IT Grundschutz modellieren | SECU

IT-Sicherheit

SECU

Grundwerte der IT-Sicherheit

- Confidentiality, Vertraulichkeit
- Integrity, Integrität
- Availability, Verfügbarkeit
- Authenticity, Authentizität
- Non-Repudiation, Nicht-Abstreitbarkeit, Verbindlichkeit

Ziele der IT-Sicherheit

Bereitstellung geeigneter und (gemäss IT-Leitlinie des Unternehmens) ausreichender Massnahmen zum Schutz von Informationen, ihrer Verarbeitung und aller Komponenten informationsverarbeitender Systeme.

Vertraulichkeit

Schutz von sensitiven Informationen (= Daten in einem Kontext) vor unberechtigtem Zugriff.

- Datenvertraulichkeit: persönliche Daten, geschäftskritische Daten
- Teilnehmer-Anonymität bei bestimmten Geschäftstransaktionen
- Anonymität von Nutz- und Vermittlungsdaten

Integrität

Schutz des Systems oder der Daten vor unautorisierter Änderung oder Zerstörung.

- Richtigkeit
- Vollständigkeit
- Konsistenz
- Aktualität
- Authentizität (richtige Zuordnung)

Verfügbarkeit

Schutz der Funktionalität von Software und Hardware. Informationen müssen bereitstehen, wenn sie durch den Geschäftsprozess benötigt werden.

- zu bestimmten Zeitpunkten
- an bestimmten Orten
- in bestimmter Qualität

Authentizität

Herkunftsgarantie, Sicherstellung der Identität eines Subjekts. Voraussetzung für Integrität und Verbindlichkeit.

Verbindlichkeit

Eindeutige Zuordnung von Aktionen einer Instanz zu genau dieser Instanz. Der Sender erhält eine Empfangsbestätigung und der Empfänger einen Authentizitätsnachweis.

- Nachweisbarkeit der Urheberschaft (Authentizität)
- Nachweisbarkeit von Kommunikationsvorgängen
- Rechtssicherheit der Kommunikation

Sicherheitskonzept

Plan	Systemabgrenzung
Plan	Bestandesaufnahme: Inventar, Ist-Zustand
Plan	Gefährdungsanalyse / Risikoanalyse
Plan	Schutzbedarf
Plan	Massnahmen
Do	Umsetzung
Check	Audit: Prüfung der Massnahmen
Act	Optimierung (iterativ)

Standards

Überblick

Organisations-bezogen		IT-GSHB	ISO 9000 ISO 13335 CobiT
IT-System-bezogen			ISO 17799
Produkt-bezogen	ITSEC/CC		
	Technisch orientiert		Management orientiert

ISO 9000

Modell, Leitlinien und Zertifizierung des Qualitätsmanagements

Zielgruppe:
Organisationen jeglichen Typs und beliebiger Grösse

www.iso.org

ISO TR 13335

Technical Report
Richtlinie zum Management von Informationssicherheit
Gute Anleitung für die Definition von Sicherheitsprozessen

Vierteiliges Werk:
- Konzepte und Modelle der IT-Sicherheit
- Managen und Planen von IT-Sicherheit
- Techniken für das Management von IT-Sicherheit
- Auswahl von Sicherheitsmassnahmen

Zielgruppe: Management
Nicht zertifizierbar

ISO/IEC 15408 / ITSEC / Common Criteria

International anerkannter Standard zur Zertifizierung von Hard- und Software-Produkten

Ziel ist der Nachweis, dass die Sicherheitsanforderungen eines IT-Produktes oder -Systems vollständig und korrekt realisiert worden sind. Ausserdem Nachweis, dass die Sicherheitsfunktionen nicht durch Schwachstellen umgehbar sind. Die CC unterscheiden 7 Prüfstufen (EAL-Stufen 1 – 7).

Zielgruppe:
Hersteller von IT-Systemen, IT-Produkten, IT-Komponenten

www.commoncriteria.org

ISO 17799

- “Code of Practice” zum IT Security Management, entstanden aus dem Britischen Standard BS 7799-1
- International anerkannter Leitfaden
- Sammlung von Empfehlungen für Informationssicherheitsverfahren und -methoden, die sich in der Praxis bewährt haben („best practices“)
- generische Standard-Sicherheitsmaßnahmen
- empfiehlt keine konkreten Sicherheitslösungen

Zertifizierung nicht möglich, aber
- auf dem BSI-Zertifikat für IT-Grundschutz mit bestätigt
- Möglichkeit der formalen Zertifizierung nach BS7799-2 www.bsi-global.com

Cobit

Control Objectives for Information and related Technology

Methode zur Kontrolle von Risiken, die sich durch den IT-Einsatz zur Unterstützung geschäftsrelevanter Abläufe ergeben.

Modell von generell anwendbaren und international akzeptierten Kontrollzielen, die in einem Unternehmen implementiert werden sollten, um eine verlässliche Anwendung der IT zu gewährleisten.

Nicht zertifizierbar
www.isaca org / www.isaca.ch

ITIL

IT Infrastructure Library
Öffentlich zugängliche Sammlung mehrerer Bücher zum Thema IT-Service-Management

Beschreibt ein systematisches Vorgehen, Prozesse und Rollen für das Management von IT-Dienstleistungen.

Ziel: Optimierung bzw. Verbesserung der Qualität von IT-Services und der Kosteneffizienz.

Nicht zertifizierbar
www.itil.org

ISO 17799

SECU

Zweck

Verständnis von IT-Sicherheit als Management-Aufgabe und Verankerung im Unternehmen durch:

- Definition und Implementierung eines Informationssicherheits-Managementsystems (ISMS)
- Entwicklung organisationsbezogener Normen und Praktiken zur Informationssicherheit
- Überwachung der Einhaltung rechtlicher Verpflichtungen betreffend Informationssicherheit

Zielgruppe

Unternehmen und Behörden

Kritische Erfolgsfaktoren

- an den Geschäftszielen ausgerichtete Sicherheitspolitik
- der Unternehmenskultur angepasste Implementierung der Informationssicherheit
- Unterstützung durch das (Top-)Management
- Trainings und Schulungen
- System zur Bemessung und Verbesserung der Informationssicherheit

Managementgebiete

- Sicherheitspolitik
- Organisation der Sicherheit
- Einstufung und Kontrolle der Werte
- Personelle Sicherheit
- Physische und umgebungsbezogene Sicherheit
- Management der Kommunikation und des Betriebs
- Zugangskontrolle
- Systementwicklung und -wartung
- Management des kontinuierlichen Geschäftsbetriebs
- Einhaltung der Verpflichtungen

CobiT	SECU
Zweck CobiT ist ein Referenzmodell für IT-Governance, welches eine Menge von Kontrollzielen für Informatikprozesse definiert. In seiner aktuellen dritten Version identifiziert das Modell 34 IT-Prozesse, welche anhand von 318 Kontroll- und Überwachungsrichtlinien bewertet werden. Über Critical Success Factors, Key Performance Indicators und andere Kennzahlen wird dem Bedarf des Managements nach Kontrolle und Messbarkeit der IT Rechnung getragen. Hierdurch kann die IT-Umgebung den von CobiT identifizierten IT-Prozessen gegenübergestellt und beurteilt werden.	**Zielgruppe** Management, Nutzer, Prüfer, Prozess- oder IT-Verantwortliche Die Kriterien werden von vielen Wirtschaftsprüfern im Rahmen der Jahresabschlussprüfung zur Prüfung der IT und ihres Umfeldes eingesetzt.
Kriterien Qualiät: • Effektivität • Effizienz Sicherheit: • Vertraulichkeit • Integrität • Verfügbarkeit Ordnungsmäßigkeit: • Zuverlässigkeit • Verbindlichkeit	
Life Cycle • Planung und Organisation • Beschaffung und Implementierung • Betrieb und Unterstützung • Überwachung aufgeteilt in 34 kritische IT-Prozesse mit ca. 300 Kernaufgaben	

IT-Grundschutzhandbuch

SECU

Ziel

- vereinfachte Erstellung von IT-Sicherheitskonzepten
- zügige Lösung häufiger Sicherheitsprobleme
- Anhebung des Sicherheitsniveaus von IT-Systemen
- Nutzung für IT-Sicherheitsrevision

www.bsi.de

Aufbau

Baukastenprinzip:
modular, typische Bereiche des IT-Einsatzes als Bausteine

pro Baustein:
- typische Gefährdungen
- pauschalisierte Eintrittswahrscheinlichkeiten
- Standardsicherheitsmassnahmen

Vorteile GSHB-Methode

- einfach und schnell: nur Soll/Ist-Vergleich der umgesetzten Massnahmen statt traditioneller Risikoanalyse
- kompakt und übersichtlich durch Referenzierung
- praxiserprobt
- effektive Wartung durch gute Dokumentation
- erweiterbar, aktualisierbar
- Marketing-Vorteile: bekannter Standard, Zertifizierung

Nachteile GSHB-Methode

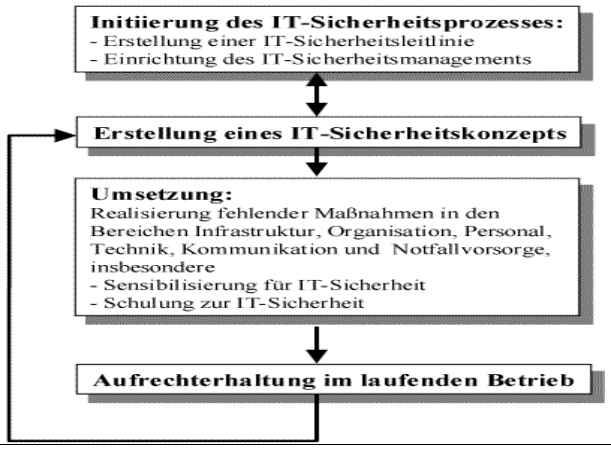
- nur komponentenorientiert, nicht prozessorientiert
- nur Baseline-Security, deckt nur ca. 80% des Schutzbedarfs ab

IT-Sicherheitsprozess

Planmässig anzuwendende Vorgehensweise, wie ein angemessenes IT-Sicherheitsniveau erreicht und aufrechterhalten werden kann.

- Enwicklung einer IT-Sicherheitspolitik
- Auswahl und Etablierung einer geeigneten Organisationsstruktur für das IT-Sicherheitsmanagement
- Erstellung eines IT-Sicherheitskonzepts
- Realisierung der IT-Sicherheitsmassnahmen
- Schulung und Sensibilisierung
- Aufrechterhaltung der IT-Sicherheit im laufenden Betrieb

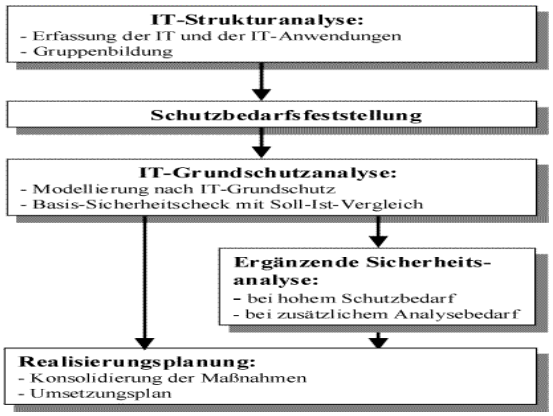
Grafik IT-Sicherheitsprozess



IT-Sicherheitskonzept

SECU

Grafik IT-Sicherheitskonzept



IT-Strukturanalyse

Analyse und Dokumentation der Struktur des vorliegenden IT-Verbundes.

- Netzplanerhebung
- Komplexitätsreduktion durch Gruppenbildung
- Erhebung der IT-Systeme (Hardware)
- Erfassung der IT-Anwendungen (Software) und der zugehörigen Informationen

Schutzbedarfsfeststellung

Ermittlung der Sicherheitsanforderungen pro Komponente in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit.

- Definition der Schutzbedarfskategorien
- Betrachtung von Schadensszenarien
- Schutzbedarfsfeststellung für IT-Anwendungen
- Schutzbedarfsfeststellung für IT-Systeme
- Schutzbedarfsfeststellung für Kommunikationsverbindungen
- Schutzbedarfsfeststellung für IT-Räume
- Interpretation der Ergebnisse:
  evtl. ergänzende Sicherheitsanalyse

Modellierung nach IT-Grundschutz

Nachbildung der betrachteten IT-Landschaft durch Bausteine des GSHB in Tabellenform (IT-Grundschutzmodell).

- Nr. und Titel des Bausteins (Gefahren und Massnahmen sind darin referenziert)
- Zielobjekt / Zielgruppe
- Ansprechpartner (Ermittlung im Basis-Sicherheitscheck)
- Hinweise

Funktion:
- Entwicklungsplan für geplanten IT-Verbund
- Prüfplan für realisierten IT-Verbund

Basis-Sicherheitscheck

Soll/Ist-Vergleich zwischen empfohlenen Standard-Sicherheitsmassnahmen und bereits realisierten Massnahmen, z.B. mit Interviews.

Tabelle pro Baustein:
- Formularkopf: Nr., Bezeichnung und Standort Zielobjekt
- Nr. und Titel der Massnahme (vorgegeben)
- Umsetzungsstatus:
  entbehrlich, ja, teilweise, nein
- Umsetzung bis (Ermittlung in Realisierungsplanung)
- verantwortlich (evtl. Ermittlung in Realisierungsplanung)
- Bemerkungen
- Kostenschätzung

Ergänzende Sicherheitsanalyse

- spezifische Risiken
- IT-Systeme mit höherem Schutzbedarf
- Kommunikationsverbindungen
  - nach aussen
  - mit hochschutzbedürftigen Daten
  - die bestimmte Daten nicht transportieren dürfen
- IT-Räume mit hohem Schutzbedarf

Methoden:
- Risikoanalyse
- Penetrationstest
- Differenz-Sicherheitsanalyse

Realisierung von IT-Sicherheitsmassnahmen

- Sichtung der Untersuchungsergebnisse:
  noch nicht umgesetzte Massnahmen mit Priorität
- Konsolidierung der Massnahmen:
  Umsetzbarkeit, Effektivität, Ersatz, Konkretisierung
- Kosten- und Aufwandschätzung:
  einmalige und wiederkehrende Investitionen
- Festlegung der Umsetzungsreihenfolge
- Festlegung der Verantwortlichkeit:
  Termin, Realisierungs- und Kontroll-Verantwortung
- Realisierungsbegleitende Massnahmen:
  Schulung, Sensibilisierung

IT-Grundschutz-Zertifikat

- Antragssteller:
  Dokumente gemäss IT-Sicherheitskonzept
- vom BSI lizenzierter Auditor:
  formale und inhaltliche Prüfung der Dokumente
  stichprobenartige Realisierungsprüfung
- unabhängige akkreditierte Zertifizierungsstelle:
  Prüfung Audit-Report
  Vergabe Zertifikat mit zwei Jahre Gültigkeit

Vorstufen:
Einstiegsstufe und Aufbaustufe (mit oder ohne Testat)
zwei Jahre gültig, nicht wiederholbar

IT-Strukturanalyse

SECU

Netzplan

Netztopologieplan: graphische Übersicht über die eingesetzten Komponenten und ihre Vernetzung.

- IT-Systeme (Server, Client, Netzkomponente, Drucker)
- LAN-Verbindungen (Ethernet, Token-Ring, Backbone)
- Kommunikationsverbindungen nach aussen

Gruppenbildung

Zusammenfassung gleichartiger Komponenten:

- vom gleichen Typ
- gleich oder nahezu gleich ins Netz eingebunden
- gleiche administrative und infrastrukturelle Rahmenbedingungen
- gleiche Anwendungen

IT-Systeme

Tabelle der vorhandenen und geplanten IT-Systeme, inkl. nicht vernetzte (nicht im Netzplan aufgeführte) IT-Systeme.

- eindeutige Bezeichnung (S=Server/C=Client/N= Netzkomponente/D=Drucker/T=TK-Anlage plus Nr.)
- Beschreibung (Typ und Funktion)
- Plattform
- Anzahl
- Standort
- Status (in Betrieb, im Test, in Planung)
- Benutzer / Administrator

IT-Anwendungen

Tabelle der wichtigsten (bezüglich Vertraulichkeit / Integrität / Verfügbarkeit) auf den betrachteten IT-Systemen laufenden und geplanten IT-Anwendungen.

- A=Anwendung plus Nr.
- Beschreibung (Anwendung / Informationen)
- personenbezogene Daten J/N
- Zuordnung zu betroffenen IT-Systemen (Verarbeitung, Transfer)

Schutzbedarfsfeststellung

SECU

Schutzbedarfskategorien

Da der Schutzbedarf meist nicht quantifizierbar ist, beschränkt sich das GSHB auf eine qualitative Unterteilung.

- niedrig bis mittel: begrenzt und überschaubar
- hoch: Schadensauswirkungen beträchtlich
- sehr hoch: existentiell bedrohlich

Schadensszenarien

In Interviews sind pro Szenario die maximalen Schäden aus dem Verlust von Vertraulichkeit / Integrität / Verfügbarkeit zu ermitteln.

- Verstoss gegen Gesetze / Vorschriften / Verträge
- Beeinträchtigung des informationellen Selbstbestimmungsrechts
- Beeinträchtigung der persönlichen Unversehrtheit
- Beeinträchtigung der Aufgabenerfüllung
- negative Aussenwirkung
- finanzielle Auswirkungen

IT-Anwendungen

Tabelle des Schutzbedarfs der IT-Anwendungen pro Grundwert (Vertraulichkeit / Integrität / Verfügbarkeit).

- A=Anwendung plus Nr.
- Beschreibung (Anwendung / Informationen)
- personenbezogene Daten J/N
- Grundwert
- Schutzbedarfskategorie
- Begründung

IT-Systeme

Tabelle des Schutzbedarfs der IT-Systeme pro Grundwert, Begründung evtl. mit Verweis auf die IT-Anwendungen.

Abhängigkeiten zu den IT-Anwendungen:

- Maximum-Prinzip:
  die schwerwiegendsten Schäden sind bestimmend
- Vererbungs-Prinzip:
  auf Ergebnis angewiesenes System erbt Schutzbedarf
- Kumulationseffekt:
  hoher Gesamtschaden durch mehrere kleine Schäden
- Verteilungseffekt:
  Clustering senkt den Schutzbedarf

Kommunikationsverbindungen

Tabelle der kritischen Kommunikationsverbindungen.

- V=Verbindung plus Nr.
- Verbindungsstrecke (Komponente A – Komponente B)
- Aussenverbindung J/N
- Übertragung hochschutzbedürftiger Informationen (pro Grundwert)
- keine Übertragung hochschutzbedürftiger Informationen

IT-Räume

Tabelle des Schutzbedarfs der IT-Räume pro Grundwert aufgrund der IT-Systeme.

- Raumbezeichnung
- Art
- Lokation
- IT-Systeme / Datenträger
- Schutzbedarfskategorien

Bausteine

SECU

Übergreifende Aspekte

- IT-Sicherheitsmanagement
- Organisation
- Personal
- Notfallkonzept
- Datensicherungskonzept
- Computervirenschutzkonzept
- Kryptokonzept
- Behandlung von Sicherheitsvorfällen
- Hard- und Softwaremanagement
- Standardsoftware

Infrastruktur

- Gebäude
- Verkabelung
- Büroraum
- Serverraum
- Datenträgerarchiv
- Raum für technische Infrastruktur
- Schutzschränke
- Häuslicher Arbeitsplatz
- Rechenzentrum

IT-Systeme

- Tragbarer PC
- PC mit wechselnden Benutzern
- Allgemeines nicht vernetztes IT-System
- Servergestütztes Netz
- Peer-to-Peer-Netz
- Novell Netware 3.x / 4.x
- TK-Anlage
- Faxgerät
- Anrufbeantworter
- Mobiltelefon

Netze

- Heterogene Netze
- Netz- und Systemmanagement
- Modem
- Firewall
- Remote Access
- LAN-Anbindung eines IT-Systems über ISDN

IT-Anwendungen

- Datenträgeraustausch
- E-Mail
- www-Server
- Lotus Notes
- Fax-Server
- Datenbanken

Gefährdungen und Massnahmen

SECU

Gefährdungen

- Höhere Gewalt
- Organisatorische Mängel (AKV)
- Menschliche Fehlhandlungen
- Technisches Versagen
- Vorsätzliche Handlungen

Massnahmen

- Infrastruktur
- Organisation
- Personal
- Hardware / Software
- Kommunikation
- Notfallvorsorge

Höhere Gewalt

- Naturkatastrophen:
  Erdbeben, Überschwemmung, Blitzschlag
- Feuer, Explosion
- Streik, Weggang von Schlüsselpersonen

Menschliche Fehlhandlungen

- Programmabsturz:
  Programmfehler, unsorgfältiges Testen
- Bedienungsfehler:
  ungenügende Plausi, mangelnde Benutzerausbildung
- fehlerhafte Produktion
- Verlust der Vertraulichkeit:
  herumliegende Daten

Technisches Versagen

- Stromausfall
- Defekt in Hardware, Klimaanlage
- Fehler in Betriebs-, Kommunikationssystem

Vorsätzliche Handlungen

- Manipulation an Geräten, Programmen, Daten
- Diebstahl von Geräten, Programmen, Daten
- Missbrauch vertraulicher Daten
- Einbringen bösartiger Software
- Hacking
- Industriespionage
- Vandalismus
- Sabotage

Massnahmen Infrastruktur

SECU

Elementarschäden

- Redundante Standorte
- Backup-Rechenzentrum
- Unterbrechungsfreie Stromversorgung USV
- Notstromaggregate
- Feuerschutzwände, Rauchmeldeanlage
- Brandlöschtechnik (z.B. Sauerstoff binden mit CO_2)
- Schutzbedürftige Räume im Gebäudezentrum
- selbsttätige Entwässerungsanlage

Technik-Ausfall

- Klimatisierung Serverraum
- System-Fernüberwachung

Kommunikationsverbindungen

- Kappung von Außenverbindungen
- gepanzerte Kabeltrassen
- drucküberwachte Kabel
- redundante Kommunikationsstrecken / Kabelführung

Unbefugter Zutritt

- Pförtnerloge
- Personen- und Fahrzeugidentifikation
- Vereinzelungsschleusen, Zutrittskontrollsystem
- Videoüberwachung
- Einbruchmeldeanlage
- Rolladensicherungen

Massnahmen Organisation

SECU

Verfügbarkeit

- regelmässige Überprüfung der Backup-Bänder
- Rücksicherung üben
- Lagerung ausserhalb Büroräume, Bankschliessfach
- Wartungsverträge
- gegenseitige Vereinbarung mit Partner-Unternehmen

Viren / Spam

- Update-Konzept Virenschutzsoftware
- Richtlinien für Internet-/E-Mail-Nutzung
- Mailadresse nicht weitergeben

Innentäter

- Geregelte Einarbeitung / Ausscheiden von Mitarbeitern
- Standardarbeitsplätze mit definierter Software
- Aufgeräumter Arbeitsplatz (clear desk)
- Datenträgerregelung (nicht unbeaufsichtigt lassen)
- Schlüsselregelung
- Regelung Passwortgebrauch
- Schulung zu Sicherheitsaspekten (Viren, Notfall, Social Engineering)
- Funktionstrennung, Vieraugen-Prinzip
- Verpflichtung zur Einhaltung von Regeln und Gesetzen

Unbefugter Zugriff

- Daten-Klassifizierung
- Einteilung in Benutzergruppen
- Vergabe und Überprüfung von Zugriffsrechten
- ID-Sperrung nach mehrfachem Authentisierungsfehler
- Freischaltungs-Ablauf bei gesperrter ID

Administrator-Ausfall

- Ernennung Administrator und Vertreter
- Regelung Verantwortlichkeiten
- Dokumentation System-Einstellungen und Änderungen
- Passwörter sicher hinterlegen
- Konfigurations-, Change- und Releasemanagement

Notfallkonzept

- Notfall-Definition mit Verhaltensregeln
- Notfall-Verantwortlicher
- Handbücher in Papierform
- Alarmierungsplan
- Eskalationsstrategie
- Ausweichmöglichkeiten
- Ersatzbeschaffungsplan
- Wiederanlaufplan

Notfallvorsorge

- Notfall-Übungen
- Versicherungen abschliessen
- Wartungsverträge abschliessen

Massnahmen Hardware/Software

SECU

Verfügbarkeit

- Backup, auch von Telearbeitsplätzen
- RAID: Redundant Array of Inexpensive Disks
- Clustered Server:
  logischer Zusammenschluss von Rechnern
  braucht Controller / Load Balancer
- Redundanter Server
- Standby-Reservesysteme
- Performance-Messung

Viren / Spam

- Virus-Warnfunktion im Bios (Bestätigung für Änderung im Bootsektor)
- restr. Browserkonfig. (aktive Inhalte, Plug-Ins, Cookies)
- Firewall mit Paketfilter, Black und White List
- Virenprüfung Download-Dateien / Mails (in und out)
- Webserver mit minimalem Betriebssystem
- Webserver-Konfiguration: Verzeichnisinhalt / symbolische Links deaktivieren
- Server-Administration über sichere Verbindung
- Spam-Filter auf Mail-Server / Firewall

Kommunikationsverbindungen

- Leitungs- oder Ende-zu-Ende-Verschlüsselung
- mehrstufige Firewalls
- Intrusion Detection System:
  Verhaltensmuster-Erkennung im internen Netz
- Intrusion Protection System:
  Reaktion auf veränderte Verhaltensmuster
- Tunneling: Protokoll im Protokoll, z.B. VPN (Virtual Private Network), Verschlüsselung ganzes Datenpaket durch Router, versteckt Absender / Empfänger
- NAT Network Address Translation: Umwandlung interner Adressen auf Routern und Firewalls in eine externe Adresse

Unbefugter Zugriff

- Passwortschutz (Boot-Passwort für Notebooks)
- Gesichertes Login mit Benutzer-ID für Applikationen
- Bildschirmsperre
- restriktive Konfiguration E-Mail-Programm
- E-Mail-Signatur
- Zugriffsschutz Mailbox (Ausnahme: Stellvertreter)
- Verschlüsselung
- Zugriffs-Protokollierung
- Closed User Group

Datenschutz

- Proxy-Server: www-Zugriffe aufräumen
- E-Mail-Protokollierung anonymisieren

Notfallvorsorge

- Regelmässige Sicherung von Daten und Konfiguration
- System-Monitoring
- Checkpoint / Restart-Fähigkeit
- automatischer Neustart
- Benutzerfehler abfangen