Projektarbeit IHK Cyber Security Advisor

Analyse der Sicherheitsanforderungen und Konzeption einer Sicherheitsrichtlinie für die Nutzung mobiler Geräte basierend auf ISO 27001 und BSI IT-Grundschutz

zur Erlangung der Zertifizierung
IHK Cyber Security Advisor

Vorgelegt von: Peter Peters

Eingereicht am: 16.07.2025

Kurs: WB CS_09

Inhaltsverzeichnis

1. RecodeHealth AG

1.1. Vorstellung des Unternehmens

Die RecodeHealth AG ist ein deutsches Unternehmen im Bereich Gesundheitstechnologie mit 100 Mitarbeitern, das sich auf Software als Medizinprodukt (SaMD) spezialisiert hat. Dieses Geschäft erfordert den sorgfältigen Schutz sensibler Patientendaten (PHI) und proprietärer Forschungs- und Entwicklungsdaten (F&E).

Dieses Projekt wurde nach einem Beinahe-Sicherheitsvorfall initiiert, bei dem ein Firmen-Tablet mit sensiblen Produktspezifikationen verloren ging. Eine Untersuchung ergab kritische Kontrolllücken, wie z. B. fehlende Verschlüsselung oder Fernlöschfunktionen. Dies deckte eine systemische Schwachstelle auf: Die weit verbreitete, unkontrollierte Nutzung mobiler Geräte durch Mitarbeiter stellt ein inakzeptables Risiko für Unternehmensdaten dar, insbesondere angesichts der Einschätzung des BSI, dass die Bedrohungslage „angespannt bis kritisch" ist.

Daher hat die Unternehmensleitung dieses Projekt in Auftrag gegeben, um die Risiken systematisch zu analysieren und ein robustes Sicherheitskonzept für alle mobilen Geräte zu entwickeln. Das Projekt folgt der bewährten ISMS-Methodik der ISO 27001 und des BSI IT-Grundschutzes und umfasst eine Schutzanforderungsanalyse, einen Soll-Ist-Vergleich und eine Risikoanalyse, die mit einer formellen Empfehlung zur Einrichtung einer sicheren und konformen mobilen Arbeitsumgebung abschließt.

1.2. IT-Infrastruktur

Mobile Endgeräte (E001): Dies ist die wichtigste Anlageklasse und Gegenstand unserer Analyse. Dazu gehören:

- Vom Unternehmen ausgegebene Smartphones (iPhones, Android-Geräte)
- Vom Unternehmen ausgegebene Tablets (iPads, Android-Tablets)
- Die Nutzung privater Geräte von Mitarbeitern (BYOD) für den Zugriff auf Unternehmensressourcen.

Sensible Unternehmensdaten (D001): Hierbei handelt es sich um kritische Informationen, auf die über mobile Geräte zugegriffen wird, die dort verarbeitet und vorübergehend gespeichert werden. Der Schutz dieser Daten ist der Hauptgrund für dieses Projekt. Dazu gehören:

- Patientengesundheitsdaten (PHI)
- Quellcode und anderes geistiges Eigentum (IP)
- Interne E-Mails und Projektdokumente.

Cloud-Kollaborationsplattform (S001): Dies ist der zentrale Dienst, mit dem mobile Geräte verbunden sind. Die Sicherung des Geräts ist untrennbar mit der Sicherung seines Zugriffs auf diese Kerndienste verbunden. Für RecodeHealth AG sind dies in erster Linie:

- Microsoft 365 (für E-Mails, Kalender, SharePoint und Teams).

2. Schutzbedarfsstruktur

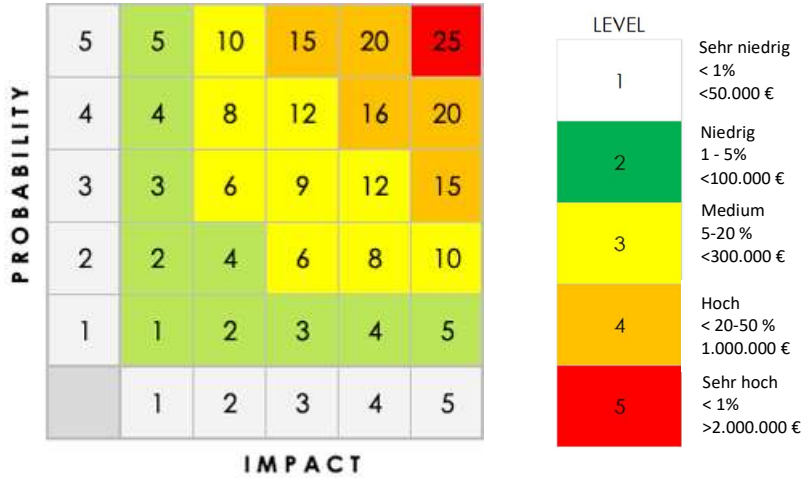
Bezeichnung und Beschreibung	Schutzziel	Schutzbedarf	Begründung
E001 Mobile Endgeräte (Smartphones & Tablets)	Vertraulichkeit	**Hoch**	Geräte greifen auf sensible Daten (E-Mails, PHI, IP) zu und speichern diese vorübergehend. Der Verlust von Geräten ist ein direkter Weg für Datenverletzungen.
	Integrität	**Hoch**	Die Integrität des Betriebssystems des Geräts ist entscheidend, um Datenmanipulationen oder die Nutzung als Ausgangspunkt für Netzwerkangriffe zu verhindern.
	Verfügbarkeit	**Hoch**	Schlüsselpersonen sind für die tägliche Kommunikation und Produktivität auf diese Geräte angewiesen.
D001 Sensible Unternehmensdaten (Patientendaten & Quellcode)	Vertraulichkeit	**Sehr hoch**	Die unbefugte Offenlegung verstößt gegen die DSGVO (für PHI) oder zerstört Wettbewerbsvorteile (für Quellcode).
	Integrität	**Sehr hoch**	Änderungen können zu Schäden für Patienten (PHI) führen oder kritische Schwachstellen in Produkten (Quellcode) verursachen.
	Verfügbarkeit	**Hoch**	Erforderlich für die fortlaufende Entwicklung, das Testen und den Vertrieb über mobile Geräte.
S001 Cloud-Kollaborationsplattform (Microsoft 365)	Vertraulichkeit	**Hoch**	Als zentraler Dienst, auf den mobile Geräte zugreifen, enthält er eine hohe Konzentration sensibler Projekt- und Geschäftsdaten.
	Integrität	**Hoch**	Die Integrität von E-Mails und Dokumenten, die mit mobilen Geräten synchronisiert werden, ist für alle Geschäftsprozesse von entscheidender Bedeutung.
	Verfügbarkeit	**Sehr hoch**	Ein Ausfall der primären Kommunikationsplattform würde alle mobilen und Remote-Arbeitsplätze lahmlegen.

3. SOLL-/IST-Abgleich

Hauptpflichten	SOLL	IST	Status	Verantwortlicher	Zeitraum
1.0 Zentrales Gerätemanagement (MDM)	4	1	**Nicht umgesetzt**: Es existiert keine zentrale Lösung zur Verwaltung mobiler Endgeräte. Die Administration erfolgt manuell durch die IT oder die Benutzer selbst. **Abweichung**: Die grundlegende Fähigkeit zur Durchsetzung von Sicherheitsrichtlinien fehlt vollständig.	IT-Leiter	In 1 Monat
2.0 Datentrennung (Container)	4	1	**Nicht umgesetzt**: Es existiert keine technische Trennung zwischen Unternehmens- und Privatdaten/-apps. **Abweichung**: Unternehmensdaten können frei in private Apps verschoben werden, was ein hohes Risiko für Datenlecks darstellt.	IT-Abteilung	In 3 Monate
3.0 App-Management	4	1	**Nicht umgesetzt**: Benutzer können jede Anwendung aus öffentlichen App-Stores installieren. Es gibt keinen Prüfprozess. **Abweichung**: Keine Kontrolle über potenziell bösartige oder datenleckende Software auf den Geräten	ISB IT-Abteilung	In 3 Monate
4.0 Incident Response (Remote Wipe)	4	1	**Nicht umgesetzt**: Es besteht keine Möglichkeit, Unternehmensdaten von einem verlorenen oder gestohlenen Gerät aus der Ferne zu sperren oder zu löschen. **Abweichung**: Ein kritischer Fehler im Incident-Response-Lebenszyklus, wie der auslösende Vorfall gezeigt hat.	IT Helpdesk ISB	Sofort bei MDM-Registrierung
5.0 Schulung der Mitarbeiter	4	4	**Umgesetzt:** Regelmäßige Schulungen. Keine Abweichungen	**IT-Leiter** **ISB**	**Regelmäßig (ein mal Pro Jahr)**

Legende Zahl SOLL/IST Stand:
4 = Alle Maßnahmen in diesem Bereich wurden umgesetzt. Es werden keine weiteren Schritt benötigt
3 = Es wurde nicht alle Maßnahmen umgesetzt, der Großteil ist jedoch bereits vorhanden.
2 = Es sind mehrere Mängel und nicht umgesetzte Mängel Vorhanden
1 = Es wurden keine Maßnahmen getroffen

4. Risikoanalyse



Risk ID	Beschreibung Schwachstellen	Beschreibung Auswirkungen	Maßnahme	Auswirkung SLE	Wahrscheinlichkeit ARO	Risiko ALE
R-001	Fehlenden Zentrales Gerätemanagement (MDM)	Datenverlust durch verlorenes/gestohlenes Gerät: Aufgrund des Fehlens eines zentralisierten MDM-Systems greift eine unbefugte Person auf sensible PHI- und F&E-Daten zu, die auf dem Gerät gespeichert sind.	3. SOLL-/IST Punkt 1.0, 4.0	5	4.5	**22.5**
R-002	Fehlende App Management	Datenverlust durch ungesicherte persönliche Apps.	3. SOLL-/IST Punkt 3.0	4	4	**16**
R-003	Fehlende Datentrennung	Netzwerkkompromittierung durch bösartige App: Die App enthält Spyware, die Daten exfiltriert oder den VPN-Zugang des Geräts nutzt, um das interne Unternehmensnetzwerk anzugreifen, was möglicherweise zu einer Ransomware-Infektion führt.	3. SOLL-/IST Punkt 2.0	4	4	**16**

5. Fazit

Die Analyse nach ISO 27001 und BSI IT-Grundschutz hat bestätigt, dass die RecodeHealth AG Informationswerte mit „sehr hohem“ Schutzbedarf wie Patientendaten (PHI) und Quellcode handhabt. Die ungesteuerte Nutzung mobiler Endgeräte ohne zentrale Verwaltung oder Sicherheitskontrollen setzt das Unternehmen kritischen Risiken wie Datenverstoß (R01), Datenleck (R02) und Netzwerkkompromittierung (R03) aus. Diese Risiken stellen eine direkte Bedrohung für die Kernwerte, den Ruf und die DSGVO-Konformität des Unternehmens dar.

Der derzeitige Ad-hoc-Ansatz ist daher nicht tragfähig. Nach dem auslösenden Vorfall mit dem verlorenen Tablet ist eine strukturierte Lösung zwingend erforderlich. Es wird der Geschäftsführung daher formell empfohlen, die Entwicklung und unternehmensweite Implementierung einer Informationssicherheitsrichtlinie für mobile Endgeräte zu autorisieren. Diese Richtlinie schafft den verbindlichen Rahmen für eine MDM-Lösung.

Das BSI erachtet eine solche Lösung als "unabdingbar für einen geregelten und sicheren Betrieb" mobiler Endgeräte.

Die Umsetzung dieser Richtlinie ist der wesentliche nächste Schritt, um die identifizierten Risiken zu mindern, regulatorische Anforderungen zu erfüllen und ein sicheres, produktives mobiles Arbeiten zu ermöglichen.