Notizen:

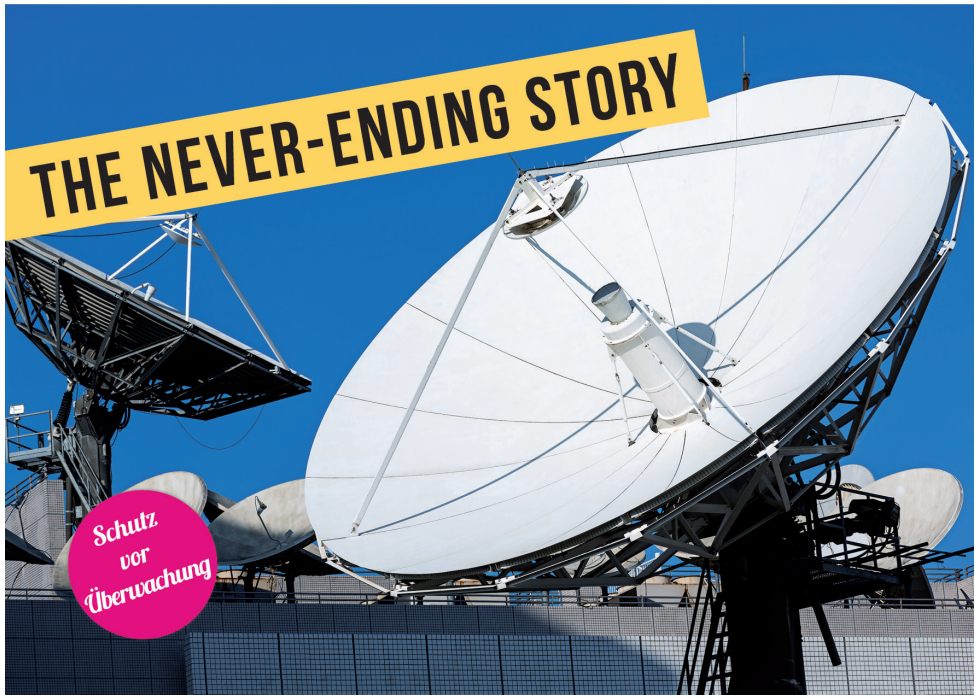
Veranstalter

KIT-Si Karlsruher IT-Sicherheitsinitiative

zkm karlsruhe

CyberForum HIGHTECH. UNTERNEHMER. NETZWERK.

KASTEL



ANTI-PRISM-PARTY

4. Staffel

KARLSRUHE SCHÜTZT SICH SELBST
ANTI-PRISM-PARTY
WWW.ANTI-PRISM-PARTY.DE

- STATION NR. 3 -

E-Mail-Verschlüsselung

E-MAIL-VERSCHLÜSSELUNG

Welches Problem wird gelöst?

- Elektronische Post (E-Mail) wird oft „einfach so“ versendet und empfangen, sowohl im privaten wie auch im geschäftlichen Umfeld. Hierbei vertrauen die Nutzer darauf, dass alle am System beteiligten Komponenten fehlerfrei funktionieren und „sicher“ sind.
- Hiervon kann in der Praxis nicht ausgegangen werden. Eine E-Mail ist de facto weniger vertraulich als eine Postkarte und kann leicht manipuliert werden. Gerade dann (aber nicht nur dann), wenn sie verwendet wird, um „sensible“ Daten zu übermitteln, sind (zusätzliche) Schutzmaßnahmen sinnvoll.
- Heute wird alles mögliche als „E-Mail-Verschlüsselung“ bezeichnet: von der Word-Datei mit Öffnen-Passwort über eine Transportverschlüsselung bis zu PGP. An diesem Stand geht es um Ende-zu-Ende-verschlüsselte E-Mails und die Beglaubigung der Identität der Kommunikationsteilnehmer.

Wo gibt es gute Anleitungen im Netz?

- http://www.verbraucher-sicher-online.de/artikel/e-mail-verschluesselung
- http://de.wikipedia.org/wiki/E-Mail-Verschlüsselung
- https://emailselfdefense.fsf.org/de/
- http://wiki.kairaven.de/open/krypto/gpg/gpganleitung
- http://www.apfelwiki.de/Main/E-Mail-ZertifikateInMailVerwenden
- https://www.lrz.de/services/pki/einf/
- http://de.wikipedia.org/wiki/CAcert

Alle Links finden Sie auch unter:
www.anti-prism-party.de/downloads

Wie heißt die Lösung? Wo kann sie bezogen werden? Welche Alternativen gibt es?

- Es gibt zwei Standards zu Ende-zu-Ende-Verschlüsselung: OpenPGP und S/MIME. S/MIME ist oft eingebaut, OpenPGP muss meist nachgerüstet werden.
- Es gibt kommerzielle und kostenfreie Lösungen. Fragen Sie uns, welche Lösung für Sie in Frage kommt.
- Neben in den E-Mail-Client integrierte Lösungen kann man E-Mails über ein Gateway oder einen lokalen Proxy leiten.
- Mehrere Anbieter haben OpenPGP und/oder S/MIME in ihren Webmail-Dienst integriert und bieten auch passende Apps dazu an. Zum Teil ist dabei ein AddOn für den Browser nötig.
- Einige Anbieter versuchen, die unten genannten Schwächen zu umgehen. Diese Lösungen binden die Kommunikationspartner jedoch an den Anbieter.

Was sind die Grenzen der Lösung?

- Zum Verschlüsseln wird ein Schlüssel des *Empfängers* benötigt. Er muss zuerst Software installieren und Schlüssel zur Verfügung stellen.
- Jeder kann Schlüssel selbst erzeugen. Die Kommunikationspartner müssen daher die Identität aller anderen prüfen. Dieses „Web of Trust“ skaliert nicht, wenn Empfänger nicht persönlich bekannt sind.
- Die „Lösung“ bei S/MIME ist, dass alle einer „vertrauenswürdigen Stelle“ (CA) vertrauen. Die Prüfung ist aufwändig und kostet jährlich Geld. „Offizielle“ Zertifikate werden für E-Mail daher eher selten benutzt.
- CAcert verlagert die Hauptarbeit (Identitätsprüfung) auf Vereinsmitglieder und kann so kostenlose Zertifikate anbieten. Aber: der zugehörige Vertrauensanker fehlt leider (noch) in den meisten Anwendungen.
- E-Mail benötigt zum Transport Metainformationen. Diese werden auch bei verschlüsselten E-Mails unverschlüsselt gesendet. In einigen Bedrohungsszenarien scheidet daher die Nutzung von E-Mail generell aus.
- Wenn der Zugriff auf E-Mails per Webbrowser möglich sein soll oder die gesamte E-Mail-Infrastruktur von einem Cloud-Anbieter verwaltet wird, ist es z.T. nötig, dem Provider seine Schlüssel anzuvertrauen.

CAcert