esse

ESSE Einführung in Security – VO 06: Organisatorische Sicherheit/Sicherheitsmanagement

Florian Fankhauser, Christian Schanes

24W

ESSE (Establishing Security) – IT Security Research Team
Research Group for Industrial Software (INSO)
https://establishing-security.at/

Agenda

- Einleitung
- Beispiele Organisatorischer Sicherheitsmaßnahmen
- Sicherheitsmanagementprozess
- (Security) Policies
- PDCA-Modell
- Standards und Normen zu IT-Sicherheit
- Sicherheitskonzepte
- Literatur
- Zusammenfassung

Technische vs. organisatorische Sicherheit

- Bestimmte Herausforderungen lassen sich besser bzw. nur durch organisatorische Maßnahmen lösen.
- „If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.“ (B. Schneier)
- Breiter Bogen unterschiedlicher Aspekte

Beispiele für technische Sicherheitsmaßnahmen

- Passkeys
- Firewall, Virenscanner
- Kryptographie
  - Verschlüsselung
  - Elektronische Signaturen
  - Hashes
- Absicherung (drahtloser) Kommunikationswege (LAN, WLAN, etc.) mittels VPN/TLS
- Sicherheits-Patches und Systemhärtung (siehe Vorlesung zu Betriebssystemsicherheit)
- Sandbox-Systeme (siehe Vorlesung zu Betriebssystemsicherheit)

Organisatorische Sicherheitsaspekte

- Primär der Aufbau des IT-Sicherheits-Managements (Sicherheitsplanung)
- GF: Formulierung einer IT-Sicherheitsleitlinie (strategische Aussagen)
- Typische Aufgaben sind z.B.
  - Eindeutige Definition von Verantwortlichkeiten inklusive Vertretungsregelungen sowie Kommunikationswege
  - IT-Benutzer:innen schulen und für Sicherheit sensibilisieren
  - Alle Maßnahmen und Veränderungen dokumentieren
  - Regelmäßige Audits
- IT-Sicherheit muss vom Management, den Administrator:innen und den IT-Benutzer:innen als fortlaufender Prozess verstanden und gelebt werden!

Beispiele Organisatorischer Sicherheitsmaßnahmen

Schulung von Mitarbeiter:innen

- Mitarbeiter:innen brauchen eine ausreichende Einführung und Schulung
- Ziel ist Etablierung eines Sicherheitsbewusstseins
- Betrifft sowohl den sicheren Umgang mit IT-Systemen, als auch Unternehmensdaten
- Regelmäßige Schulungen und Sicherheitssensibilisierungen
- Rechtzeitige Unterrichtung der Mitarbeiter:innen über Bedrohungen

Sicherung von Daten

- Verlust von Daten kann zu Einschränkungen im Betrieb und wirtschaftlichen Schäden führen
- Daher: aktive Datensicherung (Backup)
- Durchführung regelmäßiger Backups nach einem Backup-Plan
- Bei wichtigen Daten evtl. auch Sicherungskopien außerhalb des Unternehmens
- Regelmäßige Kontrolle der Backups/Test der Wiederherstellung gesicherter Daten (Restore)

Sicheres Löschen von Daten

- Besonderer Schutz für sensible Daten
- Löschen nach Ende von Aufbewahrungsfristen, Hardwaretausch etc.
- Häufiger Fall: ausrangierte HDDs enthalten interne Zahlen, Kund:inneninformationen, Zugangsdaten,...
- Einfaches Löschen nicht ausreichend – Daten können oft wiederhergestellt werden
- Verwendung von spezieller Soft- und/oder Hardware zur Zerstörung, z.B. thermisch, aktives Überschreiben
- Auslagerung an spezialisierte Unternehmen
- Durchgehende Anwendung von Verschlüsselung
- Berücksichtigung von Ausdrucken/Papier-Unterlagen

„Entsorgung“ von Aktenordnern

Updates

- Ständige Weiterentwicklung von Schadprogrammen, tw. mit sehr hohem Gefährdungsgrad
- Aufkommen neuer Technologien, die Angriffe ermöglichen oder die Angriffswahrscheinlichkeit erhöhen

- Laufende Updates der Risiko- und Bedrohungsanalysen
- Zeitnahe Installation von Sicherheitsupdates
- Wartung eingesetzter Soft- und Hardware

- $\rightarrow$ Prozesse

Dokumentation

- Soft- und Hardware, Daten, Prozesse
- Stetig aktuelle Dokumentation bildet oft Grundlage für Aufgaben
- Einzuhaltende Sicherheitsanforderungen
- Konfigurationen der (wichtigsten) Systeme
- Servicenummern der (wichtigsten) IT-Lieferanten und IT-Dienstleister
- Vertragliche Vereinbarungen, SLAs

- Prozesse (Onboarding, Offboarding,...)
- Berechtigungen

- Möglichst hoher Automatisierungsgrad

Überprüfung der Wirksamkeit von (organisatorischen) Sicherheitsmaßnahmen

- (Organisatorische) Sicherheitsmaßnahmen und Vorgaben sind regelmäßig auf Einhaltung und Wirksamkeit zu überprüfen
- $\rightarrow$ Dokumentation
- Aktualität von Software/IT-Systemen
- Einhaltung von Richtlinien seitens der Mitarbeiter:innen
- Aktualität der Notfallpläne und Dokumentationen
- Test durch externe Dienstleister, z.B. Penetrationstests
- Besteht die Erfordernis, müssen entsprechende Anpassungen vorgenommen werden

Use Checklists

(Vergleiche schienestrasseluft.de, West Pharmaceutical Services, Inc., Tesla Factory, Fremont (Maurizio Pesce), Curimedia)

Sicherheitsmanagementprozess

Festlegung der IT-Sicherheitsverantwortlichen-Rollen

- Klare Regelung von Verantwortlichkeiten und Zuständigkeiten
- Festlegung IT-Sicherheitsverantwortliche:r (CISO) (und Vertretung) durch Management
- Ansprechpartner:in bei auftretenden Sicherheitsproblemen
- Typische Rollen sind beispielsweise
  - Information Security Manager:in (Zentrale Koordination und Ansprechperson für das Thema Sicherheit)
  - Information Risk Manager:in (Erkennung, Bewertung, Management von Risiken)
  - IT-Sicherheitsbeauftragte:r (Umsetzung von Sicherheitsmaßnahmen)
  - Datenschutzbeauftragte:r (Schutz personenbezogener Daten)

Security Policies

„Die Sicherheitsrichtlinie (engl. security policy) eines Systems oder einer organisatorischen Einheit legt die Menge von technischen und organisatori- schen Regeln, Verhaltensrichtlinien, Verantwortlichkeiten und Rollen sowie Maßnahmen fest, um die angestrebten Schutzziele zu erreichen.“

„Jede Organisation ist frei, die für ihren geschäftlichen Kontext als relevant erachteten Ziele individuell festzulegen. Diese Ziele sind zu dokumentieren, was meist im Überblick in einer Security Policy erfolgt – im Deutschen meist als Sicherheitsleitlinie bezeichnet.“

(Vergleiche Eckert, IT-Sicherheit; Kersten, IT-Sicherheitsmanagement nach der neuen ISO 27001)

Inhalte von (Security) Policies

- Angestrebte IT-Sicherheitsziele
- Verfolgte IT-Sicherheitsstrategie
- Anspruch und Aussage zugleich, dass das IT-Sicherheitsniveau auf allen Ebenen der Organisation erreicht werden soll
- Die Verantwortung für die Security Policy unterliegt der Unternehmens-/Behörden/...-leitung
- Eine Policy muss von der GF verabschiedet und vorgelebt werden

Anforderungen an Policies

- Vollständigkeit der Policies
- Bekanntheit der Policies
- Verständnis und aktives „Leben“ der Policies
- Laufende Überprüfung der Einhaltung von Policies

Sicherheitsrichtlinien für Mitarbeiter:innen

- Eines der größten Risiken ist Fehlverhalten von Mitarbeiter:innen
- Policies enthalten Vorgaben, um diesem Risiko entgegenzuwirken, bzw. dieses zu mindern
- Beschreibung wie sicher und korrekt mit IT und deren Komponenten umgegangen wird
- Fortwährende Anpassung und Ergänzung aufgrund aktueller Entwicklungen wichtig (z.B. Smartphones, BYOD)

Konkrete Beispiel-Policies: TU Wien

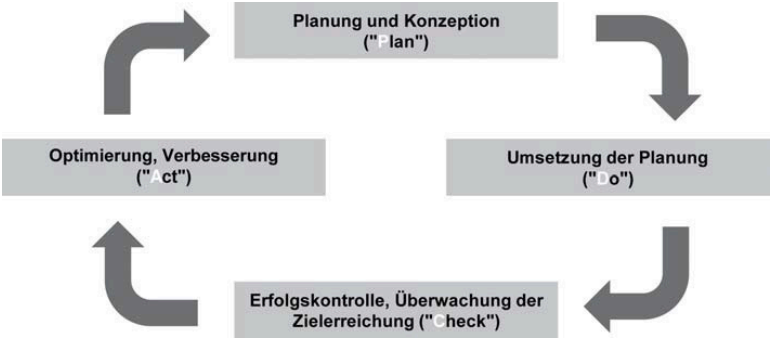
- Betriebs- und Benutzungsordnung des Zentralen Informatikdienstes (ZID) der TU Wien
- Die Security Policy der TU Wien
- Benützungsregelung für die Services von TUNET

- `https://www.it.tuwien.ac.at/regelungen`
- `https://www.tuwien.at/tu-wien/organisation/zentrale-bereiche/information-security`

Weitere Beispiele für mögliche Policies

- Nutzung der IT und des Internets am Arbeitsplatz
- Datenschutz
- Zutritts-, Zugangs- und Zugriffsschutz
- Anlage/Deaktivierung bzw. Löschung von Accounts
- Verwendung von USB-Sticks
- Private Verwendung von Notebooks
- Verschlüsselung von Daten auf mobilen Clients
- Externe Besucher:innen in Firmenräumen
- Passwort-Policy
- SANS Security Policy Templates

PDCA-Modell als Beispiel für einen Sicherheitsmanagementprozess



(Vergleiche BSI-Standard 100-1: IT-Grundschutz-Vorgehensweise)

Planung (Plan)

- Planung und Installation eines Sicherheitsmanagements anhand Risiko-, Sicherheits- und Unternehmenspolitik, der betrieblichen Anforderungen sowie der gesetzlichen Vorgaben

- Definition Vorgehensmodell zu Sicherheits-, Kontinuitäts- und Risikopolitik
- Erhebung der Sicherheits- und Kontinuitätsanforderungen
- Erstellung von Sicherheits- und Kontinuitätsrichtlinien
- Entwicklung von Sicherheitskonzepten
- Planung der Durchführung von Maßnahmen

Betreiben (Do)

- Einführung, Betrieb und Monitoring des Sicherheitsmanagements

- Schulung und Sensibilisierung von Mitarbeiter:innen
- Betrieb unter Berücksichtigung der eingeführten Sicherheits- und Kontinuitätskonzepte
- Messung und Überwachung den Anforderungen entsprechend (Erkennung & Alarmierung)
- Sammlung von Controlling-Daten, Durchführung von Ist-Soll Vergleichen

Prüfung (Check)

- Prüfung des Sicherheitsmanagements in regelmäßigen Abständen

- Tests
- Audits
- Übungen
- Sicherheitsprüfungen

- Dokumentation, Analyse/Auswertung und Bericht der Ergebnisse

Verbesserung (Act)

- Weiterentwicklung des Sicherheitsmanagements

- Identifizierung von Potenzial bzw. Änderungsbedarf
- Adaptierung beispielsweise auf Grund
  - neuer Erkenntnisse
  - neuer Gesetze
  - Veränderungen der Umwelt
- Priorisierung von Bedarfen und Erstellung einer Roadmap/eines Projektplans zur Verbesserung

Wie schaffen wir Vertrauen in die IT-Sicherheit einer Organisation/eines Produkts?

Standards & Normen zu IT-Sicherheit

- Erreichung von Vertrauen in IT-Sicherheit: Standards und Normen
- *Zertifizierung*
- Nachweis eines bestimmten Levels an IT-Sicherheit
- Einmaliger Nachweis vs. regelmäßiger erneuter Nachweis der IT-Sicherheit
- Teilweise Grundlage für Vertragsbeziehungen

- Fokus auf unterschiedliche Aspekte der IT-Sicherheit
- Betriebs-Prozesse, Entwicklungs-Prozesse, Fertigungs-Prozesse, technische Maßnahmen

- ISO 27k-Reihe, IT-Grundschutz, Common Criteria (CC), COBIT, ITIL, PCI/DSS,...

Familie von Information Security Standards: ISO 27k-Reihe

- 27000: Übersicht/Einführung ISO27k Standards inkl. verwendeter Vokabeln
- 27001: Information Security Management System (ISMS) Anforderungen
- 27002: Information security, cybersecurity and privacy protection – Information security controls
- 27005: Information Security Risk Management Standard
- und viele weitere zu unterschiedlichsten Gebieten

ISO 27001

- Entwickelt, um die Auswahl geeigneter und angemessener Sicherheitskontrollen durchzuführen
- Spezifikation von Anforderungen an Informationssicherheitsmanagementsysteme (ISMS)
- Errichtung, Umsetzung, Betrieb, Überwachung, Überprüfung, Aufrechterhaltung und Verbesserung eines dokumentierten ISMS
- Anwendbar auf Bedürfnisse von Organisationen jeglicher Art, Größe oder Ausprägung oder Teile davon

Aspekte bei der Einführung eines ISMS nach ISO 27001

- ISMS-Richtlinie, die die Grundlagen des ISMS beschreibt
- Umfang des ISMS
- Prozeduren und Maßnahmen zur Pflege eines ISMS
- Beschreibung der Methoden zur Risikobewertung
- Risikobewertung selbst
- Plan zum Umgang mit Risiken
- Dokumentation der Sicherheitsmaßnahmen und eine Beschreibung zum Nachweis der Effektivität
- Erklärung über die Anwendbarkeit der einzelnen Sicherheitsmaßnahmen
- Evtl. weitere erforderliche Dokumente

IT-Grundschutz: Idee und Konzeption

- Herausgegeben vom BSI, Deutschland
- „Kochbuch“ für normales Schutzniveau
- Praktikable Durchführung von IT-Sicherheitsanalysen
- Kosteneffektive Erhöhung des IT-Sicherheitsniveaus
  - Schnelle Identifizierung von Sicherheitsmaßnahmen
  - Schnelle Umsetzung von Sicherheitsmaßnahmen
- Angemessener Schutz durch Kombination von organisatorischen, personellen, infrastrukturellen & technischen Maßnahmen
- Verwendung eines Baukastenprinzips: Bausteine, Gefährdungen, Maßnahmen
- Soll-Ist-Vergleich empfohlene und realisierte Maßnahmen
- Einfache und arbeitsökonomische Erstellung von IT-Sicherheitskonzepten

ITIL

- Information Technology Infrastructure Library
- ITIL Sicherheitsmanagement baut auf dem ISO 27001 Standard auf
- Hinweise zu Best-Practices
- Richtlinien was man wie umsetzen soll
- Prozess-basiert
- Optimierung des operativen Betriebs von IT-Services
- Anwendung auf nahezu alle IT-Infrastrukturen möglich

(Vergleiche S. Weil)

Sicherheitskonzepte

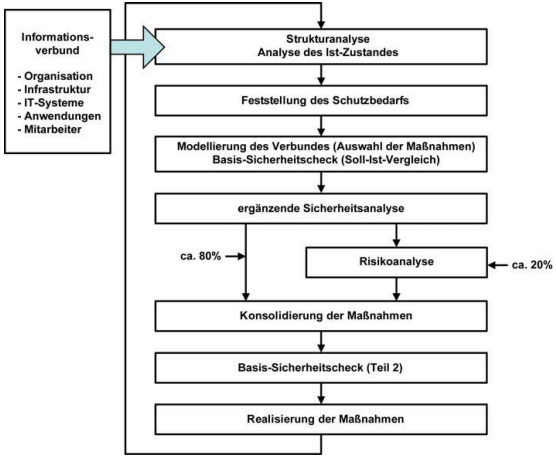
Inhalte eines IT-Sicherheitskonzepts

- Erforderliche Maßnahmen zur
- Realisierung und Aufrechterhaltung eines
- angemessenen und definierten Sicherheitsniveaus

Zu beantwortende Fragen in einem Sicherheitskonzept

- Was will ich schützen?
- Wogegen soll ich mich schützen?
- Wie kann ich diesen Schutz erzielen?
- Kann ich mir diesen Schutz leisten?

Schritte zur Erstellung eines Sicherheitskonzeptes nach IT-Grundschutz



(Vergleiche BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise)

Business Continuity (BC)

- Mögliche und erforderliche Verfahren und Konzepte,
- die bei Einwirkung existenzieller Bedrohungen
- die Erhaltung der Geschäftstätigkeit ermöglichen.

Literatur und Web-Referenzen 1/3

- Mutlaq Alotaibi, Steven Furnell, und Nathan Clarke. Information security policies: A review of challenges and influencing factors.
  In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, Seiten 352–358, Dezember 2016.
  doi: 10.1109/ICITST.2016.7856729
- Claudia Eckert. *IT-Sicherheit: Konzepte - Verfahren - Protokolle*.
  Oldenbourg, München, 9. Auflage, 2014.
  ISBN 978-3-486-77848-9
- Hans-Peter Königs. *IT-Risiko-Management mit System*.
  Vieweg+Teubner, Wiesbaden, 3. Auflage, 2009.
  ISBN 978-3-8348-0359-7

Literatur und Web-Referenzen 2/3

- Heinrich Kersten, Gerhard Klett, Jürgen Reuter, und Klaus-Werner Schröder. *IT-Sicherheitsmanagement nach der neuen ISO 27001*. Edition <kes>. Springer Vieweg, Wiesbaden. ISBN 978-3-658-14693-1
- Bundesamt fuer Sicherheit in der Informationstechnik. BSI Standard 200-1: Managementsysteme für Informationssicherheit (ISMS), 2017a. `https://www.bsi.bund.de/grundschutz`
- Bundesamt fuer Sicherheit in der Informationstechnik. BSI Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz, 2017b. `https://www.bsi.bund.de/grundschutz`

Literatur und Web-Referenzen 3/3

- Matt Bishop. *Introduction to Computer Security*.
  Pearson Education, Inc, 2003.
  ISBN 0-321-24744-2
- Ross Anderson. *Security Engineering. A Guide to Building Dependable Distributed Systems*.
  Wiley Publishing, Inc., 2. Auflage, 2008.
  ISBN 978-0-470-06852-6.
  https://www.cl.cam.ac.uk/~rja14/book.html
- Gitlab. Postmortem of database outage of January 31, 2017.
  https://about.gitlab.com/blog/2017/02/10/postmortem-of-database-outage-of-january-31/

Zusammenfassung

- Technische vs. organisatorische Sicherheit
- Beispiele für organisatorische Sicherheitsmaßnahmen
- Sicherheitsmanagement und der dahinterliegende Sicherheitsmanagementprozess
- (Security) Policies
- Beispiele für Standards: ISO 27k, IT-Grundschutz, ITIL
- Sicherheitskonzepte
- Business Continuity

Vielen Dank!

https://establishing-security.at/