

TERMIN VOR ORT	BERICHT VOM	BESPRECHUNG
12. Oktober 2026, ein halber Tag	15. Oktober 2026	20. Oktober 2026
BETRIEB	GERÄTE	BETREUUNG BISHER
18 Mitarbeiter, Büro, Lager und Werkstatt	14 Rechner und Laptops, 6 Diensthandys	Büroleitung, Dienstleister auf Zuruf

Zusammenfassung für die Geschäftsführung

Vieles läuft bei Ihnen, weil sich jemand kümmert. Nur ist kaum etwas so geregelt, dass es auch ohne diese Person funktioniert. Zwei Bereiche sind dringend: die Zugänge zu Microsoft 365 und die Datensicherung. Beides lässt sich in wenigen Wochen in Ordnung bringen, ohne große Anschaffungen. Die übrigen Punkte können Sie über die nächsten drei Monate verteilen.

Organisation und Verantwortung	● Angehen	Zuständigkeit und Vertretung sind nicht festgelegt, es gibt keine Liste der Systeme und Zugänge.
Identitäten und Zugriffe	● Dringend	Zwei-Faktor-Anmeldung nur bei 5 von 16 Konten, zwei Konten ehemaliger Mitarbeiter sind noch aktiv.
Datensicherung und Notfall	● Dringend	Die Sicherung liegt am selben Ort wie die Daten, Microsoft 365 wird gar nicht gesichert.
Netzwerk und Systeme	● Angehen	Gäste-WLAN nicht getrennt, ein alter Fernwartungszugang, kein Schutz gegen gefälschte Absender.
Endgeräte und Software	● Angehen	Zwei Rechner ohne Sicherheitsupdates, Laptops unverschlüsselt, Virenschutz-Meldungen liest niemand.
Menschen und Aufmerksamkeit	● In Ordnung	Ihre Mitarbeiter fragen bei verdächtigen Mails nach, bevor sie klicken oder bezahlen.

Was wir zuerst angehen würden

- Diese Woche:** die Konten der beiden ehemaligen Mitarbeiter sperren und die Weiterleitung an die private Adresse löschen. Danach die Zwei-Faktor-Anmeldung für alle Konten einschalten.
- In den nächsten zwei Wochen:** eine zweite Sicherung einrichten, die nicht dauerhaft am Netz hängt, und Microsoft 365 mitsichern.
- Nebenbei, in zehn Minuten:** die beiliegende Notfallkarte ausfüllen und festlegen, wer im Notfall entscheidet, wenn Sie nicht erreichbar sind.

Die sechs Bereiche im Einzelnen

Je Punkt steht, wie dringend er ist: **Dringend** heißt diese Woche, **Angehen** heißt in den nächsten drei Monaten, **Kann warten** heißt, wenn der Rest erledigt ist. **In Ordnung** steht da, wo nichts zu tun ist.

1. Organisation und Verantwortung

Angehen

- ANGEHEN** Um die IT kümmert sich die Büroleitung neben ihrer eigentlichen Arbeit. Für größere Themen gibt es einen Dienstleister, der auf Anruf kommt. Schriftlich festgelegt ist davon nichts, eine Vertretung gibt es nicht.
- ANGEHEN** Es gibt keine Übersicht, welche Systeme, Zugänge und Verträge der Betrieb hat. Das meiste weiß die Büroleitung aus dem Kopf.
- ANGEHEN** Drei Mitarbeiter nutzen ChatGPT mit privaten Konten für Angebotstexte und Mails, teils mit Namen und Adressen von Kunden. Eine Regel dazu gibt es nicht.

Was zu tun ist: eine zuständige Person und eine Vertretung benennen. Eine Liste der Systeme, Zugänge und Verträge anlegen, eine Vorlage bekommen Sie von uns. Eine kurze Regel zur KI-Nutzung: welche Werkzeuge erlaubt sind und welche Daten dort nicht hineingehören.

2. Identitäten und Zugriffe

Dringend

- DRINGEND** Die Zwei-Faktor-Anmeldung, also die Bestätigung per App beim Anmelden, ist bei 5 von 16 Konten in Microsoft 365 eingeschaltet. Bei den übrigen elf genügt ein Passwort.
- DRINGEND** Zwei Konten ehemaliger Mitarbeiter sind noch aktiv. An einem hängt eine Regel, die alle eingehenden Mails an eine private Adresse weiterleitet.
- ANGEHEN** Das Konto „buero@“ nutzen alle mit demselben Passwort, auch für drei Lieferantenportale. Wer was gemacht hat, lässt sich nicht nachvollziehen.
- ANGEHEN** Der Geschäftsführer arbeitet im Alltag mit einem Administratorkonto, also mit allen Rechten.

Was zu tun ist: die Konten der Ehemaligen sofort sperren und die Weiterleitung löschen. Die Zwei-Faktor-Anmeldung für alle einschalten, mit einer kurzen Einweisung. Das gemeinsame Konto durch ein geteiltes Postfach ersetzen, die Portalzugänge in einen Passwort-Manager. Für die Verwaltung ein eigenes Administratorkonto, das im Alltag nicht benutzt wird.

3. Datensicherung und Notfall

Dringend

- DRINGEND** Die Dateien auf dem Netzwerkspeicher im Büro werden jede Nacht gesichert, aber auf eine Festplatte, die dauerhaft am selben Gerät im selben Schrank hängt. Ein Verschlüsselungstrojaner oder ein Wasserschaden trifft beide zugleich.
- DRINGEND** Mails und Dateien in Microsoft 365 werden nicht gesichert, nur synchronisiert. Was dort gelöscht oder verschlüsselt wird, verschwindet auf allen Geräten zugleich, und der Papierkorb hält nur begrenzt.
- ANGEHEN** Beim Termin haben wir gemeinsam eine Datei aus der Sicherung zurückgeholt. Das hat in fünf Minuten geklappt. Wie lange eine komplette Wiederherstellung dauern würde, weiß niemand.
- ANGEHEN** Einen Notfallplan gibt es nicht. Die Nummer des Dienstleisters steht nur im Handy des Geschäftsführers.

Was zu tun ist: eine zweite Kopie, die nicht dauerhaft verbunden ist oder außer Haus liegt. Eine eigene Sicherung für Microsoft 365. Einmal im Jahr eine komplette Wiederherstellung üben, damit Sie wissen, wie lange Sie im Ernstfall stillstehen. Die Notfallkarte ausfüllen und dort aufhängen, wo man sie findet.

4. Netzwerk und Systeme

Angehen

- IN ORDNUNG** Der Router ist auf aktuellem Stand, Zugriffe von außen sind nicht freigegeben.
- ANGEHEN** Das Gäste-WLAN ist nicht getrennt. Handys von Besuchern und Mitarbeitern sind im selben Netz wie der Netzwerkspeicher und können ihn sehen.
- ANGEHEN** Auf einem Büro-Rechner ist noch das Fernwartungsprogramm des früheren Dienstleisters eingerichtet. Die Zugangsdaten liegen weiter bei ihm.
- ANGEHEN** Die Empfänger haben keine Anweisung von Ihnen, gefälschte Mails mit Ihrem Absender abzuweisen. Wer sich als Ihr Betrieb ausgibt, fällt dadurch schwerer auf.

Was zu tun ist: ein Gäste-WLAN einrichten, das nur ins Internet führt. Das alte Fernwartungsprogramm entfernen. Den fehlenden Eintrag gegen gefälschte Absender ergänzen, erst beobachten, dann abweisen. Die Angaben dazu stehen auf der letzten Seite für Ihren Dienstleister.

5. Endgeräte und Software

Angehen

- ANGEHEN** Zwei Rechner laufen noch mit Windows 10: die Zeiterfassung im Lager und der Rechner in der Werkstatt. Sie bekommen seit Oktober 2025 keine Sicherheitsupdates mehr.
- IN ORDNUNG** Auf den Büro-Rechnern kommen Updates automatisch und zeitnah.
- ANGEHEN** Der Virenschutz von Microsoft ist überall aktiv. Seine Meldungen sieht aber niemand, auch der Dienstleister nicht.
- ANGEHEN** Die drei Laptops im Außendienst sind nicht verschlüsselt. Geht einer verloren, sind die Daten darauf lesbar, und Sie müssten das im Zweifel als Datenpanne melden.

Was zu tun ist: die beiden Windows-10-Rechner ersetzen oder aktualisieren. Die Meldungen des Virenschutzes an eine Stelle leiten, die sie liest. Die Verschlüsselung auf den Laptops einschalten.

6. Menschen und Aufmerksamkeit

In Ordnung

- IN ORDNUNG** Im Juli hat eine Mitarbeiterin eine gefälschte Rechnung erkannt und nachgefragt, bevor bezahlt wurde. Nachfragen ist bei Ihnen normal, und das ist viel wert.
- KANN WARTEN** Eine Schulung gab es bisher nicht. Neue Mitarbeiter bekommen keine Einweisung zu Passwörtern und Mails.

Was zu tun ist: neuen Mitarbeitern am ersten Tag zehn Minuten zu Passwörtern, Mails und Nachfragen mitgeben. Eine kurze Schulung für alle kann warten, bis die dringenden Punkte erledigt sind.

Maßnahmenplan

Aufwand grob geschätzt, ohne Wartezeiten. „Dienstleister“ heißt: Ihr bisheriger Dienstleister oder wir, ganz wie Sie möchten.

Maßnahme	Aufwand	Wer
Sofort, möglichst diese Woche		
1 Konten der zwei ehemaligen Mitarbeiter sperren, Weiterleitung löschen	unter einer Stunde	Dienstleister
2 Zwei-Faktor-Anmeldung für alle 16 Konten, mit kurzer Einweisung	1 bis 2 Tage, vor allem Abstimmung	Dienstleister
3 Zweite Sicherung, die nicht dauerhaft verbunden ist oder außer Haus liegt	1 Tag	Dienstleister
4 Sicherung für Microsoft 365 (Mails, OneDrive, SharePoint)	ein halber Tag	Dienstleister
5 Notfallkarte ausfüllen, Zuständigkeit und Vertretung festlegen	eine Stunde	Sie
In den nächsten drei Monaten		
6 Komplette Wiederherstellung einmal üben, Dauer festhalten	1 Tag, außerhalb der Arbeitszeit	Dienstleister
7 Gemeinsames Konto ablösen, Passwort-Manager einführen	ein halber Tag	Dienstleister
8 Eigenes Administratorkonto für die Verwaltung	eine Stunde	Dienstleister
9 Gäste-WLAN einrichten, das nur ins Internet führt	1 bis 2 Stunden	Dienstleister
10 Fernwartungsprogramm des früheren Dienstleisters entfernen	unter einer Stunde	Sie oder Dienstleister
11 Eintrag gegen gefälschte Absender: erst vier Wochen beobachten, dann abweisen	eine Stunde, dann vier Wochen Beobachtung	Dienstleister
12 Die beiden Windows-10-Rechner ersetzen oder aktualisieren	1 Tag	Dienstleister
13 Laptops verschlüsseln	2 Stunden	Dienstleister
14 Meldungen des Virenschutzes an eine Stelle leiten, die sie liest	eine Stunde	Dienstleister
15 Liste der Systeme, Zugänge und Verträge anlegen	1 Tag	Sie, mit Vorlage
16 Regel zur KI-Nutzung festlegen und bekannt machen	eine Stunde	Sie
Kann warten		
17 Kurze Schulung zu Mails und Passwörtern für alle	eine Stunde	Dienstleister
18 Einweisung für neue Mitarbeiter am ersten Tag	zehn Minuten je Person	Sie

● Was gut läuft

- ✓ Die nächtliche Sicherung läuft, und eine Datei war beim Termin in fünf Minuten zurückgeholt.
- ✓ Die Büro-Rechner bekommen ihre Updates automatisch.
- ✓ Der Router ist aktuell, von außen ist nichts freigegeben.
- ✓ Ihre Mitarbeiter fragen bei verdächtigen Mails nach.

So geht es weiter

In der Besprechung am 20. Oktober gehen wir den Bericht mit Ihnen durch, klären Fragen und legen fest, wer was bis wann erledigt.

Umsetzen können Sie den Plan mit Ihrem bisherigen Dienstleister, selbst oder mit uns. Der Bericht gehört Ihnen.

Die Punkte unter „Sofort“ sollten bis Ende Oktober erledigt sein.

So ist dieser Bericht entstanden

Vorgespräch am 6. Oktober, etwa 20 Minuten am Telefon. Termin bei Ihnen am 12. Oktober, ein halber Tag, mit Geschäftsführer, Büroleitung und Werkstattmeister.

Angesehen haben wir gemeinsam mit Ihnen: die Verwaltung von Microsoft 365, den Netzwerkspeicher und seine Sicherung, Router und WLAN, drei Arbeitsplätze und einen Laptop als Stichprobe. Verändert haben wir dabei nichts, gescannt oder angegriffen auch nicht.

Grundlage sind die Prüfbereiche der DIN SPEC 27076. Das ist nicht der CyberRisikoCheck in der Webanwendung des BSI und kein Zertifikat. Der Bericht ist eine Momentaufnahme vom 12. Oktober 2026.

Vertraulich: Dieser Bericht ist für die Geschäftsführung bestimmt. Geben Sie ihn weiter, wenn Sie das möchten, zum Beispiel an Ihre Versicherung oder einen Kunden, der nach Ihrer IT-Sicherheit fragt.

Ihr Ansprechpartner

Samuel Kisser, Ingenius Heimdall

015678 580073 · kontakt@ingenius-heimdall.de · ingenius-heimdall.de

Technische Angaben für Ihren Dienstleister

Diese Seite ist für den, der umsetzt. Für Ihre Entscheidungen brauchen Sie sie nicht.

Microsoft 365	Business Standard, 16 lizenzierte Konten. Sicherheitsstandards aus, kein bedingter Zugriff. MFA registriert: 5 von 16. Zwei Konten ausgeschiedener Mitarbeiter aktiv, eines mit Posteingangsregel „Weiterleiten an“ externe Adresse. Automatische Weiterleitung nach außen in der Richtlinie für ausgehenden Spam erlaubt. Freigaben „Jeder mit dem Link“ in SharePoint und OneDrive erlaubt. Globaler Administrator: Konto des Geschäftsführers, im Alltag genutzt.
Datensicherung	NAS im Büro als Dateiablage, nächtliche Sicherung auf eine USB-Platte am selben Gerät, keine unveränderlichen Snapshots, keine Kopie außer Haus. Microsoft 365 ohne Sicherung. Testrücksicherung einer Datei am 12.10. erfolgreich.
Netzwerk	Router des Providers, Firmware aktuell, keine Portfreigaben. Gastzugang aus, alle Geräte einschließlich privater Handys im selben Netz wie das NAS. Fernwartungssoftware des Vordienstleisters mit unbeaufsichtigtem Zugriff auf PC-BUERO-02.
E-Mail-Domain	SPF vorhanden (Microsoft 365), DKIM in Microsoft 365 nicht aktiviert, kein DMARC-Eintrag. Vorschlag: DKIM aktivieren, dann <code>v=DMARC1; p=none; rua=mailto:...</code> für vier Wochen, Berichte auswerten, danach <code>p=quarantine</code> , später <code>p=reject</code> .
Endgeräte	2 × Windows 10 22H2 (Zeiterfassung Lager, PC Werkstatt), ohne erweiterte Sicherheitsupdates. BitLocker auf den drei Außendienst-Laptops aus. Microsoft Defender aktiv, Warnungen werden nirgends gesammelt.
KI-Werkzeuge	ChatGPT mit privaten Konten bei drei Mitarbeitern, keine Regel, kein Geschäftskonto.

Mehr zum IT-Sicherheitscheck:

ingenius-heimdall.de/it-sicherheitscheck

Ingenius Heimdall · IT-Sicherheit in Essen und im Ruhrgebiet

015678 580073 · kontakt@ingenius-heimdall.de