Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 6. Übung im SoSe 2021:
Praktische IT-Sicherheit

6.1 ISMS Einrichtungsfehler

Aufgabe:

- Nennen Sie fünf grundlegende Fehler, die beim Aufbau eines **Informations-Sicherheits-Management-Systems (ISMS)** besser vermieden werden sollten!

6.1 ISMS Einrichtungsfehler (1)

- **ISMS falsch ausrichten**:
  - Nicht alle relevanten Anforderungen (rechtlich, vertraglich, eigene Vorgaben, Stand der Technik) ermitteln vor Einrichtung des ISMS
  - Sich mit der Einrichtung selbst „zufrieden geben“
  - Methodologien wählen, die nicht adäquat zum Kontext sind

- **ISMS falsch steuern**:
  - Risikomanagement nicht auf Kontext ausrichten
  - Methoden einsetzen, die einfach oder billig erwerbbar sind
  - Einsatz lediglich vordefinierter Gefährdungskataloge
  - Risikoanalyse als „lästige“ Pflicht ansehen

6.1 ISMS Einrichtungsfehler (2)

- **Zentrale ISMS-Funktionen falsch besetzen**:
  - Den falschen Beauftragten für Informationssicherheit einsetzen – nötig ist ein erfahrener Funktionsträger, der frei von operativen Interessenkonflikten ist und den nötigen Gesamtüberblick hat
  - Falsche Auditoren einsetzen, welche nicht beide Bereiche, Technik und Organisation/Prozesse, ausreichend tief abdecken können
  - Die falschen Mitglieder ins CSIRT einsetzen – zunächst werden solche Personen benötigt, die über ausgeprägte Analysefähigkeiten verfügen, um Ursachen für Information Security Incidents zutreffend ermitteln zu können

6.1 ISMS Einrichtungsfehler (3)

- **Beim ISMS die falschen Dinge regeln**:
  - In den Policies oder Sicherheitskonzepten die Zielvorstellungen angeben und dabei die Realität nicht berücksichtigen – in den Sicherheitskonzepten ist in erster Linie der IST-Stand zu dokumentieren und nur dann ein SOLL-Ziel aufzunehmen, wenn die zugehörige Maßnahme bereits geplant ist und bisher nur noch nicht vollständig umgesetzt wurde
  - Dinge regeln, die zu abstrakt oder hinsichtlich ihrer Wirksamkeit nicht mit vertretbarem Aufwand überprüfbar sind
  - Dinge unabhängig von Risikoanalysen zu regeln
  - Muster-Policies ohne Berücksichtigung des Kontextes übernehmen

6.1 ISMS Einrichtungsfehler (4)

- **Beim ISMS Sicherheitsvorfälle falsch adressieren**:
  - Aufbau eines Information Security Incident Managements ohne ausreichende Implementierung der Erhebung von Sicherheitsvorfällen – Solche müssen erst mal von betroffenen Stellen „erkannt“ bzw. technisch geeignet aufgezeichnet werden
    → Awareness über Sicherheitslücken und Sicherheitsvorfälle
    → Security Incident Response Readiness via Protokolle, IDS, etc.
    → klar definierte Meldeketten
  - Bei der Behebung von Sicherheitsvorfällen nicht berücksichtigen, ob ggf. Schritte zur Verfolgung der Verursacher eingeleitet werden sollen (hat sonst beweisvernichtende Vorgehensweisen zur Folge, die eine straf- oder zivilrechtliche Verfolgung unmöglich machen)
  - Auswirkung von Sicherheitsvorfällen falsch einschätzen
  - Kein (zeitlich begrenztes) Exception Handling für Ausnahmen zur Beseitigung von Sicherheitsvorfällen vorsehen

6.2 Interessenausgleich zwischen Betroffene & Systemnutzer

Aufgabe:

- Nennen Sie Beispiele, in denen sich die **Interessen** der **Betroffenen** von den Interessen der **Systemnutzer** deutlich unterscheiden! Welcher Ausgleich wäre in diesen Beispielen ein möglicher Kompromiss?

6.2 Interessenausgleich zwischen Betroffene & Systemnutzer

Beispiele für abweichende Interessen:

- Systemnutzer möchten möglichst detaillierte Daten angezeigt bekommen, um sicher gehen zu können, dass sie keine fehlerhaften Daten eingeben bzw. bearbeiten. Betroffene möchten, dass verantwortliche Stellen nur so viel Daten über sich haben, wie unbedingt nötig. Der Ausgleich erfolgt daher durch das **Berechtigungskonzept**, in dem festgelegt ist, welcher Nutzer welche Daten (zu welchem Zweck) einsehen und bearbeiten darf.
- Systemnutzer wünschen eine umfassende Datensicherung, damit im Falle eines ungewollten Datenverlustes oder bei einem zeitlich späteren Vorgang noch die Historie berücksichtigt werden kann. Betroffene möchten, dass ihre Daten nur für die vorgeschriebene Dauer abrufbar sind. Der Ausgleich erfolgt daher über die Regelungen zur **Sperrung** (= „Einschränkung“ nach EU-DSGVO) von Daten.

6.3 CSIRT

Aufgabe:

- Welche Aufgaben sollte ein **Computer Security Incident Response Team (CSIRT)** ausführen?

6.3 CSIRT (1)

Aufgaben Computer Security Incident Response Team (CSIRT):

- Analyse & Bewertung von Sicherheitsvorfällen
  - Einstufung zur Kritikalität von Sicherheitsvorfällen (je kritischer, desto rascher muss Sicherheitsvorfall wirksam behandelt werden)
  - Kategorisierung von Sicherheitsvorfällen (Angriff von außen/innen, Malwarebefall, DoS-Attacke, Rechtemissbrauch befugter User, …)
- Behandlung von Sicherheitsvorfällen (inkl. Ausführung von Notfall- bzw. Ausnahmeregeln zur Beseitigung von Sicherheitsvorfällen und Rück-führung zum Normalbetrieb)
- Minimierung der Wirkung von Sicherheitsvorfällen
- Meldung über Sicherheitsvorfälle an zuständige Stellen (z.B. wg. Datenpanne oder Eskalation)
- Nachbereitung zu Erkenntnissen aus Sicherheitsvorfällen

6.3 CSIRT (2)

Aufgaben Computer Security Incident Response Team (CSIRT) gemäß EU-NIS-Richtlinie 2016/1148:

- Entgegennahme und Bearbeitung unverzüglich gemeldeter Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Verfügbarkeit der wesentlichen Dienste haben (Art. 14 Abs. 3); maßgebliche Parameter sind dabei:
  a) Zahl der von der Unterbrechung der Erbringung des wesentlichen Dienstes betroffenen Nutzer
  b) Dauer des Sicherheitsvorfalls
  c) geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet

  Für Anbieter digitaler Dienste (z.B. Cloud Computing) in Art. 16 Abs. 4 ergänzt um Ausmaß der Unterbrechung der Bereitstellung des Dienstes sowie Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten
- Unterrichtung des betroffenen Mitgliedsstaates, sofern der Vorfall erhebliche Auswirkungen auf die Verfügbarkeit wesentlicher Dienste in jenem Mitgliedstaat hat (Art. 14 Abs. 5; erstreckt sich das auf mehrere, sind alle betroffenen zu unterrichten nach Art. 16 Abs. 6)

6.3 CSIRT (3)

Aufgaben Computer Security Incident Response Team (CSIRT) gemäß EU-NIS-Richtlinie 2016/1148: (Fortsetzung)

- Überwachung von Sicherheitsvorfällen (Anhang I Ziffer 2 lit. a Punkt i)
- Ausgabe von Frühwarnungen und Alarmmeldungen sowie Bekanntmachung und Verbreitung von Informationen über Risiken und Vorfälle unter den einschlägigen Interessenträgern (Anhang I Ziffer 2 lit. a Punkt ii)
- Reaktion auf Sicherheitsvorfälle (Anhang I Ziffer 2 lit. a Punkt iii)
- dynamische Analyse von Risiken und Vorfällen und Lagebeurteilung (Anhang I Ziffer 2 lit. a Punkt iv)
- Beteiligung am CSIRTs-Netzwerk (Anhang I Ziffer 2 lit. a Punkt v)
- Zur Erleichterung der Zusammenarbeit fördern von Annahme und Anwendung gemeinsamer oder standardisierter Verfahren für Abläufe zur Bewältigung von Sicherheitsvorfällen und Risiken sowie Systeme zur Klassifizierung von Sicherheitsvorfällen, Risiken und Informationen (Anhang I Ziffer 2 lit. c)

EU-NIS-RL für digitale Dienste integriert in § 8c BSIG, allerdings ohne CSIRT-Pflicht

6.4 Informationssicherheit beim Outsourcing

Aufgabe:

- Worauf sollte ein Unternehmen aus Gründen der Informationssicherheit hinsichtlich seiner **Lieferanten / Dienstleister** achten?

6.4 Informationssicherheit beim Outsourcing (1)

Nach Kapitel 15 der **ISO/IEC 27002:2013** sollte sich ein Auftraggeber um **Informationssicherheit in Lieferantenbeziehungen** wie folgt kümmern:

- Sobald ein Auftragnehmer bzw. Lieferant Zugriff auf (Primary oder Supporting) Assets des Auftraggebers erhält, sollten mit diesem **einzuhaltende Anforderungen zur Informationssicherheit** vereinbart und dokumentiert werden.
- In einer Informationssicherheitsrichtlinie für Lieferantenbeziehungen sollte insbesondere festgelegt werden:
  - **Mindestanforderungen an die Informationssicherheit** für jede Informations- und Zugriffsart entsprechend den geschäftlichen Bedürfnissen und den Anforderungen des Auftraggebers sowie entsprechend des Risikoprofils des Auftraggebers
  - **Prozesse und Verfahren zur Überwachung** der Einhaltung der festgelegten Anforderungen an die Informationssicherheit für jede Lieferanten- und Zugriffsart
  - **Umgang mit Vorfällen und Gefahren** im Zusammenhang mit dem Lieferantenzugriff

6.4 Informationssicherheit beim Outsourcing (2)

In **Lieferantenvereinbarungen** sollte insbes. festgelegt & dokumentiert werden:

- Wie vom Auftragnehmer / Lieferant die Einhaltung gesetzlicher und regulativer **Anforderungen zu Datenschutz, geistigen Eigentumsrechten und Urheberrecht** sichergestellt wird
- Verpflichtungen zur Umsetzung vereinbarter Maßnahmen hinsichtlich
  - Zugangs- bzw. Zugriffssteuerung,
  - Leistungsüberprüfung,
  - Überwachung,
  - Berichterstattung und
  - Auditierung
- Vertragsrelevante Richtlinien zur Informationssicherheit
- Anforderungen und Verfahren für die Handhabung von Vorfällen
- Relevante Vorschriften für Unteraufträge
- Recht zur Überprüfung der Lieferantenprozesse und vertragsbezogener Maßnahmen sowie Vorlage unabhängiger Wirksamkeitskontrollberichte

6.4 Informationssicherheit beim Outsourcing (3)

In **Lieferantenvereinbarungen** sollten ferner insbesondere die Anforderungen für den Umgang mit Informationssicherheitsrisiken, die mit Informations- und Kommunikationsdienstleistungen und der Produktlieferkette verbunden sind, aufgenommen werden:

- Verpflichtung zur Weitergabe der Sicherheitsanforderungen innerhalb der gesamten Lieferkette (inkl. Unterauftragnehmer, Lieferanten des Auftragnehmers / Lieferanten)
- Zusicherung, dass bereitgestellte Informations- und Kommunikationstechnik wie erwartet funktioniert und keine unerwarteten oder unerwünschten Eigenschaften aufweist
- Festlegung von Regeln für die Mitteilung von Informationen über mögliche Probleme und Kompromisse zwischen Auftraggeber und Auftragnehmer / Lieferant

6.4 Informationssicherheit beim Outsourcing (4)

Das **vereinbarte Niveau der Informationssicherheit** sollte im Einklang mit den Vereinbarungen **aufrecht erhalten** werden insbesondere durch:

- Durchführung von Lieferanten-Audits, inkl. Problem-Nachverfolgung
- Bereitstellung von Informationen zu Informationssicherheitsvorfällen und Überprüfung dieser Informationen
- Überprüfung der Aufzeichnungen zu Informationssicherheitsereignissen, Problemen im Zuge der Auftragsausführung, Ausfällen, Fehler-Nachverfolgungen und Unterbrechungen
- Überprüfung von Aspekten der Informationssicherheit bei den Beziehungen des Auftragnehmers / Lieferanten zu seinen eigenen Lieferanten
- **Erneute Risikobeurteilung**, insbesondere bei
  - Änderungen an den vertraglichen Vereinbarungen mit dem Auftragnehmer / Lieferant
  - Neue oder geänderte Maßnahmen zur Lösung von Informationssicherheitsvorfällen und zur Verbesserung der Sicherheit
  - Nutzung neuer Technologien oder neuer Entwicklungswerkzeuge

6.4 Informationssicherheit beim Outsourcing (5)

Hier bestehen deutliche Unterschiede zwischen Auftraggeber und Auftragnehmer / Lieferant im Kontext der Supply Chain:

- Auftragnehmer hat oft **anderen Risikoappetit** als ihre Auftraggeber
  → Pönale i.d.R. weit geringer als potenzieller Schaden bei Risikoeintritt!
  → Wirtschaftliches Handeln legt teils Akzeptanz Pönale nahe
- Auftragnehmer verwendet oft **andere Methodologie zur Risikoanalyse** (oder anders ausgeprägter Methodologie) als ihre Auftraggeber
  → das steht in Beziehung zum jeweiligen Geschäftsmodell…
- Auftragnehmer hat **andere Vorstellung hinsichtlich meldepflichtiger Security Incidents** als Auftraggeber, wenn dies nicht ausdrücklich festgelegt wurde (was jedoch in der Praxis nur bedingt möglich ist…)
- Für Auftragnehmer ist es i.d.R. von **nachrangigem Interesse**, **welche Datenkategorien** im Auftrag verarbeitet werden, für Auftraggeber sind dagegen die überlassenen Daten u.U. grundlegend

→ **Das jeweils implementierte ISMS weicht stark voneinander ab!**

→ **Vorgelegtes Zertifikat genau prüfen (Scope, SoA, Aussteller)!**

6.4 Informationssicherheit beim Outsourcing (6)

- Nötig ist **Aushandlung** zwischen Auftraggeber & Auftragnehmer zu:
  1. Welche Informationen über das **Sicherheitsniveau** beim Auftragnehmer sind für realistische Bewertung der mit der Auslagerung verbundenen Risiken nötig?
  2. Welche **Kontrollrechte** sind für Auftraggeber erforderlich, um sich ein zutreffendes Bild über das Sicherheitsniveau beim Auftragnehmer vor allem hinsichtlich dessen Risikoappetit verschaffen zu können?
  3. Ab wann besteht ein ausreichendes **Vertrauen**, so dass der Auftragnehmer tatsächlich auch aufgetretene Schwachstellen dem Auftraggeber mitteilt, ohne „das Schlimmste“ befürchten zu müssen?
- Die Auslagerung selbst stellt ein **spezifisches Risiko** dar, das im Hinblick auf die Konsequenzen für den Auftraggeber (ohne unterstellte kompensatorische Maßnahmen) zu bewerten ist
- Im Rahmen des Risikomanagements sollte auch bei entsprechender Auslagerung die **zugehörigen Gefährdungen** (Bedrohungen und Verwundbarkeiten) **miteinbezogen** werden (zugesicherte Maßnahmen des Auftragnehmers dienen dann der Mitigation der ermittelten Risiken)

6.5 Informationssicherheit bei der Softwareentwicklung

Aufgabe:

- Welche Maßnahmen sollten aus Gründen der Informationssicherheit bei der **Entwicklung von Software** ergriffen werden?

6.5 Informationssicherheit bei der Softwareentwicklung (1)

Maßnahmen zur Planung der Softwareentwicklung:

- Festlegung zu erreichender Sicherheitsziele und des zu erreichenden Zielerreichungsgrades
- Festlegung über die Prüfmethoden zur Feststellung über den tatsächlich erreichten Zielerreichungsgrad
- Festlegung zu verwendender Programmierrichtlinien, Programmierstandards und Secure Coding Guidelines
- Festlegung zu den erwarteten Sicherheitsmechanismen in der zu erstellenden Software
- Festlegung zum Berechtigungs- und Benutzerrollenkonzept, welches von der Software erfüllt werden soll
- Festlegung zu den Protokollierungsfunktionen der zu entwickelnden Software

6.5 Informationssicherheit bei der Softwareentwicklung (2)

Maßnahmen zur Softwareentwicklung:

- Wirksame Abschottung Entwicklungsumgebung & Produktivumgebung
- Einsatz von anonymisierten Testdaten (bzw. nur dann von Echtdaten, wenn dies ausdrücklich entsprechend freigegeben wurde)
- Konstruktion der Sicherheitsmechanismen gemäß dem Grundsatz zur gestaffelten Abwehr, d.h. die Umgehung eines Sicherheitsmechanismus darf nicht zur Umgehbarkeit aller Mechanismen führen
- Umsetzung der Eingabevalidierung, z.B. mittels Prepared Statements, Stored Procedures bzw. Escaping Mechanismen
- Umsetzung der Ausgabevalidierung bei Schnittstellen
- Grundeinstellung der Software mit robustem Fail-Safe-Mechanismus
- Durchführung von Funktionstests, insbesondere auch zur Wirksamkeit der implementierten Sicherheitsmechanismen

6.5 Informationssicherheit bei der Softwareentwicklung (3)

Maßnahmen zur Softwareentwicklung: (Fortsetzung)

- Auflistung der bei Implementation der Software zu ändernden Voreinstellungen (insbesondere der voreingestellten Systemkennwörter)
- Datensicherung des Quelltextes (und dessen Hinterlegung)