IHK: Überprüfung von IT-Sicherheitsstandards

Aus der Praxis lernen

IHK

Ausgangslage der IHK für München und Oberbayern

- Viele unterschiedliche IHK-Aufgaben
- IHK: Anwender vielfältiger Software
- Viele Cloudanwendungen: z. T. selbst betrieben, z. T. bei Dienstleistern

- Suche nach der passenden Onlinesoftware:
  https://www.ihk-muenchen.de/de/Service/Digitalisierung/Wie-findet-man-geeignete-Software/
- Auswahlkriterien:
  - Was habe ich?
  - Was brauche ich?
  - Was gibt es auf dem Markt?
  - ….
  - Wie sicher ist die Onlinesoftware?
  - Vergabe oder nicht?

Ausgangslage der IHK für München und Oberbayern

- KO-Kriterium IT-Sicherheit: Sind Mindestanforderungen erfüllt?
- Meine Rolle: **IT-Sicherheitsbeauftragter**
- Beurteilung:
  - **Selbstauskunft der Anbieter:**
    Technische Beschreibungen
    Datenschutz: Technisch-organisatorische Maßnahmen
    Zertifizierungen
    …
  - **Überprüfbares:**
    Demo- / Testversionen der Onlinesoftware
    Erfahrungsberichte anderer Anwender
    Anbieterwebsite
    …

Vergabe und IT-Sicherheit?

- **Vergabe:**
  Formaler Vorgang, genau definiert
  → Punktesystem, erforderliche Pflichtanforderungen
  → Anbieter muss Mindestsicherheitsstandard erreichen, sonst keine Berücksichtigung bei der Vergabe.
  → Wenn Mindestsicherheitsstandard erreicht ist bzgl. Vergabe: IT-Sicherheit kein weiteres Thema

- **Keine Vergabe:**
  → Angemessene IT-Sicherheit nötig, ggf. Entscheidung der Geschäftsführung

Entstehungsgeschichte

- Zielfrage: „Erfüllt Ist die Onlineanwendung die für uns angemessene IT-Sicherheit?“

- Datenschutzrechtliche Verfahrensbeschreibung:
  Technisch-organisatorische Maßnahmen („TOMs“) der Anbieter
  → Viele, auch IT-Sicherheitstechnische Informationen
  → Aber: Es bleiben oft Fragen zur IT-Sicherheit offen

- Bedürfnis: Strukturierte, handhabbare Herangehensweise

IHK für München und Oberbayern: Musterdokument zur Selbstauskunft

- **Erste Versuche: „BSI Kriterienkatalog Cloud Computing C5“**
  → für Anbieter zu umfangreich

- **Handhabbares Musterdokument:**
  - Datenschutz: TOMs
  - Konzepte: DIN SPEC 27076, BSI C5, BSI 200…

→ IHK-Website „Muster: Onlineanwendung & IT-Sicherheit“
https://www.ihk-muenchen.de/de/Service/Digitalisierung/Informationssicherheit/Muster-Onlineanwendung-IT-Sicherheit/

IHK für München und Oberbayern: Musterdokument zur Selbstauskunft

- **Musterdokument:**
  → 5 Themenbereiche
  → Viele Selbstverständlichkeiten

1. Organisatorische Maßnahmen
2. Vertraulichkeit
3. Integrität
4. Verfügbarkeit
5. Belastbarkeit

Musterdokument: Organisatorische Maßnahmen

- Wie organisiert der Anbieter der Onlinesoftware IT-Sicherheit?

1. Informationssicherheits-Managementsystem vorhanden?
2. IT-Sicherheitsbeauftragte / Kümmerer vorhanden?
3. Alle Mitarbeiter auf die Vertraulichkeit (Datengeheimnis) verpflichtet?
4. Kennen die Mitarbeiter die Regel zur IT-Sicherheit und werden sie geschult?
5. Risikoabschätzungen bzgl. der Abhängigkeit von Subdienstleistern

Musterdokument: Vertraulichkeit

- Ist die Onlineanwendung in guten Händen?

1. Professionelles Rechenzentrum? Z. B. Zutrittskontrolle geregelt?
2. Zugangskontrolle zur Onlineanwendung: Passwörter, Zwei-Faktor-Authentifizierung, Logging der Login-Aktivitäten…
3. Zugriffskontrolle auf die IT im Büro des Anbieters: Berechtigungssystem für Mitarbeiter?
4. Anzahl und Rechte der Administratoren auf das "Notwendigste" reduziert.
5. Trennungskontrolle: Wie trennt die Onlineanwendung Daten (andere Anwendungen, andere Zwecke)?
6. Verschlüsselung: https/TLS… , Technischer Zugriff per SSH / sFTP…

Musterdokument: Integrität

- Passen die Daten und Prozesse?

1. Weitergabekontrolle: Absicherung des Anbieter-Netzwerkes (z. B. durch Firewalls, Netzwerkseparation) nach dem Stand der Technik, wobei die Komponenten regelmäßig aktualisiert werden.
2. Eingabekontrolle/Verarbeitungskontrolle:

   Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten

   Logging mind. 6 Monate / mind. 3 Monate / weniger als 3 Monate
3. Dokumentationskontrolle: Verzeichnisses von Verarbeitungstätigkeiten? Dokumentation der eingesetzten IT?
4. Auftragskontrolle: Vertrag zur Auftragsdatenverarbeitung! Kontrolle der Vertragsausführung? Beendigung des Auftrags: Daten datenschutzkonform löschen!

Musterdokument: Verfügbarkeit 1/2

- Ist alles nötigte da, sicher & getestet?

1. Rechenzentrum: Redundanz? Ausfallsicherheit: Max. 30 Min/Jahr bis über 1 Tag/Jahr

2. Sicherheit der Onlineanwendung: Technologien nach dem Stand der Technik (Software Bill of Materials?)

3. Updates, Backups der Onlineanwendung?

4. Prozess Softwareentwicklung? Software von unabhängigen Experten geprüft?

Musterdokument: Verfügbarkeit 2/2

- Ist alles nötigte da, sicher & getestet?

5. Know How des Anbieters: Kenntnisse und Handlungseinschätzungen bzgl. des Standes aktueller Schwachstellen und Gefährdungen?

6. Wie schnell Benachrichtigung über Probleme? Gibt es einen IT-notfallplan beim Anbieter?

7. Handbuch: Infos zur Notfallbehandlung?

8. Maßnahmen im Büro des Anbieters: Backups, Updates, Sicherheitssoftware…

Musterdokument: Belastbarkeit

- Sturmfestigkeit?

1. Redundante Systemauslegung

2. Ausfallsicherheitskonzept

3. Schutz vor Überlast und Denial of Service-Angriffen

Webinarreihe IT-Sicherheit, 3te Staffel

https://www.bihk.de/itsicherheit

→ PDF zum Vortrag | youtube: IHK für München und Oberbayern

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.

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**

Dankeschön für Ihre Aufmerksamkeit!

Ihre Fragen und Anmerkungen?