10 Schlüsselerkenntnisse der IHK aus dem IT-Sicherheitsvorfall

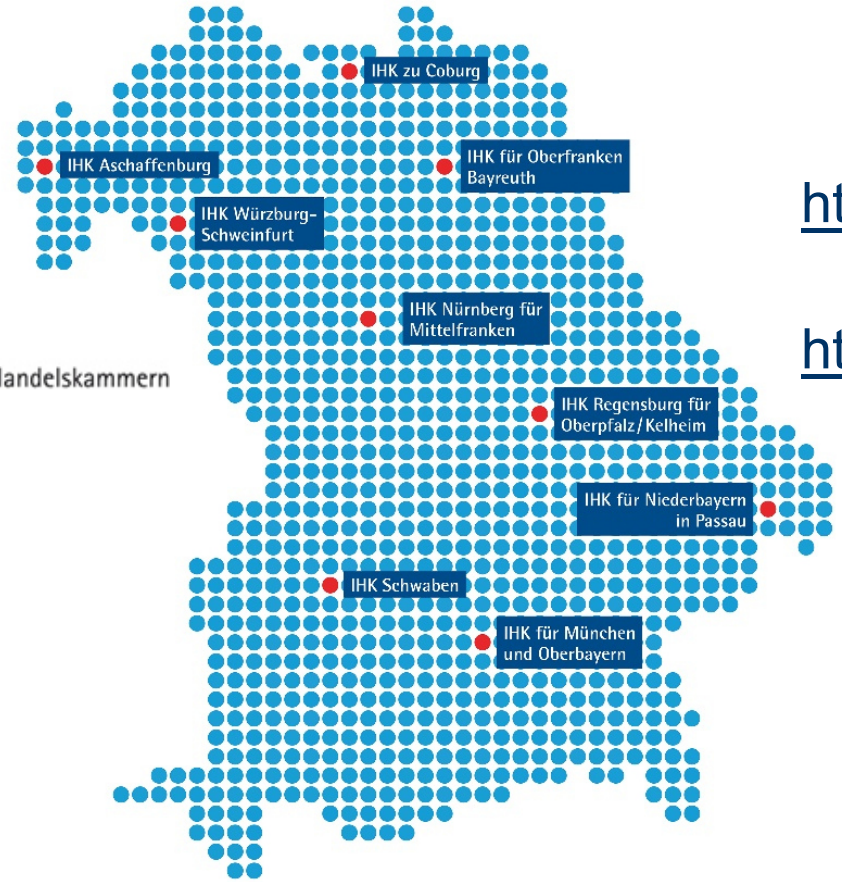
Webinarreihe IT-Sicherheit – praktisch gemacht

IHK

Digitalisierungsinitiative ihrer bayerischen IHKs

IHK

IHK Industrie- und Handelskammern in Bayern



https://www.bihk.de/itsicherheit

https://www.bihk.de/google-webinare

Webinarreihe IT-Sicherheit, 3te Staffel

20.09.23	Aus der Praxis lernen: 10 Schlüsselerkenntnisse der IHK aus dem **IT-Sicherheitsvorfall** 2022
27.09.23	Optimale Sicherheit für **Cloud- und Onlineanwendungen**: Überprüfung von IT-Sicherheitsstandards
04.10.23	Mit **Penetrationstests** auf der sicheren Seite. Was Sie von Penetrationstest erwarten dürfen und dabei beachten müssen.
11.10.23	**IT-Notfallplanung**: Bereit sein, wenn die Krise eintritt
18.10.23	Mobiles Arbeiten und Zero Trust – Spagat zwischen **Sicherheit und Benutzerfreundlichkeit**
25.10.23	Wie ticken gute Hacker? Wie kann man sie belohnen? Tipps für ein eigenes **BugBounty-Programm**
02.11.23	Das **Cyber-Sicherheitsnetzwerk** - Unterstützung nach IT-Sicherheitsvorfällen
15.11.23	**KRITIS** - Nachweis über angemessene IT Sicherheit
29.11.23	Ernstfall Cyberangriff – Richtig reagieren im **Notfall**

https://www.bihk.de/itsicherheit

Digitalimpulse im Rahmen des bayerischen Pakts für berufliche Weiterbildung 4.0

Kooperation von:

IHK Industrie- und Handelskammern in Bayern

Bayerisches Staatsministerium für Digitales

https://www.kommweiter.bayern.de/mit-unterstuetzung/pakt-fuer-berufliche-weiterbildung/

und

https://www.bihk.de/itsicherheit

Unterstützer

#GemeinsamDigital

DIHK Deutsche Industrie- und Handelskammer

CYBERsicher Transferstelle. Cybersicherheit. Mittelstand.

Sicherheitsnetzwerk München

ITSECURITY www.it-sicherheitscluster.de

ROSIK e.V.

Allianz für Cyber-Sicherheit Multiplikator

bayern innovativ Digitalisierung

Hatten Sie bereits einen IT-Sicherheitsvorfall?

- Nein - Gott sei Dank bisher nicht!
- Ja - Allerdings nur mit geringen Auswirkungen
- Ja - Mit schweren Auswirkungen
- Ich bin mir unsicher / Ich weiß es nicht genau
- Ich möchte lieber nicht antworten

IHK für München und Oberbayern – kein Kleinunternehmen

- Eingebettet in bundesweite IHK-Organisation
- Rund 500 Mitarbeiter
- 9 Standorte plus Homeoffices
- Vielzahl von Aufgaben und dafür eingesetzte Standard- wie Spezial-IT:
  - Interessenvertretung
  - Service
  - Hoheitliche Aufgaben:
    - Wirtschaftshilfen
    - Ausbildung
    - Außenwirtschaftsdokumente
    - Erlaubnisverfahren
    - Prüfungen
    - Sachverständige

IHK und IT-Sicherheit

- Sicherheit der Daten und Prozesse hat in der IHK dabei höchste Priorität
- **Ukraine-Krieg im Februar 2022**
- Bernhard Kux, meine Rolle: **IT-Sicherheitsbeauftragter**

Zentraler IT-Servicedienstleister der IHK-Organisation

- Internetzugang
- Mail
- Telefonie, Fax
- Internetanwendungen
- Zentrale Datenbanken & digitale Workflows fast aller IHKs

- IHK Cyber Emergency Response Teams (IHK-CERT)

IT-Notfall tritt ein

03.08.2022

- Auffälliges Verhalten in Systemen beim Dienstleister
- Zusammen mit externen IT-Sicherheitsexperten:
  Dienstleister entschied, die Verbindung aller Industrie- und Handelskammern zum Internet zu trennen
- Im Rückblick:
  IT-Forensiker, Bundesamt für Sicherheit in der Informationstechnik:
  Extrem professionelle Hacker am Werk

Neue Situation für die IHK für München und Oberbayern

- Reguläre Standardarbeitsplätze und Anwendungen vom Internet abgeschnitten:
  Kein Internet, kein E-Mail, kein Telefon, kein Homeoffice, (Teil-)Ausfall von Anwendungen…

- Was noch funktionierte:
  Eigenes WLAN, interne IT, spezielle Internetzugänge für Gebäude u. ä., Mobilfunk, eigene Cloudanwendungen wie die IHK-Website ihk-muenchen.de

- Rückgriff auf den bestehenden IT-Notfallplan

Haben Sie einen Notfallplan, den Sie aus der Schublade ziehen können?

- Nein, da sind wir aktuell ziemlich blank
- Ja, aber vermutlich nicht aktuell oder vollständig
- Ja, ein aktueller und erprobter Notfallplan liegt bereit

Zentraler IT-Notfallplan: 29 seitiges Worddokument

- Anhang: Notfallszenarien, insbes. zu „Kronjuwelen“ und Ransomware
- Anwender-Notfallpläne: Handlungsoptionen für Anwender
- Technische Dokumentationen: Informationen für IT-Experten
- Ergänzende Dokumente: Telefonlisten, Domainliste, Unterlagen Versicherungen, Vorlagen (z. B. für Pressemeldungen, Datenschutz-Meldepflichten) etc.

Wichtig: Alle Dokumente müssen **ausdruckbar** sein → Hinterlegung im Safe auf Papier

11.10.23, 11:00 - 12:00 Uhr: IT-Notfallplanung: Bereit sein, wenn die Krise eintritt

Grundsätzlicher Aufbau

a. Meldewege: Wie erfahre ich von Problemen?

b. Verifikation und Analyse der Meldung

c. Sofortmaßnahmen: Was muss schnell entschieden und erledigt werden?

d. Ausrufen des IT-Notfalls, IT-Notfallstab, Kommunikation

e. Notfallbetrieb und Wiederanlauf

IHK IT-Notfallplan: Meldewege, Verifikation und erste Analyse der Meldung

Fehlalarm / Betriebsstörung / Schwere Betriebsstörung / IT-Notfall / schwerer IT-Notfall?

Kriterien für die Einstufung:

- Reichen die vorhandenen Ressourcen?
- Welche Schäden für die IHK sind vorstellbar?
- Welche Reaktionsgeschwindigkeit ist nötig?
- Welche Ressourcen werden benötigt?

Hier: Telefonische Anrufe des Dienstleisters
→ Telefonische Meldekette innerhalb der IHK

Sehr klar, dass es sich um einen IT-Notfall beim Dienstleister handelt,
→ Umfang & Folgen waren allerdings noch offen

10 Erfahrungen

1. Dienstleister!?
2. Rolle des IT-Notfallplans
3. Eigenes IT-Team
4. Technische Prophylaxe: Logfiles, Onlinechecks
5. Sprachregelung festlegen!
6. Wie kommunizieren Sie, wenn Telefon & Internet weg?
7. Externe Experten!?
8. IT-Sicht - Fokus auf technische Fragestellungen: Rot & Grün
9. Anwendersicht - Fokus auf Handlungsfähigkeit: Anwender IT-Notfallplan
10. IT und Anwender zusammenbringen

Erfahrung 1: Dienstleister!?

- **Dienstleister weg?**
  → **Überlegen Sie sich, was Sie tun, wenn Ihr wichtigster (IT-)Dienstleister ausfällt?**
  Es ist dabei egal warum und wieso.

- **Dienstleister-Landschaft?**
  → **Schauen Sie sich Ihre Dienstleister-Landschaft an!**

Zu wenige Dienstleister:	Klumpenrisiko
Zu viele Dienstleister:	Management- / Komplexitätsrisiko

Wenn Ihr wichtigster Dienstleister ausfällt: Was tun Sie?

- Wir haben alternative Dienstleister schnell einsatzfähig
- Wir nutzen andere, z. B. analoge, Prozesse
- Wir beten, dass der Dienstleister bald wieder funktioniert
- Wir suchen uns schnell einen anderen Dienstleister

Zentraler IT-Notfallplan „IT-Sofortmaßnahmen“

→ Was muss sofort und schnell getan werden?

Erfahrung 2: Rolle des IT-Notfallplans

IT-Notfallplan hilft, Handlungsmöglichkeiten aufzuzeigen

→ Strukturierte Liste mit möglichen Maßnahmen

→ Entscheidung was konkret gemacht wird: Sehr einzelfallabhängig!

IHK IT-Notfallplan: Ausrufen des IT-Notfalls, IT-Notfallstab, Kommunikation

IT-Notfallplan gibt Handlungsoptionen:
Unterstützung bei Organisation und Entscheidungsfindung

- Zusammenstellen und Zusammenkommen des IT-Notfallstabes

- Aufgaben & Arbeitsweise IT-Notfallstab:
  - Kommunikationswege intern und extern?
  - Interne Folgenabschätzung
  - Meldepflichten prüfen
  - Hinzuziehen Strafverfolgungsbehörden, externe Experten?
  - ….

Sie brauchen ein internes, motiviertes und verfügbares IT- und Kommunikations-Team (oder gute Dienstleister)!

→ Beispiel:
Würde ihr interner Netzwerk-Experte in der Nacht kurzfristig zum Rechenzentrum fahren und dort Verbindungen unterbrechen können?

Kleines Unternehmen?

Ggf. müssen Sie persönlich wissen, was wo wie wann getan werden muss!

Aufbewahrungsdauer Logfiles 1 Jahr – Datenschutz vs. IT-Sicherheit?

→ Nachvollziehen eines Angriff nur mit passenden Logfiles möglich

→ Was protokollieren und wie lange wo aufbewahren (z. B. Rechtemanagement)?

→ Datenschutz: Zweckbindung entscheidend

Sprachregelung festlegen!

- Anfragen von Presse, Kunden, Mitarbeitern kommen
- Notfallplan: Vorbereitete Textmuster, die man anpassen kann
- Interne Kommunikation:
  Z. B. Bitte, keine Informationen zum Sicherheitsvorfall via SocialMedia veröffentlichen
- Bundesweite Sprachregelung nötig! → Grundsätzlicher Verweis an den Dienstleister

Wie kommunizieren Sie, wenn Telefon & Internet weg?

- SMS an die Diensthandys, ausgedruckte Telefonliste, Rückgriff auf noch verfügbare interne und externe Websites im Eigenbetrieb
- Interne und externe Notfall-Infowebsite
- Fachbereiche: Messenger-Gruppen
- Launch von Microsoft Teams
- Notfall-E-Mailadressen

Externe Experten finden und hinzuziehen!?

- Nötig?
- Wie finden: Eigene Kontakte? Cyberversicherung? BSI-Liste von zertifizierten APT Response-Dienstleistern

- Verfügbarkeit? Kosten? Vertrag?
- Experten sollten vor Ort sein: Ggf. Anreise einplanen…
- Eigene IT, Dienstleister und externe Experten zusammenbringen
- Externen Experten Arbeitsmöglichkeiten und IT-Zugang verschaffen

- **Einschätzung der externen Experten:**
  Wie ist eigene Situation und die des betroffenen Dienstleisters einzuschätzen?
  IT-technische Verbesserungsmöglichkeiten z. B. im eigenen Netz?

Haben Sie einen IT-Dienstleister für IT-Notfälle zur Hand?

- Nein, brauchen wir nicht: Wir machen Alles selbst.
- Nein, wäre aber gut wenn wir einen hätten
- Ja, die aber nicht auf IT-Sicherheit spezialisiert sind
- Ja, die auch auf IT-Notfälle spezialisiert sind

Vielzahl von Aufgaben und dafür eingesetzte Standard- wie Spezial-IT

- **Zwei Blickwinkel:**
  - IT-Sicht: Fokus auf technische Fragestellungen
  - Anwendersicht: Fokus auf Handlungsfähigkeit

Grün & Rot – Backups

- Aufteilung in grüne (sichere) und rote (unsichere) IT-Zonen, die mit Datenschleusen verbunden sind.
  Start: Alles rot → Ziel: Nur noch grüne IT-Zonen

  „Grün werden“:
  Scan der eigenen IT: “Indicators of Compromise”

→ Fragestellung: Welche Prioritäten setzt der ausgefallene Dienstleister?

(Lokale) Backups?

- Backups: Hauptziel von Angreifern → Backups isolieren und langfristig aufbewahren: Wissen Sie wie lange ein Angreifer bereits „drin“ ist?
- Backups testen!
- Auf Backup beim Dienstleister vertrauen!?

Praxis:

- Sie kommen nicht an das Backup beim Dienstleister ran.
  Oder wissen nicht, ob das Backup auch korrumpiert ist…
- Backup = **Daten** plus evtl. Anwendungssoftware plus evtl. Nutzer-Berechtigungen
  - Was wenn System für Nutzer-Berechtigungen nicht mehr verfügbar → Alternative?
  - Reichen die Daten alleine für eine Handlungsfähigkeit / Wiederaufbau
    → Lokale Daten-Backups?

Erfahrung 9: Anwendersicht - Fokus auf Handlungsfähigkeit

Anwender-Notfallpläne

- IT-Ausfall! Was tun?
- Analoge Prozesse überlegen oder reaktiveren, digitale Notlösungen schaffen?
- Stark abhängig vom jeweiligen Prozess:

Zusammenstellen von IT-Notfallplänen mit und für Anwender

Erfahrung 9: Anwendersicht - Fokus auf Handlungsfähigkeit

Beispielanwendung: Elektr. Ursprungszeugnis https://euz.ihk.de

Behörden vieler Staaten: Waren, die in ihr Hoheitsgebiet eingeführt werden sollen, von Ursprungszeugnissen oder bescheinigten Handelsrechnungen begleitet sind. Die IHK stellt die notwendigen Dokumente aus.

Deutschlandweit:

- 2020: 0,92 Mio digital 0,55 Mio manuell
- 2021: 1,10 Mio digital 0,34 Mio manuell
- 2022: 0,85 Mio digital 0,35 Mio manuell
  Siebenwöchiger Ausfall: 03.08.22 bis 26.09.22

Erfahrung 9: Anwendersicht - Fokus auf Handlungsfähigkeit

Beispielanwendung: Elektr. Ursprungszeugnis

- **Welche Probleme sind denkbar? Welche IT ist hier im Einsatz?**
  - Öffentliche Website intern oder extern nicht verfügbar?
  - Backend zur Website intern oder extern erreichbar?
  - Signatur- und Druckinfrastruktur verfügbar?
  - Archivsystem verfügbar?

- **Schadensabschätzung**:
  Welche Folgen haben die Probleme - rechtlich, intern und extern?

Erfahrung 9: Anwendersicht - Fokus auf Handlungsfähigkeit

Beispielanwendung: Elektr. Ursprungszeugnis

- **Welchen Plan A, B oder C gibt es?**
  - Andere Zugriffswege (z. B. Mobilfunk, WLAN)
  - Andere Prozesswege: Formulare aus dem Formularfachhandel persönlich / postalisch bei der IHK einzureichen
  - Zu archivierende Unterlagen vorhalten und einspeisen sobald IT wieder funktioniert
  - Erreichbarkeit für Kunden: z. B. IHK-Website mit Hinweisen zum Not-Prozess

- **Denkbare Maßnahmen zur besseren Vorbereitung auf einen IT-Notfall?**
  - (Teil-)Prozesse alternativ durchführbar, z. B. per WLAN und Laptops
  - Grundsatzfragen: Alternative Internetanbindung, Telefonie-Infrastruktur

Erfahrung 9: Anwendersicht - Fokus auf Handlungsfähigkeit

Beispielanwendung: Elektr. Ursprungszeugnis

- Ausfallkonzept: Manuelle Ausstellung und Bescheinigung von UZs
- Formularverlage: Nachdruck der Formularsätze
- IHKs: Sehr pragmatische Lösungen, persönlicher Kontakt zu den Kunden
- Bundesweit: 120.000 UZs manuell statt elektronisch ausgestellt

IT-Sicht und Anwendersicht-Sicht

Anwender IT-Notfallpläne
→ Liste von möglichen Verbesserungen:
Was ist kurz-, mittel-, langfristig machbar?

- Frontend IT-Technisch:
  Zusätzliche IT-Notfallsysteme, Beispiel: Notfall-Formulare, Notfall-Website…

- Backend IT-Technisch:
  Netzwerk-Separierung, bessere Sicherheitsmechanismen (z. B. Zwei-Faktor-Authentifizierung), umfangreicheres & längerfristige Logging, besseres Monitoring, lokale Backups…

Dankeschön für Ihre Aufmerksamkeit!

Ihre Fragen und Anmerkungen?