e-Government und IT-Sicherheit

Dipl.-Inform. Frank Losemann
losemann@actisis.com

Institut f. Telematik, Trier
und Actisis GmbH

Vortragsüberblick

- Anforderungen an
  - …IT-Sicherheit durch e-Government
  - …IT-Entwicklung und Betrieb durch IT-Sicherheit
- Herausforderung IT-Sicherheit
  - IT-Sicherheit als Prozess
  - IT-Sicherheit für und mit Menschen Bedienbarkeit, Beherrschbarkeit

Definition

Electronic Government (e-Government) bezeichnet die Nutzung des Internets und anderer elektronischer Medien zur Einbindung der Bürger und Unternehmen in das Verwaltungshandeln sowie zur Verwaltungsinternen Zusammenarbeit.

Quelle: E-Government Handbuch des BSI.

Beispiele

- Umfassende Informationen zu Verwaltungsvorgängen
- Online-Formulare
- Elektronische Anträge
- Per E-Mail zugestellte Bescheide
- Online-Bürgersprechstunden
- Diskussionsforen

Quelle: E-Government Handbuch des BSI.

Sicherheitsbegriff in 3 Aspekten

- Sicherheit (engl. Security)
  - Authentizität
  - Integrität
  - Vertraulichkeit
  - Verbindlichkeit, Nichtabstreitbarkeit
- Sicherheit (engl. Reliability)
  - Verfügbarkeit
- Sicherheit (engl. Safety)
  - Betriebssicherheit

Sicherheitskonzepte

- Menschen, Prozesse, Technologie
- Schwachstellen, Bedrohungen, Angriffe
- Sicherheits-
  - Strategie
  - Management
  - Bewusstsein

Vorgehensmodell

1. Analyse Status quo, Schutzbedarf
2. Formulierung Policy, Standards
3. Einbettung in Organisation
4. Einbettung in Technik
5. Überprüfung, Audits
6. Administration der IT-Sicherheit

Policies + Standards in der Praxis

Beispiel: Rolle Netzwerkmanager

- Szenario: Grosses Unternehmen mit mehreren Standorten
- Zentrale kauft Sicherheitskonzept für alle Netzwerke und beschließt die Umsetzung

Policies + Standards in der Praxis

Beispiel: Rolle Netzwerkmanager

- Ziel: Klare Zuständigkeiten, Ansprechpartner, Reaktionszeit
- Gegenstand: Durch Policy und Standards **redefinierte** Rolle mit neuen Rechten + Pflichten

Policies + Standards in der Praxis

Beispiel: Rolle Netzwerkmanager

- Neue Definition: Auswahl der **einen** Person anhand der Fähig-, Tätig- und Verantwortlichkeiten
- Einführung erfordert Reorganisation und Delegation von kritischen Aufgaben nach "unten" und Bündelung von Kompetenzen ggf. über Abteilungsgrenzen hinweg

Policies + Standards in der Praxis

Beispiel: Rolle Netzwerkmanager

- Erfolgskontrolle: Um eine mögliche verschleppte, unvollständige Umsetzung von Sicherheitsstandards zu entdecken bzw. zu verhindern, ist häufig eine **extern** eingekaufte Prüfung sinnvoll.

Organisierte Sicherheit

Detaillierung der Standards in Sicherheits

- Richtlinien
- Rollen
- Prozesse
- Domänen
- Marketing

Sicherheitsmarketing

- Blickwinkel auf IT-Sicherheit
  - Verhinderer
  - Überwacher
  - Kostentreiber
  - **"Business / eGov Enabler"**
- Angemessene Sicherheit
  - stetige Überprüfung, Anpassung

Sicherheits-Tests

- Funktionale Fehler fallen auf, was ist mit Sicherheitslücken?
- Sicherheitsprobleme können in organisatorischen und technischen Verfahren liegen
- Seiteneffekte von Upgrades und Konfigurationsänderungen
- Interne + externe Kompetenz stetig zur Überprüfung nutzen

S.-Technologien

Actisis IT consulting

SSL	CRL	RSA	IDS	WSDL
TLS	OCSP	DH	DRM	SOAP
IPsec	DES	ECC	OTP	XMLEnc
VPN	3DES	MD5	ACL	XMLSig
S/MIME	AES	SHA1	CHAP	XKMS
PKI	IDEA	SHA256	EAP	XrML
X.509	RC2	SET	PAM	SAML
PKCS	RC5	EFS	SSO	XACML

S.-Technologien

SSL	CRL	RSA	IDS	WSDL
TLS	OCSP	DH	DRM	SOAP
IPsec	DES	ECC	OTP	XMLEnc
VPN	3DES	MD5	ACL	XMLSig
S/MIME	AES	SHA1	CHAP	XKMS
PKI	IDEA	SHA256	EAP	XrML
X.509	RC2	SET	PAM	SAML
PKCS	RC5	EFS	SSO	XACML

- Fokus: Integrität

S.-Technologien

SSL	CRL	RSA	IDS	WSDL
TLS	OCSP	DH	DRM	SOAP
IPsec	DES	ECC	OTP	XMLEnc
VPN	3DES	MD5	ACL	XMLSig
S/MIME	AES	SHA1	CHAP	XKMS
PKI	IDEA	SHA256	EAP	XrML
X.509	RC2	SET	PAM	SAML
PKCS	RC5	EFS	SSO	XACML

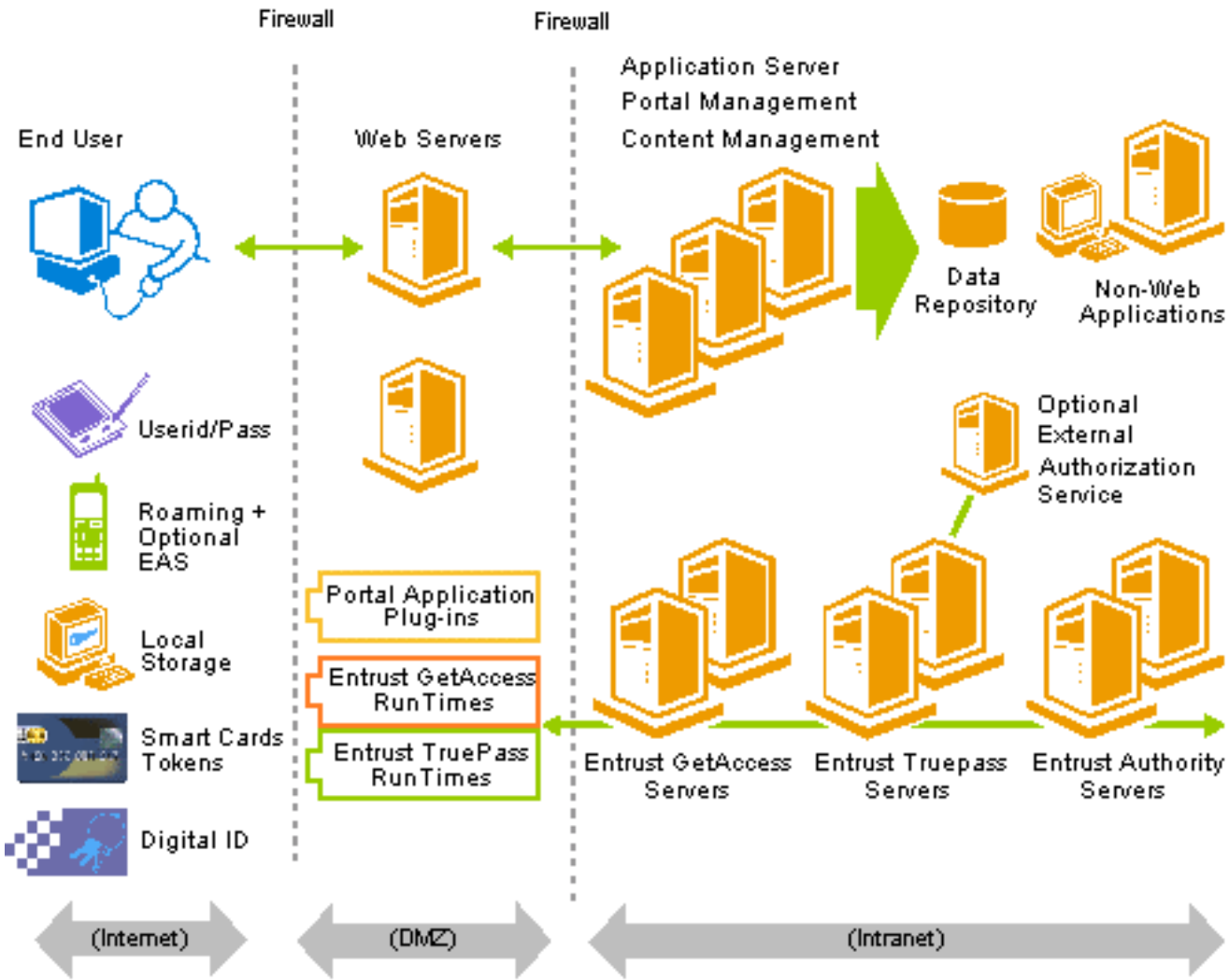
- Fokus: Authentizität

S.-Technologien

SSL	CRL	RSA	IDS	WSDL
TLS	OCSP	DH	DRM	SOAP
IPsec	DES	ECC	OTP	XMLEnc
VPN	3DES	MD5	ACL	XMLSig
S/MIME	AES	SHA1	CHAP	XKMS
PKI	IDEA	SHA256	EAP	XrML
X.509	RC2	SET	PAM	SAML
PKCS	RC5	EFS	SSO	XACML

- Fokus: Vertraulichkeit

S.-Architektur Web-Portal



Quelle: Entrust™ Website

Informationstechnik im eGovernment

- Client-Server-Architekturen
- Workflow-Systeme
- Internet-Technologien
- bestehende behördeninterne IT-Landschaft
- verfügbare E-Government-Lösungen (auch anderer Behörden)

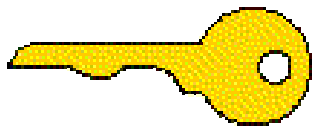
IT-Sicherheit und Datenschutz

Schwerpunkte im e-Government:

- Sicherheitsmanagement
- Verschlüsselung und Signaturen
- Authentisierungsmechanismen
- IT-Grundschutz
- Firewall-Technologie

Kryptografie

- Kerckhoffs Prinzip
- Symmetrische Kryptografie **geheime Schlüssel**

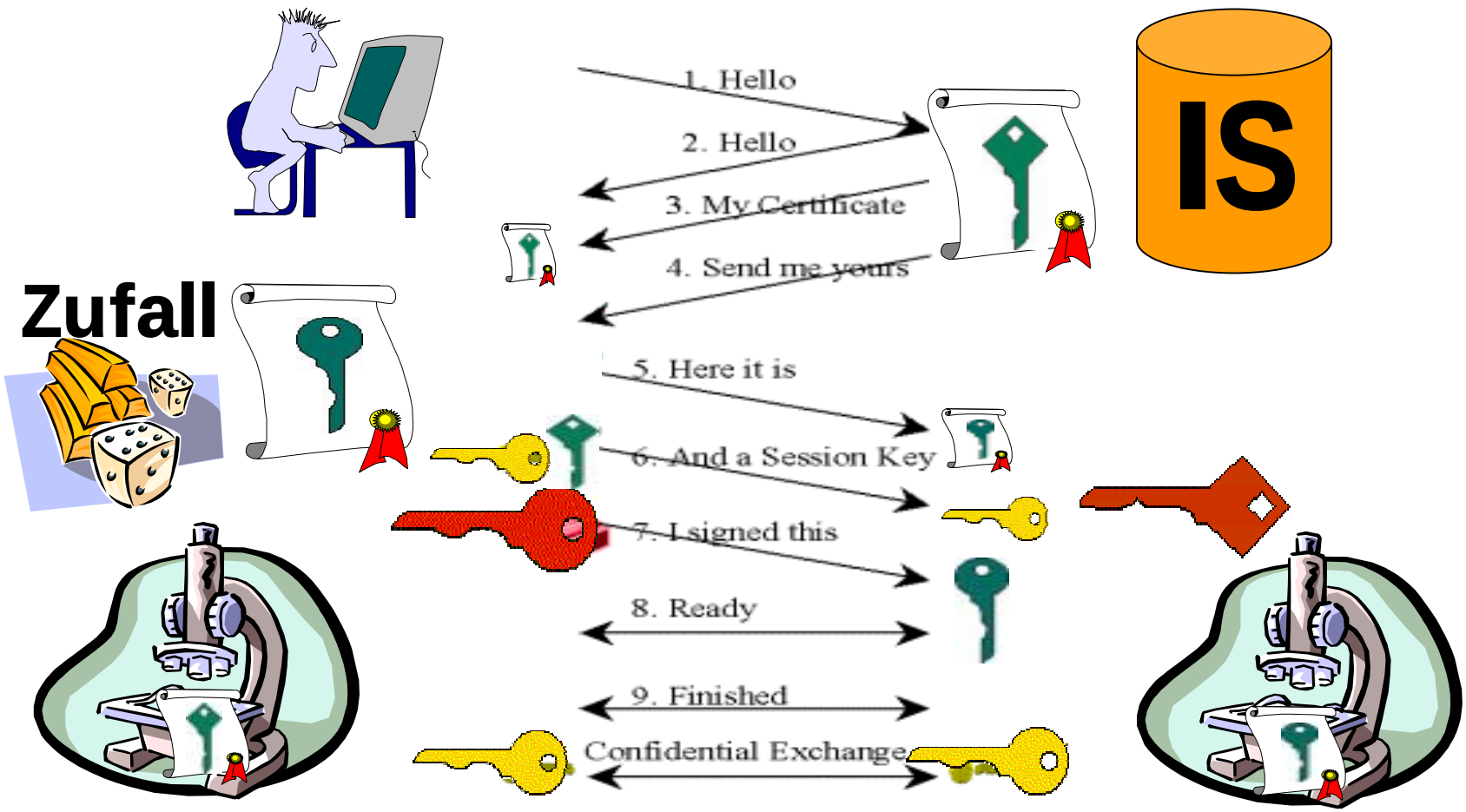


- Asymmetrische Kryptografie **private und öff. Schlüssel**

- **Zertifikate** - erleichtern das Schlüsselverteilungsproblem

- **Public-Key-Infrastruktur** Vertrauens-Management, PK-Bereitstellung, ID-Management

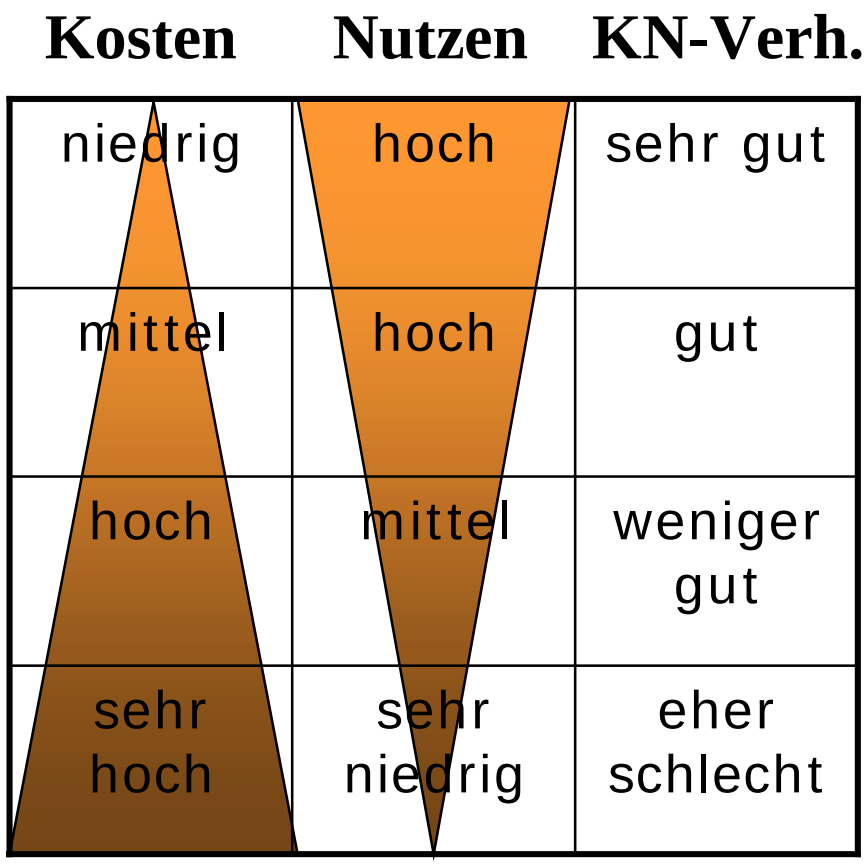
Anwendungsbeispiel SSL-Verbindung



Authentisierung durch Nutzung des Private Keys zum Zertifikat!

Verschlüsselung und Signaturen

- Authentisierung
- Digitale Signatur (formfreier Bereich)
- Sichere E-Mail
- Digitale Signatur (formgebundener Bereich)



Kosten	Nutzen	KN-Verh.
niedrig	hoch	sehr gut
mittel	hoch	gut
hoch	mittel	weniger gut
sehr hoch	sehr niedrig	eher schlecht

Quelle: vgl. KES 2003#1 Prof. Reimer

Anwendungen von Zertifikaten

- Authentizität von Daten (SSL / TLS)
- Signieren und Verschlüsseln von E-Mails
- Signieren von mobilem Code
- Authentikation von Benutzern
- Secure-SSO

- Elektronische Signatur

IT-Sicherheit und Datenschutz

Actisis IT consulting

Schwerpunkte im e-Government:

- Sicherheitsmanagement
- Verschlüsselung und Signaturen
- Authentisierungsmechanismen
- IT-Grundschutz
- Firewall-Technologie

Authentisierungs-Mechanismen

- Einteilung
  - Authentisierung durch **Wissen**
  - Authentisierung durch **Besitz**
  - Authentisierung durch **Eigenschaften** (Biometrie)
- Kombinationen sind möglich
  - Bsp: Smartcard + PIN
    (Besitz) (Wissen)

IT-Sicherheit und Datenschutz

Actisis IT consulting

Schwerpunkte im e-Government:

- Sicherheitsmanagement
- Verschlüsselung und Signaturen
- Authentisierungsmechanismen
- IT-Grundschutz
- Firewall-Technologie

IT-Grundschutz

Loseblattsammlung/Cd-Rom des BSI

- Konkrete Vorlage zum Umsetzen einer Sicherheitsstrategie
- Einteilung in Bausteine für Einzelplatz, Netzwerkrechner, Firewalls, Verkabelung...
- Beschreibung typischer Bedrohungen und Einschätzungen

IT-Grundschutz (2)

Actisis IT consulting

Für alle Module systematische Behandlung der Schichten

1. übergeordnete Aspekte
2. Infrastruktur
3. Komponenten
4. Netze
5. Anwendungen

IT-Grundschutz (3)

Empfehlung unterschiedlich aufwendiger "Standard" Sicherheits-Maßnahmen für eine Anforderung.

IT-Grundschutz (4) Zertifizierbarkeit

Nachweis, dass Sicherheitsmaßnahmen nach IT-Grundschutzhandbuch realisiert sind:

- Fremdbestätigt durch zugelassene Stellen
- 2 Vorstufen durch Selbsterklärung:
  - „IT-Grundschutz Einstiegsstufe“
  - „IT-Grundschutz Aufbaustufe“

IT-Sicherheit und Datenschutz

Actisis IT consulting

Schwerpunkte im e-Government:

- Sicherheitsmanagement
- Verschlüsselung und Signaturen
- Authentisierungsmechanismen
- IT-Grundschutz
- Firewall-Technologie

Firewall-Technologie Definition Ziele

- Kombination aus Hard- und Software-Komponenten
- Ziele:
  - Schutz des Intranets vor unerwünschten Zugriffen
  - Kontrollierter und eingeschränkter Zugang
  - Sicherer Zugang zu externen Ressourcen

Firewall-Technologie Charakteristika

- Sämtlicher Datenverkehr zwischen Intranet und Internet erfolgt ausschließlich über die Firewall
- Nur autorisierter Datenverkehr darf die Firewall passieren
- Die Firewall ist selbst unangreifbar (besonders sicher)

Sicherheitsleitlinien für Firewalls

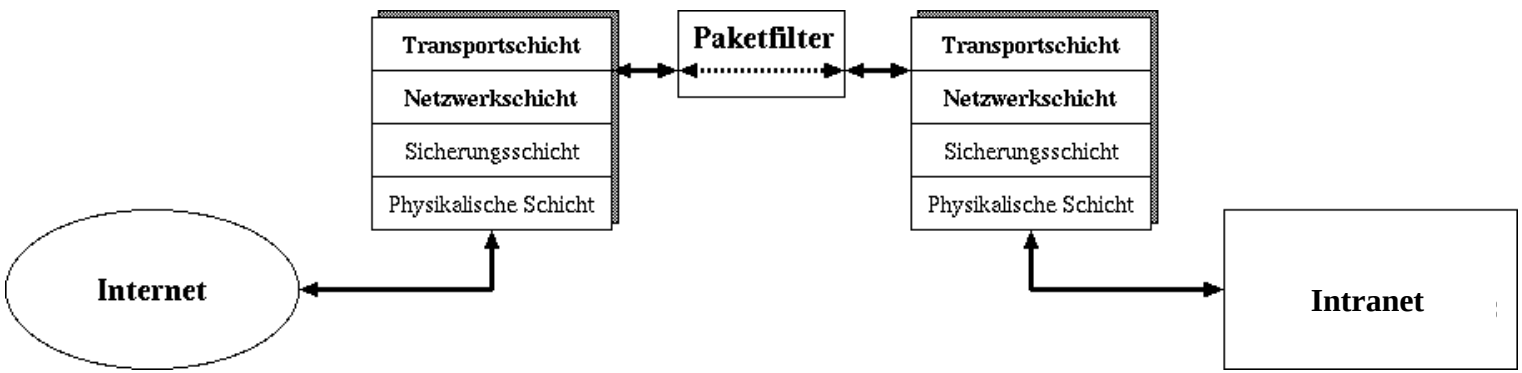
- Der Betrieb einer Firewall ist ohne IT-Sicherheitsleitlinie sinnlos!
  - Klärung der Sicherheitsziele und Verantwortlichkeiten
  - Identifizierung der schützenswerten Systeme und deren Anforderungen
  - Definition von Notfallprozeduren

Klassifikation von Firewalls

- Paketfilter
- Application-Gateways
- ...
- Personal Firewalls

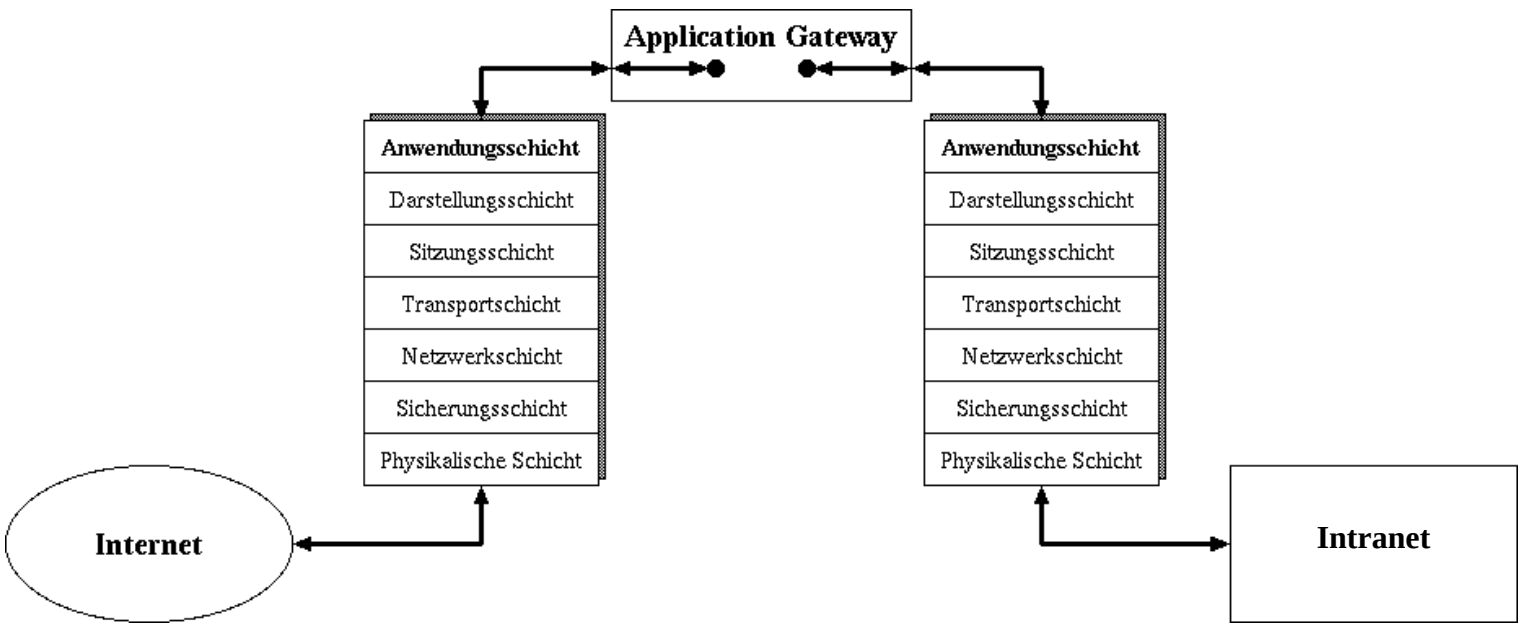
Paketfilter

- Filterung von Datenpaketen auf Netzwerk- und Transport-Schicht



Application Gateways

- Inhaltsfilterung auf der Applikationsebene



Rückblick

Schwerpunkte IT-Sicherheit im e-Government:

- Sicherheitsmanagement
  - Strategien, Standards, Richtlinien, Audits
- Verschlüsselung und Signaturen
- Authentisierungsmechanismen
- IT-Grundschutz
- Firewall-Technologie

Fazit

- Die öffentliche Verwaltung ist als Herrin der e-Government-Verfahren selbst in der Pflicht, IT-Sicherheit zu gewährleisten und auch zu überprüfen.

Hinweis

Actisis IT consulting

Die Folien zum Vortrag werden nach der Veranstaltung unter

http://www.actisis.com/kdw2003

online verfügbar gemacht.

E-Mail: losemann@actisis.com