Konterkarierung von Secure-E-Mailing

- systemische Begegnung ist gefragt -

Dauer: 40 min (Vortrag inklusive Diskussion)

GI FG-SECMGT – Workshop am 03. Februar 2012

Unternehmensberatung *Holliday Consulting*

- gegründet Anfang 2004

- berät und begleitet Umsetzungen zu den Themen:

- **Informationssicherheit**
- **IT-Prozessmanagement**
- **IT-Servicemanagement nach ITIL**

- Internetadresse: www.holliday-consulting.com

Fundamente des Secure-E-Mailing

- **zwei Verfahrensweisen sind prinzipiell zu unterscheiden:**

  - symmetrische Verfahrensweise (sVw)
    - Absender & Empfänger benutzen denselben Schlüssel
    - nicht standardisiert, herstellerspezifische Lösungen

  - asymmetrische Verfahrensweise (aVw)
    - Absender & Empfänger benutzen unterschiedliche Schlüssel (Kombination aus öffentlichem & privatem Schlüssel)
    - standardisiert, von vielen Herstellern implementiert

Fundamente des Secure-E-Mailing

- **zwei Anwendungsstandards bei aVw gibt es:**
  (jeweils gepflegt von der *I*nternet *E*ngineering *T*ask *F*orce)

  - S/MIME (**S**ecure/**M**ultipurpose **I**nternet **M**ail **E**xtensions)
    - realisiert mittels X.509-basierter Zertifikate
    - Standard geregelt in Request(s) for Comments (RFC)
      - initial 10/1995 in RFC 1847 (Security Multiparts for MIME)
      - gereift 03/1998 in RFC 2311 (S/MIME V2.0 Message Specification) und RFC 2312 (S/MIME V2.0 Certificate Handling)
      - aktuell Version S/MIME V3.2 in Gebrauch nach RFC 5751

  - OpenPGP (**P**retty **G**ood **P**rivacy nach Phil Zimmermann)
    - realisiert mittels Public-Key-Verfahren & Web-of-Trust
    - Standard geregelt in RFC 4880 (OpenPGP Message Format)
    - dabei zwei Formate in Gebrauch:
      - PGP/INLINE -> ursprüngliches Format, nicht streng standardisiert
      - PGP/MIME -> neueres Format aktuell nach RFC 3156 geregelt

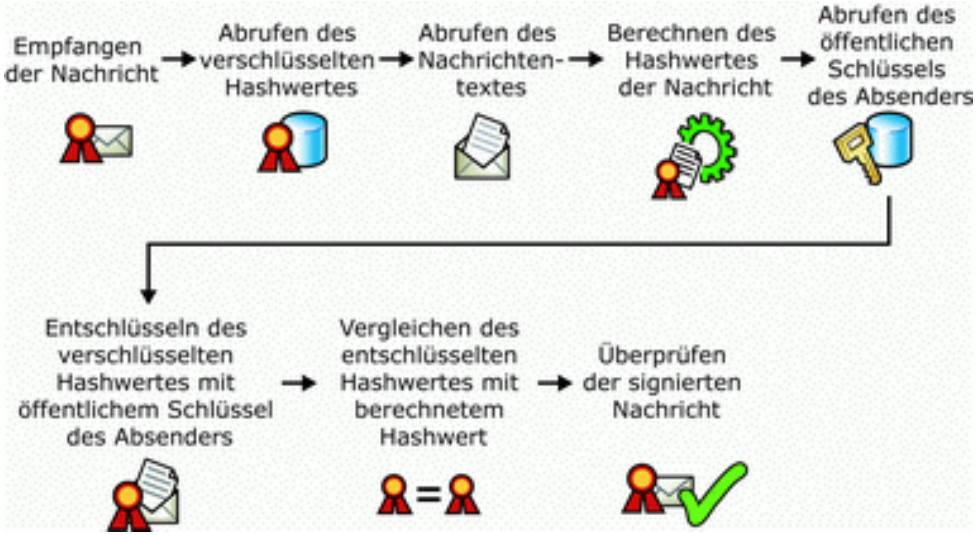
Fundamente des Secure-E-Mailing

- **zwei Anwendungsrichtungen bei aVw mit jeweils eigenen Sicherheitszielen sind zu unterscheiden:**
  - das Signieren einer Nachricht zum Zwecke der Überprüfbarkeit
    - der Datenintegrität der Nachricht (Integrität)
    - der Authentizität der Nachricht (Authentizität)
  - das Verschlüsseln einer Nachricht zum Zwecke der
    - vertraulichen Übermittlung der Nachricht (Vertraulichkeit)

Fundamente des Secure-E-Mailing

- Schema des Signierens einer Nachricht auf der Absender-Seite:

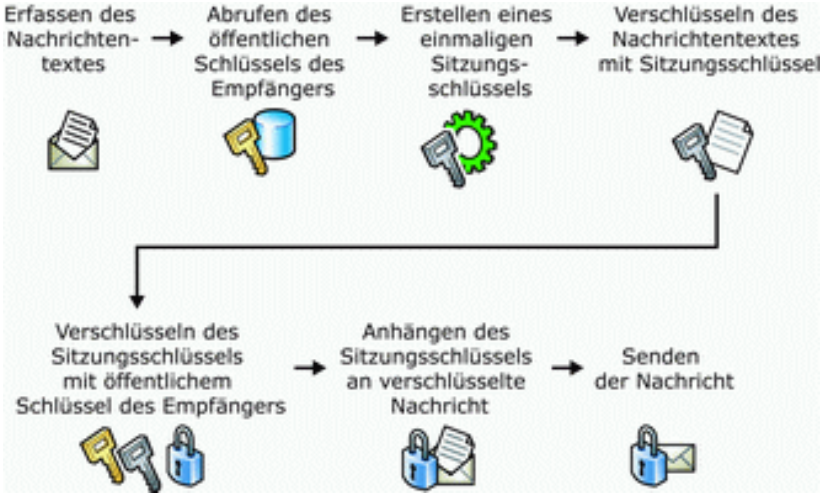
- Schema der Signaturprüfung auf der Empfänger-Seite:



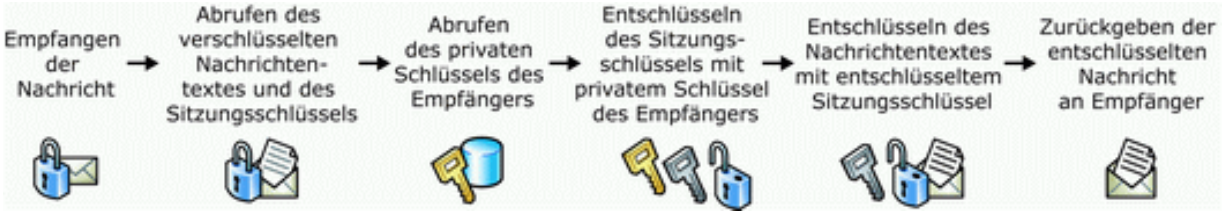
Quelle:
Microsoft TechNet-Bibliothek

Fundamente des Secure-E-Mailing

- Schema des Verschlüsselns auf der Absender-Seite:

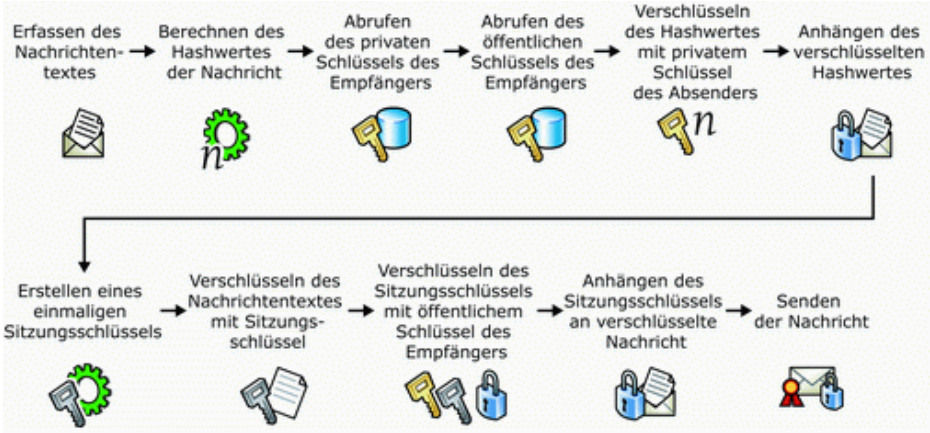


- Schema des Entschlüsselns auf der Empfänger-Seite:

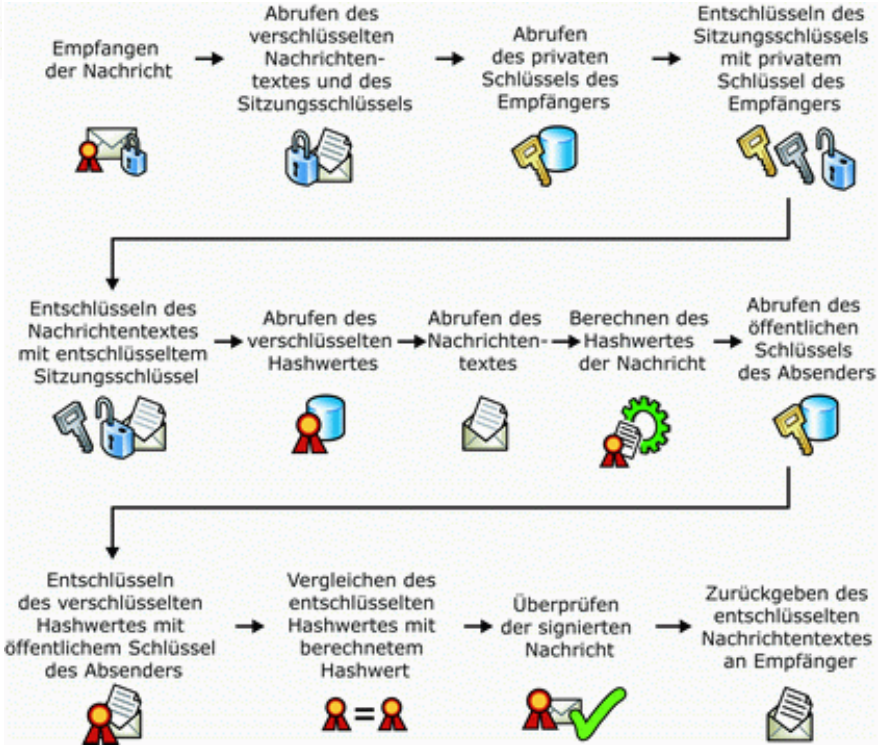


Quelle:
Microsoft TechNet-Bibliothek

Fundamente des Secure-E-Mailing



Schema des Signierens/Verschlüsselns auf der Absender-Seite



Schema der Signaturprüfung/ Entschlüsselung auf der Empfänger-Seite

Quelle:
Microsoft TechNet-Bibliothek

Fallstricke beim Secure-E-Mailing

- **zu verzeichnende Phänomene:**

1) (noch) geringer Verbreitungsgrad

2) falsche Sicherheitsannahmen

3) fehlerbehaftete Anwendung

4) unterschätzte Infrastrukturerfordernisse

5) unterschätzte Erfordernisse organisatorischer Kontinuität

6) zusätzliche Compliance-Anforderungen

7) Sicherheitsstörfälle bei wichtigen Konzeptbestandteilen

Fallstrick 1: Verbreitungsgrad

- **Phänomen: (noch) geringer Verbreitungsgrad**
  - vorwiegend nur bei Großunternehmen (DAX-Konzerne) im Gebrauch
  - gerade bei den KMUs (80 % aller angestellt Beschäftigten[1]) mit existentiellem Know-how-Schutzbedarf gering verbreitet

(Wie wir so schön in unserer Diskussion festgestellt haben:
THE PAIN IS NOT ENOUGH.)

Quelle: 1. Institut für Mittelstandsforschung (IfM), Bonn

Fallstrick 2: Falsche Annahmen

- **Phänomen: falsche Sicherheitsannahmen**
  - Beispiel: falsche Annahme des Wirkbereichs

Nach RFC 5322 besteht eine E-Mail aus:

- einer Header Section (E-Mail-Header) mit Header Fields (Absender, Empfänger, Betreff, Datum)

und

- einem E-Mail-Body (der eigentliche Nachrichteninhalt)

ABER: nur der E-Mail-Body wird signiert und/oder verschlüsselt

d.h.: eine nur im Header verfälschte E-Mail weist nach wie vor eine gültige Signatur aus!

(Seit S/MIME V3.1 bietet sich hierzu als technische Lösung das anfangs erwähnte „triple-wrapping“ an.)

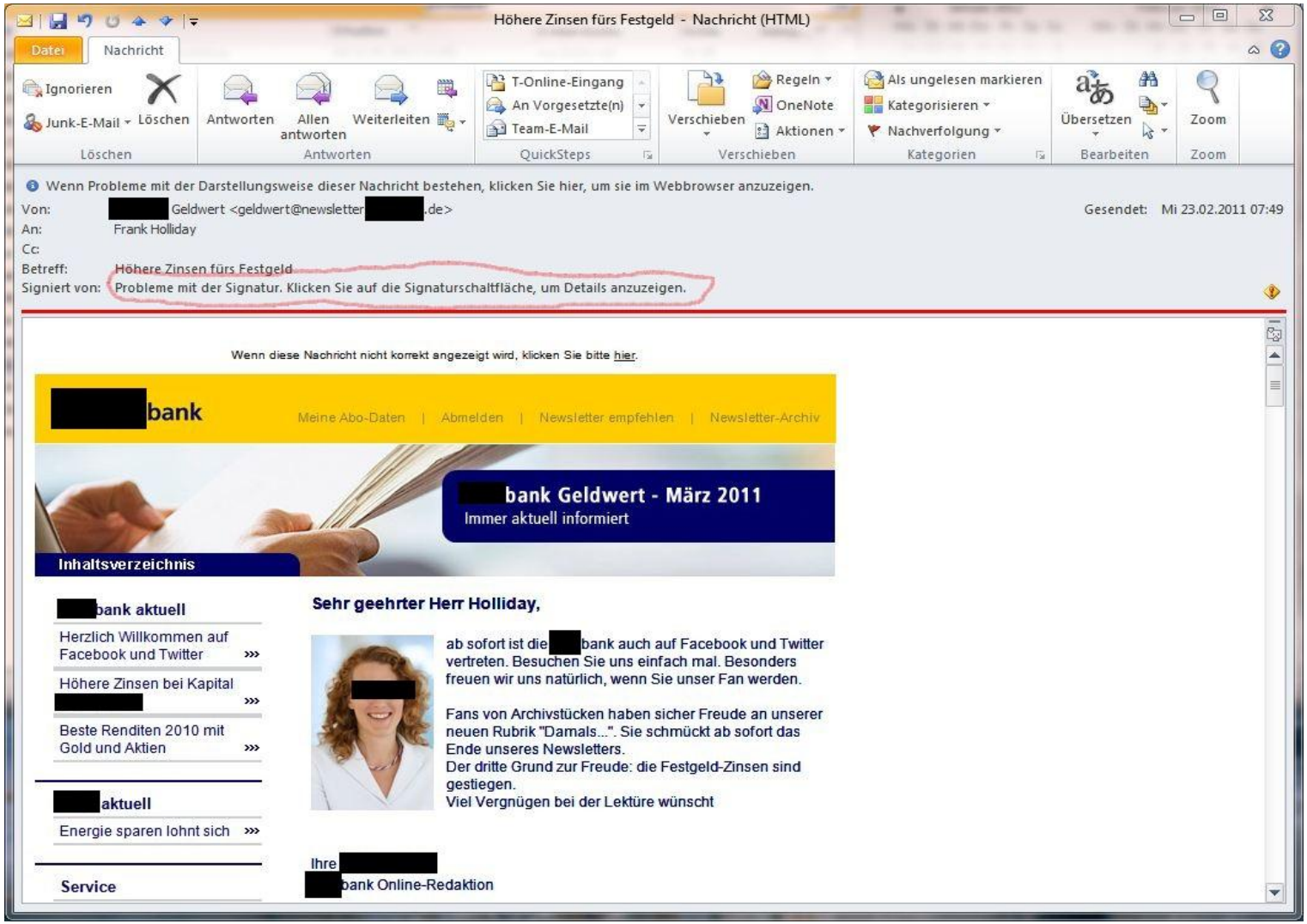
Fallstrick 3: Anwendung mit Fehler

- **Phänomen: fehlerbehaftete Anwendung**
  - Beispiel: Nachverarbeitung des E-Mail-Bodys nach erfolgter Signierung und/oder Verschlüsselung, im speziellen z.B. durch ein anschließendes Unterdrücken zusätzlicher Leerzeichen oder Leerzeilen im Mail-Text

    - so simpel der Fehler auch scheint, dass kann auch Großunternehmen passieren:

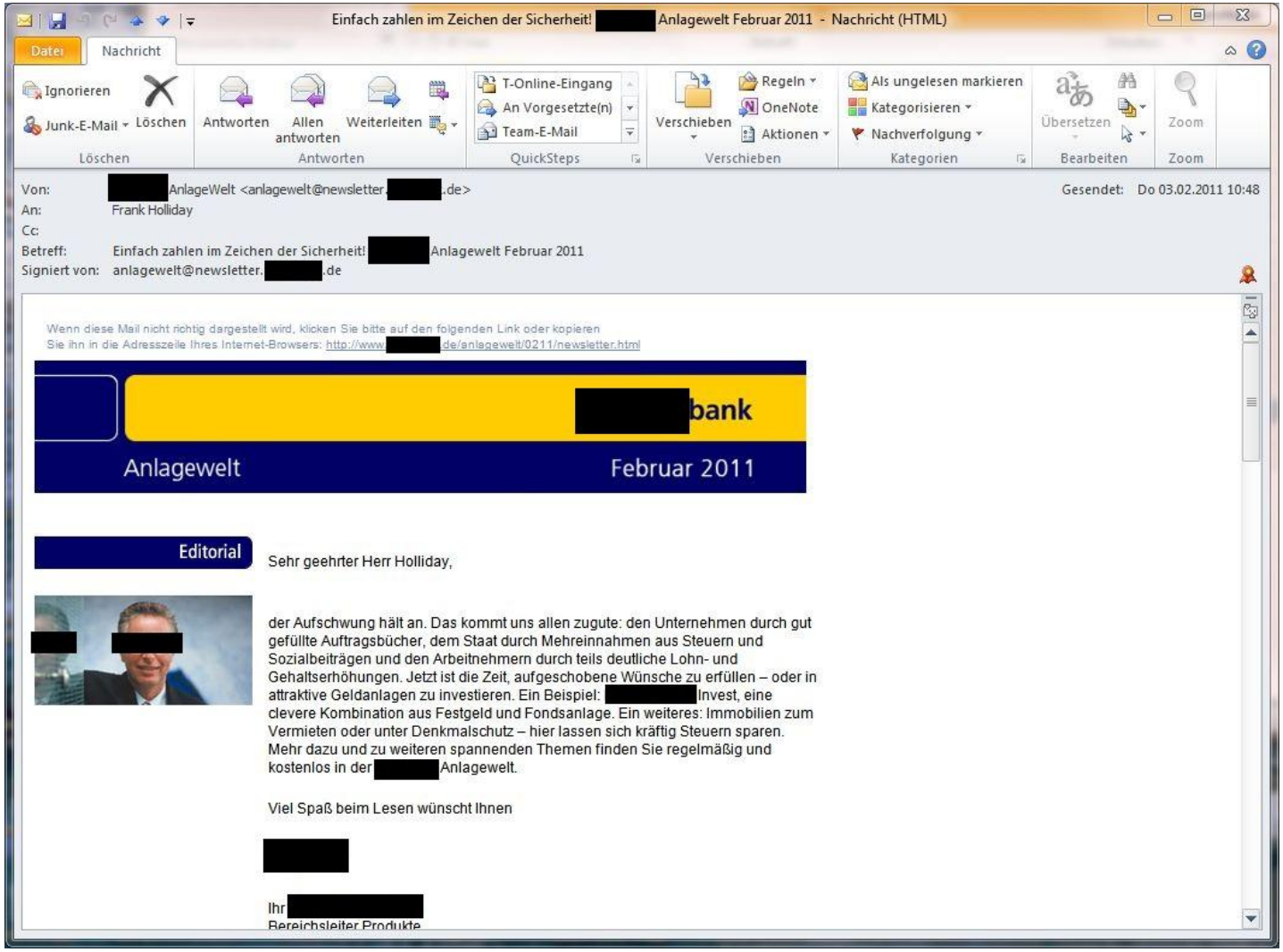
(Hier kann einfach nur gesagt werden: IS-Status-Kontrolltests sind eigentlich Standards im IS-Prozess-Geschehen.)

Fallstrick 3: Anwendung mit Fehler

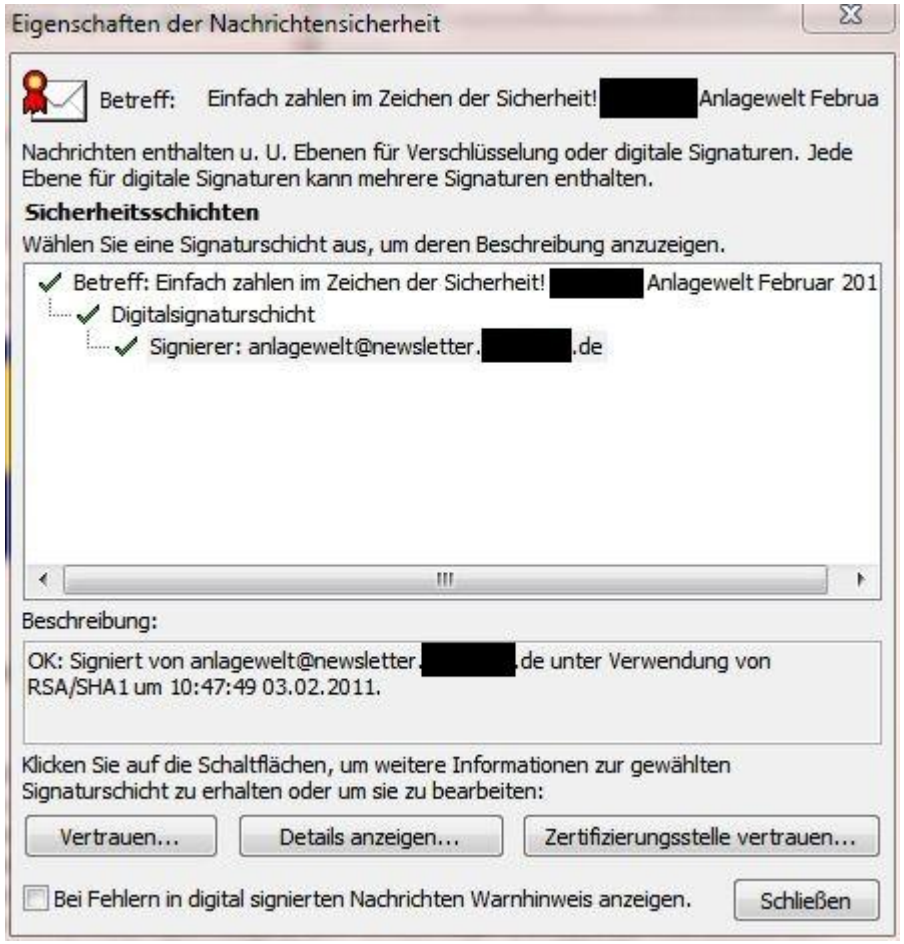


Fallstrick 3: Anwendung mit Fehler

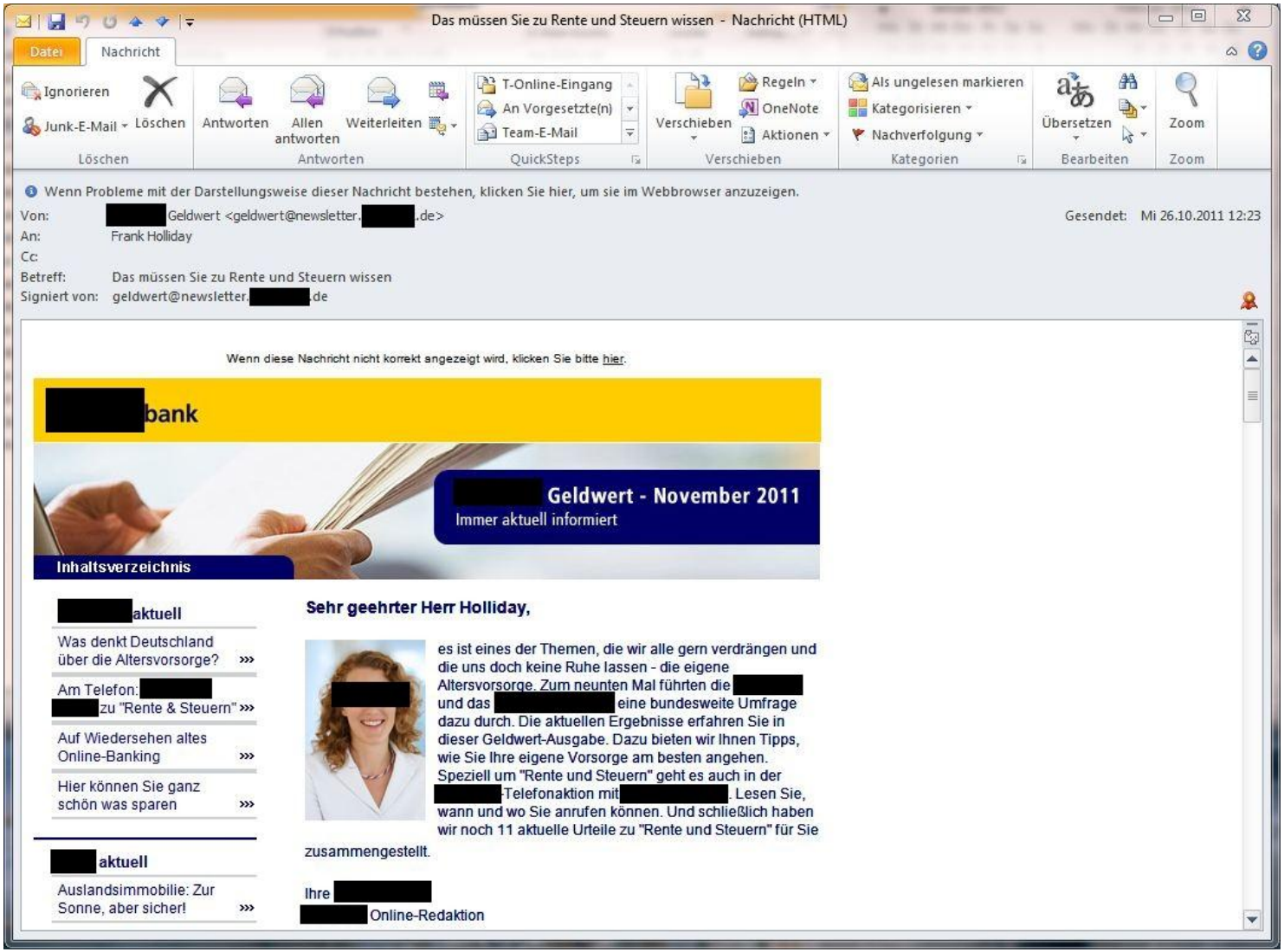
Fallstrick 3: Anwendung ohne Fehler



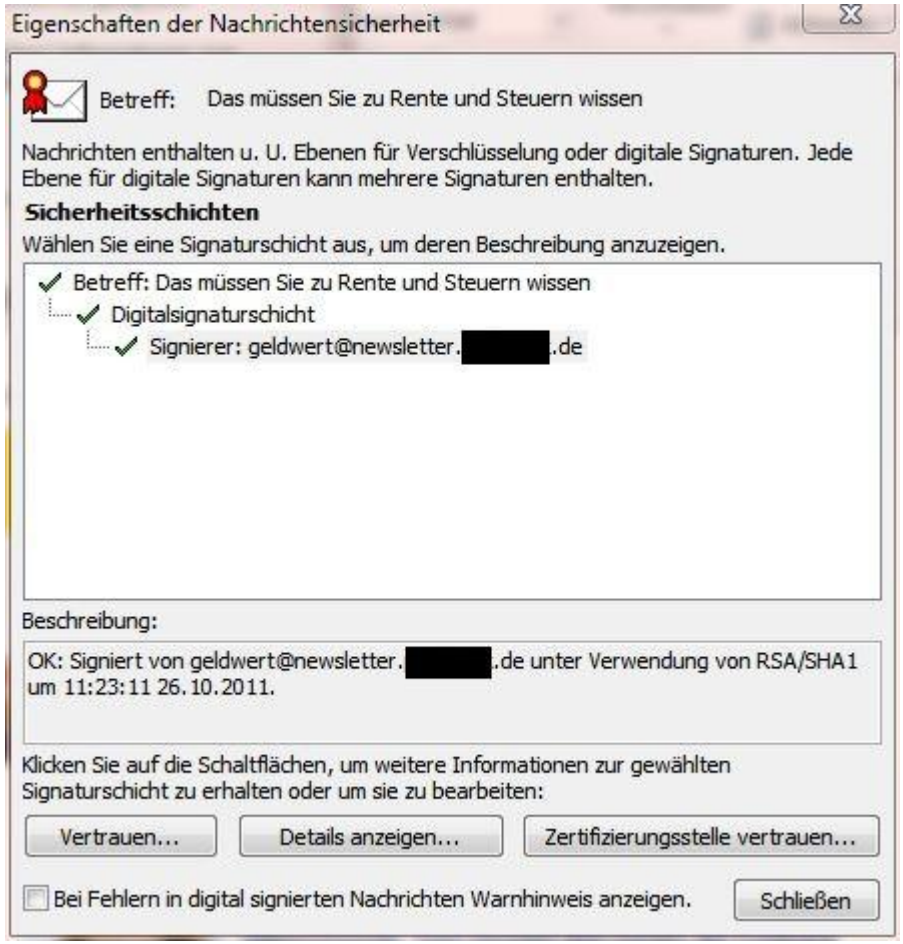
Fallstrick 3: Anwendung ohne Fehler



Fallstrick 3: Anwendung ohne Fehler



Fallstrick 3: Anwendung ohne Fehler



Fallstrick 4: Infrastruktur

- **Phänomen: unterschätzte Infrastrukturerfordernisse**

  - bei Unternehmen ist der Einsatz einer **P**ublic-**K**ey-**I**nfrastructure unabdingbar

  - ohne zentrale Secure-E-Mail-Handling- und Key-Management-Dienste sind Mitarbeiter eines Unternehmens mit dem Handling leicht überfordert

  - wegen dem geringen Verbreitungsgrad und inhomogener Systemimplementierungen sind Systembrüche die Regel, es müssen Sonderverfahren zur Verfügung stehen

    (Als Nothammer kommt hier sVw ins Spiel, z.B. mithilfe der Krypto-Open Source ‚TrueCrypt' Nachricht in einen zu kreierenden TrueCrypt file container (Empfehlung: AES-256bit-encryption mit Hash-Algorithmus SHA-2) stecken, dem Empfänger der Nachricht das ‚Volume Password' (Empfehlung: Passwort-Entropie >= 128 bits) per SMS schicken. That's it.)

Fallstrick 5: organisat. Kontinuität

- **Phänomen: unterschätzte Erfordernisse organisatorischer Kontinuität**

  - Zertifikate laufen schon auch aus Sicherheitsgründen ab, ein reibungsloses BCM des Zertifikatswesens ist unabdingbar

  - auch Zertifikatsaussteller können Lieferschwierigkeiten haben

  - zahlreiche Internet-Dienste müssen zuverlässig und sicher betrieben werden (z.B. LDAP, Webservices bei XKMS-Einsatz, CRL, OCSP etc.)

(Hier ist wirklich eine systemische Verbesserung gefragt. Technische Ansätze dazu gibt es schon, z.B. DKIM (siehe RFC 4871), DNSSEC-Nutzung durch PKA oder DNS-CERT (siehe RFC 4398). Die richtige systemische Lösung wäre aber die Schaffung eines weltweiten Zertifikate-Internet-Dienstes.)

Fallstrick 6: Compliance-Zusätze

- **Phänomen: zusätzliche Compliance-Anforderungen**
  - bei zwangsweiser Mailverschlüsselung und –signatur bedarf es der Zustimmung eines vorhandenen Betriebsrats bzw. eines Interessensausgleichs mit den Mitarbeitern
  - die Sterblichkeit von Schlüsseln und Zertifikaten bedarf einer konzeptuellen Adressierung bei der Umsetzung von gesetzlichen Archivierungspflichten und Datensicherungsmassnahmen

Fallstrick 7: fundamentale Störfälle

- **Phänomen: Sicherheitsstörfälle bei wichtigen Konzeptbestandteilen**
  - beim hierarchisch geprägten Vertrauenssystem von X.509-Zertifikaten (S/MIME) ist die Kompromittierung von vertrauens-verankernden Wurzelzertifikaten (IS-GAU) ein nicht mehr von der Hand zu weisendes Risiko (siehe DigiNotar Certificate Authority Einbruch Mitte 2011, Comodo-Zertifikatsdiebstahl Anfang 2011, RSA SecurID Einbruch März 2011)

(Wenn dann mal die Quantencomputerisierung real wird, ist obiger Konzeptbestandteil eh obsolet geworden;-)

Diskussion - Systemische Begegnung

- **Was systemisch tun beim Phänomen:**

1) (noch) geringer Verbreitungsgrad

2) falsche Sicherheitsannahmen

3) fehlerbehaftete Anwendung

4) unterschätzte Infrastrukturerfordernisse

5) unterschätzte Erfordernisse organisatorischer Kontinuität

6) zusätzliche Compliance-Anforderungen

7) Sicherheitsstörfälle bei wichtigen Konzeptbestandteilen

bedankt sich für Ihre Aufmerksamkeit und wünscht Ihnen weiter gutes Gelingen für die Informationssicherheit!

www.holliday-consulting.com