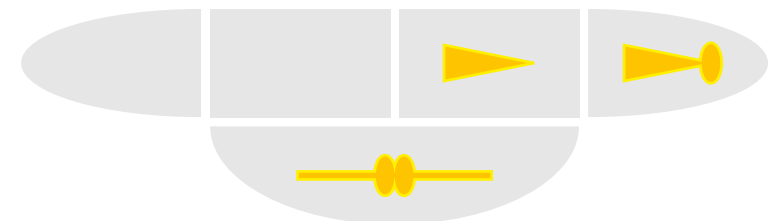

Notwendigkeit und Herangehensweise bei der Erstellung einer Sicherheitsanalyse, -konzeption und -richtlinie

eCOMM Veranstaltungsreihe 2005

Holger Kurrek
Fraunhofer-Institut für
Software- und Systemtechnik ISST

7. April 2005



Motivation

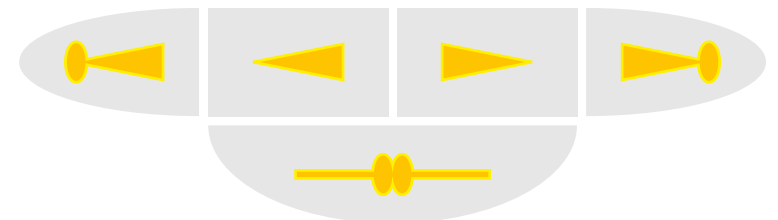
»Information ist heute das wichtigste Gut
in einem Unternehmen!«

Wettbewerbsfaktoren

Kundenvertrauen
Verfügbarkeit
Kosten

Folgerung

**IT-Sicherheit ist kein Selbstzweck, sondern ein entschei-
dender Wettbewerbsfaktor**



»Sicherheit kostet doch nur ...«

Ausreden

»Wir sind keine Bank!«
»Bei uns gibt es nichts zu holen!«
»Wir haben nichts zu verbergen!«

Fehlendes Problembewusstsein

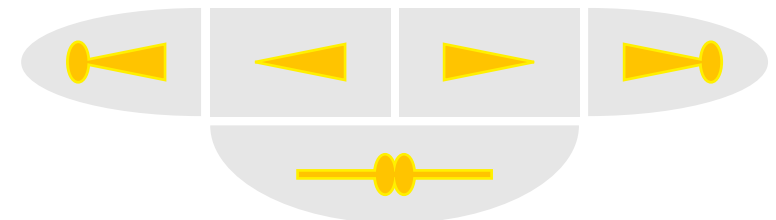
IT-Sicherheit ist ...

Kostenintensiv

Investitionen, Dokumentationen

Unbequem

Regelmäßiger Passwortwechsel, Prozessänderungen

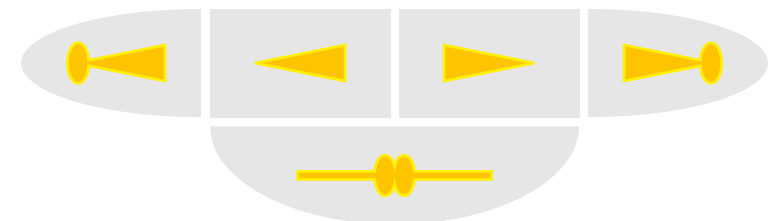


Bedrohungen

Gefahr durch Mißbrauch

- Austausch lizenzierter Inhalte
- Schädigung Dritter
- strafbare Inhalte
- Rufschaden
- Vertrauensverlust
- Gesetzesverstöße (Datenschutz)
- Schäden durch Ausfälle
- Kosten durch Personalbedarf

direkte und indirekte Schäden bzw. Kosten

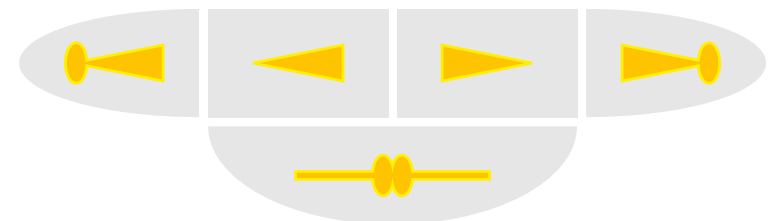


Was ist ein Rufschaden?

Mailinglisten-Server des BSI verschickte Wurm

»Durch eine Panne wurde über eine CERT-Mailingliste des Bundesamtes für Sicherheit in der Informationstechnik (BSI) am gestrigen Montagabend der Mass-Mailing-Wurm Sober.L verschickt. Nach Angaben von BSI-Sprecher Michael Dickopf gelangte der Wurm während Wartungsarbeiten ab 18:30 Uhr auf den Server.«

<http://www.heise.de/newsticker/meldung/57217>



Aktuelle Bedrohungen

Quelle: Symantec Internet Security Threat Report

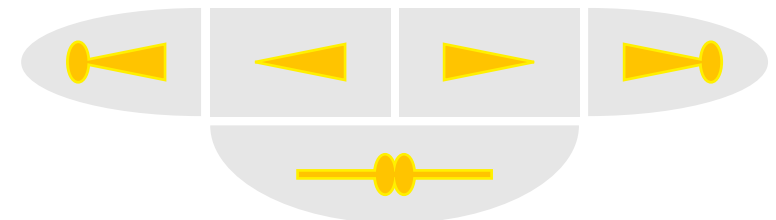
Angreifer verändern sich

Motivation

Stärkere Profitorientierung
Geld statt Ruhm

Know-how

Anstieg gezielter Angriffe
2003: 1% - 2004: >6%



IT-Sicherheit

IT-Sicherheit

ist Teil des Risiko-Managements des Unternehmens

Beispiel

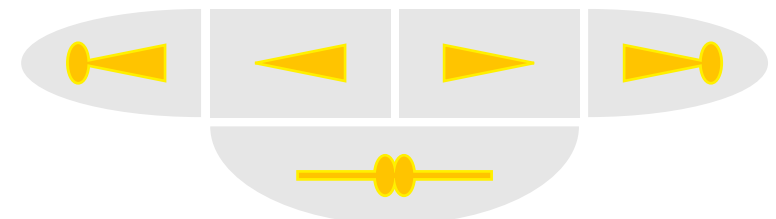
Gefährdung durch Viren, Würmer etc.
Ursache meist Fehlverhalten der Mitarbeiter
Technische Maßnahmen können allein nicht wirken
Mitarbeiter müssen motiviert werden

Organisatorische Probleme können nicht mit technischen Mitteln gelöst werden.

Management-Aufgabe

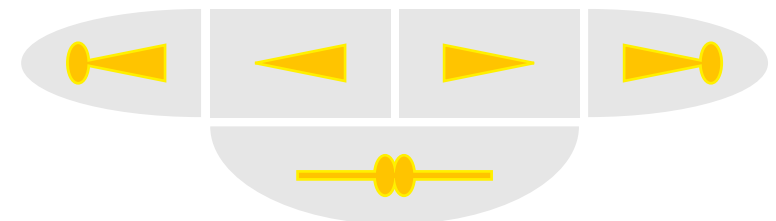
IT-Sicherheit benötigt

- Entscheidungsgewalt
- Durchsetzung und
- Budget



IT-Sicherheit - Definitionen

Sicherheit	bedeutet grundsätzlich das »Freisein von Gefahr«
Gegenstand	Informationen, IT-Systeme und Prozesse
Anforderungen	an Verfügbarkeit, Integrität und Vertraulichkeit (IT-Sicherheitsziele)
Sicheres Zusammenwirken	von Technik, Organisation und Menschen durch das IT-System in der konkreten Einsatzumgebung
Risiko-Begriff	quantitative oder qualitative Abschätzung möglicher Schäden und deren Eintrittswahrscheinlichkeit

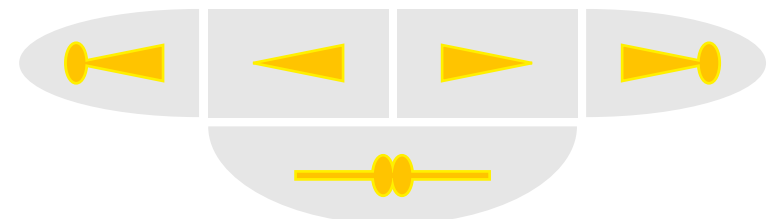


Sicherheit und Qualität

Sicherheit und Qualität haben **viel gemeinsam**:

- Qualitätsbeauftragter - Sicherheitsbeauftragter
- Qualitätsorganisation - Sicherheitsorganisation
- Qualitätspolitik - Sicherheitspolitik (policy)
- Beschreibung der Prozesse
- Verfahrensanweisungen
- Instruktionen, Checklisten
-
- Kosten, Budget

Viele Sicherheitsprobleme sind eigentlich Qualitätsprobleme, z. B. Bufferoverflow, falsche Konfigurationen etc.



IT-Sicherheit ist Risikomanagement

Hohe Abhängigkeit von IT
IT umfasst auch TK-Technik

Risiko vs. Kosten

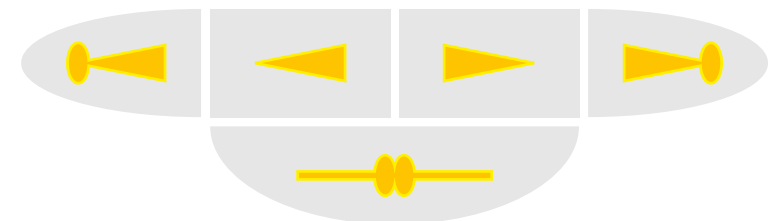
Risikoanalyse: Welche Risiken bin ich bereit zu tragen?

Es gibt keine 100-prozentige Sicherheit!

Absicherung auch durch Nicht-technische Massnahmen

- Verzicht auf Einsatz kritischer Dienste
- Anweisungen an Personal, Schulung
- Versicherung

Pflicht zum Risikomanagement z.B. durch Basel II



Kosten-Nutzen-Betrachtung bei IT-Sicherheit

Schadenskosten

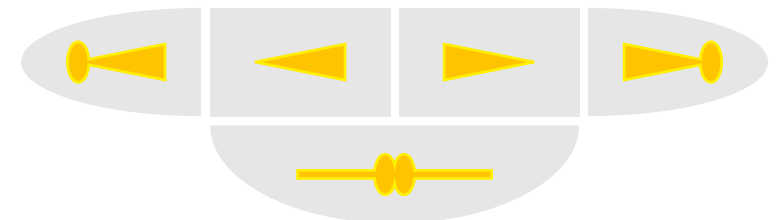
RoSI
Schäden vermeiden

Kostensituation

Basel II
Compliance
Versicherungen

Wettbewerbsfähigkeit

Wirtschaftliche Betriebsführung
Effizienz



ITIL

Fazit

ITIL beschreibt Prozesse

IT-Sicherheit ist ein Prozess

ITIL Security Management

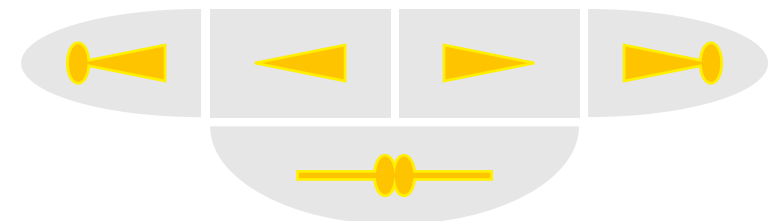
A5-Heft, Dicke 6 mm

ITIL Service Support, ITIL Service Delivery

2x A4-Buch, Dicke je 22 mm

Synergien

Dokumentationen



IT-Sicherheit kostet Geld, aber ...

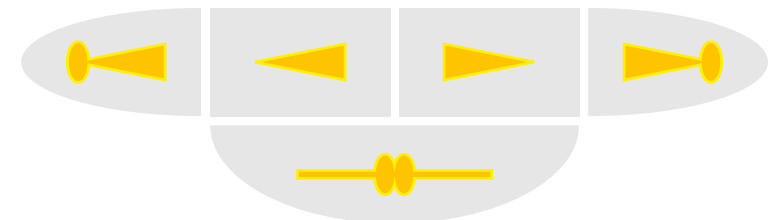
Rahmenbedingungen

- Zuständigkeiten, Verantwortlichkeiten
- Qualifikation der Administratoren
- Qualifikation der Anwender
- Überblick eingesetzter Hard- und Software - Inventory
- Netztopologie

Konzepte (nach BSI)

- Notfallvorsorge-Konzept
- Computer-Virenschutzkonzept
- Kryptokonzept
- Behandlung von Sicherheitsvorfällen
- Hard- und Software-Management
- Standardsoftware

... und deren Umsetzung!



... positive Nebenwirkungen - wirtschaftliche Vorteile

Aufwände für IT-Sicherheit verbessern
bei richtiger Umsetzung
auch Effektivität der IT

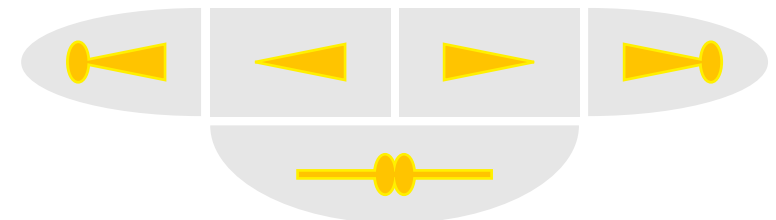
Beispiel

Verbesserung der Pflege der IT-Systeme durch

- Systematisches Vorgehen
- Verbesserte Dokumentation
- Vollständigkeit
- Vermeidung von Bedienfehlern (auch bei Admins)
- Werkzeug-Unterstützung z.B. für Software-Distribution, Backup usw.

Fazit

Ein effektiver IT-Betrieb (z.B. nach ITIL »IT Infrastructure Library«) verbessert auch die IT-Sicherheit!

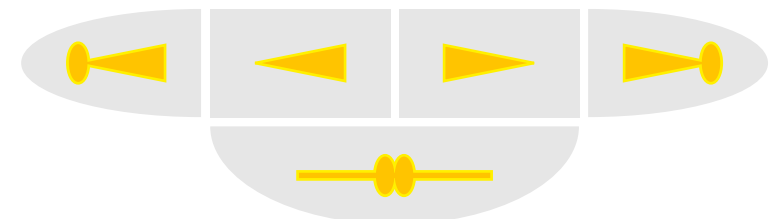


Umgang mit IT-Sicherheit

Agieren statt Reagieren
Schutzmaßnahmen gegen Bedrohungen
statt gegen Angriffe

Vorgehen

Initiierung durch Geschäftsleitung
IT-Sicherheits-Team bilden
Verantwortung klar herausarbeiten
Entscheidungs-/Weisungsbefugnisse klären
Alle Mitarbeiter einbeziehen
Budget bereitstellen



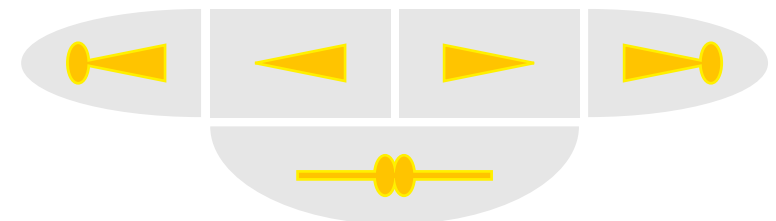
Sicherheitsziele

Beispiele

- Hohe Verfügbarkeit der DV-Systeme und Daten
- Schutz gegen Manipulation und Mißbrauch
- Erhaltung der Privatheit von Daten
- Durchsetzung der veröffentlichten Privacy-Policy
- Wahrung des guten Rufes
- Gewährleistung des Datenschutzes
- Einhaltung entsprechender gesetzlicher Vorgaben

Umsetzung

Prozeß



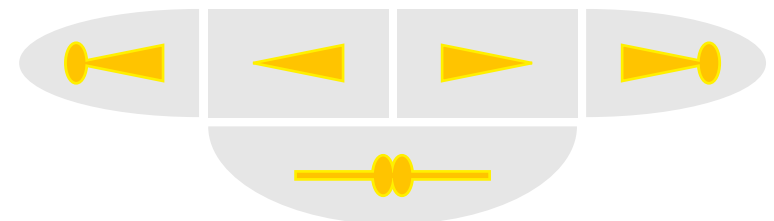
Vorgehen

- 1 Ist-Analyse: **Wo stehe ich?**
- 2 Gefährdungsanalyse:
Welche Risiken bin ich bereit zu tragen?
- 3 Umsetzung von Maßnahmen:
Was und wie muss ich dies tun?

Ganzheitliches Vorgehen ist erforderlich!

Grundlagen

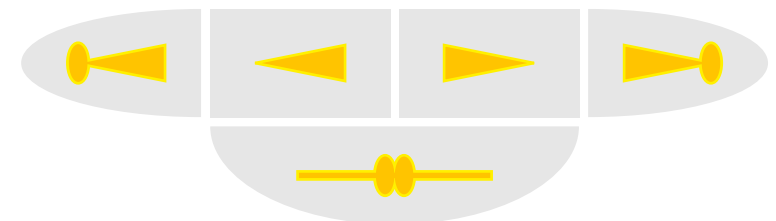
Bundesamt für Sicherheit in der Informationstechnik (BSI)
<http://www.bsi.de>
IT-Grundschutzhandbuch



Vorgehen nach BSI (1)

Schritte

- 1 Erstellung einer IT-Sicherheitsleitlinie
- 2 Auswahl und Etablierung einer geeigneten Organisationsstruktur für IT-Sicherheit
- 3 Erstellung einer Übersicht über vorhandene IT-Systeme
- 4 Festlegen der Vorgehensweise für die Erstellung des IT-Sicherheitskonzepts
- 5 Umsetzung der IT-Sicherheitsmaßnahmen
- 6 IT-Sicherheit im laufendem Betrieb
- 7 Aufrechterhalten des sicheren Betriebs



Vorgehen nach BSI (2)

M 2.191 Etablierung des IT-Sicherheitsprozesses

Verantwortlich für Initiierung:

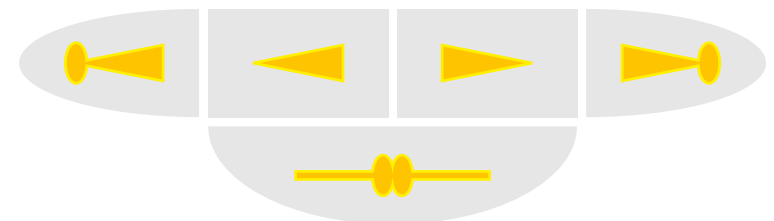
Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung:

Behörden-/Unternehmensleitung

- Die Initiative für IT-Sicherheit geht von der Behörden- bzw. Unternehmensleitung aus.
- Die Verantwortung für IT-Sicherheit verbleibt dort.
- Die Aufgabe "IT-Sicherheit" wird durch die Behörden- bzw. Unternehmensleitung aktiv unterstützt.

Einsetzung eines IT-Sicherheitsmanagement-Teams und/ oder die Benennung eines IT-Sicherheitsbeauftragten

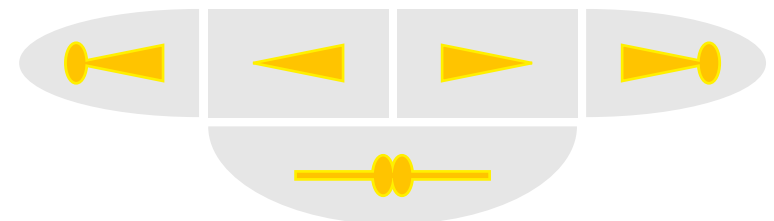


Vorgehen nach BSI (3)

Zitat

(aus dem IT-Grundschutzhandbuch des BSI):

»Der vielfach zu beobachtende sich selbst auf Arbeitsebene initiiierende IT-Sicherheitsprozess führt zwar zu einer Verbesserung der Sicherheitssituation, garantiert jedoch kein dauerhaftes Fortentwickeln des IT-Sicherheitsniveaus.«



Aufwand für IT-Sicherheit

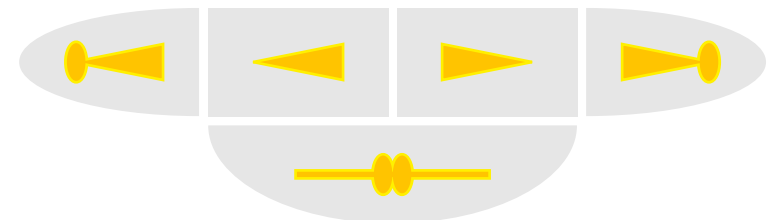
Rahmenbedingungen

- Zuständigkeiten, Verantwortlichkeiten
- Qualifikation der Administratoren
- Qualifikation der Anwender
- Überblick eingesetzter Hard- und Software - Inventory
- Netztopologie

Konzepte (nach BSI)

- Notfallvorsorge-Konzept
- Computer-Virenschutzkonzept
- Kryptokonzept
- Behandlung von Sicherheitsvorfällen
- Hard- und Software-Management
- Standardsoftware

... und deren Umsetzung!



Outsourcing von IT-Sicherheit

Analyse

Prüfung auf Schwachstellen

- Prüfung nach IT-Grundschutz

Konzeption

Erstellung der Konzepte und Dokumentation

- IT-Sicherheitshandbuch

Betrieb

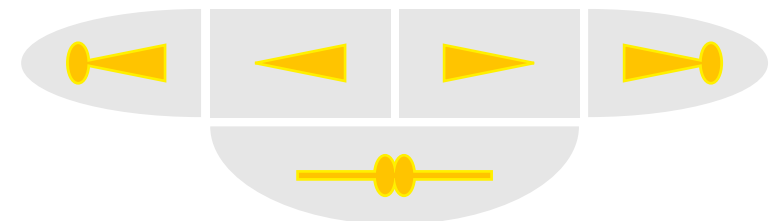
Pflege von Systemen und Konfigurationen

- Betriebskonzept

Qualitätssicherung

Sicherheits-Audits regelmäßig durchführen

- Regelmäßige Prüfung auf Schwachstellen



Gefährdungsanalyse

Prüfung

Systeme in zeitkritischen Geschäften
Komplette Kette aller notwendigen Ressourcen
Bsp.: Ziehungs-system bei Lotterie

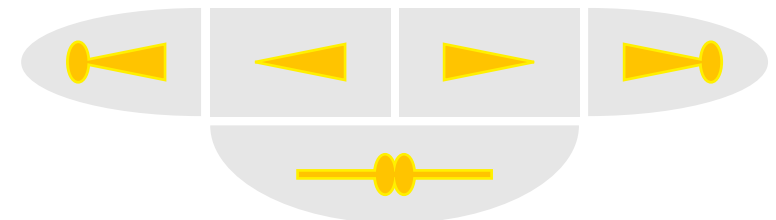
Risikomanagement

Kosten durch Ausfall - Investitionen für IT-Sicherheit
Bsp.: Was kostet ein Ausfall-Zeitraum von

- Stunde
- Tag
- Woche
- ...

Standardfälle

Kundendaten (Adressen, Ansprechpartner, ...)
Terminkalender (Fristen, ...)
Rechnungen



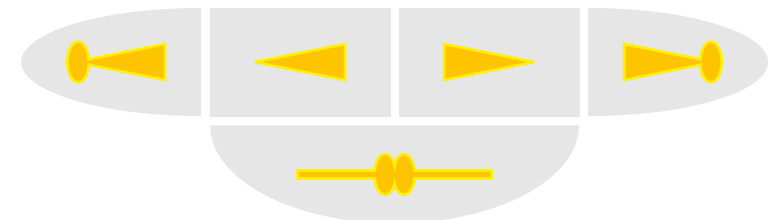
Gefahrenquellen

Organisatorisch

Unklare Verantwortlichkeiten
Fehlende Vorgaben
Fehlende Konzepte
Menschliches Versagen
»social engineering«

Technisch

Komplexität
Software-Mängel
Kostendruck



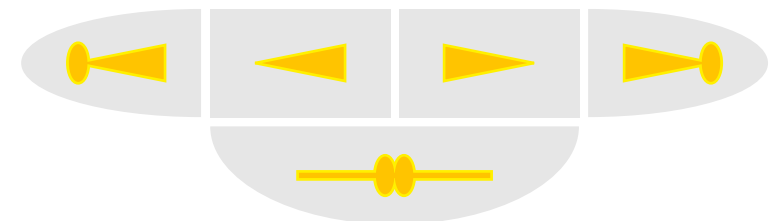
Angriffsszenario

Kombiniertes Nutzen mehrerer Bedrohungen

Vorgehen

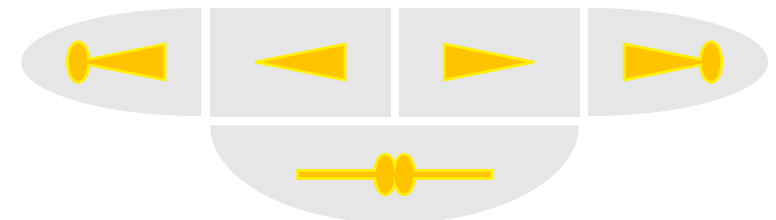
- 1 Informationen sammeln
Scans, Insider-Kenntnisse
- 2 Eindringen
Schwachstellen nutzen
- 3 Kontrolle übernehmen
Zusätzliche Rechte erlangen
- 4 Spuren verwischen
Sicherheitsfunktionen abschalten
- 5 Nutzung
Zerstörung, Mißbrauch

Parallelität und zeitliche Verteilung möglich!



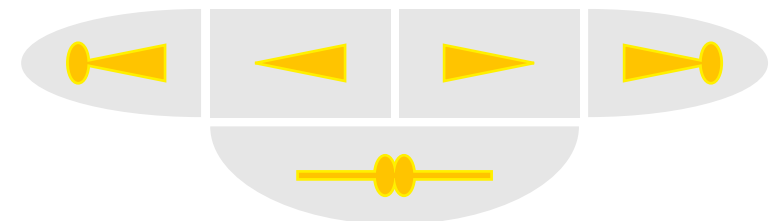
Schutzmaßnahmen ohne Sicherheitstechnik (1)

Zugangsschutz	Konsequente Nutzung Trennung von Funktionen Verteilte Verantwortlichkeit
Trennung von Funktionen	KISS-Methode (keep it small and simple) Client-Server-Architektur, dedizierte Server Definierte Schnittstellen
Zellenkonzept	»Zwiebelprinzip« Mehrschichtiger Schutz bei Netzwerk und Zugang
Redundanz	Parallele, unabhängige Systeme Lastverteilung realisieren



Schutzmaßnahmen ohne Sicherheitstechnik (2)

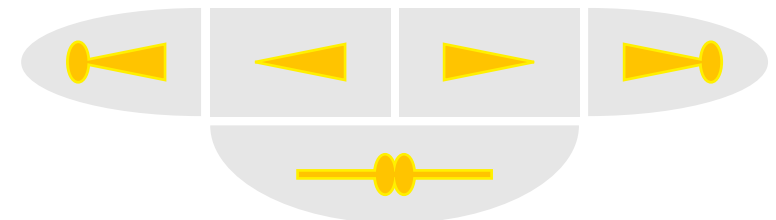
Technikauswahl	IT-Sicherheit als Entscheidungskriterium
Qualitätssicherung	Anleitungen, Checklisten, Nachvollziehbarkeit
Schulung	Sensibilisierung IT-Sicherheit in Weiterbildung aufnehmen



IT-Sicherheitskonzept

Zu betrachtende Bausteine

- Gebäude
- Verkabelung
- Serverraum
- Organisation
- Personal
- Notfallvorsorge-Konzept
- Datensicherungskonzept
- Datenträgerarchiv
- Raum für technische Infrastruktur
- Virenschutz
- Heterogene Netze
- Netz- und Systemmanagement
- Firewall
- Standardsoftware



Verkabelungsplan

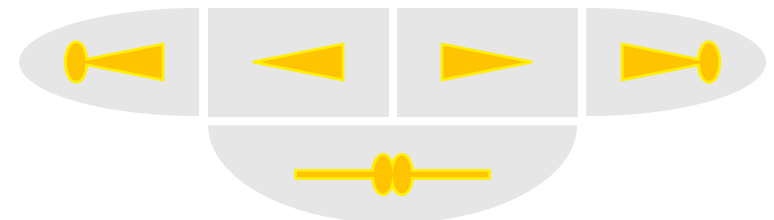
Beschreibung alle verlegten Kabel mit Typ

Beschreibung der Verteiler

Belegung der Anschlüsse im Verteiler

Anschluss der Kabel an die Verteilung

Listen und Grafik

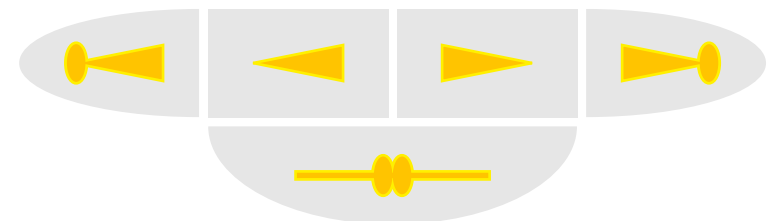


Netzwerkkonzept

Die physikalische Netzstruktur und die logische Netzkonfiguration ist dokumentiert.

- Beschreibung der Netzwerktechnik (ATM / Ethernet)
- Beschreibung der Netzwerktopologie
- Liste der angeschlossenen Geräte (aktiv / passiv)
- Grafische Darstellung des Netzes (Soll)
- Scan des Netzes mittels eines Werkzeugs (Ist)

Was ist Innen und Außen?



Firewallkonzept

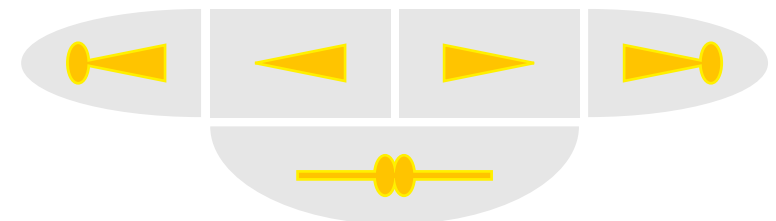
Ein Konzept für eine Firewall ist zu erstellen.

Die Sicherheitspolitik der Firewall ist ständig auf Aktualität zu überprüfen und ggfls. anzupassen.

Festlegung der Sicherheitsziele
Anpassung der Netzstruktur
Grundlegende Voraussetzungen schaffen

Auswahl der Kommunikationsanforderungen
Dienstauswahl
Organisatorische Regelungen

Die eingesetzten Paket-Filter müssen jedes ein- oder ausgehende Paket protokollieren können. Für jede aufgebaute und abgewiesene Verbindung muß eine Protokollierung durchgeführt werden (Application-Gateway), wobei auch Einschränkungen auf bestimmte Verbindungen (z. B. für einen speziellen Benutzer) möglich sind.



Systemmanagement

Nutzen

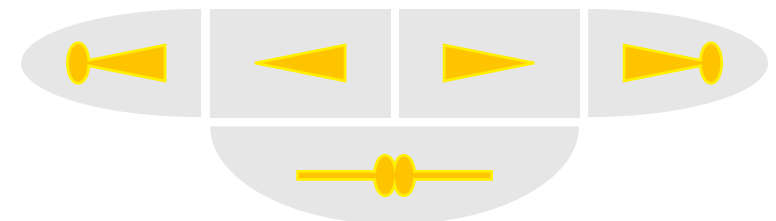
Vorfälle schnell erkennbar

Konfiguration prüf- und änderbar

Software-Distribution für Sicherheits-Updates

Datenvolumen analysieren

Sicherheitstechnik managen

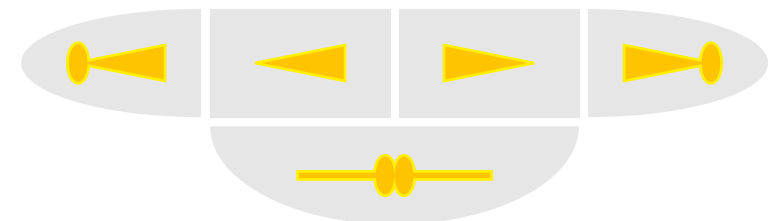


Installationsdokumentation

Es ist Aufgabe der DV-Abteilung, alle Veränderungen jeweils zu dokumentieren, insbesondere die folgenden:

- Einrichten und Update des Betriebssystems
- Einrichten und Update der Datenbanksoftware
- Einrichten und Update der Anwendungssoftware
- Einrichtung neuer Benutzer
- Einrichtung neuer Gruppen
- Änderung/Erweiterung der Hardware der Server

Betriebshandbuch (BH)

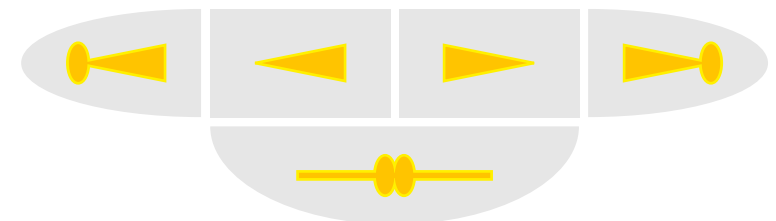


Software-Liste - Vorgehen

Ein Dokumentations- und Verteilungssystem für die eingesetzte Software sollte eingesetzt werden. Alle Einzelplatzrechner werden in unregelmäßigen Abständen von Mitarbeitern der DV-Abteilung überprüft. Dabei wird auch der Inhalt der Dateisysteme gesichtet und die Anwendungssoftware dokumentiert.

Alle serverseitig installierte Software ist ebenfalls zu dokumentieren und die Benutzerbereiche in regelmäßigen Abständen auf eigenständig installierte Software zu prüfen.

Auf allen Rechnern darf nur von der DV-Abteilung freigegebene Software eingesetzt werden.



Software-Liste

Verzeichnis aller vorhandenen Software

IT-Sicherheit

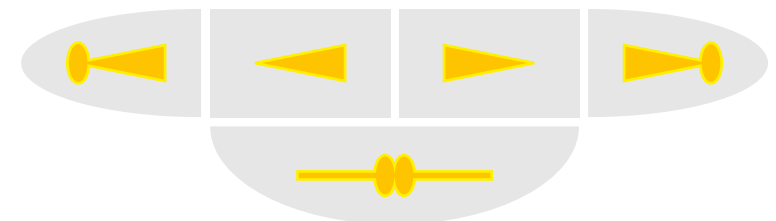
Basis für

- Gefährdungsabschätzung - Sicherheitsmeldungen
- Update-Massnahmen

Weiterer Nutzen

Basis für

- Software-Pflege
- Kostenplanung
- Lizenzierung



Anwendungsbeschreibung

Architektur

Die Anwendung und ihre Komponenten-Architektur wird global und übersichtsartig beschrieben.

Komponenten

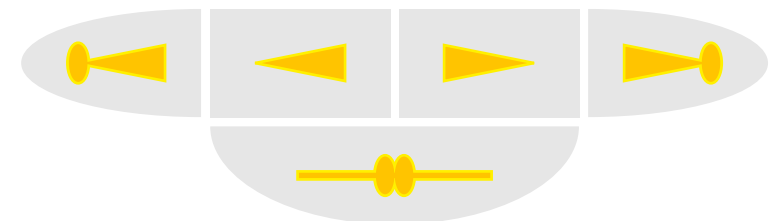
Die Anwendung und ihre Komponenten-Architektur wird aus Sicht der Datenverarbeitung beschrieben.

Benutzte Software

Eine Client/Server-Anwendung entsteht nicht von Grund auf neu, sondern setzt auf bestehende Komponenten auf, z.B. Datenbanksystemen, Schnittstellen zu bestehenden Anwendungen und Middleware.

Datenlandschaft

Die Struktur, Topologie und Dynamik der Datenlandschaft wird beschrieben. Aus Art, Verteilung und Dynamik der verwendeten Anwendungs-Daten ergeben sich direkte Einflüsse auf Anforderungen, Funktionalität und Verhalten der Anwendung.

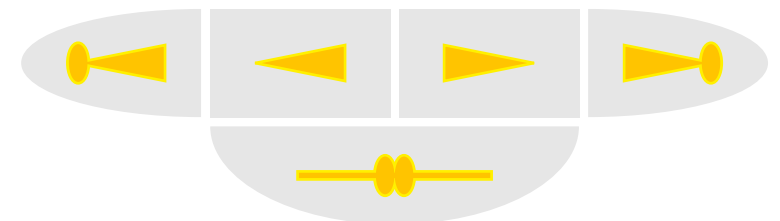


Betriebshandbuch

Im Handbuch sind Informationen für die Installation, die Einführung, den Betrieb und die Administration der Anwendungen beschrieben, sowie anzuwendende TroubleShooting Strategien.

Beginnend bei der Definition von Rollen und organisatorischer Strukturen über die notwendigen Prozesse und Prozeduren bis hin zur Beschreibung technischer Managementwerkzeuge und genereller Dienstleistungsvereinbarungen beschreibt und definiert das Betriebshandbuch alle notwendigen Elemente der Betriebsführung.

Im Betriebshandbuch sind z.B. alle Schritte dokumentiert, die beim Herauf- bzw. Herunterfahren von IT-Systemen zu beachten sind. Dabei ist besonders auf bestimmte Reihenfolge beim Mounten von Laufwerken oder Starten von Netzdiensten hinzuweisen.



The screenshot shows a Netscape Communicator browser window. The address bar contains the URL: `http://virginia/db/~gerd/bhb/io.html?cluster=1&ws=5&ae=AE`. The page content is organized into a sidebar and a main area.

Sidebar (KAD):

- Sachgebiet
- SLA-Angebote M C
- Kapazitätsplanung HOST M
 - Allgemeine Angaben M
 - CPU-Bedarf
 - Plattenspeicher-Bedarf
 - Transaktionen
 - Services
 - In-/Output-Management
 - MQM
 - Datensicherung
 - IFP
 - Sicherung
 - Auslagerung
 - IMP
- Sonstige Angaben
- Notiz Kapazität AE
- Programme M

Main Content Area (Sicherung):

Sicherung

Sicherung

Mittelwert aus tgl.Abwicklung (MB) AE: Integer (10; beliebig) [Info](#)

Max. Tageswert

AE: Integer (10; beliebig) [Info](#)

hierzu Profilingaben

AE: Memo [Info](#)

Max. Monatswert

AE: Integer (10; beliebig) [Info](#)

hierzu Profilingaben

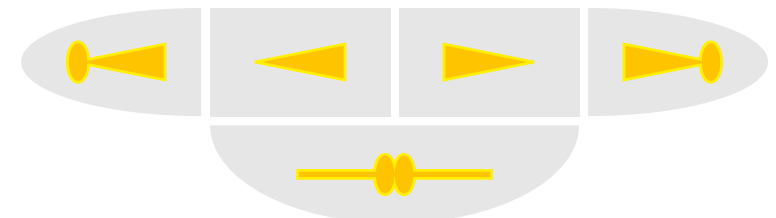
AE: Memo [Info](#)

jähr. %-Wachstum

AE: Integer (10; beliebig) [Info](#)

hierzu Terminangaben

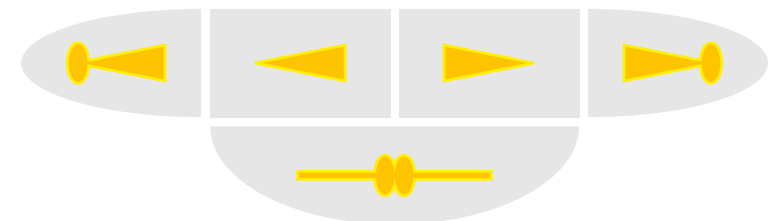
AE: Memo [Info](#)



Notfallplan

Die für die IT-Anwendung relevanten Notfallereignisse werden definiert. Die folgende Tabelle gibt vor, wer zu benachrichtigen ist und welche Maßnahmen zu treffen sind.

Notfall	Meldeweg	Maßnahme
Ausfall eines Servers	Geschäftsleitung	Ausweichen auf 2. Rechner
Ausfall/Wegfall beider Rechner	Geschäftsleitung	Ausweichen auf externen Rechner
Ausfall des Bandlaufwerkes	Geschäftsleitung	Ausweichen auf Bandlaufwerk extern
Ausfall eines Volumes im RAID-System	Geschäftsleitung	Ersatzbeschaffung
Ausfall der Mailbox	Empfänger/Absender der Daten	Ausweichen auf Datenträger
Softwareausfall	Geschäftsleitung	Fehlerbehebung Neuinstallation
Stromausfall	Geschäftsleitung Haustechnik	Fehlerbehebung Überwachung der USV



Logging-Konzept

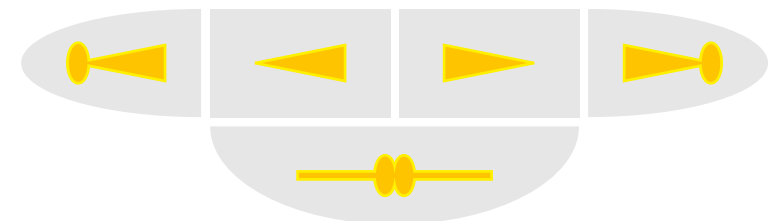
Benutzeraktivitäten auf Benutzerebene (Login, Logout, etc.) werden protokolliert.

Die Protokolle sind monatlich durch die DV-Abteilung auszudrucken und zu überprüfen.

Systemmeldungen sind zu protokollieren und täglich auf Auffälligkeiten zu untersuchen.

Protokolle der Firewall und der IDS sind zu protokollieren und täglich auf Auffälligkeiten zu untersuchen.

Keine Auswertung von leistungsbezogenen Daten zu Nutzern



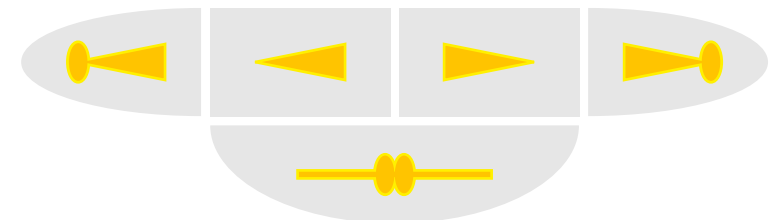
Datensicherung

Konzept

Zweck - Backup oder Archivierung
Sicherung aller Daten
Regelmäßigkeit, Verlässlichkeit - Prüfen
Wiederherstellbarkeit - Übung
Zeitraum der Aufbewahrung
Sichere Lagerung - Auslagerung

Rahmenbedingungen

SLA
Anleitung - Notfallplan
Mitarbeiter informieren



Berechtigungskonzept

Zutrittsberechtigung

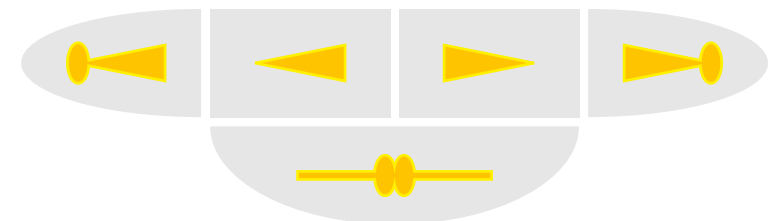
Unbefugter Zutritt zu schutzwürdigen Räumen im IT-System ist auf physischem und organisatorischen Weg zu verhindern.

- Zugangskontrolle
- Begleitung Fremder
- Pförtnerdienst

Zugriffsberechtigung

Die Ersteinrichtung der Benutzernamen und der zugehörigen Kennwörter erfolgt durch die Mitarbeiter der DV-Abteilung.

- Änderungen der Kennwörter durch die Benutzer
- Prüfbarkeit der Nutzung durch die Benutzer
- Erzwingen von regelmäßigen Passwortänderungen



Kommunikationskonzept

Massnahme

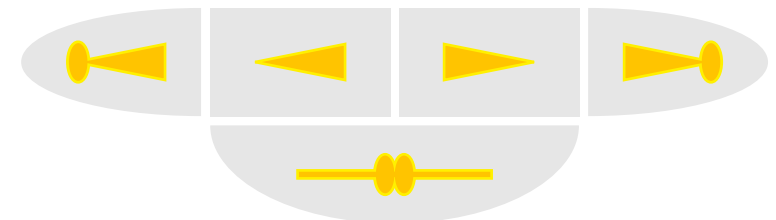
Politik festlegen

- Kommunikationspartner erfassen
- Austauschformate definieren
- Standardprozeduren für Dokumenterstellung
- Corporate Identity
- Qualifikation/Schulungen
- Vertragsinhalt

Nutzeffekte

- Kommunikation verbessern - Warnungen möglich
- Gefährdungen verringern - Kritische Formate
- Einheitliches Auftreten
- Effiziente Dokumentenerstellung
- Geringeres Kommunikationsvolumen
- Geringeres Speichervolumen

Risikomanagement



IT-Sicherheit im Einkauf

IT-Sicherheit ist ein Produktmerkmal

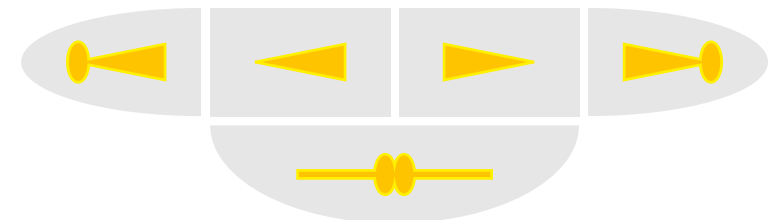
Kriterien

- Stabilität
- Anfälligkeit
- Reaktionszeiten - Patches, Ausfälle
- Komplexität
- Handhabbarkeit
- Eingrenzbarkeit von Fehlern

Vorgehen

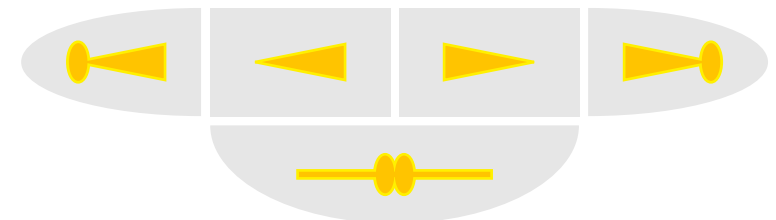
Beschaffungsprozess untersuchen

- Produktauswahl
- Abstimmung mit Infrastruktur
- Integration in IT-Strategie



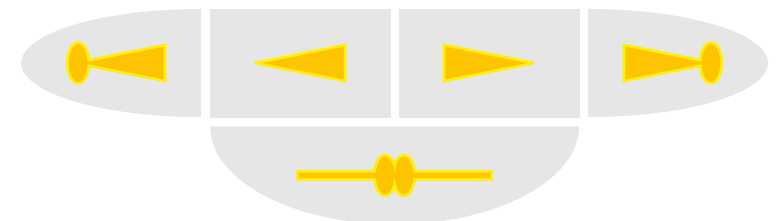
Technische Schutzbausteine

- Firewalls
- Content Scanner (z.B. Antivirensysteme)
- Intrusion Detection/Intrusion Response Systems (IDS/IRS)
- Integritätsprüfung
- VPN (virtual private network)
- PKI (public key infrastructure)
- Penetrationstest durch Security Scanner
- Quarantäne-Rechner
- Beweissicherung - Honeypot - Forensic Computing



Firewalls

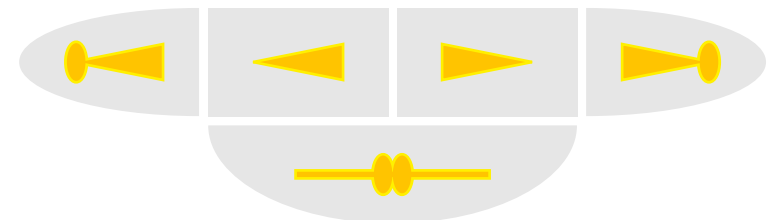
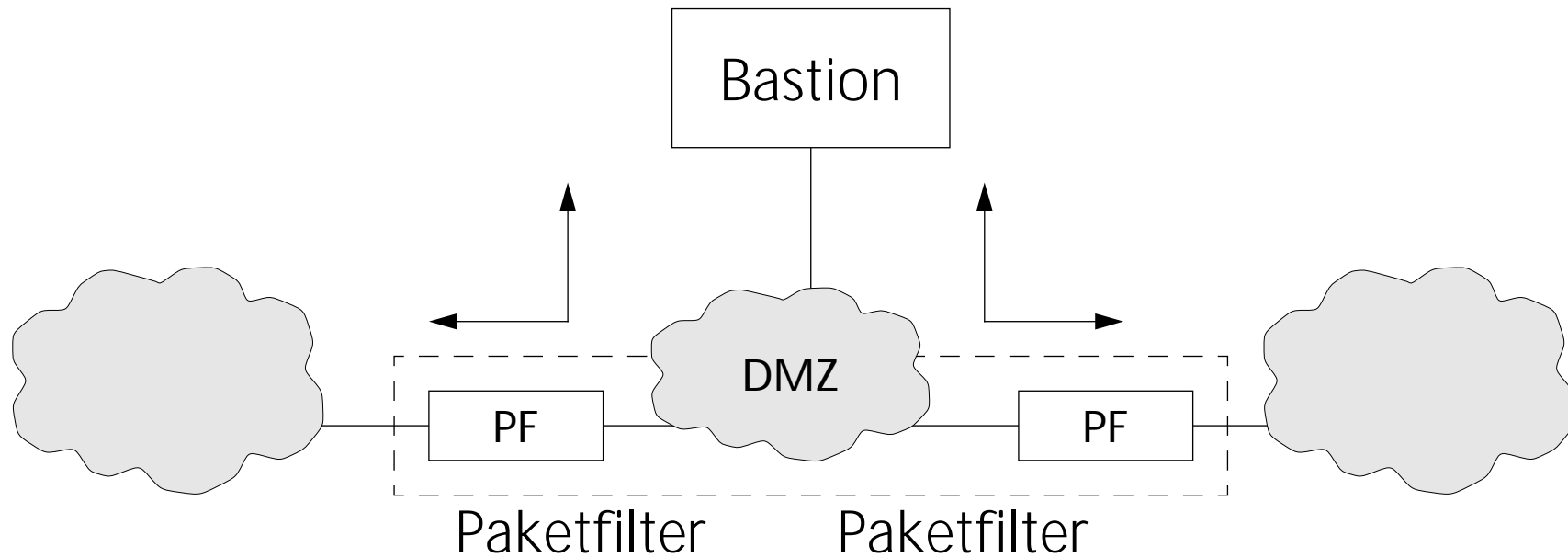
Definition	Kontrollierte Verbindung von Netzwerken
Funktion	Firewall=Konzept +Software + Hardware Policy bestimmt das Verhalten
Anforderungen	Stabiles, widerstandsfähiges System (gehärtet) Administration notwendig
Probleme	Komplexität erzeugt Angriffspunkte Schutz nur auf Basis von Netzwerkverbindungen Tunneling möglich, z.B. durch Verschlüsselung Nur Schutz gegen »Außen«
Besonderheiten	Hardwarefirewall - Appliances Personal Firewall - Keine Firewall, kein Schutz



Firewall (einstufig)

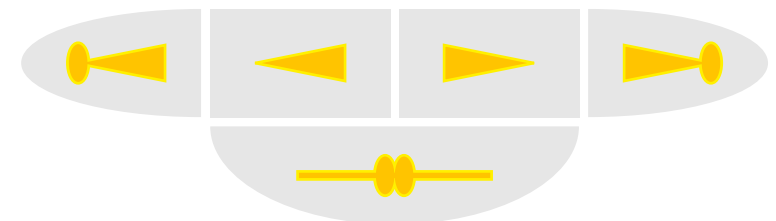
Inneres Netzwerk

Äußeres Netzwerk



Content Scanner

Definition	Prüfung von Inhalten auf Bedrohungen
Funktion	Policy definiert erlaubten Content und Verhalten Prüfung auf Signaturen von Schadfunktionen »Sandbox«-Technik
Anforderungen	Stabiles, widerstandsfähiges System (gehärtet) Administration notwendig
Probleme	Komplexität erzeugt Angriffspunkte Schutz nur gegen bekannte Bedrohungen Tunneling möglich, z.B. durch Verschlüsselung Rechtliche Probleme durch Veränderungen des Inhalts
Einsatzort	Am Zusammentreffen aller Infektionswege - Endgerät



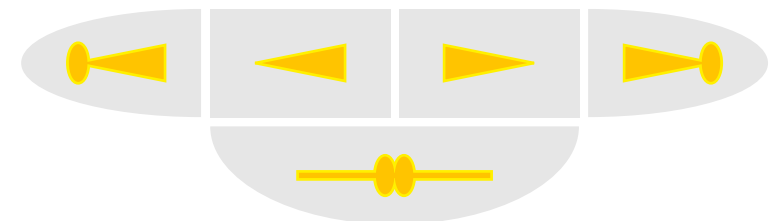
Angriffe - Ursachen

Systemschwächen

- Konfigurationsfehler
- Implementierungsfehler
- Designschwächen
- Fehlverhalten des Menschen

Ausnutzung mehrerer Schwächen möglich

Potenzierung durch Komplexität



Bedrohung Komplexität

Software-Komplexität ist proportional zum Quadrat der Anzahl der Zeilen im Quelltext

Bsp. WinNT wächst 35 % pro Jahr, IE 220 %

Effekte

Systeme werden nicht verstanden

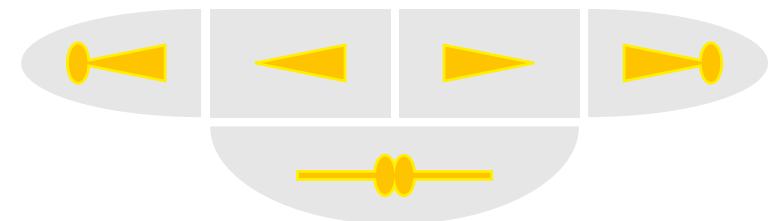
- Angriffe schierig vorhersagbar
- Gefahr von Fehlkonfigurationen
- Erreichen sicherer Zustände wird unmöglich

Ansteigen der Fehlerrate in der Software

Effekt

SANS Institute - Top 20 Internet Security Vulnerabilities

<http://www.sans.org/top20/>



System »härten«

Angriff »erwarten« - Passive Sicherheit

Komplexität verringern

- Fehlerquellen reduzieren - Dienste, Software
- Keine Hilfsmittel für Angreifer

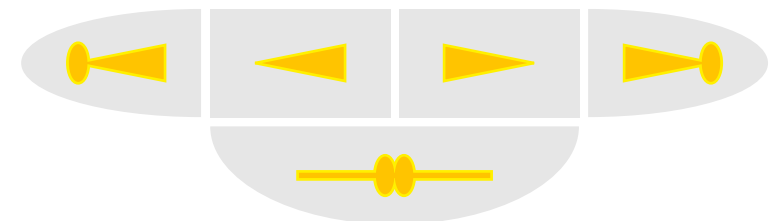
Schadenswirkung einschränken

- User-Rechte gering halten (nie Root/Administrator)
- Filesystem read-only
- Filesystem »verkleinern« (chroot-jail) - bei Servern
- Zellenkonzept - Netzwerk, Virtuelle Maschinen

Detektieren

- Integritätstest
- Scannen

Maßnahme erfordert Konzept!



Vielen Dank!

Kontakt

Fraunhofer Institut für Software- und Systemtechnik (ISST)
<http://www.isst.fraunhofer.de>

Arbeitsgruppe IT-Sicherheit
Holger Kurrek

Tel.: 030 / 24306 - 355

Mail: [Holger.Kurrek @ isst.fraunhofer.de](mailto:Holger.Kurrek@isst.fraunhofer.de)

