WERIXO INSIGHT

IT-SICHERHEITSBEWERTUNG · MUSTERBERICHT

BEISPIELBERICHT, SYNTHETISCHE DATEN

Muster Maschinenbau GmbH (fiktiv)

Externe IT-Sicherheitsbewertung. 14 Endpoints, Microsoft 365, Perimeter und Backup-Status im Prüfzeitraum erfasst.

SICHERHEITSINDEX

72/100

Gut aufgestellt, einzelne Punkte bleiben offen.

● MUSTERBERICHT · FIKTIVE DATEN · KEIN KUNDENBERICHT

REPORT-ID	ERSTELLT	PRÜFZEITRAUM	VERTRAULICHKEIT	ENGINE
MUSTER-DEMO	11. Juni 2026	Mai 2026	Musterbericht · fiktive Daten	WERIXO Insight 0.4

BERICHTSIDENTITÄT

Über diesen Bericht

ECKDATEN DES BERICHTS

KUNDE Muster Maschinenbau GmbH (fiktiv)	REPORT-ID MUSTER-DEMO
ERSTELLT 11. Juni 2026	PRÜFZEITRAUM Mai 2026
ENGINE WERIXO Insight 0.4	VERTRAULICHKEIT Musterbericht · fiktive Daten
ERSTELLT VON WERIXO (Muster)	EMPFÄNGER öffentliche Muster-Ansicht

UNTERSUCHUNGSUMFANG

Externe IT-Sicherheitsbewertung. 14 Endpoints, Microsoft 365, Perimeter und Backup-Status im Prüfzeitraum erfasst.

14	4	22	1	3	6
ENDPOINTS	SERVER	MICROSOFT-365-IDENTITÄTEN	STANDORTE	PERIMETER-ADRESSEN	BACKUP-JOBS

MUSTERBERICHT

Dies ist ein Musterbericht mit fiktiven Daten. Kein Kundenbericht, keine echten Befunde, keine echten Kennzahlen.

EXECUTIVE SUMMARY
TEIL 01 / 05

Status im Überblick

Der Schutz steht auf einem soliden Fundament und hat sich gegenüber dem Vormonat leicht verbessert. Zwei Punkte verdienen kurzfristig Aufmerksamkeit, bevor sie zum Risiko werden.

6	2	5	+4
OFFENE BEFUNDE	HOCH GEWICHTET	BETROFFENE BEREICHE	Δ ZUM VERGLEICH

SICHERHEITSINDEX

72/100

Gut aufgestellt, einzelne Punkte bleiben offen.

▲ +4 Pkt. ggü. Vergleich (68)

OFFENE BEFUNDE NACH SCHWERE

Hoch	2
Mittel	3
Niedrig	1
Kritisch	0

DAS WICHTIGSTE

01 Der Sicherheitsindex steigt um vier Punkte auf 72 von 100. Die Richtung stimmt, das Niveau ist gut, aber nicht abgeschlossen.

02 Die größte offene Lücke liegt beim Endpoint-Schutz: zwei Arbeitsplätze laufen ohne aktiven Echtzeitschutz.

03 Drei Microsoft-365-Postfächer ohne erzwungene Zwei-Faktor-Anmeldung bleiben das wahrscheinlichste Einfallstor.

IHRE ENTSCHEIDUNG

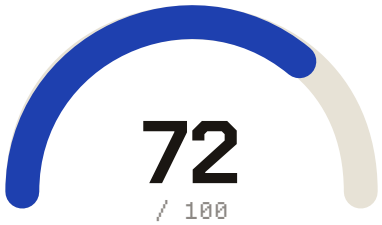
Geben Sie die Reihenfolge der drei vorrangigen Maßnahmen frei. WERIXO setzt sie im laufenden Monat um und weist die Umsetzung im nächsten Bericht nach.

Sicherheitsindex & Verlauf

72 von 100 heißt: das Fundament trägt, der Betrieb ist nicht akut gefährdet, aber zwei konkrete Lücken stehen offen. Der Wert misst die geprüften Bereiche zum Stichtag, nicht eine Garantie. Er steigt, sobald die vorrangigen Maßnahmen umgesetzt und im nächsten Bericht nachgewiesen sind.

AKTUELLER STAND

SICHERHEITSINDEX

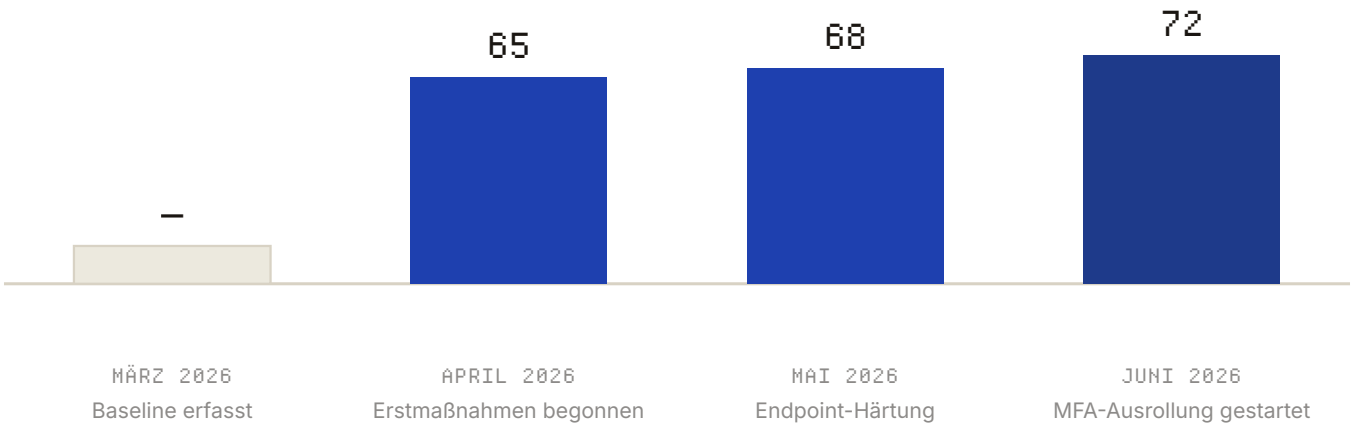


Gut aufgestellt, einzelne Punkte bleiben offen.

0 bis 40	Wesentliche Schutzmaßnahmen fehlen.
41 bis 60	Basis-Schutz mit klaren Lücken.
61 bis 80	Gut aufgestellt, einzelne Punkte offen. AKTUELL
81 bis 100	Durchgängig abgesichert.

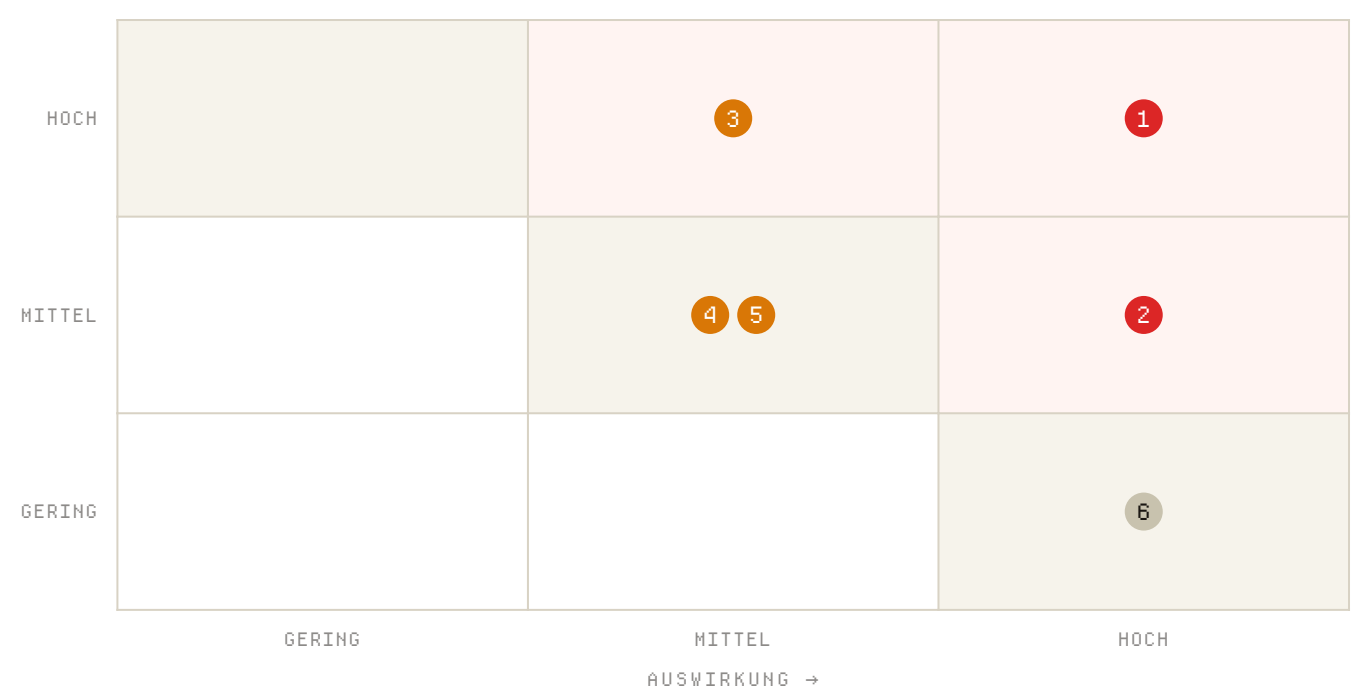
VERLAUF SEIT DER BASELINE

▲ +4 Pkt. ggü. Vormonat (68)



Wo die Befunde im Risiko stehen

Jeder Befund steht an der Stelle, die sein Risiko ausmacht: wie wahrscheinlich er eintritt (senkrecht) und wie schwer er wöge (waagerecht). Je weiter rechts oben, desto dringlicher. Die Schwere-Einstufung wägt zusätzlich vorhandene Schutzmaßnahmen ab, sie kann daher von der reinen Position abweichen.



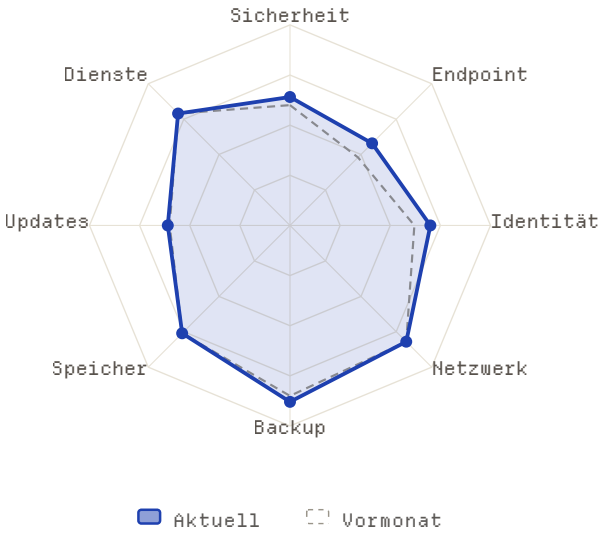
WELCHE BEFUNDE DIE MATRIX ZEIGT

1	Echtzeitschutz auf zwei Endpoints deaktiviert	Wahrsch. hoch · Auswirkung hoch
2	Patch-Rückstand auf vier Servern	Wahrsch. mittel · Auswirkung hoch
3	MFA für drei Postfächer nicht erzwungen	Wahrsch. hoch · Auswirkung mittel
4	Veraltete Firewall-Firmware am Perimeter	Wahrsch. mittel · Auswirkung mittel
5	Lokale Administratorrechte auf fünf Arbeitsplätzen	Wahrsch. mittel · Auswirkung mittel
6	Backup-Wiederherstellung seit 90 Tagen nicht getestet	Wahrsch. gering · Auswirkung hoch

Sicherheit nach Bereich

8 Prüfbereiche, jeweils von 0 bis 100 bewertet. Am stärksten steht Backup mit 88, die größte Lücke zeigt Endpoint mit 58. Das Radar zeigt das Reifeprofil im Vergleich zum Vormonat.

REIFEPROFIL ÜBER 8 PRÜFBEREICHE



BEWERTUNG, VERÄNDERUNG & BEFUNDE JE BEREICH (8 PRÜFBEREICHE)

Sicherheit	64/100	▲ +4	–	
Endpoint	58/100	▲ +10	1 BEF.	
Identität	70/100	▲ +8	2 BEF.	
Netzwerk	82/100	– 0	1 BEF.	
Backup	88/100	▲ +3	1 BEF.	
Speicher	76/100	– 0	–	
Updates	61/100	▲ +1	1 BEF.	
Dienste	79/100	– 0	–	

Alle Befunde auf einen Blick

Alle Befunde im Überblick, nach Schwere geordnet. Die Tabelle nennt für jeden den betroffenen Bereich, die Einschätzung aus Wahrscheinlichkeit und Auswirkung sowie den Bearbeitungsstand. Die schwersten werden auf den folgenden Seiten im Detail aufgeschlüsselt.

#	BEFUND	BEREICH	WAHRSCH. / AUSW.	SCHWERE	STATUS
01	Echtzeitschutz auf zwei Endpoints deaktiviert	Endpoint	hoch / hoch	Hoch	Offen
02	Patch-Rückstand auf vier Servern	Updates	mittel / hoch	Hoch	Offen
03	MFA für drei Postfächer nicht erzwungen	Identität	hoch / mittel	Mittel	Offen
04	Veraltete Firewall-Firmware am Perimeter	Netzwerk	mittel / mittel	Mittel	Offen
05	Lokale Administratorrechte auf fünf Arbeitsplätzen	Identität	mittel / mittel	Mittel	In Bearbeitung
06	Backup-Wiederherstellung seit 90 Tagen nicht getestet	Backup	gering / hoch	Niedrig	Offen

BEFUNDE IM DETAIL BEFUND 01 / 06

Echtzeitschutz auf zwei Endpoints deaktiviert

RISIKO-PROFIL

5 / 5

SCHWERE	BEREICH	STATUS
Hoch	Endpoint	Offen
WAHRSCH.	**AUSWIRKUNG**	**BEFUND**
hoch	hoch	01 / 06

WAS WIR BEOBACHTET HABEN

- Auf zwei Arbeitsplätzen in der Fertigung meldet der Schutz-Agent den Echtzeitschutz als deaktiviert.
- Der Zustand besteht seit mindestens elf Tagen, ohne dass der Schutz erneut aktiviert wurde.
- Der letzte vollständige Scan lief vor neun Tagen. Seither greift kein dauerhafter Schutz.

BETROFFENE SYSTEME

WS-FERT-04 Fertigung

WS-FERT-07 Fertigung

Abdeckung: 2 von 14 Endpoints

DER NACHWEIS

Quelle	Endpoint-Telemetrie (Agent)
Methode	Automatische Statusabfrage je Gerät
Stand der Daten	Mai 2026, Abdeckung 14 / 14 Geräte
Letzter vollständiger Scan	vor 9 Tagen, ohne Befund

Agent meldet RealTimeProtection = disabled · WS-FERT-04, WS-FERT-07 · seit 04. Mai 2026

DIE BEDROHUNG IM KLARTEXT

Ohne Echtzeitschutz wird eine Schaddatei nicht beim Ausführen geblockt, sondern bestenfalls beim nächsten manuellen Scan bemerkt. In der Fertigung, wo Dateien über Wechseldatenträger und mit Zulieferern ausgetauscht werden, wirkt diese Lücke am stärksten.

01 Eine Schaddatei erreicht den Arbeitsplatz, über E-Mail-Anhang, USB-Stick oder Download.

02 Ohne aktiven Echtzeitschutz wird sie beim Öffnen nicht blockiert.

03 Die Schadsoftware wird ausgeführt und kann sich von dort im Netz weiterbewegen.

04 Auffällig wird sie erst beim nächsten vollständigen Scan, im ungünstigen Fall Tage später.

WARUM DIESE EINSTUFUNG

EINTRITTSWAHRSCHEINLICHKEIT · HOCH

Der Zustand besteht seit elf Tagen auf zwei aktiv genutzten Fertigungs-Arbeitsplätzen. Der übliche Infektionsweg über das Ausführen einer Datei steht offen.

AUSWIRKUNG · HOCH

Ein infizierter Fertigungs-Client dient als Brückenkopf ins Netz und macht Konstruktions- und Auftragsdaten auf den verbundenen Servern erreichbar.

Gesamteinstufung Hoch, nicht kritisch. Kritisch wäre der Befund bei einem beobachteten aktiven Vorfall. Ein solcher liegt nicht vor, der periodische Scan läuft weiter. Die hohe Einstufung beruht auf der offenen Tür, nicht auf einem eingetretenen Schaden.

WAS FÜR DEN BETRIEB AUF DEM SPIEL STEHT

- Stillstand in der Fertigung, falls ein Client bereinigt oder vom Netz getrennt werden muss.
- Zugriff auf Konstruktions- und Auftragsdaten, die auf den verbundenen Servern liegen.
- Im Ernstfall kann ein Sicherheitsvorfall meldepflichtig werden (NIS2-Kontext). WERIXO unterstützt bei der Vorbereitung, garantiert aber keine Rechtsfolge.

BEHEBUNG SCHRITT FÜR SCHRITT

01 Echtzeitschutz reaktivieren — WERIXO · Tag 0 bis 1

Auf WS-FERT-04 und WS-FERT-07 sofort wieder einschalten.

02 Abschalten sperren — WERIXO · Tag 1 bis 3

Per Geräte-Richtlinie das Deaktivieren durch lokale Nutzer unterbinden.

03 Vollständigen Scan anstoßen — WERIXO · Tag 1 bis 3

Beide Geräte vollständig prüfen und das Ergebnis dokumentieren.

04 Ursache klären — WERIXO + Kunde · Tag 3 bis 7

Feststellen, warum der Schutz deaktiviert war (Nutzer, Software-Konflikt, Update).

05 Alarm einrichten — WERIXO · Tag 3 bis 7

Eine Meldung scharf schalten, die künftiges Deaktivieren sofort sichtbar macht.

SO WEISEN WIR DEN ABSCHLUSS NACH

- Der Schutz-Agent meldet RealTimeProtection = enabled auf beiden Geräten, durchgehend über sieben Tage.
- Der vollständige Scan ist ohne Fund abgeschlossen und protokolliert.
- Im Folgebericht erscheint der Befund als „geschlossen“ mit Datum.
- Solange ein Gerät das Kriterium reißt, bleibt der Befund offen, auch bei kurzzeitiger Reaktivierung.

Erstmals erfasst: Mai 2026 · Status: Offen seit Erfassung

Bezug: NIS2 Art. 21 (Risikomanagement) · BSI-Grundschutz SYS.2.2 (Clients)

BEFUNDE IM DETAIL BEFUND 02 / 06

Patch-Rückstand auf vier Servern

RISIKO-PROFIL

4 / 5

SCHWERE	BEREICH	STATUS
Hoch	Updates	Offen
WAHRSCH.	**AUSWIRKUNG**	**BEFUND**
mittel	hoch	02 / 06

WAS WIR BEOBACHTET HABEN

- Vier Server liegen mehr als 30 Tage hinter dem freigegebenen Patchstand.
- Betroffen sind sicherheitsrelevante Updates, nicht nur Funktions-Updates.
- Ein Wartungsfenster für das Einspielen ist derzeit nicht fest terminiert.

DER NACHWEIS

Quelle	Patch- & Versionsstand (Agent)
Methode	Versionsabgleich gegen Herstellerfreigabe
Stand der Daten	Mai 2026, Abdeckung 18 Systeme
Ältester Rückstand	über 30 Tage

4 Server über 30 Tage hinter Freigabestand · SRV-AD-01 = Verzeichnisdienst

BETROFFENE SYSTEME

SRV-FILE-01 Dateiserver

SRV-FILE-02 Dateiserver

SRV-AD-01 Verzeichnisdienst

SRV-APP-01 Anwendung

Abdeckung: 4 System(e)

DIE BEDROHUNG IM KLARTEXT

Bekannte Schwachstellen in nicht gepatchten Diensten sind öffentlich dokumentiert und werden gezielt gesucht. Ein Verzeichnisdienst ist ein besonders lohnendes Ziel, weil er die Anmeldungen im ganzen Netz steuert.

01 Eine bekannte, öffentlich dokumentierte Schwachstelle bleibt ungepatcht offen.

02 Sie erlaubt einem Angreifer mehr Rechte oder das Ausführen von Code auf dem Server.

03 Über den Verzeichnisdienst lassen sich weitere Konten und Systeme erreichen.

04 Aus einem Server-Problem wird ein Problem für das gesamte Netz.

WARUM DIESE EINSTUFUNG

EINTRITTSWAHRSCHEINLICHKEIT · MITTEL

Die Server sind nicht direkt aus dem Internet erreichbar, aber intern. Für bekannte Lücken sind Angriffswege öffentlich verfügbar.

AUSWIRKUNG · HOCH

Datei- und Verzeichnisdienste tragen den laufenden Betrieb. Der Verzeichnisdienst steuert Anmeldungen, ein Kompromiss betrifft alle Konten.

Gesamteinstufung Hoch. Die Wahrscheinlichkeit ist mittel, die mögliche Auswirkung über den Verzeichnisdienst hoch. Die Einstufung folgt der Auswirkung, weil ein zentraler Dienst betroffen ist.

WAS FÜR DEN BETRIEB AUF DEM SPIEL STEHT

- Ausfall zentraler Datei- und Anmeldedienste legt das Arbeiten still.
- Ein kompromittierter Verzeichnisdienst betrifft sämtliche Konten gleichzeitig.
- Die Wiederherstellung nach einem Vorfall ist deutlich aufwändiger als ein geplantes Wartungsfenster.

BEHEBUNG SCHRITT FÜR SCHRITT

01 Wartungsfenster festlegen — WERIXO + Kunde · Tag 0 bis 3

Einen Termin mit dem Kunden abstimmen, der den Betrieb nicht stört.

02 Updates staffeln — WERIXO · Tag 3 bis 7

Verzeichnisdienst und Dateiserver zuerst, vorher prüfen.

03 Im Fenster einspielen — WERIXO · Tag 3 bis 10

Mit Rückfallpunkt (Snapshot) vor dem Einspielen.

04 Versionsstand prüfen — WERIXO · Tag 7 bis 10

Nach dem Einspielen den Freigabestand bestätigen.

05 Patch-Fenster verankern — WERIXO + Kunde · Tag 10 bis 30

Einen wiederkehrenden monatlichen Termin als Prozess festlegen.

SO WEISEN WIR DEN ABSCHLUSS NACH

- [ ] Der Versionsabgleich zeigt alle vier Server auf dem Freigabestand.
- [ ] Kein offener sicherheitsrelevanter Rückstand über 30 Tage.
- [ ] Ein wiederkehrendes Patch-Fenster ist terminiert und dokumentiert.
- [ ] Der Folgebericht zeigt den Befund als geschlossen.

Erstmals erfasst: Mai 2026 · Status: Offen seit Erfassung

Bezug: NIS2 Art. 21 · BSI-Grundschutz OPS.1.1.3 (Patch-Management)

BEFUNDE IM DETAIL BEFUND 03 / 06

MFA für drei Postfächer nicht erzwungen

RISIKO-PROFIL

4 / 5

SCHWERE	BEREICH	STATUS
Mittel	Identität	Offen
WAHRSCH.	**AUSWIRKUNG**	**BEFUND**
hoch	mittel	03 / 06

WAS WIR BEOBACHTET HABEN

- Drei Microsoft-365-Postfächer melden sich ohne erzwungene Zwei-Faktor-Anmeldung an.
- Für diese Konten genügt aktuell ein Passwort, ein zweiter Faktor ist optional.
- Die übrigen 19 Identitäten nutzen die Zwei-Faktor-Anmeldung bereits.

DER NACHWEIS

Quelle	Microsoft-365-Konfiguration (API)
Methode	Abfrage des MFA-Status je Identität
Stand der Daten	Mai 2026, Abdeckung 22 Identitäten
MFA erzwungen	19 von 22

MFA erzwungen 19/22 · ohne: buchhaltung@, einkauf@, info@ (geteilt)

BETROFFENE SYSTEME

- Postfach buchhaltung@
- Postfach einkauf@
- Postfach info@ geteilt

Abdeckung: 3 System(e)

DIE BEDROHUNG IM KLARTEXT

Konten ohne zweiten Faktor fallen bei Phishing oder einem geleakten Passwort sofort. Buchhaltung und Einkauf haben Zugriff auf Zahlungs- und Bestellprozesse, ein typisches Ziel für Rechnungsbetrug.

01 Eine Phishing-Mail oder ein geleaktes Passwort liefert die Zugangsdaten.

02 Ohne zweiten Faktor genügt das Passwort für den vollen Zugriff.

03 Im Postfach lassen sich Rechnungen, Bestellungen und Kontakte einsehen.

04 Ein Angreifer lenkt im Namen des Kontos Zahlungen um oder greift weitere Mitarbeiter an.

WARUM DIESE EINSTUFUNG

EINTRITTSWAHRSCHEINLICHKEIT · HOCH

Postfächer sind aus dem Internet erreichbar, Phishing ist alltäglich. Ohne zweiten Faktor schützt nur das Passwort.

AUSWIRKUNG · MITTEL

Betroffen sind einzelne Postfächer, allerdings Buchhaltung und Einkauf mit direktem Finanzbezug.

Gesamteinstufung Mittel. Hohe Wahrscheinlichkeit, mittlere Auswirkung je Konto. Das geteilte info@-Postfach braucht eine eigene Lösung über benannte Zugänge.

WAS FÜR DEN BETRIEB AUF DEM SPIEL STEHT

- Rechnungsbetrug und umgeleitete Zahlungen über ein übernommenes Buchhaltungs- oder Einkaufskonto.
- Vertrauensverlust bei Kunden und Lieferanten, wenn aus dem Konto Betrug läuft.
- Aufwand zur Aufklärung und Rücksprache mit Geschäftspartnern.

BEHEBUNG SCHRITT FÜR SCHRITT

01 MFA erzwingen — WERIXO · Tag 0 bis 7
Für buchhaltung@ und einkauf@ verbindlich aktivieren.

02 Geteiltes Postfach lösen — WERIXO + Kunde · Tag 7 bis 21
info@ auf benannte Zugänge umstellen, dann MFA je Person.

03 Richtlinie setzen — WERIXO · Tag 14 bis 30
Bedingten Zugriff mit MFA-Pflicht für alle Identitäten prüfen.

04 Nutzer einweisen — WERIXO · Tag 7 bis 14
Kurze Anleitung zur Authenticator-App für die betroffenen Personen.

SO WEISEN WIR DEN ABSCHLUSS NACH

- [ ] Die API-Abfrage zeigt MFA erzwungen für 22 von 22 Identitäten.
- [ ] Das geteilte Postfach ist durch benannte Zugänge ersetzt.
- [ ] Eine Richtlinie erzwingt MFA für neue Konten automatisch.
- [ ] Der Folgebericht zeigt den Befund als geschlossen.

Erstmals erfasst: Mai 2026 · Status: Offen seit Erfassung

Bezug: NIS2 Art. 21 · BSI-Grundschutz ORP.4 (Identitätsmanagement)

BEFUNDE IM DETAIL BEFUND 04 / 06

Veraltete Firewall-Firmware am Perimeter

RISIKO-PROFIL

3 / 5

SCHWERE	BEREICH	STATUS
Mittel	Netzwerk	Offen
WAHRSCH.	**AUSWIRKUNG**	**BEFUND**
mittel	mittel	04 / 06

WAS WIR BEOBACHTET HABEN

- Die Perimeter-Firewall läuft auf einer Firmware-Version mit bekannten Schwachstellen.
- Eine aktuellere, vom Hersteller freigegebene Version steht bereit.
- Das Update wurde im Prüfzeitraum noch nicht eingespielt.

BETROFFENE SYSTEME

`FW-PERIM-01` Perimeter-Firewall

Abdeckung: 1 System(e)

DER NACHWEIS

Quelle	Perimeter-Erreichbarkeit (Externer Scan)
Methode	Firmware-Version gegen Herstellerfreigabe
Stand der Daten	Mai 2026, 3 Perimeter-Adressen
Update	verfügbar, nicht eingespielt

FW-PERIM-01 · Firmware unter Herstellerfreigabe · bekannte Schwachstellen dokumentiert

DIE BEDROHUNG IM KLARTEXT

Die Firewall steht am Übergang zum Internet. Eine Schwachstelle in der Firmware ist besonders heikel, weil das Gerät selbst die Grenze bildet, die es schützen soll.

01 Eine bekannte Schwachstelle in der Firmware ist öffentlich dokumentiert.

02 Das Gerät ist von außen erreichbar, es bildet den Perimeter.

03 Ein erfolgreicher Angriff hebelt die Schutzgrenze aus, statt sie zu durchqueren.

04 Von der Firewall aus ist der Weg ins interne Netz kurz.

WARUM DIESE EINSTUFUNG

EINTRITTSWAHRSCHEINLICHKEIT · MITTEL

Die Schwachstelle ist bekannt, die Ausnutzung verlangt einen gezielten Angriff. Ein offenes Admin-Login wurde nicht beobachtet.

AUSWIRKUNG · MITTEL

Ein Perimeter-Gerät ist betroffen. Die Segmentierung dahinter begrenzt den unmittelbaren Schaden.

Gesamteinstufung Mittel. Die Lücke betrifft die Schutzgrenze selbst, ist aber ohne gezielten Angriff nicht trivial auszunutzen. Das verfügbare Update schließt sie.

WAS FÜR DEN BETRIEB AUF DEM SPIEL STEHT

- Wegfall der Schutzgrenze zwischen Internet und internem Netz.
- Potenzieller Zugang zum internen Netz über das Perimeter-Gerät.
- Ein Firewall-Ausfall stört auch den legitimen Internetzugang des Betriebs.

BEHEBUNG SCHRITT FÜR SCHRITT

01 Konfiguration sichern — WERIXO · Tag 0 bis 14

Vor dem Update einen Rückfallpunkt der Firewall-Konfiguration anlegen.

02 Firmware einspielen — WERIXO · Tag 0 bis 14

Die freigegebene Version in einem kurzen Wartungsfenster aufspielen.

03 Gegen Baseline prüfen — WERIXO · Tag 0 bis 14

Nach dem Update die Konfiguration gegen die Baseline abgleichen.

04 Admin-Zugang schließen — WERIXO · Tag 0 bis 14

Den Verwaltungszugang der Firewall auf VPN oder intern beschränken.

SO WEISEN WIR DEN ABSCHLUSS NACH

- [ ] Der Versionsabgleich zeigt die Firmware auf dem Freigabestand.
- [ ] Die Konfiguration entspricht der Baseline.
- [ ] Der Admin-Zugang ist nicht mehr offen aus dem Internet erreichbar.
- [ ] Der Folgebericht zeigt den Befund als geschlossen.

Erstmals erfasst: Mai 2026 · Status: Offen seit Erfassung

Bezug: NIS2 Art. 21 · BSI-Grundschutz NET.3.2 (Firewall)

BEFUNDE IM DETAIL BEFUND 05 / 06

Lokale Administratorrechte auf fünf Arbeitsplätzen

RISIKO-PROFIL

3 / 5

SCHWERE	BEREICH	STATUS
Mittel	Identität	In Bearbeitung
WAHRSCH.	**AUSWIRKUNG**	**BEFUND**
mittel	mittel	05 / 06

WAS WIR BEOBACHTET HABEN

- Fünf Arbeitsplätze arbeiten dauerhaft mit lokalen Administratorrechten.
- Die Umstellung auf Standardrechte hat begonnen, ist aber noch nicht abgeschlossen.
- Lokale Adminrechte vergrößern den Schaden, falls ein Konto übernommen wird.

BETROFFENE SYSTEME

WS-BUERO-02 Büro

WS-BUERO-05 Büro

WS-FERT-01 Fertigung

WS-FERT-03 Fertigung

WS-VERTRIEB-01 Vertrieb

Abdeckung: 5 System(e)

DER NACHWEIS

Quelle	Endpoint-Telemetrie (Agent)
Methode	Abfrage der lokalen Gruppenmitgliedschaft
Stand der Daten	Mai 2026, Abdeckung 14 / 14 Geräte
Betroffen	5 von 14 Arbeitsplätzen

5/14 Arbeitsplätze mit dauerhaften lokalen Adminrechten · Umstellung begonnen

DIE BEDROHUNG IM KLARTEXT

Lokale Adminrechte bedeuten: wird ein Konto übernommen, kann Schadsoftware sich tief einnisten und Schutzmechanismen abschalten. Diese Lücke verstärkt jede andere, sie ist selten der Einstieg, aber oft der Brandbeschleuniger.

01 Ein Nutzerkonto wird übernommen (Phishing, Schaddatei).

02 Mit lokalen Adminrechten kann Schadsoftware Schutz abschalten und sich dauerhaft einnisten.

03 Aus einem begrenzten Vorfall wird die vollständige Kompromittierung des Geräts.

04 Der Aufwand zur sauberen Bereinigung steigt deutlich.

WARUM DIESE EINSTUFUNG

EINTRITTSWAHRSCHEINLICHKEIT · MITTEL

Die Rechte sind eine Voraussetzung, kein Einstieg. Wirksam werden sie erst zusammen mit einer Kontoübernahme.

AUSWIRKUNG · MITTEL

Der Schaden je Vorfall steigt, die Bereinigung wird aufwändiger. Betroffen ist das einzelne Gerät, nicht direkt das ganze Netz.

Gesamteinstufung Mittel, Tendenz sinkend. Die Umstellung läuft bereits. Der Befund bleibt offen, bis keine dauerhaften Adminrechte mehr außerhalb dokumentierter Ausnahmen bestehen.

WAS FÜR DEN BETRIEB AUF DEM SPIEL STEHT

- Größerer Schaden je Sicherheitsvorfall durch tiefere Einnistung.
- Aufwändigere und längere Bereinigung betroffener Geräte.
- Lokale Adminrechte erleichtern die Ausbreitung von Schadsoftware.

BEHEBUNG SCHRITT FÜR SCHRITT

01 Bedarf aufnehmen — WERIXO + Kunde · läuft

Klären, wer Adminrechte wofür tatsächlich braucht.

02 Rechte zurücknehmen — WERIXO · Tag 0 bis 30

Dauerhafte Adminrechte durch bedarfsweise Vergabe ersetzen.

03 Standard als Richtlinie — WERIXO · Tag 30 bis 60

Standardnutzer ohne lokale Adminrechte als Vorgabe verankern.

04 Ausnahmen befristen — WERIXO · Tag 30 bis 60

Notwendige Ausnahmen dokumentieren und mit Ablaufdatum versehen.

SO WEISEN WIR DEN ABSCHLUSS NACH

- Die Abfrage zeigt keine dauerhaften lokalen Adminrechte außerhalb dokumentierter, befristeter Ausnahmen.
- Eine Richtlinie hält neue Geräte auf Standardrechten.
- Die Ausnahmenliste ist gepflegt und befristet.
- Der Folgebericht zeigt den Fortschritt bis zum Abschluss.

Erstmals erfasst: April 2026 · Status: In Bearbeitung

Bezug: NIS2 Art. 21 · BSI-Grundschutz ORP.4 (Identitätsmanagement)

BEFUNDE IM DETAIL BEFUND 06 / 06

Backup-Wiederherstellung seit 90 Tagen nicht getestet

RISIKO-PROFIL

2 / 5

SCHWERE	BEREICH	STATUS
Niedrig	Backup	Offen
WAHRSCH.	**AUSWIRKUNG**	**BEFUND**
gering	hoch	06 / 06

WAS WIR BEOBACHTET HABEN

- Die Sicherungen laufen täglich und erfolgreich, lokal und an einen zweiten Ort.
- Eine echte Rücksicherung wurde im Prüfzeitraum nicht nachgewiesen.
- Ein Backup ohne Restore-Test bleibt eine Annahme, kein Nachweis.

BETROFFENE SYSTEME

6 Backup-Jobs täglich, lokal und zweiter Ort

Abdeckung: 1 von 6 Backup-Jobs

DER NACHWEIS

Quelle	Backup-Protokolle (API)
Methode	Abgleich von Lauf, Erfolg und letztem Restore-Test
Stand der Daten	Mai 2026, 6 Jobs
Letzter Restore-Test	über 90 Tage / nicht dokumentiert

6/6 Jobs laufen erfolgreich · letzter dokumentierter Restore-Test über 90 Tage

DIE BEDROHUNG IM KLARTEXT

Ein Backup, das nie zurückgespielt wurde, ist eine Annahme. Im Ernstfall zeigt sich erst dann, ob die Rücksicherung vollständig und nutzbar ist, und dann ist es zu spät, das Verfahren zu üben.

01 Ein Datenverlust tritt ein (Ransomware, Defekt, Fehlbedienung).

02 Die Wiederherstellung soll aus dem Backup erfolgen.

03 Ohne vorherigen Test zeigt sich jetzt erst, ob die Daten vollständig und nutzbar zurückkommen.

04 Fehlt etwas, ist es im Ernstfall nicht mehr zu korrigieren.

WARUM DIESE EINSTUFUNG

EINTRITTSWAHRSCHEINLICHKEIT · GERING

Die Sicherungen laufen nachweislich erfolgreich. Ein Datenverlust tritt selten ein.

AUSWIRKUNG · HOCH

Im Ernstfall hängt der gesamte Betrieb an der Wiederherstellung. Eine ungeprüfte Rücksicherung ist ein Risiko genau dann, wenn es darauf ankommt.

Gesamteinstufung Niedrig, aber als offene Nachweis-Lücke geführt. Die Wahrscheinlichkeit ist gering, die Auswirkung im Eintrittsfall hoch. Ein Restore-Test schließt die Lücke mit geringem Aufwand.

WAS FÜR DEN BETRIEB AUF DEM SPIEL STEHT

- Ungewisse Wiederherstellung im Katastrophenfall.
- Mögliche längere Ausfallzeit, wenn die Rücksicherung nicht wie erwartet funktioniert.
- Eine Backup-Investition ohne belegten Nutzen.

BEHEBUNG SCHRITT FÜR SCHRITT

01 Restore-Test durchführen — WERIXO · Tag 0 bis 30

Einen repräsentativen Job vollständig zurückspielen.

02 Ergebnis dokumentieren — WERIXO · Tag 0 bis 30

Wiederherstellungszeit und Vollständigkeit festhalten.

03 Test verankern — WERIXO + Kunde · Tag 30 bis 90

Den Restore-Test als wiederkehrenden Quartals-Prozess einplanen.

SO WEISEN WIR DEN ABSCHLUSS NACH

- [ ] Ein dokumentierter, erfolgreicher Restore-Test liegt im Prüfzeitraum vor.
- [ ] Die Wiederherstellungszeit ist bekannt und dokumentiert.
- [ ] Ein Quartals-Test ist terminiert.
- [ ] Der Folgebericht zeigt den Befund als geschlossen.

Erstmals erfasst: Mai 2026 · Status: Offen seit Erfassung

Bezug: NIS2 Art. 21 · BSI-Grundschutz CON.3 (Datensicherung)

Patches & Schwachstellen

Der Abgleich des Software-Inventars gegen den lokalen CVE-Katalog. Aufgelistet werden nur Treffer, die aus den erfassten Installationen ableitbar sind. Ein vollstaendiger Patchstand je Geraet setzt eine Endpoint-Management-Anbindung voraus.

STAND Im aktuellen Scan wurden keine bekannten Schwachstellen aus dem Software-Inventar abgeleitet.

Lokaler CVE-Katalog, ohne externen Live-Feed. Kein Treffer bedeutet nicht, dass keine Schwachstellen bestehen.

Worauf die Befunde beruhen

Jeder Befund ist nur so belastbar wie seine Quelle. Diese Seite zeigt je Quelle, wie viel sie erfasst, wie aktuell sie ist und wie verlässlich die Aussage trägt.

DATENQUELLEN, ABDECKUNG & VERTRAUEN

DATENQUELLE	ART	DATENSÄTZE	STAND	ABDECKUNG	VERTRAUEN
Endpoint-Telemetrie	Agent	14 Geräte	Mai 2026	100%	Hoch
Patch- & Versionsstand	Agent	18 Systeme	Mai 2026	100%	Hoch
Microsoft-365-Konfiguration	API	22 Identitäten	Mai 2026	100%	Hoch
Perimeter-Erreichbarkeit	Externer Scan	3 Adressen	Mai 2026	100%	Mittel
Backup-Protokolle	API	6 Jobs	Mai 2026	100%	Hoch
Netzwerk-Inventar	Scan	Kernnetz	Juni 2026	70%	Mittel

WAS DIE DATEN BELEGEN, UND WAS NICHT

Endpoint-Telemetrie	BELEGT	Schutzstatus, Scan-Stand und Echtzeitschutz je Gerät.
	GRENZE	Geräte ohne Agent sind nicht erfasst.
Patch- & Versionsstand	BELEGT	Installierte Updates und Versionsstände.
	GRENZE	Keine Aussage über aktive Ausnutzung.
Microsoft-365-Konfiguration	BELEGT	MFA-Status, Postfach- und Anmeldekonfiguration.
	GRENZE	Nur Konfiguration, keine Inhalte.
Perimeter-Erreichbarkeit	BELEGT	Von außen erreichbare Dienste und Ports.
	GRENZE	Momentaufnahme, keine Daueraufzeichnung.
Backup-Protokolle	BELEGT	Lauf und Erfolg der Sicherungen.
	GRENZE	Ohne Restore-Test kein Nachweis der Wiederherstellung.
Netzwerk-Inventar	BELEGT	Aktive Geräte im Kernnetz.
	GRENZE	Randsegmente noch nicht vollständig erfasst.

Was geprüft wurde

Der Bericht bewertet die hier aufgeführten Systeme. Ein klar abgegrenzter Scope macht nachvollziehbar, worauf sich Score und Befunde beziehen und worauf nicht.

5	49	1	kuratiert
KATEGORIEN	SYSTEME ERFASST	STANDORTE	ERFASSUNG

ERFASSTE SYSTEME

KATEGORIE	ANZAHL	BESCHREIBUNG
Arbeitsplätze	14	Windows-Clients in Büro und Fertigung
Server	4	Zwei Datei-, ein Verzeichnis-, ein Anwendungsserver
Microsoft-365-Identitäten	22	Postfächer und geteilte Konten
Perimeter-Adressen	3	Statische öffentliche IP-Adressen
Backup-Jobs	6	Täglich, lokal und an einen zweiten Ort

Der Scope umfasst die im Prüfzeitraum erfassten Systeme. Geräte ohne Agent oder außerhalb der erfassten Netze sind nicht enthalten und werden im nächsten Zyklus ergänzt.

Was von außen erreichbar ist

Drei Dienste sind aus dem Internet erreichbar. Die Tabelle ordnet jeden ein: was er ist, über welchen Port er läuft und ob er eine zweite Betrachtung verdient.

3	2	1	keine
ERREICHBARE DIENSTE	ERWARTET & ABGESICHERT	ZU PRÜFEN	AKTIVE ANGRIFFE

ERREICHBARE DIENSTE

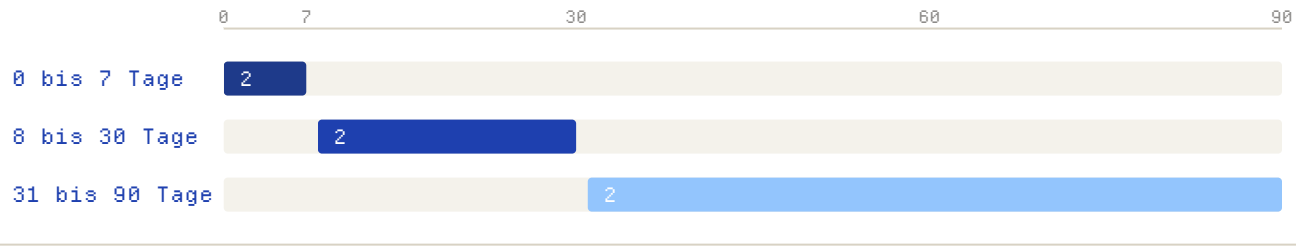
DIENST	PORT	BEWERTUNG	HINWEIS
HTTPS (Web)	443/tcp	Erwartet	Verschlüsselt, aktuelles Zertifikat.
VPN-Gateway	51820/udp	Erwartet	Zugang nur mit Schlüssel, kein offenes Login.
RDP	3389/tcp	Prüfen	Direkt erreichbar. Besser hinter das VPN legen.

Zwei der drei erreichbaren Dienste sind für den Betrieb nötig und abgesichert. Der dritte, ein direkt erreichbarer Fernzugriff, ist der Punkt mit dem größten Hebel. Aktive Angriffe auf diese Adressen wurden im Prüfzeitraum nicht beobachtet. Die Einordnung beruht auf der Erreichbarkeit, nicht auf einem konkreten Vorfall.

Der Weg nach vorn

Die Maßnahmen verteilen sich auf drei Zeitfenster, geordnet nach Dringlichkeit. Der Zeitplan zeigt, was wann greift, von der Sofortlücke bis zur dauerhaften Härtung.

ZEITPLAN ÜBER 90 TAGE



WORAUF JEDE PHASE ZIELT

0 bis 7 Tage	**Sofortmaßnahmen · 2 Maßnahmen** Die akuten Lücken schließen, bevor sie zum Vorfall werden.
8 bis 30 Tage	**Kurzfrist · 2 Maßnahmen** Wiederkehrende Prozesse verankern, damit Lücken nicht zurückkehren.
31 bis 90 Tage	**Mittelfrist · 2 Maßnahmen** Nachweise und Härtung, die den Schutz dauerhaft tragen.

Was wann ansteht

Alle Maßnahmen auf einen Blick, geordnet nach Zeitfenster. Was zuerst kommt, schließt die größte Lücke, nicht das, was am leichtesten fällt. WERIXO empfiehlt jede Maßnahme und setzt sie nach Freigabe um, der nächste Bericht weist die Wirkung nach.

0 BIS 7 TAGE Sofortmaßnahmen

2 Maßnahmen

Echtzeitschutz reaktivieren — BEFUND 01

Schließt die unmittelbarste Lücke. Ohne dauerhaften Schutz bleibt Schadsoftware bis zum nächsten Scan unbemerkt.

Patchstand der vier Server angleichen — BEFUND 02

Bekannte Schwachstellen werden geschlossen, bevor sie ausgenutzt werden können.

8 BIS 30 TAGE Kurzfrist

2 Maßnahmen

Zwei-Faktor-Anmeldung erzwingen — BEFUND 03

Drei Postfächer ohne zweiten Faktor sind das wahrscheinlichste Einfallstor. Die Pflicht schließt es.

Patch-Fenster als Prozess verankern — BEFUND 02

Ein wiederkehrendes Wartungsfenster verhindert, dass der Rückstand erneut entsteht.

31 BIS 90 TAGE Mittelfrist

2 Maßnahmen

Restore-Test der Backups durchführen — BEFUND 06

Erst eine nachgewiesene Rücksicherung macht aus dem Backup einen belastbaren Schutz.

Lokale Adminrechte zurücknehmen — BEFUND 05

Weniger dauerhafte Adminrechte begrenzen den Schaden, falls ein Konto übernommen wird.

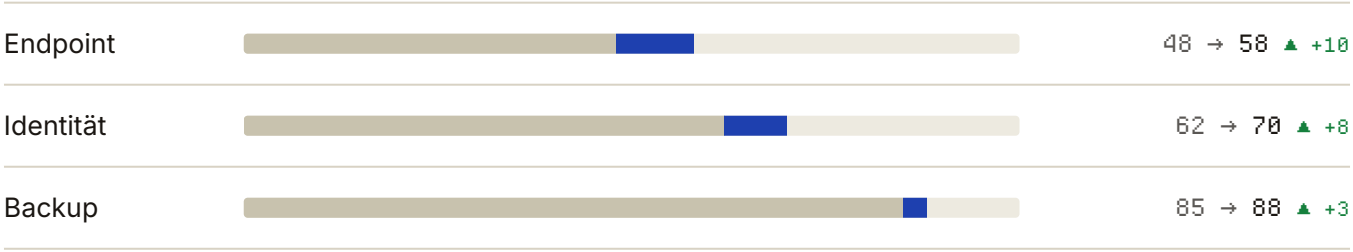
Was WERIXO bewegt hat

Seit dem letzten Bericht hat WERIXO an den damals vorrangigen Punkten gearbeitet. Der Sicherheitsindex ist in diesem Zeitraum von 68 auf 72 gestiegen.

+4	3	1	3
PUNKTE INDEX	GESCHLOSSEN	NEU HINZU	BEREICHE BEWEGT

Der Index steigt, weil drei Befunde geschlossen wurden und nur einer neu hinzukam. Der Zuwachs von vier Punkten spiegelt die Endpoint-Härtung und den Beginn der MFA-Ausrollung.

VORHER / NACHHER JE BEARBEITETEM BEREICH



ERLEDIGTE ARBEIT

- **Endpoint-Härtung umgesetzt**
  Drei zuvor offene Endpoint-Lücken geschlossen.
- **MFA-Ausrollung gestartet**
  19 von 22 Identitäten nutzen jetzt den zweiten Faktor.
- **Backup-Überwachung eingerichtet**
  Fehlgeschlagene Sicherungen werden jetzt gemeldet.

WAS DIE UMSETZUNG AUFHÄLT (LIEGT BEIM KUNDEN)

- **Wartungsfenster Server-Patches**
  Termin für das Einspielen der Server-Updates ist noch nicht freigegeben.
- **MFA für geteiltes Postfach**
  Das geteilte info@-Postfach braucht eine Entscheidung über benannte Zugänge.

Was jetzt zu entscheiden ist

Drei Entscheidungen stehen an. Jede ist eine Freigabe, kein Detailauftrag. WERIXO setzt die Umsetzung um und weist sie im nächsten Bericht nach.

FREIGABEN DER GESCHÄFTSFÜHRUNG

1 Reihenfolge der Sofortmaßnahmen freigeben

EMPFOHLEN Diese Woche

WERIXO setzt Echtzeitschutz und Patchstand im laufenden Monat um und weist die Umsetzung im nächsten Bericht nach.

OHNE ENTSCHEIDUNG Ohne Freigabe bleiben zwei Arbeitsplätze ohne aktiven Echtzeitschutz.

2 Zwei-Faktor-Pflicht für alle Postfächer beschließen

EMPFOHLEN Bis 30. Juni

Betrifft drei verbleibende Konten. Schließt das wahrscheinlichste Einfallstor.

OHNE ENTSCHEIDUNG Drei Postfächer bleiben allein mit Passwort erreichbar.

3 Wartungsfenster für Updates festlegen

Bis 15. Juli

Ein fester Termin pro Monat hält den Patchstand aktuell, ohne den Betrieb zu stören.

OHNE ENTSCHEIDUNG Der Patch-Rückstand entsteht ohne festen Rhythmus erneut.

Wie wir bewerten und was offen bleibt

Der Sicherheitsindex fasst acht Prüfbereiche zu einem Wert von 0 bis 100 zusammen. Jeder Bereich wird aus den erhobenen Daten bewertet, nicht geschätzt.

DIE 8 PRÜFBEREICHE

Sicherheit | Endpoint | Identität | Netzwerk | Backup | Speicher | Updates | Dienste

WIE DER SCORE ENTSTEHT

Jeder Bereich erhält einen Wert von 0 bis 100. Der Gesamtindex ist der gewichtete Durchschnitt, wobei offene Befunde nach Schwere abgezogen werden. Ein kritischer Befund wiegt schwerer als ein niedriger. So bildet eine Zahl den Stand ab, ohne ihn zu glätten.

Die Bewertung läuft monatlich gegen dieselben Quellen und dieselbe Baseline. Dadurch ist jeder Wert mit dem Vormonat vergleichbar, und Fortschritt wird sichtbar, statt im Bauchgefühl zu bleiben.

GRENZEN DER BEWERTUNG

01 Der Bericht bewertet den Stand zum Stichtag. Er ist eine Momentaufnahme, keine Dauerüberwachung und keine Garantie für die Zukunft.

02 Bewertet werden nur die erfassten Systeme. Geräte ohne Agent oder außerhalb der erfassten Netze fehlen und sind als Lücke benannt.

03 Der Index ist eine Orientierung, kein Prüfsiegel. Er ersetzt weder ein Audit noch eine Zertifizierung.

04 WERIXO unterstützt bei der NIS2-Vorbereitung. Der Bericht ist kein Nachweis vollständiger NIS2-Konformität und keine Rechtsberatung.

Quellen & Abdeckung

Jeder Befund ist nur so verlässlich wie seine Quelle. Diese Übersicht zeigt, welche Quellen aktiv waren und wie vollständig sie erfasst haben.

QUELLEN IM PRÜFZEITRAUM

QUELLE	STATUS	LETZTE AKTUALISIERUNG	ABDECKUNG
Endpoint-Agent	Aktiv	11. Juni 2026	14 / 14 Geräte
Microsoft-365-API	Aktiv	11. Juni 2026	22 / 22 Identitäten
Perimeter-Scan	Aktiv	10. Juni 2026	3 / 3 Adressen
Backup-API	Aktiv	11. Juni 2026	6 / 6 Jobs
Netzwerk-Inventar	Teilweise	09. Juni 2026	Kernnetz erfasst

Alle Quellen liefern unter der Marke WERIXO. Die eingesetzten Werkzeuge bleiben im Hintergrund. Eine teilweise erfasste Quelle senkt die Aussagekraft im betroffenen Bereich, sie wird offen ausgewiesen.

So geht es weiter

Der Bericht endet nicht mit einer Liste, sondern mit einem klaren nächsten Schritt. So bleibt der Schutz in Bewegung.

DIE NÄCHSTEN SCHRITTE

1 **Freigaben erteilen**
Die drei Entscheidungen aus Teil 04 freigeben.
Geschäftsführung
Diese Woche

2 **WERIXO setzt nach Freigabe um**
Echtzeitschutz, Patchstand und MFA werden nach Freigabe umgesetzt.
WERIXO
Laufender Monat

3 **Nachweis im nächsten Bericht**
Der Folgebericht zeigt die Wirkung am Index.
WERIXO
Nächster Zyklus

IHR ANSPRECHPARTNER

Fragen zur Einordnung beantwortet Ihr WERIXO-Team direkt. Eine kurze Rückmeldung zu den Freigaben genügt, den Rest übernimmt WERIXO.