherweise zu Diebstahl von Anmeldedaten, lateraler Bewegung und Einsatz von Ransomware führen kann

Schwache oder standardmäßige Anmeldedaten – SNMP (6 Server):

- **Bewertung:** 9,5 (kritisch)
- **Sicherheitslücke:** Schwache oder standardmäßige SNMP-Community-Zeichenfolge (anonym) ermöglicht Angreifern den unbefugten Zugriff auf Netzwerkgeräte. Dies kann mithilfe automatisierter Tools oder manueller Ermittlung ausgenutzt werden, um auf Gerätekonfigurationen, laufende Prozesse und aktive Verbindungen zuzugreifen und möglicherweise den Betrieb neu zu konfigurieren oder zu stören.
- **Hosts und Anmeldedaten:** 192.168.XXX.XX (5406rzl2 vertrieb), 192.168.XXX.XX (2510g-48 serverraum), 192.168.XXX.XX (coreswitch), 192.168.XXX.XX (ke-m), 192.168.XXX.XX (ke-s) und 192.168.XXX.XX (hp-2530-8g labor) (**anonym)**
- **Auswirkungen:**
  - Gefährdung kritischer Infrastrukturen auf betroffenen Hosts
  - Mögliche unbefugte Sichtbarkeit und Kontrolle über Netzwerkgeräte
  - Mögliche Störung des Netzwerkbetriebs je nach Zugriffsebene

Apache Solr – Sicherheitslücke beim Lesen beliebiger Dateien:

- **Bewertung:** 9,4 (kritisch)
- **Sicherheitslücke:** Apache Solr ermöglicht es nicht authentifizierten Angreifern, beliebige Dateien zu lesen. Betroffen sind Versionen vor 9.4 und 10.0, wodurch vollständiger Zugriff auf alle auf dem Solr-Server gehosteten Daten möglich ist.
- **Host:** 192.168.XXX.XX (Mustermann041.Mustermann.local) Port **8983**
- **Auswirkungen:**
  - Unbefugter Zugriff auf alle Daten auf dem Solr-Server
  - Mögliche Offenlegung sensibler Informationen
  - Könnte als Einstiegspunkt für weitere Angriffe dienen

Credential Dumping – Security Account Manager (SAM)-Datenbank (16 Server):

- **Bewertung:** 9,2 (kritisch)
- **Sicherheitslücke:** Die SAM-Datenbank auf Windows-Hosts speichert lokale Benutzeranmeldedaten als NTLM-Hashes. Angreifer mit Administratorrechten können diese Hashes mit Tools wie Mimikatz oder Impacket aus der Registrierung, dem Speicher oder Sicherungsdateien extrahieren.
- **Hosts:** 192.168.XXX.XX (Mustermann043.Mustermann.local), 192.168.XXX.XX (Mustermann030.Mustermann.local), 192.168.XXX.XX (Mustermann037.Mustermann.local), 192.168.XXX.XX (Mustermann019.Mustermann.local), 192.168.XXX.XX (Mustermann038.Mustermann.local), 192.168.XXX.XX (Mustermann193.Mustermann.local), 192.168.XXX.XX (Mustermann201.Mustermann.local), 192.168.XXX.XX (Mustermann196.Mustermann.local), 192.168.XXX.XX (Mustermann195.Mustermann.local), 192.168.XXX.XX (Mustermann229.Mustermann.local), 192.168.XXX.XX (Mustermann194.Mustermann.local), 192.168.XXX.XX (Mustermann189.Mustermann.local), 192.168.XXX.XX (Mustermann188.Mustermann.local), 192.168.XXX.XX (Mustermann937.Mustermann.local), 192.168.XXX.XX (Mustermann136.Mustermann.local) und 192.168.XXX.XX (Mustermann191.Mustermann.local)
- **Auswirkungen:**
  - Angreifer können sich als beliebiger lokaler Benutzer anmelden, Pass-the-Hash-Angriffe durchführen und sich lateral durch die Umgebung bewegen, um auf weitere Systeme und sensible Daten zuzugreifen.

Wiederverwendung von Anmeldedaten – lokale Windows-Administratorkonten (25 Server):

- **Bewertung:** 9,2 (kritisch)
- **Sicherheitslücke:** Die Anmeldedaten eines lokalen Administrators (Administrator) wurden auf mehreren Windows-Hosts wiederverwendet, sodass Angreifer mit erhöhten Berechtigungen auf andere Computer zugreifen konnten.
- **Hosts und Anmeldedaten:** 192.168.XXX.XX (Mustermann016.Mustermann.local), 192.168.150.2 (Mustermann054.Mustermann.local), 192.168.XXX.XX (Mustermann023.Mustermann.local), 192.168.XXX.XX (Mustermann009.Mustermann.local), 192.168.XXX.XX (Mustermann025.Mustermann.local), 192.168.XXX.XX (Mustermann056.Mustermann.local), 192.168.XXX.XX

(Mustermann002.Mustermann.local), 192.168.XXX.XX
(Mustermann040.Mustermann.local), 192.168.XXX.XX
(Mustermann017.Mustermann.local), 192.168.XXX.XX
(Mustermann042.Mustermann.local), 192.168.XXX.XX
(Mustermann027.Mustermann.local), 192.168.XXX.XX
(Mustermann041.Mustermann.local), 192.168.XXX.XX
(Mustermann055.Mustermann.local), 192.168.XXX.XX
(Mustermann010.Mustermann.local), 192.168.XXX.XX
(Mustermann019.Mustermann.local), 192.168.XXX.XX
(Mustermann059.Mustermann.local), 192.168.XXX.XX
(Mustermann006.Mustermann.local), 192.168.XXX.XX
(Mustermann008.Mustermann.local), 192.168.XXX.XX
(Mustermann022.Mustermann.local), 192.168.XXX.XX
(Mustermann036.Mustermann.local), 192.168.XXX.XX
(Mustermann005.Mustermann.local), 192.168.XXX.XX
(Mustermann031.Mustermann.local), 192.168.XXX.XX
(Mustermann032.Mustermann.local), 192.168.XXX.XX
(Mustermann014.Mustermann.local) und 192.168.XXX.XX
(Mustermann029.Mustermann.local) (**Administrator)**

- **Auswirkungen:**
  - Angreifer können sich lateral durch die Umgebung bewegen, mehrere Hosts mit einem einzigen Anmeldezugang vollständig kompromittieren und auf sensible Daten auf den betroffenen Rechnern zugreifen.

D. Empfohlene Maßnahmen

1. Beseitigung der Schwachstellen

Die Beseitigung der Schwachstellen ist aus den detaillierten Berichten weitgehend ersichtlich. Bei Bedarf unterstützen wir Sie gerne weiter.

2. Zukünftige Reduzierung der Angriffsfläche

Zur zukünftigen Reduzierung empfehlen wir folgende Maßnahme(n) im Bereich Cybersicherheit:

- Wöchentliche automatische interne und externe Scans, um die sich ständig verändernde IT-Infrastruktur so regelmäßig wie möglich zu sichern.

Anhang

II. Vereinbarter Umfang des Tests

In der Vorbereitungsphase wurde vereinbart, dass der Test in der ersten Durchführung mehrere Teile umfassen soll:

- Überprüfung der Anfälligkeit von außen
    - Scan mit dem Tool „nessus" zur Erkennung von Schwachstellen
- Verfügbarkeit kritischer Informationen im Internet
    - Erfassung von Konten usw.
- Überprüfung der Schwachstellen von innen mit automatischer Erkennung
    - Scan mit NodeZero von horizon3.ai
- Empfehlung für Maßnahmen
    - Beseitigung der Schwachstellen
    - Reduzierung der Angriffsfläche in Zukunft

Die Ergebnisse werden in einer Zusammenfassung mit einem detaillierten Anhang zusammengestellt und dem Kunden übergeben.

Dies erfolgt in mehreren Schritten:

- Vorbereitende Informationsbeschaffung
- Remote-Implementierung auf Basis der gewonnenen Erkenntnisse
- Implementierung vor Ort entsprechend dem Umfang
- Zusammenstellung der gefundenen Schwachstellen und Angriffsmöglichkeiten
- Erstellung der Berichte