Rusantech

LESEPROBE

BLOG

PRAXIS-LEITFADEN / AUSGABE 2026

IT-Sicherheit im Kleinbetrieb

Acht Maßnahmen für sichere Zugänge, getestete Backups und einen klaren Notfallplan



ACHT MASSNAHMEN / 30 TAGE / BETRIEBSWERKZEUG

Gentian Rusani

blog.rusantech.de

EINSTIEG

Freitag um 16 Uhr

Bei Metallbau Linde öffnet die Büroleiterin am Freitag die Zeichnung für den ersten Auftrag am Montag. Die Datei trägt ihren üblichen Namen, lässt sich aber nicht öffnen. Der Werkstattrechner zeigt inzwischen mehrere Dateien mit veränderter Endung. Das Unternehmen hat einen Sicherungsordner. Er steht im selben Netzwerk und war über denselben Zugang erreichbar wie der Arbeitsordner.

An diesem Freitag entscheidet kein einzelnes Produkt darüber, ob die Werkstatt am Montag arbeiten kann. Das Team braucht eine Kopie von vor der Veränderung, einen Weg, sie sicher zu öffnen, und jemanden, der beurteilt, ob der betroffene Rechner wieder verwendet werden darf. Für die laufenden Aufträge braucht es eine Ersatzliste. Die Leitung muss wissen, wen sie anruft, wenn Mail und Adressbuch ausfallen.

Diese Fragen bilden den Kern dieses Leitfadens. Ihr sichert Dateien und Dienste so, dass ihr eine Rückkehr erproben könnt. Ihr prüft, welche Konten euch aus dem Betrieb aussperren könnten. Und ihr legt fest, wie Zahlungen, Geräte und Meldungen behandelt werden, wenn es schnell gehen muss.

Drei Betriebe begleiten euch durch das Buch

Metallbau Linde arbeitet mit Zeichnungen, Angebotsständen und mobilen Einsätzen. **Die Praxis am Park** braucht eine funktionsfähige Anmeldung und einen sicheren Zugriff auf ihr Fachsystem. **Das Bistro Abendbrot** hängt an Reservierungen, Kasse und dem Internetanschluss. Alle drei Betriebe, ihre Vorfälle und ihre Zahlen sind fiktiv. Die beschriebenen Entscheidungen sollen euch helfen, euren eigenen Ablauf zu prüfen.

> **Wenn gerade ein Vorfall läuft, nehmt Kapitel 8 und die Notfallkarte. Für eine geplante Verbesserung beginnt ihr auf der nächsten Seite.**

START IN 30 MINUTEN

Drei Nachweise aus eurem Betrieb

Ihr braucht eine Person, die den Alltag kennt, und eine zweite, die sie vertreten kann. Nehmt keine Einstellungen vor. Sammelt Belege für drei Fragen und schreibt jeweils auf, was fehlt. Der Unterschied zwischen „irgendwer macht das“ und einem nachweisbaren Zustand ist euer Ausgangspunkt.

Zeit	Frage	Was als Antwort taugt
00–10 Min.	Wie kommen wir an die Aufträge von gestern, wenn der Arbeitsordner ausfällt?	Ein datierter Sicherungsstand, eine zugelassene Wiederherstellungsstelle und eine zuständige Person. Ein Test folgt in Kapitel 1.
10–20 Min.	Wer kann Mail und zentrale Konten übernehmen, wenn ein Handy verloren geht?	Ein vorgesehenes Ersatzverfahren, das auf einem getrennten Weg erreichbar ist. Codes und Passwörter bleiben im dafür vorgesehenen Speicher.
20–30 Min.	Wen erreichen wir ohne Firmenmail, wenn der Rechner oder das Konto verdächtig ist?	Eine bekannte Telefonnummer, Zuständigkeit und ein zweiter Kontakt auf der gedruckten Karte.

Ordnet die Lücken nach dem nächsten Arbeitstag

Müsst ihr morgens Patienten empfangen, Einsätze disponieren oder Bestellungen bezahlen? Wählt eine Lücke, die genau diese Arbeit stoppen würde. Wenn eure einzige Sicherung am Rechner hängt und niemand eine Wiederherstellung zeigen kann, ist das ein guter erster Auftrag an die IT. Wenn die Sicherung nachweisbar funktioniert, aber ein altes Administratorkonto von außen erreichbar ist, kann dessen Absicherung zuerst dran sein.

Tragt die gewählte Lücke ins Excel-Blatt „Maßnahmen“ ein. Ergänzt einen Namen oder eine Rolle, ein Datum und den erwarteten Beleg. „Backup machen“ genügt als Aufgabe kaum. „Büro öffnet bis Donnerstag die Zeichnung von Dienstag aus einer getrennten Sicherung in einer Testablage“ kann jemand abnehmen.

DATENSICHERUNG

Der Arbeitsordner ist weg



Am Freitag hatte Linde in der Projektablage noch drei geänderte Zeichnungen und zwei neue Zusagen. Bei einer Rückkehr auf den Stand vom Donnerstag fehlen diese Änderungen. Das Büro kann zwei Zusagen anhand der freigegebenen Auftragsbestätigungen rekonstruieren. Bei der dritten Zeichnung weiß der Monteur nur, dass der Kunde ein Maß geändert hat. Der Auftrag bleibt gesperrt, bis das bestätigte Maß vorliegt.

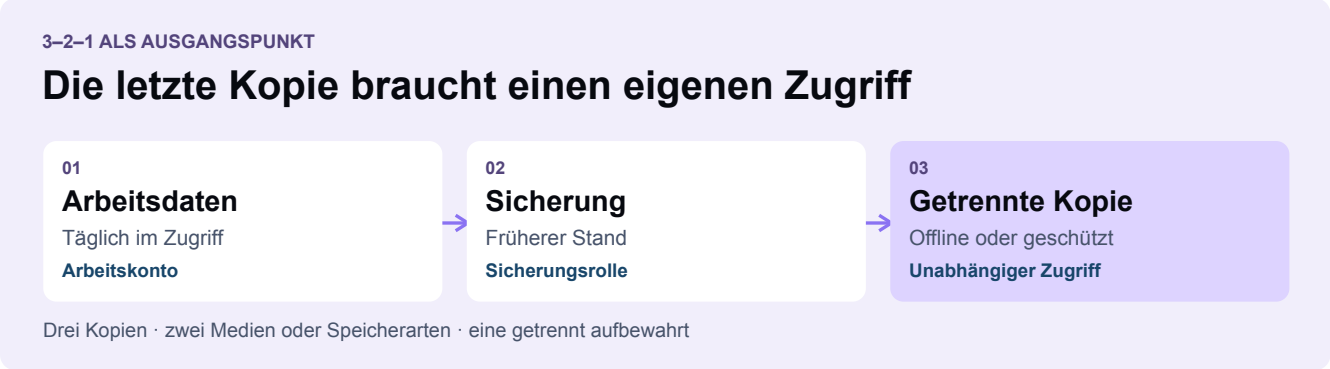
Ein brauchbares Backup besteht aus einer erreichbaren Kopie und einem Verfahren, das Daten wieder in die Arbeit bringt. Legt zuerst fest, was zurückkommen muss. Dazu können Datenbank, Anhänge, Einstellungen, Benutzerrechte, Schlüssel und Lizenzinformationen gehören. Welche Bestandteile nötig sind, hängt von der Anwendung ab. Das klärt ihr vor dem ersten Test mit dem Anbieter.

Die erste Entscheidung

Linde sichert Projektordner und Auftragsliste getrennt von der produktiven Anmeldung. Das Büro vereinbart für beide ein Ziel und prüft einen älteren Stand. Der Dienstleister dokumentiert, wie eine saubere Testumgebung aufgesetzt wird. Die Maßnahme gilt erst als belegt, wenn die Vertretung aus dem Ergebnis wieder einen Auftrag lesen kann. [1] [2]

SICHERUNGSARCHITEKTUR

Drei Kopien und ein getrennter Zugriff



Die 3-2-1-Regel beschreibt eine häufig verwendete Ausgangsbasis. Zählt die Arbeitsdaten mit und haltet insgesamt drei Kopien auf zwei unterschiedlichen Medien oder Speicherarten, davon eine an einem getrennten Ort. Für einen Angriff zählt außerdem, ob der Angreifer die Kopie verändern oder löschen kann. Ein gemeinsames Administratorkonto für Arbeitsumgebung und Sicherung schafft einen gemeinsamen Ausfallpunkt. [1] [2]

Prüft die Trennung am konkreten Zugriff

Bei Linde hängt eine Platte nur während eines geplanten Sicherungslaufs an einem dafür vorgesehenen Gerät. Eine weitere Kopie liegt getrennt und verschlüsselt. Der Schlüssel ist über den vereinbarten Notfallweg erreichbar. Bei einer Online-Sicherung kann ein getrenntes Konto und eine geschützte Aufbewahrung mit Sperre gegen frühzeitiges Löschen helfen. Prüft, wer die Sperre ändern kann und was ein Verlust des Hauptkontos bedeutet.

Wo Synchronisierung hilfreich ist

Die Synchronisierung verteilt aktuelle Dateien auf Geräte und kann Versionshistorien bieten. Wenn eine Löschung oder Verschlüsselung weitergegeben wird, seht ihr den Fehler möglicherweise überall. Verwendet die vorhandene Versionshistorie dort, wo sie einen getesteten Rückweg bietet. Für kritische Daten prüft ihr zusätzlich einen Sicherungsstand, der unabhängig vom normalen Schreibzugriff erhalten bleibt.

> **Ein dauerhaft angeschlossenes Laufwerk ist eine Kopie. Für einen Angriff braucht ihr mindestens einen erprobten Stand, den der normale Arbeitszugriff nicht einfach überschreiben kann.**

WIEDERHERSTELLUNG

Eine Datei zurückholen und prüfen

Legt im normalen Betrieb mit dem Dienstleister eine getrennte Testablage fest. Nutzt eine unkritische Musterdatei oder einen freigegebenen Testdatensatz. Wählt eine ältere Version mit einer bekannten Änderung, etwa eine Zeichnung, in der ihr auf einer Testseite ein Maß geändert habt. Haltet Versionsdatum und erwartetes Merkmal fest.

Testet vom Zugriff bis zur Öffnung

01 Die Vertretung startet die Uhr. Sie findet die Anleitung und den vorgesehenen Zugang zur Sicherung.

02 Sie wählt den richtigen Sicherungsstand. Der Rückweg führt in einen getrennten Ordner oder eine Testumgebung.

03 Sie öffnet die Datei mit dem vorgesehenen Programm. Name, Inhalt und Version stimmen mit dem erwarteten Muster überein.

04 Sie protokolliert Dauer, fehlende Rechte, Auffälligkeiten und die sichere Löschung der Testkopie nach der vereinbarten Regel.

Vermeidet einen falschen Erfolg

Eine Datei mit passendem Namen kann leer, veraltet oder beschädigt sein. Lasst eine Person aus dem Fachbereich die entscheidende Stelle öffnen. Bei einer Datenbank prüft der Dienstleister die Konsistenz und die Anwendung mit einem geeigneten Verfahren. Eine Dateiübung ersetzt diesen Systemtest nicht.

Falls der Test scheitert

Notiert genau, an welcher Station er endet. „Kein Zugriff“ kann bedeuten, dass die Rolle fehlt, der Wiederherstellungsschlüssel verloren ist oder das Programm die Datei nicht öffnen kann. Der nächste Auftrag nennt die konkrete Hürde. Wiederholt denselben Fall nach der Korrektur. Bei einem echten Verdacht auf Schadsoftware entscheidet die zuständige IT über einen geeigneten Stand und die isolierte Wiederherstellung. [1] [2] [5]

FALLAKTE R-002

38 Minuten und trotzdem keine Freigabe

FALL R-002

Zwei Zeitziele und zwei verschiedene Ergebnisse

Alter der Daten

4,5 Std.

Ziel ≤ 4 Std. Verfehlt

Zeit bis zur Öffnung

38 Min.

Ziel ≤ 6 Std. Erreicht

Beim ersten Test um 10 Uhr stellt Linde die Zeichnung nach 38 Minuten wieder her. Sie stammt von 05:30 Uhr. In der Übung fällt der Ordner um 10 Uhr aus. Der verwendbare Stand liegt damit viereinhalb Stunden zurück. Das Zeitziel für den Wiederanlauf ist erreicht. Das Vier-Stunden-Ziel für den Datenstand ist verfehlt.

Messgröße	Soll	Ist und Folge
Datenalter	Höchstens 4 Std.	4,5 Std. · Sicherungsplan prüfen
Wiederanlauf	Höchstens 6 Std.	38 Min. · im Ziel für diesen Test
Dateiinhalt	Passendes Maß, korrekte Version	In der Testumgebung geöffnet und bestätigt
Vollständigkeit	Zeichnung und aktuelle Auftragsliste	Liste im ersten Lauf nicht geprüft

So schließt das Team die Lücke

Der Dienstleister passt das Intervall an den Arbeitsrhythmus an und ergänzt die Auftragsliste im Prüfauftrag. Beim Wiederholungstest liegt der geeignete Stand 2,5 Stunden zurück. Zeichnung und Liste werden getrennt geöffnet. Die Büroleitung vermerkt, dass der Nachweis nur für diesen Umfang gilt. Eine vollständige Wiederherstellung des Rechnungsprogramms wird als eigene Übung geplant.

Wann der Erfolg verfällt

Nach Wechsel von Speicher, Sicherungsdienst, Verschlüsselung oder Zugriffsrollen wiederholt ihr die Probe. Legt auch für den laufenden Betrieb einen passenden Wiederholungstermin fest. Linde prüft stichprobenartig nach Änderungen und plant eine feste Wiederanlaufübung im Kalender. Den letzten Beleg verlinkt das Team im Blatt „Restore“.

PHISHING UND ZAHLUNGEN

Die Rechnung passt fast



Eine Materialrechnung kommt in einem bekannten E-Mail-Verlauf. Betrag, Ansprechpartner und Projekt stimmen. Neu ist nur die IBAN. Die Büroleiterin erkennt keine auffälligen Tippfehler. Sie ruft die Nummer aus dem bereits geprüften Lieferantenstamm an. Der Lieferant bestätigt, dass sich seine Bankverbindung nicht geändert hat. Das Team stoppt die Zahlung und meldet den Vorgang.

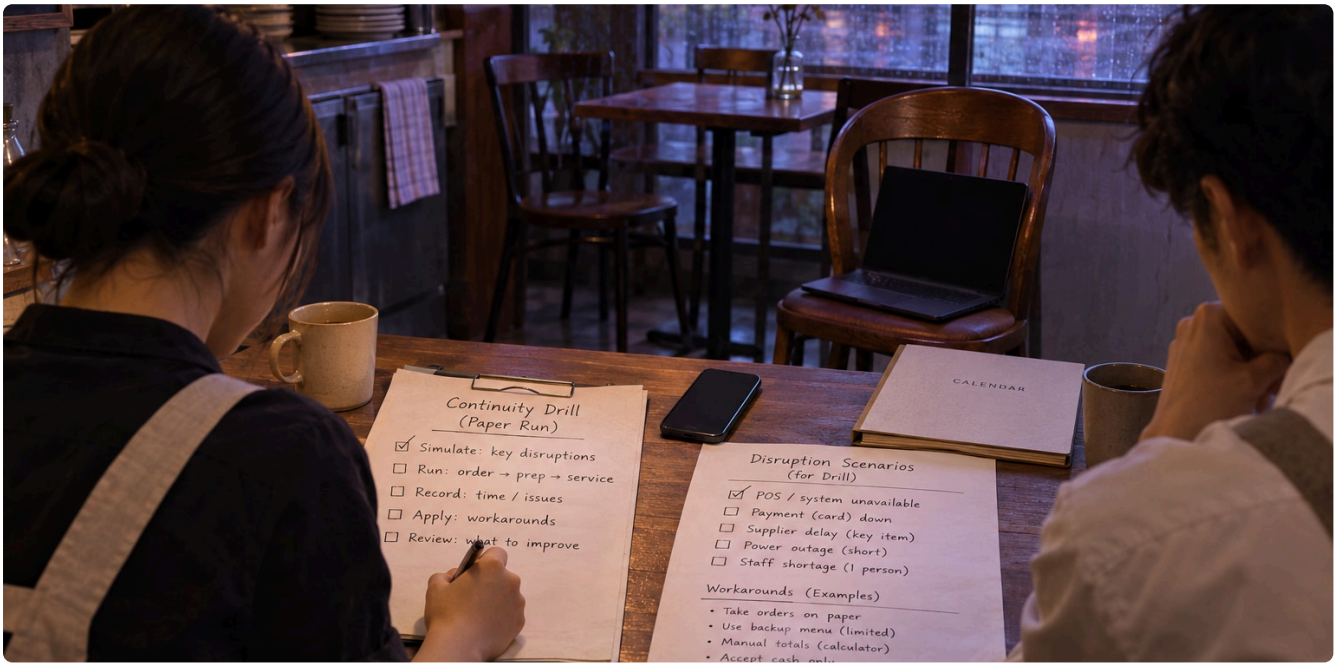
Der Fall zeigt, warum eine Regel für Änderungen zuverlässiger ist als ein Bauchgefühl bei E-Mails. Selbst echte Absenderkonten können übernommen werden. Im Zahlungsprozess zählt, ob jemand eine neue Bankverbindung über einen unabhängigen, bereits bekannten Weg verifiziert. Haltet Anlass, Zeitpunkt und Ergebnis fest, bevor ihr den Stammdatensatz ändert. [1] [9]

Drei Schritte in der Übung

Die Annahme erkennt die Änderung. Eine zuständige Person überprüft sie über den bekannten Kontakt. Die Freigabe sieht den dokumentierten Beleg. Wenn eine dieser drei Stationen fehlt, verbessert ihr den Prozess an dieser Stelle. Ob das Team die Mail als „Phishing“ einordnet, kann es danach mit der IT klären.

NOTFALLPLAN

Was ihr in den ersten Minuten entscheidet



Im Bistro fällt am Samstag vor Öffnung das Büro-Notebook aus. Der Bildschirm zeigt eine ungewöhnliche Meldung. Die Reservierungsliste liegt in einem gemeinsamen Ordner. Die Schichtleitung versucht nicht, die Ursache selbst zu finden. Sie stoppt die Arbeit am betroffenen Gerät, ruft über ihr bekanntes Telefon die zuständige IT an und beginnt ein Protokoll auf Papier.

Wählt den Weg nach der Beobachtung

Bei Verdacht auf Schadsoftware trennt ihr das betroffene Gerät nach Notfallplan und soweit sicher möglich vom Netzwerk, etwa per Kabel und WLAN. Bei einer Produktionsanlage oder einem Gerät mit Sicherheitsfunktion handelt ihr nur nach abgestimmter Anweisung. Lasst Stromzustand, Beweissicherung und weitere Abschaltung von der IT beurteilen. Bei einer Kontoübernahme ist zusätzlich die Sperre beim Dienst nötig. Bei Zahlungsbetrug zählt der schnelle Kontakt zur Bank. [2] [5]

> **Meldet kurz: Was ist passiert, wann fiel es auf, welches System ist betroffen, was habt ihr schon getan und wie seid ihr unabhängig erreichbar? Verwendet einen bekannten, möglichst nicht betroffenen Kanal.**

Rusantech

EINSATZKARTE 01

Notfallkarte am Arbeitsplatz

Druckt diese Seite aus. Ergänzt vorher die bekannten Kontaktdaten und den Ersatzweg.

Im Ernstfall die Arbeit am betroffenen Gerät stoppen und über einen sicheren Kanal melden.

Was fällt auf?	Was ihr zuerst tut
Dateien verändern sich oder das Gerät zeigt einen verdächtigen Hinweis	Nach Notfallplan sicher vom Netz trennen, wenn möglich. IT und Leitung anrufen. Nicht löschen oder aufräumen.
Fremde Anmeldung oder Passwort eingegeben	IT oder Anbieter über bekannten Kontakt erreichen. Dienst, Konto und Uhrzeit nennen.
Verdächtige oder ausgeführte Zahlung	Bank und Leitung sofort über bekannte Nummer anrufen. Buchungsreferenz bereithalten.
Dienstgerät verloren	IT und Leitung anrufen. Gerätekennung, letzte Sichtung und verknüpfte Dienste nennen.

IT und Vertretung · bekannte Rufnummern

Betriebsleitung und Vertretung

Bank oder weiterer Kontakt

Sicherer Meldeweg, falls Firmenmail ausfällt

Stand der Karte und zugriffsgerechter Ablageort

Beim Anruf: Zeitpunkt, betroffener Dienst, Beobachtung und bereits erfolgte Handlung nennen.

Rusantech

PRAXIS-LEITFADEN / BLOG

Euer nächster Sicherheitsnachweis

Öffnet eine Datei aus einer getrennten Sicherung.
Probt den Ersatzweg für ein wichtiges Konto.
Findet den Notfallkontakt ohne Firmenmail.



58 Buchseiten · 9 Excel-Blätter · 10 Einsatzkarten

Zum Rusantech Blog

Gentian Rusani · Ausgabe 2026