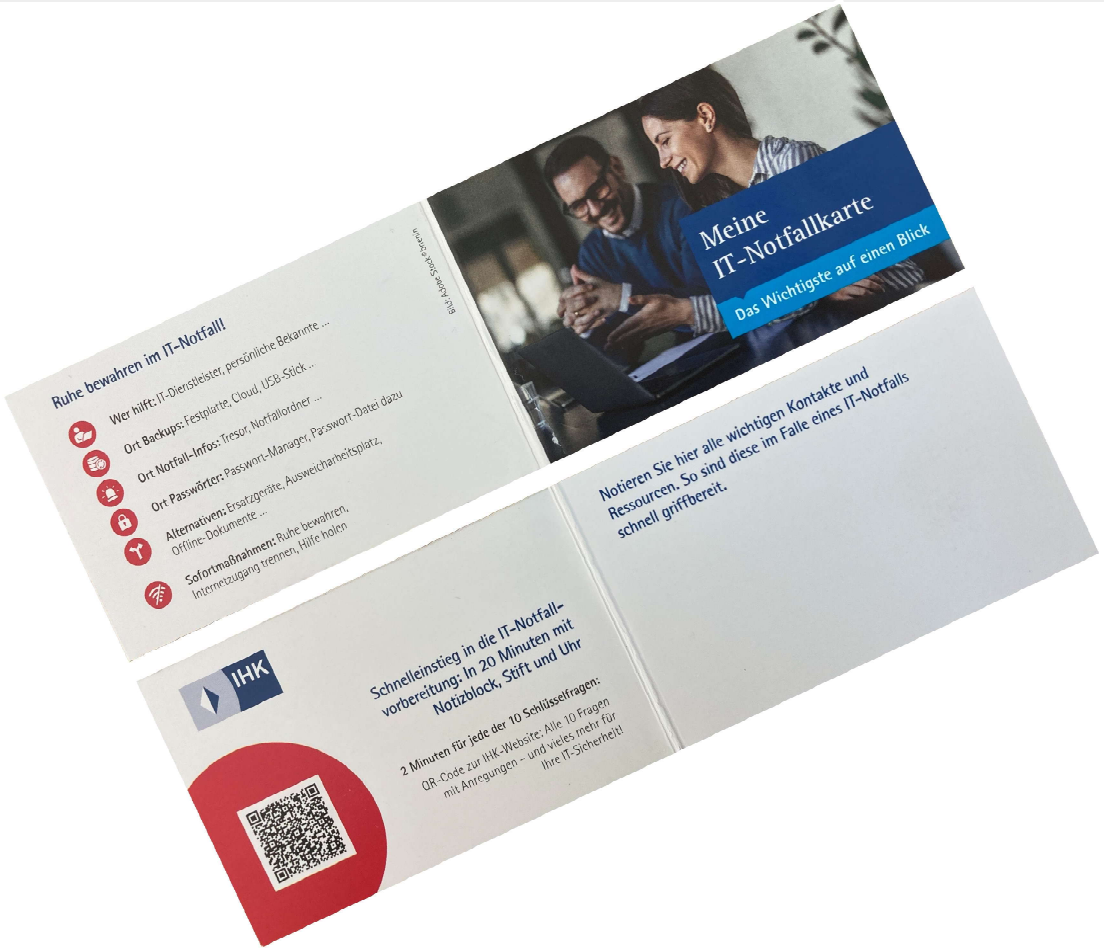
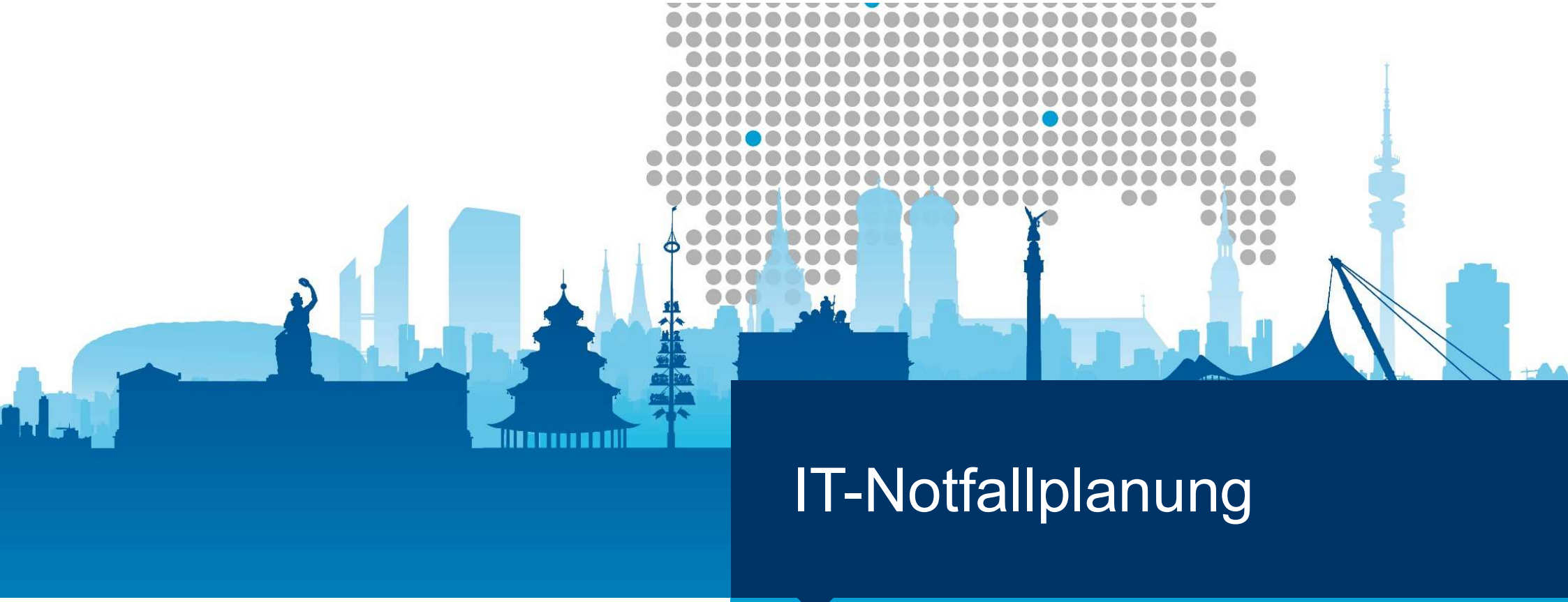
Workshop!

Sie brauchen für diesen Workshop etwas zum schreiben!

- Papier, Stift
- Digital





IT-Notfallplanung

Gut gerüstet für den Krisenfall

IHK

Ihr Impulsgeber

Bernhard Kux

Referent für Cybersicherheit, digitale Infrastruktur, Digitalisierung

089-5116 1705
kux@muenchen.ihk.de
https://www.linkedin.com/in/bernhardkux/

Dieser Workshop

Das haben wir vor:

- Warum IT-Notfallplan? Ziele IT-Notfallplan?
- 10 Fragen an Sie

Wer nimmt hier teil?

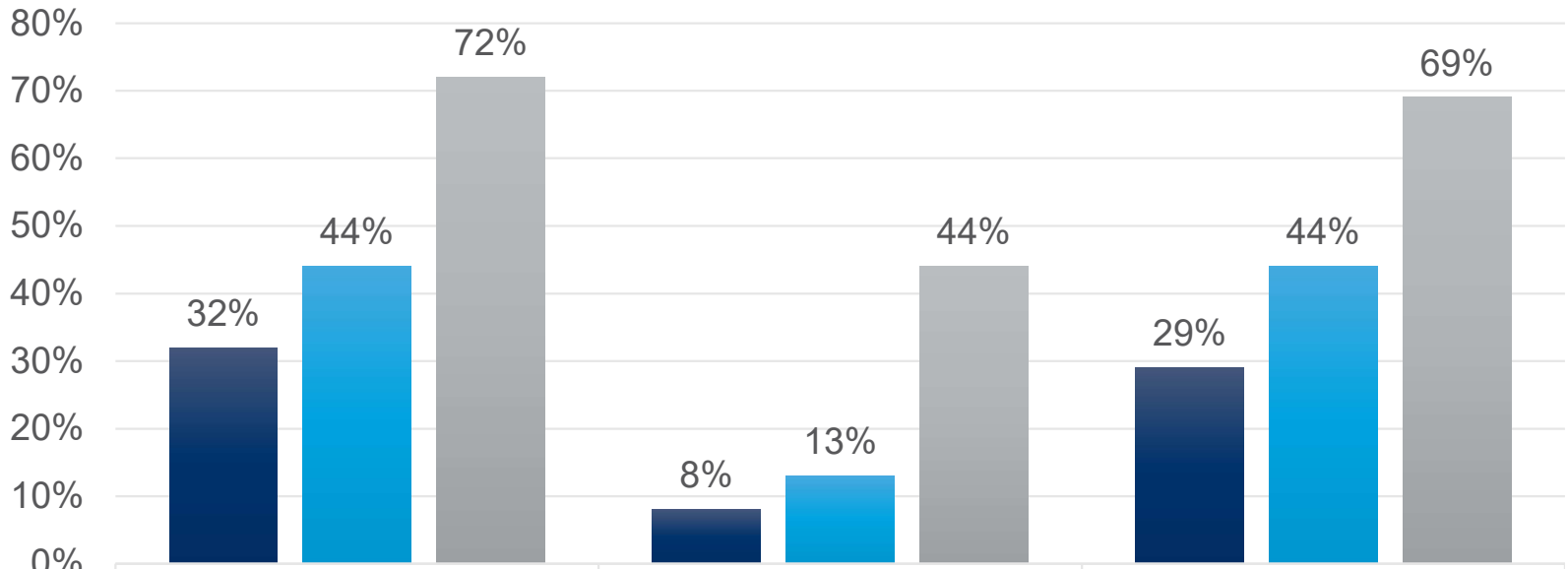
Personen, die gemeinsam eine IT nutzen:

- Einzelunternehmer / Einzelunternehmerin
- 2 Personen
- Mehr als 2 Personen

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

Ziel IT-Notfallplan:

IT-Notfallplan

Nachteile IT-Notfallplan:

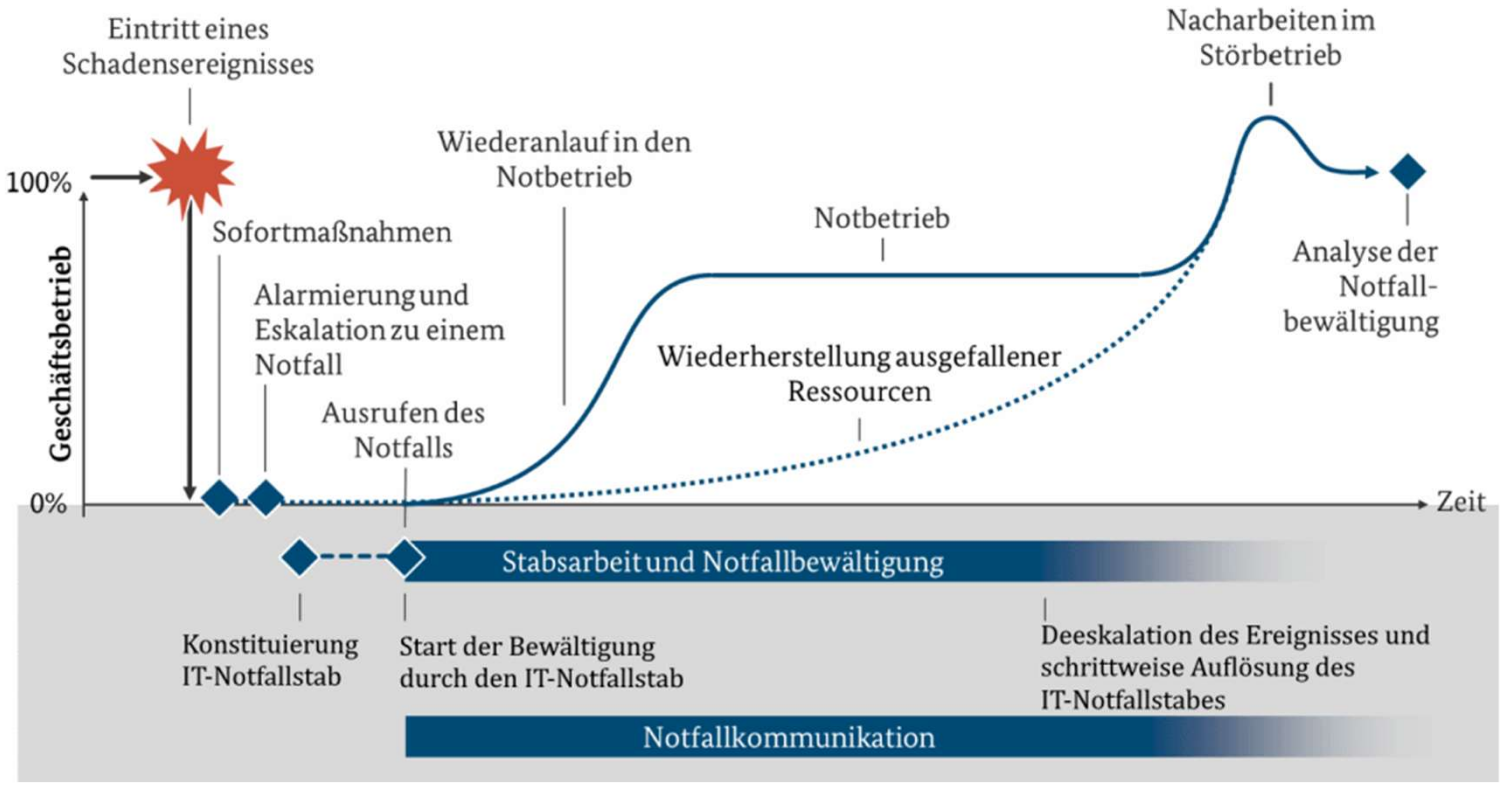
Kostet Geld, Zeit, Nerven…: Erstellung und Aktualisierung

Verbesserung IT & Prozesse

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

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

Kümmerer? Was ist wichtig?

Bitte notieren Sie auf Ihrem Block:

1. **Wer kümmert sich in Ihrem Unternehmen wie intensiv um IT-Sicherheit?**
   →Sie? Dienstleister (Website, Cloud…)? Mit welchem Aufwand?
2. **Was ist Ihr wichtigster IT-gestützter Prozess im Unternehmen? (wichtig = z. B. wenn nicht verfügbar, hoher Schaden)**
   → Kundenmanagement (CRM), Finanz- und Buchhaltungsprozesse (Rechnungen…), Logistik und Warenwirtschaftssysteme (ERP), Onlineshop, Website, E-Mail…
   → 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 am Samstagabend aus?
   Montagmorgen: Wichtigster Prozess seit Freitagnacht am Boden?

   Meldewege? Monitoring?
   Bieten Sie ein BugBounty-Programm?
   Beobachten Sie / IT-Sicherheitskümmerer
   Presse, Schwachstellen ihrer Software, Darknet etc.?

IT-Notfallteam? Wer kann noch helfen?

Bitte notieren Sie auf Ihrem Block:

4. **IT-Notfallteam: Welche Personen sind involviert wenn wichtigster Prozess von IT-Notfall betroffen?**
   → IT-Experten? Dienstleister? Kunden? Lieferanten? Sie? …
   → Entscheidungsebene: Sie?

5. **Welche externen Hilfeeinrichtungen 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, Dienstleister, Presse…
   Wie, wenn Mail und Festnetz weg? Handy, Notfallwebsite, Social Media, Messenger…

Bitte notieren Sie auf Ihrem Block:

8. **Notbetrieb:**
   Wie könnte das für den wichtigsten Prozess aussehen?
   → Inbetriebnahme der vorhandenen Notfall-IT (zuletzt wann getestet?)?
   Umstellung der Prozesse (z. B. analog statt digital)?
   Warten auf die wiederhergestellte 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 der „alten 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: Sensibilisierung für IT-Risiken –
TIPP: Digitalführerschein https://difue.de

→ Am IT-Notfallplan weiterarbeiten

IHK-Website

www.ihk-muenchen.de/informationssicherheit/

22.05.2025: Passwörter - Sichere Erstellung und Verwaltung

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

IHK-NEWSLETTER BLEIBEN SIE INFORMIERT!