Busch
IT-Service GmbH

IT MADE IN GERMANY

ZUM AUSFÜLLEN, AUSDRUCKEN UND HINLEGEN

Der IT-Notfallplan

Vorlage · Ausgabe 2026

Wer macht was in den ersten 60 Minuten — festgehalten, bevor es soweit ist.

Im Ernstfall zählt nicht, wer am meisten weiß. Es zählt, wer als Erstes weiß, was zu tun ist. Füllen Sie diese Vorlage einmal in Ruhe aus, drucken Sie sie aus und legen Sie sie dorthin, wo Ihr Team sie findet — auch dann, wenn kein Rechner mehr läuft.

DIESER NOTFALLPLAN GILT FÜR

Angabe	Eintrag
Unternehmen	
Standort(e)	
Version / Stand	
Erstellt am	
Nächste Überprüfung am	
Anzahl Mitarbeitende	

VERANTWORTLICH IM NOTFALL

Rolle	Name / Funktion
Notfall-Verantwortliche/r	
Stellvertretung	
Nächste Überprüfung am	
Freigegeben durch Geschäftsführung	
Datum / Unterschrift	

WICHTIG **MINDESTENS DREI ABLAGEORTE**

1.Ausgedruckt dort, wo die Technik steht.
2. Ausgedruckt bei der oder dem Notfall-Verantwortlichen zu Hause.
3. Digital außerhalb Ihres Firmennetzes, zum Beispiel im Cloud-Speicher Ihres IT-Dienstleisters.
Ein Plan, der nur auf dem verschlüsselten Dateiserver liegt, ist im Ernstfall kein Plan.

1 So arbeiten Sie mit dieser Vorlage

IN 60 MINUTEN AUSGEFÜLLT — UND DANN LIEGEN GELASSEN

Diese Vorlage ist kein Konzept zum Lesen, sondern ein Arbeitsblatt zum Beschriften. Nehmen Sie sich eine Stunde, am besten gemeinsam mit der Person, die Ihre IT betreut. Lieber heute zu 80 Prozent fertig als nie zu 100.

So gehen Sie vor

01 Ausfüllen — mit dem, der Ihre IT kennt

Kontakte, Systeme und Prioritäten kennt selten eine Person allein. Setzen Sie sich mit Ihrem IT-Dienstleister oder Ihrer internen IT zusammen.

02 Ausdrucken und verteilen

Papier funktioniert ohne Strom, ohne Netz und ohne Anmeldung. Genau darum geht es.

03 Einmal im Jahr durchsprechen

60 Minuten am Konferenztisch: „Angenommen, heute Morgen ist alles verschlüsselt — wer ruft wen an?“ Das reicht für den Anfang. Notieren Sie das Ergebnis im Übungs-Log (Baustein 8).

04 Nach jedem Vorfall nachziehen

Jede echte Störung zeigt, was in der Liste gefehlt hat. Diese fünf Minuten sind die wertvollsten des ganzen Plans.

Die acht Bausteine

Nr.	Baustein	Inhalt	Seite
01	**Deckblatt & Geltungsbereich**	Wer verantwortet den Plan, ab wann gilt er	1
02	**Notfall-Kontaktliste**	Intern und extern — mit privaten Nummern	3–4
03	**Eskalationsmatrix**	Störung, Notfall oder Krise — und wer entscheidet	5
04	**Sofortmaßnahmen: vier Szenarien**	Die ersten 60 Minuten zum Abhaken	6–9
05	**System-Inventar**	Was hängt woran — und wie dringend ist es	10
06	**Kommunikationsplan**	Wer informiert wen, inklusive Meldefristen	11
07	**Wiederanlauf-Reihenfolge**	In welcher Reihenfolge alles zurückkommt	12
08	**Übungs-Log**	Was die letzte Übung ergeben hat	13

GRUNDLAGE Woran sich die Vorlage orientiert

Diese Vorlage orientiert sich am **BSI-Standard 200-4 (Business Continuity Management)** des Bundesamtes für Sicherheit in der Informationstechnik. Die Inhalte wurden von Busch IT-Service GmbH in eine praxisorientierte und übersichtliche Form übertragen, damit Unternehmen die wichtigsten Maßnahmen zur Vorbereitung auf IT-Notfälle einfach erfassen, umsetzen und regelmäßig überprüfen können. Der vollständige BSI-Standard ist kostenlos beim Bundesamt für Sicherheit in der Informationstechnik erhältlich

TRANSPARENZ Was diese Vorlage nicht ersetzt

Ein IT-Notfallplan ist ein wichtiger Bestandteil der betrieblichen IT-Sicherheit, ersetzt jedoch weder ein professionelles Backup- und Wiederherstellungskonzept noch technische Schutzmaßnahmen oder eine Cyberversicherung.

Er kann einen Cyberangriff oder Systemausfall nicht verhindern. Er hilft Ihrem Unternehmen jedoch dabei, im Ernstfall strukturiert zu reagieren, Ausfallzeiten zu reduzieren und die richtigen Maßnahmen einzuleiten.

2 Wen wir zuerst erreichen müssen

Tragen Sie private Mobilnummern ein, nicht nur die Durchwahl.
Im Notfall hängt das Firmen-Telefon am selben Netz wie alles andere, und das Firmen-Postfach wird oft als Erstes abgeschaltet. Klären Sie die Einwilligung der Betroffenen vorher — schriftlich, einmal.

INTERNE NOTFALL-KONTAKTLISTE

ROLLE	NAME	TEL. PRIVAT / MOBIL	E-MAIL AUSSERHALB DER FIRMA	ERREICHBAR
Geschäftsführung				
Stellvertretung GF				
Notfall-Verantwortliche/r				
Stellvertretung				
IT intern				
Datenschutz-Koordination				
Personal / Betriebsrat				
Standort 2				
Buchhaltung / Zahlungen				
Empfang / Telefonzentrale				

Spalte „Erreichbar“: Wann ist die Person realistisch erreichbar — und wer übernimmt außerhalb dieser Zeiten?

MELDEWEG WER MELDET AN WEN?

Mitarbeitende melden eine Störung an:

.....

Diese Person alarmiert bei Verdacht auf Angriff:

.....

Und außerhalb der Geschäftszeiten:

.....

FAUSTREGEL LIEBER EINMAL ZU VIEL ANRUFEN

Der häufigste Fehler in kleinen Betrieben ist nicht die falsche Maßnahme, sondern die verlorene Stunde, in der niemand jemanden anruft, weil niemand sich zuständig fühlt.

Deshalb steht auf dieser Seite genau eine Person mit Namen — und genau eine Stellvertretung.

2 Die Nummern, die Sie nicht googeln wollen

Wenn das Netz weg ist, funktioniert auch die Suche nach der Support-Hotline nicht mehr. Kunden- und Vertragsnummern gehören mit auf diese Seite — ohne sie hilft Ihnen keine Hotline weiter.

EXTERNE NOTFALL-KONTAKTLISTE

FUNKTION	FIRMA / ANBIETER	ANSPRECHPARTNER	TELEFON	KUNDEN- / VERTRAGSNR.
IT-Dienstleister (Notfall)				
Internet-Provider				
Telefonanlage / VoIP				
Rechenzentrum / Hoster				
Microsoft-365- / Cloud-Partner				
Hersteller Fachanwendung				
Cyber-Versicherung (Schaden)				
Datenschutzbeauftragte/r				
Datenschutz-Aufsichtsbehörde				
Polizei — Cybercrime (ZAC)				
Bank · Sperr-Hotline				
Steuerberatung / Lohnbüro				
Elektriker / Haustechnik				

HINWEIS **ZWEI ADRESSEN, DIE VIELE NICHT KENNEN**

Zentrale Ansprechstelle Cybercrime (ZAC): Jedes Bundesland hat eine — sie nimmt Anzeigen von Unternehmen auf und berät. Nummer einmal heraussuchen und oben eintragen.
Ihre Datenschutz-Aufsichtsbehörde richtet sich nach dem Sitz Ihres Unternehmens. Ermitteln Sie die zuständige Behörde und tragen Sie sie oben ein.

IM ERNSTFALL **KUNDEN VON Busch IT-Service GmbH**

Rufen Sie an, schreiben Sie keine E-Mail —
bei einem Angriff ist Ihr Postfach oft das erste System, das abgeschaltet wird.

Freecall **0800 203 32 02**

Busch IT-Service GmbH
Dresdener Straße 7
51067 Köln

info@busch-it.gmbh
www.busch-it.gmbh

3 Wann ist es ein Notfall?

Ohne klare Stufen passiert eines von zwei Dingen: Entweder wird jede Kleinigkeit zur Chefsache, oder ein echter Angriff wird drei Stunden lang als „Drucker klemmt wieder" behandelt. Legen Sie die Grenzen vorher fest — schriftlich.

STUFE 1

STÖRUNG

BEISPIELE
- Ein Arbeitsplatz startet nicht
- Drucker oder Scanner streikt
- Eine Anwendung ist langsam
- Ein Passwort ist gesperrt

REICHWEITE
Eine Person oder ein Gerät.
Alle anderen arbeiten weiter.

WER ENTSCHEIDET
IT-Verantwortliche/r intern.

WAS PASSIERT
Normales Ticket beim IT-Dienstleister, übliche Reaktionszeit. Keine Alarmierung.

STUFE 2

NOTFALL

BEISPIELE
- Server oder Anwendung ist weg
- Internet oder Telefon fällt aus
- Verdacht auf Schadsoftware
- Ein E-Mail-Konto verhält sich fremd

REICHWEITE
Eine Abteilung oder mehrere Personen können nicht arbeiten.

WER ENTSCHEIDET
IT-Verantwortliche/r — und informiert die Geschäftsführung sofort, nicht erst zum Feierabend.

WAS PASSIERT
Notfallnummer des Dienstleisters, passende Sofortmaßnahmen-Checkliste abarbeiten, Uhrzeiten mitschreiben.

STUFE 3

KRISE

BEISPIELE
- Verschlüsselung / Erpressung
- Daten sind abgeflossen
- Der Betrieb steht komplett
- Kunden oder Behörden sind betroffen

REICHWEITE
Das ganze Unternehmen — oder Dritte, deren Daten Sie verarbeiten.

WER ENTSCHEIDET
Geschäftsführung. Der Krisenstab tritt zusammen.

WAS PASSIERT
Meldepflichten prüfen (siehe Baustein 6), Versicherung einschalten, eine Stimme nach außen, alles protokollieren.

GRUNDREGEL **IM ZWEIFEL EINE STUFE HÖHER**

Eine zu hoch eingestufte Störung kostet ein paar Telefonate. Eine zu niedrig eingestufte Krise kostet Tage.
Niemand im Team bekommt Ärger dafür, zu früh Alarm geschlagen zu haben — schreiben Sie diesen Satz Ihren Leuten ausdrücklich auf.

UNSERE SCHWELLEN **Bei uns gilt**

Stufe 2 ab … betroffenen Personen

.....

Stufe 3 ab … Stunden Stillstand

.....

Immer sofort Stufe 3 bei

.....

KRISENSTAB **Wer sitzt am Tisch**

Leitung:

.....

Technik:

.....

Kommunikation nach außen:

.....

4 A Ransomware: Dateien sind verschlüsselt

Erkennungszeichen: Dateien lassen sich nicht mehr öffnen, haben fremde Endungen, oder auf dem Bildschirm steht eine Erpresserbotschaft. Arbeiten Sie diese Liste von oben nach unten ab.

- ☐ 01 **Betroffene Geräte sofort vom Netz trennen**
  Netzwerkkabel ziehen, WLAN ausschalten. Nicht herunterfahren — im Arbeitsspeicher stecken Spuren, die später gebraucht werden.
- ☐ 02 **Nichts löschen, nichts „aufräumen", nichts neu installieren**
  Jeder gut gemeinte Aufräumversuch vernichtet Beweise und mögliche Wiederherstellungswege.
- ☐ 03 **Notfall-Verantwortliche/n und Geschäftsführung alarmieren**
  Das ist Stufe 3. Per Telefon, nicht per E-Mail.
- ☐ 04 **IT-Dienstleister über die Notfallnummer anrufen**
  Nummer und Kundennummer stehen auf Seite 4. Uhrzeit des Anrufs notieren.
- ☐ 05 **Backups vom Netz nehmen und prüfen**
  Angreifer suchen zuerst die Sicherungen. Externe Datenträger abziehen, Zugänge zum Backup-System sperren lassen.
- ☐ 06 **Erpresserbotschaft mit dem Handy fotografieren**
  Bildschirmfoto genügt nicht, wenn das Gerät gleich vom Netz geht. Auch die Dateiendungen mitfotografieren.
- ☐ 07 **Team informieren: Geräte aus lassen**
  Keine Rechner einschalten, keine Anhänge öffnen, keine USB-Sticks tauschen, nichts nach außen kommunizieren.
- ☐ 08 **Cyber-Versicherung melden — bevor Sie Dienstleister beauftragen**
  Viele Policen verlangen die Meldung vorab und stellen eigene Spezialisten. Sonst bleiben Sie auf den Kosten sitzen.
- ☐ 09 **Anzeige erstatten und Meldepflichten prüfen**
  Zentrale Ansprechstelle Cybercrime der Polizei. Sind personenbezogene Daten betroffen, läuft die 72-Stunden-Frist (Baustein 6).
- ☐ 10 **Nicht zahlen, ohne die Geschäftsführung und die Versicherung zu fragen**
  Eine Zahlung ist eine Unternehmensentscheidung mit rechtlichen Folgen — keine technische.

ACHTUNG DER TEUERSTE REFLEX

„Erst mal alles neu aufsetzen, dann sehen wir weiter."

Danach lässt sich weder klären, wie die Angreifer hereinkamen, noch ob sie noch da sind — und die Versicherung fragt genau danach.

PROTOKOLL ERSTE BEOBACHTUNG

Wann bemerkt (Datum, Uhrzeit)

.....

Durch wen, an welchem Gerät

.....

Was war zu sehen

.....

4 B Server oder Infrastruktur ist ausgefallen

Erkennungszeichen: Mehrere Personen kommen nicht mehr an Dateien, Warenwirtschaft oder Fachanwendung. Erst klären, ob es ein Ausfall oder ein Angriff ist — davon hängt alles Weitere ab.

- ☐ 01 **Ausfall oder Angriff?**
  Fremde Dateiendungen, Erpresserbotschaft, unbekannte Benutzerkonten? Dann sofort auf Szenario A wechseln (Seite 6).
- ☐ 02 **Umfang feststellen und aufschreiben**
  Welche Systeme, welche Standorte, wie viele Personen, seit wann. Zwei Sätze auf Papier reichen — aber schreiben Sie sie.
- ☐ 03 **Vor Ort nachsehen: Strom, Notstromversorgung, Netzwerk**
  Blinkt etwas rot, piept etwas, ist es zu warm im Technikraum? Aus der Ferne sieht man das nicht.
- ☐ 04 **IT-Dienstleister informieren — mit Uhrzeit und Foto**
  Fehlermeldungen abfotografieren, bevor jemand den Bildschirm wegklickt.
- ☐ 05 **Notbetrieb starten**
  Was geht auch ohne dieses System? Auftragsannahme auf Papier, Kasse offline, Terminabsprachen per Telefon. Das Inventar auf Seite 10 sagt Ihnen, was betroffen ist.
- ☐ 06 **Mitarbeitende informieren — eine Ansage, ein Kanal**
  Was ist passiert, was funktioniert noch, wann kommt die nächste Info. Nichts ist schlimmer als zehn Flurgerüchte.
- ☐ 07 **Zusagen an Kunden prüfen**
  Welche Liefertermine, Angebote oder Termine sind heute gefährdet? Frühzeitig absagen ist besser als still verstreichen lassen.
- ☐ 08 **Wiederanlauf nach Prioritätenliste — nicht nach Lautstärke**
  Die Reihenfolge steht auf Seite 12. Sie wurde in Ruhe festgelegt, genau für diesen Moment.
- ☐ 09 **Nach der Behebung: Ursache und Datenstand dokumentieren**
  Welche Daten fehlen seit dem letzten Backup? Wer trägt sie nach — und bis wann?

VOR ORT **WO IST WAS?**

Technik-/Serverraum, Schlüssel bei

.....

Sicherungskasten / Notstrom (USV)

.....

Zugang außerhalb der Geschäftszeiten

.....

VORHER KLÄREN **DIE ZWEI ZAHLEN, DIE ZÄHLEN**

Wie lange darf dieses System ausfallen, bevor es wehtut? Und wie viel Arbeit dürfen Sie verlieren — eine Stunde, ein Tag?

Beide Zahlen bestimmen, was Ihr Backup können muss. Tragen Sie sie auf Seite 12 ein.

4 C E-Mail-Konto übernommen oder Phishing angeklickt

Erkennungszeichen: Kunden antworten auf Mails, die niemand geschrieben hat. Im Postfach fehlen Nachrichten. Es tauchen Regeln auf, die keiner angelegt hat. Oder jemand hat Zugangsdaten auf einer nachgebauten Anmeldeseite eingegeben.

- ☐ 01 **Passwort ändern — von einem anderen, sauberen Gerät**
  Wenn der Rechner selbst betroffen sein könnte, ändern Sie das Passwort nicht auf ebendiesem Rechner.
- ☐ 02 **Alle aktiven Anmeldungen beenden**
  Ein neues Passwort allein wirft niemanden hinaus, der schon angemeldet ist. Der IT-Dienstleister erzwingt die Abmeldung auf allen Geräten.
- ☐ 03 **Zwei-Faktor-Authentifizierung prüfen und aktivieren**
  Fremde Geräte oder Authenticator-Apps aus dem Konto entfernen, Telefonnummern kontrollieren.
- ☐ 04 **Posteingangsregeln und Weiterleitungen kontrollieren**
  Der Klassiker: eine Regel leitet alles mit „Rechnung" heimlich weiter und verschiebt es in den Papierkorb.
- ☐ 05 **Gesendete Nachrichten und Papierkorb durchsehen**
  Wurde in Ihrem Namen geschrieben? An wen, mit welchem Inhalt, mit welchen Anhängen?
- ☐ 06 **Zahlungen sofort stoppen und prüfen**
  Wurde eine Rechnung mit geänderter Bankverbindung verschickt oder bezahlt? Bank anrufen, Sperr-Hotline steht auf Seite 4.
- ☐ 07 **Empfänger warnen — über einen anderen Weg**
  Kurz und sachlich, am besten telefonisch: „Wir hatten heute einen Vorfall in unserem Postfach. Bitte prüfen Sie Nachrichten von uns von … bis …"
- ☐ 08 **IT-Dienstleister die Anmeldeprotokolle prüfen lassen**
  Woher kamen die Anmeldungen, wie lange lief der Zugriff, sind weitere Konten betroffen?
- ☐ 09 **Datenschutz prüfen: Sind personenbezogene Daten abgeflossen?**
  Ein fremder Zugriff auf ein Postfach mit Kunden- oder Personaldaten ist im Regelfall eine meldepflichtige Datenpanne. Baustein 6.
- ☐ 10 **Passwörter aller Dienste ändern, die an diesem Postfach hängen**
  Über „Passwort vergessen" öffnet ein übernommenes Postfach fast jede andere Tür.

PROTOKOLL BETROFFENES KONTO

Konto / Person

.....

Verdacht seit

.....

Geprüft durch

.....

WICHTIG KEINE SCHULDFRAGE IM RAUM

Wer auf eine gefälschte Mail hereingefallen ist und es sofort meldet, hat richtig gehandelt.

Betriebe, in denen dafür geschimpft wird, erfahren beim nächsten Mal erst Wochen später davon.

4 D Internet oder Provider ist ausgefallen

Erkennungszeichen: Keine Website erreichbar, Cloud-Anwendungen tot, Telefon still.
Wenn Ihre Telefonanlage über das Internet läuft — und das tut sie heute fast immer —, fällt sie mit aus.

- ☐ 01 **Reicht die Störung über Ihr Haus hinaus?**
  Über das Mobilfunknetz die Störungsseite des Providers prüfen. Nachbarbetrieb anrufen. Das spart eine Stunde Fehlersuche im eigenen Serverraum.
- ☐ 02 **Router und Firewall einmal neu starten — dokumentiert**
  Einmal, mit Uhrzeit. Nicht dreimal im Kreis, während der Dienstleister parallel misst.
- ☐ 03 **Ersatzweg aktivieren**
  Mobilfunk-Router, Handy-Hotspot oder zweiter Anschluss. Wer das erst im Ernstfall besorgt, wartet Tage.
- ☐ 04 **Festlegen, wer den Ersatzweg zuerst bekommt**
  Ein Hotspot trägt keine 30 Personen. Auftragsannahme, Kasse und Warenwirtschaft zuerst.
- ☐ 05 **Rufumleitung schalten**
  Festnetznummer auf ein Mobiltelefon umleiten — das geht meist beim Anbieter im Kundenportal, per Mobilfunk erreichbar.
- ☐ 06 **Kunden informieren**
  Kurzer Hinweis auf Anrufbeantworter und, wenn möglich, auf der Website. Eine Ersatz-Mobilnummer nennen.
- ☐ 07 **Störung offiziell melden und Ticketnummer notieren**
  Uhrzeit der Meldung mitschreiben. Das ist später die Grundlage für Entschädigung oder Vertragsgespräche.
- ☐ 08 **Nach der Rückkehr aktiv testen**
  Internet, Telefonie, VPN und Cloud-Anwendungen einzeln prüfen. „Es geht wieder" ist kein Test — und Rufumleitungen wieder abschalten.

VORBEREITET UNSER ERSATZWEG

Ersatz-Internet (Gerät, Standort, SIM/Vertrag)

.....

Rufumleitung: Ziel-Nummer

.....

Zugang zum Kundenportal des Providers bei

.....

NOTBETRIEB WAS OHNE INTERNET TROTZDEM WEITERLÄUFT

Aufträge nehmen wir an über

.....

Kasse / Kartenzahlung ersatzweise

.....

Ansage auf dem Anrufbeantworter

.....

ÜBERSEHEN ALARMANLAGE, TORE, ZEITERFASSUNG

Am Internet hängen mehr Dinge als der Bildschirmarbeitsplatz: Zutrittskontrolle, Alarmanlage, Torsteuerung, Zeiterfassung, Kartenzahlung. Notieren Sie im Inventar auf Seite 10 auch diese Systeme — sonst fehlen sie genau dann in der Liste, wenn jemand vor einem Tor steht, das nicht aufgeht.

5 Ihre Systeme — und was passiert, wenn eins fehlt

Diese Tabelle ist das Herzstück des Plans. Sie beantwortet im Ernstfall die wichtigste Frage: Womit fangen wir an? Die ersten beiden Zeilen sind Beispiele — überschreiben Sie sie.

SYSTEM / ANWENDUNG	WOZU WIRD ES GEBRAUCHT	HÄNGT AB VON	PRIORITÄT	VERANTWORTLICH
Warenwirtschaft	*Aufträge, Lieferscheine, Rechnungen*	*Server, Netzwerk, Anmeldung*	*1*	*M. Muster / IT-Dienstleister*
Zeiterfassung	*Arbeitszeiten, Lohnabrechnung*	*Internet, Cloud-Anbieter*	*3*	*Personalbüro*

LEGENDE **WAS DIE PRIORITÄTEN BEDEUTEN**

1 — Ohne das steht der Betrieb.
Muss als Erstes zurück, im Zweifel noch am selben Vormittag.

2 — Am selben Tag.
Es tut weh, aber ein halber Tag lässt sich überbrücken.

3 — Kann warten.
Innerhalb der Woche reicht.

NICHT VERGESSEN **AUCH DAS SIND SYSTEME**

Telefonanlage · E-Mail · Dateiablage · Buchhaltung · Kassensystem · CAD, Konstruktion oder Planung · Zutrittskontrolle und Alarm · Maschinensteuerung · Zeiterfassung · Website und Shop · Fernzugriff für den Außendienst.

6 Wer sagt wem was — und bis wann

Diese Tabelle ist das Herzstück des Plans. Sie beantwortet im Ernstfall die wichtigste Frage: Womit fangen wir an? Die ersten beiden Zeilen sind Beispiele — überschreiben Sie sie.

WER WIRD INFORMIERT	DURCH WEN	AUF WELCHEM WEG	BIS WANN	WAS GESAGT WIRD
Mitarbeitende				
Betroffene Kunden				
Lieferanten / Partner				
Bank				
Cyber-Versicherung				
Datenschutz-Aufsichtsbehörde			**72 Stunden**	
Betroffene Personen (DSGVO)			**Bei hohem Risiko**	
BSI (falls NIS2 gilt)			**24 Stunden**	
Polizei / ZAC				
Presse & Öffentlichkeit				

FRISTEN ZWEI UHREN, DIE KEINE VERHANDLUNGSSACHE SIND

DSGVO, Artikel 33: Sind personenbezogene Daten betroffen und besteht ein Risiko für die betroffenen Personen, müssen Sie den Vorfall **binnen 72 Stunden nach Bekanntwerden** Ihrer Datenschutz-Aufsichtsbehörde melden. Bei hohem Risiko sind zusätzlich die Betroffenen selbst zu informieren (Artikel 34). Die Uhr läuft ab dem Moment, in dem Sie Kenntnis erlangen — nicht ab dem Moment, in dem alles geklärt ist.

NIS2: Fällt Ihr Unternehmen unter die NIS2-Regulierung, kommt eine zweite Frist dazu: eine **Erstmeldung binnen 24 Stunden** an das BSI, gefolgt von einer ausführlicheren Meldung und einem Abschlussbericht. Ob Sie betroffen sind, hängt von Branche und Unternehmensgröße ab — klären Sie das einmal vorab und halten Sie das Ergebnis hier fest:

.....

VORLAGE ERSTE SPRACHREGELUNG

„Wir haben heute eine technische Störung in unseren Systemen festgestellt und arbeiten gemeinsam mit unserem IT-Dienstleister an der Klärung.
Sobald wir Genaueres wissen, melden wir uns aktiv bei Ihnen. Rückfragen bitte an *[Name, Telefon].*“

Keine Spekulation über Ursache, Schuld oder Umfang, solange nichts geprüft ist. Nichts ist teurer als eine Aussage, die Sie am nächsten Tag zurücknehmen müssen.

EINE STIMME NACH AUSSEN SPRICHT

Name, Rolle:

.....

Vertretung:

.....

Alle anderen verweisen auf:

.....

Das gilt auch für Anfragen von Journalisten und für Beiträge in sozialen Netzwerken.

7 Die Reihenfolge, in der alles zurückkommt

Im Ernstfall ruft jede Abteilung „wir zuerst“. Diese Liste entscheidet das vorher — in Ruhe und nach Abhängigkeiten, nicht nach Lautstärke

REIHENFOLGE **DIE TECHNISCHE KETTE**

Strom & Netzwerk → Anmeldung und Benutzerverwaltung → Datei- und Datenbankserver → Fachanwendungen → Arbeitsplätze → Nebensysteme. Was weiter oben steht, muss laufen, damit das Darunterliegende überhaupt starten kann.

RANG	SYSTEM	LÄUFT WIEDER NACH	SETZT VORAUS	WER MACHT ES	ERLEDIGT
1					☐
2					☐
3					☐
4					☐
5					☐
6					☐
7					☐
8					☐
9					☐
10					☐

UNSERE ZIELWERTE **WAS WIR AUSHALTEN**

Priorität-1-
Systeme müssen zurück sein nach ____ Stunden

.....

Wir dürfen höchstens ____ Stunden Arbeit verlieren

.....

Die zweite Zahl bestimmt, wie oft gesichert werden muss. Wer nur nachts sichert, verliert im schlimmsten Fall einen ganzen Arbeitstag.

EHRLICHE FRAGE **WANN HABEN SIE ZULETZT ZURÜCKGESPIELT?**

Ein Backup, das noch nie wiederhergestellt wurde, ist ein Versprechen — keine Sicherung.

Halten Sie hier fest, wann zuletzt eine echte Rückspielprobe stattgefunden hat.

Letzter Wiederherstellungstest am / durch

.....

8 Ein Plan, der nie geübt wurde, ist Papier

Sie brauchen keine Katastrophenübung. Sechzig Minuten am Konferenztisch, ein Szenario durchgesprochen, drei Lücken gefunden — das ist mehr, als die meisten Betriebe je gemacht haben.

DATUM	SZENARIO	WER WAR DABEI	WAS FUNKTIONIERT HAT	WAS GEFEHLT HAT — UND WER ES BIS WANN NACHTRÄGT

VORSCHLAG **DREI FRAGEN FÜR DIE ERSTE ÜBUNG**

1. Es ist Montagmorgen, nichts lässt sich öffnen — wer ruft als Erstes wen an?

2. Das Firmen-Postfach ist abgeschaltet: Wie erreichen wir unsere zehn wichtigsten Kunden?

3. Der Notfall-Verantwortliche ist im Urlaub. Wer übernimmt — und weiß die Person das?

DANACH **DER PLAN IST EIN LEBENDES DOKUMENT**

Nach jeder Übung und nach jedem echten Vorfall: Versionsnummer auf dem Deckblatt hochzählen, neu ausdrucken, alte Ausdrucke einsammeln.

Sonst kursieren im Ernstfall drei Fassungen mit drei verschiedenen Telefonnummern.

SIE WOLLEN DAS NICHT ALLEIN AUSFÜLLEN?

Busch IT-Service GmbH unterstützt Sie dabei, die Vorlage gemeinsam durchzugehen — Kontakte, Prioritäten und Meldewege. Für eine erste Abstimmung erreichen Sie uns über die folgenden Kontaktdaten:

0800 203 32 02
info@busch-it.gmbh
www.busch-it.gmbh

Busch IT-Service GmbH
Dresdener Straße 7
51067 Köln

Termin online auswählen

QUELLEN **GRUNDLAGE DIESER VORLAGE**

Orientiert am BSI-Standard 200-4 (Business Continuity Management) des Bundesamts für Sicherheit in der Informationstechnik — für Betriebe mit 10 bis 100 Mitarbeitenden auf ein pflegbares Format eingedampft. www.bsi.bund.de · Meldefristen nach Artikel 33 und 34 DS-GVO sowie nach der NIS2-Richtlinie.

Diese Vorlage ersetzt keine Rechtsberatung.