e.solutions Partnerfirmennetzwerk

Unterlagen für die Schulung zur Informationssicherheit in ihrem Unternehmen

e.solutions

Motivation

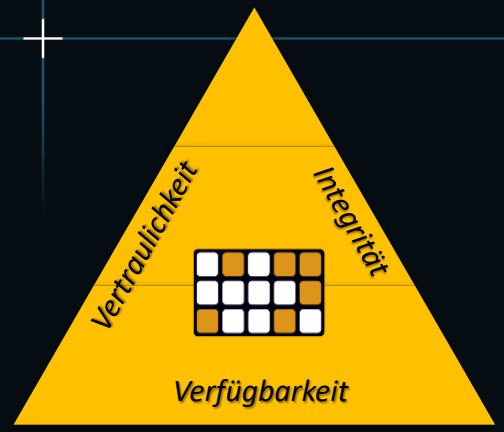
- *Verschärfte Sicherheitslage!*
  - Aktuelle Angriffsvorfälle (Komplexität & Häufigkeit)
- *Wachsende Komplexitäten*
  - Schnittstellen (intern / extern / international)
- *Auditanforderungen zur Informationssicherheit*
  - TISAX: VDA ISA
  - NIS2 – EU weite Gesetzgebung zur Netzwerk- und Informationssicherheit

Definitionen

Informationssicherheit	IT-Sicherheit	Datensicherheit	Datenschutz

▪ Schutz der CIA Prinzipien
▪ Informationen
  ▪ in allmöglichen Formen
  ▪ auf verschiedenen Systemen
▪ Technische und organisatorische Schutzmaßnahmen
  ▪ ISMS Organisation
  ▪ Richtlinien
  ▪ Audits
	▪ Schutz der IT-Systemen
	▪ Teilbereich der Informations-sicherheit
	▪ Technische Schutzmaßnahmen
	  ▪ Firewall
	  ▪ Verschlüsselung
	  ▪ Antivirus
	  ▪ 2 Faktor Authentifizierung
		▪ Schutz von Daten
		  ▪ Verlust
		  ▪ Verfälschung
		  ▪ Beschädigung
		  ▪ Wiederherstellung
		▪ Teilbereich der Informations-sicherheit
		▪ Beispiele
		  ▪ Backup
		  ▪ Datenlöschung
			▪ Schutz von personenbezogenen Daten
			▪ DSGVO (Datenschutz Grundverordnung)
			▪ Beispiele
			  ▪ private Anschrift
			  ▪ Geburtsdatum
			  ▪ biometrische Daten
			  ▪ Datenmaskierung

Ziele



- *Schutzziele gemäß CIA Modell*
  - **Confidentiality: Vertraulichkeit**
    - Informationen, die nicht zur allgemeinen Veröffentlichung bestimmt sind, sind nur den dafür Berechtigten zugänglich zu machen.
  - **Integrity: Integrität**
    - Eine fehlerfreie Verarbeitung der Informationen sowie der Schutz vor unberechtigter Veränderung ist zu gewährleisten.
  - **Availability: Verfügbarkeit**
    - Informationen sind innerhalb eines vereinbarten Zeitraums zur Verfügung zu stellen.
- *„need-to-know“*
  - Mitarbeiter bekommt nur die Informationen, die zur Erfüllung seiner Aufgabe nötig sind
- *Schutz vor unbefugten Zugriff, Manipulation, Sabotage, wirtschaftliche Schäden, etc.*

e.solutions

Gefährdungen und Angriffsziele

E-Mail:

- Zugriff auf Mailbox von Kollegen
- Weiterleitung
- Verschlüsselung von E-Mails an Kunden
- Signierung von E-Mails
- Weitergabe von Kontaktinformationen

Daten:

- Zugriffsschutz
- Soziale Netzwerke
- Umgang mit Passwörtern
- USB-Sticks und andere Datenträger
- Datensicherung
- Archivierung

Schutzziele:

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Sprache:

- Schutz vor Mithörern
- Abhörsichere Konferenzen
- Social Engineering
- Weitergabe von Kontaktinformationen

Papierdokumente:

- mobiler Arbeitsplatz
- Drucken
- Postversand
- Konferenzräume
- Datensicherung
- Vernichtung

Best Practices der e.solutions GmbH

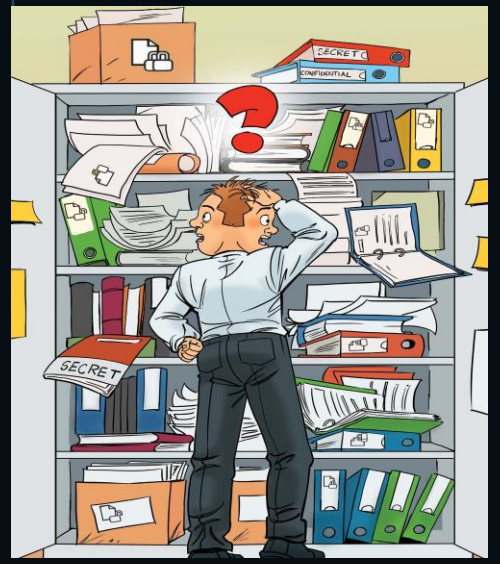
Fotografier/Aufnahmeverbot

Sicherheitszonen

Ausweistragepflicht

e.solutions

Best Practices der e.solutions GmbH



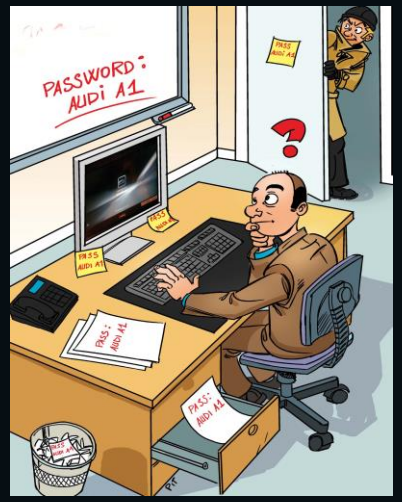
- *Klassifizierung der Daten*
  - öffentlich: z. B. Informationen der eso-Homepage
  - intern: z. B. Organigramm, Firmenkennzahlen
  - vertraulich z. B. Produktionsplanung, Releasepläne
  - streng Vertraulich: z. B. Prototypen, Code

- *Schutz der Informationen (auch Dokumente, Speichermedien)*
  - Schütze e.solutions Informationen vor unbefugten Zugriff (need to know Prinzip)
  - Bewahre e.solutions Geräte und Dokumente sicher auf
  - Vernichte Dokumente nach Gebrauch (hier stehen Datentonnen meist bei den Druckern bereit) und lösche e.solutions Medien nach Absprache mit uns
  - Drucker nach Papierende auffüllen ➢ Ansonsten kommt der Druckauftrag beim nächsten User heraus!

e.solutions

Best Practices der e.solutions GmbH

- *Schutz vor ungebetenen „Gästen“*
  - Sei wachsam, unterbinde Tailgating
  - Dokumentiertes Besuchermanagement ist empfehlenswert:
  - z. B. Besucherliste am Empfang, Besucherausweis
- *Verwendung von SmartCards*
  - SmartCard & PIN sind eine 2-Faktor-Authentifizierung: Wissen & Besitz
    - Die Karte ist der erste Faktor und die PIN ist der zweite Faktor
    - Sicherer Umgang mit PIN, Passwörtern etc.
  - Aufbewahrung SmartCard getrennt vom Rechner und stets im persönlichen Zugriff
    - Beim Verlassen des Rechners mitnehmen – immer!



e.solutions

Best Practices der e.solutions GmbH

- *Trennung Arbeit vs. privat*
  - Keine private Musik, Hörbücher, Online-Streaming, etc. auf e.solutions Arbeitsgeräten
  - Keine illegalen Downloads
  - Kein Peer-2-Peer Sharing
  - Keine Browser-Plugins zur Synchronisation
  - Keine Firmendaten auf privaten Geräten
  - Keine Cloud-Dienste zur Synchronisation oder Speicherung

- *E-Mail Verschlüsselung*
  - Bitte den Informationsaustausch per E-Mail verschlüsseln
    - MandatoryTLS bei hohen Schutzbedarf
  - Voraussetzung, eso.IT und Partnerfirmen haben Verfahren beidseitig implementiert.

Verhalten bei Sicherheitsvorfällen

- *Wenn ein Sicherheitsvorfall bekannt wird oder ein Vorfall/Verdacht aufkommt, bitte unverzüglich an*

eso.Group.CERT@esolutions.de

oder an

+49 8458 3332-911

melden.

Beispiele für Sicherheitsvorfälle:

- Verlust/Fund/Diebstahl von Material und/oder Information
- Angriff auf Informationen
- Ausspähversuch von Personen, Material und/oder Informationen
- Unautorisierter Zutritt zu Gebäuden
- Unbefugter Zugang zu Systemen oder Zugriff auf Daten
- Auslösen der Einbruchmeldeanlage
- Beschädigung der Tarnung eines Prototyps
- Social Engineering
- …

e.solutions

Fragen und Kontakt

Frage bitte per E-Mail an:

eso.Group.Informationssicherheit@esolutions.de

Melden von Informationssicherheitsvorfällen per E-Mail an:

eso.Group.CERT@esolutions.de