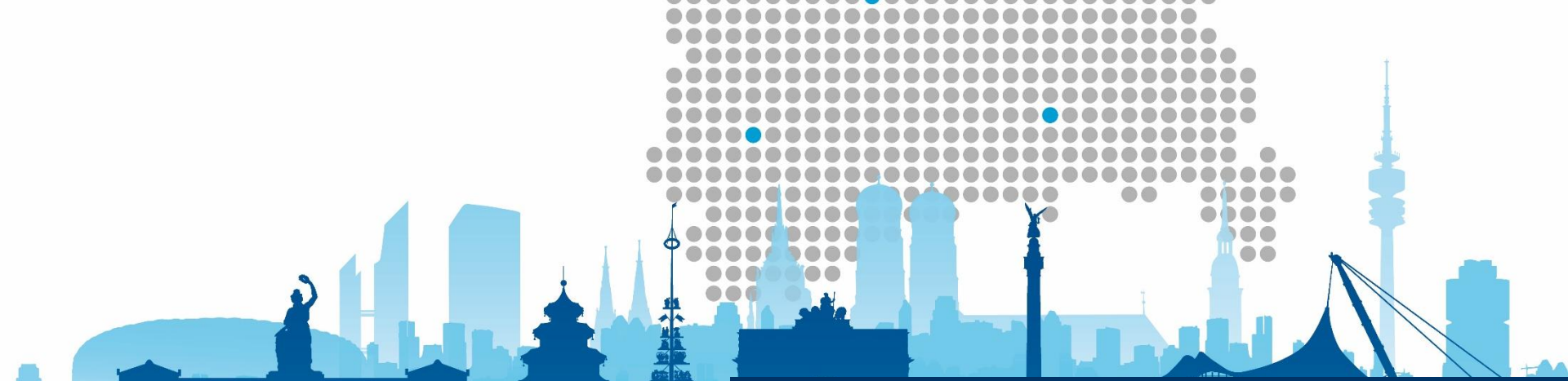


IT-Notfallplanung

Gut gerüstet für den Krisenfall

IHK

Wer steht vor Ihnen?

Bernhard Kux

- IHK: Referent Cybersicherheit, digitale Infrastruktur, Digitalisierung
- IHK: 17 Jahre IT-Sicherheitsbeauftragter
- 089 – 5116 -1705
- kux@muenchen.ihk.de
- www.linkedin.com/in/bernhardkux

Dieser Workshop

Das haben wir vor:

- Warum IT-Notfallplan? Ziele IT-Notfallplan?
- Was ist ein IT-Notfall?
- Standardansätze: ISO, BSI...
- Muster für IT-Notfallplanung
- 10 Fragen an Sie

Wer nimmt hier teil?

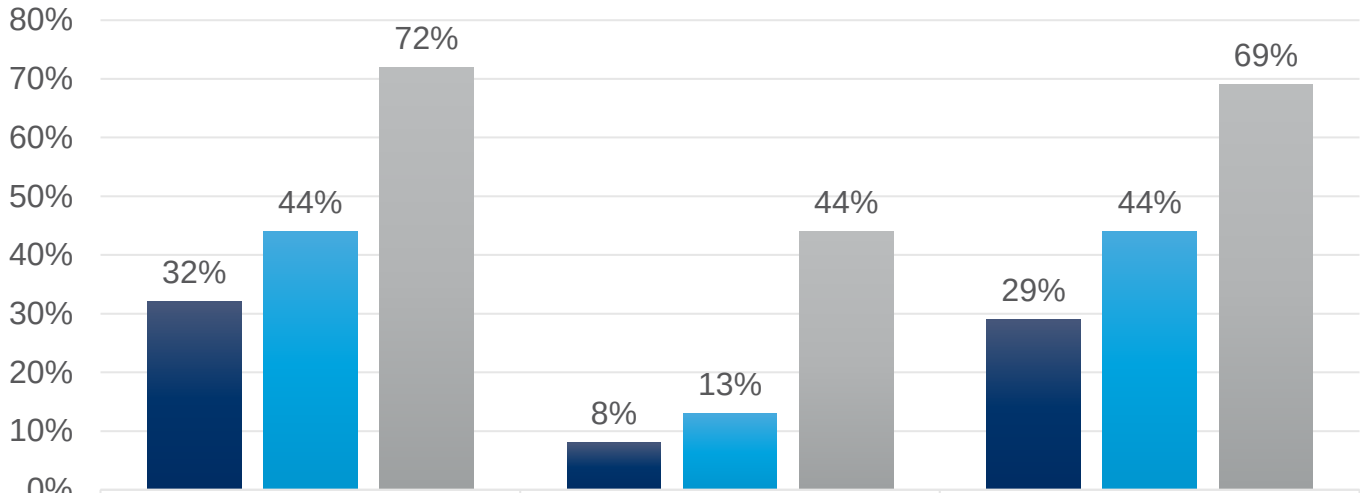
Mitarbeiterzahl im Unternehmen:

- bis 19 Mitarbeiter
- 20 bis 249 Mitarbeiter
- mehr als 249 Mitarbeiter

Haben Sie einen IT-Notfallplan?

- Ja
- Nein

IHK Digitalisierungsumfrage



	Notfallplan	Notfallübungen	Informationssicherheits-beauftragte(r)
bis 19 Mitarbeiter	32%	8%	29%
20-249 Mitarbeiter	44%	13%	44%
mehr als 249 Mitarbeiter	72%	44%	69%

IT-Notfallplan

Ziele IT-Notfallplan:

- Auf IT-Ausfälle oder Sicherheitsvorfälle vorbereitet sein
- Geschäftskritischen Prozesse schnellstmöglich wiederherstellen können
- Schäden minimieren und Handlungsfähigkeit bewahren.

IT-Notfallplan

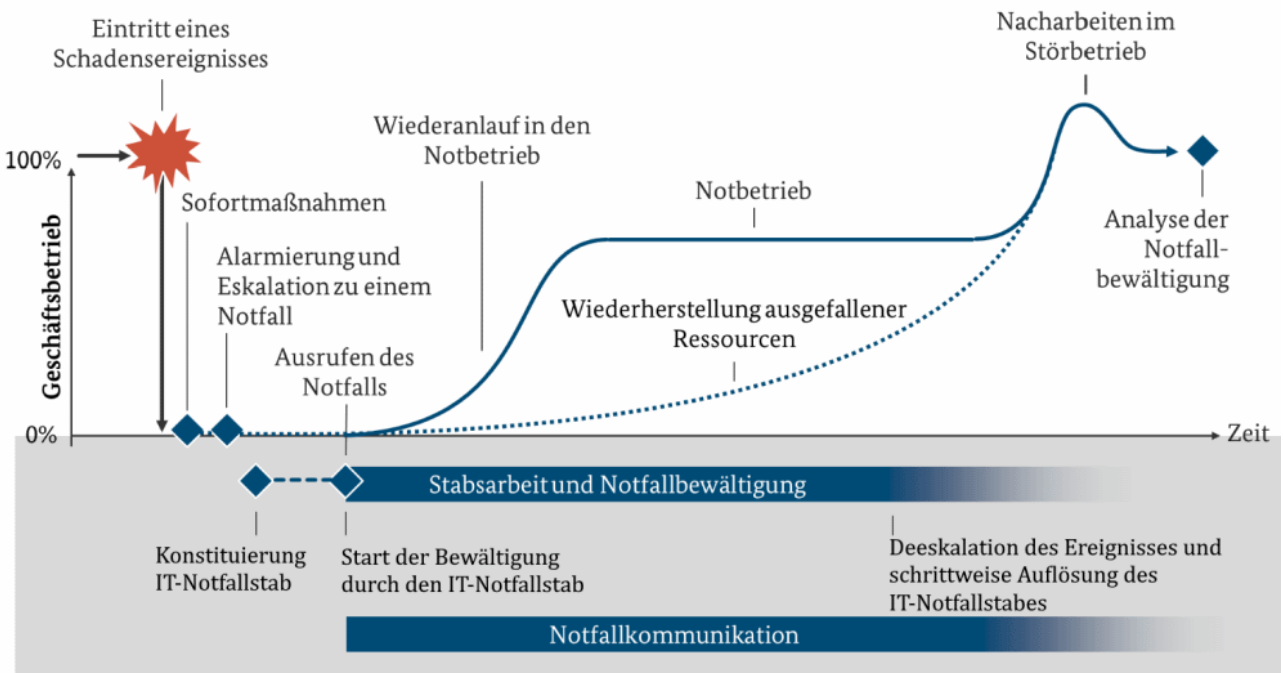
Nachteile IT-Notfallplan:

- Erstellung und Aktualisierung kostet Geld, Zeit, Nerven…
- Verbesserung IT & Prozesse kostet Geld, Zeit, Nerven…

Vorteile IT-Notfallplan:

- Zeitgewinn im IT-Notfall
- Handlungsoptionen erkennen
- Pflichten berücksichtigen
- Vor dem IT-Notfall: Gutes Gefühl

IT-Notfall: Verlauf nach BSI 200-4



Ursachen für IT-Notfälle

- **Technische Ursachen:**
  Hardware-Ausfälle, Probleme mit Software, Netzwerken, Datenbanken…
- **Angriffe:**
  Ransomware, Phishing, Malware, Datenlecks, Überlastungen (DDoS), Sabotage…
- **Menschliches Versagen:**
  Fehlbedienung, Fehlkonfiguration, Verlust von Zugangsdaten, mangelndes Know-How…
- **Externe Einflüsse:**
  Naturkatastrophen, Stromausfall, Vandalismus…
- **Organisatorische Schwächen:**
  Keine Redundanz, kein Backup, veraltete Abwehrsoft- und Hardware
- **Externe Dienstleister, Lieferkettenprobleme:**
  Ausfall IT-Dienstleister, Cloud- oder SaaS-Anwendung

IHK: 3. August 2022

Hauptdienstleister:

- Plötzlicher Ausfall: Kein Internet, keine Mail, kein Telefon, keine Anwendungen
- Unklar wie lange

IT-Notfallplan:

- Checkliste für Handlungsoptionen: Was tun?
- IT-Notfallteam, IT-Team, Dienstleister…
- Interne & externe Kommunikation: Sprachregelungen & Mitarbeiter

Vorhandene Ansätze: ISO 2700X

ISO 27001:2022
Einführung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines Informationssicherheits-Managementsystems (ISMS)

ISO 27002:2022: Maßnahmen zur Steigerung der Informationssicherheit
Kapitel 5.29 „Betriebsunterbrechungen“

Kapitel 5.30 „IKT-Bereitschaft für Business Continuity“
- Zuständigkeiten und Verantwortlichkeiten
- Business Continuity Plans (BCP)
- Regelmäßige Risikobewertung und –analyse
- Angemessene Organisationsstruktur
- Mitarbeiter: Schulung, Sensibilisierung
- Testen und Überprüfen

Vorhandene Ansätze: ISO 22301, TISAX, KRITIS, NIS2

ISO 22301: Business Continuity Management (BCM)

- Grundsätzliche Geschäftsprozesse (nicht nur IT)
- Fokus auf der Aufrechterhaltung des Geschäftsbetriebs

TISAX (Automobilindustrie), KRITIS, NIS2:

Risikoanalyse (insb. Lieferkette) → IT-Notfallplan wird eingefordert

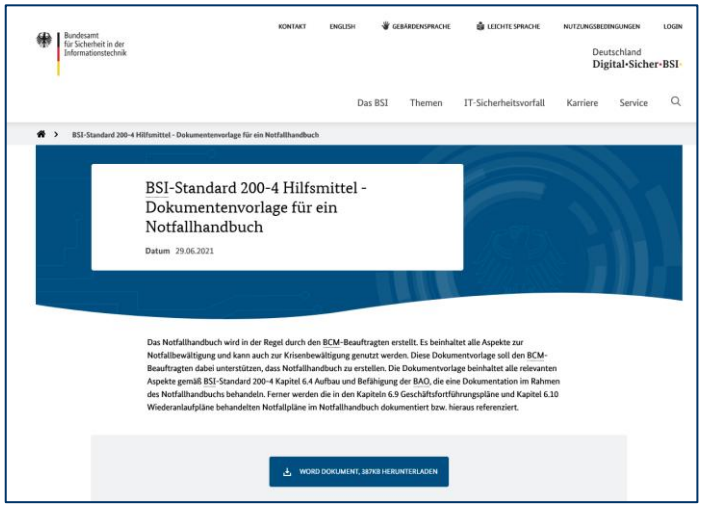
Muster für IT-Notfallplanung:

- BSI-Onepager „Einstieg ins IT-Notfallmanagement für kleinere und mittelständische Unternehmen (KMU)“
- BSI 200-4
- KonBriefing Research
- Österreichisches Informationssicherheitshandbuch
- Muster IHK für München und Oberbayern

Beispiel BSI 200-4

Mustervorlagen:

- Notfallhandbuch
- Geschäftsfortführungsplan, Notbetrieb
- Wiederanlauf- / Wiederherstellungsplan
- …



Grundprinzip Notfallhandbuch

Notfallhandbuch Inhalt:

- Grundsätzliches: Ziel, Geltungsbereich, Definitionen
- Sofortmaßnahmen
- Alarmierung, Eskalation
- IT-Notfallteam: wer, wo, wann, wie…
- Geschäftsfortführung, Notbetrieb
- Wiederanlauf
- Anhänge: Kontakte…

Beispiel BSI 200-4: Geschäftsfortführungsplan - Word

Szenario: Ausfall von E-Mail

IT-Service	BC-Strategie/ BC-Lösung	Gilt für Geschäfts-prozess(e)	RTA/ RTO	RPA/RPO	Maßnahmen, um den Notbetrieb zu erreichen (Wiederanlauf in den Notbetrieb)	Maßnahmen für die Geschäftsfortführung (Notbetrieb)	Maßnahmen zur Rückführung in den Normalbetrieb (Nacharbeiten im Störbetrieb)
E-Mail	*2/Nutzung von Telefon und Fax*	*Alle*	*1 Tag/ < 2 Tage*	*Alle 8 Std./Vor-tageswert (Nacht-sicherung)*	• *Ausweichen auf Telefon, Fax („Workaround“)* • *Vorgefertigte Bandansage auf zentraler Hotlinenummer durch die IT-Abteilung bespielen lassen. Die Bandansage ist an folgender Stelle abgelegt: <Ablageort / Link>* • *Vorgefertigte Information auf Website durch die Öffentlichkeitsarbeit (ÖA)-Abteilung hinterlegen lassen. Die Information ist an folgender Stelle abgelegt: <Ablageort / Link>* • *[…]*	• *Kommunikation erfolgt via alternativer Kommunikationsmittel* • *<Notfallteam A> prüft das Fax und den Anrufbeantworter alle 30 Minuten auf eingehende Nachrichten und leitet diese ggf. weiter* • *Ggf. zusätzliche Kräfte aktivieren, um Arbeitsrückstände zu minimieren* • *Bearbeitete Anfragen dokumentieren. Das vorgefertigte Schema liegt an folgender Stelle ab: <Ablageort / Link zum Dokument>*	• *Wiederhergestellt und ungelesene Emails prüfen* • *Bearbeitete Anfragen mit den wiederhergestellten und ungelesenen Emails abgleichen* • *Zuordenbare und bereits bearbeitete Email-Anfragen löschen* • *Nicht zuordenbare bzw. nicht bearbeitete Anfragen nacharbeiten* • *Arbeitsrückstand ggf. mit zusätzlicher Unterstützung abarbeiten* • *BCM-Koordinator meldet an*

Glossar:

BC: Business Continuity

RTA (Recovery Time Achievable) / RTO (Recovery Time Objective):
Wie schnell Notfall-Lösung betriebsbereit?

RPA (Recovery Point Achievable) / RPO (Recovery Point Objective):
zugesicherter / geforderter Datensicherungszyklus

IHK-Muster: IT-Notfallplan Anwender - Excel

++++ Funktionsbereich .... ++++ Funktionsbereich ... ++++

Stand 10.10.2023, IT-Notfallplan: Funktionsbereich ....N.N., N.N.

Anwendung	Problem	Priorität	Wichtigste Anwendungsfälle	Analoger Prozess	Erforderlicher IT-Service	Anmerkung / Begründung	Auswirkungen			Workaround / Plan A	Plan B	Maßnahme zur Vorbereitung auf einen IT-Notfall
							Rechtliche Folgen	Außenwirkung	Innenwirkung			
Anwendung 1	Netzwerklaufwerk steht nicht zur Verfügung			nein	Netzwerklaufwerk						./.	
Anwendung 2	E-Mail steht nicht zur Verfügung			nein	E-Mail, Internet					Kommunikation per Notfallmailadresse	Kommunikation per Onlineformular	Notfallmailadressen inkl. Zugriff auf DNS für Domainkonfiguration (MX)
	Internet steht nicht zur Verfügung			ja						Kommunikation per Briefpost	Kommunikation persönlich vor Ort	Notfall-Laptop mit Internet per Mobilfunk

BSI-Onepager

Onepager „Einstieg ins IT-Notfallmanagement für kleinere und mittelständische Unternehmen (KMU)“:

1. Vorbereitung: Kümmerer, Kronjuwelen, Kontakte…
2. Bereitschaft: IT-Notfall erkennen & einschätzen
3. Bewältigung: Wer kann helfen? Was kann / muss / soll getan werden?
4. Nachbereitung: Was besser machen?

Kümmerer? Was ist wichtig?

Bitte notieren Sie auf Ihrem Block:

1. **Wer kümmert sich in Ihrem Unternehmen um IT-Sicherheit?**
   → IT-Leiter? IT-Sicherheitsbeauftragter? Dienstleister? Sie? …

2. **Was ist Ihr wichtigster IT-gestützter Prozess im Unternehmen? (wichtig = z. B. wenn nicht verfügbar, hoher Schaden)**
   → Kundenmanagement (CRM), Finanz- und Buchhaltungsprozesse (Gehälter, Rechnungen…), Logistik und Warenwirtschaftssysteme (ERP), OnlineShop, Website…
   → In Ruhe entscheiden, was wichtig ist und was weniger wichtig ist…

Wie erfahren Sie von Problemen?

Bitte notieren Sie auf Ihrem Block:

3. **Wie würden Sie von Problemen beim wichtigsten Prozess erfahren?**
   → Wie sehen Problem-Meldewege für Mitarbeiter und Kunden am Samstagabend aus?
   Bieten Sie ein BugBounty-Programm?
   Beobachten Sie / IT-Sicherheitskümmerer Presse, Schwachstellen, Darknet etc.?

IT-Notfallteam? Wer kann noch helfen?

Bitte notieren Sie auf Ihrem Block:

4. **IT-Notfallteam(s): Welche Personen sind involviert wenn wichtigster Prozess von IT-Notfall betroffen?**
   → Unmittelbare IT: Interne, IT-Experten, Dienstleister? Sie? …
   → Entscheidungsebene: Personalabteilung, Öffentlichkeitsarbeit, Rechtsabteilung, Vertriebsleiter…?

5. **Welche externen Hilfe-Einrichtungen könnten / sollten / müssen einbezogen werden? Wie entscheiden ob?**
   → Polizei (ZAC), Cyberversicherung, regulärer IT-Dienstleister, spezieller IT-Sicherheitsdienstleister, Meldepflichten…

Was ist sofort zu tun? Kommunikation?

Bitte notieren Sie auf Ihrem Block:

6. **Sofortmaßnahmen: Was muss man ohne Zögern tun?**
   → Beweise sichern (Logfiles, Bildschirm abfotografieren…), Backups sichern (funktionsfähig?), Abtrennen der Problem-IT, Situation nachvollziehbar machen (Protokoll starten)…

7. **Mit welchen Betroffenen müssten Sie wie kommunizieren?**
   →Wer: z. B. Kunden, Mitarbeiter, Dienstleister, Presse…
   Wie, wenn Mail und Festnetz weg? Diensthandies, Notfallwebsite, Socialmedia, Messenger…

Notbetrieb und Wiederherstellung

Bitte notieren Sie auf Ihrem Block:

8. **Notbetrieb:**
   Wie könnte das für den wichtigsten Prozess aussehen?
   → Inbetriebnahme der vorhandenen Notfall-IT (zuletzt gestestet wann?)? Umstellung der Prozesse (z. B. analog statt digital)? Warten auf die wiederherstellte IT?

9. **Wiederherstellung: Aufwand, Arbeit, Chance, Neuanfang…**
   → IT wieder 1:1 wie vor dem IT-Notfall wieder aufbauen?
   Oder Neuaufbau mit neuer IT? Oder: Beerdigen „alter IT“?
   → Datenmigration Notbetrieb zur wiederhergestellten IT?

Wie machen Sie weiter?

Bitte notieren Sie auf Ihrem Block:

10. Wie machen Sie weiter?

→ **Kümmerer** für IT-Sicherheit festlegen & Ressourcen ausstatten!

→ **Grundlegende IT-Hausaufgaben machen:**
Technische Absicherung: Firewall, Updates…
Daten sichern: Backups, Zugriffskontrolle…
Schulung der Mitarbeiter: Sensibilisierung für IT-Risiken…

→ Am IT-Notfallplan weiterarbeiten

IHK-Website

www.ihk-muenchen.de/informationssicherheit/

Gut zu wissen

Pack ma´s digital

Unter dem Motto „Pack ma‘s digital“ engagiert sich die IHK für München und Oberbayern, um kleine und mittlere Unternehmen bei der Digitalisierung zu unterstützen und die Zukunft des Standorts Oberbayern zu sichern.

packmasdigital.de

Aktuelles und Veranstaltungen:

ihk-muenchen.de

Anmeldung zum Newsletter:

ihk-muenchen.de/newsletter

Aufzeichnungen von Webinaren:

ihk-muenchen.de/webinare