Argos Security

INCIDENT-READY-HANDBUCH

Vorbereitet, bevor es ernst wird.

Der komplette Werkzeugkasten für Ihren IR-Notfallplan: 20 ausfüllbare Vorlagen – von der Alarmierungskaskade bis zum Wiederanlaufplan – mit Anleitung, Beispielen und den Fragen, die jedes Incident-Response-Team in Stunde eins stellt.

20
ausfüllbare Vorlagen

7 Schritte
zum eigenen IR-Notfallplan

Stunde 1
entscheidet über den Schaden

Argos Security GmbH · Cyber Defense aus München · argos.security
Stand: Juli 2026 · Version 1.0

Im Ernstfall – IR-Hotline 24/7
+49 89 45 24 24-112

Warum dieses Handbuch?

Ob ein Cyberangriff zur Krise wird, entscheidet sich selten an der Technik – sondern daran, wie gut die ersten Stunden vorbereitet sind.

Die Zahlen sind eindeutig: Der deutschen Wirtschaft entstehen durch Angriffe jährlich Schäden von über 200 Milliarden Euro (Bitkom), ein einzelner Vorfall kostet deutsche Unternehmen im Durchschnitt mehrere Millionen Euro (IBM Cost of a Data Breach). Und doch scheitern die ersten Stunden fast nie an fehlenden Sicherheitsprodukten – sondern an fehlenden Telefonnummern, unklaren Zuständigkeiten, Backups, die niemand findet, und Meldefristen, die niemand kennt.

Genau dafür ist dieses Handbuch da. Es bündelt die 20 Dokumente, nach denen ein externes Incident-Response-Team in Stunde eins fragt – als ausfüllbare Vorlagen mit Beispielen. Alle Beispiele folgen einem durchgängigen, fiktiven Fall: der Muster Maschinenbau GmbH aus Augsburg (1.200 Mitarbeitende), die an einem Freitagmorgen um 04:15 Uhr eine Ransomware-Note auf ihrem Terminalserver entdeckt. So sehen Sie nicht nur, **was** auszufüllen ist, sondern **wie die Dokumente im Ernstfall ineinandergreifen**.

So nutzen Sie die Vorlagen

Jede Vorlage beginnt mit einer Erklärseite (Warum? Wann? Wo aufbewahren?) und einem ausgefüllten Beispiel, danach folgen die Formularblätter. Alle Felder sind elektronisch ausfüllbar – am Rechner in Acrobat, Vorschau oder im Browser – und ebenso zum Ausdrucken und handschriftlichen Ausfüllen geeignet. Drei Grundsätze gelten für das gesamte Paket:

1. **Offline verfügbar machen.**
   Drucken Sie die wichtigsten Dokumente aus und verwahren Sie sie außerhalb der IT – im Tresor, an der Pforte, zu Hause beim Krisenstab. Bei Ransomware ist das PDF auf dem Server nicht erreichbar.

2. **Pflegen statt ablegen.**
   Jede Vorlage trägt Felder für Stand, Version und nächste Prüfung. Ein veralteter Notfallplan ist gefährlicher als gar keiner – er erzeugt falsche Sicherheit. Empfohlener Rhythmus: halbjährlich.

3. **Vertraulich behandeln.**
   Netzplan, Break-Glass-Konten und Dienstleister-Zugänge sind für Angreifer ebenso wertvoll wie für Ihre Verteidiger. Die betroffenen Vorlagen tragen einen Vertraulichkeits-Hinweis – nehmen Sie ihn ernst.

Ein ehrliches Wort vorab: Diese Vorlagen machen Ihr Unternehmen messbar besser vorbereitet – und sie ersetzen keinen geübten Ernstfall. Die Erfahrung aus hunderten Einsätzen zeigt: Der Unterschied zwischen einem Plan auf Papier und einem Plan, der um 04:15 Uhr funktioniert, liegt in der Validierung durch Menschen, die den Ernstfall regelmäßig erleben. Genau dafür gibt es Partner wie Argos.

In 7 Schritten zum eigenen IR-Notfallplan

Die 20 Vorlagen sind Bausteine. In dieser Reihenfolge werden daraus ein funktionierender Notfallplan – realistisch sind dafür 4–8 Wochen neben dem Tagesgeschäft.

1. **Verantwortung klären → IR-01, IR-04**
   Besetzen Sie Krisenstab und Alarmierungskaskade – mit Vertretern und privaten Mobilnummern. Klären Sie Entscheidungsbefugnisse, bevor sie gebraucht werden: Wer darf nachts das Internet kappen?

2. **Das Wichtigste inventarisieren → IR-09, IR-10, IR-11, IR-12**
   Backups, Systeme mit Kritikalität, Netzsegmente, Notfallkonten. Der Praxistest: Könnte ein Externer allein mit diesen vier Dokumenten Ihre Umgebung verstehen? Dann sind sie gut genug.

3. **Kommunikation vorbereiten → IR-05, IR-06, IR-19**
   Ersatzkanäle einrichten (und testen!), Textbausteine für Mitarbeitende, Kunden und Presse vorformulieren, Stakeholder mit Meldefristen erfassen. Im Ernstfall formuliert niemand mehr in Ruhe.

4. **Recht & Versicherung fixieren → IR-07, IR-08, IR-13, IR-18**
   Meldepflichten mit Fristen und Zuständigen, Versicherungs-Obliegenheiten, Datenschutz-Dokumentation. Hier entscheidet Vorbereitung darüber, ob Deckung und Fristen halten – klären Sie das mit Ihrem Datenschutzbeauftragten und Rechtsbeistand.

5. **Den Ernstfall regeln → IR-02, IR-03, IR-14, IR-15, IR-17**
   Erstmaßnahmen-Checkliste und Logbuch griffbereit, Abschalt-Entscheidungen vorab freigegeben, Beweissicherung und Entscheidungsprotokoll vorbereitet. Das sind die Dokumente für 04:15 Uhr.

6. **Wiederanlauf planen → IR-16, IR-20**
   Geschäftsprozesse priorisieren (nach Umsatz und Vertragsstrafen, nicht nach Servern), IT-Reihenfolge mit Abhängigkeiten festlegen, Dienstleister-Zugänge und 24/7-Nummern erfassen.

7. **Üben, prüfen, wiederholen**
   Ein Plan, der nie geprobt wurde, ist eine Hypothese. Spielen Sie den Ernstfall mindestens jährlich durch – als Tabletop Exercise mit Krisenstab – und prüfen Sie alle Vorlagen halbjährlich auf Aktualität.

Wo ein Partner den Unterschied macht: Die Schritte 1–6 können Sie mit diesem Paket weitgehend selbst gehen. Erfahrungsgemäß lohnt sich externe Begleitung an drei Stellen: bei der **Validierung** (sind Kritikalitäten und Abhängigkeiten realistisch?), bei der **Übung** (eine professionell moderierte Tabletop Exercise deckt Lücken auf, die kein Selbsttest findet) – und bei der Frage, **wer im Ernstfall tatsächlich um 04:15 Uhr ans Telefon geht**. Ein IR-Retainer mit garantierten Reaktionszeiten und ein 24/7-SOC machen aus Ihrem Plan ein gelebtes System. Sprechen Sie mit uns – ein kostenloses 30-Minuten-Erstgespräch genügt für eine erste Standortbestimmung: **kontakt@argos.security · +49 89 45 24 24-100**

Die 20 Vorlagen im Überblick

Priorität A = Erste-Stunde-Set (im Ernstfall sofort gebraucht) · Priorität B = Tag 1 bis 3 und Vorbereitung. Alle Vorlagen folgen ab der nächsten Seite.

Nr.	Vorlage	Prio	Wofür Sie sie brauchen
IR-01	Notfall-Kontaktliste & Alarmierungskaskade	A	Wer entscheidet, wer ist Techniker – und wie erreichen wir beide, auch nachts?
IR-02	Erstmaßnahmen-Checkliste: Die ersten 60 Minuten	A	Abarbeitbare Reihenfolge für den Admin um 04:15 Uhr – verhindert forensik-zerstörende Fehler
IR-03	Incident-Logbuch & Zeitleiste	A	Wer hat wann was entdeckt und getan – Basis für Forensik, Versicherung und Meldungen
IR-04	Krisenstab-Rollenkarten	A	Acht Rollen mit Befugnissen, Vertretern und den ersten drei Handlungen je Rolle
IR-05	Out-of-Band-Kommunikationsplan	A	Kommunizieren, wenn E-Mail, Teams und Telefonanlage ausgefallen oder mitgelesen sind
IR-06	Kommunikations-Templates	A	Vorformulierte Lückentexte für Mitarbeitende, Kunden und Presse – juristisch abgewogen
IR-07	Meldepflichten-Matrix & Behördenmeldung	A	DSGVO, NIS-2, KRITIS, DORA, Versicherer: wer meldet was, wann, wohin
IR-08	Cyberversicherungs-Datenblatt & Obliegenheiten	A	Police, 24/7-Schadenhotline und die Pflichten, an denen Deckung sonst scheitert
IR-09	Backup-Übersicht	A	Sind Backups offline, getestet, wiederherstellbar? Entscheidet über Verhandeln oder Wiederherstellen
IR-10	Asset- & System-Inventar mit Kritikalität	A	Was gibt es, was ist kritisch, was hängt woran – inkl. Domains, SaaS und Log-Quellen
IR-11	Netzplan-Steckbrief	A	Segmente, Übergänge, Isolationspunkte – die Standardfrage Nr. 2 jedes IR-Teams
IR-12	Admin- & Break-Glass-Konten	A	Welche Notfallkonten existieren und wo die Zugangsdaten versiegelt liegen
IR-13	Datenschutz-Vorfall-Erfassungsbogen	B	Pflichtdokumentation nach Art. 33 Abs. 5 DSGVO inklusive Risikoabwägung
IR-14	Entscheidungsprotokoll & -Tagebuch der GF	B	Krisenentscheidungen nachvollziehbar dokumentiert – schützt die Geschäftsleitung persönlich
IR-15	Isolations- & Abschalt-Entscheidungsmatrix	B	Vorab freigegeben: Wer darf was trennen, was kostet es, wie geht es wieder an
IR-16	Dienstleister-, Vertrags- & Zugangs-Übersicht	B	Wer hat Fernzugriff (häufigster Einfallsweg), wer liefert Logs, wer ist nachts erreichbar
IR-17	Beweissicherung & Chain-of-Custody	B	Gerichtsverwertbare Beweiskette mit Hashwerten, Siegeln und Übergabeprotokoll
IR-18	Betroffenen-Benachrichtigung (Art. 34 DSGVO)	B	Prüfschema, Pflichtinhalte und neutraler Mustertext für die Benachrichtigung
IR-19	Stakeholder-Übersicht mit Meldepflichten	B	Bank, Wirtschaftsprüfer, A-Kunden: wer erfährt es von Ihnen – statt aus der Presse
IR-20	Wiederanlauf- & Notbetriebsplan	B	Geschäftsprozess-Prioritäten, manuelle Workarounds und die IT-Restore-Reihenfolge

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

Notfall-Kontaktliste & Alarmierungskaskade

Die erste Frage jedes Incident-Response-Teams lautet: **„Wer entscheidet, wer ist Techniker – und wie erreichen wir beide, wenn E-Mail und Telefonanlage ausgefallen sind?“** Diese Vorlage beantwortet sie in Sekunden statt Stunden. Einmal ausfüllen, ausdrucken, offline verwahren – halbjährlich prüfen.

Warum dieses Dokument?

Zwischen Entdeckung und arbeitsfähigem Krisenstab vergehen im Schnitt mehrere Stunden – meist durch Nummernsuche und unklare Zuständigkeiten. Mit gepflegter Kaskade ist der Krisenstab typischerweise innerhalb der ersten Stunde arbeitsfähig.

Wann brauchen Sie es?

In der ersten Stunde jedes Vorfalls – nachts, am Wochenende, im Urlaub des Erstbesetzten. Deshalb gehören private Mobilnummern und Vertreter zwingend hinein.

Wo aufbewahren?

Ausgedruckt außerhalb der IT: Tresor, Pforte, zu Hause bei jedem Kaskadenmitglied. Bei Ransomware ist das PDF auf dem Server nicht erreichbar.

So funktioniert die Alarmierungskaskade – Beispiel Stufe 3 (Verdacht Ransomware)

1. **Entdecker** – meldet telefonisch, nicht per E-Mail
2. **IT-Bereitschaft** – trennt betroffene Systeme, Rückmeldung ≤ 15 Min.
3. **IT-Leitung** – ruft Geschäftsführung und IR-Hotline parallel
4. **Krisenstab** – Lagebesprechung ≤ 60 Min., Ersatzkanal aktiv

Grundregel: Nicht erreichbar nach 2 Versuchen / 10 Minuten → Vertreter anrufen und in der Kaskade fortfahren. Kommunikation über Ersatzkanäle – der Angreifer liest im kompromittierten System möglicherweise mit.

So sieht ein ausgefüllter Eintrag aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg (fiktiv)

Rolle im Notfall	Name	Mobil dienstlich	Mobil privat	Vertretung (Name + Mobil)	Entscheidungsbefugnis
Krisenstabsleitung	K. Sommer (GF)	0151 000 001	0170 000 011	R. Ehlers · 0160 000 021	alle Abschaltungen
IT-Entscheider	T. Berger (IT-Ltg.)	0151 000 002	0171 000 012	M. Yilmaz · 0175 000 022	Netzsegment-Isolation
Datenschutz (ext. DSB)	Dr. A. Frentz	089 000 003	–	Kanzlei-Hotline 24/7	Meldung Art. 33 DSGVO

⚠ **Die Spalte „Mobil privat“ ist nicht verhandelbar.** Diensthandys hängen oft am kompromittierten Mobile-Device-Management, Firmentelefonie an der betroffenen IT. Klären Sie die Nutzung privater Nummern vorab mit Betriebsrat und Datenschutz – nur für den Notfallordner, nicht fürs Adressbuch.

Halbjährliche Prüfung: ☐ Nummern getestet ☐ Vertreter aktuell ☐ Offline-Kopien am Ort
Geprüft am: _____ von: _____

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

UNTERNEHMEN	STAND / VERSION	VERANTWORTLICH	ORT DER OFFLINE-KOPIE	NÄCHSTE PRÜFUNG

INTERNE SCHLÜSSELROLLEN IM NOTFALL

Rolle im Notfall	Name	Mobil dienstlich	Mobil privat	Vertretung (Name + Mobil)	Entscheidungsbefugnis
Krisenstabsleitung					
IT-Entscheider					
Kommunikation					
Datenschutz (DSB)					
Recht / Justiziar					
Personal / Betriebsrat					
Finanzen / Versicherung					
Betrieb / Produktion					
Protokollführung					

NOTIZEN

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

EXTERNE NOTFALLKONTAKTE

Organisation	Zweck / Kategorie	24/7-Hotline	Vertrags- / Policen-Nr.	Ansprechpartner / Stichwort
	IR-Dienstleister / SOC			
	Cyber-Versicherung			
	Rechtsbeistand IT-Recht			
	Datenschutz-Aufsichtsbehörde			
	LKA / ZAC (Zentrale Ansprechstelle Cybercrime)			
	Internet-Provider			
	Hoster / Cloud-Anbieter			
	Hausbank			

Tipp aus der Einsatzpraxis: Rufen Sie jede 24/7-Nummer einmal testweise an, bevor Sie sie eintragen. Notieren Sie das Stichwort, das die Hotline verlangt (Kunden-Nr., Police, Codewort) – das spart im Ernstfall die kritischen ersten Minuten.

NOTIZEN

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

ALARMSTUFEN

Stufe	Auslösekriterien (wann gilt diese Stufe?)	Wer darf sie ausrufen?	Wer wird alarmiert?
1 · IT-Störung			
2 · Sicherheitsvorfall			
3 · Krisenfall			

ALARMIERUNGSKETTE (REIHENFOLGE DER ANRUFE)

Nr.	Wer ruft an (Rolle)	Wen (Rolle)	Rückmeldung binnen	Wenn nicht erreichbar
1				
2				
3				
4				
5				

ERSATZKANÄLE & SAMMELPUNKTE (WENN E-MAIL / TELEFONANLAGE AUSGEFALLEN)

	Eintrag
Messenger-Ersatzkanal (Dienst, Gruppenname, Admin)	
Physischer Sammelpunkt (Raum, Schlüssel bei)	
Erste Lagebesprechung: ___ Minuten nach Alarm	
Codewort für Alarmierung (optional)	

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

Erstmaßnahmen-Checkliste: Die ersten 60 Minuten

Zwischen Entdeckung und Eintreffen externer Hilfe vergehen Stunden – in denen erfahrungsgemäß genau die Fehler passieren, die Forensik zerstören: **Server ausschalten, neu starten, Backups überschreiben, Anmeldung mit Domain-Admin auf kompromittierten Systemen.** Diese Checkliste gibt dem Admin nachts um drei eine abarbeitbare Reihenfolge – und dokumentiert zugleich, was getan wurde.

Warum dieses Dokument?

Die ersten 60 Minuten entscheiden, ob Beweise erhalten bleiben und ob sich der Angreifer weiterbewegen kann. Eine vorgedruckte Reihenfolge verhindert die typischen Panik-Fehler – und jede abgehakte Zeile ist zugleich Dokumentation.

Wann brauchen Sie es?

Sofort bei jedem Verdacht, noch bevor externe Hilfe eintrifft – gedacht für die Person, die den Vorfall entdeckt oder als Erste alarmiert wird.

Wo aufbewahren?

Ausgedruckt im Notfallordner neben Kontaktliste (IR-01) und Logbuch (IR-03): Tresor, Pforte, Bereitschaftstasche. Bei Ransomware ist die digitale Ablage nicht erreichbar.

Die vier Grundregeln der ersten Stunde

1. **Trennen, nicht ausschalten** – Netzkabel/WLAN/Port, Zustand fotografieren
2. **Alarmieren** – Kaskade nach IR-01, telefonisch – nicht per E-Mail
3. **Backups schützen** – vom Netz trennen, Replikation stoppen
4. **Dokumentieren** – jede Maßnahme mit Uhrzeit ins Logbuch IR-03

Grundregel: Keine Anmeldung mit privilegierten Konten auf verdächtigen Systemen – jede Anmeldung liefert dem Angreifer möglicherweise frische Zugangsdaten.

So sieht ein ausgefüllter Eintrag aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg (fiktiv) · Vorfall MM-2026-001: Ransomnote auf TS-02, Freitag 04:15 Uhr

Erl.	Maßnahme	Uhrzeit	Durchgeführt von	Bemerkung
☑	2. Nicht ausschalten, nicht neu starten – betroffene Systeme nur vom Netz trennen, Zustand fotografieren	04:22	M. Yilmaz	TS-02 Netzwerkkabel gezogen; Foto der Ransomnote per privatem Handy (IMG_0041)
☑	4. Backups prüfen und sofort vom Netz trennen / Replikation stoppen	04:31	M. Yilmaz	Veeam-Repository per Switchport deaktiviert; letzte Sicherung Do 23:00 intakt

⚠ **Warum nicht ausschalten?** Im Arbeitsspeicher liegen Schlüssel und Spuren, die das IR-Team braucht – ein ausgeschalteter Server verliert diese flüchtigen Beweise unwiederbringlich. Die Trennung vom Netz stoppt den Angreifer genauso, erhält aber den Zustand.

Halbjährliche Prüfung: ☐ Punkte an eigene Umgebung angepasst ☐ Offline-Kopien am Ort ☐ mit IT-Bereitschaft geübt
Geprüft am: _____ von: _____

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

UNTERNEHMEN	STAND / VERSION	VERANTWORTLICH	ORT DER OFFLINE-KOPIE	NÄCHSTE PRÜFUNG

INCIDENT-NR.	DATUM	BLATT-NR.

SOFORTMASSNAHMEN – IN DIESER REIHENFOLGE ABARBEITEN

Erl.	Maßnahme	Uhrzeit	Durchgeführt von	Bemerkung
☐	**1.** Ruhe bewahren, Logbuch beginnen (IR-03), Uhrzeit notieren			
☐	**2.** Nicht ausschalten, nicht neu starten – betroffene Systeme nur vom Netz trennen (Kabel/WLAN/Switchport); Zustand fotografieren (Bildschirm, Ransomnote)			
☐	**3.** Alarmierungskette auslösen (IR-01) – telefonisch, nicht per E-Mail			
☐	**4.** Backups prüfen und sofort vom Netz trennen, Replikation stoppen – bevor sie verschlüsselt oder überschrieben werden			
☐	**5.** Keine Anmeldung mit privilegierten Konten (Domain-Admin!) auf verdächtigen Systemen			
☐	**6.** Isolations-Matrix anwenden (IR-15): Was wird getrennt, wer entscheidet?			

⚠ **Uhrzeiten von EINER Referenzuhr nehmen** (z. B. Ihr Mobiltelefon) und jede Zeile sofort ausfüllen – nicht abends aus dem Gedächtnis. Die Checkliste wird später Teil der Beweiskette.

SOFORTMASSNAHMEN (FORTSETZUNG)

Erl.	Maßnahme	Uhrzeit	Durchgeführt von	Bemerkung
☐	**7.** Externe Zugänge sperren: VPN, RDP, Wartungszugänge von Dienstleistern			
☐	**8.** Kommunikation nicht über potenziell kompromittierte Systeme (E-Mail!) – Ersatzkanal aus IR-01 nutzen			
☐	**9.** Kein Kontakt zu Erpressern, nichts löschen, keine Lösegeld-Entscheidung ohne Krisenstab			
☐	**10.** Beweise sichern: nichts „aufräumen“, keine Virenscans mit automatischer Löschung starten			

UNTERNEHMENSSPEZIFISCHE PUNKTE (BEI DER VORBEREITUNG ERGÄNZEN)

Erl.	Maßnahme	Uhrzeit	Durchgeführt von	Bemerkung
☐				
☐				
☐				
☐				
☐				

NOTIZEN

Incident-Logbuch & Zeitleiste

Das Logbuch ist das erste Dokument, das der IR-Leiter aufschlägt: Es rekonstruiert, **was wann von wem entdeckt, entschieden und getan wurde** – Grundlage für Forensik, Versicherung, die 72-Stunden-Meldung nach Art. 33 DSGVO und spätere Gerichtsverwertbarkeit. Ohne Logbuch widersprechen sich nach 48 Stunden die Erinnerungen aller Beteiligten.

Warum dieses Dokument?

Forensik, Versicherung und Behörden fragen zuerst nach der Zeitleiste. Und: Wer dokumentieren muss, handelt überlegter – das Logbuch diszipliniert in der hektischsten Phase.

Wann brauchen Sie es?

Ab der ersten Minute jedes Vorfalls – Eintrag Nr. 1 ist die Entdeckung. Danach jede Beobachtung, Maßnahme, Entscheidung und externe Kommunikation, fortlaufend nummeriert.

Wo aufbewahren?

Mehrere Blanko-Blätter ausgedruckt im Notfallordner – mit Klemmbrett und Kugelschreiber. Handschriftlich ist völlig okay; digital ist im Ransomware-Fall oft nichts erreichbar.

So bleibt die Zeitleiste verwertbar

1. **Eine Referenzuhr** – alle Uhrzeiten von derselben Uhr, Zeitzone notieren
2. **Sofort eintragen** – nicht abends aus dem Gedächtnis rekonstruieren
3. **Beweis referenzieren** – Foto-Nr., Datei, Screenshot – und wo es abgelegt ist
4. **Blatt abschließen** – Schreiber + Blatt-Nr. eintragen, nächstes Blatt beginnen

Grundregel: Lieber zu viel als zu wenig – auch „nichts Neues seit 14:00“ ist ein Eintrag. Streichungen nur durchstreichen, nie unkenntlich machen.

So sieht ein ausgefülltes Logblatt aus

BEISPIEL – Muster Maschinenbau GmbH (fiktiv) · Incident „MM-2026-001 Ransomware“, Blatt 1, Schreiber: T. Berger

Nr.	Zeit (MESZ)	Ereignis / Maßnahme	Typ	System	Von / Entschieden von
1	05.06. 04:15	Ransomnote „readme.txt“ auf TS-02 entdeckt	Beob.	TS-02	M. Yilmaz
2	05.06. 04:22	TS-02 vom Netz getrennt (Kabel), Foto IMG_0041	Maßn.	TS-02	M. Yilmaz
3	05.06. 04:48	Entscheidung: Internet-Breakout getrennt	Entsch.	FW-01	T. Berger / GF telefonisch
4	05.06. 05:10	Cyber-Versicherung Hotline informiert, Vorgangs-Nr. 88-1234	Komm.	–	K. Sommer

⚠ **Handschriftlich ist okay – lieber zu viel als zu wenig.** Uhrzeiten von EINER Referenzuhr nehmen (z. B. ein bestimmtes Mobiltelefon) und die Zeitzone auf jedem Blatt vermerken. Abweichende Systemuhren sind einer der häufigsten Gründe, warum Zeitleisten vor Versicherung und Gericht wackeln.

Halbjährliche Prüfung: ☐ genügend Blanko-Blätter im Ordner ☐ Klemmbrett + Stift dabei ☐ Referenzuhr festgelegt
Geprüft am: _____ von: _____

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

UNTERNEHMEN	STAND / VERSION	VERANTWORTLICH	ORT DER OFFLINE-KOPIE	NÄCHSTE PRÜFUNG

INCIDENT-BEZEICHNUNG	INCIDENT-NR.	BLATT-NR.	SCHREIBER DES BLATTES	ZEITZONE

LOGBUCH – EIN EINTRAG PRO ZEILE, FORTLAUFEND NUMMERIERT

Nr.	Datum + Uhrzeit	Ereignis / Beobachtung / Maßnahme	Typ	System / Konto	Durchgef. / gemeldet von	Entschieden von	Beweismittel (wo abgelegt?)
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				

Typ: **B** = Beobachtung · **M** = Maßnahme · **E** = Entscheidung · **K** = Kommunikation extern | Bei Entscheidungen immer „Entschieden von" ausfüllen.

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

INCIDENT-BEZEICHNUNG	INCIDENT-NR.	BLATT-NR.	SCHREIBER DES BLATTES	ZEITZONE

LOGBUCH – EIN EINTRAG PRO ZEILE, FORTLAUFEND NUMMERIERT

Nr.	Datum + Uhrzeit	Ereignis / Beobachtung / Maßnahme	Typ	System / Konto	Durchgef. / gemeldet von	Entschieden von	Beweismittel (wo abgelegt?)
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				

Typ: **B** = Beobachtung · **M** = Maßnahme · **E** = Entscheidung · **K** = Kommunikation extern | Bei Entscheidungen immer „Entschieden von“ ausfüllen.

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

INCIDENT-BEZEICHNUNG	INCIDENT-NR.	BLATT-NR.	SCHREIBER DES BLATTES	ZEITZONE

LOGBUCH – EIN EINTRAG PRO ZEILE, FORTLAUFEND NUMMERIERT

Nr.	Datum + Uhrzeit	Ereignis / Beobachtung / Maßnahme	Typ	System / Konto	Durchgef. / gemeldet von	Entschieden von	Beweismittel (wo abgelegt?)
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				

Typ: **B** = Beobachtung · **M** = Maßnahme · **E** = Entscheidung · **K** = Kommunikation extern | Bei Entscheidungen immer „Entschieden von“ ausfüllen.

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

Krisenstab-Rollenkarten – Besetzung, Befugnisse, erste Handlungen

Der Krisenstab scheitert selten am Fachwissen – er scheitert daran, dass in den ersten Stunden niemand weiß, **wer welche Entscheidung treffen darf**. Diese Rollenkarten definieren acht feste Rollen mit Aufgaben, Befugnissen, den ersten drei Handlungen und je zwei Vertretern. So ist auch ein Vertreter, der zum ersten Mal einspringt, sofort arbeitsfähig.

Warum dieses Dokument?

In den ersten sechs Stunden weiß ohne Rollenkarten niemand, wer sprechen, abschalten oder beauftragen darf. Jede Karte beantwortet das vorab – inklusive der drei ersten Handlungen nach Alarmierung.

Wann brauchen Sie es?

Sobald Alarmstufe 3 ausgerufen ist. Die Karten werden in der ersten Lagebesprechung verteilt – auch an Vertreter, die die Rolle noch nie ausgeübt haben.

Wo aufbewahren?

Ausgedruckt im Notfallordner und im Krisenraum. Jedes Stabsmitglied erhält seine eigene Karte zusätzlich nach Hause – der Ernstfall beginnt nachts.

So sieht eine ausgefüllte Rollenkarte aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg (fiktiv) · Rollenkarte „Kommunikation“

ROLLE Leitung Krisenkommunikation — Besetzung: S. Weber (Leiterin Marketing & Kommunikation) · Vertretung: J. Roth, K. Steiner

Aufgaben: Sprachregelung erstellen und fortschreiben; alle internen/externen Texte freigeben (Vier-Augen-Prinzip mit Recht); Presseanfragen bündeln – niemand außer GF und ihr spricht mit Medien; Social-Media-Kanäle beobachten; Mitarbeiter-Info mindestens 1× täglich, auch wenn es nichts Neues gibt („Kein Update ist auch ein Update“).

Entscheidungsbefugnis: Freigabe aller Texte bis Stufe „Holding Statement“; Interviews nur mit GF-Freigabe. **Berichtet an:** Krisenstabsleitung (K. Sommer, GF).

Erste drei Handlungen: 1. Templates aus IR-06 ziehen, Mitarbeiter-Erstinfo binnen 2 Stunden über die Ersatzkanäle (IR-05) verbreiten. 2. Empfang und Zentrale briefen: Anfragen notieren, nichts bestätigen, Rückruf zusagen. 3. Monitoring starten (Google, LinkedIn, Branchenpresse).

⚠ **Die Protokollführung wird immer vergessen – und ist die Rolle, die hinterher Anwaltshonorare spart.** Versicherer, Wirtschaftsprüfer und Behörden fragen Monate später, wer wann was auf welcher Grundlage entschieden hat. Besetzen Sie die Rolle ab Minute eins – und planen Sie Ablösung: Krisen dauern länger als ein Wochenende.

Halbjährliche Prüfung: ☐ Besetzung aktuell ☐ beide Vertreter benannt ☐ Karten verteilt
Geprüft am: _____ von: _____

UNTERNEHMEN	STAND / VERSION	VERANTWORTLICH	ORT DER OFFLINE-KOPIE	NÄCHSTE PRÜFUNG

ROLLE 1 Krisenstabsleitung

i. d. R. Geschäftsführung / Vorstand · berichtet an: Gesellschafter / Beirat

Aufgaben: beruft den Krisenstab ein und leitet jede Lagebesprechung · trifft Grundsatzentscheidungen (Abschaltungen, Lösegeld-Frage – nie ohne Recht und Versicherer) · priorisiert Geschäftsprozesse (IR-20) · spricht neben der Kommunikation als Einziger mit Medien · hält Gesellschafter und Bank informiert.

+ weitere Aufgabe

Entscheidungsbefugnis bis ___ EUR bzw. entscheidet über

Erste Handlung nach Alarmierung – 1.

2.

3.

Besetzung	Name	Funktion im Normalbetrieb	Mobil dienstlich	Mobil privat
Hauptbesetzung				
Vertreter 1				
Vertreter 2				

ROLLE 2 IT- / Forensik-Koordination

berichtet an: Krisenstabsleitung

Aufgaben: leitet die technische Eindämmung · einzige Schnittstelle zum externen IR-Team · setzt Isolations-Entscheidungen um und dokumentiert sie · sichert Beweise und Logs (nichts löschen, nichts neu aufsetzen ohne Freigabe) · steuert den IT-Wiederanlauf nach Freigabe je System (IR-20, Teil B).

+ weitere Aufgabe

Entscheidungsbefugnis bis ___ EUR bzw. entscheidet über

Erste Handlung nach Alarmierung – 1.

2.

3.

Besetzung	Name	Funktion im Normalbetrieb	Mobil dienstlich	Mobil privat
Hauptbesetzung				
Vertreter 1				
Vertreter 2				

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

ROLLE 3 Recht & Datenschutz

inkl. 72-h-Meldung Art. 33 DSGVO · berichtet an: Krisenstabsleitung

Aufgaben: prüft und überwacht alle Meldepflichten (Art. 33/34 DSGVO, NIS-2, Verträge) – dokumentiert den Fristbeginn · steuert externe Kanzlei und Datenschutzbeauftragten · berät bei der Lösegeld-Frage (u. a. sanktionsrechtliche Prüfung) · gibt alle Texte juristisch frei (Vier-Augen-Prinzip mit Kommunikation) · begleitet Beweissicherung.

+ weitere Aufgabe

Entscheidungsbefugnis bis ___ EUR bzw. entscheidet über

Erste Handlung nach Alarmierung – 1.

2.

3.

Besetzung	Name	Funktion im Normalbetrieb	Mobil dienstlich	Mobil privat
Hauptbesetzung				
Vertreter 1				
Vertreter 2				

ROLLE 4 Kommunikation (intern + extern)

einziger Freigeber für Texte · berichtet an: Krisenstabsleitung

Aufgaben: erstellt die Sprachregelung und schreibt sie fort (IR-06) · gibt alle internen/externen Texte frei (Vier-Augen mit Recht) · bündelt Presseanfragen – niemand sonst spricht mit Medien · beobachtet Social Media und Branchenpresse · Mitarbeiter-Info mindestens 1× täglich („Kein Update ist auch ein Update“).

+ weitere Aufgabe

Entscheidungsbefugnis bis ___ EUR bzw. entscheidet über

Erste Handlung nach Alarmierung – 1.

2.

3.

Besetzung	Name	Funktion im Normalbetrieb	Mobil dienstlich	Mobil privat
Hauptbesetzung				
Vertreter 1				
Vertreter 2				

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

ROLLE 5 HR / Betriebsrat-Schnittstelle

berichtet an: Krisenstabsleitung

Aufgaben: informiert den Betriebsrat früh und fortlaufend · regelt Arbeitszeiten, Schichten und Freistellungen im Notbetrieb · zentrale Anlaufstelle für Mitarbeiterfragen („Was heißt das für meinen Arbeitsplatz?“) · organisiert die Telefonketten mit (IR-05) · beobachtet die Stimmung in der Belegschaft und meldet sie in die Lagebesprechung.

+ weitere Aufgabe

Entscheidungsbefugnis bis ___ EUR bzw. entscheidet über

Erste Handlung nach Alarmierung – 1.

2.

3.

Besetzung	Name	Funktion im Normalbetrieb	Mobil dienstlich	Mobil privat
Hauptbesetzung				
Vertreter 1				
Vertreter 2				

ROLLE 6 Betrieb / Produktion

berichtet an: Krisenstabsleitung

Aufgaben: bewertet die Auswirkungen auf Produktion, Lager und Lieferungen · aktiviert die manuellen Workarounds (IR-20, Teil A) · meldet Puffer, Liefertermine und drohende Vertragsstrafen in die Lagebesprechung · koordiniert Werkschutz, Standorte und Frühschicht-Information · stimmt Wiederanlauf-Prioritäten aus Betriebssicht ab.

+ weitere Aufgabe

Entscheidungsbefugnis bis ___ EUR bzw. entscheidet über

Erste Handlung nach Alarmierung – 1.

2.

3.

Besetzung	Name	Funktion im Normalbetrieb	Mobil dienstlich	Mobil privat
Hauptbesetzung				
Vertreter 1				
Vertreter 2				

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

ROLLE 7 Finanzen (Liquidität & Versicherung)

berichtet an: Krisenstabsleitung

Aufgaben: meldet den Schaden unverzüglich an den Cyber-Versicherer – **vor** Beauftragung externer Dienstleister (Kostenübernahme!) · sichert Liquidität und Zahlungsverkehr über Bank-Notverfahren · dokumentiert alle Kosten und Schäden für die Regulierung · hält Kontakt zu Bank und Wirtschaftsprüfer (mit GF) · prüft Lohnlauf-Termine.

+ weitere Aufgabe

Entscheidungsbefugnis bis ___ EUR bzw. entscheidet über

Erste Handlung nach Alarmierung – 1.

2.

3.

Besetzung	Name	Funktion im Normalbetrieb	Mobil dienstlich	Mobil privat
Hauptbesetzung				
Vertreter 1				
Vertreter 2				

ROLLE 8 Protokollführung / Dokumentation

führt das Entscheidungs-Tagebuch · berichtet an: Krisenstabsleitung

Aufgaben: führt das Entscheidungs-Tagebuch der Geschäftsleitung ab Minute eins · protokolliert jede Lagebesprechung mit Zeitstempel und Informationslage („Was wussten wir, was nicht?“) · notiert auch verworfene Alternativen · sammelt Belege für Versicherer und Prüfer · erinnert den Stab an Wiedervorlagen und offene Folgeaktionen.

+ weitere Aufgabe

Entscheidungsbefugnis bis ___ EUR bzw. entscheidet über

Erste Handlung nach Alarmierung – 1.

2.

3.

Besetzung	Name	Funktion im Normalbetrieb	Mobil dienstlich	Mobil privat
Hauptbesetzung				
Vertreter 1				
Vertreter 2				

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

SITZUNGSRHYTHMUS & VERTRETUNGSREGELN

	Eintrag
Lagebesprechung in der Anfangsphase: alle ___ Stunden	
Ab Tag 3: Rhythmus und feste Uhrzeiten	
Vertretungsregel (wann übernimmt der Vertreter, wie wird übergeben?)	
Ort / Kanal der Lagebesprechung (physisch + Ersatzkanal aus IR-05)	

ABLÖSUNGSPLAN AB STUNDE ___ (SCHICHTBETRIEB – KRISEN DAUERN LÄNGER ALS EIN WOCHENENDE)

Schicht	von – bis (Uhrzeit)	Leitung der Schicht	Kernbesetzung (Rollen)
Schicht 1			
Schicht 2			
Schicht 3			

Tipp aus der Einsatzpraxis: Planen Sie die Ablösung am ersten Tag, nicht am dritten. Übermüdete Entscheider treffen ab Stunde 20 messbar schlechtere Entscheidungen – und genau diese Entscheidungen werden später von Versicherern und Prüfern seziert.

PFLEGEVERMERK

Stand vom	Nächste Prüfung	Verantwortlich

NOTIZEN

Out-of-Band-Kommunikationsplan

Legt fest, wie Ihr Unternehmen intern und extern kommuniziert, wenn **E-Mail, Teams, Telefonanlage und Intranet ausgefallen oder kompromittiert** sind. Der wichtigste Grundsatz steht in diesem Dokument ganz oben: Über potenziell kompromittierte Systeme wird nicht über den Vorfall gesprochen – der Angreifer liest möglicherweise mit.

Warum dieses Dokument?

Bei Ransomware fallen erfahrungsgemäß E-Mail, Messenger und VoIP-Telefonie gleichzeitig aus – genau dann, wenn am meisten kommuniziert werden muss. Ersatzkanäle funktionieren nur, wenn sie vorher eingerichtet und getestet sind.

Wann brauchen Sie es?

Ab Minute eins jedes Vorfalls: Der Krisenstab kommuniziert von Anfang an über den Ersatzkanal – auch wenn die Firmen-IT noch zu laufen scheint. Ob sie sauber ist, weiß zu diesem Zeitpunkt niemand.

Wo aufbewahren?

Ausgedruckt im Notfallordner und bei jedem Krisenstabsmitglied zu Hause. Die Messenger-Gruppe wird heute eingerichtet, nicht im Ernstfall – dann fehlen die Nummern.

Die Kanal-Kaskade: Für jeden Zweck drei Wege – erst wenn einer ausfällt, kommt der nächste

1	→	2	→	3
Primärkanal der normale Weg – nur wenn nachweislich sauber		**Ersatzkanal 1** außerhalb der Firmen-IT: Signal/Threema, private Mobilnummern		**Ersatzkanal 2** Telefonkette, Aushang, Sammelpunkt, Statusseite

Grundregel: Im Zweifel gilt die gesamte Firmen-IT als mithörbar. Krisenstab-Interna laufen ausschließlich über Kanäle außerhalb der eigenen Infrastruktur – bis das IR-Team Entwarnung gibt.

So sieht ein ausgefüllter Plan im Einsatz aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg (fiktiv) · Vorfall MM-2026-001

Als am Freitag um 04:15 Uhr die Ransomnote auf dem Terminalserver TS-02 entdeckt wurde, waren auch Exchange und Teams betroffen; die VoIP-Telefonanlage fiel um 05:02 Uhr aus. Der Krisenstab kommunizierte ab Minute eins über die vorab eingerichtete Signal-Gruppe „MM-Krisenstab“ (12 Mitglieder, Admin: S. Weber). Die 34 Führungskräfte wurden über drei Telefonketten (Kettenstarter: Werkleiter, Vertriebsleiter, Verwaltungsleiter – jeweils private Mobilnummern) bis 07:30 Uhr erreicht. Für Kunden wurde die vorbereitete Mobilnummer +49 160 … freigeschaltet und die Ansage der toten Telefonanlage beim Provider auf den vorformulierten Text umgestellt: „Aufgrund einer technischen Störung sind wir derzeit eingeschränkt erreichbar. In dringenden Fällen erreichen Sie uns unter …“. Die Belegschaft der Frühschicht wurde per Aushang am Werkstor und um 9 Uhr in der Kantine informiert.

⚠ **Über kompromittierte Systeme wird nicht über den Vorfall gesprochen.** Der Angreifer liest im gekaperten E-Mail-System möglicherweise mit – und erfährt so Ihre Gegenmaßnahmen, Ihre Versicherungssumme und Ihre Verhandlungslinie. Alles Vorfallbezogene läuft über die Ersatzkanäle dieses Plans.

Halbjährliche Prüfung: ☐ Messenger-Gruppe getestet ☐ Telefonketten geübt ☐ Ansagetext hinterlegt
Geprüft am: _____ von: _____

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

UNTERNEHMEN	STAND / VERSION	VERANTWORTLICH	ORT DER OFFLINE-KOPIE	NÄCHSTE PRÜFUNG

KANAL-MATRIX – WER WIRD IM AUSFALL WIE ERREICHT?

Zielgruppe / Zweck	Primärkanal	Ersatzkanal 1	Ersatzkanal 2	Verantwortlich	Vorbereitet?
Krisenstab intern					☐
Führungskräfte					☐
Alle Mitarbeiter					☐
Kunden					☐
Öffentlichkeit / Presse					☐
					☐

MESSENGER-GRUPPE DES KRISENSTABS (AUSSERHALB DER FIRMEN-IT)

	Eintrag
Dienst (z. B. Signal, Threema – nicht der Firmen-Messenger!)	
Gruppenname	
Administrator + Vertreter (Name, Mobil privat)	
Mitglieder = Krisenstab vollständig? ☐ eingerichtet am	
Verifizierungsregel bei Neuaufnahme (woran erkennen wir, dass die Nummer wirklich zum Kollegen gehört?)	

Tipp aus der Einsatzpraxis: Senden Sie einmal im Quartal eine Testnachricht in die Gruppe („Funktionstest, keine Aktion nötig“). So fallen ausgeschiedene Mitglieder, gewechselte Nummern und stumme Geräte auf – vor dem Ernstfall, nicht in ihm.

TELEFONKETTEN (JE ABTEILUNG / BEREICH EINE ZEILE)

Abteilung / Bereich	Kettenstarter (Name)	Mobil privat	Anzahl Glieder	Letzter Test am

EXTERNE ERREICHBARKEIT IM AUSFALL

	Eintrag
Ersatz-Rufnummer für Kunden (Mobil/Prepaid, wer verwahrt das Gerät?)	
Umleitung/Ansage der Telefonanlage: wer stellt sie beim Provider um?	
Externe Statusseite / Domain außerhalb der eigenen Infrastruktur	
Wer pflegt die Statusseite (Name + Zugang von wo)?	

VORFORMULIERTER ANSAGETEXT (LÜCKEN HEUTE FÜLLEN)

„Aufgrund einer technischen Störung sind wir derzeit eingeschränkt erreichbar. In dringenden Fällen erreichen Sie uns unter _____ . Bestellungen und Liefertermine bearbeiten wir – bitte haben Sie etwas Geduld. Aktuelle Informationen finden Sie unter _____ . Vielen Dank für Ihr Verständnis.“

⚠ **Der Ansagetext nennt bewusst keine Ursache.** „Technische Störung“ genügt – alles Weitere entscheidet die Kommunikation nach der Sprachregelung (IR-06). Hinterlegen Sie den Text heute beim Telefonanbieter, damit er im Ernstfall per Anruf aktiviert werden kann.

PHYSISCHE KANÄLE

Eintrag
Schwarze Bretter (Standorte, wer hängt aus?)
Werkstor- / Eingangs-Aushang (wer, Vorlage wo?)
Ort für Betriebsversammlung / Schichtinfo (z. B. Kantine, Uhrzeit-Regel)
Empfang / Zentrale: Sprachregelung liegt aus? Wer brieft?

PHYSISCHER SAMMELPUNKT DES KRISENSTABS

Eintrag
Krisenraum (Gebäude, Raum, Ausstattung: Whiteboard, LTE-Router, Drucker)
Schlüssel / Zugang bei
Ausweichort außerhalb des Standorts
Erste Lagebesprechung: ____ Minuten nach Alarmierung

OFFLINE-REGELN

Regel	Umgesetzt?
Ausdruck dieses Plans + Notfall-Kontaktliste bei jedem Krisenstabsmitglied zu Hause, Stand: _____	☐
Notfallordner (IR-01 bis IR-06) an der Pforte / im Tresor, außerhalb der IT	☐
Private Mobilnummern mit Betriebsrat/Datenschutz abgestimmt (nur Notfallordner)	☐
LTE-Router / Ersatz-Laptops gelagert und getestet (nicht domänengebunden)	☐

NOTIZEN

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

Kommunikations-Templates für Mitarbeiter, Kunden, Presse

Vorformulierte, juristisch abgewogene Lückentexte für die drei kritischsten Zielgruppen – plus eine Sprachregelungs-Seite. Im Ernstfall müssen nur noch Fakten eingesetzt werden: **Tonalität, Struktur und die heiklen Nicht-Aussagen** (keine Spekulation, keine Schuldzuweisung, keine Täterbenennung) sind bereits eingebaut.

Warum dieses Dokument?

Unter Druck bei null anzufangen produziert die Fehler, die später zitiert werden: Spekulation, voreilige Entwarnung, Täterbenennung. Mit Templates bleibt nur noch Einsetzen und Freigeben.

Wann brauchen Sie es?

Mitarbeiter-Erstinfo binnen 2 Stunden, Kunden-Info am ersten Tag, Holding Statement sobald die erste Presseanfrage eingeht – und die kommt oft schneller als die Forensik.

Wo aufbewahren?

Ausgedruckt im Notfallordner, digital auf einem nicht domänengebundenen Gerät der Kommunikation. Jeder Text durchläuft vor Versand die Freigabe-Zeile am Blattende.

So klingen die ausgefüllten Templates

BEISPIEL – Muster Maschinenbau GmbH, Augsburg (fiktiv) · Vorfall MM-2026-001

TEMPLATE C – AUSGEFÜLLTES PRESSE-HOLDING-STATEMENT

„Die Muster Maschinenbau GmbH ist am 13. März Ziel eines IT-Sicherheitsvorfalls geworden. Unsere IT-Systeme wurden umgehend vorsorglich vom Netz getrennt, um Schaden zu begrenzen. Wir arbeiten mit externen IT-Forensikern zusammen und haben die zuständigen Behörden, darunter das Landeskriminalamt, eingeschaltet. Die Produktion läuft in einem geordneten Notbetrieb weiter. Zum Umfang des Vorfalls und zu betroffenen Daten können wir zum jetzigen Zeitpunkt keine gesicherten Angaben machen; wir informieren, sobald belastbare Erkenntnisse vorliegen. Pressekontakt: presse@muster-mb.de, +49 821 …“

TEMPLATE A – ERSTER SATZ DER MITARBEITER-ERSTINFO

„Liebe Kolleginnen und Kollegen, wir haben heute Nacht einen Angriff auf unsere IT-Systeme festgestellt. Bitte lasst alle Rechner ausgeschaltet, bis eure Führungskraft grünes Licht gibt – das ist keine Übung, aber auch kein Grund zur Sorge um eure Arbeitsplätze. Wir informieren euch heute um 14 Uhr am Schwarzen Brett und über die Telefonkette erneut.“

⚠ **Der Halbsatz zu den Arbeitsplätzen ist Gold wert.** Die Belegschaft denkt am ersten Tag nicht an Daten – sie denkt an ihren Job. Und: Jeder Text verlässt das Haus erst nach der Freigabe-Zeile (Kommunikation + Recht + Krisenstabsleitung). Ein-Sprecher-Prinzip – alle Presseanfragen laufen über eine Person.

UNTERNEHMEN	STAND / VERSION	VERANTWORTLICH	ORT DER OFFLINE-KOPIE	NÄCHSTE PRÜFUNG

WIR SAGEN … (VERBINDLICHE FORMULIERUNGEN)

	Formulierung
1	„IT-Sicherheitsvorfall“ – nicht „Hackerangriff“, nicht „Katastrophe“
2	„Die Untersuchung läuft“ – solange nichts forensisch gesichert ist
3	„Wir haben externe Spezialisten hinzugezogen“
4	
5	
6	

WIR SAGEN NICHT … (ROTE LINIEN)

	Tabu-Formulierung – und warum
1	Nicht „Hackerangriff durch [Gruppe]“ – keine Täterbenennung, solange nichts bestätigt ist
2	Nicht „alle Daten sind sicher“, solange unbestätigt – voreilige Entwarnung fällt auf das Unternehmen zurück
3	Keine Spekulation über Ursache, Umfang oder Schuldige – auch nicht „off the record“
4	
5	

EIN-SPRECHER-PRINZIP

	Name + Mobil (privat)
Sprecher (einziger Ansprechpartner für Medien)	
Stellvertretung	
Interviews nur mit Freigabe durch	

Empfang und Zentrale gehören zur Sprachregelung: Anfragen notieren, nichts bestätigen, Rückruf zusagen. Dieser Dreisatz liegt ausgedruckt am Empfang – er ist die häufigste undichte Stelle der ersten Stunden.

TEMPLATE A – MITARBEITER-ERSTINFO (BINNEN 2 STUNDEN, ÜBER ERSATZKANÄLE AUS IR-05)

Vor dem Ausfüllen: nur Gesichertes nennen · keine Spekulation über Ursache oder Täter · den Satz zur Arbeitsplatz-Sicherheit nicht streichen – er nimmt der Belegschaft die größte Sorge des ersten Tages.

Liebe Kolleginnen und Kollegen,

am _____ um _____ Uhr haben wir Folgendes festgestellt (1 Satz, nur Gesichertes):

_____

Was wir sofort getan haben: _____

_____

Was das für dich heißt:

1. Rechner und Systeme: _____
2. Kommunikation läuft bis auf Weiteres über: _____
3. Bitte keine Auskünfte an: _____

Das ist keine Übung – aber auch kein Grund zur Sorge um eure Arbeitsplätze. Wir informieren euch offen und regelmäßig, auch wenn es nichts Neues gibt.

Nächstes Update: um _____ Uhr, über/am _____

Ansprechpartner für Fragen: _____

Freigegeben durch: Kommunikation ☐ Recht ☐ Krisenstabsleitung ☐ Uhrzeit: _____ Versandkanal: _____

TEMPLATE B – KUNDEN-INFO (TAG 1; A-KUNDEN MIT VERTRAGLICHER MELDEFRIST ZUERST – SIEHE IR-19)

Vor dem Ausfüllen: Versand über einen Ersatzkanal, wenn E-Mail kompromittiert sein kann · keine Zusagen zu Daten („prüfen wir derzeit“ ist die ehrliche Antwort) · feste nächste Info zusagen und einhalten.

Betreff: _____

Sehr geehrte Damen und Herren,

wir informieren Sie über einen IT-Sicherheitsvorfall in unserem Haus. Sachstand (2 Sätze):

_____

_____

Auswirkung auf Ihre Aufträge / Ihre Daten (oder: „prüfen wir derzeit“):

_____

Was wir tun: _____

Ihr Ansprechpartner: _____ erreichbar über (Ersatzkanal!): _____

Wir informieren Sie spätestens binnen _____ Stunden erneut – auch wenn es keinen neuen Sachstand gibt.

Freigegeben durch: Kommunikation ☐ Recht ☐ Krisenstabsleitung ☐ Uhrzeit: _____ Versandkanal: _____

⚠ **Prüfen Sie vor dem Versand die vertraglichen Meldefristen** (IR-19): Rahmenverträge von A-Kunden enthalten oft Meldepflichten binnen 24 Stunden – wer zu spät informiert, verwandelt einen IT-Vorfall in einen Vertragsverstoß.

TEMPLATE C – PRESSE-HOLDING-STATEMENT (SOBALD DIE ERSTE ANFRAGE EINGEHT)

Vor dem Ausfüllen: bestätigen, was ohnehin sichtbar ist – mehr nicht · Sofortmaßnahmen und eingeschaltete Stellen zeigen Handlungsfähigkeit · die „Keine-Angaben-zu“-Zeile diszipliniert jede Nachfrage · Muster: siehe Seite 1.

Die _____ ist am _____ Ziel eines IT-Sicherheitsvorfalls geworden.

Bestätigung des Vorfalls (1 Satz, nur Gesichertes):

_____

Sofortmaßnahmen: _____

_____

Eingeschaltete Stellen (Behörden, Forensik): _____

Zum jetzigen Zeitpunkt können wir keine Angaben machen zu:

_____

Wir informieren, sobald belastbare Erkenntnisse vorliegen.

Pressekontakt: _____

Freigegeben durch: Kommunikation ☐ Recht ☐ Krisenstabsleitung ☐ Uhrzeit: _____ Versandkanal: _____

⚠ **Ein Holding Statement ist kein Interview.** Es wird schriftlich verschickt, wörtlich und vollständig – und es gilt, bis der Krisenstab eine neue Fassung freigibt. Telefonische Nachfragen beantwortet ausschließlich der benannte Sprecher mit genau diesem Text.

FREIGABE- & VERSAND-PROTOKOLL (JEDE VERSENDETE FASSUNG EINE ZEILE)

Datum / Uhrzeit	Text / Template + Version	Zielgruppe	Freigegeben durch (K / R / KSL)	Versandkanal	Versendet durch

Warum ein Versand-Protokoll? Monate später fragen Versicherer und Aufsichtsbehörden, wer wann welche Information erhalten hat. Dieses Blatt beantwortet die Frage in einer Minute – und verhindert, dass zwei Fassungen desselben Textes parallel kursieren.

NOTIZEN

Meldepflichten-Matrix & Behördenmeldung

Im Ernstfall beantwortet diese Matrix in Minuten: **„Wer muss was, wann, an wen melden?“** Sie verhindert die zwei teuersten Fehler nach einem Cybervorfall – verpasste Fristen und vergessene Meldewege. Die Vorbereitungsbögen (Blätter 4–6) sammeln alle Angaben, die die Meldeportale abfragen.

Stand: Juli 2026 – aktuelle Rechtslage prüfen

Warum dieses Dokument?

Meldepflichten laufen parallel: DSGVO, NIS-2, Police, Verträge. Vorab ausgefüllt wird die Matrix zur Abhakliste statt zur Rechtsrecherche im Ernstfall.

Wann brauchen Sie es?

Sofort nach Bekanntwerden – die 72-h-Frist der DSGVO läuft ab Bekanntwerden, nicht ab forensischer Bestätigung. Die NIS-2-Frühwarnung sogar binnen 24 h.

Wo aufbewahren?

Ausgedruckt im Notfallordner, hinter der Kontaktliste (IR-01). Die Vorbereitungsbögen als Kopiervorlage – pro Vorfall ein frischer Satz.

Die NIS-2-Meldekette ans BSI – drei Fristen, ein Vorfall

1. **Frühwarnung – binnen 24 h**
   Erstinformation: Verdacht auf rechtswidrige Handlung? Grenzüberschreitende Auswirkung?
2. **Meldung – binnen 72 h**
   Erstbewertung: Schweregrad, Auswirkungen, Kompromittierungsindikatoren (IoCs)
3. **Abschlussbericht – binnen 1 Monat**
   Ursache, ergriffene Maßnahmen, ggf. grenzüberschreitende Folgen

Parallel läuft die DSGVO: Meldung nach Art. 33 an die Aufsichtsbehörde unverzüglich, i. d. R. binnen 72 h ab Bekanntwerden. Die NIS-2-Fristen gelten nur für „wichtige“/„besonders wichtige“ Einrichtungen nach dem deutschen Umsetzungsgesetz zum BSIG.

So sieht ein ausgefüllter Eintrag aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg, 1.200 MA · Vorfall MM-2026-001 (fiktiv)

Meldepflicht / Rechtsgrundlage	Trifft zu?	Frist	Empfänger + Meldeweg	Intern zuständig	Freigabe durch
Art. 33 DSGVO	Ja	unverzüglich, i. d. R. binnen 72 h ab Bekanntwerden	BayLDA, Online-Meldeportal	Dr. A. Frentz (ext. DSB), Vertr.: Kanzlei-Hotline	GF K. Sommer
NIS-2 / BSIG	Prüfen	Frühwarnung 24 h · Meldung 72 h · Abschluss 1 Monat	BSI-Meldeportal	T. Berger (IT-Ltg.)	GF K. Sommer
Cyberversicherung HanseCyber, Police CV-2024-88123	Ja	unverzüglich (Ziff. 7.2 AVB)	24/7-Hotline 0800 555 0199	Fr. Lindner (Finanzen)	GF K. Sommer

⚠ **Rechtlicher Hinweis:** Fristen Stand Juli 2026; die NIS-2-Umsetzung in deutsches Recht kann Details ändern – prüfen Sie die aktuelle Fassung des BSIG. Ob Ihr Unternehmen unter NIS-2, KRITIS oder DORA fällt, ist eine Einzelfallprüfung mit Ihrem rechtlichen Beistand.

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

UNTERNEHMEN	STAND / VERSION	VERANTWORTLICH	GEPRÜFT AM	NÄCHSTE PRÜFUNG

GESETZLICHE MELDEPFLICHTEN (VORBELEGT – BITTE PRÜFEN, ERGÄNZEN ODER STREICHEN)

Meldepflicht / Rechtsgrundlage	Trifft zu? Ja / Nein / Prüfen	Auslöser	Frist	Empfänger + Meldeweg (Portal, URL, Telefon)	Intern zuständig (Name, Mobil)	Freigabe durch
Art. 33 DSGVO		Verletzung des Schutzes personenbezogener Daten, außer voraussichtlich kein Risiko	unverzüglich, i. d. R. binnen 72 h ab Bekanntwerden; Verspätung ist zu begründen			
Art. 34 DSGVO		voraussichtlich hohes Risiko für betroffene Personen	unverzüglich	betroffene Personen (Kanal: siehe IR-18)		
NIS-2 / BSIG		erheblicher Sicherheitsvorfall – nur „wichtige“/„besonders wichtige“ Einrichtungen	Frühwarnung 24 h · Meldung 72 h · Abschlussbericht 1 Monat (nach dt. Umsetzungsgesetz)	BSI-Meldeportal		
KRITIS-Betreiber		erhebliche Störung der kritischen Dienstleistung	unverzüglich	BSI		
DORA (nur Finanzunternehmen)		schwerwiegender IKT-bezogener Vorfall	eigene, engere Meldefristen	zuständige Finanzaufsicht		

VERTRAGLICHE PFLICHTEN & FREIWILLIGE MELDUNGEN (VORBELEGT)

Meldepflicht / Grundlage	Trifft zu?	Auslöser	Frist	Empfänger + Meldeweg	Intern zuständig	Freigabe durch
Cyberversicherung (Police)		jeder Verdacht eines versicherten Ereignisses	laut Police, meist „unverzüglich“ – Obliegenheit! (Details: IR-08)			
Vertragspartner / Kunden (z. B. AVV)		vertragliche Informationspflichten, z. B. aus Auftragsverarbeitungsverträgen	Frist laut Vertrag			
Strafanzeige (freiwillig)		Verdacht einer Straftat	keine Frist	ZAC des Landeskriminalamts		

WEITERE MELDEPFLICHTEN (BRANCHENSPEZIFISCH PRÜFEN UND ERGÄNZEN)

Meldepflicht / Rechtsgrundlage	Trifft zu?	Auslöser	Frist	Empfänger + Meldeweg	Intern zuständig	Freigabe durch
BaFin / Bundesbank						
TKG (TK-Anbieter)						
Geschäftsgeheimnis-gesetz						

Tipp aus der Einsatzpraxis: Tragen Sie in „Empfänger + Meldeweg“ nicht nur die Behörde ein, sondern die konkrete URL des Meldeportals und eine Telefonnummer – und legen Sie vorab Zugangsdaten bzw. ein Konto an, wo das Portal es erlaubt. Nachts um zwei ist keine Zeit für eine Registrierung.

NOTIZEN

BLOCK 1 – VORAB AUSFÜLLBAR: STAMMDATEN FÜR JEDE BEHÖRDENMELDUNG

Angabe	Eintrag
Verantwortlicher (Firma, Rechtsform)	
Anschrift	
Register-Nr. (Handelsregister)	
Zuständige Datenschutz-Aufsichtsbehörde	
Datenschutzbeauftragte/r (Name, Kontakt)	
Ansprechpartner für Rückfragen (Name, Funktion, Mobil, E-Mail)	
Branche / Sektor	
BSI-Registrierungsnummer (NIS-2-Registrierungspflicht)	
Zahl Mitarbeiter / Jahresumsatz (für Einordnung)	

Meldung in Etappen ist zulässig: Art. 33 Abs. 4 DSGVO erlaubt es, Informationen schrittweise nachzureichen, wenn noch nicht alles bekannt ist. Melden Sie fristgerecht mit dem, was Sie haben, und kündigen Sie die Nachmeldung an – das ist besser, als die Frist für vollständige Antworten zu reißen. Beispiel Muster Maschinenbau GmbH: „Nachmeldung angekündigt: exakte Betroffenenzahl nach Abschluss der Log-Analyse, voraussichtlich 18.03.“

NOTIZEN

BLOCK 2 – ANGABEN FÜR DIE MELDUNG NACH ART. 33 DSGVO AN DIE AUFSICHTSBEHÖRDE

Angabe	Eintrag
Zeitpunkt des Bekanntwerdens (Datum, Uhrzeit – fristauslösend!)	
Art der Verletzung (Vertraulichkeit / Integrität / Verfügbarkeit)	
Betroffene Datenkategorien	
Kategorien betroffener Personen + Zahl (ggf. „ca.“)	
Ungefähre Zahl betroffener Datensätze	
Voraussichtliche Folgen für Betroffene	
Ergriffene / geplante Maßnahmen	
Grenzüberschreitend? (betroffene Länder, federführende Behörde)	
Nachmeldung geplant? (was fehlt noch, bis wann)	
Gemeldet am / Uhrzeit / Aktenzeichen	

NOTIZEN

BLOCK 3 – NIS-2 / BSI-MELDUNG (NUR FÜR „WICHTIGE“/„BESONDERS WICHTIGE“ EINRICHTUNGEN)

Stufe / Frist	Abgefragte Inhalte	Unsere Angaben	Gemeldet am / Aktenzeichen
Frühwarnung binnen 24 h	Verdacht auf rechtswidrige Handlung? Grenzüberschreitende Auswirkung?		
Meldung binnen 72 h	Erstbewertung Schweregrad, Auswirkungen, Kompromittierungsindikatoren (IoCs)		
Abschlussbericht binnen 1 Monat	Ursache, Maßnahmen, ggf. grenzüberschreitende Folgen		

BLOCK 4 – NACHWEIS: WER HAT WANN WAS ÜBER WELCHEN KANAL GEMELDET?

Datum / Uhrzeit	Empfänger	Kanal (Portal, Telefon, E-Mail)	Aktenzeichen	Meldender

NOTIZEN

Cyberversicherungs-Datenblatt & Obliegenheiten

Alle deckungsrelevanten Informationen Ihrer Cyberpolice auf einem Blatt: Notfallnummer, Policennummer, Deckungssummen – und vor allem die **Obliegenheiten, an deren Verletzung die Deckung scheitert.** Aus Sicht von Schadenregulierern das Dokument mit dem höchsten Euro-pro-Seite-Wert im ganzen Notfallordner.

Stand: Juli 2026 – aktuelle Rechtslage prüfen

Warum dieses Dokument?

Die häufigsten Deckungsprobleme: verspätete Schadenanzeige, eigenmächtig beauftragte Forensiker, neu aufgesetzte Systeme vor der Beweissicherung des Versicherers. Dieses Blatt verhindert drei dieser vier Klassiker.

Wann brauchen Sie es?

In der ersten Stunde – nachts um zwei findet sonst niemand Policennummer und Notfall-Hotline. Und: Versicherer VOR jeder Beauftragung externer Dienstleister anrufen.

Wo aufbewahren?

Ausgedruckt im Notfallordner und bei der internen Zuständigkeit (Finanzen) – sinnbildlich: am Kühlschrank des CISO. Nach jeder Policenänderung aktualisieren.

So sieht ein ausgefülltes Datenblatt aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg, 1.200 MA · Vorfall MM-2026-001 (fiktiv)

Feld	Eintrag
Versicherer / Police / Makler	HanseCyber Versicherung AG · Police CV-2024-88123 · Makler Südassekuranz (Hr. Weller, 0821 000 300)
24/7-Schadenhotline	**0800 555 0199** · schaden@hansecyber.example · Stichwort: Policennummer bereithalten
Deckungssummen	5 Mio. € Eigenschaden · 5 Mio. € Drittschaden · BU 3 Mio. € (Haftzeit 12 Monate, Karenzzeit 12 h) · Selbstbehalt 50.000 €
Meldefrist laut Police	„unverzüglich, spätestens binnen 5 Werktagen“ (Ziff. 7.2 AVB Cyber 2023)
Panel-Pflicht	Ja – Forensik nur über das Versicherer-Panel, sonst ist die Kostenübernahme gefährdet
Zusagen aus dem Antrag	MFA auf allen Remote-Zugängen · tägliche Offline-Backups
Intern zuständig	Fr. Lindner (Leitung Finanzen) · Vertretung: K. Sommer (GF)

⚠ **Rechtlicher Hinweis:** Maßgeblich sind ausschließlich Ihre Versicherungsbedingungen. Dieses Blatt ersetzt nicht die Lektüre der Police. Klären Sie Obliegenheiten mit Ihrem Makler bzw. Versicherer – im Zweifel **vor** jeder Maßnahme im Schadenfall anrufen.

UNTERNEHMEN	STAND / VERSION	VERANTWORTLICH	NÄCHSTE PRÜFUNG

24/7-Schadenhotline des Versicherers – im Schadenfall ZUERST anrufen

RUFNUMMER + STICHWORT / KUNDEN-NR.

POLICE & ANSPRECHPARTNER

Angabe	Eintrag
Versicherer	
Policennummer	
Vermittler / Makler (Name, Telefon, E-Mail)	
Laufzeit / Erneuerungsdatum	
E-Mail für die Schadenanzeige	

DECKUNGSSUMMEN & SELBSTBEHALT

Baustein	Deckungssumme / Eintrag
Eigenschaden	
Drittschaden (Haftpflicht)	
Betriebsunterbrechung (inkl. Haftzeit / Karenzzeit)	
Krisenkommunikation / PR	
Rechtskosten	
Lösegeld-Baustein (ja / nein, Bedingungen)	
Selbstbehalt(e)	

MELDEFRIST LAUT POLICE

Angabe	Eintrag
Wörtliches Zitat der Meldeklausel + Fundstelle (Ziffer der AVB)	

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

OBLIEGENHEITEN-CHECKLISTE – IM SCHADENFALL ABHAKEN

Obliegenheit	Beachtet / erledigt am (Datum, Uhrzeit)	Durch (Kürzel)
☐ Schadenanzeige unverzüglich erstattet		
☐ Weisungen des Versicherers eingeholt, **bevor** externe Dienstleister beauftragt wurden		
☐ Vom Versicherer benannte/freigegebene IR-Dienstleister genutzt (Panel-Pflicht?)		
☐ Schadenminderungspflicht beachtet		
☐ Keine Anerkenntnisse / Zahlungen ohne Zustimmung des Versicherers		
☐ Beweise erhalten (keine vorschnelle Neuinstallation)		

VOM VERSICHERER GESTELLTE / ANERKANNTE DIENSTLEISTER

Kategorie	Firma	24/7-Kontakt	Freigabe durch Versicherer am
Forensik / Incident Response			
Krisen-PR / Kommunikation			
Rechtsbeistand			

ZUSAGEN AUS DEN RISIKOFRAGEN DES ANTRAGS – „WAS MÜSSEN WIR EINHALTEN?“

Zusage (z. B. MFA, Offline-Backups, Patch-Zyklen)	Fundstelle (Antrag / Fragebogen)	Eingehalten? Geprüft am

INTERNE ZUSTÄNDIGKEIT

Rolle	Name, Funktion, Mobil
Zuständig für die Schadenmeldung	
Vertretung	

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

Backup-Übersicht

Bei Ransomware entscheidet eine einzige Frage über Verhandeln oder Wiederherstellen: **Gibt es Backups, die der Angreifer nicht erreichen konnte – und wurden sie je erfolgreich zurückgespielt?** Das IR-Team braucht Speicherorte, Netztrennung und den letzten Restore-Test – nicht das Marketing-Datenblatt der Backup-Software.

Warum dieses Dokument?

Ob wiederhergestellt werden kann, hängt an drei Spalten: Offline-Trennung, Zugriffsweg, Restore-Test. Diese Übersicht macht die Lücken sichtbar – heute, nicht im Ernstfall.

Wann brauchen Sie es?

In Stunde 1 beim Schützen der Backups (IR-02, Punkt 4), danach bei der Entscheidung Wiederherstellen vs. Verhandeln und für die Wiederanlauf-Planung.

Wo aufbewahren?

Ausgedruckt im Notfallordner + zweiter Brandabschnitt. Praxisfall: Die Backups waren da – aber die Passwörter der Backup-Konsole lagen nur im verschlüsselten Passwortmanager.

Backups in der ersten Stunde

1. **Replikation stoppen** – Copy-Jobs und Sync sofort anhalten
2. **Ziele vom Netz** – Repository/NAS per Switchport oder Kabel trennen
3. **Sauberer Stand** – letzte intakte Sicherung identifizieren + notieren
4. **Restore mit Freigabe** – erst nach Forensik-Freigabe des IR-Teams

Grundregel: Nie in die Produktivumgebung zurücksichern, solange der Angreifer drin sein könnte – sonst wird auch das Backup verbrannt.

So sieht ein ausgefüllter Eintrag aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg (fiktiv)

Was	Methode	Ziel	Offline?	Letzter Restore-Test
Alle VMs RZ Augsburg	Veeam B&R	Repo-Server RZ (lokal)	**nur online (!)**	12.03.2026: 1 VM, ok, 40 min
Wochenstände	Veeam Copy-Job	LTO-9-Tapes, Bankschließfach	Air-Gap, wöchentl. Wechsel	12.03.2026: File-Restore ok
M365 (Mail, SharePoint)	SaaS-Backup-Dienst	Cloud EU, eigener Tenant	immutable 30 T.	**nie (!)**
ERP-DB	DB-Dump + Copy-Job	NAS Leipzig	online, eigenes Konto	20.05.2026: Voll-Restore Testumgebung, 6 h

⚠ **Backups mit Domänen-Anmeldung und Online-Erreichbarkeit gelten im Ransomware-Fall als verloren.** Prüfen Sie die Spalten „Offline/immutable“ und „Zugriff aus dem Produktivnetz“ heute – nicht im Ernstfall. Ein Restore, der nie getestet wurde, ist keine Wiederherstellung, sondern eine Hoffnung.

Halbjährliche Prüfung: ☐ Restore-Test aktuell ☐ Offline-Kette intakt ☐ Passwort offline
Geprüft am: _____ von: _____

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

UNTERNEHMEN	STAND / VERSION	VERANTWORTLICH	ORT DER OFFLINE-KOPIE	NÄCHSTE PRÜFUNG

BACKUP-ZIELE & JOBS – EINE ZEILE PRO BACKUP-ZIEL/-JOB

Was wird gesichert (Systeme/Daten, Inventar-Nr. → IR-10)	Software / Methode	Ziel / Speicherort (Gerät + physischer Ort)	Offline / immutable?	Zugriff aus Produktivnetz?	Frequenz + Aufbewahrung
			☐ Air-Gap/Tape ☐ Immutable Storage ☐ nur online (!)	☐ ja ☐ nein mit Domänen-Konto: ☐ ja ☐ nein	
			☐ Air-Gap/Tape ☐ Immutable Storage ☐ nur online (!)	☐ ja ☐ nein mit Domänen-Konto: ☐ ja ☐ nein	
			☐ Air-Gap/Tape ☐ Immutable Storage ☐ nur online (!)	☐ ja ☐ nein mit Domänen-Konto: ☐ ja ☐ nein	
			☐ Air-Gap/Tape ☐ Immutable Storage ☐ nur online (!)	☐ ja ☐ nein mit Domänen-Konto: ☐ ja ☐ nein	
			☐ Air-Gap/Tape ☐ Immutable Storage ☐ nur online (!)	☐ ja ☐ nein mit Domänen-Konto: ☐ ja ☐ nein	
			☐ Air-Gap/Tape ☐ Immutable Storage ☐ nur online (!)	☐ ja ☐ nein mit Domänen-Konto: ☐ ja ☐ nein	
			☐ Air-Gap/Tape ☐ Immutable Storage ☐ nur online (!)	☐ ja ☐ nein mit Domänen-Konto: ☐ ja ☐ nein	
			☐ Air-Gap/Tape ☐ Immutable Storage ☐ nur online (!)	☐ ja ☐ nein mit Domänen-Konto: ☐ ja ☐ nein	

„Nur online“ heißt: Der Angreifer kann das Backup im Ransomware-Fall erreichen – diese Zeile heute entschärfen.

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

RESTORE-TESTS, ZUGÄNGE & SCHLÜSSEL – GLEICHE ZEILEN WIE BLATT 1

Was (wie Blatt 1)	Letzter erfolgreicher Restore-TEST (Datum, was, durch wen)	Geschätzte Dauer Vollrestore	Backup-Konsole: Wer hat Zugang – und wo liegt das Passwort AUSSERHALB des Netzes?	Verschlüsselungspasswort / Key des Backups: Verwahrort

Tipp aus der Einsatzpraxis: Konsolen-Passwort und Verschlüsselungs-Key gehören in den versiegelten Umschlag zu den Break-Glass-Konten (IR-12) – nicht in den Passwortmanager, der im Ernstfall mitverschlüsselt ist.

NOTIZEN

Asset- & System-Inventar mit Kritikalität

Das IR-Team muss binnen Stunden wissen: **Was gibt es überhaupt, was davon ist geschäftskritisch, wo läuft es – und wer kennt es?** Ohne Kritikalitätsbewertung ist die Priorisierung von Forensik und Wiederanlauf reines Raten. Und was nicht im Inventar steht, wird bei der Bereinigung übersehen – der klassische Weg zur Re-Infektion.

Warum dieses Dokument?

Gerade die vergessenen Systeme (alte Server, Appliances, OT) sind häufig das Einfallstor. Dazu gehören auch Domains, Zertifikate, SaaS-Dienste – und die Log-Quellen, ohne die Forensik blind ist.

Wann brauchen Sie es?

In Stunde 1 zur Priorisierung der Forensik (flüchtige Log-Quellen zuerst!), danach für Isolations-Entscheidungen (IR-15) und die Wiederanlauf-Reihenfolge.

Wo aufbewahren?

VERTRAULICH: Für Angreifer ist diese Liste ebenso wertvoll wie für Responder. Nur ausgedruckt im Tresor + zweiter Brandabschnitt, nie unverschlüsselt aufs Fileshare.

So sieht ein ausgefüllter Eintrag aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg, 1.200 MA, Automobilzulieferer (fiktiv)

Host	Funktion	Krit.	RTO	Standort	Abhängig von	Internet?
DC-01/DC-02	Active Directory	K1	4 h	RZ Augsburg / Azure	–	nein
ERP-DB-01	ERP-Datenbank (Produktion + Faktura)	K1	8 h	RZ Augsburg	DC, SAN-01	nein
TS-02	Terminalserver Vertrieb	K2	24 h	RZ Augsburg	DC, ERP	nein
WEB-SHOP	Ersatzteil-Shop	K2	24 h	Hoster CloudNord, FRA	Shop-DB	ja: 443
CNC-GW-03	OT-Gateway Halle 2	K1	2 h	Halle 2	keins (autark)	**ja: Fernwartung TCP 5900 (!)**

⚠ **Der Eintrag CNC-GW-03 zeigt, warum diese Liste Gold wert ist:** eine vergessene Fernwartung, die vor dem IR-Team niemand auf dem Schirm hatte. Nehmen Sie bewusst auch die „unwichtigen" Systeme auf – Appliances, Altsysteme, Testserver: Was nicht im Inventar steht, wird bei der Bereinigung übersehen.

Halbjährliche Prüfung: ☐ neue Systeme ergänzt ☐ Zertifikats-Abläufe geprüft ☐ Log-Aufbewahrung aktuell
Geprüft am: _____ von: _____

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

UNTERNEHMEN	STAND / VERSION	VERANTWORTLICH	ORT DER OFFLINE-KOPIE	NÄCHSTE PRÜFUNG

SYSTEME – EINE ZEILE PRO SYSTEM (K1 = ÜBERLEBENSWICHTIG, K2 = WICHTIG, K3 = VERZICHTBAR/TAGE)

System- / Hostname	Funktion (was tut es fürs Geschäft?)	Kritikalität	RTO	Standort · Phys/VM/ Cloud/SaaS	OS + Version	IP-Adresse(n) / Netzsegment	Abhängig von (AD, DB, Lizenzserver ...)	Verantwortlich intern / Dienstleister	Aus dem Internet erreichbar? Ports?
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:

RTO = maximal tolerierbare Ausfallzeit. Dienstleister-Betreuung mit Namen eintragen – Notfallnummern gehören in IR-01.

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

SYSTEME (FORTSETZUNG)

System- / Hostname	Funktion (was tut es fürs Geschäft?)	Kritikalität	RTO	Standort · Phys/VM/ Cloud/SaaS	OS + Version	IP-Adresse(n) / Netzsegment	Abhängig von (AD, DB, Lizenzserver …)	Verantwortlich intern / Dienstleister	Aus dem Internet erreichbar? Ports?
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:

NOTIZEN

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

DOMAINS & ZERTIFIKATE

Domain / Zertifikat	Zweck	Registrar / CA	Ablaufdatum	Zugang verwaltet von	DNS-Hoster

SAAS-DIENSTE

Dienst	Zweck	Admin-Konto-Inhaber	Kritikalität	SSO?
			☐ K1 ☐ K2 ☐ K3	☐ ja ☐ nein
			☐ K1 ☐ K2 ☐ K3	☐ ja ☐ nein
			☐ K1 ☐ K2 ☐ K3	☐ ja ☐ nein
			☐ K1 ☐ K2 ☐ K3	☐ ja ☐ nein
			☐ K1 ☐ K2 ☐ K3	☐ ja ☐ nein
			☐ K1 ☐ K2 ☐ K3	☐ ja ☐ nein
			☐ K1 ☐ K2 ☐ K3	☐ ja ☐ nein

Tipp aus der Einsatzpraxis: Abgelaufene Zertifikate und vergessene Domains blockieren im Ernstfall die Wiederherstellung (Mail-Zustellung, VPN, Shop). Ablaufdaten hier pflegen – und bei SaaS prüfen: Hängt der Admin-Zugang am kompromittierten SSO?

LOG-QUELLEN – WAS WIRD WO WIE LANGE GESPEICHERT?

Quelle	Wo gespeichert (lokal / Syslog / SIEM / Cloud)	Aufbewahrungs-dauer	Zeitzone / NTP-Sync?	Wie exportieren (Tool, Format, wer kann es?)	Zentral gesammelt?
Firewall					☐ ja ☐ nur lokal (flüchtig!)
VPN					☐ ja ☐ nur lokal (flüchtig!)
AD / DC Security-Log					☐ ja ☐ nur lokal (flüchtig!)
M365 / Entra Sign-in					☐ ja ☐ nur lokal (flüchtig!)
Mail-Gateway					☐ ja ☐ nur lokal (flüchtig!)
Proxy / DNS					☐ ja ☐ nur lokal (flüchtig!)
Endpoint / EDR / AV					☐ ja ☐ nur lokal (flüchtig!)
Server-Eventlogs					☐ ja ☐ nur lokal (flüchtig!)
Hypervisor					☐ ja ☐ nur lokal (flüchtig!)
Physische Zutrittssysteme					☐ ja ☐ nur lokal (flüchtig!)
					☐ ja ☐ nur lokal (flüchtig!)
					☐ ja ☐ nur lokal (flüchtig!)

⚠ **Wenn die Firewall nur 7 Tage speichert und der Initial Access drei Wochen her ist, ist die Spur weg.** Diese Übersicht entscheidet in Stunde 1, welche flüchtigen Quellen zuerst gesichert werden. Zeilen mit „nur lokal“ und kurzer Aufbewahrung heute entschärfen.

Netzplan-Steckbrief

„Zeigen Sie mir Ihren Netzplan“ ist Standardfrage Nummer zwei jedes IR-Teams – davon hängt ab, wie sich ein Angreifer bewegen konnte und wo sich Isolationsgrenzen ziehen lassen. In der Realität existiert oft nur ein veralteter Visio-Plan auf dem (verschlüsselten) Fileserver. Diese Vorlage erzwingt die handhabbare Minimal-Version: Segmente, Übergänge, Internet-Breakouts, Standortkopplungen.

Warum dieses Dokument?

Ohne Segmentübersicht keine Isolationsentscheidung: Was kann getrennt werden, und was fällt dann aus? Der Steckbrief beantwortet das, bevor das IR-Team stundenlang Switches nachverfolgen muss.

Wann brauchen Sie es?

In Stunde 1 bei der Eindämmung (zusammen mit der Isolations-Matrix IR-15) und danach bei der Rekonstruktion der Angriffswege.

Wo aufbewahren?

VERTRAULICH: Ein Netzplan ist für Angreifer eine Schatzkarte. Nie unverschlüsselt digital im normalen Netz – nur Ausdruck im Tresor + zweiter Brandabschnitt.

In vier Schritten zum Notfall-Netzplan

1. **Segmente listen** – VLAN, IP-Bereich, Zweck, Inhalt
2. **Übergänge markieren** – welche Firewall verbindet welche Segmente
3. **Außenverbindungen** – Breakouts, VPN, Standleitungen, Fernwartung Dritter
4. **Skizze zeichnen** – Handzeichnung genügt – Raster-Blatt am Ende

Beispiel Muster Maschinenbau: 6 Segmente (Clients, Server, OT Halle 1+2, DMZ, Gäste-WLAN, Azure via S2S-VPN), zwei Internet-Breakouts (Augsburg + Werk Leipzig) – und rot markiert: die Fernwartungs-VPNs zweier Maschinenbauer in die OT.

So sieht ein ausgefüllter Eintrag aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg (fiktiv)

Segment	VLAN / IP	Zweck	Übergänge	Isolierbar? Wie?	Folgen der Isolation
Clients	VLAN 10 · 10.10.0.0/16	Arbeitsplätze beide Standorte	→ Server via FW-01	ja: Regelgruppe „Clients-Out“ deaktivieren	kein Zugriff auf ERP/Mail, Produktion läuft
OT Halle 1+2	192.168.50.0/24	CNC-Steuerungen, Leitstand	→ Server via FW-01	ja: FW-Regel #240 ODER Patchfeld B, Ports 12–16 ziehen	keine Auftragsübertragung an CNC; Produktion läuft lokal ca. 4 h weiter

⚠ **Fernwartungszugänge Dritter sind der häufigste Initial-Access-Pfad.** Tragen Sie jede Außenverbindung vollständig ein – besonders Dienstleister-VPNs in Server- und OT-Segmente. Wer sie trennen kann und wie, muss hier stehen, nicht im Kopf eines einzelnen Admins.

Halbjährliche Prüfung: ☐ Segmente aktuell ☐ Außenverbindungen vollständig ☐ Skizze erneuert
Geprüft am: _____ von: _____

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

UNTERNEHMEN	STAND / VERSION	VERANTWORTLICH	ORT DER OFFLINE-KOPIE	NÄCHSTE PRÜFUNG

NETZSEGMENTE – EINE ZEILE PRO SEGMENT

Segment-Name	VLAN-ID / IP-Bereich (CIDR)	Zweck / was steht drin	Übergänge zu welchen Segmenten (über welche Firewall?)	Isolierbar?	Wie? (Regel, Port, Stecker)	Folgen der Isolation (was fällt aus?)
Clients				☐ ja ☐ nein		
Server				☐ ja ☐ nein		
OT / Produktion				☐ ja ☐ nein		
DMZ				☐ ja ☐ nein		
Gäste-WLAN				☐ ja ☐ nein		
				☐ ja ☐ nein		
				☐ ja ☐ nein		
				☐ ja ☐ nein		

Vorbelegte Segment-Namen bei Bedarf durchstreichen und anpassen – wichtig ist, dass kein Segment fehlt (auch Gäste, Kameras, Telefonie, Gebäudetechnik).

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

AUSSENVERBINDUNGEN – ALLES, WAS DAS NETZ MIT DER WELT VERBINDET

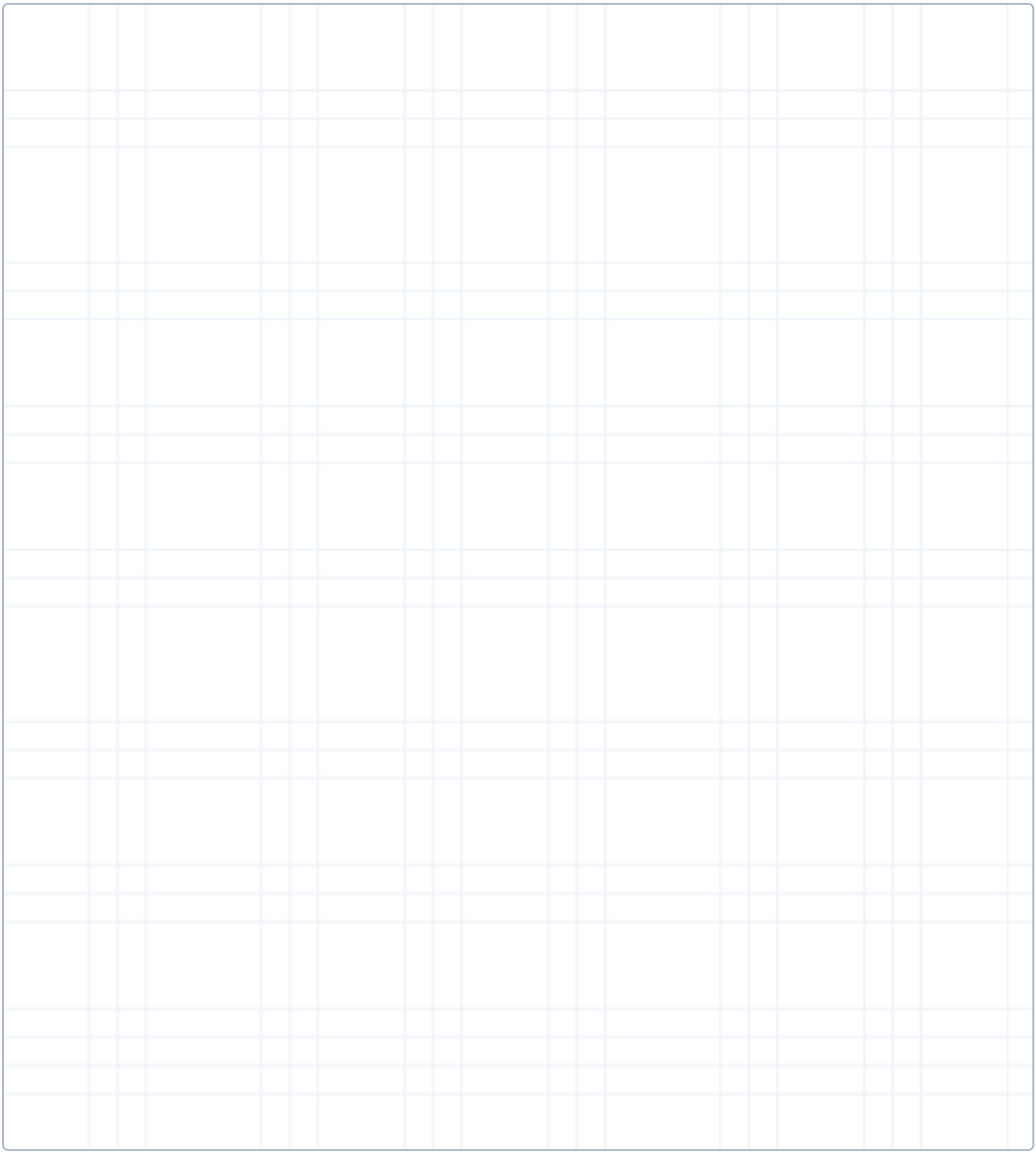
Verbindung	Endpunkt / Gegenstelle	Gerät (Firewall/Router, Modell, Standort)	Wer kann sie trennen – und wie?	Fernwartungszugänge Dritter darüber?
Internet-Breakout 1				☐ nein ☐ ja:
Internet-Breakout 2				☐ nein ☐ ja:
S2S-VPN (Cloud/Werk)				☐ nein ☐ ja:
Client-VPN				☐ nein ☐ ja:
MPLS / Standortkopplung				☐ nein ☐ ja:
Standleitung Partner				☐ nein ☐ ja:
				☐ nein ☐ ja:
				☐ nein ☐ ja:
				☐ nein ☐ ja:

Tipp aus der Einsatzpraxis: Für jede Verbindung muss die Antwort auf „Wer kann sie trennen – und wie?“ ohne Rückfrage funktionieren: Name, Gerät, Regel oder Stecker. „Der Dienstleister macht das“ zählt nur mit 24/7-Nummer in IR-01.

NOTIZEN

NETZSKIZZE – HANDZEICHNUNG GENÜGT

Segment · Firewall / Übergang · Internet / extern · VPN / Fernwartung Dritter (Dienstleister-Name dazuschreiben!)



Skizzieren Sie: alle Segmente als Kästen, dazwischen die Firewalls/Übergänge, oben die Internet-Breakouts und Cloud-Anbindungen, gestrichelt jede Fernwartung von extern. Datum an die Skizze – ein alter Plan ist gefährlicher als keiner.

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

Admin- & Break-Glass-Konten

Das IR-Team braucht sofort privilegierten Zugriff auf Firewall, Hypervisor, AD und Cloud – **über Konten, die nicht kompromittiert sind.** Diese Liste enthält KEINE Passwörter: Sie dokumentiert, welche Notfallkonten existieren und wo deren Zugangsdaten sicher verwahrt sind (versiegelter Umschlag im Tresor, Offline-Passwortmanager).

Warum dieses Dokument?

Hat der Angreifer Domain-Admin, ist jedes Alltagskonto verdächtig. Dedizierte Break-Glass-Konten sind der einzige saubere Weg zurück in die eigene Infrastruktur.

Wann brauchen Sie es?

In Stunde 1, wenn Firewall, Hypervisor oder Tenant erreichbar sein müssen, ohne kompromittierte Konten zu benutzen – und bei jedem Test und Passwortwechsel der Notfallkonten.

Wo aufbewahren?

Nur als Ausdruck im Tresor, Zweitexemplar im anderen Brandabschnitt oder Bankschließfach. Die Umschläge mit den Zugangsdaten getrennt von dieser Liste versiegeln.

Break-Glass richtig benutzen

1. **Umschlag öffnen** – nur nach Freigabe, 4-Augen-Prinzip
2. **Ins Logbuch** – Öffnung sofort in IR-03: wer, wann, warum
3. **Konto nutzen** – Alarm bei Login ist gewollt
4. **Danach rotieren** – Passwort wechseln, neu versiegeln, Test terminieren

Grundregel: Break-Glass-Konten werden nie im Alltag benutzt – jede Anmeldung außerhalb eines Notfalls ist ein Alarmsignal.

So sieht ein ausgefüllter Eintrag aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg (fiktiv)

System	Konto	Typ	Verwahrort	Letzter Test
AD Forest	bg-admin-01	Break-Glass	Umschlag 1, Tresor GF Augsburg	02.05.2026 ok
M365 / Entra	breakglass@musterm.onmicrosoft.com	Break-Glass, MFA-ausgenommen, Alarm bei Login	Umschlag 2, Tresor GF + Kopie Bankschließfach	02.05.2026 ok
FW-01	fw-emergency	dediziert, nur Konsole	Umschlag 3, Serverraum-Tresor	14.01.2026 ok

⚠ **Dieses Blatt niemals digital im Firmennetz ablegen.** Nur Ausdruck + Tresor – für Angreifer ist es der Wegweiser zu den Kronjuwelen. Die Öffnung eines Umschlags gehört sofort ins Incident-Logbuch (IR-03), danach: Passwort wechseln und neu versiegeln.

Halbjährliche Prüfung: ☐ alle Logins getestet ☐ Umschläge versiegelt ☐ Zweitverwahrort aktuell
Geprüft am: _____ von: _____

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

UNTERNEHMEN	STAND / VERSION	VERANTWORTLICH	ORT DER OFFLINE-KOPIE	NÄCHSTE PRÜFUNG

BREAK-GLASS- / NOTFALLKONTEN – KEINE PASSWÖRTER EINTRAGEN, NUR VERWAHRORTE

System / Ebene	Kontoname	Kontotyp	MFA?	Verwahrort der Zugangsdaten (Umschlag-Nr., Tresor)	Zweitverwahrort (anderer Brandabschnitt / Standort)
AD Forest		☐ dediziertes Break-Glass ☐ Standard-Admin ☐ Hersteller-Default (!)	☐ ja, Methode: ☐ ausgenommen (bewusst)		
Azure / M365-Tenant		☐ dediziertes Break-Glass ☐ Standard-Admin ☐ Hersteller-Default (!)	☐ ja, Methode: ☐ ausgenommen (bewusst)		
Firewall		☐ dediziertes Break-Glass ☐ Standard-Admin ☐ Hersteller-Default (!)	☐ ja, Methode: ☐ ausgenommen (bewusst)		
Hypervisor		☐ dediziertes Break-Glass ☐ Standard-Admin ☐ Hersteller-Default (!)	☐ ja, Methode: ☐ ausgenommen (bewusst)		
Backup-Konsole		☐ dediziertes Break-Glass ☐ Standard-Admin ☐ Hersteller-Default (!)	☐ ja, Methode: ☐ ausgenommen (bewusst)		
Core-Switch		☐ dediziertes Break-Glass ☐ Standard-Admin ☐ Hersteller-Default (!)	☐ ja, Methode: ☐ ausgenommen (bewusst)		
		☐ dediziertes Break-Glass ☐ Standard-Admin ☐ Hersteller-Default (!)	☐ ja, Methode: ☐ ausgenommen (bewusst)		

„Hersteller-Default (!)“ heißt: Standard-Zugangsdaten des Herstellers – sofort ändern, das ist keine Notfall-Lösung, sondern eine offene Tür.

FREIGABE & PFLEGE DER NOTFALLKONTEN

System / Konto (wie Blatt 1)	Wer darf öffnen? (Rollen, 4-Augen-Prinzip?)	Letzter Test des Kontos (Datum – funktioniert Login noch?)	Letzter Passwortwechsel

PRIVILEGIERTE ROLLEN IM ALLTAG – WELCHE KONTEN SIND BEI KOMPROMITTIERUNG EINER PERSON ZU SPERREN?

Person	Systeme mit Admin-Rechten	Konto-Namen

Tipp aus der Einsatzpraxis: Testen Sie jedes Break-Glass-Konto halbjährlich per echtem Login – abgelaufene Passwörter und deaktivierte Konten fallen sonst erst im Ernstfall auf. Jeden Test hier dokumentieren.

Datenschutz-Vorfall-Erfassungsbogen

Die interne Pflichtdokumentation nach **Art. 33 Abs. 5 DSGVO** – für **jede** Datenschutzverletzung, auch die, die am Ende nicht meldepflichtig ist. Der Bogen hält Fakten, Auswirkungen, Abhilfemaßnahmen und vor allem die Risikoabwägung fest: **warum wurde (nicht) gemeldet?** Genau das prüft die Aufsichtsbehörde.

Stand: Juli 2026 – aktuelle Rechtslage prüfen

Warum dieses Dokument?

Die meisten Unternehmen scheitern nicht an der Meldung, sondern an der Dokumentation. Art. 33 Abs. 5 verlangt sie so, dass die Behörde die Compliance prüfen kann – auch bei Nicht-Meldung.

Wann brauchen Sie es?

Sofort ab Bekanntwerden jeder Verletzung – der Zeitpunkt des Bekanntwerdens löst die 72-h-Frist des Art. 33 aus und gehört als erstes in den Bogen.

Wo aufbewahren?

Als Kopiervorlage im Notfallordner; ausgefüllte Bögen chronologisch beim Datenschutzbeauftragten ablegen – sie sind Ihr Verzeichnis der Datenschutzverletzungen.

So sieht ein ausgefüllter Bogen aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg, 1.200 MA · Vorfall MM-2026-001 (fiktiv)

Feld	Eintrag
Vorfall-ID / Erfasser	MM-2026-001 · erfasst von Dr. A. Frentz (ext. DSB) am 12.03.2026, 14:20
Bekanntwerden (fristauslösend)	12.03.2026, 09:45 – Hinweis des SOC (Argos CDC): Exfiltration vom HR-Fileserver
Art / betroffene Daten	Vertraulichkeit · Bewerberdaten (Lebensläufe, Zeugnisse), ca. 340 Personen / ca. 1.900 Dokumente
Risikobewertung	**hohes Risiko** – unverschlüsselte Bewerbungsunterlagen mit teils sensiblen Angaben, Täter unbekannt (Ransomware-Gruppe TS-02), Veröffentlichung auf Leak-Seite möglich
Entscheidung	Meldung Art. 33: Ja, 13.03.2026, 11:10 ans BayLDA (innerhalb 72 h) · Art. 34: Ja, E-Mail an die 340 Bewerber am 16.03.2026
Abhilfe	kompromittiertes Konto gesperrt, MFA erzwungen, Fileserver segmentiert

⚠ **Rechtlicher Hinweis:** Die Risikobewertung ist eine Einzelfallentscheidung – beteiligen Sie stets Ihren Datenschutzbeauftragten. Dieser Bogen ersetzt nicht die Meldung selbst; nutzen Sie dafür das Meldeportal Ihrer Aufsichtsbehörde (Angaben dafür: IR-07, Vorbereitungsbögen).

INTERNE VORFALL-ID	ERFASST VON	DATUM DER ERFASSUNG	STATUS (OFFEN / ABGESCHLOSSEN)

ZEITPUNKTE & ENTDECKUNG

Angabe	Eintrag
Zeitpunkt des Vorfalls (soweit bekannt)	
Zeitpunkt des Bekanntwerdens (Datum, Uhrzeit – fristauslösend!)	
Entdeckungsweg (wie wurde der Vorfall bekannt?)	

BESCHREIBUNG DES VORFALLS

ART DER VERLETZUNG & BETROFFENE DATEN

Kategorie (Zutreffendes ankreuzen)	Details / Anmerkungen
Art der Verletzung: ☐ Vertraulichkeit ☐ Integrität ☐ Verfügbarkeit	
Kategorien betroffener Daten: ☐ Stammdaten ☐ Kontaktdaten ☐ Gesundheitsdaten ☐ Finanzdaten ☐ Zugangsdaten ☐ besondere Kategorien (Art. 9) ☐ sonstige	

UMFANG

Angabe	Eintrag
Kategorien betroffener Personen + ungefähre Zahl (ggf. „ca.“)	
Ungefähre Zahl betroffener Datensätze	

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

VORAUSSICHTLICHE FOLGEN FÜR DIE BETROFFENEN

RISIKOBEWERTUNG (PFLICHTFELD – MIT BEGRÜNDUNG)

Bewertung	Bewertet am / durch (DSB einbinden!)
☐ kein Risiko ☐ Risiko ☐ hohes Risiko	

Begründung der Risikobewertung (Pflichtfeld – z. B. Sensibilität der Daten, Verschlüsselung, Täterlage, Veröffentlichungsrisiko):

ENTSCHEIDUNG: MELDUNG AN DIE AUFSICHTSBEHÖRDE (ART. 33 DSGVO)?

Entscheidung	Eintrag
☐ Ja – gemeldet am (Datum, Uhrzeit), Aktenzeichen	
☐ Nein – Begründung	
Bei Meldung nach 72 h: Begründung der Verzögerung	

ENTSCHEIDUNG: BENACHRICHTIGUNG DER BETROFFENEN (ART. 34 DSGVO)?

Entscheidung	Eintrag
☐ Ja – am / über Kanal (Details: IR-18)	
☐ Nein – Begründung (ggf. Ausnahme nach Art. 34 Abs. 3)	

ERGRIFFENE ABHILFEMASSNAHMEN

MASSNAHMEN ZUR MINDERUNG DER FOLGEN FÜR BETROFFENE

BETEILIGTE

Angabe	Eintrag
Datenschutzbeauftragte/r eingebunden am	
Auftragsverarbeiter betroffen? (Name)	
Auftragsverarbeiter informiert am / durch	
Weitere Beteiligte (SOC, Forensik, Versicherer …)	

ABSCHLUSS

Angabe	Eintrag
Vorfall abgeschlossen am	
Lessons Learned (was ändern wir?)	

Unterschrift Datenschutzbeauftragte/r	Unterschrift Verantwortlicher (Geschäftsleitung)

Entscheidungsprotokoll & -Tagebuch der Geschäftsleitung

Protokolliert jede Krisenentscheidung mit Zeitstempel, damaligem Kenntnisstand, Alternativen und Beratern. Monate später verlangen Cyber- und D&O-Versicherer, Wirtschaftsprüfer, Aufsichtsbehörden und ggf. Gerichte genau diese Rekonstruktion – **wer sie nicht hat, wird an der Rückschau gemessen statt am damaligen Wissen.**

Stand: Juli 2026 – aktuelle Rechtslage prüfen

Warum dieses Dokument?

Die Business Judgment Rule (§ 43 GmbHG, § 93 AktG) schützt Organmitglieder nur bei nachweislich informierter Entscheidung. NIS-2 macht die Geschäftsleitung zudem persönlich verantwortlich – Delegation entlastet nicht vollständig.

Wann brauchen Sie es?

Ab Stunde sechs jedes Krisenfalls – dann aber lückenlos. Teil A (Tagebuch) für den laufenden Betrieb, Teil B (Einzelblatt) für tragweite Entscheidungen wie Shutdown, Lösegeld, Wiederanlauf.

Wo aufbewahren?

Beim Protokollführer des Krisenstabs, als Kopiervorlage im Notfallordner. Einträge zeitnah erfassen, nicht rückwirkend glätten – auch verworfene Optionen notieren.

So sieht ein ausgefüllter Eintrag aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg, 1.200 MA · Vorfall MM-2026-001 (fiktiv)

Feld	Eintrag
Tagebuch-Eintrag Nr. 7 (Teil A)	15.03.2026, 10:20 – „Kein Kontakt zur Erpressergruppe TS-02, keine Zahlung; Wiederherstellung aus Backups wird beauftragt." Entscheider: K. Sommer (GF)
Konsultiert	T. Berger (IT-Ltg.), Argos IR-Team (Forensik), RA Dr. Steiner, Cyber-Versicherer (HanseCyber-Hotline, Fr. Lang)
Informationslage zu diesem Zeitpunkt	Backups der letzten Nacht laut Forensik integer und offline; Exfiltration noch nicht ausgeschlossen; Lösegeldforderung 1,2 Mio. USD; Versicherer bestätigt Deckung der Wiederherstellungskosten
Erwogene Alternativen	(a) Verhandlung zur Zeitgewinnung – verworfen, da Backups verfügbar; (b) Zahlung – verworfen: keine Garantie, Compliance-Risiko
Folgeaktionen / Wiedervorlage	Restore-Reihenfolge festlegen (T. Berger, bis 15.03., 18:00) · DSGVO-Fristen prüfen (Dr. A. Frentz, bis 16.03., 12:00) · Wiedervorlage: 16.03., 8-Uhr-Lage – gez. KS
Einzelentscheidung (Teil B, Protokoll 04/2026)	12.03.2026, 16:30, Krisen-Call: „Sofortige Volltrennung der Produktionsstandorte Augsburg und Győr vom Firmennetz trotz Lieferverpflichtungen" – Grundlage: SOC-Bericht Argos CDC, 15:40 (laterale Bewegung Richtung OT-Netz); Rat: RA Dr. Steiner (Pönale-Risiko ca. 80 T€/Tag beherrschbar), Versicherer-Hotline 16:10 (Zustimmung, Schadenminderung)

⚠ **Rechtlicher Hinweis:** Ob und wie Haftungsprivilegien greifen, hängt von Rechtsform und Einzelfall ab – lassen Sie sich anwaltlich beraten. Ziehen Sie bei Erwägung von Lösegeldzahlungen zwingend Rechtsbeistand und Versicherer hinzu (u. a. sanktionsrechtliche Prüfung).

VORFALL-NR.	PROTOKOLLFÜHRER/IN	BLATT-NR.

ENTSCHEIDUNGS-TAGEBUCH – JEDE WESENTLICHE ENTSCHEIDUNG, ZEITNAH

Nr.	Datum / Uhrzeit	Entscheidung (Klartext) + Begründung	Entscheider / anwesend / konsultiert	Informationslage: was wussten wir – was nicht?	Erwogene Alternativen	Folgeaktionen: Was / Wer / bis wann · Wiedervorlage	Kürzel

Einträge zeitnah erfassen, nicht rückwirkend glätten. Auch verworfene Optionen notieren.

ENTSCHEIDUNGS-TAGEBUCH – FORTSETZUNG

Nr.	Datum / Uhrzeit	Entscheidung (Klartext) + Begründung	Entscheider / anwesend / konsultiert	Informationslage: was wussten wir – was nicht?	Erwogene Alternativen	Folgeaktionen: Was / Wer / bis wann · Wiedervorlage	Kürzel

Einträge zeitnah erfassen, nicht rückwirkend glätten. Auch verworfene Optionen notieren.

PROTOKOLL-KOPF

Protokoll-Nr.	Datum	Uhrzeit	Ort / Medium (z. B. Krisen-Call)

TEILNEHMER

Angabe	Eintrag
Anwesende / Teilnehmer (Name, Rolle)	
Protokollführer/in	
Entscheidungsgegenstand (prägnant, 1–2 Sätze)	

INFORMATIONSGRUNDLAGE: VORLIEGENDE FAKTEN / BERICHTE (MIT VERWEIS, Z. B. „FORENSIK-ZWISCHENBERICHT V. …“, „EINSCHÄTZUNG VERSICHERER V. …“)

Angabe	Eintrag
Bekannte Unsicherheiten („was wissen wir noch nicht?“)	

EINGEHOLTER RAT

Quelle	Name	Kernaussage
☐ Rechtsanwalt		
☐ Datenschutzbeauftragte/r		
☐ Forensik / IR-Dienstleister		
☐ Versicherer		
☐ Sonstige		

GEPRÜFTE HANDLUNGSALTERNATIVEN (MINDESTENS 2)

Alternative	Chancen	Risiken

ENTSCHEIDUNG (WORTLAUT) + WESENTLICHE BEGRÜNDUNG

ABSTIMMUNG MIT DEM VERSICHERER

Abstimmung erfolgt?	Eintrag
☐ Ja – wann, mit wem	
☐ Nein – warum nicht	

UMSETZUNG & WIEDERVORLAGE

Verantwortlich für die Umsetzung	Umsetzung bis wann	Wiedervorlage / Überprüfung am

UNTERSCHRIFTEN DER ENTSCHEIDER

Name, Funktion + Unterschrift	Name, Funktion + Unterschrift	Name, Funktion + Unterschrift

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

Isolations- & Abschalt-Entscheidungsmatrix

Die härtesten Minuten eines Vorfalls sind Abschalt-Entscheidungen unter Unsicherheit: **Internet kappen? AD herunterfahren? Produktion stoppen?** Diese Matrix wird vorher in Ruhe mit der Geschäftsführung ausgefüllt – damit nachts um drei klar ist, wer was ohne Rückfrage trennen darf und was es kostet.

Warum dieses Dokument?

Aus der Praxis eines IT-Leiters: „Bei uns hat die Diskussion ‚Dürfen wir das Werk offline nehmen?' vier Stunden gekostet – vier Stunden, in denen der Angreifer weitergearbeitet hat."

Wann brauchen Sie es?

Ausfüllen: jetzt, mit Unterschrift der Geschäftsführung. Anwenden: in Stunde 1 bei Punkt 6 der Erstmaßnahmen-Checkliste (IR-02) – zusammen mit dem Netzplan-Steckbrief (IR-11).

Wo aufbewahren?

Ausgedruckt im Notfallordner direkt neben IR-02. Jede Vorab-Freigabe braucht Datum und Unterschrift – eine mündliche Zusage von vor zwei Jahren trägt nachts um drei nicht.

Vom Verdacht zur Trennung – ohne Vier-Stunden-Diskussion

1. **Verdacht einordnen** – welcher Auslöser liegt vor?
2. **Zeile finden** – Maßnahme in der Matrix nachschlagen
3. **Stufe prüfen** – wer darf entscheiden – Vorab-Freigabe vorhanden?
4. **Trennen + Logbuch** – durchführen, Uhrzeit und Entscheider in IR-03

Grundregel: Trennen ist fast immer reversibel – zerstörte Forensik nie. Im Zweifel isolieren statt ausschalten.

So sieht ein ausgefüllter Eintrag aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg (fiktiv)

Maßnahme	Auswirkung	Stufe	Durchführung
Internet-Breakout Augsburg trennen	kein Mail/Web/Shop; Produktion läuft	IT-Bereitschaft **sofort**; vorab freigegeben 15.04.2026, K. Sommer	FW-01: Regel „WAN-Kill" aktivieren, 2 min
Client-VPN aus	Homeoffice offline (ca. 180 MA)	IT-Bereitschaft sofort	FW-01: VPN-Portal deaktivieren
OT-Segment isolieren	keine neuen CNC-Aufträge, Puffer 4 h	IT-Leitung	Patchfeld B, Ports 12–16
DC herunterfahren	**Alles** steht	GF + IR-Team – nur auf Anweisung	vCenter (nicht ohne Forensik-Freigabe!)

⚠ **Die wichtigste Zeile ist die letzte:** Domänencontroller und Server nie ohne Forensik-Freigabe herunterfahren – im Arbeitsspeicher liegen die Spuren. Holen Sie Vorab-Freigaben für die reversiblen Trennungen schriftlich ein, mit Datum und Unterschrift der Geschäftsführung.

Halbjährliche Prüfung: ☐ Freigaben aktuell ☐ Durchführungswege getestet ☐ mit GF besprochen
Geprüft am: _____ von: _____

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

UNTERNEHMEN	STAND / VERSION	VERANTWORTLICH	ORT DER OFFLINE-KOPIE	NÄCHSTE PRÜFUNG

ENTSCHEIDUNGSMATRIX – EINE ZEILE PRO MASSNAHME, VORAB MIT DER GESCHÄFTSFÜHRUNG AUSFÜLLEN

Maßnahme	Typischer Auslöser (bei welchem Verdacht?)	Geschäfts-auswirkung (was fällt aus, ab wann Kosten?)	Entscheidungs-stufe	Vorab-Freigabe erteilt?	Technische Durchführung (wo, welche Regel/Stecker, Dauer?)	Rücknahme (wie wieder anschalten, was vorher prüfen?)
Internet-Breakout trennen			☐ IT-Bereitschaft sofort ☐ IT-Leitung ☐ GF	☐ nein ☐ ja, Datum + Unterschrift:		
Client-VPN deaktivieren			☐ IT-Bereitschaft sofort ☐ IT-Leitung ☐ GF	☐ nein ☐ ja, Datum + Unterschrift:		
M365- / Cloud-Sitzungen widerrufen			☐ IT-Bereitschaft sofort ☐ IT-Leitung ☐ GF	☐ nein ☐ ja, Datum + Unterschrift:		
Standortkopplung kappen			☐ IT-Bereitschaft sofort ☐ IT-Leitung ☐ GF	☐ nein ☐ ja, Datum + Unterschrift:		
Netzsegment isolieren (welches? → IR-11)			☐ IT-Bereitschaft sofort ☐ IT-Leitung ☐ GF	☐ nein ☐ ja, Datum + Unterschrift:		

ENTSCHEIDUNGSMATRIX (FORTSETZUNG)

Maßnahme	Typischer Auslöser (bei welchem Verdacht?)	Geschäfts-auswirkung (was fällt aus, ab wann Kosten?)	Entscheidungs-stufe	Vorab-Freigabe erteilt?	Technische Durchführung (wo, welche Regel/Stecker, Dauer?)	Rücknahme (wie wieder anschalten, was vorher prüfen?)
Produktion stoppen			☐ IT-Bereitschaft sofort ☐ IT-Leitung ☐ GF	☐ nein ☐ ja, Datum + Unterschrift:		
DC / Server herunterfahren – nur mit IR-Team!			☐ IT-Bereitschaft sofort ☐ IT-Leitung ☐ GF	☐ nein ☐ ja, Datum + Unterschrift:		
			☐ IT-Bereitschaft sofort ☐ IT-Leitung ☐ GF	☐ nein ☐ ja, Datum + Unterschrift:		
			☐ IT-Bereitschaft sofort ☐ IT-Leitung ☐ GF	☐ nein ☐ ja, Datum + Unterschrift:		
			☐ IT-Bereitschaft sofort ☐ IT-Leitung ☐ GF	☐ nein ☐ ja, Datum + Unterschrift:		

Tipp aus der Einsatzpraxis: Die Spalte „Rücknahme“ wird am häufigsten vergessen – wer das Internet kappt, muss auch wissen, was vor dem Wiederanschalten geprüft sein muss (Passwörter rotiert? EDR ausgerollt? Freigabe des IR-Teams?).

NOTIZEN

Dienstleister-, Vertrags- & Zugangs-Übersicht

Das IR-Team muss binnen Stunden wissen: **Welche Dritten haben Zugriff auf unser Netz** (der häufigste Initial-Access-Vektor!), wen brauchen wir für Sperrungen und Log-Auszüge – und welche vertraglichen Melde- und Reaktionspflichten bestehen? Im Ernstfall entscheidet die 24/7-Nummer des Hosters darüber, ob eine kompromittierte Website in Minuten oder Tagen offline geht.

Warum dieses Dokument?

Dienstleister-Zugänge sind der häufigste Weg des Angreifers ins Netz – und die vergessene Dauer-VPN-Verbindung wird bei der Bereinigung übersehen. Wer hier gepflegt hat, sperrt in Minuten statt Tagen.

Wann brauchen Sie es?

In Stunde eins (Zugänge sperren, Top-5 anrufen) und an Tag 1 bis 3: Meldepflichten aus AVV und Verträgen laufen parallel zur Technik – auch Ihre Dienstleister müssen Ihnen melden, und Sie ihnen.

Wo aufbewahren?

Nur Ausdruck im Tresor / Notfallordner und verschlüsselte Offline-Kopie. Diese Liste zeigt jedem Angreifer die Türen ins Netz – sie gehört nie unverschlüsselt aufs Fileshare.

So sieht ein ausgefüllter Eintrag aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg (fiktiv)

Dienstleister	Leistung	Netz-Zugang	Sperrung durch uns	24/7-Notfallkontakt
NetCom Süd	ISP beide Standorte	nein	–	0800 000100, Kd-Nr. 4711
CloudNord	Hosting Ersatzteil-Shop	nein (eigene Umgebung)	Portal-Login	24/7-Ticket + Tel., liefert Access-Logs 90 T.
ERP-Partner Huber & Co.	ERP-Betreuung, AVV v. 02/2024	**ja: Dauerhaft-VPN auf ERP-DB-01 (!)**	FW-Regel #118, Konto „huber-svc“	Mo–Fr 8–18 Uhr (kein 24/7!)
WerkzeugTec AG	Fernwartung CNC Halle 2	ja: VPN auf Anforderung	Konto „wtec-remote“ deaktivieren	Hotline 24/7
CloudPay HR SaaS GmbH	Lohnabrechnung, AVV Legal/AVV-07	nein (Datenhosting: Gehaltsdaten 1.200 MA)	SSO-Konto sperren	soc@cloudpay..., 24/7 · meldet „unverzüglich, spät. 24 h“ (§ 9 AVV)

⚠ **Zeile 3 ist der Klassiker: Dauer-VPN eines Dienstleisters ohne 24/7-Erreichbarkeit.** Freitagnacht steht der Zugang offen, aber niemand geht ans Telefon. Solche Zeilen werden **vor** dem Ernstfall entschieden entschärft: Zugang auf Anforderung statt dauerhaft, eigenes Konto, dokumentierte Sperrung.

Halbjährliche Prüfung: ☐ Zugänge noch nötig? ☐ Notfallnummern getestet ☐ AVV-Fristen aktuell
Geprüft am: _____ von: _____

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

UNTERNEHMEN	STAND / VERSION	VERANTWORTLICH	ORT DER OFFLINE-KOPIE	NÄCHSTE PRÜFUNG

IM VORFALL ZUERST KONTAKTIEREN – TOP 5

Nr.	Dienstleister	24/7-Nummer	Kunden-Nr. / Stichwort	Warum zuerst?
1				
2				
3				
4				
5				

HAUPTTABELLE DIENSTLEISTER (1/2) – ZUGANG, SPERRUNG, ERREICHBARKEIT

Dienstleister	Leistung + Kritikalität (K1–K3)	Netz-Zugang? nein / ja: Art (VPN, Fernwartung), Systeme, permanent oder auf Anforderung	Wie sperren wir selbst? (Konto, FW-Regel)	24/7-Notfallkontakt + Vertrags-/Kd-Nr.	SLA / Reaktionszeit im Notfall

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

HAUPTTABELLE DIENSTLEISTER (2/2) – FORTSETZUNG

Dienstleister	Leistung + Kritikalität (K1–K3)	Netz-Zugang? nein / ja: Art (VPN, Fernwartung), Systeme, permanent oder auf Anforderung	Wie sperren wir selbst? (Konto, FW-Regel)	24/7-Notfallkontakt + Vertrags-/Kd-Nr.	SLA / Reaktionszeit im Notfall

Denken Sie an die unscheinbaren Zugänge: Maschinen-Fernwartung, Aufzugs- und Gebäudetechnik, Drucker-Dienstleister, Zeiterfassung, Kaffeemaschinen-Telemetrie. Was nicht in dieser Liste steht, wird bei der Bereinigung übersehen – und führt zur Re-Infektion.

VERTRÄGE & MELDEPFLICHTEN (JE DIENSTLEISTER EINE ZEILE – REIHENFOLGE WIE HAUPTTABELLE)

Dienstleister	Vertragsart (AVV / SLA / NDA) + Fundstelle/Ablage offline	Meldepflicht des Dienstleisters an uns (Frist laut Vertrag)	Unsere Informationspflicht an ihn?	Haftungsregelung / -grenze	Subunternehmer bekannt? / letzte Prüfung

LOG-LIEFERFÄHIGKEIT (FÜR FORENSIK ENTSCHEIDEND)

Dienstleister	Kann Logs liefern? (welche, wie lange rückwirkend)	Wie anfordern (Portal, Ticket, Tel.)?	Angefordert am / durch

NOTIZEN

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

Beweissicherung & Chain-of-Custody

Lückenlose Dokumentation, **wer wann welches Beweismittel gesichert, übernommen und weitergegeben hat** – vom forensischen Image bis zum versiegelten Datenträger. Ohne intakte Chain of Custody sind forensische Ergebnisse vor Gericht angreifbar und für Regressansprüche sowie die Schadenregulierung entwertet.

Stand: Juli 2026 – aktuelle Rechtslage prüfen

Warum dieses Dokument?

Versicherer verlangen Beweiserhalt regelmäßig als Obliegenheit. Und im Zivilprozess – gegen Täter, Dienstleister oder in der D&O-Frage – zählt nur, was nachweisbar unverändert gesichert wurde.

Wann brauchen Sie es?

Ab der ersten Sicherungsmaßnahme – und vor jeder Neuinstallation. Der häufigste Fehler: Systeme werden neu aufgesetzt, bevor Beweise gesichert sind.

Wo aufbewahren?

Als Kopiervorlage im Notfallordner: pro Beweismittel ein Stammblatt mit Übergabekette. Das Original-Protokoll bleibt beim Beweismittel bzw. beim Verwahrort.

So sieht ein ausgefülltes Protokoll aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg, 1.200 MA · Vorfall MM-2026-001 (fiktiv)

Feld	Eintrag
Beweismittel-ID / Beschreibung	BM-2026-001-01 · Notebook Dell Latitude 5540, S/N 7GHK..., Hostname MMA-HR-017 („Patient Zero“ der Phishing-Mail)
Sicherung	12.03.2026, 11:05 durch M. Roth (Argos Security, IR-Team) · forensisches Image via Write-Blocker
Hashwerte	SHA-256 Original = Kopie: a3f9... · Original versiegelt (Siegel-Nr. 00412), Tresor Raum 1.08
Übergabekette	Nr. 1 – 12.03., 11:30: Roth → T. Berger (Muster GmbH, IT-Ltg.), Zweck: Verwahrung · Nr. 2 – 14.03., 09:00: Berger → Kurier (versiegelt) → Forensiklabor NordForensics GmbH, Zweck: Analyse

⚠ **Rechtlicher Hinweis:** Führen Sie forensische Sicherungen nach Möglichkeit durch geschulte Fachkräfte durch – unsachgemäße Sicherung kann Beweise unbrauchbar machen. Stimmen Sie den Umfang der Beweissicherung mit Versicherer und ggf. Ermittlungsbehörden ab.

BEWEISMITTEL-ID	VORFALL-ID	ANGELEGT AM / DURCH

BEWEISMITTEL – BESCHREIBUNG (PRO BEWEISMITTEL EIN BLATT)

Angabe	Eintrag
Gerät / Datenquelle (z. B. Notebook, Server, Log-Export)	
Hersteller, Modell	
Seriennummer	
Hostname / Kennung	
Fundort / Quelle	

SICHERUNG

Angabe	Eintrag
Datum / Uhrzeit der Sicherung	
Sichernde Person + Firma	
Sicherungsmethode (z. B. forensisches Image; Write-Blocker ja/nein)	
Hashwert SHA-256 – Original	
Hashwert SHA-256 – Kopie (muss identisch sein)	
Speicherort des Originals (versiegelt? Siegel-Nr.)	
Foto beigefügt? □ ja □ nein – Ablageort	

NOTIZEN (ZUSTAND, BESONDERHEITEN, LAUFENDE PROZESSE BEIM AUSSCHALTEN …)

ÜBERGABEKETTE (CHAIN OF CUSTODY) – JEDE ÜBERGABE DOKUMENTIEREN

Lfd. Nr.	Datum / Uhrzeit	Übergeben von (Name, Unterschrift)	Übernommen von (Name, Firma, Unterschrift)	Zweck der Übergabe	Zustand / Siegel-Nr.	Aufbewahrungsort
1						
2						
3						
4						
5						
6						
7						
8						

ABSCHLUSS DES BEWEISMITTELS

Vernichtung / Rückgabe am	Durch (Name, Firma)	Freigabe durch (Name, Funktion)

ÜBERSICHT ALLER BEWEISMITTEL ZUM VORFALL (SAMMELLISTE)

Beweismittel-ID	Beschreibung (Gerät / Datenquelle)	Gesichert am / durch	Hash geprüft am	Aktueller Aufbewahrungsort	Status (verwahrt / übergeben / vernichtet)

Tipp aus der Einsatzpraxis: Kopieren Sie für jedes Beweismittel die Blätter 2 und 3 als Satz. Vergeben Sie IDs nach dem Muster BM-[Vorfall]-[laufende Nr.] (z. B. BM-2026-001-01) und notieren Sie den Hashwert sofort bei der Sicherung – nachträglich ist er wertlos.

NOTIZEN

Betroffenen-Benachrichtigung (Art. 34 DSGVO)

Bereitet die Benachrichtigung betroffener Personen bei voraussichtlich hohem Risiko vor: **Prüfschema, Pflichtinhalte nach Art. 34 Abs. 2 i. V. m. Art. 33 Abs. 3 und ein neutraler Mustertext zum Ausfüllen.** Verhindert beides: die verspätete und die panisch-fehlerhafte Kommunikation.

Stand: Juli 2026 – aktuelle Rechtslage prüfen

Warum dieses Dokument?

Bei hohem Risiko ist die Benachrichtigung Pflicht – unverzüglich, in klarer und einfacher Sprache. Wer erst im Ernstfall formuliert, riskiert Fristen, Formfehler und ungewollte Schuldanerkenntnisse.

Wann brauchen Sie es?

Sobald die Risikobewertung (IR-13) „hohes Risiko“ ergibt – oder die Aufsichtsbehörde die Benachrichtigung anordnet. Erst prüfen, ob eine Ausnahme nach Art. 34 Abs. 3 greift.

Wo aufbewahren?

Als Kopiervorlage im Notfallordner, zusammen mit IR-13. Den freigegebenen Text und den Versandnachweis zum Vorfall archivieren.

So sieht ein ausgefüllter Bogen aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg, 1.200 MA · Vorfall MM-2026-001 (fiktiv)

Feld	Eintrag
Prüfung	Hohes Risiko bejaht (Veröffentlichung der Bewerberdaten auf Leak-Seite angekündigt), keine Ausnahme nach Art. 34 Abs. 3 einschlägig
Logistik	E-Mail an die 340 betroffenen Bewerber am 16.03.2026 · Absender: karriere@muster-mb.example · Hotline über HR (Fr. Vogt)
Mustertext (Auszug)	„… wir informieren Sie, dass am 12.03.2026 Unbefugte Zugriff auf einen Server mit Bewerbungsunterlagen hatten. Betroffen sein können Ihr Lebenslauf und Ihre Zeugnisse. Wir empfehlen, auf ungewöhnliche E-Mails zu achten …“
Ansprechpartnerin	Datenschutzbeauftragter Dr. A. Frentz (extern), datenschutz@muster-mb.example

⚠ **Rechtlicher Hinweis:** Der Mustertext (Blatt 3) ist ein neutrales Formulierungsbeispiel und muss auf den Einzelfall angepasst und rechtlich geprüft werden. Keine Schuldanerkenntnisse formulieren – Freigabe durch Rechtsbeistand und ggf. Versicherer einholen.

VORFALL-ID (AUS IR-13)	BEARBEITET VON	DATUM

TEIL 1 – PRÜFUNG: MUSS BENACHRICHTIGT WERDEN?

Prüfschritt	Ergebnis / Begründung
Hohes Risiko bejaht? (Risikobewertung aus IR-13 übernehmen)	
☐ Ausnahme Art. 34 Abs. 3 lit. a: wirksame Verschlüsselung o. ä. Vorkehrungen	
☐ Ausnahme lit. b: nachfolgende Maßnahmen beseitigen das hohe Risiko	
☐ Ausnahme lit. c: unverhältnismäßiger Aufwand → öffentliche Bekanntmachung (wie?)	
Anordnung der Aufsichtsbehörde erhalten? (Datum, Inhalt)	
Entscheidung + Begründung	

FREIGABE DER ENTSCHEIDUNG

Geschäftsleitung (Name, Datum)	Recht (Name, Datum)	Datenschutzbeauftragte/r (Name, Datum)

TEIL 2 – PFLICHTINHALTE DER BENACHRICHTIGUNG (ART. 34 ABS. 2 I. V. M. ART. 33 ABS. 3)

Inhalt	Enthalten? / Wo im Text
☐ Klare, einfache Sprache (kein Fachjargon)	
☐ Art der Verletzung beschrieben	
☐ Name + Kontaktdaten DSB / Anlaufstelle	
☐ Wahrscheinliche Folgen der Verletzung	
☐ Ergriffene / vorgeschlagene Maßnahmen	
☐ Konkrete Empfehlungen an Betroffene (z. B. Passwortwechsel, Phishing-Warnung)	

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

NEUTRALER MUSTERTEXT – LÜCKEN AUSFÜLLEN, ANPASSEN, RECHTLICH PRÜFEN LASSEN

Betreff: Wichtige Information zum Schutz Ihrer Daten

Sehr geehrte/r _____ [Anrede / Name],

wir informieren Sie, dass am _____ [Datum] Unbefugte Zugriff auf _____ [System, z. B. „einen Server mit Bewerbungsunterlagen“] hatten. Betroffen sein können _____ [Datenkategorien]. Nach derzeitigem Kenntnisstand _____ [nur gesicherte Fakten – keine Spekulation].

Mögliche Folgen für Sie: _____ [z. B. Phishing-Versuche]. Wir haben umgehend folgende Maßnahmen ergriffen: _____ [Maßnahmen].

Wir empfehlen Ihnen: _____ [z. B. auf ungewöhnliche E-Mails achten, Passwörter ändern].

Ihre Ansprechpartnerin / Ihr Ansprechpartner: _____ [Name, Funktion], erreichbar unter _____ [E-Mail, Telefon]. Weitere Informationen: _____ [FAQ-Seite / Hotline].

_____ [Ort, Datum] · _____ [Absender, Funktion]

FREIGABE DES TEXTES (VIER-AUGEN-PRINZIP)

Kommunikation (Name, Uhrzeit)	Recht (Name, Uhrzeit)	Geschäftsleitung (Name, Uhrzeit)	Versicherer informiert am

TEIL 3 – LOGISTIK DER BENACHRICHTIGUNG

Angabe	Eintrag
Kanal: ☐ E-Mail ☐ Brief ☐ Website ☐ öffentliche Bekanntmachung	
Absender (Adresse / Postfach – muss erreichbar sein!)	
Zeitpunkt des Versands (geplant / erfolgt)	
Sprachen der Benachrichtigung	
Hotline / FAQ eingerichtet? (wer betreut sie, Nummer, URL)	
Abstimmung mit Aufsichtsbehörde erfolgt am / mit	
Abstimmung mit Versicherer erfolgt am / mit	
Abstimmung mit PR / Kommunikation erfolgt am / mit	

VERSANDNACHWEIS

Datum / Uhrzeit	Kanal	Anzahl Empfänger	Nachweis (Ablageort, z. B. Versandprotokoll)	Durch

NOTIZEN

Stakeholder-Übersicht mit Melde- und Informationspflichten

Eine vorab gepflegte Liste aller Stellen, die im Krisenfall **aktiv informiert werden müssen oder wollen** – von der Hausbank über den Cyber-Versicherer bis zum A-Kunden mit vertraglicher Meldepflicht. Sie legt fest, wer aus dem Krisenstab wen bis wann mit welcher Kernbotschaft anspricht – damit kein wichtiger Partner aus der Presse erfährt, was passiert ist.

Warum dieses Dokument?

Meldefristen stehen verstreut in Policen, Rahmenverträgen und Gesetzen. Im Ernstfall hat niemand Zeit, sie zu suchen – verpasste Fristen kosten Deckung, Vertragsstrafen und Vertrauen.

Wann brauchen Sie es?

Ab Stufe 3: Versicherer binnen Stunden (vor Beauftragung Externer!), A-Kunden laut Vertrag oft binnen 24 h, Behörden nach gesetzlicher Frist – und die Bank, bevor Gerüchte sie erreichen.

Wo aufbewahren?

Ausgedruckt im Notfallordner, gemeinsam mit der Notfall-Kontaktliste (IR-01). Nach jedem Vertragsabschluss mit Meldeklausel wird hier eine Zeile ergänzt.

So sieht ein ausgefüllter Auszug aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg (fiktiv) · Vorfall MM-2026-001

Stakeholder	Pflicht / Frist	Informiert durch / wann	Kernbotschaft & Status
Cyber-Versicherer HanseCyber Versicherung AG, 24/7-Schadenhotline	Police CV-2024-88123: Meldefrist „unverzüglich“ (Obliegenheit!)	Fr. Lindner (Finanzen), binnen 4 h nach Stufe 3 – **vor** Beauftragung externer Dienstleister (Kostenübernahme!)	Erledigt: 13.03., 07:10 Uhr ✓
Hausbank Stadtsparkasse Augsburg, Fr. Maier (Firmenkunden)	keine Frist – aber Vertrauensschutz	GF K. Sommer persönlich, Tag 1	„Zahlungsverkehr läuft über Notverfahren, Liquidität gesichert, wir melden uns täglich.“ ✓
A-Kunde Alpenwerk AG	Rahmenvertrag § 14: Meldung von IT-Vorfällen **binnen 24 h!**	Vertriebsleiter, Tag 1	Kernbotschaft aus Template B (IR-06) ✓
LKA Bayern / ZAC · Landesdatenschutz	Anzeige freiwillig · Art. 33 DSGVO: 72 h ab Kenntnis	Recht, Tag 1 · Dr. A. Frentz (ext. DSB)	Fristbeginn dokumentiert im Entscheidungs-Tagebuch, Nr. 4

⚠ **Der Versicherer kommt vor dem Forensiker.** Wer externe Dienstleister beauftragt, bevor der Cyber-Versicherer zugestimmt hat, riskiert die Kostenübernahme – viele Policen verlangen Dienstleister aus dem Panel des Versicherers. Die Reihenfolge der Anrufe entscheidet über sechsstellige Beträge.

Halbjährliche Prüfung: ☐ Fristen gegen Verträge geprüft ☐ Ansprechpartner aktuell ☐ Zuständigkeiten besetzt
Geprüft am: _____ von: _____

UNTERNEHMEN	STAND / VERSION	VERANTWORTLICH	ORT DER OFFLINE-KOPIE	NÄCHSTE PRÜFUNG

Organisation	Ansprechpartner + Funktion	Telefon / Mobil (nicht nur E-Mail!)	Meldefrist (vertraglich/gesetzlich, Police/§)	Informiert durch (Rolle) + Trigger	Kernbotschaft (1 Zeile)	Erledigt am / durch
CYBER- / D&O-VERSICHERER						
Quelle der Pflicht geprüft am _____ (Vertrag / Police / Gesetz), durch _____						
HAUSBANK(EN)						
Quelle der Pflicht geprüft am _____ (Vertrag / Police / Gesetz), durch _____						
WIRTSCHAFTSPRÜFER						
Quelle der Pflicht geprüft am _____ (Vertrag / Police / Gesetz), durch _____						
BEIRAT / GESELLSCHAFTER						
Quelle der Pflicht geprüft am _____ (Vertrag / Police / Gesetz), durch _____						

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

Organisation	Ansprechpartner + Funktion	Telefon / Mobil (nicht nur E-Mail!)	Meldefrist (vertraglich, §/Klausel)	Informiert durch (Rolle) + Trigger	Kernbotschaft (1 Zeile)	Erledigt am / durch
TOP-10-KUNDEN (VERTRAGLICHE MELDEPFLICHTEN ZUERST PRÜFEN!)						
Quelle der Pflicht geprüft am _____ (Vertrag / Police / Gesetz), durch _____						
KRITISCHE LIEFERANTEN / DIENSTLEISTER (DETAILS IN IR-16)						
Quelle der Pflicht geprüft am _____ (Vertrag / Police / Gesetz), durch _____						

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

Organisation	Ansprechpartner / Meldeweg (Portal, Hotline)	Telefon / Mobil	Meldefrist (gesetzlich – Rechtslage prüfen!)	Informiert durch (Rolle) + Trigger	Kernbotschaft / Inhalt	Erledigt am / durch
BEHÖRDEN						
LKA / ZAC (Anzeige freiwillig)						
Landesdatenschutz-Aufsicht (Art. 33 DSGVO: i. d. R. 72 h ab Kenntnis)						
BSI (nur bei NIS-2- / KRITIS-Pflicht: Frühwarnung 24 h)						
Quelle der Pflicht geprüft am _____ (Gesetz, Stand beachten – NIS-2-Umsetzung kann Details ändern), durch _____						
INTERNE GREMIEN & UMFELD						
Betriebsrat						
Vermieter / Werkschutz						
Quelle der Pflicht geprüft am _____ (Vertrag / Police / Gesetz), durch _____						

Reihenfolge-Regel: Erst Versicherer, dann Behörden nach Frist, dann Kunden mit Vertragspflicht, dann alle übrigen – und jeder wichtige Partner **vor** der Presseinformation. Wer aus der Zeitung erfährt, was passiert ist, bleibt kein Partner.

Wiederanlauf- & Notbetriebsplan

Zwei Teile, ein Ziel: **Teil A** übersetzt die Geschäftsstrategie in Wiederanlauf-Prioritäten und manuelle Workarounds – sonst priorisiert im Ernstfall die IT nach technischer Logik statt nach Umsatz, Vertragsstrafen und Liquidität. **Teil B** legt die IT-Wiederanlauf-Reihenfolge nach Abhängigkeiten fest – mit Freigabe je System, denn ein zu früh gestartetes System führt zur Re-Infektion.

Warum dieses Dokument?

„Welcher Prozess muss zuerst wieder laufen?“ kann im Ernstfall niemand aus dem Stegreif beantworten. Wer die Reihenfolge erst herleiten muss, verliert Tage – und zahlt Vertragsstrafen, die eine Zeile in diesem Plan verhindert hätte.

Wann brauchen Sie es?

Erarbeitet wird es in Ruhe vor der Krise – im Ernstfall ist es ab der Eindämmung das wichtigste Arbeitsdokument: Notbetrieb ab Stunde eins, Wiederanlauf nach Freigabe des IR-Teams.

Wo aufbewahren?

Ausgedruckt im Notfallordner und bei Betrieb/Produktion. Die Offline-Ressourcen (Blanko-Formulare, Kundenlisten auf Papier) lagern dort, wo der Workaround sie braucht.

Vom Geschäft zur Technik – so entsteht die Wiederanlauf-Reihenfolge

Grundregel: Kein System geht ans Netz, bevor es für „sauber“ erklärt wurde – der häufigste Fehler der Wiederanlauf-Phase ist die Re-Infektion aus einem übersehenen System.

So sieht ein ausgefüllter Auszug aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg (fiktiv) · Vorfall MM-2026-001

Prio 1 – Warenausgang/Versand: Vertragsstrafen bei Alpenwerk AG ab 48 h Lieferverzug (25 T€/Tag). Max. Ausfall: 24 h. Workaround: Lieferscheine handschriftlich auf vorgedruckten Blanko-Formularen (Ordner „Notbetrieb“, Schrank Versandbüro), Spediteur-Avisierung per Privathandy des Versandleiters; Abgleich nachträglich. Verantwortlich: H. Gruber. · **Prio 1 – Lohnlauf (Monatsende in 9 Tagen):** 1.200 Gehälter. Workaround: externes Lohnbüro hat Datenstand Vormonat; Abschlagszahlung in Vormonatshöhe über Bank-Notverfahren (mit Fr. Maier, Sparkasse, vorabgestimmt). Verantwortlich: Fr. Lindner (Finanzen). · **Prio 2 – Auftragsannahme:** telefonisch über Ersatznummer, Erfassung auf Papierformular AN-01, Nachpflege nach Restore. · **Prio 3 – Marketing/Webshop-Analytics:** wartet.

Freigegebene IT-Reihenfolge: 1. ERP-Versandmodul · 2. Zahlungsverkehr · 3. E-Mail-Grundbetrieb · 4. CAD/PLM · 5. Rest. – In Teil B beginnt die technische Kette davor mit den Fundamenten: DC-01 (AD, Neuaufbau + autoritativer Restore, 8 h) → DNS/DHCP → ERP-DB-01 (Restore Stand Do 23:00, 6 h) → ERP-App → TS-02 (Neuinstallation – war Patient Zero, kein Restore!).

⚠ **Die IT priorisiert nach Servern, das Geschäft nach Geld.** Ohne Teil A dieses Plans wird im Ernstfall das technisch Naheliegende zuerst wiederhergestellt – nicht das, was Vertragsstrafen, Liquidität und Gehälter sichert. Die Top-5-Reihenfolge auf dem letzten Blatt gibt die Geschäftsführung deshalb vorab frei.

UNTERNEHMEN	STAND / VERSION	VERANTWORTLICH	ORT DER OFFLINE-KOPIE	NÄCHSTE PRÜFUNG

TEIL A (1/2) – GESCHÄFTSPROZESSE UND IHRE PRIORITÄT (EINE ZEILE PRO PROZESS)

Geschäftsprozess	Bereich / Owner	Warum kritisch? (Umsatz, Vertragsstrafe, Gehälter, Sicherheit)	Max. tolerierbare Ausfallzeit (Std./Tage)	Wiederanlauf-Priorität (1–3)	Benötigte IT-Systeme	Abhängig-keiten

TEIL A (2/2) – NOTBETRIEB: MANUELLE WORKAROUNDS (REIHENFOLGE WIE BLATT ZUVOR)

Geschäftsprozess	Manueller Workaround (Formulare, Ort, wer ist geschult?)	Benötigte Ressourcen offline (Blanko-Lieferscheine, Kundenliste auf Papier, Ersatz-Laptop mit LTE …)	Verantwortlich für Notbetrieb	Wie lange durchhaltbar?

Ein Workaround, der nie geübt wurde, ist ein Gerücht. Lassen Sie jeden manuellen Notbetrieb einmal im Jahr eine Stunde lang real durchspielen – erst dann zeigt sich, ob die Blanko-Formulare auffindbar, die Schlüssel vorhanden und die Vertreter geschult sind.

TEIL B – IT-WIEDERANLAUF NACH ABHÄNGIGKEITEN (WIEDERANLAUF ERST NACH FREIGABE JE SYSTEM!)

Nr.	System (Verweis Inventar)	Voraussetzung (muss vorher laufen)	Weg: Restore aus Backup / Neuinstallation / bereinigen	Freigabe „sauber“ durch (IR-Team / wen?)	Funktionstest (was, durch wen?)	Gesch. Dauer	Erledigt am / Kurzzeichen
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							

⚠ **Patient Zero wird nie aus dem Backup wiederhergestellt.** Das zuerst kompromittierte System (im Beispiel: TS-02) wird neu installiert – ein Restore holt die Hintertür zurück. Die Fundamente kommen zuerst: Active Directory vor allem anderen, Datenbank vor Applikation.

TOP-5-REIHENFOLGE FÜR DIE IT – FREIGEGEBEN VOM KRISENSTAB

Prio	System / Modul	Geschäftsgrund (aus Teil A)	Zieltermin nach Freigabe
1			
2			
3			
4			
5			

FREIGABE DURCH DIE GESCHÄFTSFÜHRUNG

Freigegeben am (Datum)	Name Geschäftsführung (Druckbuchstaben)	Unterschrift

Eintrag
Letzte Übung / Probe des Notbetriebs am
Nächste Übung geplant am / verantwortlich

Die Unterschrift ist der Punkt, an dem aus einer Liste eine Entscheidung wird. Im Ernstfall diskutiert niemand mehr die Reihenfolge – sie ist von der Geschäftsführung freigegeben, und das IR-Team arbeitet sie ab. Änderungen entscheidet der Krisenstab und dokumentiert sie im Entscheidungs-Tagebuch.

NOTIZEN