



Prüfbericht IT-Sicherheit

Muster GmbH · Steuerberatungskanzlei

Erstprüfung vom 25.08.2026

Perspektiven: Extern, WLAN, Intern

Vertraulich – nur für den Auftraggeber

Beispielbericht mit frei erfundenen Daten

1 Management-Zusammenfassung

Gesamtbewertung: Rot – dringender Handlungsbedarf. Es gibt kritische oder hohe Funde. Diese sollten innerhalb weniger Tage behoben werden.

Wir haben das Netz der Muster GmbH (Steuerberatungskanzlei, 15 Arbeitsplätze) am 25.08.2026 aus drei Perspektiven geprüft und 9 Funde festgestellt. Ein Standort, Internet über einen Business-Router mit integrierter Firewall, ein Gäste-WLAN, ein Fileserver, ein Multifunktionsdrucker.

Schweregrad	Anzahl
Kritisch	1
Hoch	3
Mittel	3
Niedrig	2

Die drei wichtigsten Punkte

1. Fernwartungszugang (RDP) ist direkt aus dem Internet erreichbar
2. Firewall-Firmware veraltet, bekannte Sicherheitslücke vorhanden
3. Fileserver-Freigabe für alle Mitarbeiter mit Schreibrechten, enthält Mandantendaten

Empfehlung

Kritische und hohe Funde innerhalb von zwei Wochen beheben und anschließend einen Nachtest durchführen lassen. Die Reihenfolge ergibt sich aus dem Maßnahmenplan in Kapitel 5.

Schweregrade

Kritisch: sofort handeln, Angriff jederzeit möglich. **Hoch:** innerhalb weniger Tage beheben. **Mittel:** in den nächsten Wochen beheben. **Niedrig:** bei der nächsten Wartung erledigen.

2 Prüfumfang und Vorgehen

Extern – Angriff aus dem Internet

Wir haben geprüft, was ein Angreifer aus dem Internet von Ihrer Kanzlei sieht: Ihren Internetanschluss mit Router und Firewall, Ihre Website und die Einstellungen Ihrer E-Mail-Domain. Eine Firewall ist der Türsteher Ihres Netzes – sie entscheidet, welche Verbindungen von außen hinein dürfen.

- Öffentliche IP-Adresse des Internetanschlusses (203.0.113.10)
- Website muster-gmbh.example (198.51.100.25)
- E-Mail-Domain muster-gmbh.example (SPF, DKIM, DMARC)

WLAN – Angriff über das Funknetz

Wir haben uns wie ein Besucher in Ihr Gäste-WLAN eingebucht und geprüft, ob man von dort aus an Ihre Kanzleisysteme gelangt. Zusätzlich haben wir bewertet, was die Funknetze schon vor der Anmeldung über Sie verraten.

- Gäste-WLAN „MusterGmbH-BR500-Gast“ (192.168.20.0/24)
- Mitarbeiter-WLAN „MusterGmbH-BR500“
- Trennung zwischen Gäste-WLAN und internem Netz

Intern – Angriff von innen

Wir haben geprüft, was ein Angreifer erreichen kann, der bereits einen Arbeitsplatz in Ihrem Netz kontrolliert – etwa nach einem geöffneten Schadanhang in einer E-Mail. Dazu haben wir ein kleines Prüfgerät (Node) im internen Netz angeschlossen, das die Systeme von innen untersucht.

- Internes Netz 192.168.10.0/24
- Fileserver FS01 mit Freigaben
- 15 Arbeitsplätze, Multifunktionsdrucker

3 Übersicht der Funde

Nr.	Schweregrad	Fund	Perspektive
F-01	Kritisch	Fernwartungszugang (RDP) ist direkt aus dem Internet erreichbar	Extern
F-02	Hoch	Firewall-Firmware veraltet, bekannte Sicherheitslücke vorhanden	Extern
F-03	Hoch	Fileserver-Freigabe für alle Mitarbeiter mit Schreibrechten, enthält Mandantendaten	Intern
F-04	Hoch	Gäste-WLAN nicht vom internen Netz getrennt	WLAN
F-05	Mittel	Drucker-Weboberfläche mit Standardpasswort	Intern
F-06	Mittel	E-Mail-Domain ohne DMARC-Eintrag, Fälschung von Absendern möglich	Extern
F-07	Mittel	Zwei Arbeitsplätze ohne aktuelle Sicherheitsupdates	Intern
F-08	Niedrig	Webserver gibt Versionsnummer preis	Extern
F-09	Niedrig	WLAN-Name verrät Firmenname und Routermodell	WLAN

4 Funde im Detail

F-01 · Kritisch · Fernwartungszugang (RDP) ist direkt aus dem Internet erreichbar

Problem: Der Fernwartungszugang zu Ihrem Terminalserver ist für jeden im Internet sichtbar. RDP (Remote Desktop Protocol) ist das Windows-Verfahren, mit dem man sich aus der Ferne an einem Rechner anmeldet. Über die Weiterleitung im Router kann jeder weltweit die Anmeldemaske aufrufen.

Risiko: Solche Zugänge werden rund um die Uhr automatisiert nach schwachen Passwörtern abgesucht. Gelingt eine Anmeldung, hat der Angreifer direkten Zugriff auf Ihr Netz und die Mandantendaten. Offene RDP-Zugänge gehören zu den häufigsten Einfallstoren für Erpressungstrojaner (Ransomware).

Maßnahme: Weiterleitung von Port 3389 im Router entfernen. Fernzugriff nur noch über ein VPN (verschlüsselter Tunnel ins Firmennetz) mit Zwei-Faktor-Anmeldung erlauben. (Aufwand ca. 2 Stunden, zuständig: IT-Dienstleister)

Betroffen Internetanschluss / Router (203.0.113.10); Terminalserver TS01 (192.168.10.10)

Port / Dienst 3389/tcp · Microsoft Terminal Services (RDP)

CVE –

Technischer Befund Portweiterleitung 203.0.113.10:3389 → 192.168.10.10:3389. Network Level Authentication aktiv, keine Kontosperre nach Fehlversuchen konfiguriert.

F-02 · Hoch · Firewall-Firmware veraltet, bekannte Sicherheitslücke vorhanden

Problem: Auf Ihrem Router mit Firewall läuft eine Software-Version (Firmware) von vor über einem Jahr. Für diese Version ist eine Sicherheitslücke öffentlich bekannt, die der Hersteller inzwischen geschlossen hat.

Risiko: Für öffentlich bekannte Lücken gibt es oft fertige Angriffswerkzeuge. Ein Angreifer könnte damit die Firewall übernehmen und den gesamten Datenverkehr der Kanzlei mitlesen oder umleiten.

Maßnahme: Aktuelle Firmware des Herstellers einspielen und automatische Update-Benachrichtigung aktivieren. Danach Konfiguration sichern. (Aufwand ca. 1 Stunde, zuständig: IT-Dienstleister)

Betroffen	Business-Router BR-500 (Beispielmodell) (203.0.113.10)
Port / Dienst	443/tcp · Verwaltungsoberfläche (HTTPS)
CVE	CVE-2025-0000x (Platzhalter)
Technischer Befund	Firmware 7.2.1 erkannt, aktuell ist 7.4.3. Verwaltungsoberfläche zusätzlich aus dem Internet erreichbar.

F-03 · Hoch · Fileserver-Freigabe für alle Mitarbeiter mit Schreibrechten, enthält Mandantendaten

Problem: Die Freigabe „Daten“ auf Ihrem Fileserver (zentraler Dateiablage-Rechner) darf von allen Benutzern gelesen und verändert werden – auch die Ordner mit Mandantenakten und Lohnunterlagen.

Risiko: Ein einziger infizierter Arbeitsplatz reicht, damit ein Erpressungstrojaner alle Mandantendaten verschlüsseln kann. Zudem kann jeder Mitarbeiter Daten einsehen, die er für seine Arbeit nicht braucht – ein Problem für Verschwiegenheit und DSGVO.

Maßnahme: Berechtigungen nach Aufgaben vergeben: Mandantenordner nur für zuständige Teams, Lohnunterlagen nur für die Lohnverrechnung. Schreibrechte auf das Nötige beschränken. (Aufwand ca. 1 Tag, zuständig: IT-Dienstleister mit Kanzleileitung)

Betroffen	Fileserver FS01, Freigabe „Daten“ (192.168.10.5)
Port / Dienst	445/tcp · SMB-Dateifreigabe
CVE	–
Technischer Befund	Freigabe \\FS01\Daten: Gruppe „Jeder“ mit Vollzugriff (Freigabe- und NTFS-Ebene). Rund 41.000 Dateien betroffen.

F-04 · Hoch · Gäste-WLAN nicht vom internen Netz getrennt

Problem: Wer im Gäste-WLAN angemeldet ist, kann Ihre internen Systeme erreichen, zum Beispiel den Fileserver und den Drucker. Das Gäste-WLAN sollte nur den Weg ins Internet freigeben.

Risiko: Ein Besucher oder jemand im Wartebereich mit dem Gäste-Passwort hätte denselben Netzzugang wie ein Mitarbeiter-PC. Zusammen mit F-03 wären die Mandantendaten direkt erreichbar.

Maßnahme: Gäste-WLAN im Router in ein eigenes, abgeschottetes Netz legen (Gast-Isolation aktivieren) und Zugriffe auf 192.168.10.0/24 sperren. (Aufwand ca. 1 Stunde, zuständig: IT-Dienstleister)

Betroffen	Gäste-WLAN „MusterGmbH-BR500-Gast“ (192.168.20.0/24); Internes Netz (192.168.10.0/24)
Port / Dienst	alle · Routing zwischen VLANs
CVE	–
Technischer Befund	Von 192.168.20.0/24 aus erreichbar: 192.168.10.5 (445/tcp), 192.168.10.50 (80/tcp, 443/tcp). Keine Firewall-Regel zwischen den Netzen.

F-05 · Mittel · Drucker-Weboberfläche mit Standardpasswort

Problem: Die Verwaltungsseite Ihres Multifunktionsdruckers ist mit dem Passwort geschützt, das ab Werk eingestellt war und im Handbuch steht.

Risiko: Wer die Verwaltung übernimmt, kann Scan-Ziele umstellen und so gescannte Dokumente an sich selbst schicken lassen oder hinterlegte Zugangsdaten für E-Mail und Netzordner auslesen.

Maßnahme: Eigenes, starkes Passwort für die Druckerverwaltung setzen und im Passwort-Manager hinterlegen. (Aufwand ca. 15 Minuten, zuständig: Intern)

Betroffen	Multifunktionsdrucker MFP-01 (192.168.10.50)
Port / Dienst	80/tcp, 443/tcp · Druckerverwaltung (HTTP/HTTPS)
CVE	–
Technischer Befund	Anmeldung mit Werkspasswort erfolgreich. Im Gerät hinterlegt: SMTP-Zugangsdaten und Scan-Ziel \\FS01\Scans.

F-06 · Mittel · E-Mail-Domain ohne DMARC-Eintrag, Fälschung von Absendern möglich

Problem: Für Ihre E-Mail-Domain fehlt ein DMARC-Eintrag. DMARC ist eine Angabe im Internet-Telefonbuch (DNS), die Empfängern sagt, wie sie mit gefälschten E-Mails in Ihrem Namen umgehen sollen.

Risiko: Betrüger können E-Mails verschicken, die scheinbar von Ihrer Kanzlei kommen – etwa mit gefälschten Zahlungsaufforderungen an Ihre Mandanten. Viele Empfänger-Postfächer lassen solche Mails ohne DMARC ungehindert durch.

Maßnahme: DMARC-Eintrag anlegen, zunächst im Beobachtungsmodus, nach vier Wochen auf „Ablehnen“ umstellen. DKIM-Signatur beim E-Mail-Anbieter aktivieren. (Aufwand ca. 1 Stunde, zuständig: IT-Dienstleister)

Betroffen	E-Mail-Domain (muster-gmbh.example)
Port / Dienst	– · DNS (TXT-Einträge)
CVE	–
Technischer Befund	_dmarc.muster-gmbh.example: kein Eintrag. SPF vorhanden („~all“), DKIM-Signatur nicht aktiv.

F-07 · Mittel · Zwei Arbeitsplätze ohne aktuelle Sicherheitsupdates

Problem: Auf zwei Arbeitsplätzen wurden seit rund vier Monaten keine Sicherheitsupdates mehr installiert. Die übrigen 13 Rechner sind aktuell.

Risiko: Ungepatchte Rechner sind das bevorzugte Ziel von Schadsoftware. Ein einziger veralteter Rechner kann als Sprungbrett ins restliche Netz dienen.

Maßnahme: Updates auf beiden Rechnern nachholen und prüfen, warum die automatische Verteilung dort nicht greift. Updatestand monatlich kontrollieren. (Aufwand ca. 2 Stunden, zuständig: IT-Dienstleister)

Betroffen	Arbeitsplatz PC-07 (192.168.10.121); Arbeitsplatz PC-12 (192.168.10.134)
Port / Dienst	– · Windows Update
CVE	mehrere (kumulative Updates der letzten 4 Monate)
Technischer Befund	Letztes kumulatives Update auf beiden Geräten vor ca. 4 Monaten. Update-Dienst auf PC-12 deaktiviert.

F-08 · Niedrig · Webserver gibt Versionsnummer preis

Problem: Ihr Webserver nennt bei jeder Anfrage seine genaue Software-Version.

Risiko: Das ist für sich keine Lücke, erleichtert Angreifern aber die Suche nach passenden Schwachstellen, sobald für diese Version eine bekannt wird.

Maßnahme: Versionsangabe in der Webserver-Konfiguration abschalten (beim Hosting-Anbieter anfragen). (Aufwand ca. 15 Minuten, zuständig: Hosting-Anbieter)

Betroffen	Website muster-gmbh.example (198.51.100.25)
Port / Dienst	443/tcp · HTTPS (Webserver)
CVE	–
Technischer Befund	Antwort-Header „Server: Apache/2.4.57 (Debian)“.

F-09 · Niedrig · WLAN-Name verrät Firmenname und Routermodell

Problem: Der Name Ihrer Funknetze (SSID) enthält Ihren Firmennamen und das Routermodell.

Risiko: Ein Angreifer in der Nähe weiß damit sofort, welches Netz zu Ihrer Kanzlei gehört und welche Gerätelücken er ausprobieren könnte.

Maßnahme: WLAN-Namen ohne Firmen- und Modellbezug vergeben. (Aufwand ca. 15 Minuten, zuständig: Intern)

Betroffen	WLAN „MusterGmbH-BR500“ und „MusterGmbH-BR500-Gast“ (–)
Port / Dienst	– · WLAN (SSID-Aussendung)
CVE	–
Technischer Befund	Zwei SSIDs mit Firmenname und Modellbezeichnung „BR500“ sichtbar.

5 Maßnahmenplan

Prio	Maßnahme	Aufwand	Zuständig	Fund
1	Weiterleitung von Port 3389 im Router entfernen. Fernzugriff nur noch über ein VPN (verschlüsselter Tunnel ins Firmennetz) mit Zwei-Faktor-Anmeldung erlauben.	ca. 2 Stunden	IT-Dienstleister	F-01
2	Aktuelle Firmware des Herstellers einspielen und automatische Update-Benachrichtigung aktivieren. Danach Konfiguration sichern.	ca. 1 Stunde	IT-Dienstleister	F-02
3	Berechtigungen nach Aufgaben vergeben: Mandantenordner nur für zuständige Teams, Lohnunterlagen nur für die Lohnverrechnung. Schreibrechte auf das Nötige beschränken.	ca. 1 Tag	IT-Dienstleister mit Kanzleileitung	F-03
4	Gäste-WLAN im Router in ein eigenes, abgeschottetes Netz legen (Guest-Isolation aktivieren) und Zugriffe auf 192.168.10.0/24 sperren.	ca. 1 Stunde	IT-Dienstleister	F-04
5	Eigenes, starkes Passwort für die Druckerverwaltung setzen und im Passwort-Manager hinterlegen.	ca. 15 Minuten	Intern	F-05
6	DMARC-Eintrag anlegen, zunächst im Beobachtungsmodus, nach vier Wochen auf „Ablehnen“ umstellen. DKIM-Signatur beim E-Mail-Anbieter aktivieren.	ca. 1 Stunde	IT-Dienstleister	F-06
7	Updates auf beiden Rechnern nachholen und prüfen, warum die automatische Verteilung dort nicht greift. Updatestand monatlich kontrollieren.	ca. 2 Stunden	IT-Dienstleister	F-07
8	Versionsangabe in der Webserver-Konfiguration abschalten (beim Hosting-Anbieter anfragen).	ca. 15 Minuten	Hosting-Anbieter	F-08
9	WLAN-Namen ohne Firmen- und Modellbezug vergeben.	ca. 15 Minuten	Intern	F-09

Dieser Bericht ist ein Beispiel. Alle Namen, Adressen, IP-Adressen (RFC 5737 / RFC 1918) und Funde sind frei erfunden. CVE-Angaben sind Platzhalter.