

# Reale Nutzung kryptographischer Verfahren in TLS/SSL

CeBIT 2009/03/06

**Dominique Petersen**  
**petersen (at) internet-sicherheit.de**

Institut für Internet-Sicherheit  
<https://www.internet-sicherheit.de>  
Fachhochschule Gelsenkirchen  
**CeBIT 2009, Halle 9, Stand D06**



# Agenda

- Einleitung
- Entstehung
- Verschlüsselung mit TLS/SSL
- Betrachtung von HTTPS
- Betrachtung von E-Mail-Verkehr
- Sicherheitsmaßnahmen
- Fazit

- Das Internet ist offen und die gesetzlichen Rahmenbedingungen weltweit sehr unterschiedlich
- Sehr viele Anwendungen im Internet wie Eingabe von Passwörtern und Kreditkarten-Informationen
- Daher Notwendigkeit für Verschlüsselung im unsicheren Internet
- Vorherrschender Ansatz für Verschlüsselung ist die Verwendung von Transport Layer Security (TLS) und Secure Sockets Layer (SSL)

- 1993 wurde die erste Version von Mosaic fertig gestellt
- 1994 hat Netscape Communications Version 1.0 von Secure Sockets Layer (SSL) veröffentlicht
- Bereits 5 Monate später Version 2.0
- 1996 erschien Version 3.0
- 1999 wurde SSL von der IETF als Standard festgelegt (RFC 2246) und in Transport Layer Security (TLS) umbenannt
  - SSL 3.0 wurde mit wenigen Unterschieden TLS 1.0
  - TLS unterstützt viele neue kryptographische Verfahren
- Seitdem nur wenige Sicherheitsverbesserungen in TLS (1.1, 1.2)

# Verschlüsselung mit TLS/SSL (1/2)

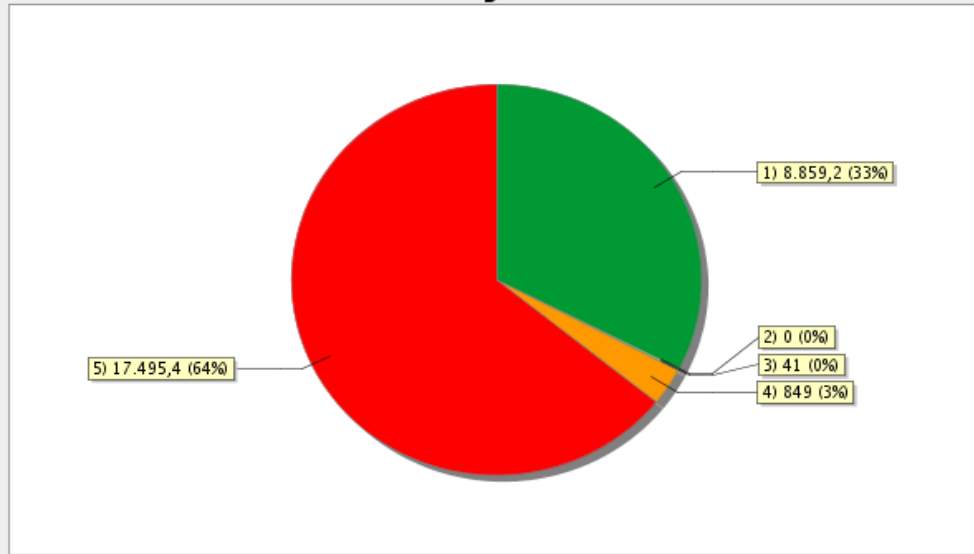
- Hybrides Verschlüsselungsverfahren
- Hauptaufgaben von TLS/SSL:
  - Die **Authentikation der Kommunikationspartner** unter Verwendung von **asymmetrischen Verschlüsselungsverfahren und Zertifikaten** sowie Austausch eines gemeinsamen Sitzungsschlüssel (Session-Key).
  - Die **vertrauliche Ende-zu-Ende-Datenübertragung** mit Hilfe **symmetrischer Verschlüsselungsverfahren** unter der Nutzung des gemeinsamen Sitzungsschlüssels.
  - Die **Sicherstellung der Integrität der transportierten Daten** unter Verwendung von **Message Authentication Codes**.

- Cipher Suites
  - Kombinationen aus **Schlüsselaustauschverfahren**, **Verschlüsselungsverfahren mit Schlüssellänge** sowie ein **Verfahren zum Integritätscheck** (Kombinationsmöglichkeiten sind in den RFCs definiert)
  - Schlüsselaustausch: RSA, DH-RSA, DH-DSS, ...
  - Verschlüsselungsverfahren: AES, Camellia, 3DES, RC4, DES, ...
  - Integritätscheck: SHA1, RIPE-MD, MD5
  - → Nutzung in HTTPS, SMTPS, POP3S, IMAPS, ...

# Betrachtung von HTTPS (1/3)

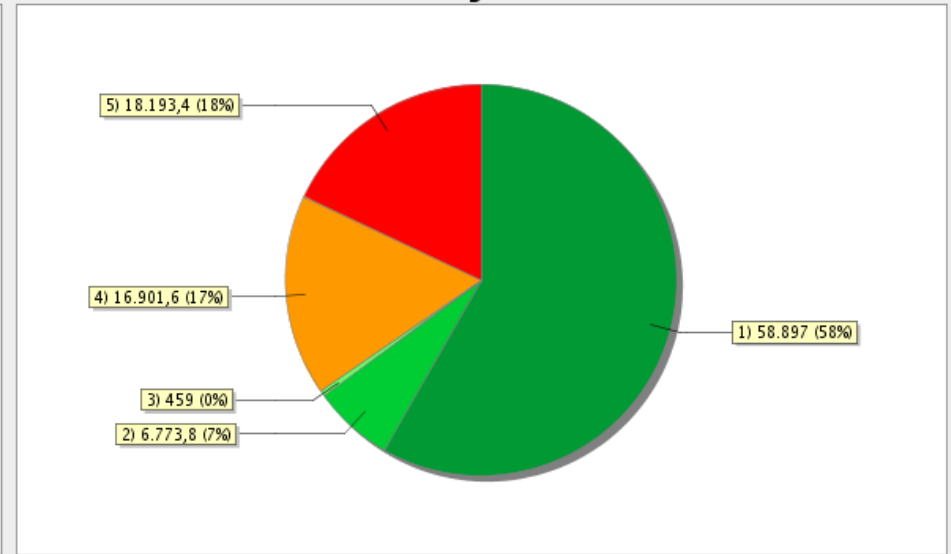
- Im Durchschnitt sind ca. 5 – 15% des HTTP-Verkehrs verschlüsselt
- FB Informatik Jan. 2007: RC4/{MD5,SHA1} 67%, AES/SHA1 33%
- FB Informatik Jan. 2008: RC4/{MD5,SHA1} 35%, AES/SHA1 65%

HTTPS FB5 Januar 2007



- 1) HTTPS (cipher/TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA)
- 2) HTTPS (cipher/TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA)
- 3) HTTPS (cipher/TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA)
- 4) HTTPS (cipher/TLS\_RSA\_WITH\_RC4\_128\_SHA)
- 5) HTTPS (cipher/TLS\_RSA\_WITH\_RC4\_128\_MD5)

HTTPS FB5 Januar 2008

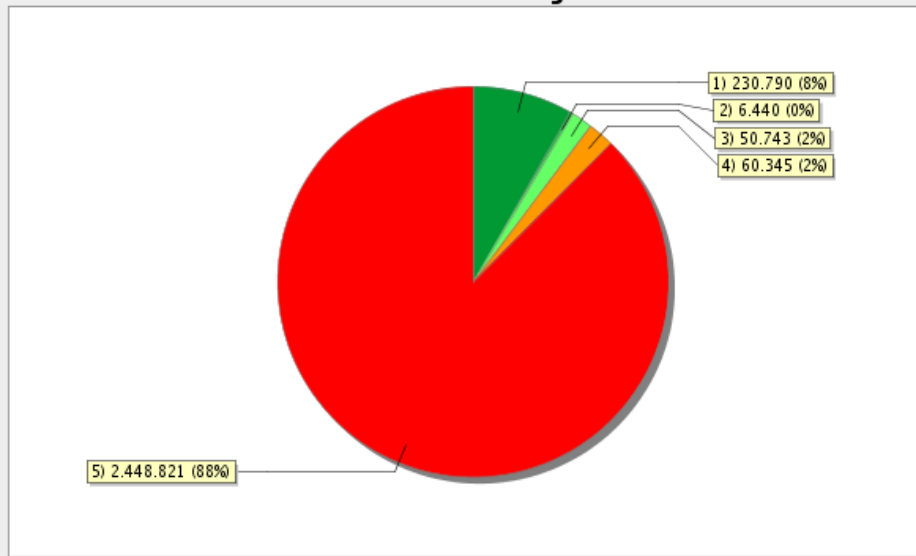


- 1) HTTPS (cipher/TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA)
- 2) HTTPS (cipher/TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA)
- 3) HTTPS (cipher/TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA)
- 4) HTTPS (cipher/TLS\_RSA\_WITH\_RC4\_128\_SHA)
- 5) HTTPS (cipher/TLS\_RSA\_WITH\_RC4\_128\_MD5)

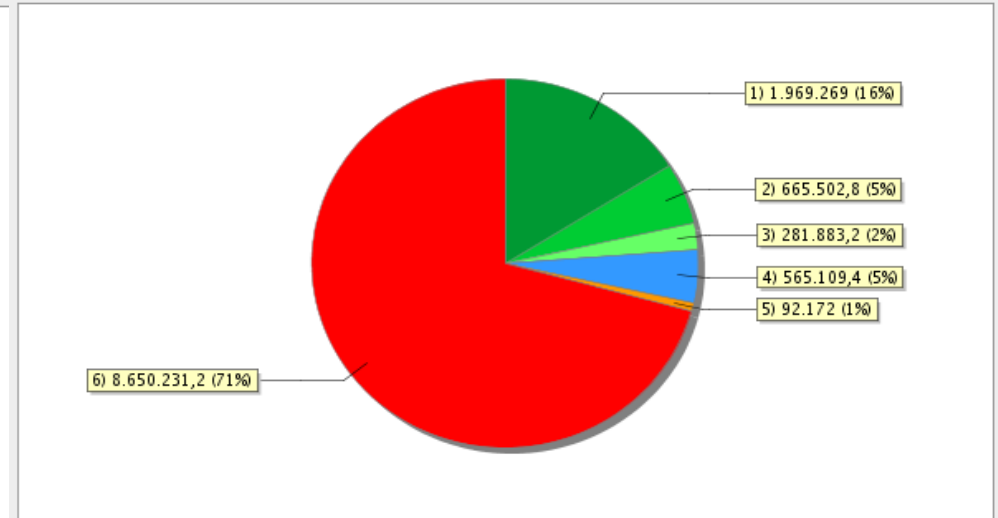
# Betrachtung von HTTPS (2/3)

- Business-Firma Jan. 2008: RC4/MD5 88%, AES/SHA1 10%
- Internet-Service-Provider 2008: RC4/MD5 71%, AES/SHA1 23%, Triple-DES/SHA1 5%

HTTPS Business-Firma Januar 2008



HTTPS Internet-Service-Provider 2008

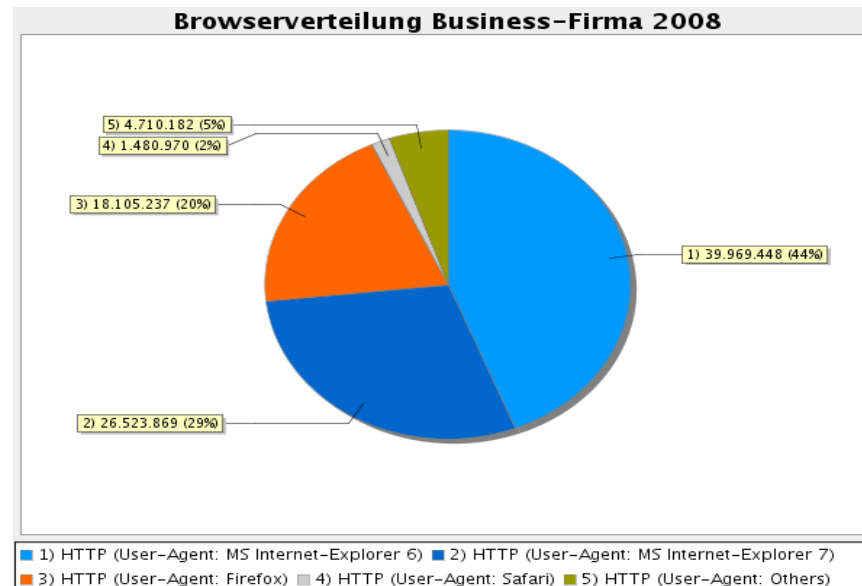


- 1) HTTPS (cipher/TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA)
- 2) HTTPS (cipher/TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA)
- 3) HTTPS (cipher/TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA)
- 4) HTTPS (cipher/TLS\_RSA\_WITH\_RC4\_128\_SHA)
- 5) HTTPS (cipher/TLS\_RSA\_WITH\_RC4\_128\_MD5)

- 1) HTTPS (cipher/TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA)
- 2) HTTPS (cipher/TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA)
- 3) HTTPS (cipher/TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA)
- 4) HTTPS (cipher/TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA)
- 5) HTTPS (cipher/TLS\_RSA\_WITH\_RC4\_128\_SHA)
- 6) HTTPS (cipher/TLS\_RSA\_WITH\_RC4\_128\_MD5)

# Betrachtung von HTTPS (3/3)

- Browser-Betrachtung bei der Business-Firma
  - Anteil des Internet-Explorer 6 beträgt 44% (verschlüsselt nur mit max. 128 Bit)
  - Vermutung: Die Web-Server verwenden noch zahlreiche veraltete Software-Komponenten und -Konfigurationen
  - Erklärt auch die gelegentliche Benutzung eines leeren Session-Keys (= Klartextübermittlung!)

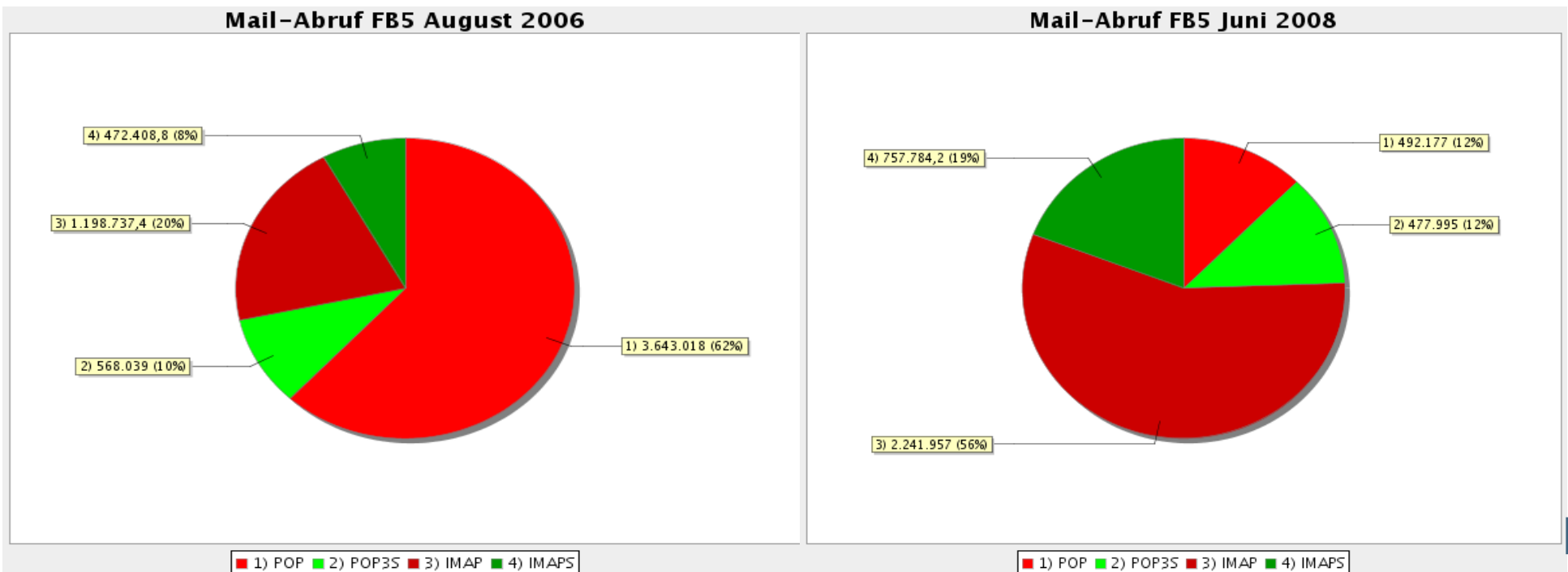


# Betrachtung von E-Mail-Verkehr (1/3)

- Versenden von E-Mails (SMTP(S)) im FB Informatik
  - Geringer Anteil von unter einem Prozent bei allen E-Mails überhaupt verschlüsselt
  - Bei Annahme einer SPAM-Rate von 80% bleiben 97% „echte“ E-Mails übrig, die unverschlüsselt übertragen werden

# Betrachtung von E-Mail-Verkehr (2/3)

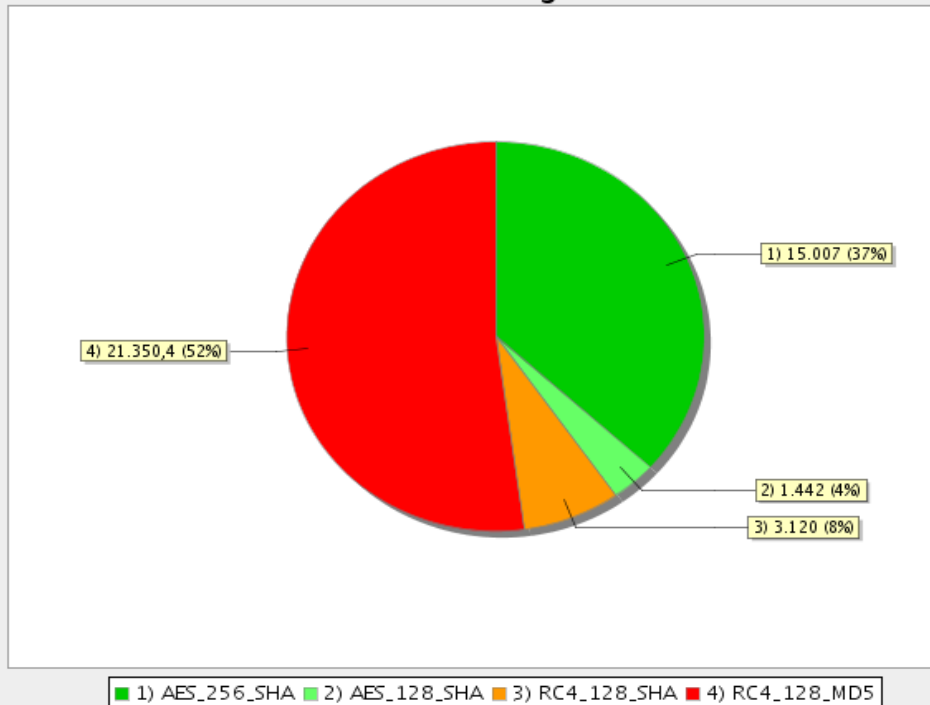
- Abrufen von E-Mails (POP3(S), IMAP(S)) im FB Informatik
  - Aug. 2006: 18% verschlüsselt, 82% unverschlüsselt
  - Jun. 2008: 32% verschlüsselt, 68% unverschlüsselt
  - Deutliche Zunahme von IMAP(S) (neuere Technologie) von 28% auf 76%



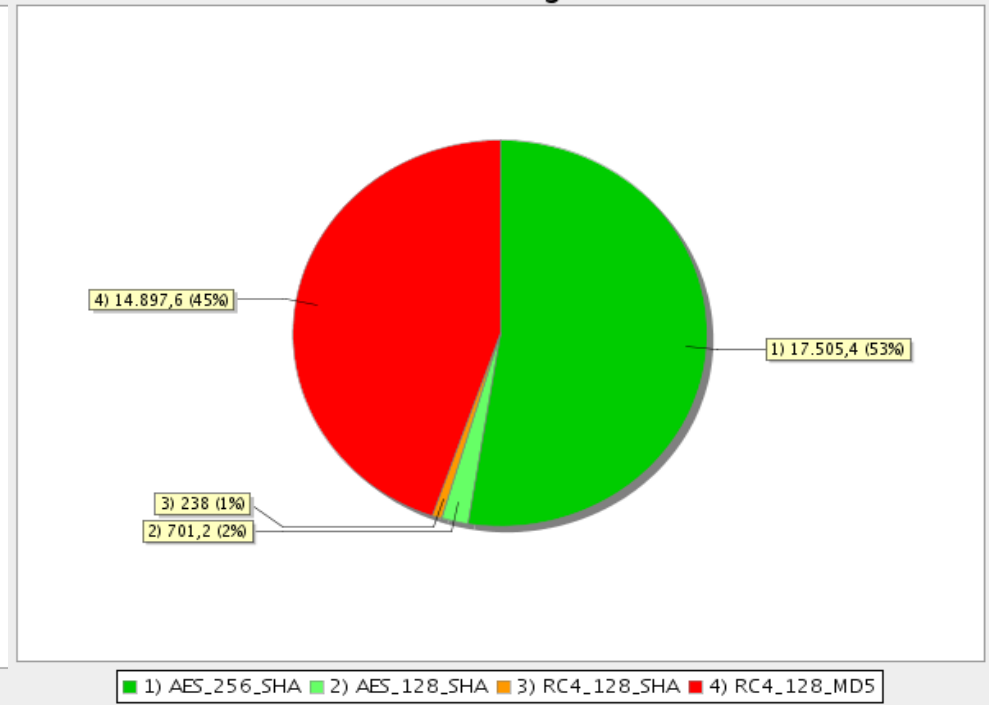
# Betrachtung von E-Mail-Verkehr (3/3)

- Verwendete Verschlüsselungsverfahren der Abrufe von E-Mails (POP3(S), IMAP(S)) im FB Informatik
  - Jahr 2006: RC4/MD5 52%, AES/SHA1 41%
  - Jahr 2008: RC4/MD5 45%, AES/SHA1 55%

Summenvergleich



Summenvergleich



- Erhöhung des Sicherheitsbewusstseins bei Benutzern und Server-Betreibern
- Server-Betreiber:
  - Stärkere Differenzierung der zu schützenden Informationen
  - Überprüfung verwendeter Verschlüsselungsverfahren mit Leitungsorientierten Analyse-Tools wie dem Internet-Analyse-System (IAS) und Optimierung der Server-Infrastruktur
- Benutzer:
  - Nutzung neuester, ausgereifter Programme
  - Konsequente Deaktivierung unsicherer Konfigurationseinstellungen

- Verschlüsselung von 5 – 15% beim gesamten HTTP-Verkehr kein wirkliches Problem
- Bei bis zu 88% der verschlüsselten HTTP-Kommunikation werden unsichere Verschlüsselungsverfahren benutzt -> Problem
- Genutzte Verschlüsselungen des E-Mail-Verkehrs mit bis zu 69% Klartext sehr gering
- Von diesen verschlüsselten Verbindungen sind rund 50% noch immer unsicher

**Besuchen Sie uns auch in Halle 9 am Stand D06**

**Vielen Dank für Ihre Aufmerksamkeit**

**Fragen ?**

**Dominique Petersen**  
**petersen (at) internet-sicherheit.de**

Institut für Internet-Sicherheit  
<https://www.internet-sicherheit.de>  
Fachhochschule Gelsenkirchen  
**CeBIT 2009, Halle 9, Stand D06**

