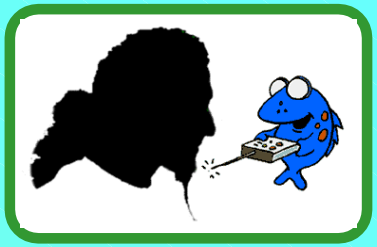
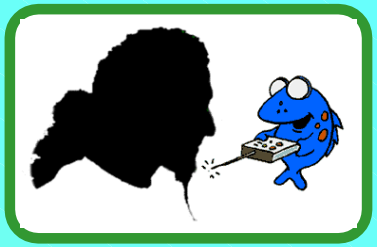


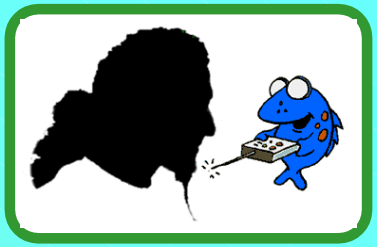
more Network Security

Definition



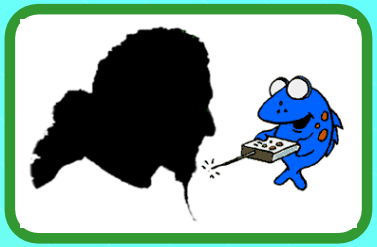
- Sicherheit beschreibt in dieser Vorlesung
  - Methoden zum unerlaubten Zugriff auf Computernetzwerke und
  - Vermeidung derselben
  - Konzepte und Beispiele destruktiver Software und wie man ihrer Herr wird
  - Methoden zur Erhaltung der Privatsphäre in Daten und Systemen
  - Schutz von Computersystemen gegen verschiedene Arten von Zugriffsversuchen, die nicht erwünscht sind
- Sicherheit steht in dieser Vorlesung nicht für
  - Zuverlässigkeit (Dependability) und Ausfallsicherheit im Allgemeinen

Motivation zum Angriff



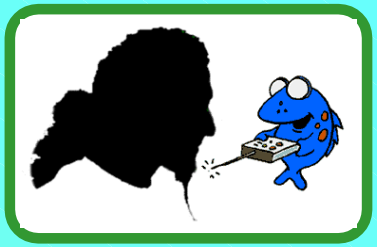
- Konkurrenz
- Hacking als Spiel, Sport und Spaß
- Spionage
- Unfähigkeit
- absichtliche Sicherheitschecks
- Rache

Problemzonen



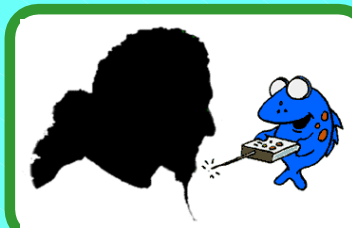
- Übergänge zwischen Domänen
  - LAN zu WAN
  - Organisationseinheiten
- Datenhaltungskomponenten
  - Wechselspeicher
  - Server / Datenbanken
- Anwender-Zugänge (Terminals)

Abwehrmaßnahmen im Netz



- Topologische Maßnahmen
- Filter
- Proxies
- Maskierung / Adreßübersetzung
- Tunneling
- Überwachung

Topologische Abwehrmaßnahmen (1)



Insel

fremdes Firmennetz

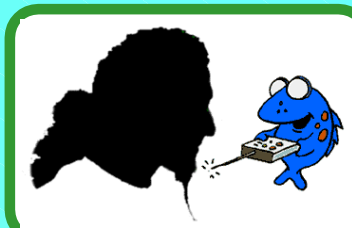
Internet

Telefonnetz

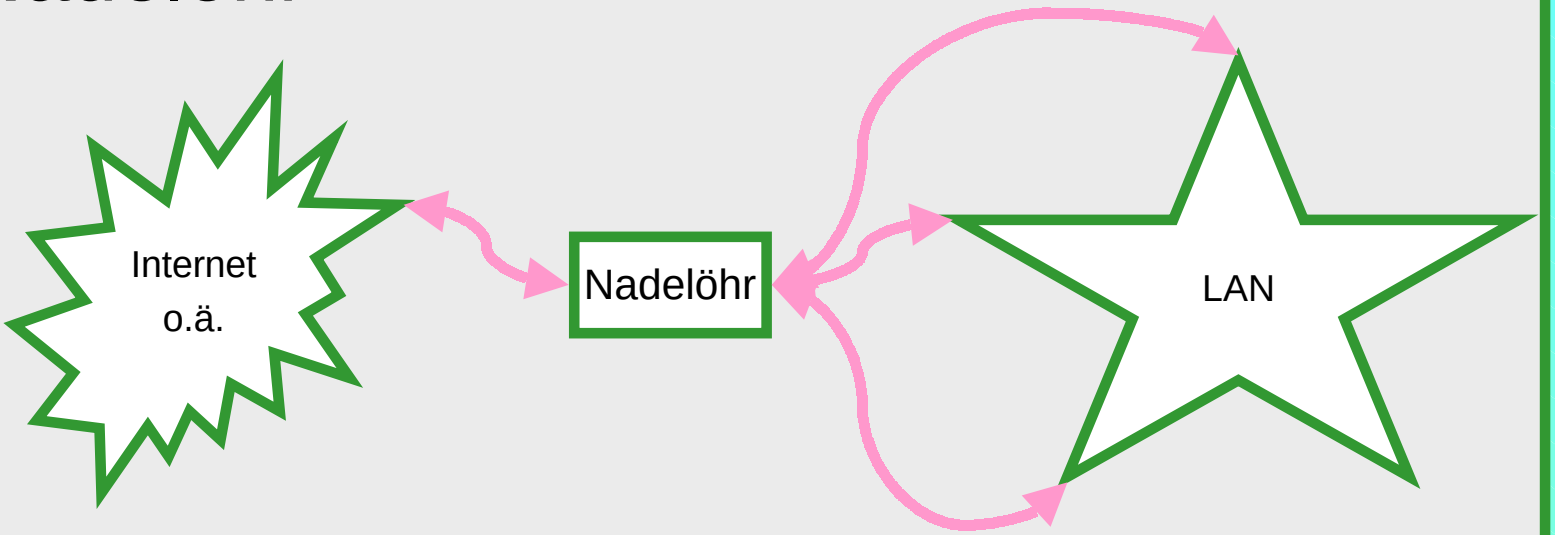
Insel-Details

- eine Insel ist schlicht nicht mit der Außenwelt verbunden
- Vorteile:
  - Angriffe von außen sehr schwierig
  - Überschaubarkeit erhöht sich
- Nachteile:
  - Nutzung externer Infrastruktur nicht möglich
  - unzufriedene Anwender
  - Drang zu Hintertürchen stark

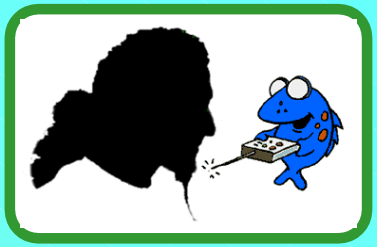
Topologische Abwehrmaßnahmen (2)



Nadelöhr



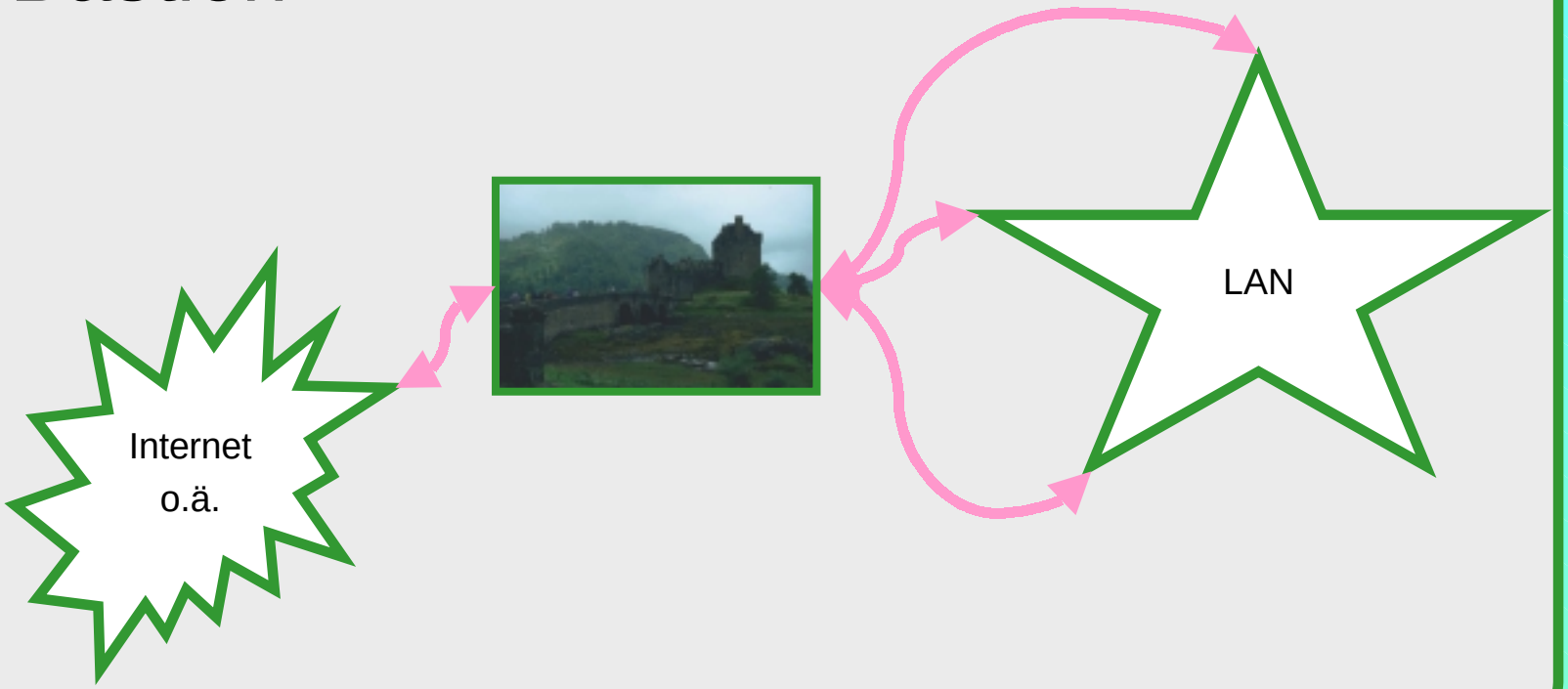
Nadelöhr-Details



- Zugriffe von und nach “außen” über wenige, schmale Durchgänge führen
- Vorteile:
  - bessere Überwachbarkeit
- Nachteile:
  - hohe Performanceanforderungen
  - selten: Einschränkungen des Benutzers “innen”

Topologische Abwehrmaßnahmen (3)

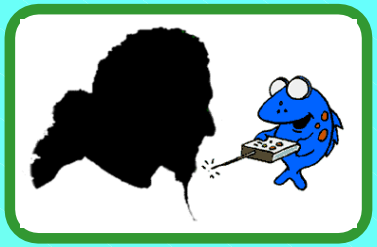
Bastion



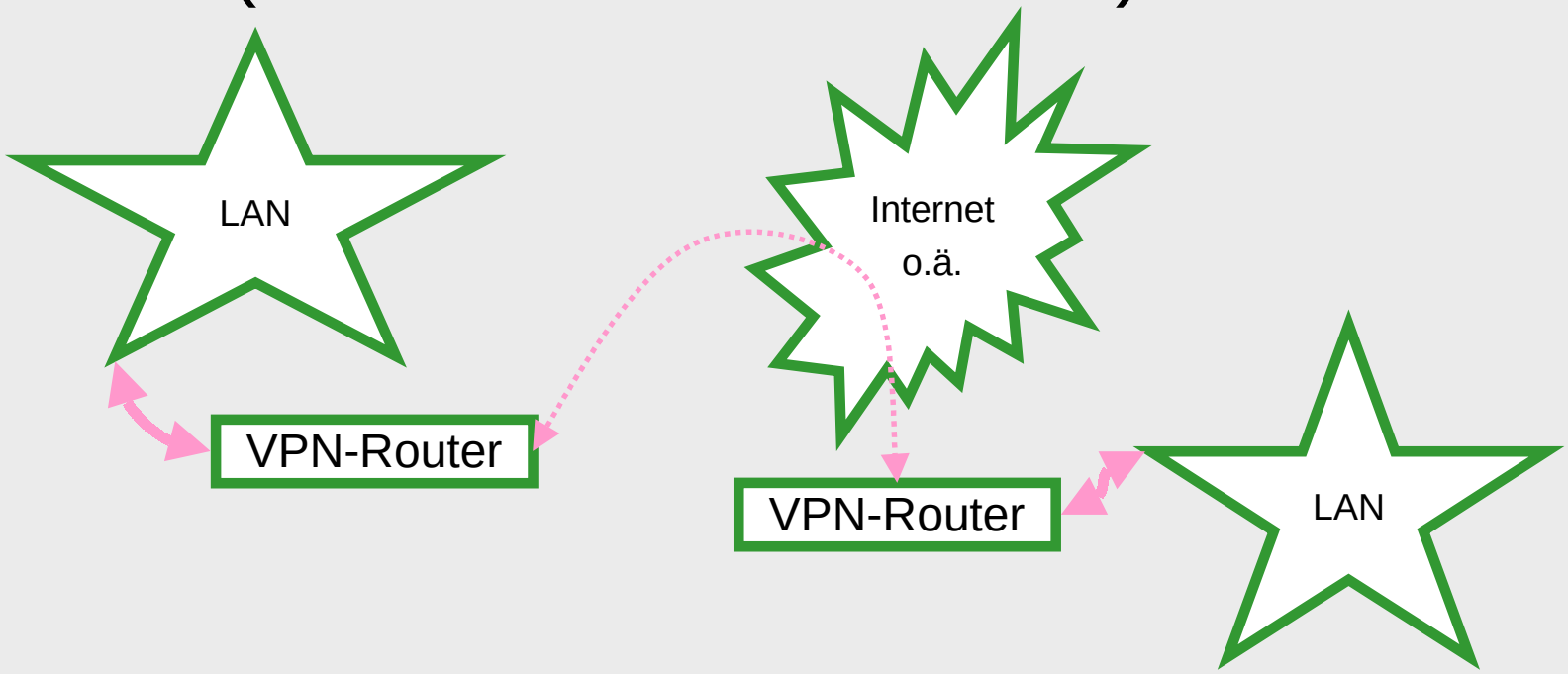
Bastion-Details

- meist mehrstufiges Grenznetz wird dem am Nadelöhr lokalen vorgelagert (Vorbild: Ritterburg)
- Vorteile:
  - sehr exakte Möglichkeiten zur Definition für Zugänge von Außen
- Nachteile:
  - erheblicher Aufwand
  - Einschränkung der Freiheit von inneren Benutzern

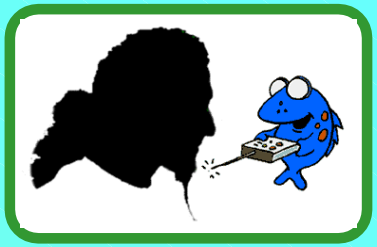
Topologische Abwehrmaßnahmen (4)



VPN (Virtual Private Network)

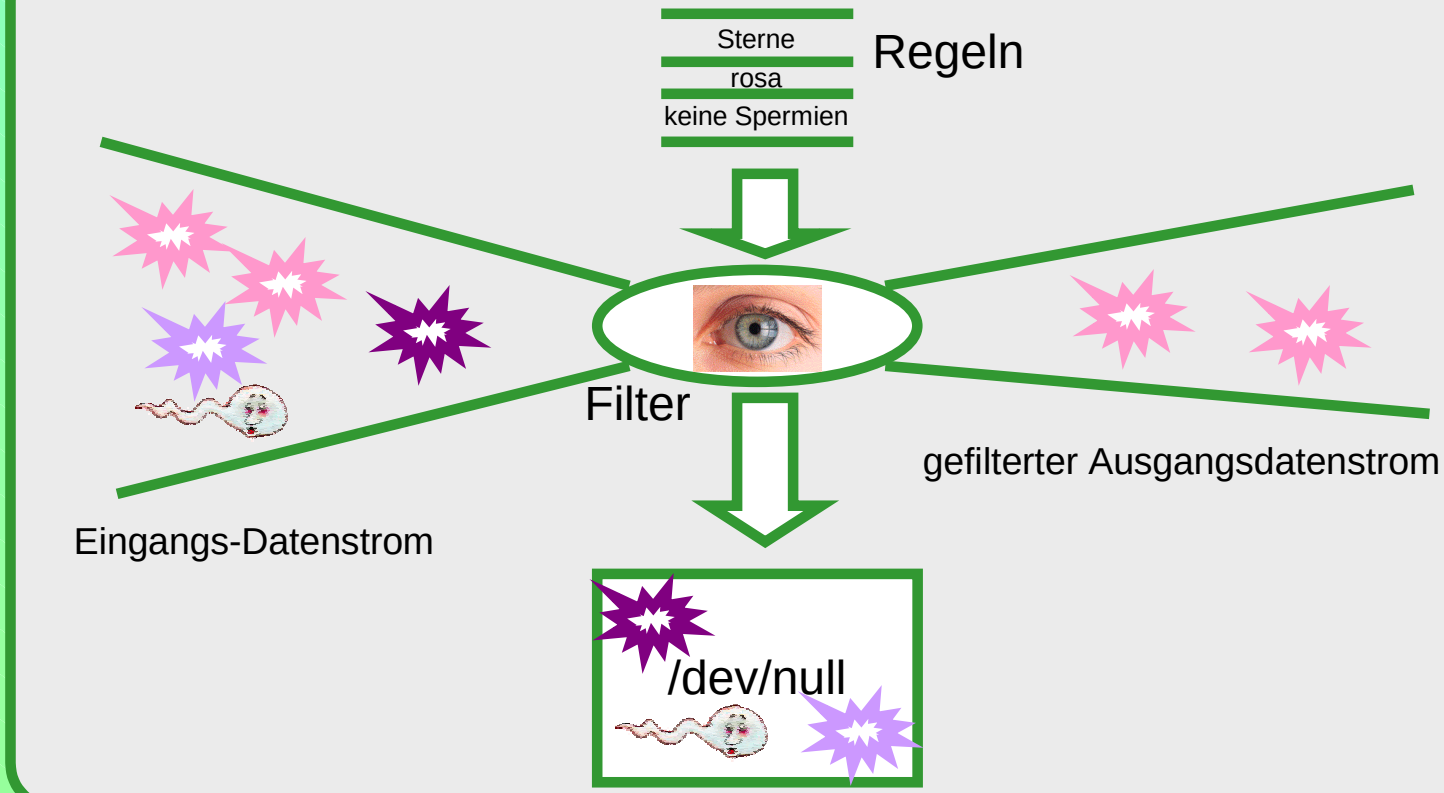


VPN Details

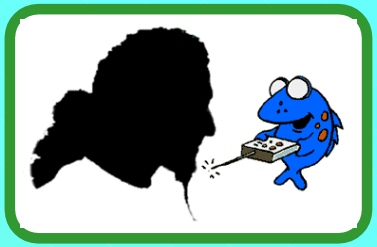


- lokale Inseln werden über → Tunneling miteinander verbunden
- Vorteile:
  - perfekte Erhaltung der Privatsphäre
  - Kosteneinsparung durch Nutzung öffentlicher Datentransportwege
- Nachteile:
  - (noch) Indeterministische Performance
  - Infrastruktur des “Außen” wird nur teilweise genutzt
  - spezielle Mechanismen an den Übergängen erforderlich

Filter

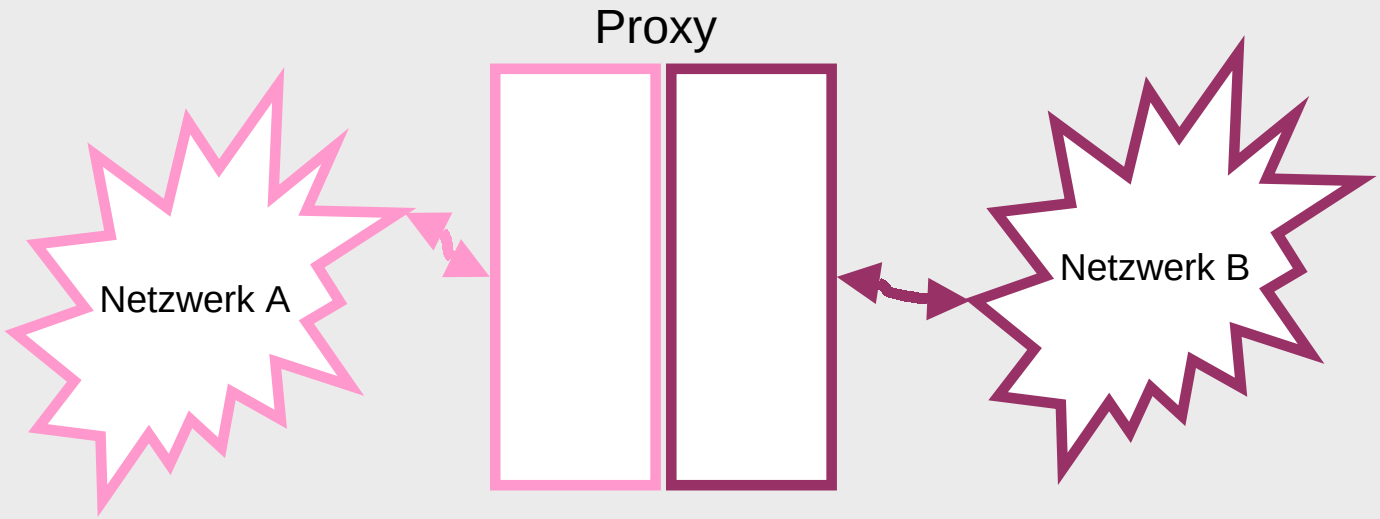


Filter Details

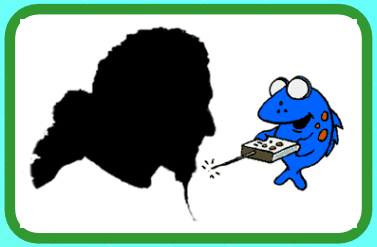


- am Übergang zwischen Protokollschichten oder an der Verbindung zweier Interfaces derselben Protokollebene werden Regeln definiert, welche Inhalte von Paketen erlaubt und welche verboten sind
- Vorteile:
  - definierte Möglichkeit zur Verkehrskontrolle
- Nachteile:
  - zur Erhaltung der Performance ist Aufwand nötig
  - fehlerträchtiger Konfigurationsaufwand
  - einfache Filter sind über gefälschte Adressen zu täuschen

Proxies



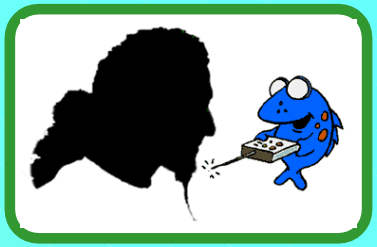
Proxy Details



- Vermittlungseinheit, die auf einer Seite horcht, d.h. als Server auftritt, und auf der anderen Seite unter eigener Identität sendet, d.h. als Client auftritt, kann an verschiedenen Ebenen angreifen
  - Proxy ARP vermitteln auf der Netzwerkschicht
  - Circuit Level Proxies vermitteln auf der Transportschicht
  - Application Gateways vermitteln in den Applikationsschichten
- Vorteile:
  - gefälschte Pakete tieferer Ebenen werden ausgepackt und damit unwirksam
  - durch Caching nicht immer Client-Datentransfer nötig
  - Authentisierungsmöglichkeiten
- Nachteile:
  - Hard- und Softwareaufwand
  - Einschränkung der verwendbaren Protokolle

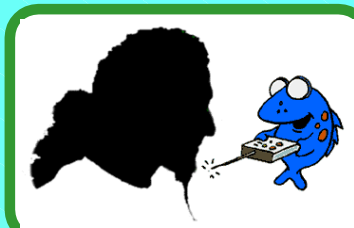
Masquerading

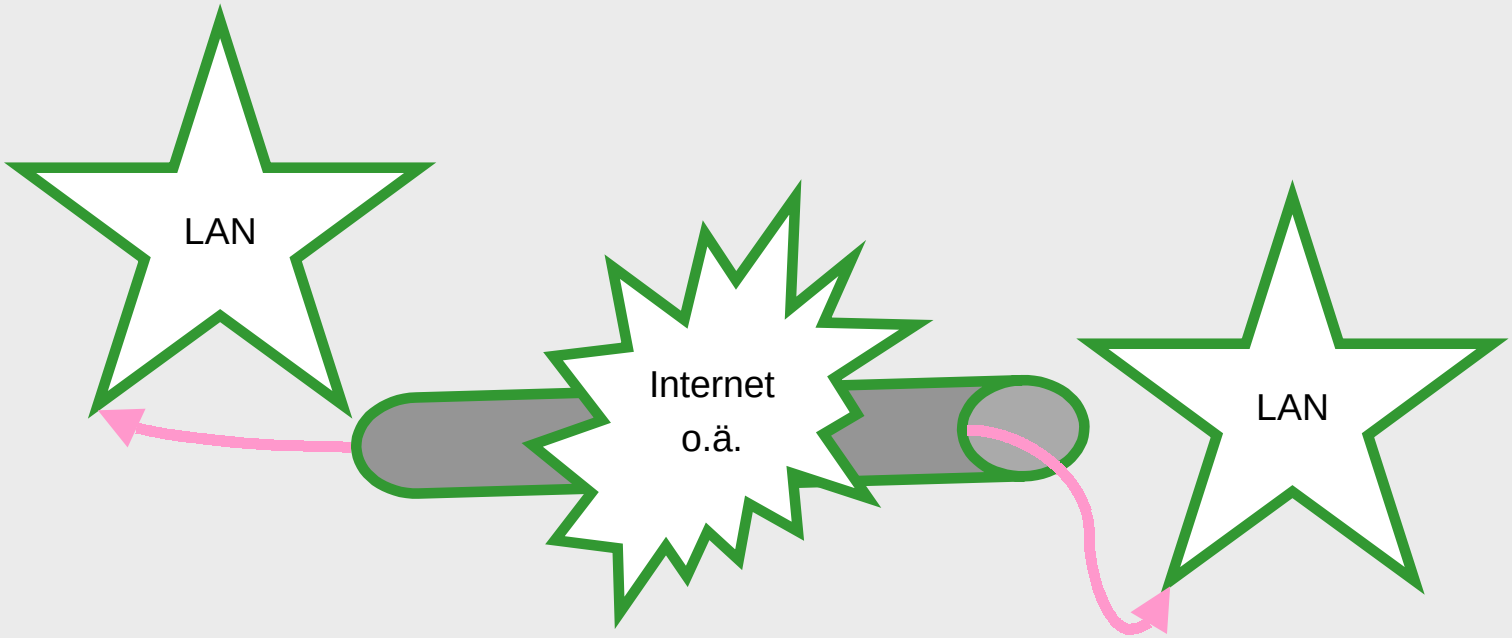
Masquerading Details



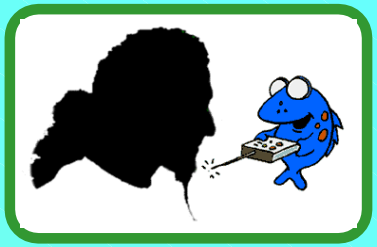
- Viele Adressen des Netzwerk-Schicht-Protokolls werden unter Verwendung einer Transportschicht-Port-Kodierung auf wenige abgebildet - ähnlich einem Layer 3 Proxy
  - Bekannteste Beispiele: NAT, Linux IP-Masquerading
- Vorteile:
  - lokale Adressen außen nicht sichtbar
  - Einsparung von Adressen
- Nachteile:
  - zusätzlicher Hard- und Softwareaufwand
  - eingehende Verbindungen an lokale Server-Adressen verwässern das Konzept

Tunneling



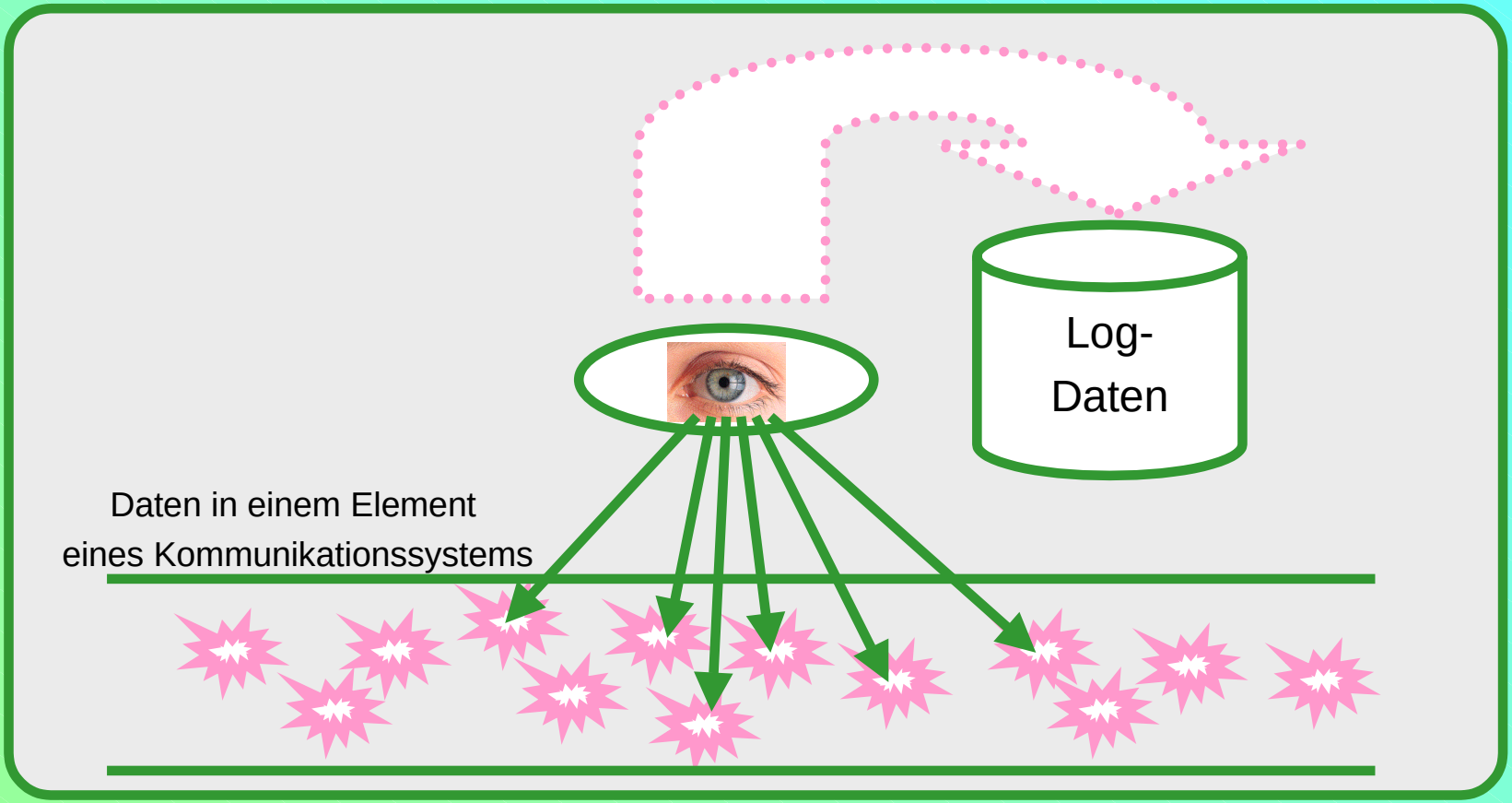


Tunneling Details

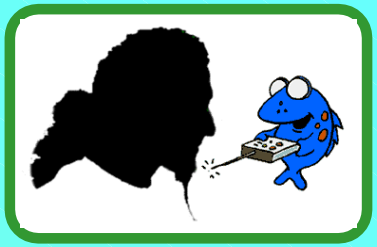


- insbesondere für → VPNs verwendete Methode, Netzwerkschicht-Pakete in ebensolche optional verschlüsselt zu verpacken, um Netzwerke zum Transport anderer Netzwerke zu verwenden
- Vorteile:
  - Abhörsicherheit
- Nachteile:
  - erhöhter Protokoll-Overhead

Überwachung

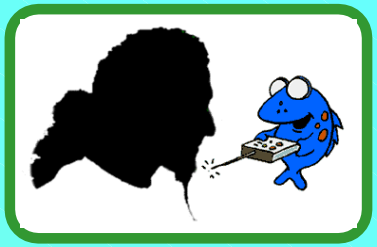


Überwachungsdetails



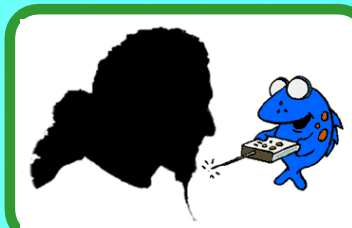
- möglichst transparent wird in Leitungen oder an Netzwerkknoten notiert, was für Transfers stattfinden
- Vorteile:
  - Ereignisse können ausgelöst werden, wenn Regeln verletzt werden
  - nachträgliche Möglichkeit, nachzuvollziehen, wer wann was getan hat in Bezug auf Zugriffsrechte und Kosten
- Nachteile:
  - Speicherplatzaufwand
  - Aufwand an Personal / Aufmerksamkeit

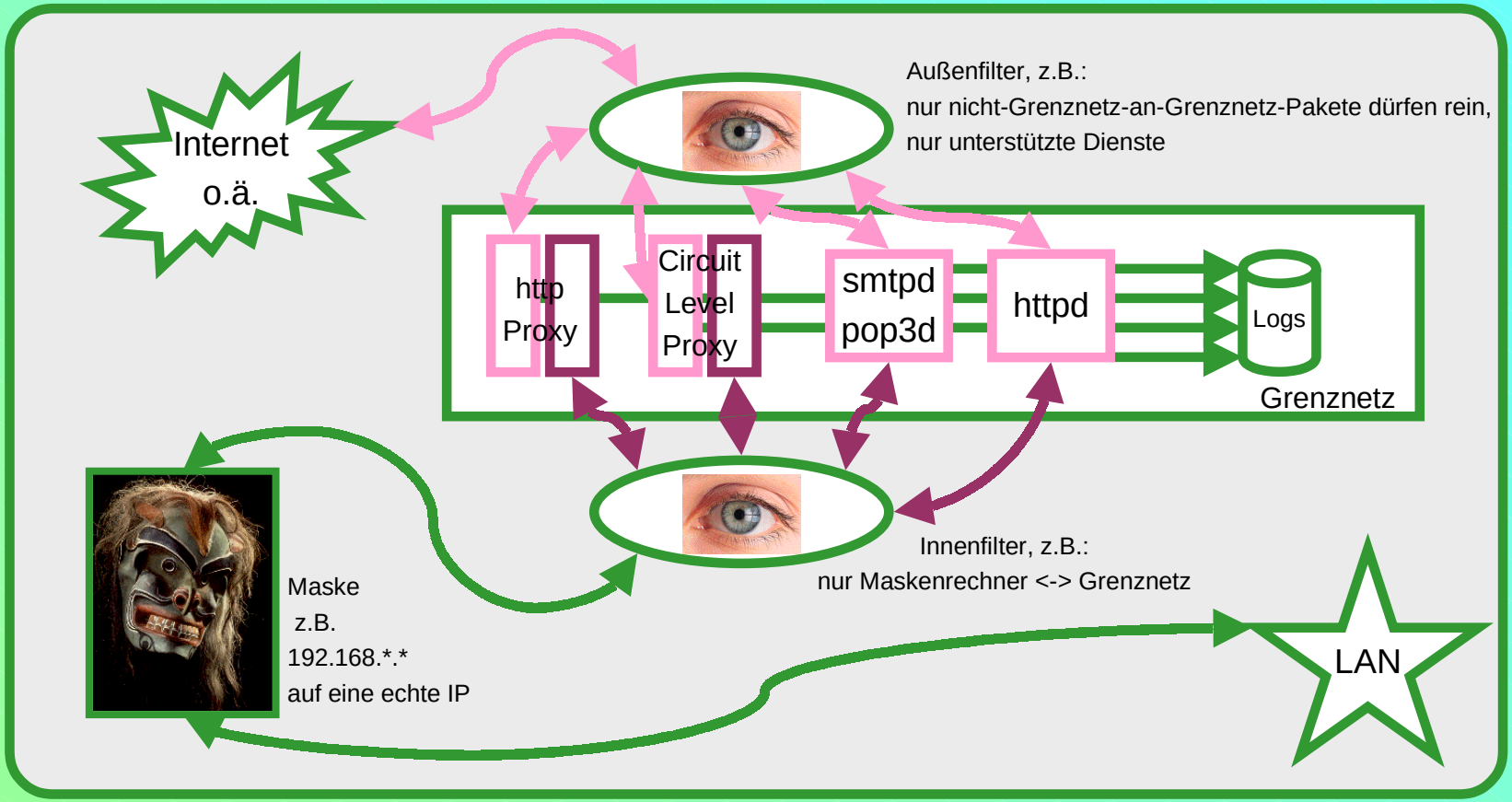
Grundregeln der Netzwerksicherung



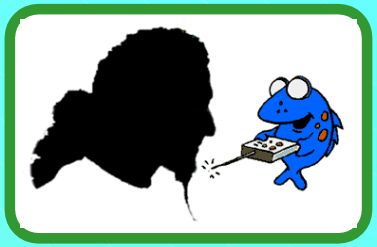
- zunächst alles verbieten und nur definierte Verbindungen explizit zulassen
- je mehr Schichten zur Sicherung zur Verfügung stehen, desto sicherer das Gesamtsystem
- je eingeschränkter die Zahl der zu überwachenden Punkte ist, desto leichter fällt die Sicherungsaufgabe
- Aufwand bei der Sicherung spart Aufwand im Ernstfall

Kombinations-Beispiel



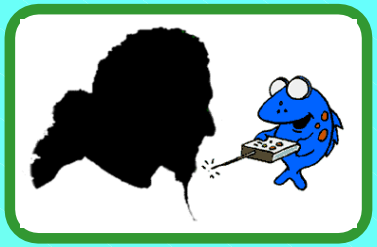


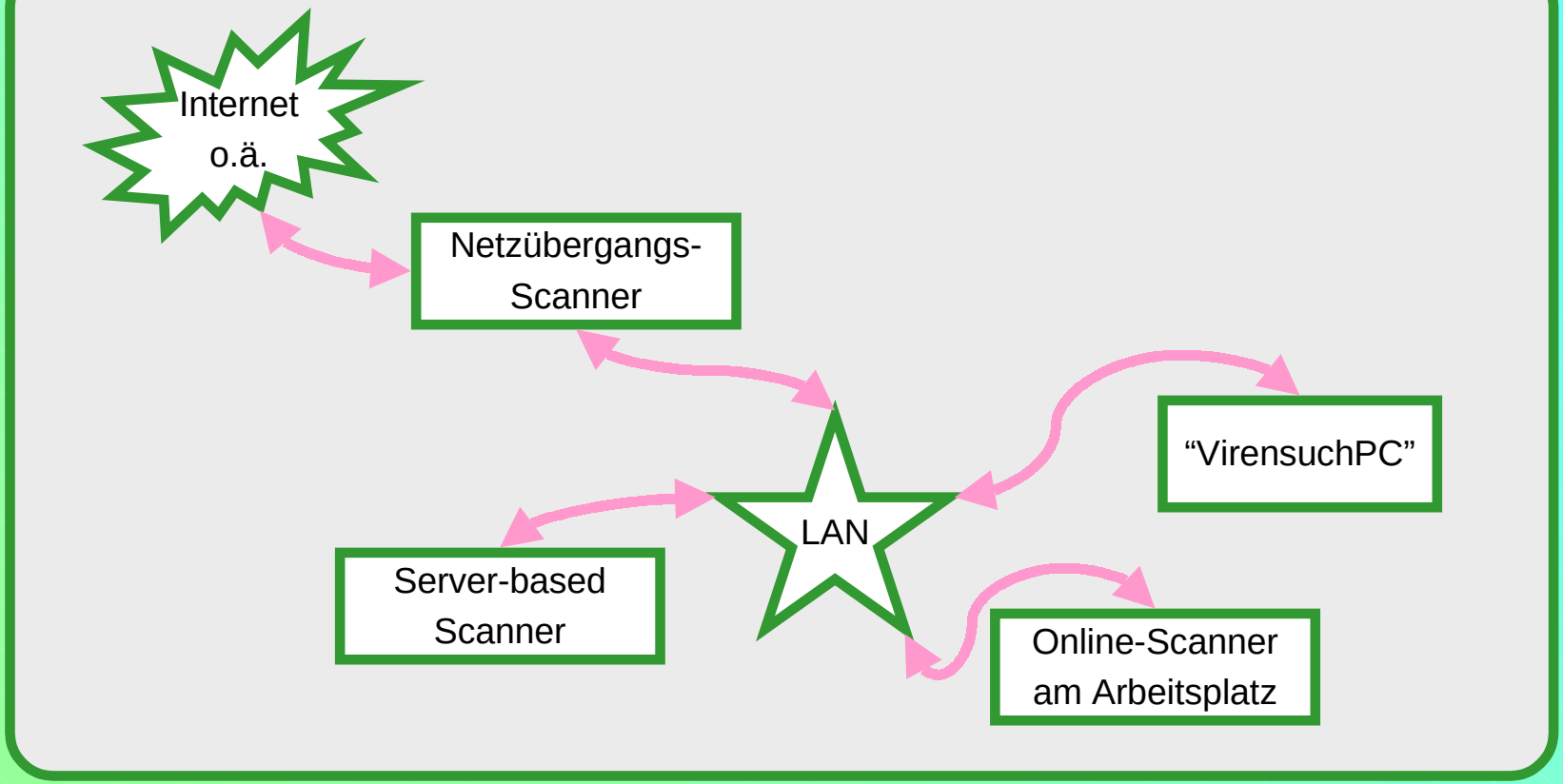
Typen destruktiver Software



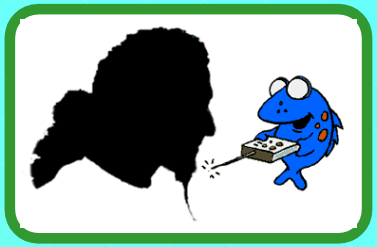
- Viren
  - Linkviren, z.B. CIH
  - Bootviren, z.B. SCA
  - Macroviren, z.B. Melissa
- Trojanische Pferde
  - Backdoors, z.B. Back Ocrifice
  - Würmer, z.B. Internet Worm
- Netzwerkattackensoftware
- defekte Software
  - z.B. mfc42.dll oder Backup-Programme ohne Restore

Hilfe gegen destruktive Software





Problempunkte Destruktiver Software

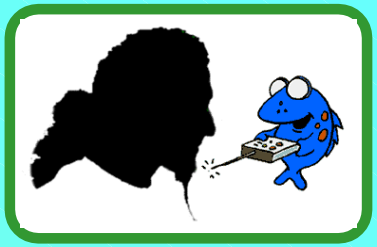


- Blauäugigkeit
  - erst handeln, wenn was passiert ist
  - trusted Beziehungen
- Aufwand
  - Produktivität wird durch Sicherheitskonzepte nicht unmittelbar erhöht
- Aktualität
  - Scanner-Update-Problematik
  - neue Technologien und Verhaltensweisen unterwandern alte Sicherheitskonzepte
  - Vielfalt ist unermeßlich, die Zahl der bekannten Exemplare destruktiver Software geht in die zehntausend
- Kompatibilität
  - durch Softwaremonopolisierung werden die Angriffsflächen immer breiter

System Security

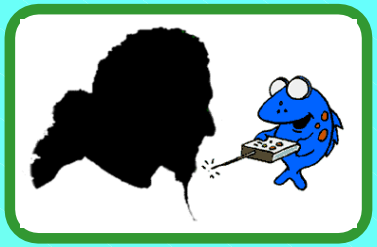
- wie Netzwerke müssen auch die darin enthaltenen Einzelsysteme zugriffssicher sein
- die Sicherung folgt ähnlichen Prinzipien, jedoch auf einer anderen Ebene
- Methoden:
  - Authentifizierung
  - Domänenbildung
  - Logging
  - mehrschichtige Sicherung
  - physikalische Maßnahmen

Authentifizierung



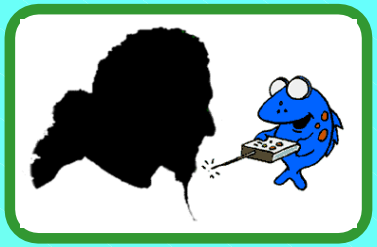
- Mittel:
  - Benutzernamen, Passworte und Rollen/Gruppen
  - eindeutige Kennzeichen wie Fingerabdrücke, Stimmabbilder, Retinascans
  - Schlüssel jeglicher Ausprägung
- Abbildung auf Access Control Lists

Domänenbildung



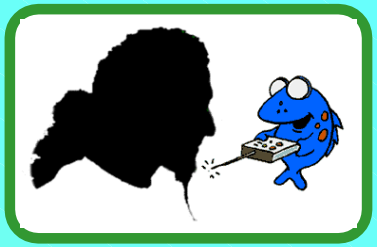
- Rollen:
  - auf einzelnen Systemen
  - auf Systemgruppen (z.B. NIS, MS-Domänenbenutzer)
- Subnetze:
  - kontrollierbare Übergänge zwischen getrennt gesicherten Systemgruppen

Schichten der Sicherung



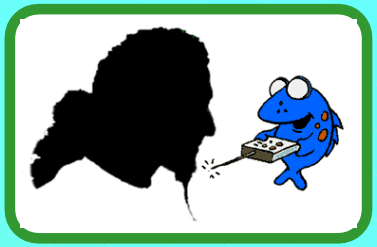
- Login
- Applikationen/Dienste
- Ressourcen
  - Filesystem
  - Speicherräume
  - I/O-Geräte
- physikalisch
  - Zugang zum System und Leitungen kontrollieren

Zusammenfassung: Konzepte



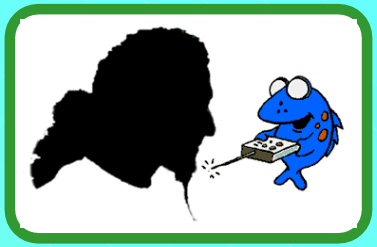
- Kombination vieler einzelner Sicherungsmechanismen
- Authentisierung und Verschlüsselung wo immer der Aufwand vertretbar ist
- Sicherheit durch Mehrstufigkeit
- Logging/Überwachung von Vorgängen
- geplant konzeptionelles Vorgehen statt Wildwuchs

Zusammenfassung: Policies



- Regeln, die Sicherheit durch Überschaubarkeit handlebar machen
  - Einschränkung der erlaubten Hard- und Softwaresysteme auf solche, die sicherbar sind
  - Einschränkung der Rechte von Rollen auf ein für ihre Arbeit nötiges Maß
  - Notfallpläne, die die Reaktion auf Sicherheitsprobleme und eindeutige Zuständigkeiten bestimmen

Tools



- TIS Firewall Toolkit
- Linux IP Filtering / Masquerading / Transparent Proxy
- die “großen”, z.B.
  - TIS Gauntlet (http://www.nai.com/products/security/prodserv/gauntlet/default.asp)
  - Checkpoint Firewall-1 (http://www.checkpoint.com/products/firewall-1/index.html)
- dedizierte Geräte, z.B. filternde Router
- Scanner, Sniffer