IT-Notfallplan: Stand 2025-09-20

Notizen für die Erstellung des IT-Notfallplan

- **Gestaltung**: Achten Sie auf „Druckbarkeit“, d.h. formatieren Sie evtl. URL/ Links „lesbar“
    - Schlecht: Hier der Link-BSI
    - Gut und lang: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/BSI-Standard-200-4_Hilfsmittel/BSI_Standard_200_4_Hilfsmittel_node.html
    - Gut und kurz: https://t1p.de/00e5p
    - Alternativ als QR-Code:
- **Verteilerkreis & Aufbewahrung**:

Ein IT-Notfallplan enthält sehr sensible und personenbezogene Daten. Daher wählen Sie den Verteilerkreis so klein wie möglich, z.B. Geschäftsführung, IT-Notfallstab, Rechtsbeistand

    - Bewahren Sie den *ausgedruckten* IT-Notfallplan nur an sicheren, abschliessbaren Orten auf, (Bank-)Safe, robuster, abschliessbarer Schrank, etc. Nutzen Sie für die digitale Version einen dedizierten, mit MFA abgesicherten Speicherplatz, z.B. eigene Nextcloud Instanz.

- **Aktualität**: Überprüfen Sie die Aktualität (Kontakte etc.) mindestens einmal pro Quartal. Setzen Sie sich eine wiederkehrende Terminerinnerung.

1. Vorbereitung, Training & BCM

- **Verantwortung**: für den IT-Notfallplan ist verantwortlich...
  - in der Geschäftsführung: Anrede Vorname Name
  - in der IT: Anrede Vorname Name
- **IT-Notfallstab:**
  - Der IT-Notfallstab ist definiert: Teilnehmer, Rollen, Aufgaben
  - Statten Sie mindestens 1-2 IT-Mitarbeiter des IT-Notfallstabs (zusätzlich) mit Non-Windows Systemen wie z.B. Apple oder Linux aus
  - Die „Out-Of-Band"-Kommunikation mit einer sicheren Nachrichten-App, z.B. Threema, ist etabliert und wird aktiv gelebt: eingesetzte Nachrichten-App…
  - Ein sicherer online Speicherort ist eingerichtet, um Daten auch mit externen Teilnehmern *schnell* auszutauschen, z.B. eigene Nextcloud: eingesetzter Speicherort...
- **IT-Sicherheit**:
  - ALLE Endgeräte (Notebooks, PCs, etc.) sind mit aktueller IT-Sicherheitssoftware ausgestattet: eingesetzte Software...
  - ALLE (virtuellen) Server sind mit aktueller IT-Sicherheitssoftware ausgestattet: eingesetzte Software...
  - ALLE Firewalls sind auf aktuellem Stand, erhalten regelmäßige Sicherheits-Updates vom Hersteller und sind in der (Software-)Wartung: eingesetzte Software...
- **Backup**:
  - Ein geprüftes und aktuelles Backup-Konzept liegt vor: Name, Speicherort...
  - Backups von allen relevanten Systemen werden regelmäßig durchgeführt und auf Wiederherstellung getestet: eingesetzte Software...
  - Die Backups (Tapes/ HDDs, etc.) werden an mindestens zwei verschiedenen Orten aufbewahrt, z.B. anderes Gebäude, (Bank-)Safe, Nextcloud etc.: Ort 1, Ort 2, Ort 3, ...
- **BCM – Business Continuity Management**:
  - Ein geprüftes und aktuelles BCM-Konzept liegt *idealerweise* vor: Name, Speicherort…
  - Kernpunkte sind z.B. Ausfall von: Telefonie, Email, File-Server, ERP, Endgeräte (Notebooks, PCs), Server, Backup-Server
  - Jeweils betrachtete Zeiträume: ein Tag, eine Woche, ein Monat

2. Einschlag

- **Ruhe schaffen & bewahren**:
  - Hängen Sie ein Schild mit „IT-Notfall – bitte nicht stören!“ an Ihre Tür
  - Aktivieren Sie automatisches Antworten in Ihrem Email-Postfach für INTERN mit z.B. „IT-Notfall – wir sind dran!“
  - Setzen Sie eine Status-Meldung auf Teams etc. „IT-Notfall“
  - Starten Sie mit dem Team ein Logfile(s) (.txt) und notieren Sie sich fortlaufend Stichpunkte oder nutzen Sie online Nexcloud Dokumente zum zentralen Austausch
- **Einsatz IT-Notfallstab**
  - Bleiben Sie ruhig
  - Je nach Situation, setzen Sie alle Passwörter (der User) zurück und ändern entsprechende Administratoren Passwörter. Stellen Sie UNBEDINGT sicher, dies nur auf garantiert „sauberen“ Systemen durchzuführen (Key-Logger, etc.).
  - Schaffen Sie Struktur, z.B. kurze Team-Updates alle 30 Minuten.
  - Fokussieren Sie auf das wirklich Wesentliche. Trinken und Essen Sie, machen Sie kleine Pausen nach Absprache mit dem Team
- **Kontakt IT-Sicherheit Dienstleister**
  - "First-Responder & Forensik"
    - Nutzen Sie die Ihnen bereits bekannte Hotline und berichten kurz den Vorfall
    - Starten Sie eine Video-Konferenz mit allen relevanten Teilnehmern, nutzen Sie, wenn möglich, immer den gleichen Termin/ Channel
  - Cyber-Versicherung
    - Melden Sie zeitnah den Vorfall Ihrer Cyber-Security Versicherung
    - Idealerweise kann Sie hierbei der Rechtsbeistand unterstützen
  - Hausbank
    - Informieren Sie den Sicherheitsberater Ihrer Hausbank durch die Geschäftsleitung (CFO)
    - Beraten Sie sich über zusätzliche (temporäre) Maßnahmen im speziell ausgehenden Zahlungstransfer

3. Erste Hilfe

- **"Sicherheit geht vor."**
  - Leben geht vor. Ein brennender Server ist tragisch, kann aber ersetzt werden.
  - Reagieren Sie ruhig und entschlossen. Ein IT-Notfall ist ein Notfall. Es wird kollateral Schäden geben. Eine kurze Rücksprache mit dem Team kann hilfreich sein, um schnell ein Meinungsbild zu erhalten.
  - Auch bei einem IT-Notfall müssen Sie irgendwann schlafen. Sprechen Sie sich, falls möglich, mit Ihrem Team ab. Nutzen Sie Power-Naps und das Notiz-Logfile (oder Nextcloud), um sich schnell aufzufrischen.
- **Betroffene IT-Systeme isolieren/ abschalten**
  - **Operativ**: je nach Sicherheitssoftware wird das betroffene/ kompromittierte System sofort isoliert. Bei manuellen Entscheidungen ist unsere Empfehlung: wenn Sie sich bei einem System unsicher sind, schalten Sie es aus.
  - **Präventiv**: fokussieren Sie sich auf das Kernsystem (ERP). Reduzieren Sie Einfallsvektoren und nehmen (Sekundär-)Umsysteme vom Netz, z.B. File-Server, Print-Server, Web-Portale, etc.
  - **Situativ**: schränken Sie Zugänge (vorübergehend) stark ein, z.B. nach Geo-Daten oder Arbeitszeiten am Hauptstandort. Sicherheit geht vor.
- **Auf "Notstrom" umschalten**
  - Eventuell müssen Sie bereits automatisierte Prozesse temporär teil-automatisieren mit manuellen Export- und Import Interim Prozessen.
  - Bei Ransomware Attacken empfiehlt es sich, ausgewählten Key-Usern in den Fachabteilungen Non-Windows Systeme (temporär) zur Verfügung zu stellen, z.B. Apple, Linux
  - Definieren Sie kurze Updates für die Key-User in den Fachabteilungen, z.B. alle zwei Stunden im Stand-Up Format, max. 10min

4. Kommunikation

- **Unternehmensführung intern**
  - Ein Austausch zwischen Unternehmensführung und IT-Notfallstab empfiehlt sich ca. alle 4 Stunden für ca. 20min
  - Je nach Situation gilt: „Das Gras wächst nicht schneller, wenn man daran zieht.“
- **Mitarbeiter**
  - Informieren Sie Ihre Mitarbeiter einmal täglich, z.B. 18:00 Uhr über die Ereignisse des Tages. Je nach Situation über das „Schwarze Brett“ oder via Email an die geschäftliche oder private Email Adresse (mit Einverständnis).
  - Finden Sie eine gute Mischung aus (vertraulichen) technischen Details und Relevanz für das Unternehmen.
- **Extern**
  - Informieren Sie eventuell betroffene Kunden/ Partner umgehend. Besprechen Sie die Inhalte vorab mit Ihrem Rechtsbeistand und der Geschäftsführung.
  - Falls Sie externe Web-Portale oder Webshops abschalten müssen, stellen Sie in der Zwischenzeit eine vorbereitete „Wartungsseite“ online.

5. Erste Ordnung: Kernsysteme

- **IT-Notfallstab arbeitet in RUHE**
  - Priorisieren und fokussieren unbedingt auf die Kernsysteme (ERP)
  - Notieren sie unbedingt alle Erkenntnisse, idealerweise zentral und online, z.B. Nextcloud
  - Bitten Sie die Fachabteilungen um Geduld und Unterstützung
- **IT-Sicherheit Dienstleister arbeitet in RUHE**
  - Analyse und Forensik benötigen Zeiträume
  - Unterstützen Sie den/ die Dienstleister mit zeitnahen Rückmeldungen
  - Stellen Sie Fragen und halten Ihre Notizen auf dem Laufenden
- **Überprüfung Backup**
  - Sobald der Zeitpunkt der Infiltration bekannt ist, überprüfen Sie vorhandene Backups
  - Eventuell benötigen Sie eine gesonderte (temporäre) Systemlandschaft zur Wiederherstellung von Backups. Kontaktieren Sie entsprechend IT-Dienstleister für Unterstützung.
  - Falls Sie Backup-Bänder von Ihrem Bank-Safe benötigen, beachten Sie (eventuell) die Öffnungszeiten

TOP3 Kernsysteme

Kernsysteme	Kontakt	Mobil Geschäft	Email Geschäft	FQDN	IP(s)
Kernsystem 1					
Kernsystem 2					
Kernsystem 3					

6. Aufgabenverteilung

- **Volle Unterstützung für IT-Notfallstab**
  - „Hätten wir dies, hätten wir das…“ hilft nicht weiter. Schauen Sie nach vorne.
  - An die Geschäftsleitung: investieren Sie in Pizza, Schokolade und Cola/ Kaffee
  - An die Mitarbeitenden: ein kurzes „Hallo, wollte mal sehen, wie es euch geht?“ hilft hier-und-da
- **Mitarbeiter im BCM-Modus**
  - Ein IT-Notfall ist eine Sondersituation. Unterstützen Sie so gut Sie in IHREM Bereich können.
  - Personalabteilung (HR): je nach Situation können Überstundenabbau oder spontaner Urlaub unterstützen
  - BCM ist dynamische Stabilität. Nur weil etwas heute nicht möglich ist, heisst das nicht, dass es in zwei Tagen vielleicht mit einem Workaround wieder geht.
- **Dienstleister Unterstützung**
  - Versuchen Sie einen „Kaltstart“ zu vermeiden. Informieren Sie sich frühzeitig über mögliche Dienstleister, die zu Ihnen passen und Ihnen im IT-Notfall verlässlich zur Seite stehen können.
  - Idealerweise können Sie auf langjährige, partnerschaftliche Dienstleister zählen. Diese kennen bereits Ihre System und können meist sehr schnell produktiv unterstützen.
  - Bauen Sie sich ein kleines Netzwerk von vertrauensvollen Dienstleistern auf. Im IT-Notfall können Sie so schnell auch mal eine zweite Meinung einholen.

7. Zweite Ordnung: Kern- und Umsysteme

- **Kernsysteme sind wieder "Grün"**
  - Bleiben Sie aufmerksam.
  - Priorisieren Sie die Bereiche, die wieder produktiv mit den Systemen arbeiten, z.B. „Finance first“.
  - Bringen Sie langsam wieder Last auf die produktiven Systeme, z.B. starten Sie manuell automatisierte Prozesse (Hintergrundjobs etc.).
- **Umsysteme schrittweise in RUHE hochfahren**
  - Überprüfen Sie die Umsysteme auf Sicherheitslücken BEVOR Sie diese wieder hochfahren, bzw. von „Aussen“ wieder erreichbar machen.
  - Dokumentieren Sie den Wiederanlauf.
  - Planen Sie Puffer ein, z.B. alle 4 Stunden ein weiteres System
- **Überprüfung Prozesse durch Key-User**
  - Lassen Sie ausgewählte Prozesse & Transaktionen durch die Key-User in den Fachbereichen „end-to-end“ durchführen. Falls möglich, zu Beginn auf den Test-Systemen und nach erfolgreichem Resultat in den produktiven Systemen. Hier hilft auch die Unterstützung von z.B. „befreundeten“ (Pilot-)Kunden.
  - Führen Sie eine zentrale Liste mit den Prozess Ergebnissen auf die die Key-User gemeinsam zugreifen und editieren können.
  - Etablieren Sie diese (temporären) Überprüfungen über einen Meilenstein hinweg, z.B. Monatsabschluss.

TOP5 Umsysteme

Umsysteme	Kontakt	Mobil Geschäft	Email Geschäft	FQDN	IP(s)
Umsystem 1					
Umsystem 2					
Umsystem 3					
Umsystem 4					
Umsystem 5					

8. Übersicht

- **Entwarnung**
  - Entwarnung kann es nur für den aktuellen Vorfall geben. Leider.
  - Nutzen Sie die Kommunikation über die Entwarnung zur Sensibilisierung der Mitarbeitenden.
  - Idealerweise können Sie die Entwarnung mit einer kurzen Zusammenkunft der Mitarbeitenden verbinden.
- **Hyper-Care**
  - Je nach Angriffsvektor empfiehlt sich eine 2-4 wöchige Hyper-Care Phase. In dieser Zeit gilt für den IT-Notfallstab ein erhöhter Fokus auf geringere Auffälligkeiten.
  - Änderung der Melde-Filter von evtl. „nur HIGH“ auf „LOW, MID und HIGH“, um alle Meldungen prüfen zu können.
- **Ent-Spannung**
  - Nach der Cyber-Attacke ist vor der nächsten Cyber-Attacke.
  - Planen Sie (rollierenden) Überstundenabbau und/ oder Urlaub für den IT-Notfallstab ein.
  - Geschäftsleitung: investieren Sie in ein (kleines) Team-Event

9. Lernkurve

- **Dokumentation Vorfall**
  - Investieren Sie unbedingt ausreichend Zeit in die Aufarbeitung des Vorfalls, um zukünftige Wiederholungen zu vermeiden.
  - Nutzen Sie Ihre Notizen, um eine prägnante Zusammenfassung für die Cyber-Security Versicherung erstellen zu können.
  - Teilen Sie Ihre Erfahrungen mit anderen Unternehmen, z.B. über CIO Netzwerke.
- **Umfrage BCM bei Mitarbeitern**
  - Je nach Situation/ Ablauf, nutzen Sie die Ereignisse, um von den Mitarbeitenden zu erfahren, wie das aktuelle BCM-Konzept verbessert werden kann.
  - Bauen Sie offene Fragen in die Umfrage mit ein, um eventuell ganz neue Erkenntnisse zu gewinnen.
- **Validierung Dienstleister**
  - Überprüfen Sie möglichst objektiv die Qualität der Unterstützung ihrer Dienstleister.
  - Wie war die Verfügbarkeit, Reaktionszeit, Tiefe des Verständnisses und allgemeine Kompetenz?
  - Wurde der Vorfall gemeinsam als „Team of Teams“ bearbeitet oder haben Sie anderes erlebt?
  - Wie ist der Blick nach Vorne? Welche präventiven Vorschläge/ Ideen kamen von welchem Dienstleister?
  - Sind Sie zufrieden mit Ihrer Cyber-Security Versicherung?
- **Kaizen/ KVP**
  - Wäre der Vorfall vermeidbar gewesen? Falls ja, wie?
  - Was hat sich seit dem Vorfall sichtlich/ spürbar verändert?
  - Hat der Vorfall die Mitarbeitenden sensibler gemacht? Falls ja, ist es messbar?

10. Kontakte

Intern: Unternehmensführung

Rolle	Inhaber	Geschäftsführer	Finanzen	Rechtsabteilung	...
Name					
Mobil Geschäft					
Mobil Privat					
Email Geschäft					
Email Privat					

Intern: IT-Notfallstab

Rolle	IT Leiter	IT Admin	IT Sicherheit	ERP	...
Name					
Mobil Geschäft					
Mobil Privat					
Email Geschäft					
Email Privat					

Extern: Cyber-Versicherung & IT-Dienstleister

Rolle	Cyber-Versicherung	IT-Sicherheit	Hard- und Software	Netzwerk	...
Name					
Ansprechpartner					
Mobil Geschäft					
Email Geschäft					

Extern: TOP5 Kunden & Lieferanten

Firma	Kontakt	Mobil Geschäft	Email Geschäft	Bereich	Notizen...
Firma 1					
Firma 2					
Firma 3					
Firma 4					
Firma 5					