Firewallkonzept im Campuskartenprojekt

Thomas Hildmann, Thomas J. Wilke

Vortrag zum Treffen der Arbeitsgruppe Datensicherheit der TU Berlin

Berlin, den 21.11.2001

Gliederung

- Sicherheitstechnische Grundsätze
- Sicherheitsregeln
- Firewall-Architektur
- Zusatzanforderungen von Abteilung Ib
- Grafische Firewall und Alternativen
- Campuskartensystem und Filterfirewall
- Resümee

Sicherheitstechnische Grundsätze

Verständnis

- **Abstrakte Definition**

  Sicherheit ist ein relatives Maß, das angibt, wie wahrscheinlich ein Ereignis (oder eine Gruppe von Ereignissen) in einem definierten Umfeld eintritt.

- **Elementbezogene Definition**

  Sicherheit ist ein Maß für die Schutzbedürftigkeit von Objekten oder Subjekten in einem definierten Umfeld. Die Schutzbedürftigkeit korreliert mit der (z.B. wirtschaftlichen) Bedeutung, die dem Objekt oder Subjekt im jeweiligen Umfeld zugeschrieben wird.

Sicherheitstechnische Grundsätze

Gefährdungsursachen

Angriffe

- innere Angriffe
- äußere Angriffe
- Kombination aus äußeren und inneren Angriffen

Fehlfunktionen

- Falsche Bedienung
- Fehlerhafte Herstellung
- Unzureichendes Wirkprinzip oder Konstruktion

Kombination aus Fehlfunktion und Angriff

Sicherheitstechnische Grundsätze

Anwendungssysteme

- **Software**

  Softwaresysteme sind in der Regel nicht vollständig korrekt. D.h., diese sind auf Arbeitsprozessebene und/oder softwaretechnischer Ebene angreifbar:

  Trojaner, Buffer Overflow, Anwendungsmakros.

- **Client-Serversysteme**

  Client-Serversysteme sind aufgrund der ihnen zugrundeliegenden Wirkprinzipien angreifbar: Brute Force, Denial of Service, Kompromittierung der Kommunikation.

- **Anwendungsinteroperabilität**

  Gegenwärtige Datenverarbeitungssysteme schließen eine gegenseitige Beeinflussung von verschiedenen Anwendungen prinzipiell nicht aus.

Sicherheitstechnische Grundsätze

Kommunikation / Interaktion

Folgende Eigenschaften werden im Campuskartenprojekt für die Kommunikation / Interaktion zugrunde gelegt.

- **Autentität**
  Impliziert Sicherstellung des korrekten Gebrauchs einer Identität
- **Vertraulichkeit**
  direkte und indirekte
- **Korrektheit**
  Korrekte Korrelation zwischen Willenserklärung und Kontext
- **Verbindlichkeit**
  Voraussetzungen: Autoentität und Korrektheit

Sicherheitsregeln

Leitlinien

Einbeziehung und Umsetzung von sicherheitstechnisch relevanten Leitlinien:

- BSI-Grundschutzhandbuch
- Sicherheitsrahmenkonzept der TU-Berlin
- Sicherheitstechnische Taxonomie der Systembereiche gemäß den Leitlinien

Sicherheitsregeln

Passwortautorisation

Passwortautorisation ist bei erhöhtem Schutzbedarf unzureichend.

- organisatorischer Aufwand bei zentraler Verteilung:
  Einmal-Passwörter, Passwortverteilung, zusätzlicher Support
- Benutzerergonomie <-> Sicherheit
  schwache Passwörter, Wartezeiten <-> unsichere Aufbewahrung kryptischer Passwörter
- Unzureichende Schutzverfahren für die PWA
  Brute Force, Denial of Service, Verfügbarkeit qualitativ hochwertiger Werkzeuge zur Kompromittierung des Verfahrens

Sicherheitsregeln

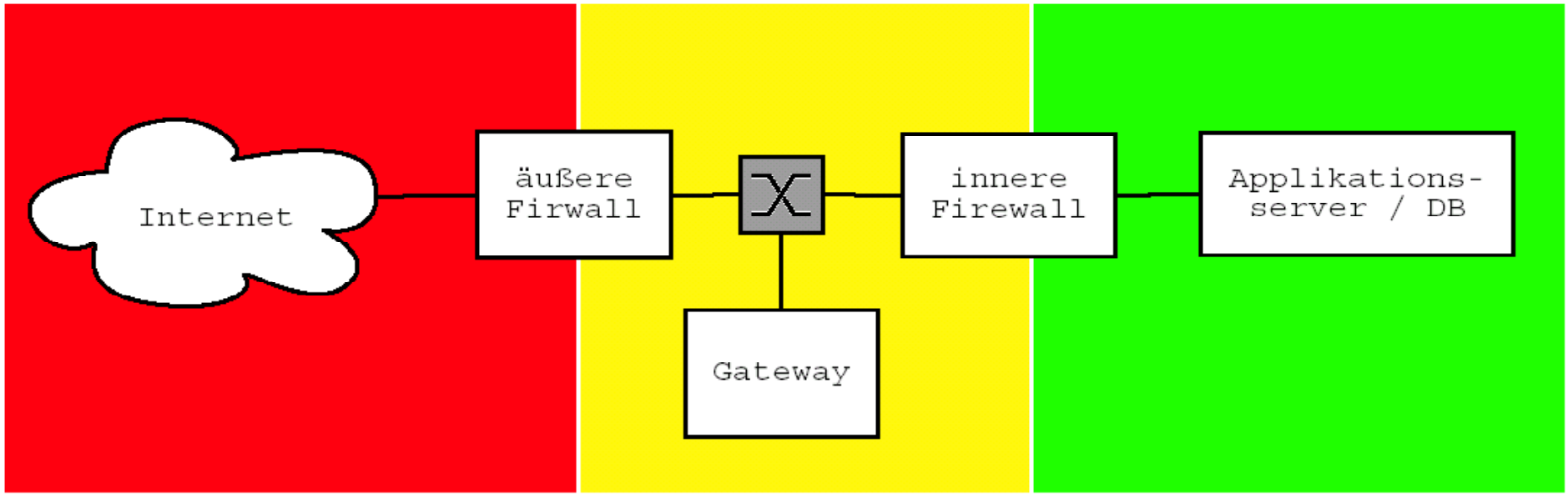
Reduzierung der Gefahrenkomplexität

- **Entkopplung von Identifikation und Autorisierung:**
  Vermeidung von Datenspuren und Wahrung der Vertraulichkeit
- **Beschränkung der direkten Kommunikationsfähigkeit:**
  Es können lediglich diejenigen Elemente direkt in Interaktion treten, die dies zur Erbringung ihrer Funktion benötigen.
- **Beschränkung der Informationsverfügbarkeit**
  Jedes Subjekt des Campuskartensystems hat lediglich auf die Daten Zugriff, die es zur Erbringung seiner Aufgaben benötigt.
- **Mehrparteienprinzip**
  Die Komponenten des Campuskartensystems sind dezentral organisiert. Jede Komponente hat lediglich die Informationen, die sie benötigt.

Firewall-Architektur

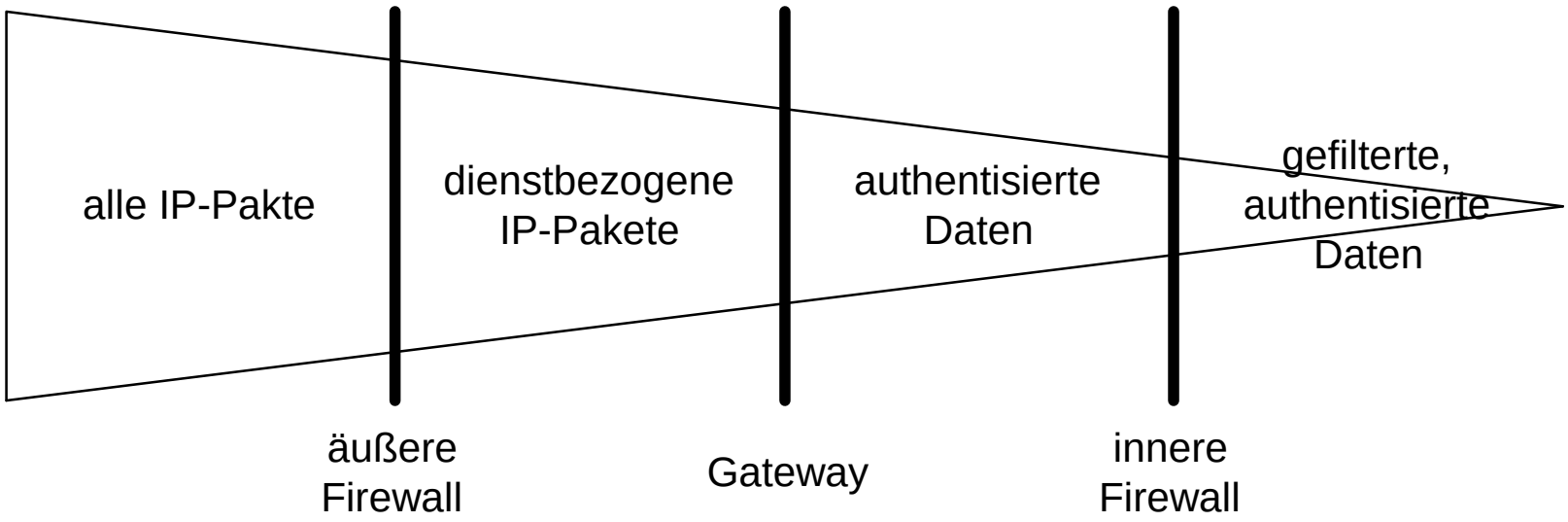
Am Beispiel der Abteilung Ib

Applikations-Firewall Typ II



Firewall-Architektur

Filterstaffelung bei Applikations-Firewalls



Firewall-Architektur

Zonen und sicherheitstechnische Taxonomie

Allgemein unterscheidet man die externe Zone, die DMZ und die interne Zone.

Spezialfall an der TU: externe Zone, DMZ, LAN und Applikationszone.

Zusatzanforderungen von Abt. Ib

- Nutzung von E-Mail und WWW von den Arbeitsplätzen aus auf denen mit personenbezogenen Daten umgegangen werden soll.
- Direkter, ungefilterter Zugriff auf das DBMS mit den personenbezogenen Daten.
- Anpassung der Software, z.B. mittels dem „Privacy Enhanced Access Controlsystems“ nicht möglich.
- Einsatz von Windows NT auf den Workstations.

Grafische Firewall und Alternativen

Alternative Lösungsansätze

1. Trennung der Verarbeitungsumgebung von sicherheits-technisch divergierenden Anwendungen. (zwei getrennte Netzwerke gemäß BSI Grundschutzhandbuch)

2. Grafische Firewall

3. Sicherung der Clients durch Anschluss an das ZUV-Netz

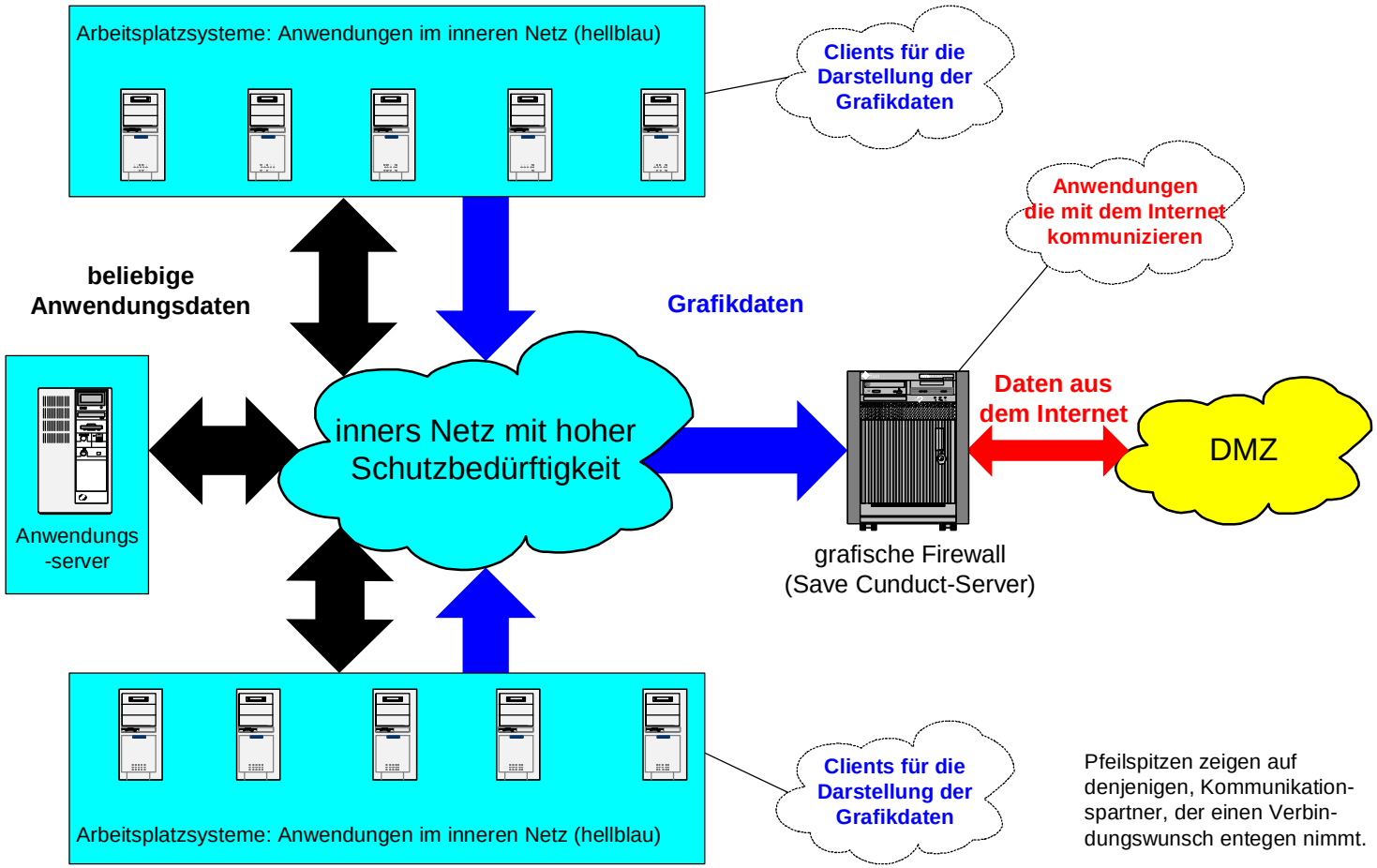
Grafische Firewall und Alternativen

Getrennte Verarbeitungsumgebung

- Vorteil:
  - Die Sicherheit der personenbezogenen Daten wird auf keinen Fall gefährdet.
- Nachteile:
  - Doppelter Platz und Wartungsaufwand
  - Vergleichsweise hohe Kosten
  - Keine idealen Arbeitsbedingungen

Grafische Firewall und Alternativen

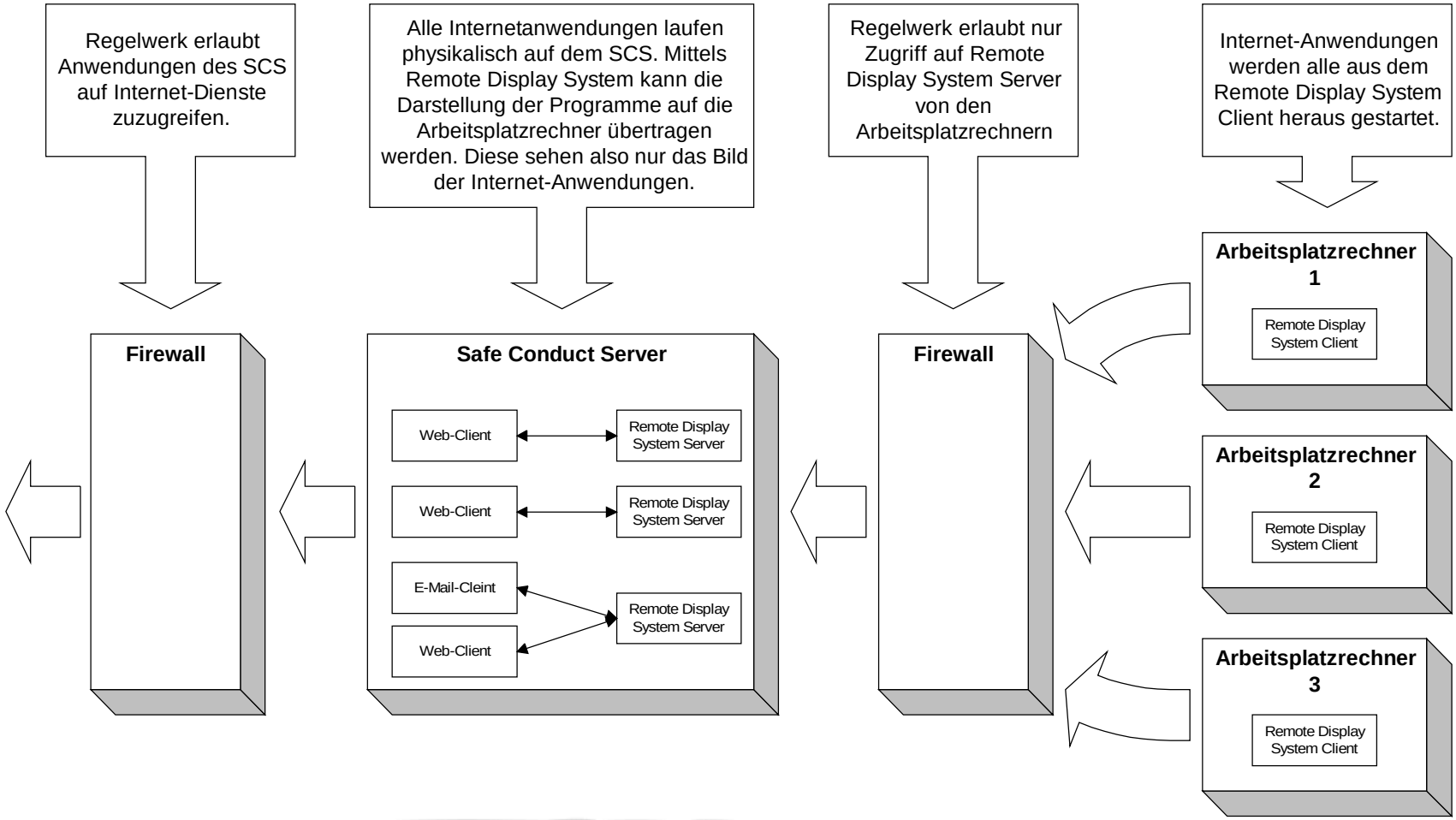
Funktionsprinzip einer grafischen Firewall



Pfeilspitzen zeigen auf denjenigen, Kommunikation-spartner, der einen Verbin-dungswunsch entegen nimmt.

Grafische Firewall und Alternativen

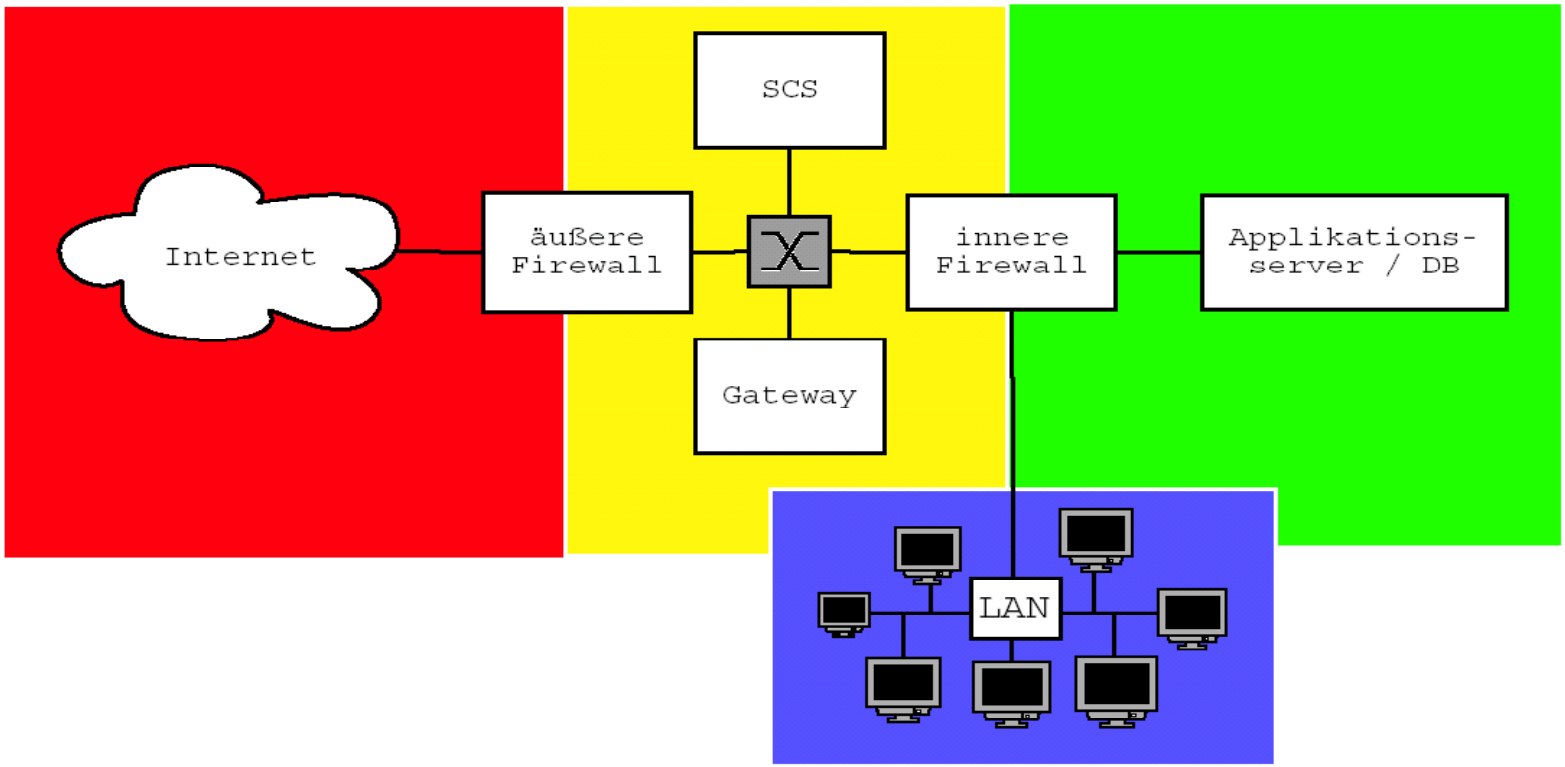
Funktionsprinzip einer grafischen Firewall



Grafische Firewall und Alternativen

Firewallkonfiguration

Applikations-Firewall Typ IIIb



Grafische Firewall und Alternativen

Gegenüberstellung: GFW versus FFW

- Es findet kein direkter Datenaustausch zuwischen offenem und internem Netz statt.
- Daten aus dem offenen Netz werden auf der GFW verarbeitet.
- Lediglich Bilddaten erreichen interne Netzknoten.
- Keine derartig mögliche Gefährdung
- Interne Netzknoten sind immer Verbindungsinitiator.

- Es findet ein direkter Datenaustausch zwischen offenem und internem Netz statt.
- Daten aus dem offenen Netz werden auf internen Netzknoten verarbeitet.
- Daten aus offenem Netz werden nur gefiltert & erreichen interne Netzknoten (Filterregeln).
- Filterregeln sind konfigurierbar.
- Externe Netzknoten können Verbindungsinitiatoren sein.

Grafische Firewall und Alternativen

Gegenüberstellung: GFW versus FFW

- Internes Netz ist vor unbekannten Angriffen geschützt.
- Kompromittierungsbereich auf eine Sitzung bzw. auf GFW begrenzt.
- Mehrere strukturell unterschiedliche Kompromittierungsverfahren sind nötig, um das interne Netz zu erreichen.
- Mehrstufiges Sicherungsverfahren
- GFW muss über hohe Rechenleistung verfügen.
- Keine Implikationen bei Einführung neuer Applikationen

- Internes Netz kann nur vor bekannten Angriffen geschützt werden.
- Kompromittierungsbereich kann sich auf bis zu alle internen Netzknoten erstrecken.
- Mit einem Kompromittierungsverfahren kann das innere Netz erreicht werden.
- Einstufiges Sicherungsverfahren
- Bei Kontenfilterung muss FFW über hohe Rechenleistung verfügen.
- Gegebenfalls hoher Aufwand bei Einführung neuer Applikationen.

Campuskartensystem und FFW

- Funktionsverfahren des Campuskartensystems erfordern eine offenere FFW-Konfiguration als diejenigen, die das Sicherheitskonzept der ZUV vorsieht.
- Filterfirewalls können die Kompromittierung von Bereichen mit hoher Schutzbedürftigkeit nicht im vergleichbaren Maße verhindern wie GFW aufgrund der unterschiedlichen Wirkungsprinzipien.

Resümee

- Der Bereich Ib hat eine hohe Schutzbedürftigkeit aufgrund der dort verarbeiteten personenbezogenen Daten. Es sollen dort sicherheitskritische Anwendungen zum Einsatz kommen.
- Das Konzept der grafischen Firewall ist die konsequente Weiterentwicklung der „Urfirewallsysteme“. Mit ihm wird eine „galvanische“ Trennung von Computernetzen realisiert.
- Funktionsverfahren des Campuskartensystems funktionieren nicht mit der gegenwärtigen ZUV-FW-konfig.

Weiter Informationen

Ansprechpartner / Vortrag

Ansprechpartner: Thomas Hildmann
hildmann@prz.tu-berlin.de

Thomas J. Wilke
tjw@prz.tu-berlin.de

Vortrag: https://bach.prz.tu-berlin.de/events/FW-CKP/