Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

E-Mail Sicherheit

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

E-Mail Sicherheit
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Cyber-Sicherheitsprobleme
- E-Mail-Verschlüsselung
- Zusammenfassung

E-Mail Sicherheit
→ Inhalt

- **Ziele und Ergebnisse der Vorlesung**
- Cyber-Sicherheitsprobleme
- E-Mail-Verschlüsselung
- Zusammenfassung

Ziele und Ergebnisse der Vorlesung
→ E-Mail Sicherheit

- Gutes Verständnis für die generellen **Cyber-Sicherheitsprobleme** des E-Mail-Dienstes.

- Erlangen der Kenntnisse über die E-Mail-Sicherheitslösungen: **PGP**, **S/MIME** und **E-Mail-Gateways**.

E-Mail Sicherheit
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- **Cyber-Sicherheitsprobleme**
- E-Mail-Verschlüsselung
- Zusammenfassung

Cyber-Sicherheitsprobleme
→ Weltweit kann jeder E-Mails versenden! (1)

- Sehr gute Eigenschaft für **gewünschte** E-Mails!

- Problematisch für **ungewollte** E-Mails (Werbung, politische Inhalte, kriminelle Absichten, …) → „**Spam**“.

- **Kritisch** bei E-Mails mit **Malware** (Viren, Würmen, Trojanern …) oder auch **Phishing E-Mails**.
  - ***Händische Ausführung*** eines E-Mail-Anhangs.
  - ***Verlinken aus der E-Mail*** heraus auf eine kompromittierte Webseite.
  - ***Automatisch durch Ausnutzung einer Sicherheitslücke*** in dem benutzten E-Mail Programm.

Cyber-Sicherheitsprobleme

→ Weltweit kann jeder E-Mails versenden! (2)

- Aus diesen Gründen müssen geeignete Anti-Malware-Systeme in die E-Mail-Infrastruktur eingebunden werden.
- Die Nutzer müssen die Gefahren kennen.
- Die eigene E-Mail-Infrastruktur verhindert das Senden nicht und der Sender wird nicht eindeutig verifiziert.
- Laut einer Studie der ENISA ist der **Spam-Anteil** größer als **95 %** in der E-Mail-Infrastruktur.
- Schlecht konfigurierte und betriebene E-Mail-Server sind eine Gefahr.

Cyber-Sicherheitsprobleme
→ Eine E-Mail ist wie eine Postkarte! (1)

- Es wird vom E-Mail-Dienst **keine Vertraulichkeit** garantiert!
  - Gewährleistung nur auf dem Transportweg vom Client zum ersten Mail-Server.
  - Passworte, Kreditkartennummern und Bankdaten sowie vertrauliche Unternehmensinformationen, wie Kundendaten, Entwicklungsdaten, Kalkulationen, usw. sind ansonsten im **Klartext** zugreifbar!
- Die Möglichkeiten eine E-Mail abzugreifen sind sehr hoch.
  - In einigen Ländern werden alle E-Mails analysiert.
  - Untersuchungen und Befragungen zeigen auf, dass weniger als 4 % aller E-Mails verschlüsselt werden.
  - Es wird aber auch aufgezeigt, dass über 40 % der E-Mails in Business-Prozessen verwendet werden.

Cyber-Sicherheitsprobleme
→ Eine E-Mail ist wie eine Postkarte! (2)

- Aus diesem Grund sollten zusätzliche **E-Mail-Verschlüsselungstechnologien** eingesetzt werden.

- In Unternehmen muss eine **Sensibilisierung** für E-Mail-Verschlüsselung geschaffen werden.

Cyber-Sicherheitsprobleme
→ Fehlende Nachweisbarkeit (1/2)

- Der Absender einer E-Mail und die Echtheit des Inhaltes einer E-Mail können nicht verifiziert werden.
  - Gab es Manipulationen während der Übertragung?
- Außerdem können Sender und Empfänger nicht sicher sein, mit wem sie E-Mails austauschen.
- Die Gewissheit, dass eine E-Mail angekommen ist (Bestellungen, usw.) hängt von der **Qualität von E-Mail-Servern** anderer ab, auf die der Sender keinen Einfluss hat (vertraglich, rechtlich, …).
- Die Verbindlichkeit einer Bestellung durch eine E-Mail (Zimmer, Tagungsräume, usw.) ist nicht zweifelsfrei möglich, da der Sender jede E-Mail-Adresse annehmen kann.

Cyber-Sicherheitsprobleme
→ Fehlende Nachweisbarkeit (2/2)

- Mit Hilfe einer **digitalen Signatur** auf der Basis von **Public-Key-Verfahren** kann eine E-Mail signiert werden und damit ist eine gesetzliche **Verbindlichkeit** von E-Mails realisierbar.

- Außerdem werden auf der Geschäftsebene Sicherheitsfunktionen gebraucht, die z.B. durch die Bestätigung des Empfangs auf der Anwendungsebene oder auf der Infrastrukturebene Verbindlichkeit herstellen.

E-Mail Sicherheit
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Cyber-Sicherheitsprobleme
- **E-Mail-Verschlüsselung**
- Zusammenfassung

E-Mail-Verschlüsselung
→ Überblick

- Bis auf einige isolierte **PGP- und S/MIME**-Inseln, gibt es in der Praxis kaum fundierte Cyber-Sicherheitskonzepte für unternehmensweite und übergreifende E-Mail-Verschlüsselungslösungen.

- Die Ursachen für die geringe Nutzung sind:
  - Unwissen über die Risiken.
  - Hohe Kosten für die E-Mail-Verschlüsselungsinfrastruktur (z.B. durch Clientsoftware, Token, Lesegeräte, Rollout, Helpdesk, Zertifikatsmanagement, usw.).

E-Mail-Verschlüsselung

→ End-to-End Verschlüsselungslösungen (1)

- End-to-End Verschlüsselungslösungen für E-Mails haben sich in der Praxis kaum durchgesetzt.

- Neben den hohen Kosten und aufwendiger Administration kranken die End-to-End-Lösungen an den folgenden **Problemfeldern**:
  - **Interoperabilitätsprobleme**, insbesondere bei unternehmensübergreifender und produktübergreifende Verschlüsselung
  - **Message-Recovery-Problematik**
  - **Vertreter-Regeln**
  - **Malware-Problematik in E-Mail-Anhängen** (Testen nicht möglich, da verschlüsselt)

E-Mail-Verschlüsselung

→ End-to-End Verschlüsselungslösungen (2)

- End-to-End Konzepte sind individuelle Konzepte, d.h. sie benötigen so viele Schlüssel wie Mitarbeiter im Unternehmen sind.
  - Zugriff muss auch nach Ausscheiden eines Mitarbeiters gewährleistet werden.
  - Die Schlüssel der Mitarbeiter müssen bei diesen Konzepten entweder an zentraler Stelle hinterlegt werden, oder jede E-Mail muss zusätzlich mit einem „Hauptschlüssel“ - also doppelt - verschlüsselt werden.
  - Die gleiche Problematik gilt für die Vertretung bei Abwesenheit des Mitarbeiters.

E-Mail-Verschlüsselung

→ End-to-End Verschlüsselungslösungen (3)

- Bei der Prüfung verschlüsselter Mail-Anhänge auf Malwarebefall wären aufwendige Umverschlüsselungen erforderlich, da Anti-Malware-Programme nur im Klartext die Anhänge analysieren können.
  - Hier müssen dann auf den IT-Systemen besondere Anti-Malware-Maßnahmen getroffen werden, um nach der Entschlüsselung die Anhänge auf Malwarebefall zu untersuchen (z.B. SSL/TLS Interception mittels Proxy Server).

E-Mail-Verschlüsselung

→ PGP und S/MIME sowie deren Unterschiede (1)

- **PGP (GNUPGP)** und **S/MIME** sind E-Mail-Sicherheitslösungen, die sich weitestgehend auf dem Markt als Standards für die Sicherheit von E-Mails etabliert haben.
  - Beide E-Mail-Sicherheitslösungen sind zueinander **nicht kompatibel**.
  - Im Wesentlichen unterscheiden sich die Konzepte beider Standards beim verwendeten **Nachrichtenformat**, **Vertrauensmodell**, **Schlüsselformat** und der **Schlüsselverwaltung**.

E-Mail-Verschlüsselung

→ PGP und S/MIME sowie deren Unterschiede (2)

- **Nachrichtenformat:**
  - S/MIME baut auf dem **Multipurpose Internet Mail Extension (MIME)** Datenformat auf, das auch von regulären E-Mails als Datenformat genutzt wird.
  - S/MIME nutzt lediglich eine Erweiterung des MIME-Datenformats, das um zusätzliche kryptographische Elemente erweitert wurde.
  - Durch diese gemeinsame Grundlage ist die Nutzung von S/MIME auf vielen E-Mail-Programmen ohne weiteres möglich.
  - PGP benötigt hingegen **zusätzliche Erweiterungen und Software**, um seine kryptographischen Funktionen erfüllen zu können.
  - PGP ist aus einem anfangs privaten Projekt entstanden. *(Phil Zimmermann)*
  - S/MIME wurde von einem Konsortium von Herstellern entwickelt.

E-Mail-Verschlüsselung

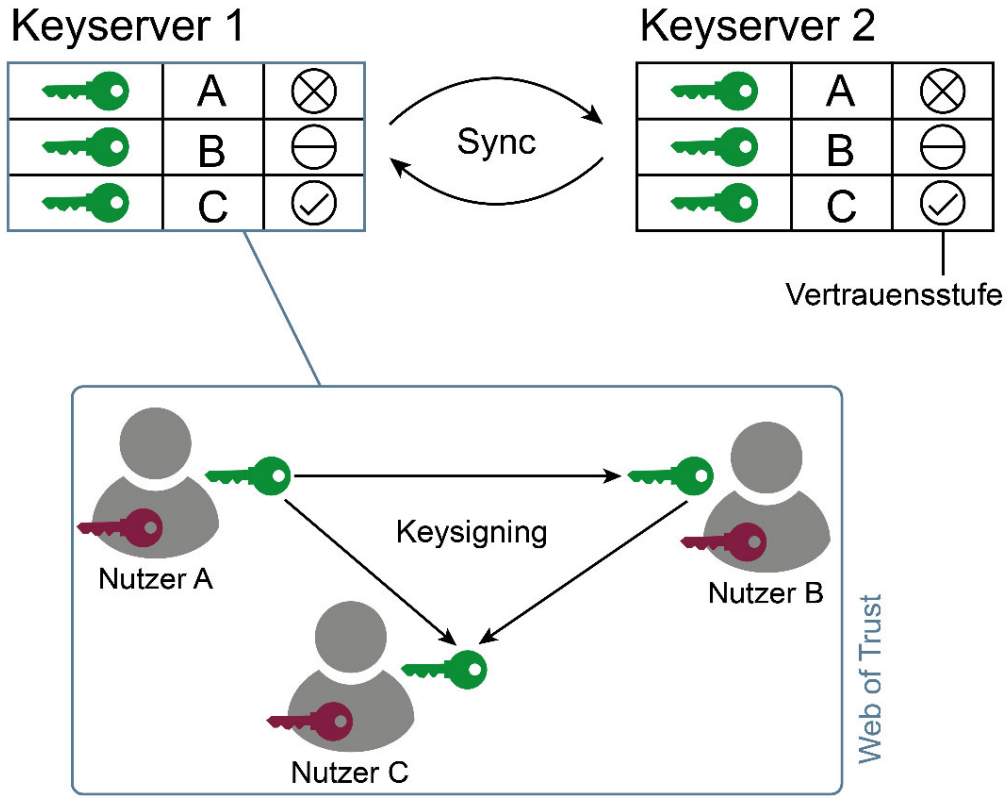
→ PGP und S/MIME sowie deren Unterschiede (3)

- **Vertrauensmodelle:**
  - Bei jedem Public Key Verfahren stellt das Cyber-Sicherheitsbedürfnis **Gewährleistung der Authentizität der öffentlichen Schlüssel** eine besondere Aufgabe da.
  - Die Vertrauensstruktur ist bei beiden E-Mail-Sicherheitslösungen PGP und S/MIME sehr unterschiedlich.
  - Um die Authentizität eines öffentlichen Schlüssels der Nutzer zu gewährleisten, gibt es **verschiedene Vertrauensmodelle** für unterschiedlichen Public-Key-Lösungen.

E-Mail-Verschlüsselung

→ Prinzipielles Vertrauensmodell von PGP

- Dezentrale Vertrauensstruktur - **„Web of Trust“**:
  - Keine zentrale administrative Instanz.
  - Jeder Nutzer kann einen öffentlichen Schlüssel signieren und somit zur Vertrauenswürdigkeit der Authentizität beitragen.



E-Mail-Verschlüsselung

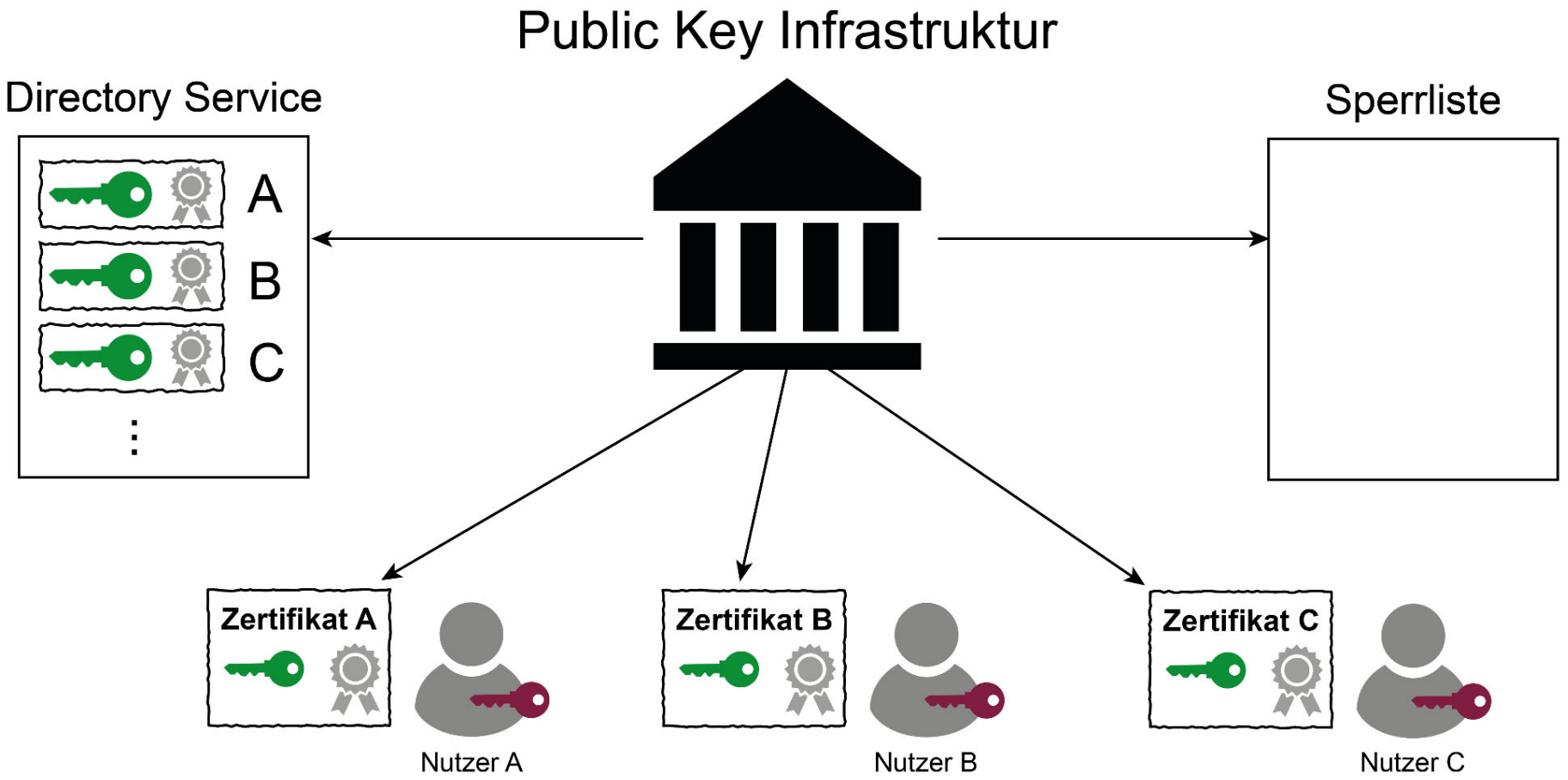
→ Prinzipielles Vertrauensmodell von S/MIME (1)

- Gewährleistung der Authentizität des öffentlichen Schlüssels durch **elektronische Zertifikate**, die von **Zertifizierungsinstanzen** erstellt werden.
  - Stark hierarchisches und zentralisiertes Vertrauensmodell.

- Es gibt drei unterschiedliche Klassen von Zertifikaten:
  - **Klasse-1:** Die Echtheit der E-Mail-Adresse wird verifiziert und in die Signatur aufgenommen.
  - **Klasse-2:** Neben der E-Mail-Adresse ist auch der Name, die Firma oder Organisation des Antragstellers enthalten. Abgleich erfolgt mit dem Personalausweis und dem Handelsregister.
  - **Klasse-3:** Der Antragsteller muss sich persönlich bei einer Zertifizierungsstelle verifizieren lassen.

E-Mail-Verschlüsselung

→ Prinzipielles Vertrauensmodell von S/MIME (2)



E-Mail-Verschlüsselung

→ Schlüsselerstellung und Schlüsselformat (1)

- Prinzipiell kann bei beiden Verfahren jeder ein Schlüsselpaar bzw. ein Zertifikat erstellen.

- **PGP:**
  - Jeder kann ein gültiges Schlüsselpaar erstellen und auch für Verschlüsselung und Signierung von E-Mails nutzen.
  - Jeder kann **einen primären** öffentlichen Schlüssel und **mehrere sekundäre** auf derselben Identität verwalten (Schlüsselbund).
  - Der primäre öffentliche Schlüssel kann mehr als eine Nutzer-ID mit jeweils mehreren Signaturen beinhalten.
  - Jeder einzelne dieser öffentlichen Schlüssel kann auch bei Bedarf wiederrufen werden.

E-Mail-Verschlüsselung

→ Schlüsselerstellung und Schlüsselformat (2)

- **S/MIME:**
  - Jeder ist im Prinzip in der Lage ein Zertifikat zu erstellen, jedoch ist dies kein gültiges Zertifikat.
  - Gültige Zertifikate können nur durch eine zentrale Zertifizierungsinstanz (PKI) erstellt werden.
  - In der Regel ist das ein kostenpflichtiger Vertrauensdienstanbieter.
  - Das Schlüsselformat von S/MIME kann nur einen einzigen öffentlichen Schlüssel, eine Benutzer-ID und eine Signatur verwalten.
  - Dieser kann auch nur durch eine offizielle Zertifizierungsstelle signiert werden.

E-Mail-Verschlüsselung
→ Widerrufen eines Schlüssels (1/2)

- **PGP:**
  - Der widerrufende Schlüssel wird auf den Schlüsselservern, wo auch die aktiven Schlüssel liegen, gespeichert.
  - Bei einem Widerruf wird der Schlüssel um eine spezielle Signatur erweitert.
  - Wird ein Schlüssel auf Gültigkeit überprüft, kann festgestellt werden, ob dieser widerrufen wurde oder noch gültig ist.
  - Für eine Überprüfung wird eine Internet-Verbindung benötigt.
  - Da es bei PGP keine höhere zentrale Instanz wie bei S/MIME gibt, kann nur der Schlüsselinhaber einen Widerruf für einen seiner öffentlichen Schlüssel durchführen.

E-Mail-Verschlüsselung
→ Widerrufen eines Schlüssels (2/2)

- **S/MIME:**
  - Nutzung von Certificate Revocation Lists (CRLs).
  - Das sind Sperrlisten, die alle gesperrten Schlüssel beinhalten.
  - Die CRLs werden von den entsprechenden Zertifizierungsstellen (CA) aktualisiert und verwaltet.
  - Die Nutzer müssen sich regelmäßig aktualisierte Sperrlisten herunterladen oder über einen Service prüfen.
  - Im Gegensatz zu PGP ist bei S/MIME eine Überprüfung auf einen gesperrten öffentlichen Schlüssel auch ohne Internet möglich, da die Listen lokal gespeichert werden können.
  - Wird ein Zertifikat bzw. ein Schlüssel widerrufen, kann der Schlüsselinhaber nur einen Antrag stellen, dieser muss dann durch die CA erst bestätigt werden.

E-Mail-Verschlüsselung

→ Gateway E-Mail-Sicherheitslösungen (1)

- Ein E-Mail-Gateway realisiert die Cyber-Sicherheitsfunktionen:
  - **Entschlüsselung** und **Verifizierung** von eingehenden E-Mails.
  - **Verschlüsselung** und **Signierung** von ausgehenden E-Mails.
  - In der Regel für die Standards **PGP** und **S/MIME** möglich**.**
- Auf diese Weise wird ein hoher **Nutzerkomfort** geschaffen.
- Hohe **Komptabilität** zwischen unterschiedlichen Gerätetypen und Betriebssystemen.
- **Keine Ende-zu-Ende-Verschlüsselung**.
- Die Einhaltung und Anwendung von **Policies** bezüglich der E-Mail-Sicherheit wird durch die zentrale Umsetzung deutlich begünstig.

E-Mail-Verschlüsselung

→ Gateway E-Mail-Sicherheitslösungen (2)

- Auf der Gegenseite kann ebenfalls ein E-Mail-Sicherheits-Gateway stehen oder eine entsprechende Client-Software.
  - Sonst: Erstellung von verschlüsselten, selbstextrahierenden Dateien möglich (Entschlüsselung mittels Passphrase).

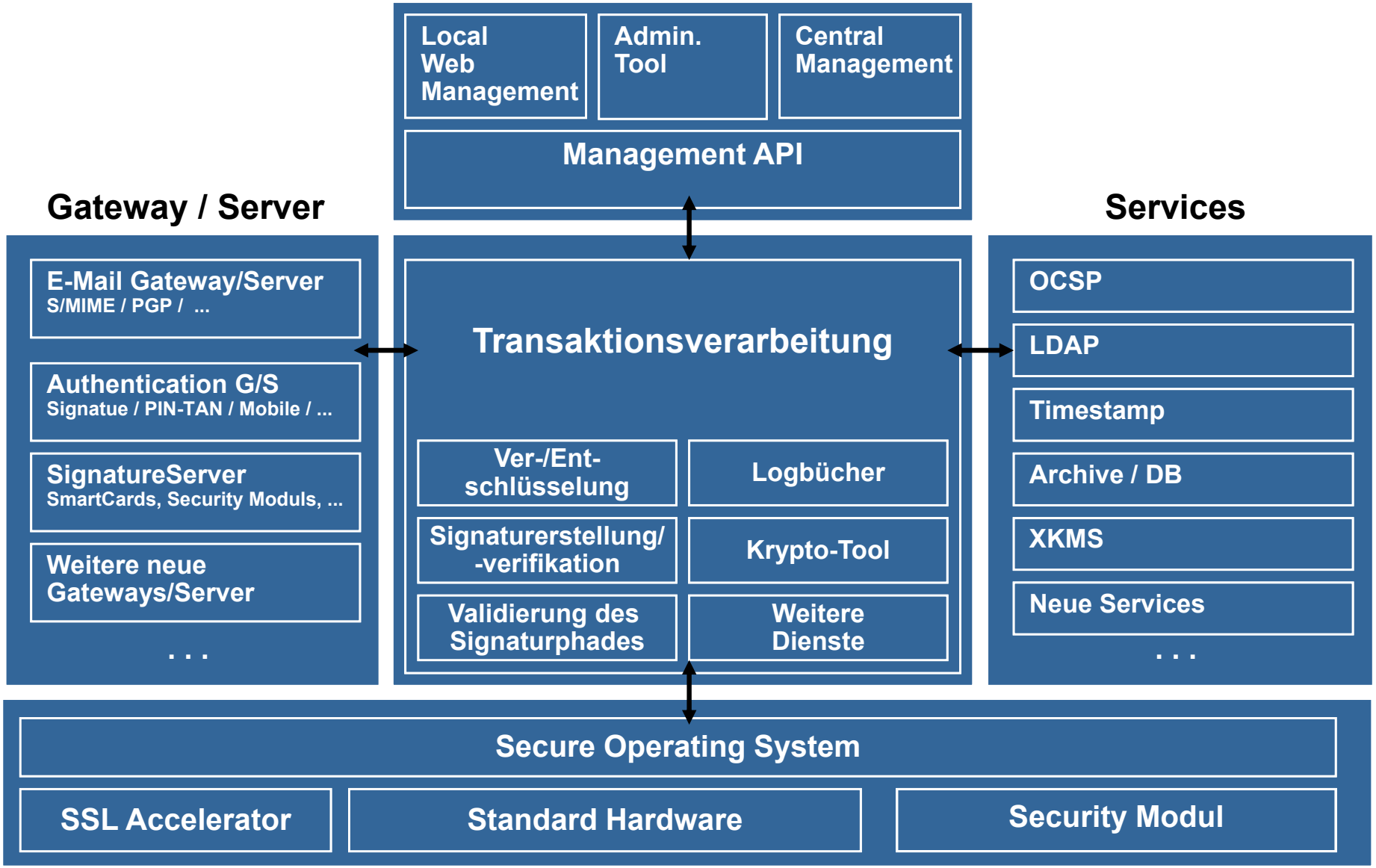
- Vertreterregelung sowie die zentrale Überprüfung der E-Mail-Anhänge einfach realisierbar.

Was ist eine *virtuelle* Poststelle?

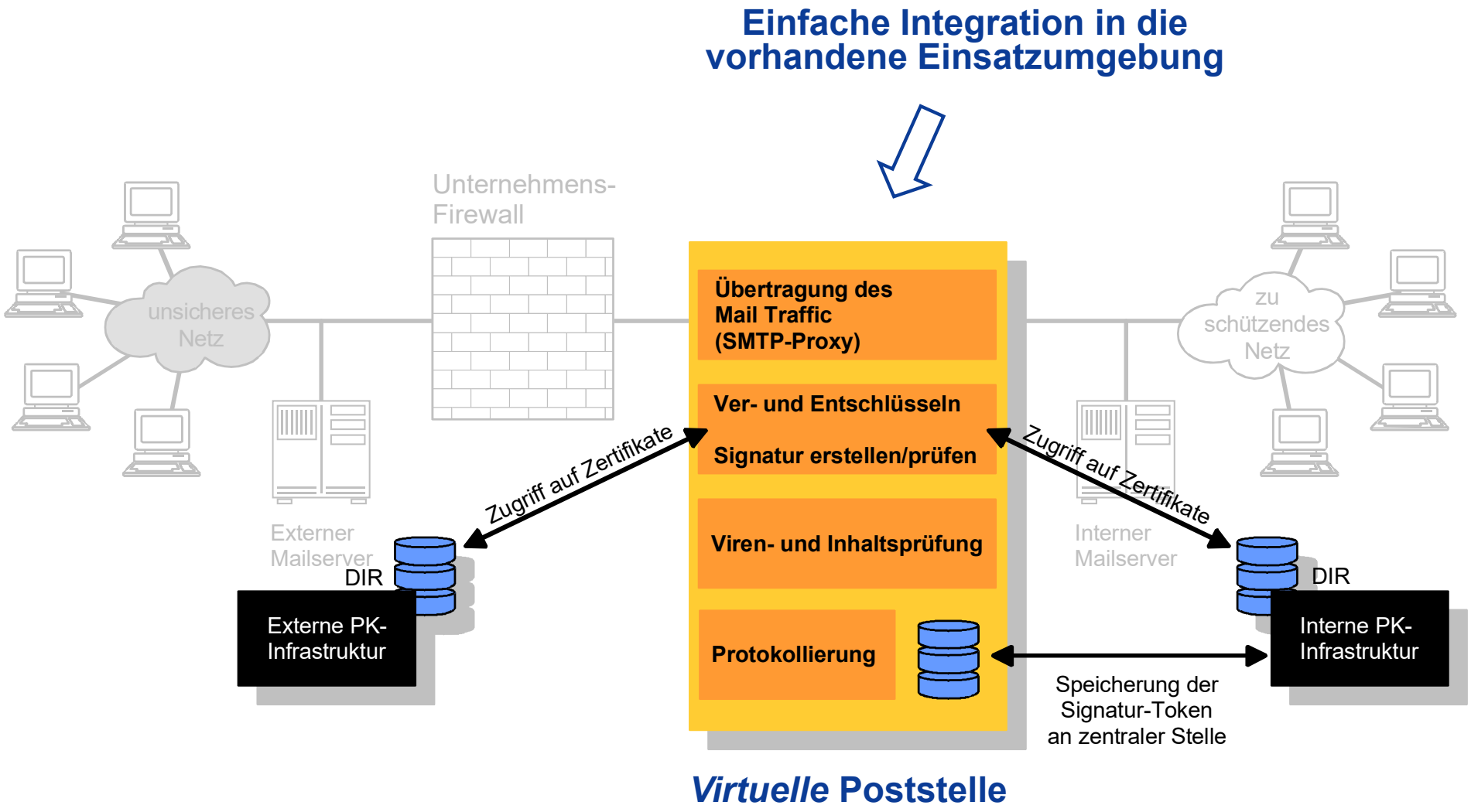
- **Zentrale Security Plattform**
  - **Sie stellt Sicherheitsdienste für eine gesicherte Kommunikation der vertrauenswürdigen elektronischen Prozesse zur Verfügung.**

- **Sicherheitsdienste der *virtuellen* Poststelle sind:**
  - **Vertraulichkeit** der übertragenen und gespeicherten Informationen
  - **Datenintegrität** der Mails, Dateien und sonstigen Informationen
  - **Authentifikation** für die angebotenen Anwendungen (z.B. über Web)
  - **Verbindlichkeit** der ausgetauschten Informationen und Prozesse
  - **Protokollierung und Beweissicherung** der Aktionen, die über die *virtuelle* Poststelle durchgeführt wurden **!**

Architektur der *virtuellen* Poststelle



Die *virtuelle* Poststelle (E-Mail Sicherheit)
→ Pragmatisches Technologie-Konzept



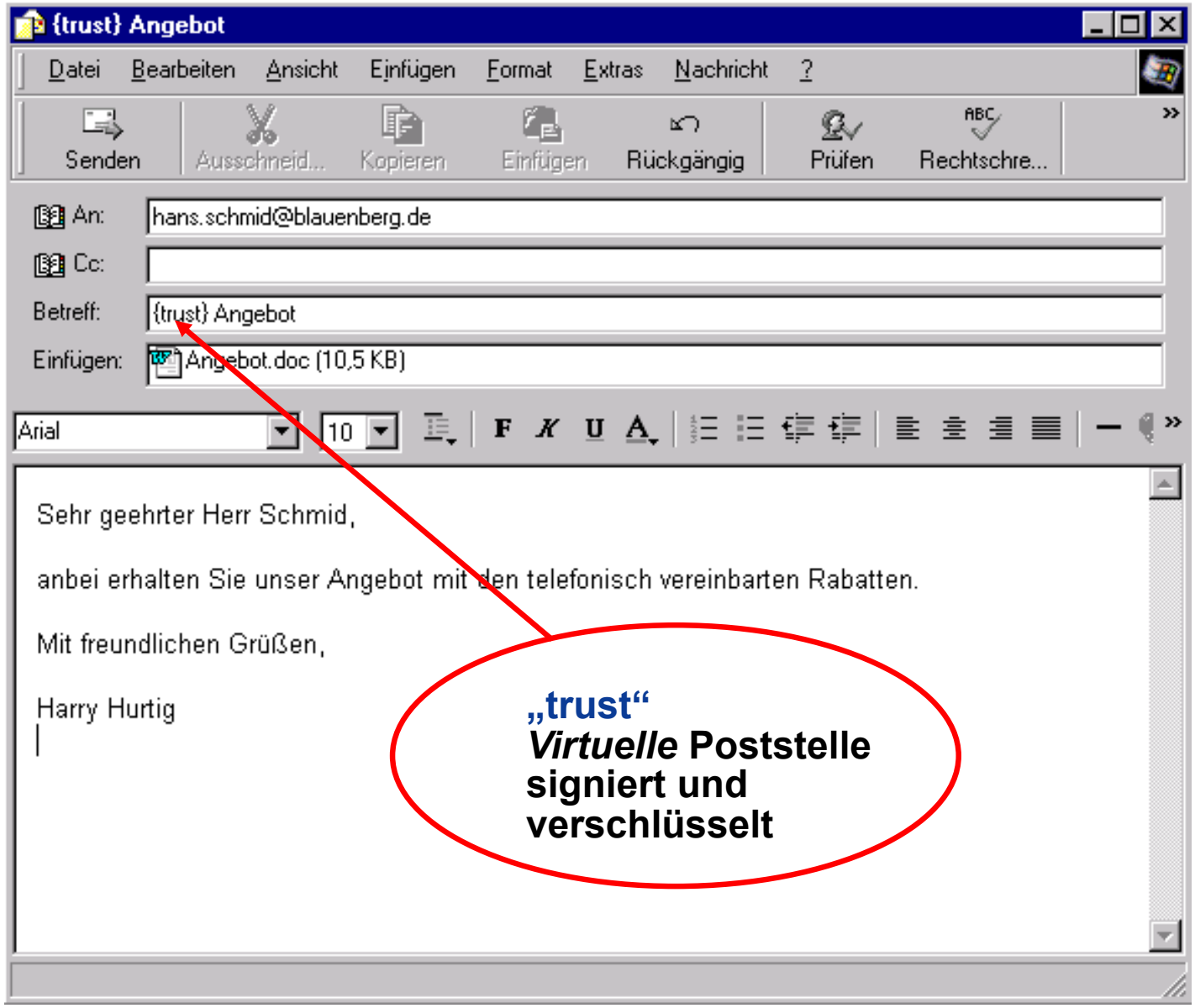
Sichere E-Mail Kommunikation

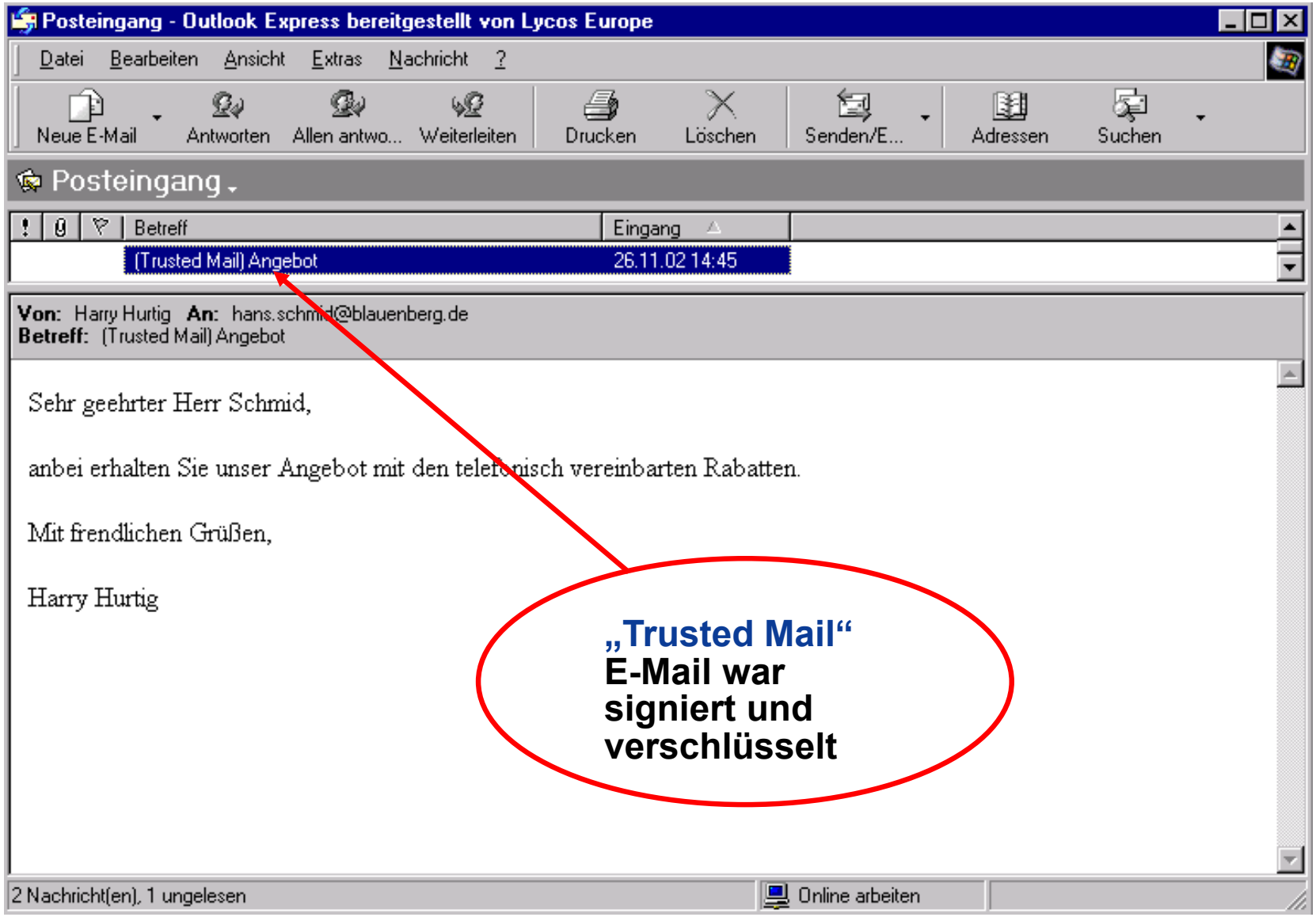
- **Unterschiedliche Methoden**
  - S/MIME (ISIS-MTT)
  - PGP
  - Passphrasen-geschützte Verschlüsselung

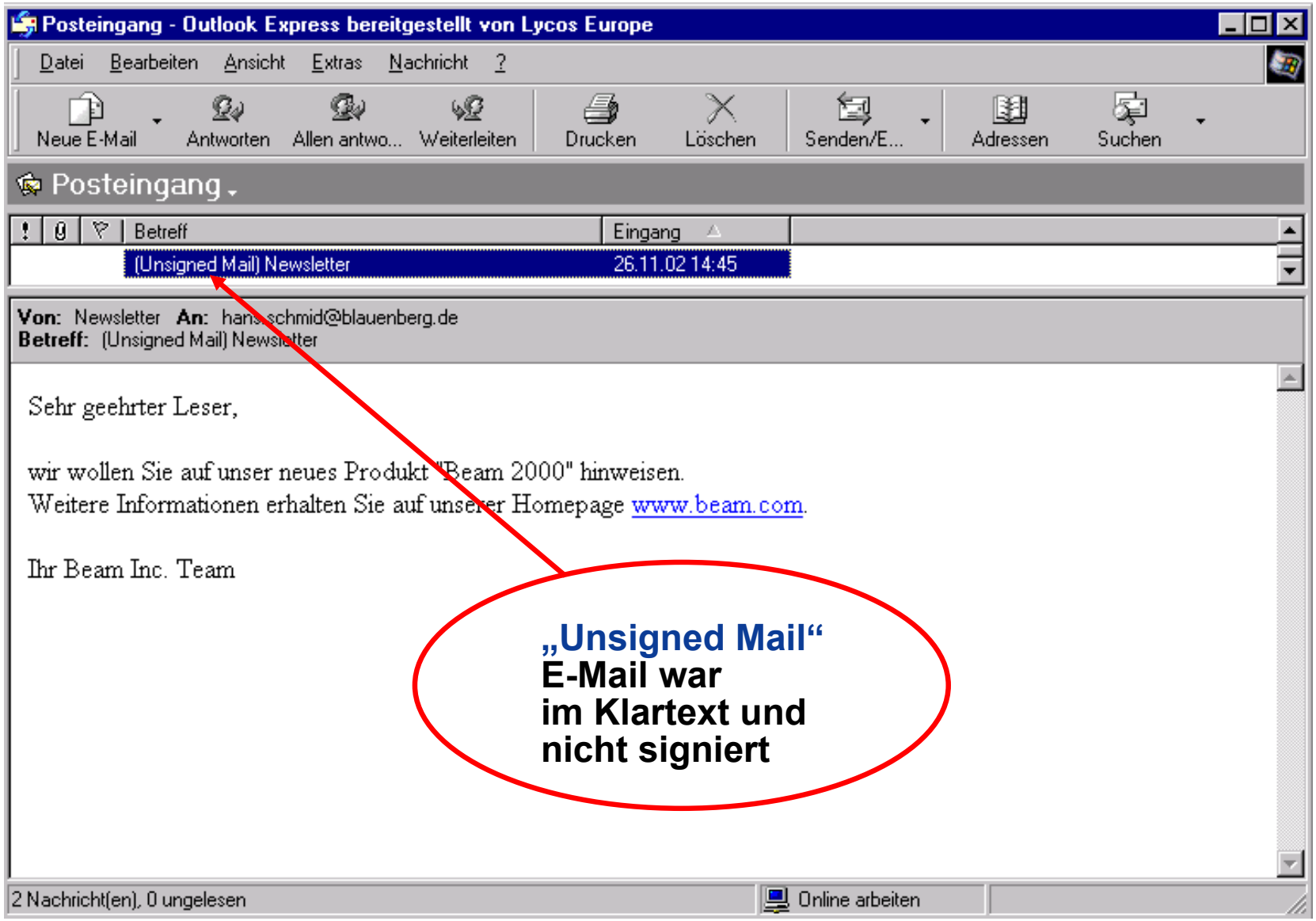
- **Ablauf beim Versenden von E-Mails**
  - ***„Regelbasiert“***
    - **In der virtuellen Poststelle wird definiert**, bei welcher E-Mail-Adresse, die E-Mail durch die *virtuelle* Poststelle digital signiert und/oder verschlüsselt werden soll (z.B. „*@w-hs.de“).
  - ***„Benutzergesteuert“***
    - **Der Benutzer steuert** z.B. über das Betreff-Feld, ob die E-Mail durch die *virtuelle* Poststelle digital signiert und/oder verschlüsselt werden soll.

Aktionen kontrolliert mittels E-Mail-Subject

{sign}	**Die Mail wird signiert.**
{crypt}	**Die Mail wird verschlüsselt.**
{trust}	**Die Mail wird signiert und verschlüsselt.**
{private}	**Die Mail wird einem Passphrasen-geschützte System verschlüsselt.**







E-Mail-Verschlüsselung
→ E-Mail made in Germany (1/2)

- Initiative von „GMX“, „Telekom“ und „Web.de“.
  - Verschlüsselung der E-Mail Kommunikationen zwischen dem IT-Endgerät und E-Mail-Servern (MTAs).
- E-Mail-Daten werden **immer TLS/SSL-verschlüsselt** übermittelt und so vor unberechtigtem Lesen geschützt.
  - Egal, ob Zugriff mittels Browser oder App auf dem Smartphone, Tablet, Notebook oder PC.
  - E-Mail-Programme müssen TLS/SSL aktiviert haben.
  - Damit bietet „E-Mail made in Germany“ einen guten Basis-Schutz für die E-Mail Kommunikation.
- Die E-Mails sind aber bei dieser Lösung auf den E-Mail-Servern (MTA) selber im **Klartext**.

E-Mail-Verschlüsselung
→ E-Mail made in Germany (2/2)

E-Mail-Verschlüsselung
→ De-Mail (1/2)

- De-Mail ist eine **kostenpflichtige** Alternative, um vertrauliche E-Mails sicher und verbindlich elektronisch zu versenden und zu empfangen.

- Wie bei „E-Mail made in Germany“, werden die E-Mail-Daten immer zwischen den IT-System und E-Mail-Server und zwischen den E-Mail-Servern **TLS/SSL-verschlüsselt** und **-integritätsgesichert** übermittelt.
  - Optional kann eine **Ende-zu-Ende Verschlüsselung** genutzt werden.

- Ursprünglich wurde die De-Mail als sicheres und verbindliches elektronisches Pendant zum regulären Briefverkehr entwickelt.

E-Mail-Verschlüsselung
→ De-Mail (2/2)

- Die De-Mail-Dienste stützen sich auf eine gesetzliche Grundlage von **eIDAS**.
  - Die gesetzliche Verbindlichkeit und Gewährleistung des Erhalts der E-Mail steht bei der Nutzung von De-Mail im Vordergrund.

- Anbieter von De-Mail müssen durch das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** in regelmäßigen Abständen akkreditiert werden.

- Um die Verbindlichkeit zu gewährleisten, muss bei der Registrierung ein **Identitätsnachweis** durchgeführt werden.

E-Mail-Verschlüsselung
→ De-Mail-Einschreiben (1/4)

- Der Absender erhält zusätzlich **qualifiziert signierte Bestätigungen:**
  - Wann die E-Mail verschickt wurde.
  - Wann sie an das Postfach des Empfängers ausgeliefert wurde.

- **Persönlich:**
  - Das erforderliche **Authentisierungsniveau** von Absender und Empfänger muss mindestens **hoch** sein, um die E-Mail lesen zu können, beispielsweise wegen der besonderen Vertraulichkeit der Nachricht.

E-Mail-Verschlüsselung
→ De-Mail-Einschreiben (2/4)

- **Absender-Bestätigt:**
  - Das erforderliche **Authentisierungsniveau** des Absenders muss wegen der besonderen Verbindlichkeit der E-Mail mindestens **hoch** sein.
  - Der De-Mail-Provider des Absenders bestätigt nach Entgegennahme der E-Mail mittels **qualifizierter Signatur**, dass er den angegebenen Nachrichteninhalt von dem Absender entgegengenommen hat und dieser sich mindestens mit hoch authentisiert hat.
  - Der Empfänger erhält dadurch einen glaubwürdigen **(„starken“) Nachweis der Authentizität** des Absenders und der **Integrität** der Nachricht.

E-Mail-Verschlüsselung
→ De-Mail-Einschreiben (3/4)

- **Versandbestätigung:**
  - Der De-Mail-Anbieter des Absenders erstellt eine **qualifiziert signierte Bestätigung**, dass er eine referenzierte E-Mail zu einem bestimmten **Zeitpunkt** für den Versand an einen bestimmten Empfänger entgegengenommen hat.

- **Zugangsbestätigung:**
  - Der De-Mail-Anbieter des Empfängers erstellt nach Ablage der E-Mail in das Postfach des Empfängers eine **qualifiziert signierte Bestätigung**, dass er eine referenzierte E-Mail zu einem bestimmten **Zeitpunkt** in das Postfach des Empfängers eingestellt hat.

E-Mail-Verschlüsselung
→ De-Mail-Einschreiben (4/4)

- **Abholbestätigung:**
  - Der De-Mail-Anbieter des Empfängers erstellt nach einer sicheren Anmeldung des Nutzers und bei Vorhandensein einer E-Mail mit Abholbestätigungs-Anforderung im Postfach des Empfängers eine **qualifiziert signierte Bestätigung**, dass der Nutzer eine E-Mail einsehen konnte.

E-Mail-Verschlüsselung
→ Manuelle Dateiverschlüsselung (1/2)

- Herstellung von Vertraulichkeit ohne sichere Infrastruktur.
- Verschlüsselte Dateien werden bei diesem Verfahren als Anhang an die E-Mail angehangen.
  - Die E-Mail dient lediglich zum Transport der Datei.
- Eine Einsicht durch Dritte ist aufgrund der Verschlüsslung der Datei auf dem Transportweg nicht möglich.
- Austausch der Passphrase ist eine weitere Herausforderung.
- Die Authentizität der Nachricht kann nicht verifiziert werden, da keine Vertrauensstruktur wie bei PGP und S/MIME vorhanden ist.

E-Mail-Verschlüsselung
→ Manuelle Dateiverschlüsselung (2/2)

- Ein Anwendungsbeispiel könnte der Versand einer vertraulichen PDF sein.
  - Der Sender versieht die PDF mit einer Passphrase und verschlüsselt die Datei.
  - Die verschlüsselte Datei wird als Anhang einer E-Mail zum Empfänger versendet.
  - Anschließend wird die Passphrase über einen zweiten Kanal übertragen, beispielweise über SMS oder telefonisch.
  - Die größte Sicherheit bietet ein persönlicher Austausch der Passphrase, jedoch ist das in der Praxis nicht immer realisierbar.
  - Der Anhang wird lokal beim Empfänger runtergeladen und mithilfe der Passphrase entschlüsselt.
  - Ob die PDF wirklich vom erwarteten Sender stammt, kann nicht verifiziert werden.

E-Mail-Verschlüsselung

→ Vor- und Nachteile sowie Skalierbarkeit (1)

Lösung	Vorteile	Nachteile	Skalierbarkeit
PGP	• Open Source • kostenfrei • Ende-zu-Ende Verschlüsselung	• komplexes Verfahren • veränderte User-Experience • Web of Trust als Sicherheitsanker • verschlüsselt gespeicherte E-Mails sind nicht mehr durchsuchbar • Verlust des privaten Schlüssels oder Passworts führt zum Verlust der verschlüsselten E-Mails	• gute Skalierbarkeit • Einsatz möglich in allen Unternehmensgrößen
S/MIME	• Ende-zu-Ende Verschlüsselung • einfache Verwendung • kein Schlüsselmanagement durch den Nutzer	• Identitätsüberprüfung zur Steigerung des Vertrauens • Achtsamkeit nötig • veränderte User Experience • Verlust des privaten Schlüssels oder Passworts führt zum Verlust der verschlüsselten E-Mails	• gute Skalierbarkeit • Einsatz möglich in allen Unternehmensgrößen

E-Mail-Verschlüsselung

→ Vor- und Nachteile sowie Skalierbarkeit (2)

Lösung	Vorteile	Nachteile	Skalierbarkeit
E-Mail-Gateway	• hoher Nutzerkomfort • Policy-konforme Verschlüsselung • kein geändertes Bedienerverhalten • Unterstützung verschiedene Standards • Zentrale Schlüsselverwaltung • Malware-Prüfung vor Zustellung der Mails • revisionssicher • Data-Loss-Prevention	• hohe Anschaffungskosten • begrenzte Kapazitäten • keine Ende-zu-Ende Verschlüsselung • hoher Konfigurationsaufwand • hoher Aufwand bei der Erstellung einer Policy	• sehr gute Skalierbarkeit • Einsatz geeignet für mittlere und große Unternehmen
E-Mail made in Germany	• hoher Nutzerkomfort Transportverschlüsselung • Zusätzlich kann auch unabhängig von der E-Mail made in Germany PGP und S/MIME verwendet werden	• keine standardmäßige Ende-zu-Ende Verschlüsselung	• Einsatz für jede Unternehmensgröße geeignet

E-Mail-Verschlüsselung

→ Vor- und Nachteile sowie Skalierbarkeit (3)

Lösung	Vorteile	Nachteile	Skalierbarkeit
De-Mail	• hoher Nutzerkomfort • Transportverschlüsselung • optionale Ende-zu-Ende Verschlüsselung • Verbindlichkeit der E-Mail ist gesetzlich gewährleistet • Nutzerregistrierung erfordert eine Identitätsprüfung • mehrere Anbieter vorhanden	• kostenpflichtig • Postfach muss regelmäßig eingesehen werden • lange Anmeldezeiten zur Prüfung der Identität des Antragstellers • Empfänger muss ebenfalls bei De-Mail registriert sein • geringe Verbreitung inkompatibel mit anderen E-Mail-Diensten	• Einsatz für jede Unternehmensgröße geeignet
Manuelle Datei-verschlüsselung	• Datei bleibt nach dem Herunterladen geschützt, E-Maildient nur als Transport • Keine Infrastrukturerweiterung notwendig	• Inhalt der Mail bleibt unverschlüsselt • Sicherheit ist abhängig vom Format und der Software • Passwortstärke legt Sicherheitsniveau fest • händische Ver- und Entschlüsselung der Dokumente • benötigt verschlüsselten Kommunikationskanal für den Schlüsselaustausch	• Skalierung schlecht bei vielen Dokumenten

E-Mail Sicherheit
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Cyber-Sicherheitsprobleme
- E-Mail-Verschlüsselung
- **Zusammenfassung**

E-Mail Sicherheit
→ Zusammenfassung

- Die E-Mail-Anwendung wird in vielen Bereichen verwendet, in denen Vertrauenswürdigkeit und Vertrauen eine besondere Rolle spielen.

- Aus diesem Grund ist es wichtig, dass die richtigen **Cyber-Sicherheitsmechanismen** genutzt werden, damit das Risiko eines Schadens bei der Nutzung von E-Mail minimiert werden kann.

- **PGP und S/MIME** sind E-Mail-Sicherheitslösungen, die beide auf unterschiedlichen konzeptionellen Strukturen beruhen und dadurch beide ihre **Vor- und Nachteile** besitzen.

- Welche Lösung sich am besten zur E-Mail-Sicherheit eignet, kommt letztendlich immer auf den **individuellen Anwendungsfall** und Anforderungen des Nutzers oder Organisation an.
  - In der Praxis nutzen Privatpersonen und kleiner KMUs mehr PGP und große Unternehmer mehr S/MIME.

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

E-Mail Sicherheit

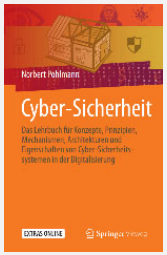
Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

Anhang / Credits

Wir empfehlen

- **Cyber-Sicherheit**
  Das **Lehrbuch** für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, Springer Vieweg Verlag, Wiesbaden 2022
  https://norbert-pohlmann.com/cyber-sicherheit/



- **7. Sinn im Internet (Cyberschutzraum)**
  https://www.youtube.com/cyberschutzraum

CYBER SCHUTZRAUM

- **Master Internet-Sicherheit**
  https://it-sicherheit.de/master-studieren/

(M) MASTER internet-sicherheit.

Besuchen und abonnieren Sie uns :-)

WWW
https://www.internet-sicherheit.de

Facebook
https://www.facebook.com/Internet.Sicherheit.ifis

Twitter
https://twitter.com/_ifis

https://twitter.com/ProfPohlmann

YouTube
https://www.youtube.com/user/InternetSicherheitDE/

Prof. Norbert Pohlmann
https://norbert-pohlmann.com/

Quellen Bildmaterial

Eingebettete Piktogramme:
- Institut für Internet-Sicherheit – if(is)

Der Marktplatz IT-Sicherheit

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.
https://www.it-sicherheit.de/

Literatur
→ Artikel / Bücher

S. Feld, N. Pohlmann: „E-Mail-Adress-Harvesting: Wie schütze ich mich vor dem E-Mail-Adress-Klau?“, IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 02/2008
https://norbert-pohlmann.com/wp-content/uploads/2015/08/225-E-Mail-Adress-Harvesting-Wie-schütze-ich-mich-vor-dem-E-Mail-Adress-Klau-Prof.-Norbert-Pohlmann.pdf

N. Pohlmann: „Bedrohungen und Herausforderungen des E-Mail-Dienstes - Die Sicherheitsrisiken des E-Mail-Dienstes im Internet", DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 09/2010
https://norbert-pohlmann.com/wp-content/uploads/2015/08/266-Bedrohungen-und-Herausforderungen-des-E-Mail-Dienstes-–-Die-Sicherheitsrisiken-des-E-Mail-Dienstes-im-Internet-Prof.-Norbert-Pohlmann.pdf

N. Pohlmann: "Firewall-Systeme - Sicherheit für Internet und Intranet, E-Mail-Security, Virtual Private Network, Intrusion Detection System, Personal Firewalls“, 5. aktualisierte und erweiterte Auflage, 604 Seiten, MITP-Verlag, Bonn 2003
http://norbert-pohlmann.com/app/uploads/2015/08/Firewall-Systeme.pdf

N. Pohlmann: "Cyber-Sicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, ISBN 978-3-658-25397-4; 594 Seiten, Springer-Vieweg Verlag, Wiesbaden 2019
https://norbert-pohlmann.com/cyber-sicherheit/