

it-sa 2014 Auditorium Bundesverband IT-Sicherheit e.V.

Nürnberg, 08.10.2014

**Mehr Verschlüsselung im Unternehmen?
Ein Jahr nach Snowden – noch ist viel zu tun**

Hajo Giegerich, Giegerich & Partner GmbH

Warum sichere Datenkommunikation?

Mitgliederdaten der CDU geklaut UPDATE

 vorlesen / MP3-Download

Wie erst jetzt bekannt wurde, ist das [Mitgliedernetz](#) der CDU schon im August 2009 Opfer eines Angriffs geworden. Darüber informierte die Partei an diesem Freitag betroffene Mitglieder [per E-Mail](#). Es habe sich herausgestellt, dass die Einbrecher beim Angriff Zugriff auf Mitgliederdaten hatten und diese dann am 12.08.2011 im Internet veröffentlichten. Dabei handelte es sich um den Nachnamen, eine interne Kennnummer und die E-Mail Adresse.

02.08.2012 16:06

Kundendaten bei Online-Brillenladen Mister Spex geklaut UPDATE

 vorlesen / MP3-Download

Unbekannte konnten bei einem [Hackerangriff](#) auf den Internetoptiker [Mister Spex](#) auf die Kundendatenbank zugreifen. Laut dem Berliner Unternehmen hatten die Angreifer dabei Zugriff auf Adressdaten und Passwörter und habe diese möglicherweise auch kopiert. Gehasst waren die Passwörter demnach nicht. Zahlungsinformationen seien nicht betroffen, da diese laut Mister Spex nicht gespeichert werden.



Datenklau im großen Stil Chinesische Hacker spähnen High-Tech-Konzern aus

Dienstag, 14.02.2012, 11:51

★★★★★ (7)



Twittern 17



ZUM THEMA

Telekommunikation
Apple und Microsoft
kaufen Nortel-
Hauptdarsteller

Dank gestohlener Passwörter haben vermutlich aus China stammende Hacker jahrelang den inzwischen insolventen Nortel-Konzern ausspioniert. Sie hätten „Zugang zu allem gehabt“, offenbarte nun ein Manager.

sicherheit e.V.



Erneuter Datenklau Hacker knacken 93 000 Konten bei Sony

Witbuch, 12.10.2011, 10:10

★★★★★ (5)

Twittern 1



Erst im April hatten sich Hacker Zugriff auf Millionen Userkonten bei Sony verschafft. Nun ist der Elektronikriese erneut ins Visier von Cyberkriminellen geraten: Daten von fast Hunderttausend Kunden wurden gestohlen.

Die Angreifer hätten auf breiter Front versucht, in Nutzerkonten bei Sonys Online Diensten einzudringen, teilte der japanische Elektronikriese mit. In 93 000 Fällen sei es Eindringlingen gelungen, Kundennummern

Datenklau bei der Citibank gelang durch simple URL-Manipulation



Laut einem Bericht der New York Times gelang der Diebstahl von rund 200.000 Kundendaten durch einen äußerst simplen Angriff.

Kundendaten bei der Citibank entwendet



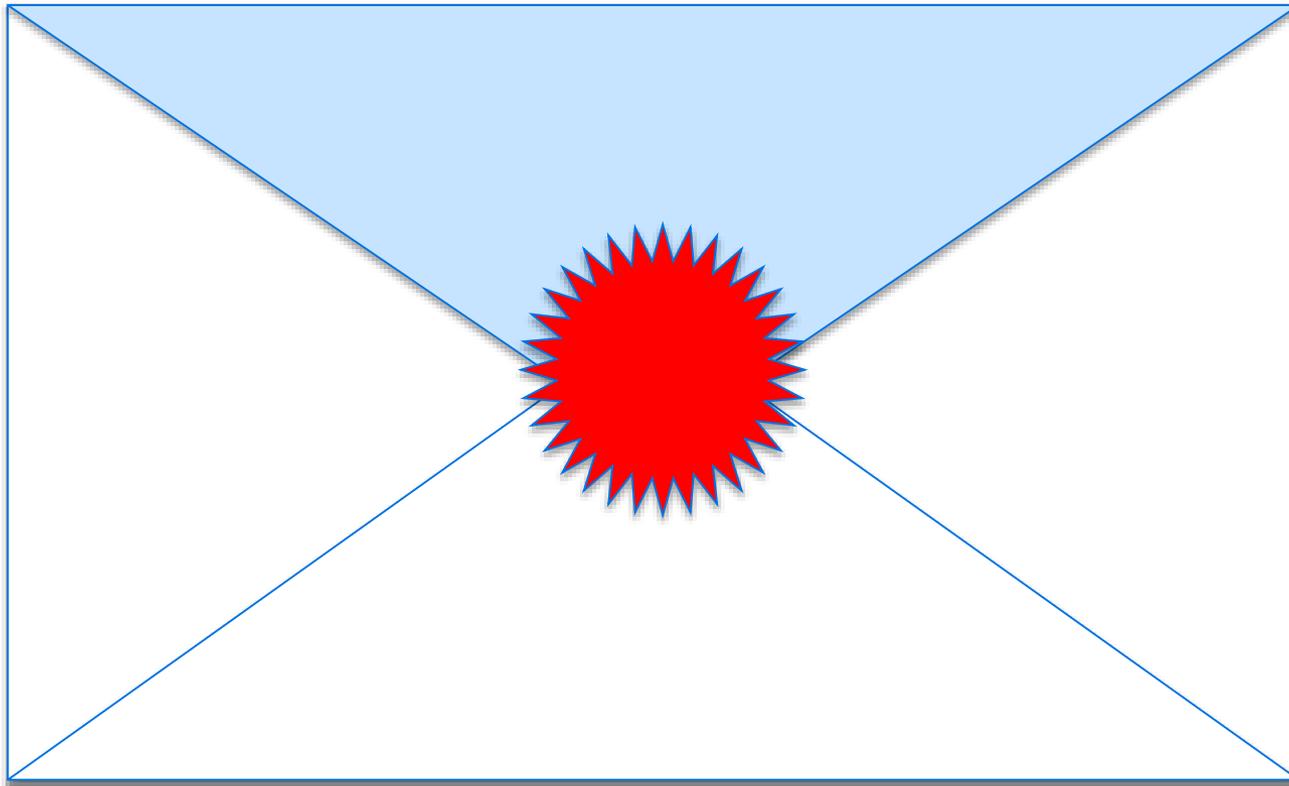
Bei dem Einbruch wurden laut der US-Bank die persönlichen Daten von etwa 200.000 Kreditkartenkunden entwendet. Der Vorfall wurde bei einer Routinekontrolle entdeckt.

Gute Gründe

- Wahrung von Geschäftsinteressen
- Verhinderung von unfreundlichem Informationsabfluß (Wirtschaftsspionage)
- Wettbewerbsvorteile ausbauen und halten
- Erfüllung gesetzlicher Vorschriften (z.B. Datenschutz)

Analoge Welt – heile Welt?

Ein Ausflug zur „guten alten Post“



Kennzeichen des Briefes

- Geschlossen – Inhalt nicht unmittelbar einsehbar
- Durch das Briefgeheimnis geschützt
- Nachweis der Zustellung möglich

➔ Aber: Inhalt im Klartext lesbar, wenn geöffnet

E-Mail – die digitale „Postkarte“

Ihr vertraut man vieles (vertrauliche) an...

Senden | Speichern | Schließen |   |  |  Namen überprüfen

An...

Cc...

Bcc...

Betreff:

 Anlagen...

Lieber Interessent,

dieses Angebot ist vertraulich und speziell für Sie erstellt. Bitte machen Sie es keinem Dritten zugänglich.

Geheimnisvolle Grüße
Giegerich & Partner GmbH

Müssen wir alles im Klartext schreiben? Geheimnisse verschlüsselt auf die E-Mail!

Senden | Speichern | Schließen |     Namen überprüfen

An...

Cc...

Bcc...

Betreff:

 Anlagen...

```
-----BEGIN PGP MESSAGE-----  
Version: GnuPG v2.0.17 (MingW32)  
Comment: Using gpg4o v2.1.64.1653 - http://www.gpg4o.de/  
Charset: utf-8  
  
hQEMAwruW21QpvMwAQf/WZif/yrWout6ZHnUPuCnc9gOq1J4kpNMGzq8GnAkfQW  
L6RW+KMRNRLPBJDGR8g2TaQOuSXPG5hOmrNuyxhpFaPmq0eLghSeicsTHXMWNgc  
Ykj7kbwlSCHCW/AEbfTmAH90yBHheU28UN4WCw/BUjNksiwb9eP2sApotgiGS3M  
hXsTkoDYSBCar3itVxipDCCAROnRqbHv8uilbGxvqz7t+lhgbMycccaKdZ0BqQX
```

Sinnvolle Anwendungsszenarien bei vertraulichem Inhalt

E-Mailverschlüsselung - wenn vertrauliche Informationen eine vertrauenswürdige Umgebung verlassen:

- **Nachrichten an Personen außerhalb des Unternehmens**
z.B. Kunden, Lieferanten, Auftragsdatenverarbeiter
- **Nachrichten innerhalb des Unternehmens, sofern besondere Schutzwürdigkeit gegeben ist**
z.B. Personaldaten, Forschungsergebnisse, Konzepte etc.
- **Nachrichten an Personen innerhalb des Unternehmens, wenn diese über nicht vertrauenswürdige Netze kommunizieren**
z.B. im Ausland befindlich und VPN unterbunden

Technologien für sicheren E-Mail-Verkehr

Für unterschiedliche Anwendungszwecke

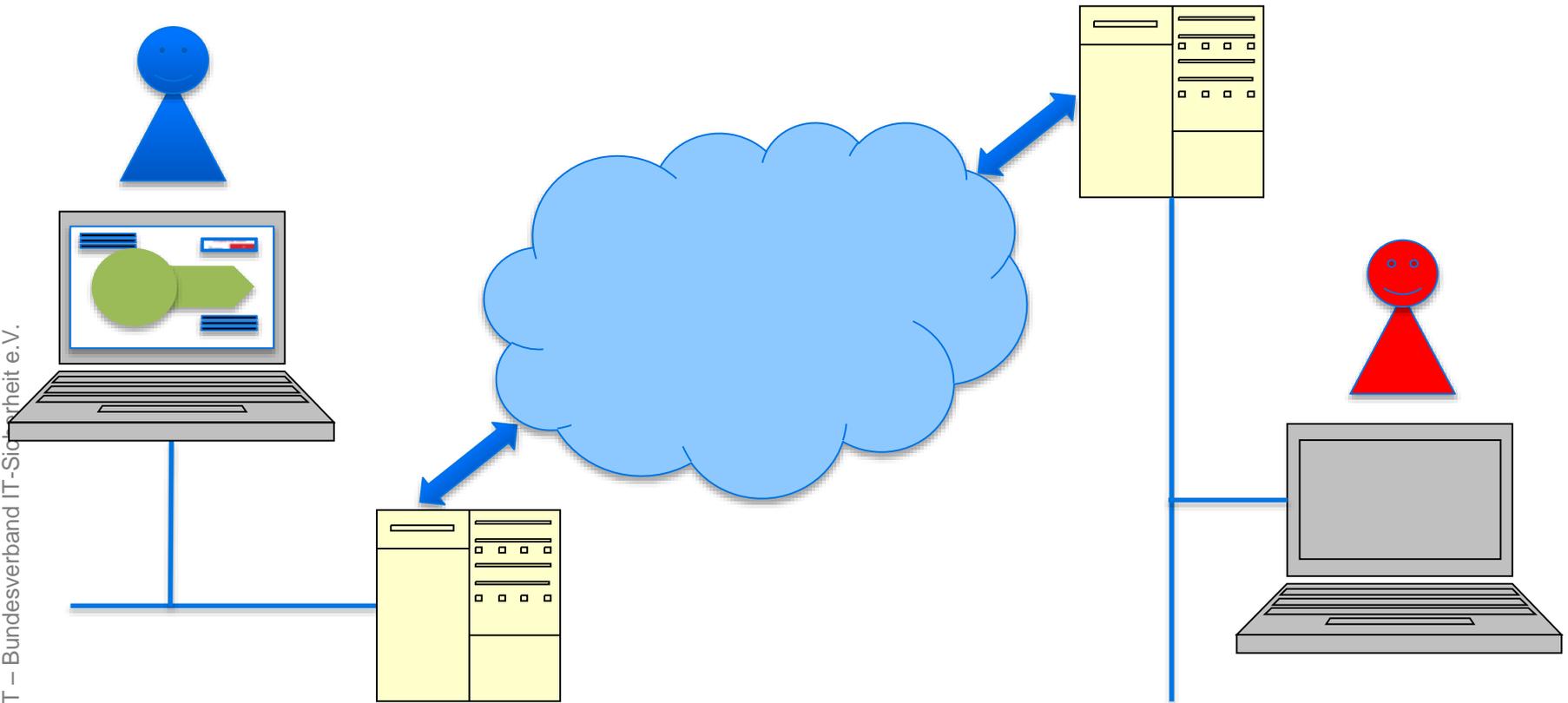
- **(Passwort)-Verschlüsselte Archive als Anhang zur E-Mail**
z.B. RAR-Archive
- **OpenPGP basierte Nachrichtenverschlüsselung**
für verschiedene Plattformen verfügbar
- **S/MIME basierte Nachrichtenverschlüsselung**
für verschiedene Plattformen verfügbar
- **DE-Mail**
vom Bund initiierte und lizenzierte Plattform zur sicheren
Nachrichtenkommunikation
- **Andere**
ePostbrief, E-Mail made in Germany

Wer verschlüsselt hier – Client oder Server?

Clientbasierte Verschlüsselungsmethoden

- Gewährleisten eine durchgehende (Ende-zu-Ende) Verschlüsselung zwischen Sender und Empfänger
- Bieten maximale Vertraulichkeit
- Sind auf jedem Client separat einzurichten
- Fordern (in größeren Organisationen) erhöhten administrativen Aufwand
- Zur Erfüllung ges. Vorschriften (z.B. GdPdU) sind ggf. zusätzliche Maßnahmen in der Schlüsselverwaltung erforderlich.

Clientbasierte Verschlüsselungsmethoden

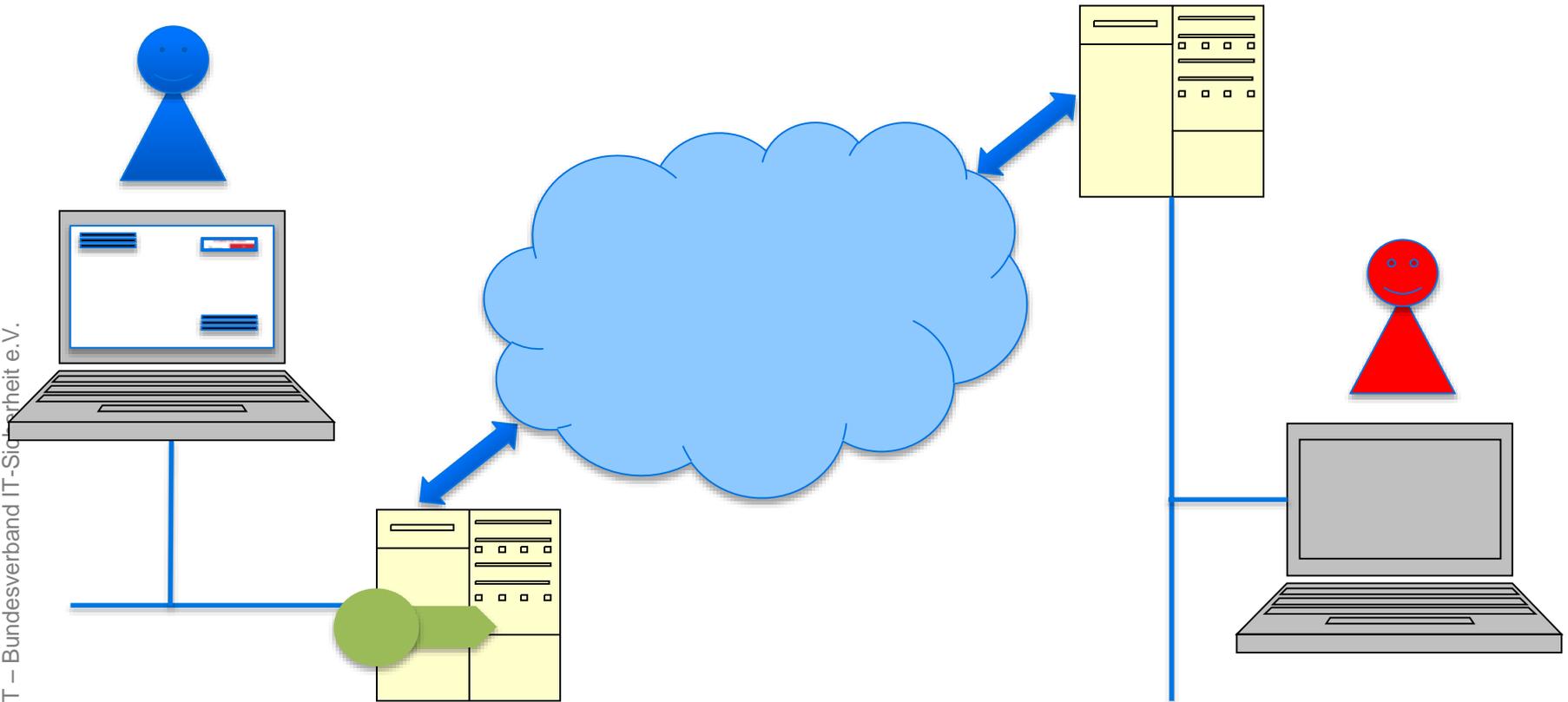


Serverbasierte Verschlüsselungsmethoden

- Verschlüsselung erfolgt auf Mailserver
- Bieten Vertraulichkeit zwischen den Mailservern
- Erfordern in der Regel keine Clientseitige Einrichtung
- Verlagern den administrativen Aufwand auf die Serverseite
- Zur Erfüllung ges. Vorschriften (z.B. GdPdU) sind ggf. zusätzliche Maßnahmen erforderlich

**GEMISCHTE LÖSUNGEN
MÖGLICH!**

Serverbasierte Verschlüsselungsmethoden

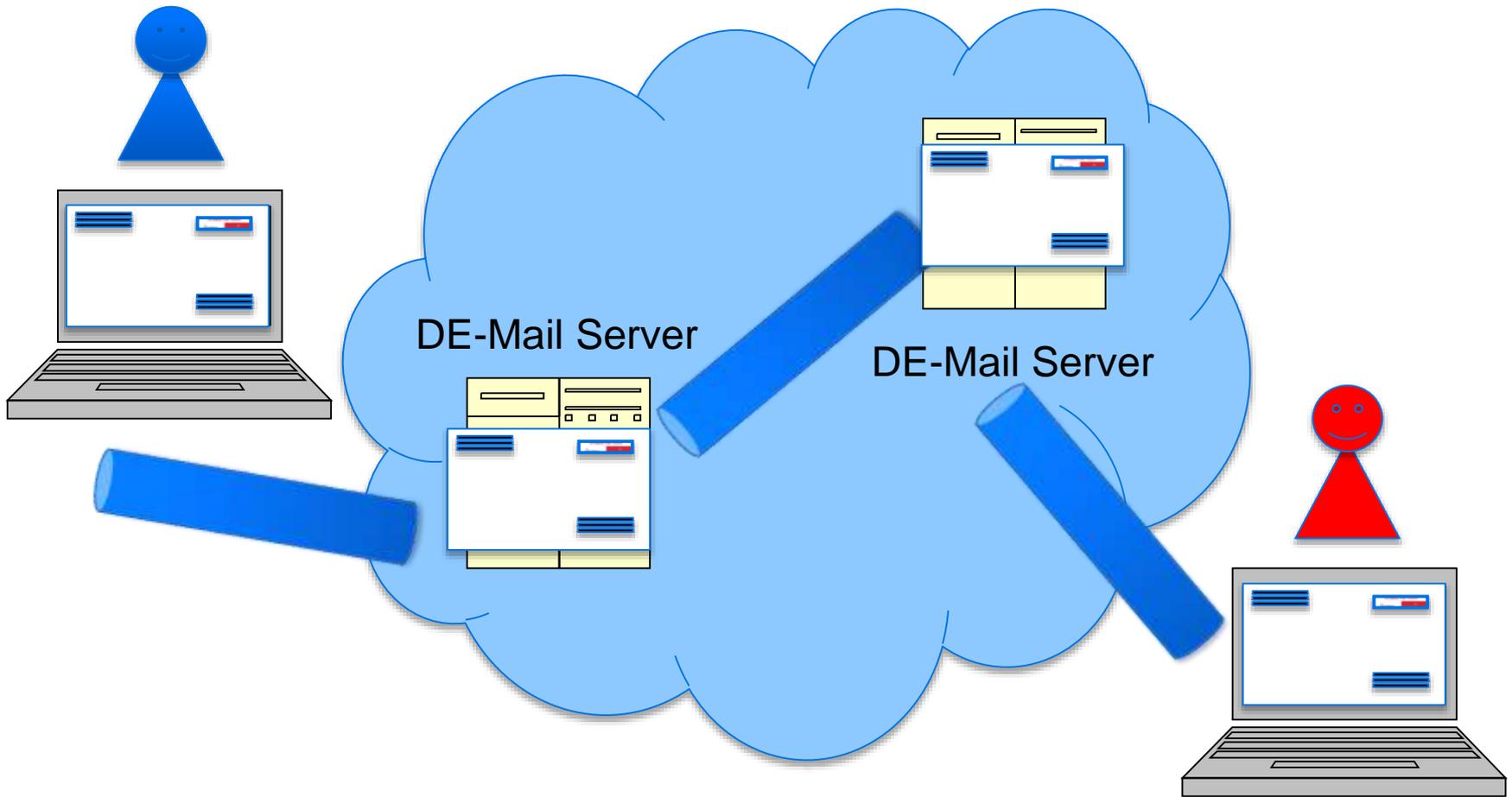


DE-Mail – „Einschreibebrief in digital“

- Umsetzung einer EU-Richtlinie, nach der alle Behörden bis Ende 2009 elektronische Nachrichten akzeptieren sollen
- Basiert auf E-Mail – ist davon aber ein getrennter Dienst
- Ziel: Verbindlichkeit des elektronischen Geschäftsbriefes
- Einige Angebote im Markt (Deutsche Telekom, 1&1 und Andere)
- Verschlüsselung durch TLS (Transport Layer Security) gewährleistet

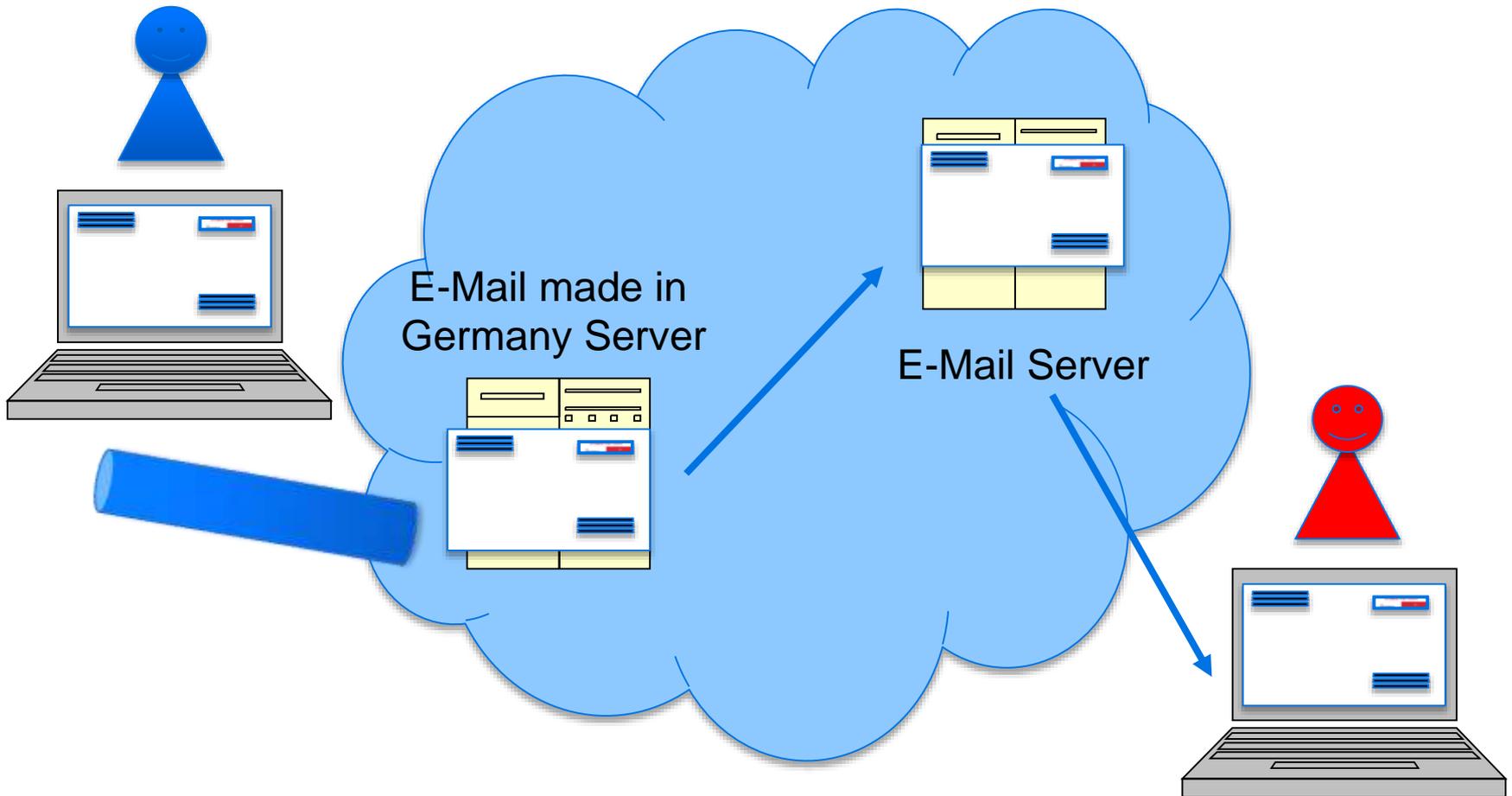


Technisches Prinzip: Keine Ende-zu-Ende Verschlüsselung!



So ähnlich: E-Mail made in Germany!

Hybride Lösung ermöglicht mailen in alle Netze



Keine Einheitsgröße!

- Technologieauswahl stark von Schutzbedarf und Aufwandsbereitschaft abhängig
- Behördenkommunikation soll künftig Nutzung von DE-Mail erfordern
- Weltweite Kommunikation über Industrie-Standards
- Kombination von Verfahren (z.B. DE-Mail mit OpenPGP und S/MIME möglich und verschiedentlich ratsam)

**Vielen Dank für Ihre
Aufmerksamkeit!**

Impressum

Giegerich & Partner GmbH
Robert-Bosch-Str. 18
63303 Dreieich
Deutschland
Telefon: +49-(0)6103-5881-0
Telefax: +49-(0)6103-5881-39
Internet: www.giepa.de

Copyrights

Die durch den Betreiber erstellten Inhalte und Werke dieser Präsentation unterliegen dem deutschen Urheberrecht. Die Vervielfältigung, Bearbeitung, Verbreitung und jede Art der Verwertung außerhalb der Grenzen des Urheberrechts bedürfen der schriftlichen Zustimmung des Autors bzw. Erstellers.