Seite 5.3 Informationstechnische Schutzziele bei der Kommunikation

Prüfungsziel

Du sollst erklären können, welche informationstechnischen Schutzziele bei digitaler Kommunikation wichtig sind und wie man sie im privaten und betrieblichen Bereich beachtet.

Für die Prüfung sind hier vor allem wichtig:

- informationstechnische Schutzziele bei der Kommunikation
- Sicherheitsbewusstsein bei der Nutzung von IT-Technik
- IT-Sicherheit im privaten und betrieblichen Bereich
- Erfahrungen in virtuellen Räumen reflektieren
- Gefahren bei Social Media kennen
- Zuständigkeitsabgrenzung bei Kommunikation und Information
- sicherer Umgang mit dienstlichen E-Mails
- kurzer, zielführender, höflicher und korrekter Informationsaustausch
- Netiquette
- Nachrichten aus Sicht der Empfänger betrachten
- sensibler Umgang mit Adressatenlisten
- mögliche juristische Konsequenzen von Äußerungen über den Arbeitgeber
- Social Engineering erkennen und Schäden vermeiden

Was sind informationstechnische Schutzziele?

Informationstechnische Schutzziele beschreiben, was bei Informationen und IT-Systemen geschützt werden soll.

Die wichtigsten Schutzziele sind:

Schutzziel	Bedeutung
Vertraulichkeit	Informationen dürfen nur berechtigte Personen sehen
Integrität	Informationen dürfen nicht unbemerkt verändert werden
Verfügbarkeit	Informationen und Systeme müssen bei Bedarf nutzbar sein
Authentizität	Absender, Nutzer oder Systeme müssen echt und überprüfbar sein
Nachvollziehbarkeit	Vorgänge sollen später nachvollzogen werden können

---

Vertraulichkeit

Vertraulichkeit bedeutet, dass Informationen nur für berechtigte Personen zugänglich sind.

Beispiele:

- Kundendaten nicht an falsche Empfänger senden
- Passwörter nicht per Klartext verschicken
- interne Dokumente nicht öffentlich teilen
- E-Mails nur an berechtigte Personen senden
- Screenshots vor Weitergabe prüfen
- Cloud-Freigaben begrenzen

Beispiel aus der IT:

Ein Screenshot aus einem Ticketsystem enthält Kundendaten.

Vor dem Versenden müssen sensible Daten geschwärzt oder entfernt werden.

Integrität

Integrität bedeutet, dass Informationen vollständig und unverändert bleiben.

Beispiele:

- Dokumente dürfen nicht unbemerkt verändert werden
- Konfigurationsdateien müssen korrekt bleiben
- Logdateien dürfen nicht manipuliert werden
- Anhänge dürfen nicht durch Schadsoftware verändert werden
- Arbeitsanweisungen müssen aktuell und richtig sein

Beispiel aus der IT:

Eine Konfigurationsdatei wird per E-Mail verschickt.

Wenn sie unterwegs verändert wird, kann ein System falsch eingerichtet werden.

Verfügbarkeit

Verfügbarkeit bedeutet, dass Informationen, Systeme und Kommunikationsmittel bei Bedarf nutzbar sind.

Beispiele:

- E-Mail-System funktioniert
- Ticketsystem ist erreichbar
- VPN-Zugang steht bereit
- interne Wiki-Seiten sind verfügbar

- Telefonie und Chat funktionieren
- wichtige Dokumente sind nicht nur lokal auf einem Gerät gespeichert

Beispiel aus der IT:

Wenn das Ticketsystem ausfällt, können Störungen schlechter bearbeitet werden.

Deshalb sind Backups, Monitoring und Notfallpläne wichtig.

Authentizität

Authentizität bedeutet, dass eine Person, Nachricht oder ein System echt ist.

Beispiele:

- Absender einer E-Mail prüfen
- verdächtige Links nicht anklicken
- Identität am Telefon prüfen
- digitale Signaturen nutzen
- Zertifikate prüfen
- keine Zugangsdaten an unbekannte Personen herausgeben

Beispiel:

Eine E-Mail sieht aus, als käme sie vom Geschäftsführer und fordert eine schnelle Überweisung.

Vor dem Handeln muss geprüft werden, ob die Nachricht wirklich echt ist.

Nachvollziehbarkeit

Nachvollziehbarkeit bedeutet, dass Handlungen später geprüft oder verstanden werden können.

Beispiele:

- Tickets sauber dokumentieren
- Änderungen an Systemen protokollieren
- Entscheidungen schriftlich festhalten
- E-Mail-Verläufe geordnet ablegen
- Berechtigungsänderungen dokumentieren
- wichtige Anweisungen nicht nur mündlich geben

Beispiel aus dem Support:

Wenn ein Ticket ohne Dokumentation geschlossen wird, kann später niemand nachvollziehen, was gemacht wurde.

Sicherheitsbewusstsein bei IT-Nutzung

Sicherheitsbewusstsein bedeutet, mögliche Gefahren zu erkennen und vorsichtig mit IT-Systemen und Informationen umzugehen.

Einfach gesagt:

Man denkt mit, bevor man klickt, sendet, speichert oder teilt.

Wichtig im Betrieb:

- keine unbekannten Anhänge öffnen
- Links prüfen
- starke Passwörter nutzen
- MFA verwenden, wenn vorgesehen
- Geräte sperren, wenn man den Arbeitsplatz verlässt
- keine vertraulichen Daten offen liegen lassen
- verdächtige Vorfälle melden
- private und dienstliche Nutzung trennen
- Sicherheitsrichtlinien beachten

IT-Sicherheit im privaten und betrieblichen Bereich

IT-Sicherheit betrifft nicht nur den Arbeitsplatz.

Auch privates Verhalten kann den Betrieb beeinflussen.

Beispiele:

- dienstliche E-Mails auf privaten Geräten
- private Cloudspeicher für Firmendaten
- schwache Passwörter
- gleiche Passwörter privat und dienstlich
- Social-Media-Beiträge über den Arbeitgeber
- Phishing über private Messenger
- unsichere WLAN-Netze

Wichtig:

Dienstliche Daten gehören nicht unkontrolliert in private Systeme.

Virtuelle Räume

Virtuelle Räume sind digitale Umgebungen, in denen Menschen zusammenarbeiten oder kommunizieren.

Beispiele:

- Videokonferenz
- Chat
- Online-Meeting
- Cloud-Dokument
- Ticketsystem
- Lernplattform
- Social-Media-Gruppe
- Forum
- Online-Projektboard

Erfahrungen in virtuellen Räumen reflektieren

Reflektieren bedeutet, das eigene Verhalten zu überdenken.

Fragen zur Reflexion:

- War meine Nachricht klar?
- War der Ton angemessen?
- Habe ich die richtigen Empfänger gewählt?
- Habe ich vertrauliche Inhalte geschützt?
- Habe ich andere ausreden lassen?
- Habe ich unnötige Informationen geteilt?
- Habe ich Missverständnisse verursacht?
- War der Kommunikationskanal passend?

Social Media und IT-Sicherheit

Social Media kann private und betriebliche Risiken verursachen.

Risiken:

- Informationen über Arbeitgeber werden öffentlich
- Angreifer sammeln Informationen über Mitarbeiter
- Phishing über soziale Netzwerke
- gefälschte Profile
- Rufschädigung
- Preisgabe interner Projekte
- Veröffentlichung vertraulicher Informationen
- unbedachte Kommentare
- Verletzung von Persönlichkeitsrechten

Beispiel: Social-Media-Risiko

Ein Mitarbeiter postet:

„Heute wieder Chaos im Serverraum. Kunde XY ist seit Stunden offline.“

Problem:

- Kundenname wird öffentlich
- interner Vorfall wird bekannt
- Imageschaden möglich
- Vertraulichkeit verletzt
- arbeitsrechtliche Folgen möglich

Zuständigkeitsabgrenzung bei Kommunikation und Information

Zuständigkeitsabgrenzung bedeutet, dass klar ist, wer welche Informationen geben darf und wer wofür verantwortlich ist.

Warum ist das wichtig?

Nicht jeder darf jede Auskunft geben.

Beispiele:

Situation	Zuständig
Presseanfrage	Geschäftsführung oder Pressestelle
Datenschutzvorfall	Datenschutzbeauftragter / zuständige Stelle
IT-Sicherheitsvorfall	IT-Sicherheitsverantwortliche
Kundenbeschwerde	zuständiger Kundenbetreuer
Vertragsfrage	Vertrieb oder Rechtsabteilung
Personalfrage	Personalabteilung
technische Störung	IT-Support oder Fachteam

Beispiel für falsche Zuständigkeitsabgrenzung

Ein Azubi antwortet einem Kunden eigenständig auf eine rechtliche Frage zum Datenschutz.

Problem:

Der Azubi ist dafür wahrscheinlich nicht zuständig.

Richtiges Verhalten:

- Anfrage aufnehmen

- keine verbindliche Aussage machen
- an zuständige Stelle weiterleiten
- Rückmeldung dokumentieren

Sicherer Umgang mit dienstlichen E-Mails

Dienstliche E-Mails müssen sorgfältig, höflich und sicher geschrieben werden.

Wichtige Regeln:

- klare Betreffzeile
- höfliche Anrede
- kurze und verständliche Formulierung
- sachlicher Ton
- richtige Empfänger auswählen
- CC und BCC bewusst nutzen
- Anhänge prüfen
- vertrauliche Inhalte schützen
- keine Passwörter im Klartext senden
- vor dem Senden nochmal prüfen
- keine unbestätigten Informationen verbreiten

Kurzer, zielführender, höflicher und korrekter Informationsaustausch

Eine gute dienstliche E-Mail ist:

Eigenschaft	Bedeutung
kurz	keine unnötigen Informationen
zielführend	Empfänger erkennt, was zu tun ist
höflich	respektvoller Ton
korrekt	sachlich richtig und sprachlich angemessen
vollständig	wichtige Informationen fehlen nicht
sicher	keine unnötigen vertraulichen Daten

Beispiel für schlechte E-Mail

```
Betreff: Problem

Hi,
geht nicht. Bitte schnell machen.
```

Gruß

Problem:

- unklarer Betreff
- keine genaue Fehlerbeschreibung
- kein System genannt
- keine Dringlichkeit begründet
- nicht zielführend

Beispiel für bessere E-Mail

Betreff: VPN-Zugang für Benutzer Müller funktioniert seit 09:30 Uhr nicht

Hallo Support-Team,

der Benutzer Max Müller kann sich seit ca. 09:30 Uhr nicht mehr per VPN verbinden.
Fehlermeldung: „Authentifizierung fehlgeschlagen“.
Ein Neustart des Clients wurde bereits versucht.

Bitte prüft den Zugang.

Viele Grüße

Warum besser?

- klarer Betreff
- konkrete Beschreibung
- Zeitpunkt genannt
- Fehlermeldung genannt
- bisherige Schritte genannt
- höflich und sachlich

Netiquette

Netiquette bedeutet höfliche und angemessene Umgangsformen in digitaler Kommunikation.

Wichtige Netiquette-Regeln:

- höflich bleiben
- sachlich schreiben
- keine Beleidigungen
- keine komplett großgeschriebenen Nachrichten
- Ironie vorsichtig einsetzen

- andere ausreden lassen
- keine unnötigen Nachrichtenfluten
- passende Kanäle nutzen
- keine vertraulichen Inhalte in öffentliche Kanäle
- vor dem Senden nachdenken

Nachrichten aus Sicht der Empfänger betrachten

Bevor eine Nachricht gesendet wird, sollte man überlegen, wie sie beim Empfänger ankommt.

Fragen:

- Ist die Nachricht verständlich?
- Ist der Ton respektvoll?
- Weiß der Empfänger, was zu tun ist?
- Fehlen wichtige Informationen?
- Sind zu viele Informationen enthalten?
- Könnte die Nachricht falsch verstanden werden?
- Darf der Empfänger diese Informationen sehen?

Sensibler Umgang mit Adressatenlisten

Adressatenlisten müssen sorgfältig verwendet werden.

Begriffe:

Feld	Bedeutung
An	direkte Empfänger
CC	Personen erhalten die Nachricht zur Kenntnis
BCC	Empfänger sind für andere nicht sichtbar

Risiken bei Adressatenlisten

Fehler	Risiko
falscher Empfänger	vertrauliche Informationen gelangen an falsche Person
zu viele Personen in CC	unnötige Informationsweitergabe
offene Verteilerliste	E-Mail-Adressen werden sichtbar
kein BCC bei großen Gruppen	Datenschutzproblem möglich
„Allen antworten“ unüberlegt	Informationen werden unnötig verbreitet

---

Beispiel: Adressatenfehler

Eine E-Mail mit Kundendaten wird versehentlich an einen externen Empfänger mit ähnlichem Namen gesendet.

Mögliche Folgen:

- Datenschutzvorfall
- Meldepflicht möglich
- Vertrauensverlust
- interne Nacharbeit
- Schulungsbedarf

Richtiges Verhalten:

- Empfänger vor dem Senden prüfen
- Autovervollständigung kontrollieren
- bei sensiblen Daten besondere Vorsicht
- Fehler sofort melden

Äußerungen über den Arbeitgeber in sozialen Netzwerken

Äußerungen über den Arbeitgeber können Konsequenzen haben.

Problematisch sind zum Beispiel:

- Beleidigungen
- Veröffentlichung interner Informationen
- Kundendaten
- Geschäftsgeheimnisse
- Fotos aus gesicherten Bereichen
- falsche Behauptungen
- Rufschädigung
- vertrauliche Projektinformationen

Wichtig:

Auch private Beiträge können arbeitsrechtliche oder juristische Folgen haben, wenn sie den Arbeitgeber, Kunden oder Kollegen betreffen.

Beispiel für problematischen Beitrag

```
Unser Chef hat keine Ahnung. Außerdem ist Kunde XY wegen unserer schlechten IT gerade komplett lahmgelegt.
```

Problem:

- beleidigende Aussage
- Kundendaten oder Kundenbezug
- interne Störung öffentlich gemacht
- Rufschädigung
- mögliche arbeitsrechtliche Folgen

Social Engineering

Social Engineering bedeutet, dass Angreifer Menschen manipulieren, um an Informationen, Zugänge oder Handlungen zu kommen.

Einfach gesagt:

Nicht die Technik wird zuerst angegriffen, sondern der Mensch.

Typische Social-Engineering-Methoden

Methode	Erklärung
Phishing	gefälschte E-Mail oder Website
Spear-Phishing	gezieltes Phishing gegen bestimmte Personen
Vishing	Betrug per Telefon
Smishing	Betrug per SMS oder Messenger
Pretexting	Angreifer gibt falsche Identität oder Geschichte vor
Tailgating	Angreifer folgt unberechtigt durch eine Tür
CEO-Fraud	angebliche Anweisung der Geschäftsführung
USB-Drop	präparierter USB-Stick wird absichtlich platziert

Beispiel: Social Engineering per Telefon

Eine Person ruft im Unternehmen an und sagt:

„Ich bin vom IT-Support. Wir müssen Ihr Konto prüfen. Bitte nennen Sie mir Ihr Passwort.“

Richtiges Verhalten:

- Passwort niemals nennen
- Identität prüfen
- Gespräch beenden, wenn verdächtig
- Vorfall melden

- zuständige IT-Sicherheitsstelle informieren

Warnzeichen für Social Engineering

- ungewöhnlicher Zeitdruck
- Drohungen oder Druck
- Bitte um Passwort oder Zugangscode
- ungewöhnliche Zahlungsaufforderung
- unbekannter Absender
- gefälschte E-Mail-Adresse
- unerwarteter Anhang
- verdächtiger Link
- Bitte um Umgehung von Regeln
- Geheimhaltung wird verlangt

Schäden durch Social Engineering vermeiden

Wichtige Maßnahmen:

- Sicherheitsbewusstsein entwickeln
- Passwörter nie weitergeben
- Identität von Anfragenden prüfen
- verdächtige E-Mails melden
- Links prüfen
- Anhänge nur bei vertrauenswürdiger Quelle öffnen
- keine fremden USB-Sticks verwenden
- Besucherregeln beachten
- keine Türen für Unberechtigte öffnen
- klare Meldewege nutzen
- Schulungen ernst nehmen

Bezug zur Prüfung

In der Prüfung können Situationen beschrieben werden, bei denen du entscheiden sollst, welches Verhalten sicher und korrekt ist.

Typische Aufgaben:

- Schutzziele zuordnen
- Vertraulichkeit bei E-Mails erkennen
- Fehler bei Adressatenlisten bewerten
- Social Engineering erkennen
- sichere E-Mail-Kommunikation auswählen
- Netiquette-Regeln anwenden

- Social-Media-Äußerungen beurteilen
- Zuständigkeiten richtig einordnen

Typische Prüfungsfrage 1

Nenne drei informationstechnische Schutzziele.

Antwort anzeigen

Drei wichtige Schutzziele sind Vertraulichkeit, Integrität und Verfügbarkeit.

Typische Prüfungsfrage 2

Was bedeutet Vertraulichkeit?

Antwort anzeigen

Vertraulichkeit bedeutet, dass Informationen nur für berechtigte Personen zugänglich sind.

Typische Prüfungsfrage 3

Was bedeutet Integrität?

Antwort anzeigen

Integrität bedeutet, dass Informationen vollständig und unverändert bleiben und nicht unbemerkt manipuliert werden.

Typische Prüfungsfrage 4

Was bedeutet Verfügbarkeit?

Antwort anzeigen

Verfügbarkeit bedeutet, dass Informationen, Systeme und Dienste bei Bedarf nutzbar sind.

Typische Prüfungsfrage 5

Warum ist Authentizität bei Kommunikation wichtig?

Antwort anzeigen

Weil geprüft werden muss, ob Absender, Nachricht oder System echt sind. Dadurch können gefälschte Nachrichten und Betrugsversuche erkannt werden.

Typische Prüfungsfrage 6

Was bedeutet Netiquette?

Antwort anzeigen

Netiquette bedeutet höfliche und angemessene Umgangsformen in digitaler Kommunikation.

Typische Prüfungsfrage 7

Warum muss man Adressatenlisten sorgfältig prüfen?

Antwort anzeigen

Weil vertrauliche oder personenbezogene Informationen sonst an falsche oder zu viele Personen gelangen können.

Typische Prüfungsfrage 8

Warum können Äußerungen über den Arbeitgeber in sozialen Netzwerken problematisch sein?

Antwort anzeigen

Weil sie interne Informationen, Kundendaten, Geschäftsgeheimnisse oder beleidigende Aussagen enthalten können. Das kann arbeitsrechtliche oder juristische Folgen haben.

Typische Prüfungsfrage 9

Was ist Social Engineering?

Antwort anzeigen

Social Engineering ist eine Angriffsmethode, bei der Menschen manipuliert werden, um Informationen, Zugangsdaten oder bestimmte Handlungen zu erhalten.

Typische Prüfungsfrage 10

Nenne drei Warnzeichen für Social Engineering.

Antwort anzeigen

Warnzeichen sind zum Beispiel ungewöhnlicher Zeitdruck, Bitte um Passwörter, verdächtige Links, unbekannte Absender, Drohungen oder die Aufforderung, Regeln zu umgehen.

Merksatz

- Vertraulichkeit = nur Berechtigte dürfen Informationen sehen
- Integrität = Informationen bleiben korrekt und unverändert
- Verfügbarkeit = Systeme und Informationen sind nutzbar
- Authentizität = Echtheit von Absendern, Nutzern und Systemen
- Netiquette = höfliche digitale Umgangsformen
- E-Mails müssen kurz, zielführend, höflich, korrekt und sicher sein
- Adressatenlisten immer sorgfältig prüfen
- Social Media kann arbeitsrechtliche und juristische Folgen haben
- Social Engineering greift den Menschen an, nicht nur die Technik
- Passwörter niemals weitergeben

Revision #1
Created 26 May 2026 13:05:26 by Admin
Updated 26 May 2026 13:47:57 by Admin