

Konterkarrierung 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-Service-Management nach ITIL**
- **Internetadresse:** www.holliday-consulting.com



■ 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 *Internet Engineering Task Force*)
 - ◆ 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

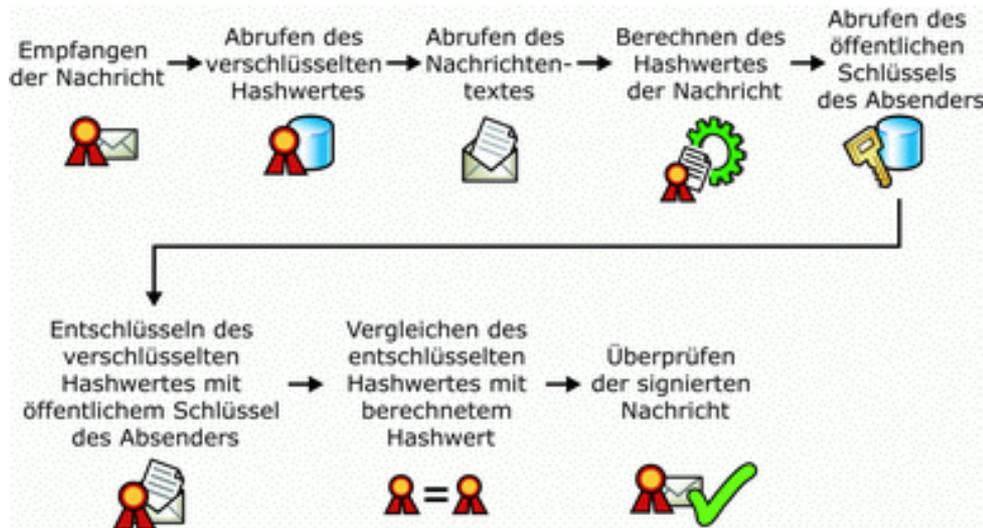
- **zwei Anwendungsrichtungen bei aVw mit jeweils eigenen Sicherheitszielen sind zu unterscheiden:**
 - ◆ das Signieren einer Nachricht zum Zwecke der Überprüfbarkeit
 - der Datenintegrität der Nachricht (Integrität)
 - der Authentizität der Nachricht (Authentizität)
 - ◆ das Verschlüsseln einer Nachricht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

Fundamente des Secure-E-Mailing

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



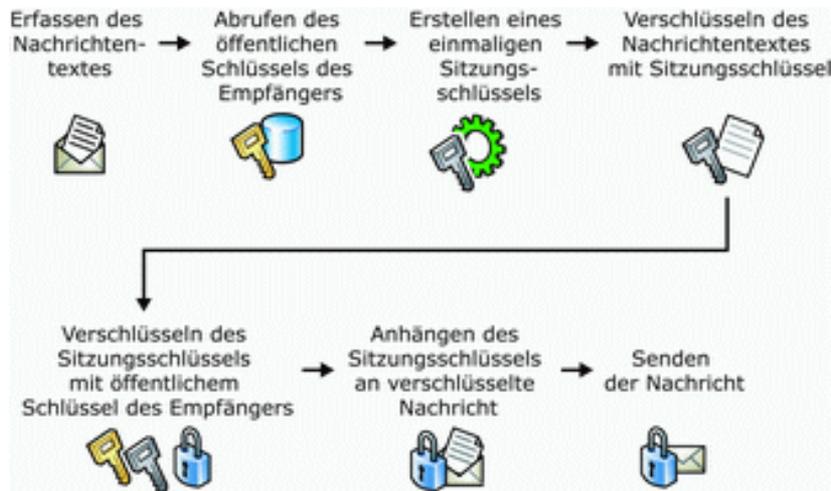
- ◆ Schema der Signaturprüfung auf der Empfänger-Seite:



Quelle:
Microsoft TechNet-Bibliothek

Fundamente des Secure-E-Mailing

- ◆ Schema des Verschlüsseln auf der Absender-Seite:

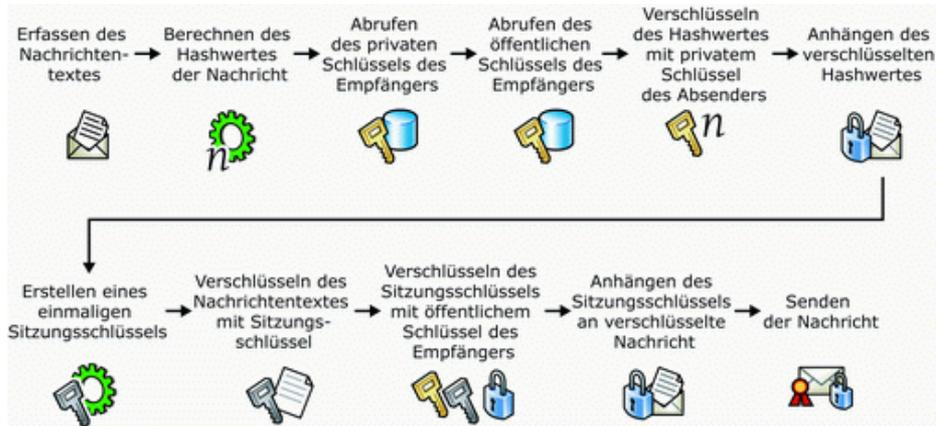


- ◆ Schema des Entschlüsselns auf der Empfänger-Seite:



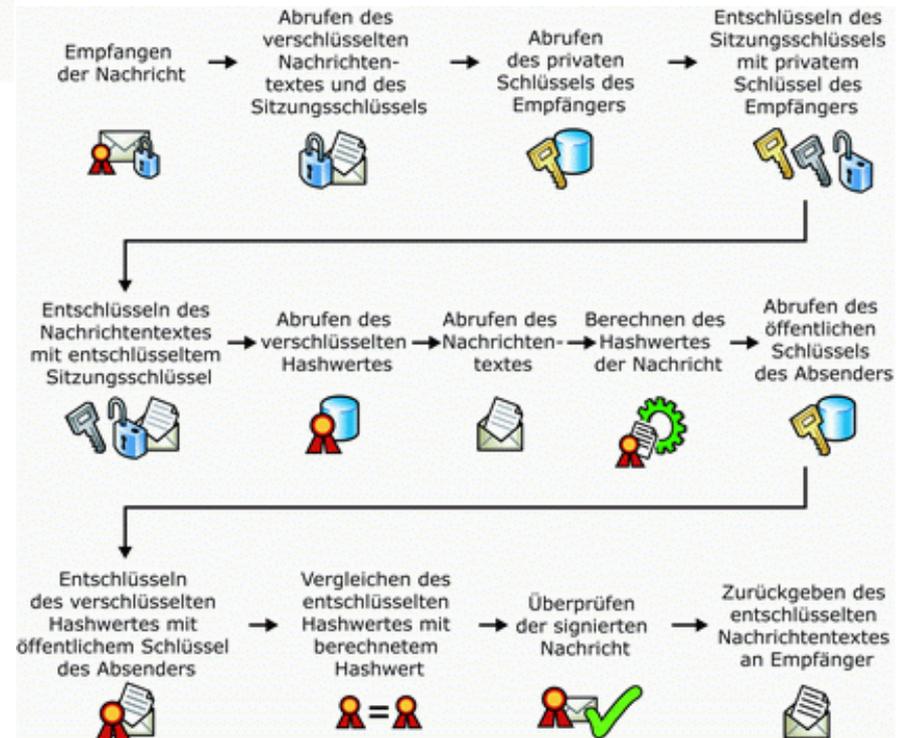
Quelle:
Microsoft TechNet-Bibliothek

Fundamente des Secure-E-Mailing



Schema des Signierens/Verschlüsseln 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 Beschäftigten¹) mit existentielltem Know-how-Schutzbedarf gering verbreitet

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

Fallstrick 2: Falsche Annahmen

■ Phänomen: falsche Sicherheitsannahmen

- ◆ Beispiel: falsche Annahme des Wirkungsbereichs

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

The screenshot shows an Outlook window titled "Höhere Zinsen fürs Festgeld - Nachricht (HTML)". The ribbon includes "Datei" and "Nachricht" tabs. The "Nachricht" ribbon has various actions like "Ignorieren", "Löschen", "Antworten", "Allen antworten", "Weiterleiten", "T-Online-Eingang", "An Vorgesetzte(n)", "Team-E-Mail", "Verschieben", "Regeln", "OneNote", "Aktionen", "Als ungelesen markieren", "Kategorisieren", "Nachverfolgung", "Übersetzen", and "Zoom".

The email header shows:
Von: [redacted] Geldwert <geldwert@newsletter.[redacted].de>
An: Frank Holliday
Cc:
Betreff: Höhere Zinsen fürs Festgeld
Signiert von: Probleme mit der Signatur. Klicken Sie auf die Signaturschaltfläche, um Details anzuzeigen.

The main content of the email is a newsletter from "bank". It features a yellow header with the bank logo and navigation links: "Meine Abo-Daten", "Abmelden", "Newsletter empfehlen", and "Newsletter-Archiv". Below the header is a blue banner for "bank Geldwert - März 2011" with the tagline "Immer aktuell informiert".

The newsletter content includes an "Inhaltsverzeichnis" section with links to "bank aktuell", "Herzlich Willkommen auf Facebook und Twitter", "Höhere Zinsen bei Kapital", and "Beste Renditen 2010 mit Gold und Aktien".

The main body of the newsletter features a photo of a woman and the text:
Sehr geehrter Herr Holliday,
ab sofort ist die bank auch auf Facebook und Twitter vertreten. Besuchen Sie uns einfach mal. Besonders freuen wir uns natürlich, wenn Sie unser Fan werden.
Fans von Archivstücken haben sicher Freude an unserer neuen Rubrik "Damals...". Sie schmückt ab sofort das Ende unseres Newsletters.
Der dritte Grund zur Freude: die Festgeld-Zinsen sind gestiegen.
Viel Vergnügen bei der Lektüre wünscht

The footer of the newsletter includes "Ihre bank Online-Redaktion".

A red circle highlights the "Signiert von:" line in the email header, indicating a signature error.

Fallstrick 3: Anwendung mit Fehler

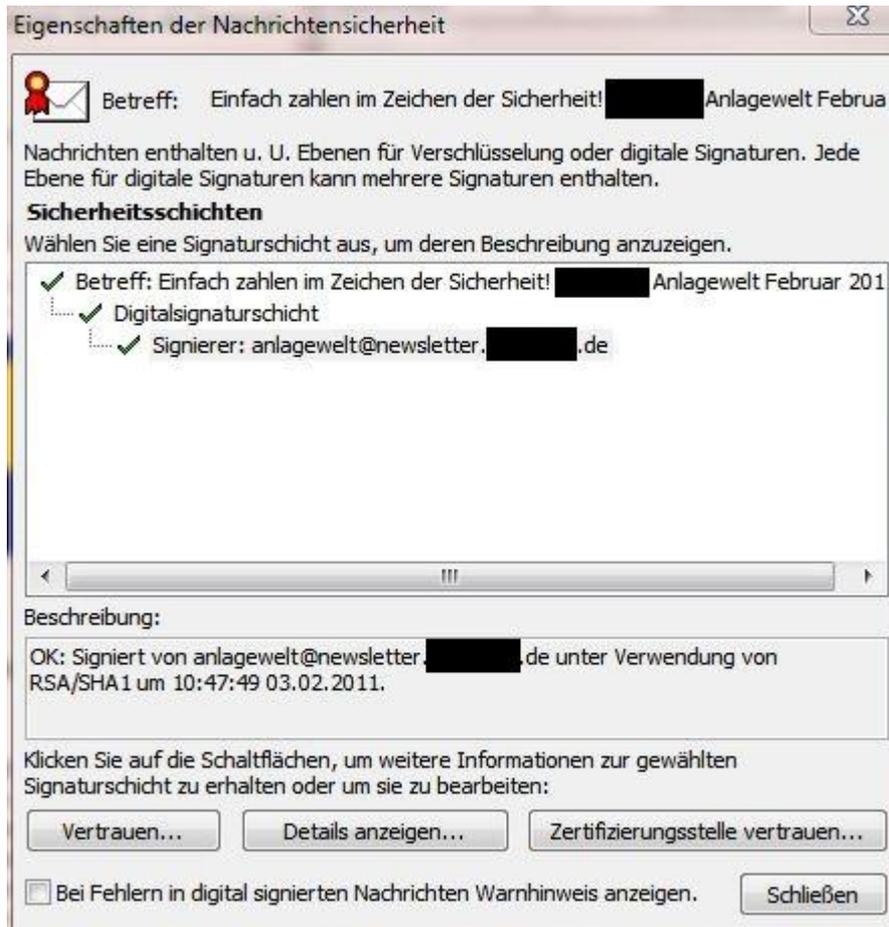


Fallstrick 3: Anwendung ohne Fehler

The screenshot shows an Outlook window with the following details:

- Title Bar:** Einfach zahlen im Zeichen der Sicherheit! [redacted] AnlageWelt Februar 2011 - Nachricht (HTML)
- Toolbar:** Includes icons for Ignorieren, Junk-E-Mail, Löschen, Antworten, Allen antworten, Weiterleiten, T-Online-Eingang, An Vorgesetzte(n), Team-E-Mail, Verschieben, Regeln, OneNote, Aktionen, Nachverfolgung, Übersetzen, and Zoom.
- Header:**
 - Von: [redacted] AnlageWelt <anlagewelt@newsletter.[redacted].de>
 - An: Frank Holliday
 - Cc:
 - Betreff: Einfach zahlen im Zeichen der Sicherheit! [redacted] AnlageWelt Februar 2011
 - Signiert von: anlagewelt@newsletter.[redacted].de
 - Gesendet: Do 03.02.2011 10:48
- Body:**
 - Wenn diese Mail nicht richtig dargestellt wird, klicken Sie bitte auf den folgenden Link oder kopieren Sie ihn in die Adresszeile Ihres Internet-Browsers: [http://www.\[redacted\].de/anlagewelt/0211/newsletter.html](http://www.[redacted].de/anlagewelt/0211/newsletter.html)
 - Header:** [redacted] bank, Anlagewelt, Februar 2011
 - Section:** Editorial
 - Text:** Sehr geehrter Herr Holliday,
 - Image:** A small portrait of a man in a suit.
 - Main Text:** der Aufschwung hält an. Das kommt uns allen zugute: den Unternehmen durch gut gefüllte Auftragsbücher, dem Staat durch Mehreinnahmen aus Steuern und Sozialbeiträgen und den Arbeitnehmern durch teils deutliche Lohn- und Gehaltserhöhungen. Jetzt ist die Zeit, aufgeschobene Wünsche zu erfüllen – oder in attraktive Geldanlagen zu investieren. Ein Beispiel: [redacted] Invest, eine clevere Kombination aus Festgeld und Fondsanlage. Ein weiteres: Immobilien zum Vermieten oder unter Denkmalschutz – hier lassen sich kräftig Steuern sparen. Mehr dazu und zu weiteren spannenden Themen finden Sie regelmäßig und kostenlos in der [redacted] Anlagewelt.
 - Closing:** Viel Spaß beim Lesen wünscht Ihnen [redacted]
 - Signature:** Ihr [redacted], Bereichsleiter Produkte

Fallstrick 3: Anwendung ohne Fehler



Fallstrick 3: Anwendung ohne Fehler

Das müssen Sie zu Rente und Steuern wissen - Nachricht (HTML)

Daten Nachricht

Ignorieren Löschen Antworten Allen antworten Weiterleiten T-Online-Eingang An Vorgesetzte(n) Team-E-Mail Verschieben Regeln OneNote Aktionen Als ungelesen markieren Kategorisieren Nachverfolgung Übersetzen Zoom

Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.

Von: [redacted] Geldwert <geldwert@newsletter.[redacted].de> Gesendet: Mi 26.10.2011 12:23
An: Frank Holliday
Cc:
Betreff: Das müssen Sie zu Rente und Steuern wissen
Signiert von: geldwert@newsletter.[redacted].de

Wenn diese Nachricht nicht korrekt angezeigt wird, klicken Sie bitte [hier](#).

[redacted] bank

Geldwert - November 2011
Immer aktuell informiert

Inhaltsverzeichnis

[redacted] aktuell

Was denkt Deutschland über die Altersvorsorge? >>>
Am Telefon: [redacted] zu "Rente & Steuern" >>>
Auf Wiedersehen altes Online-Banking >>>
Hier können Sie ganz schön was sparen >>>

[redacted] aktuell

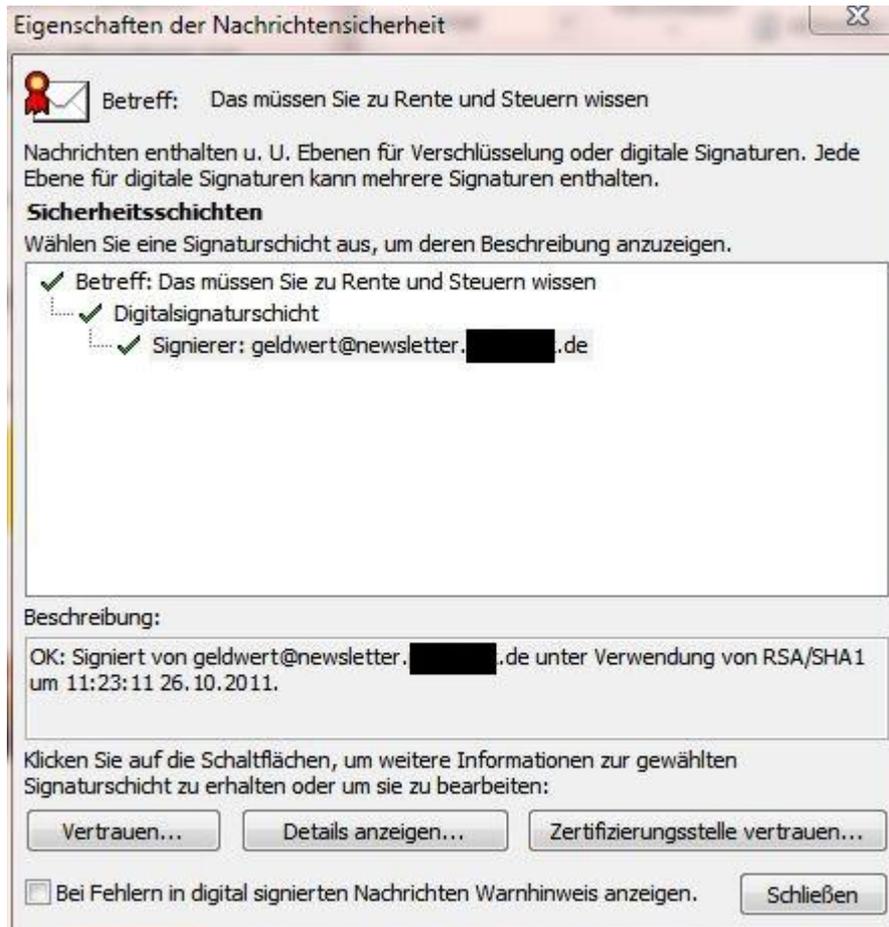
Auslandsimmobilie: Zur Sonne, aber sicher! >>>

Sehr geehrter Herr Holliday,

 es ist eines der Themen, die wir alle gern verdrängen und die uns doch keine Ruhe lassen - die eigene Altersvorsorge. Zum neunten Mal führten die [redacted] und das [redacted] eine bundesweite Umfrage dazu durch. Die aktuellen Ergebnisse erfahren Sie in dieser Geldwert-Ausgabe. Dazu bieten wir Ihnen Tipps, wie Sie Ihre eigene Vorsorge am besten angehen. Speziell um "Rente und Steuern" geht es auch in der [redacted] Telefonaktion mit [redacted]. Lesen Sie, wann und wo Sie anrufen können. Und schließlich haben wir noch 11 aktuelle Urteile zu "Rente und Steuern" für Sie zusammengestellt.

Ihre [redacted]
[redacted] Online-Redaktion

Fallstrick 3: Anwendung ohne Fehler



Fallstrick 4: Infrastruktur

■ Phänomen: unterschätzte Infrastrukturerfordernisse

- ◆ bei Unternehmen ist der Einsatz einer **Public-Key-Infrastructure** 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](#) \geq 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.)

■ Phänomen: zusätzliche Compliance-Anforderungen

- ◆ bei zwangsweiser Mailverschlüsselung und –signatur bedarf es der Zustimmung eines vorhandenen Betriebsrats bzw. eines Interessenausgleichs 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 vertrauensverankernden 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;-)

■ **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

Holliday Consulting - Dipl.-Ing. Frank W. Holliday

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

www.holliday-consulting.com

