

Risiko- & Potential-Bericht

Dachdeckerei M. Bergmann GmbH - Musterbericht

Bewertung der IT im Hinblick auf Ausfallsicherheit und Wirtschaftlichkeit, Begehung am 31.07.2026, Bericht vom 03.08.2026

Wichtige Hinweise: Tagessätze und Materialanteil sind branchenübliche Annahmen. Im Mandat werden sie durch die Zahlen des Betriebs ersetzt. Der Musterbericht zeigt Auszüge, ausgearbeitet sind zwei Achsen und der Notfallplan.

Zusammenfassung

POTENTIAL

10.700 € p.a.

RISIKO

147.300 € im Eintrittsfall

NACHINVEST

24.460 € einmalig

ZUZÜGLICH NACHINVEST

2.050 € p.a.

Der Nachinvest von 24.460 € ist Risikovorsorge und nimmt ein Schadensszenario von 147.300 € vom Tisch. 19.000 € davon entfallen auf den Serverersatz, der bei einem acht Jahre alten Gerät ohne Herstellersupport ohnehin ansteht.

Das Potential von 10.700 € p. a. stammt aus dem Umstieg der Buchhaltung in die Cloud. Zusätzlich sinkt der einmalige Aufwand für den Ersatzrechner um 900 €. Aus dem Potential sind die laufenden 2.050 € für den Notfallplan gedeckt; netto verbleiben 8.650 € im Jahr.

Detail Bewertung

Potential / Risiko

● Infrastruktur	hohes Risiko	● Personenabhängigkeiten	moderates Potential *
● Software & Lizenzen	hohes Risiko	● Anbieterabhängigkeiten	moderates Risiko *
● Daten & DSGVO	moderates Risiko *	● Skalierbarkeit & Nachhaltigkeit	großes Potential *
● Security & Risiko	moderates Risiko *	● Schatten-IT & Prozesslücken	keine relevanten Befunde

* nicht Teil des Berichts

Größte Potentiale

Buchhaltung in die Cloud: Belegfluss, Stundenerfassung, Wartung. **10.700 €**

Größte Risiken

Server und Backup im selben Raum, Rückspielbarkeit nie geprüft. **119.900 €**

Buchhaltungsrechner ohne Sicherheitsupdates, Online-Banking läuft darauf. **27.400 €**

Kein dokumentierter Notfallplan. Verlängert jeden Ausfall um ein Vielfaches.

A1: Infrastruktur

Dachdeckerei M. Bergmann GmbH - Musterbericht

Bewertung der IT im Hinblick auf Ausfallsicherheit und Wirtschaftlichkeit, Begehung am 31.07.2026, Bericht vom 03.08.2026

R 1: Server der Software DachWerk Kalkulation

● Baujahr 2018, acht Jahre alt, Herstellersupport ausgelaufen. Standort: Werkstatt, ungekühlt, staubbelastet. Das Backup läuft auf einem NAS im selben Raum. Ein Rückspielversuch ist nicht dokumentiert. Eine USV ist vorhanden, ein Test ist nicht dokumentiert. USV-Batterien halten drei bis fünf Jahre; bei einem Gerät im Alter des Servers ist ohne Wechselnachweis von einer erschöpften Batterie auszugehen. Sie überbrückt dann nichts, sondern meldet im Ernstfall nur den Stromausfall.

Risiko: Ein Verschlüsselungstrojaner findet das NAS im selben Netz und verschlüsselt es mit. Oder der RAID-Controller eines acht Jahre alten Servers ohne Herstellersupport gibt auf. In beiden Fällen ist das Backup die einzige Rettung. Das bedeutet Totalverlust aller Aufmaße, Kalkulationen und der Kundenhistorie. Ein Backup, das nie zurückgespielt wurde, ist kein Backup.

Summe im Risikofall: 49.400 € Stillstand + 70.500 € Folgeschäden = rund 120.000 €.
Das Gewährleistungsrisiko aus bis zu fünf Jahren Bauleistung ist darin nicht enthalten.

Modellrechnung der Ausfallkurve basierend auf:

Jahresumsatz netto 2,4 Mio €, Personalstruktur 17 gewerblich (3 Kolonnen), 5 Büro/Bauleitung/GF, Produktive Arbeitstage 220 (Witterung, Winterpause), durchschnittlicher Tagesumsatz 10.900 €, Materialanteil 38 %, Vollkostensatz gewerblich / Büro 46 € / 48 € je Stunde. Bewertet wird der entgangene Deckungsbeitrag (Tagesumsatz abzüglich Materialanteil, rund 6.800 € je Tag) zuzüglich der Personalkosten, die ohne Gegenwert weiterlaufen. Die Stufen gehen in der Praxis ineinander über; jede ist deshalb am unteren Rand ihres Bereichs angesetzt und liegt bis zu zehn Prozent unter dem rechnerischen Wert. Die Modellrechnung ist damit die Untergrenze, nicht der Erwartungswert, der je nach Unternehmen unterschiedlich ist.

Im Risikofall:

Eingeschränkt arbeitsfähig: etwa 12 Arbeitstage, bis zum Normalbetrieb: 4–6 Wochen.

Tag 1-2	Büro steht. Keine Angebote, keine Rechnungen, keine Disposition. Baustellen laufen zunächst weiter.	1.900 € / Tag
Tag 3-4	Materialnachschub bricht ab, weil Bestelldaten und Aufmaße fehlen. Erste Kolonne steht.	3.800 € / Tag
Tag 5-8	Voller Stillstand. Alle Kolonnen ohne Arbeitsvorbereitung, Gerüststandzeiten laufen weiter.	6.500 € / Tag
Tag 9-12	Anlauf. Teilbetrieb auf rekonstruierter Datenbasis.	3.000 € / Tag

Womit sich die Kosten auf ~ **49.400 €** bei 12 Tagen belaufen, dazu kommen prognostizierte **70.500 €** Folgeschäden:

Ersatzserver, Lizenzen, Einrichtung, Migration.	16.000 € Ausgabe
Datenrückführung aus Fremdquellen (DATEV, Datanorm) und Nachpflege.	2.500 € Ausgabe
Wiederaufbau der betriebseigenen Kalkulationsbasis.	10.000 € Ausgabe
Nicht schlussgerechnete Leistung ohne Aufmaß.	27.000 € Verlust
Streitige Nachträge mangels Nachweis.	15.000 € Verlust

Für Bauleistungen gelten vier bis fünf Jahre Gewährleistung (je nach Vertrag). Ohne Aufmaß- und Fotodokumentation kann der Betrieb bei einem Mängelvorgang aus diesem Zeitraum nicht gehalten werden.

Sofortmaßnahmen: Backup zurückspielen testen, vom Netzwerk trennen und in einem anderen Raum lagern. Ausgaben ~ 500 €
Mittelfristig (3 Monate): neuer Server mit ausgelagertem Backup und Virtualisierung ~ 19.000 €. Zusammen 19.500 €
Die Virtualisierung sorgt dafür, dass der Rückspielvorgang auch auf abweichender Ersatzhardware gelingt. Ein ausgelagertes und geprüft rückspielbares Backup senkt die Wiederanlaufzeit von zwölf Tagen auf Stunden.

A1: Infrastruktur

Dachdeckerei M. Bergmann GmbH - Musterbericht

Bewertung der IT im Hinblick auf Ausfallsicherheit und Wirtschaftlichkeit, Begehung am 31.07.2026, Bericht vom 03.08.2026

H 1: Buchhaltung in der Cloud

● Der Buchhaltungsrechner ist Baujahr 2018, acht Jahre alt, Herstellersupport ausgelaufen. Standort: Büro. Das Backup läuft auch hier auf einem NAS. Es handelt sich nicht um dasselbe NAS wie beim DachWerk Kalkulationsserver. Ein Rückspielversuch ist auch nicht dokumentiert. Eine USV ist vorhanden, ein Test ist nicht dokumentiert. USV-Batterien halten drei bis fünf Jahre; bei einem Gerät im Alter des Servers ist ohne Wechselnachweis von einer erschöpften Batterie auszugehen. Sie überbrückt dann nichts, sondern meldet im Ernstfall nur den Stromausfall.

Hebel: Statt einen leistungsstärkeren Rechner zu kaufen, HandwerksBuha neu zu installieren und das Backupproblem zu lösen, wäre ein Umstieg auf eine Cloud möglich. Anforderungen an eine Cloud-Lösung: Rechenzentrum und Datenspeicherung in Deutschland, GoBD-konform, Backups durch den Hersteller, Exportierbarkeit, Kündigungsfristen und Übertragbarkeit des Vertrags. Idealerweise eine App, mit der sich die Handwerker projektbezogen unterwegs ein- und auschecken können. Die App sollte auch offline funktionieren und die erfassten Daten nachtragen. Die Anforderungen erfüllt z. B. HandwerksBuhaCloud.

Summe der Ersparnis: 10.700 € / p.a. + 900 € einmalig.

Modellrechnung basierend auf:

Personalstruktur 17 gewerblich (3 Kolonnen), 5 Büro/Bauleitung/GF

Vollkostensatz Büro 48 € je Stunde.

manuelle Stundenerfassung: ca. 2 Stunden / Woche für 17 Mitarbeiter.

Cloud-Abo Buchhaltung.	1.800 € / Kosten p.a.
HandwerksBuha Update- und Wartungsvertrag.	800 € / Ersparnis p.a.
entfällt: Rechnerersatz anteilig.	900 € / Ersparnis einmalig
Belegfluss zum Steuerberater digital statt Ordner.	5.500 € / Ersparnis p.a.
Stundenzettel digital statt Abtippen (17 Gewerbliche).	5.000 € / Ersparnis p.a.
geringerer Vorerfassungsaufwand in der Buchführungsgebühr.	1.200 € / Ersparnis p.a.

2.000 € p. a. Bruttoentlastung sind unmittelbar zahlungswirksam. Dem stehen 1.800 € p. a. für das Cloud-Abo gegenüber; die unmittelbare Nettoentlastung beträgt damit 200 € p. a. Die übrigen 10.500 € sind gewonnene Bürozeit von rund 220 Stunden im Jahr, etwa fünfeinhalb Arbeitswochen, bewertet mit dem Vollkostensatz Büro. Sie werden zu Geld, wenn diese Zeit anders eingesetzt wird: Angebote schreiben, Nachträge verfolgen, Aufmaße dokumentieren. Bei voller Auftragslage ist das der eigentliche Wert; bei Personalabbau wäre es eine Einsparung.

Womit sich der Hebel netto auf ~ **10.700 €** p.a. beläuft.

Statt eines leistungsstärkeren Geräts für rund 1.800 € genügt ein Modell für 900 €. Der Rechner selbst wird in Achse 2 (Software & Lizenzen) behandelt; hier fließt nur die Einsparung von **900 €** durch das schwächere Modell ein.

Sofortmaßnahmen: Das Risiko des Backups ist auch hier gegeben. Deshalb: Backup von NAS 2 zurückspielen testen, vom Netzwerk trennen und in einem anderen Raum lagern. Ausgaben ~ 500 €

Risiko: Cloud heißt neue Anbieterabhängigkeit, Daten außer Haus, ein Abo, das dauerhaft läuft, und ohne Internet steht die Buchhaltung.

A2: Software & Lizenzen

Dachdeckerei M. Bergmann GmbH - Musterbericht

Bewertung der IT im Hinblick auf Ausfallsicherheit und Wirtschaftlichkeit, Begehung am 31.07.2026, Bericht vom 03.08.2026

R 2: Buchhaltungsrechner läuft auf Windows 10

● Wie schon in H1 (Seite 3) festgehalten, ist der Buchhaltungsrechner Baujahr 2018. Er ist acht Jahre alt, der Herstellersupport ist ausgelaufen. Standort: Büro. ESU wurde nicht gebucht. Das Gerät erhält seit zehn Monaten keine Sicherheitsupdates.

Risiko: Der ungepatchte Rechner wird kompromittiert. Auf dem Gerät liegen Zahlungsverkehr, Lohn- und Personaldaten. Seit dem 14. Oktober 2025 erhält Windows 10 keine Sicherheitsupdates mehr. Auf diesem Gerät laufen Buchhaltung, Lohndaten und der Zugang zum Firmenkonto. Es ist damit das lohnendste Ziel im Betrieb und zugleich das einzige ohne aktuelle Absicherung.

Das trifft den Betrieb doppelt. Bei einer nicht autorisierten Zahlung besteht grundsätzlich ein Erstattungsanspruch. Bei einer vorsätzlichen oder grob fahrlässigen Verletzung der vereinbarten Sicherheits- und Sorgfaltspflichten kann der Betrieb jedoch für den vollständigen Schaden haften. Der Betrieb eines ungepatchten Systems verschlechtert dabei die rechtliche und tatsächliche Ausgangslage erheblich. Artikel 32 DSGVO verlangt Maßnahmen nach dem Stand der Technik. Bei einem Vorfall wird aus einem Unglück eine Pflichtverletzung. Eine Cyberversicherung kann aus demselben Grund die Leistung verweigern.

Summe im Risikofall: 27.400 € zuzüglich Bußgeld nach Art. 83 DSGVO.

ESU als Brücke bis zum Gerätetausch (Jahr 1+2 kumulativ).	160 € / Kosten einmalig
Ersatz Buchhaltungsrechner (schwächeres Modell wenn H1 umgesetzt wird).	900 € / Kosten einmalig
Umgeleitete Lieferantenzahlung, kein Erstattungsanspruch. Prognose.	18.000 € / Verlust einmalig
Forensik, Bereinigung, Neuaufsetzen.	4.000 € / Verlust einmalig
Meldung nach Art. 33 DSGVO, Information der 22 Betroffenen nach Art. 34, rechtliche Begleitung.	3.500 € / Verlust einmalig
Ausfall des Buchhaltungsarbeitsplatzes während der Bereinigung (5 Tage).	1.900 € / Verlust einmalig

Einem Nachinvest von **1.060 €** steht ein Eventualschaden von rund **27.400 €** gegenüber.

Extended Security Updates schließen die Lücke, aber nur befristet: Sie kosten pro Gerät 61, 122 und 244 US-Dollar in den Jahren eins bis drei, sind kumulativ nachzukaufen und stehen maximal drei Jahre nach dem Ende des regulären Supports zur Verfügung.

Sofortmaßnahmen: Online-Banking vom Windows-10-Rechner nehmen, bis der Ersatz da ist. Ein anderes Gerät oder das Smartphone genügt. Aufwand null, Ausgaben null.

Einschränkung: Besser ein anderer Rechner im Büro, das Smartphone nur als Übergang für ein paar Tage.

NOTFALLPLAN

Dachdeckerei M. Bergmann GmbH - Musterbericht

Bewertung der IT im Hinblick auf Ausfallsicherheit und Wirtschaftlichkeit, Begehung am 31.07.2026, Bericht vom 03.08.2026

Der Multiplikator

● **Befund:** Es existiert kein dokumentierter Notfallplan. Keine Kontaktliste, keine Wiederanlaufreihenfolge, keine Vertretungsregelung, kein hinterlegter Zugang zu Passwörtern und Lizenzen. Im Ernstfall entscheidet, wer gerade da ist und was er im Kopf hat.

Ein Notfallplan ist keine neunte Achse. Er multipliziert jede andere. Auf Seite A1 sehen Sie den Effekt in Zahlen: zwölf Tage Wiederanlauf statt weniger Stunden, weil niemand weiß, ob das Backup zurückspielbar ist und in welcher Reihenfolge was wieder laufen muss.

Maßnahmen: Ein Notfallhandbuch mit folgenden Daten anlegen und pflegen: Kontaktdaten von IT-Dienstleister, Softwarehersteller, Steuerberater und Versicherung. Welches System zuerst wieder laufen muss (z. B. Kalkulation zuerst, dann Buchhaltung). Wie lange jedes System ausfallen darf und wie viel Datenverlust tolerierbar ist. Wer entscheidet, wenn der Inhaber nicht erreichbar ist und dessen Kontaktdaten.

Summe: 3.400 € einmalig, 2.050 € p.a. - gegen ein Schadensszenario von 120.000 € allein auf Achse 1.

Modellrechnung basierend auf den Findings und Modelldaten der vorherigen Seiten.

LTE-Fallback im Router (Internetausfall).	500 € / Kosten einmalig
Mobilfunktarif für den Fallback.	450 € / Kosten p.a.
Backup außer Haus, automatisiert.	600 € / Kosten p.a.
Vorkonfigurierter Notfall-Arbeitsplatz (Laptop).	1.200 € / Kosten einmalig
USV beider Systeme prüfen, Batterien tauschen.	400 € / Kosten p.a.
Passwortsafe mit hinterlegtem Notfallzugang.	200 € / Kosten einmalig
Notfallhandbuch erstellen (pauschal rund 30 Std.).	1.500 € / Kosten einmalig
Jährliche Überprüfung der Daten und des Handbuchs, Wartung der Hard- und Software.	600 € / Kosten p.a.

Sofortmaßnahmen: Notfallkontakte auf einer Seite zusammenstellen und ausdrucken: IT-Dienstleister, Softwarehersteller, Steuerberater, Versicherung, Bank, Schlüsselmitarbeiter. Eine Kopie im Büro, eine außer Haus. Aufwand rund eine Stunde (48 €), keine Sachkosten.

Hinweis: Alternativ kann der neue Buchhaltungsrechner aus H1 die Rolle des Notfallgeräts übernehmen, wenn er als Laptop gekauft wird. Das spart 1.200 €, bringt aber zwei neue Risiken. Ein Laptop wird leichter gestohlen, wegen der Buchhaltungsdaten muss er also verschlüsselt sein, mit hinterlegtem Wiederherstellungsschlüssel im Passwortsafe. Und ein Gerät in Doppelrolle verdoppelt das Risiko: Fällt es aus, fehlt Buchhaltung und Notfallgerät zugleich. Ein separat vorgehaltenes Gerät hat dafür die umgekehrte Schwäche: es wird nie benutzt und ist im Ernstfall veraltet. Beide Wege funktionieren nur, wenn das Gerät Teil der jährlichen Übung ist und regelmäßig gewartet wird.