LS – Die Häcker AG

Ihr Unternehmen, die Häcker AG, bietet Dienstleistungen im Bereich Sicherheit von IT-Infrastruktur an und führt Zertifizierungen nach ISO 27001 durch. Kürzlich jedoch wurde Ihr Unternehmen selbst Opfer eines gezielten Hackerangriffs. Die Angreifer nutzten eine Schwachstelle in der Netzwerkstruktur aus, wodurch sensible Kundendaten und interne Geschäftsgeheimnisse „geleakt“ wurden.

Der Vorfall führte zu einer temporären Beeinträchtigung der Verfügbarkeit zentraler Systeme, was Verzögerungen in Projekten und einen Reputationsschaden bei Kunden verursachte. Das Management hat daraufhin beschlossen, die IT-Sicherheit grundlegend zu verbessern und Sicherheitsmaßnahmen zu verstärken.

Sie als angehende Fachinformatiker wurden beauftragt, eine **Schutzbedarfsanalyse** für Ihren Arbeitsbereich durchzuführen. Ziel ist es, Schwachstellen und Risiken aufzudecken, den Schutzbedarf für Systeme und Daten zu bewerten und konkrete Maßnahmen zu entwickeln, um zukünftige Angriffe und Ausfälle zu verhindern.

Im Dokument *DieHäckerAG.pdf* finden Sie Informationen zu Ihrem Arbeitsbereich incl. Netzplan und IT-Infrastruktur.

Aufgabenstellung

Im Folgenden sollen Sie Ihren Arbeitsbereich in der Häcker AB genauer untersuchen.

1. **Analysieren** Sie die Systeme und Daten in Ihrem Arbeitsbereich auf mögliche Schwachstellen, die Angreifer ausnutzen könnten.

   1.1 Welche Systeme, Anwendungen und Daten sind Bestandteil Ihres Arbeitsbereichs? Erstellen Sie eine Auflistung mit den folgenden Gruppen:
   - Server-Hardware
   - Netzwerk und dessen Komponenten (Switch, Router,...)
   - Arbeitsgeräte (PC, Laptops, ...)
   - Anwendungen und Dienste (z. B. ERP-Systeme, spezielle Software)
   - Daten (z. B. Kundendaten, Entwicklungsdaten, Zugangsdaten)

   1.2 Gibt es Schnittstellen zu anderen Systemen oder externen Partnern? Listen Sie auf.
   1.3 Besteht eine Dokumentation?

2. **Bewerten** Sie den Schutzbedarf anhand der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit (CIA). Für die Bewertung müssen Sie zunächst festlegen, was man in Ihrem Fall als „Leichte Störung“, Erheblicher Schaden“ und „Existenzbedrohender Schaden“ versteht. Man unterscheiden nur diese drei Kategorien. Legen Sie diese für Ihren Arbeitsbereich fest.

   2.1 *Vertraulichkeit*
   Welche Informationen dürfen nur bestimmten Personen zugänglich sein? Erstellen Sie ebenfalls eine Liste.
   Welche Folgen hätte ein unbefugter Zugriff? Ordnen Sie die gefundenen Informationen den Folgen zu:
   - Leichte Störung

- Erheblicher Schaden, wie z. B. Reputationsverlust
- Existenzbedrohender Schaden

2.2 *Integrität*

Welche Daten oder Systeme müssen frei von Manipulationen sein? Listen Sie auf. (z. B. Konfigurationsdateien von Systemen, Software-Quellcode, usw.)
Welche Folgen hätte ein unbefugter Zugriff? Ordnen Sie die gefundenen Informationen den Folgen zu:

- Leichte Störung
- Erheblicher Schaden, wie z. B. Reputationsverlust
- Existenzbedrohender Schaden

2.3 Verfügbarkeit

Welche Systeme und Daten müssen immer verfügbar sein. Nennen Sie die Systeme, wie z. B. IT-Infrastruktur, Produktions- und Kundensysteme, Email- und Kommunikations-Systeme. Erstellen Sie ebenfalls eine Matrix mit den drei Folgen-Kategorien.

3. Bedrohungen und Schwachstellen auflisten

3.1 Bedrohungen. Nennen Sie Bedrohungen, die durch

- menschliches Fehlverhalten
- technisches Versagen
- höhere Gewalt (Brand, Feuer,...)
- Cyberangriffe (z. B. Phishing, Malware, Ransomware, Rootkit,...)

entstehen können.

3.2 Wo liegen Schwachstellen in Ihrem Arbeitsbereich? Nennen Sie welche aus den Bereichen:

- Software
- Zugriffsrechten
- Backups
- Physische Sicherheit. (z. B. Zugang zu Räumen)

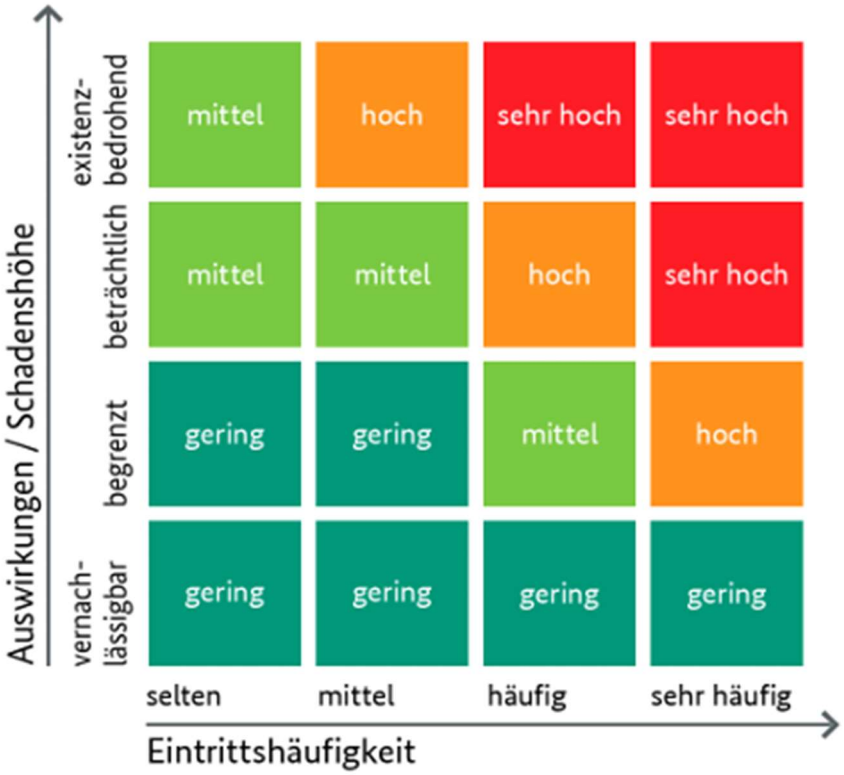
4. Bewertung des Schutzbedarfs

Ergänzen Sie die unten stehende Tabelle, in der alle Systeme und Daten (sog. Schutzobjekte) aufgelistet werden, die Sie gefunden haben. Ordnen Sie diesen in den Kategorien „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“ jeweils einen Schutzbedarfs-Level zu.

Schutzobjekt	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Schutzbedarf insgesamt**
Kundendatenbank	Hoch	Hoch	Mittel	Hoch
E-Mail-System	...			
Entwickler-PCs				
...				

5. **Maßnahmen** ergreifen zur Risikominderung
   Überlegen Sie sich zunächst welche
   - Technischen
   - Organisatorischen und
   - Physischen

   Maßnahmen Sie treffen können, um die Schutzobjekte schützen zu können.



Listen Sie mindestens fünf Gefährdungen auf und lokalisieren Sie diese in der oben dargestellten Risikomatrix. Die Gefährdungen, die im Bereich „sehr hoch“ liegen müssen mit hoher Priorität angegangen werden, was die Maßnahmen betrifft.
Siehe hierzu auch die Liste „Elementare Gefährdungen“ vom BSI. (Infopool)