Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 9. Übung im SoSe 2018:
Praktische IT-Sicherheit

9.1 Sicherheitskonzept Telearbeit

Aufgabe:

- Entwerfen Sie ein **Sicherheitskonzept** zur Nutzung von Laptops, mit denen im Zuge von Telearbeit (Home Office oder Außendienst) auch vertrauliche Daten bearbeitet und an den eigentlichen Unternehmens-standort übertragen werden!

9.1 Sicherheitskonzept Telearbeit (1)

- Festplatte des Laptops gemäß dem Stand der Technik verschlüsseln
- systemseitiges Abklemmen externer Laufwerke & Wechseldatenträger; Einrichtung eines Boot-Schutzes
- kein Zugriff auf Betriebssystemebene und Konfigurationen der eingesetzten IT-Komponenten (→ Nutzerrechte, keine Administrationsrechte)
- vorzugsweise Identifizierungs- und Authentisierungsmechanismus mittels Smartcard- oder Fingerabdruckverfahren
- monatliche Änderung der Zugangs- und Zugriffspassworte durch den Beschäftigten unter Einhaltung der Komplexitätsvorschriften
- Erschwerung mehrfach missglückter Neuanmeldeversuche (durch Geringhalten zulässiger Fehlversuche und sukzessive Erhöhung der Zeitabstände für erneute Versuche)
- Automatische Bildschirmsperre bei fehlender Aktivität von 10 Minuten und deren Aufhebung nur mittels Authentifizierung

9.1 Sicherheitskonzept Telearbeit (2)

- Konfiguration minimal entsprechend der zu erfüllenden Aufgaben
- Protokollierung aller sicherheitsrelevanten Aktivitäten
- Virenscanner so installieren, dass dieser bei jeder Anmeldung am LAN und in regelmäßigen Abständen auch während einer bestehenden Verbindung automatisch aktualisiert wird
- kein freier Zugriff auf das Internet
- Freischaltung nur der zur Aufgabenerfüllung zwingend erforderlichen Ports
- Kommunikation zwischen Laptop und LAN nur unter Ausnutzung einer dem Stand der Technik entsprechende starke Transportverschlüsselung (üblicherweise Triple-DES); ein Verbindungsaufbau darf nur nach ausdrücklicher Bestätigung durch den Beschäftigten erfolgen
- Absicherung einer erfolgreichen Datenübertragung mittels Quittierungsverfahren

9.1 Sicherheitskonzept Telearbeit (3)

- zur Telearbeit dürfen ausschließlich gestellte IT-Komponenten (Hardware und Software) eingesetzt, an den Einstellungen keine Änderungen vorgenommen und keine weiteren IT-Komponenten angeschlossen werden
- Zutrittsrecht des Arbeitgebers zum Telearbeitsplatz ist mit dem Beschäftigten zu vereinbaren
- Laptop ist in einem klar separierten und verschließbaren Arbeitszimmer so aufzustellen, dass keine unbefugte Einsichtnahme auf den Bildschirm (weder im Zuge des Betretens des betreffenden Arbeitszimmers noch durch Beobachtung durch etwaige Fenster) stattfinden kann
- streng vertrauliche Unterlagen dürfen außerhalb der Arbeitszeit bzw. Tätigkeit des betreffenden Beschäftigten ausschließlich in verschließbaren Behältnissen gelagert werden

9.2 Serversicherheit

Aufgabe:

- Listen Sie empfehlenswerte Maßnahmen zur **Serversicherheit** auf!

9.2 Serversicherheit (1)

Serversicherheit = Sicherheit der eingesetzten Server

→ Physische Sicherheit der Server + Vorgaben zur Administration von Servern

- Zugangsbefugnis nur für Administratoren
- Nicht mehr benötigte Zugangsberechtigungen unverzüglich entziehen
- Zugangsmittel, wie z.B. Chipkarten, Token, Kennwörter, PIN, etc., vor unbefugter Verwendung sichern
- Vergabe von Zugangsberechtigungen vorzugsweise durch andere Administratoren (soweit möglich) → keine Selbstbefugniserteilung
- Verwendung starker Kennwörter zur Administration:
  ° ausreichende Länge (mind. 12-stellig; für User reicht 8-stellig)
  ° mit aktivierten Komplexitätsregeln
  ° mit ausreichend kurzer Zeitspanne (max. 3 Monate)
- Administrative Passwörter nicht serverseitig im Klartext speichern
- Keine Verwendung allgemeiner Administrationsaccounts (wie z.B. „Admin“ oder „System“) oder voreingestellter Default-User (→ personalisierten Administrationsaccount einsetzen)

9.2 Serversicherheit (2)

- Fernzugriff auf Serversysteme nur über eine nach aktuellem Stand der Technik verschlüsselte Verbindung
- Voreingestellte Standardpasswörter ändern, bevor ein Server produktiv genutzt wird; Änderung vor Produktivsetzung prüfen
- Prüfen, ob Serversysteme bei Eintritt eines Fehlerfalls über sichere und ausreichend robuste Default-Einstellungen verfügen, um einen Wiederanlauf in der vorgesehenen Zeit zu ermöglichen
- Die Überwindung eines einzigen Sicherheitsmechanismusses darf nicht zur Kompromittierung des gesamten Serversystems führen
- Serversysteme dürfen nur solche Fehlermeldungen an Benutzer senden, die nicht unnötig interne Konfigurationszustände offenbaren; dies gilt vor allem im Rahmen des Anmeldeverfahrens an einem Serversystem
- Inaktive Sitzungen nach Ablauf einer kurzen Zeitspanne systemseitig beenden
- Stets alle erforderlichen Sicherheitspatches zeitnah einspielen
- Serversysteme härten (→ Entfernung nicht benötigter Dienste & Ressourcen)

9.2 Serversicherheit (3)

- Bei der Aktualisierung von Software prüfen, ob die vorgenommene Härtung danach weiterhin Bestand hat oder ggf. in der neuen Version entsprechend nachgezogen werden muss
- Für eingesetzte Hardware & Software muss für vorgesehene Einsatzdauer ein ausreichender Support des jeweiligen Herstellers bzw. Distributors bzw. der entwickelnden Stelle zugesichert sein
- Gespeicherte Daten müssen für Dauer der Aufbewahrungsfrist weiterhin lesbar sein (→ ggf. rechtzeitig in migrationsfähigem Format auf anderes Serversystem umziehen)
- Regelmäßiger Sicherheitscheck der eingesetzten Serversysteme
- Verfolgung abrufbarer Schwachstellenmeldungen zu den eingesetzten Serversystemen
- Wenn ein Server einem Angriff ausgesetzt ist, sollte dies einen aufgezeichneten Event auslösen, der zeitnah vom zuständigen Administrator bearbeitet werden kann

9.3 Informationssicherheit beim Outsourcing

Aufgabe:

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

9.3 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

9.3 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

9.3 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

9.3 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

9.3 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)!**

9.3 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)

9.4 Informationssicherheit bei der Softwareentwicklung

Aufgabe:

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

9.4 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

9.4 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

9.4 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)

9.5 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?

9.5 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.