Hardware-Box sorgt für mehr E-Mail-Sicherheit

Autor(en): **Honegger, Faby**

Objekttyp: **Article**

Zeitschrift: **Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association Suisse des Electriciens, de l'Association des Entreprises électriques suisses**

Band (Jahr): **93 (2002)**

Heft 17

PDF erstellt am: **30.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-855443

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

Hardware-Box sorgt für mehr E-Mail-Sicherheit

Eine Umstellung auf verschlüsselten E-Mail-Verkehr war für viele Firmen bisher zu kompliziert. Das könnte sich jetzt mit dem Secure-E-Mail-Server SEPP[1)] ändern, einem mit dem Innovationspreis «Technologiestandort Schweiz 2002» ausgezeichneten Produkt der Schweizer Security-Firma Onaras. Endlich können vertrauliche Informationen wie Finanzdaten, Verträge oder Offerten ohne Bedenken per E-Mail verschickt und empfangen werden. SEPP ist eine Hardware-Box im Firmennetzwerk, die den E-Mail-Verkehr automatisch verschlüsselt, ohne dass die Benutzer irgendetwas dafür tun müssen. SEPP stellt sicher, dass E-Mails wirklich nur vom Empfänger gelesen werden können und unverändert bei ihm ankommen. Zusätzlich werden alle E-Mails und Attachments automatisch auf Viren überprüft. Seine ausgeklügelte Rule Engine erlaubt eine problemlose Anpassung an die jeweilige Firmen-Sicherheitspolitik.

Pro Jahr werden 2,6 Billionen[2)] E-Mails verschickt, viele davon im Geschäftsverkehr mit vertraulichen Business-, Mitarbeiter- oder Kundeninformationen. Viele Firmen schützen ihre sensitiven Daten mit einer Firewall gegen

Faby Honegger

unbefugten Zugriff von aussen. Wie viele vertrauliche Informationen die Firma per E-Mail verlassen, ist ihnen nicht bewusst: Offerten, Finanzberichte, Geschäftsgeheimnisse, persönliche Mitarbeiterdaten, ja sogar geheime Passwörter werden per elektronische Post hin- und hergeschickt.

Die meisten E-Mail-Benutzer wissen nicht, dass eine E-Mail nicht sicherer ist als eine Postkarte auf dem normalen Postweg. Sie kann auf ihrem Weg, der oft um die halbe Welt führt, von jedermann gelesen, kopiert oder verändert werden, ohne dass Empfänger oder Sender etwas bemerken. Auch sind die E-Mail-Passwörter leicht zu knacken, so dass die Nachrichten ganz bequem vom Mail-Server abgeholt werden können, wiederum ohne dass irgendjemand etwas bemerkt.

Selbst wenn keine vertraulichen Informationen per elektronische Post verschickt werden, kann Schaden durch den E-Mail-Verkehr entstehen. Wie die Beispiele von «I love you», «Nimda» oder «Sircom» zeigen, werden in letzer Zeit Virusangriffe immer häufiger per E-Mail ausgeführt. Auch so genannte trojanische Pferde werden auf diesem Weg bequem an der Firewall vorbei geschleust.

Verschlüsselungsverfahren

Bei den eingesetzten Verschlüsselungsverfahren unterscheidet man zwischen der Private-Key- oder *symmetrischen* Verschlüsselung und der Public-Key- oder *asymmetrischen* Verschlüsselung. Bei der symmetrischen Verschlüsselung müssen beide Parteien den gleichen Schlüssel besitzen, den sie vorher über einen sicheren Kanal ausgetauscht haben (Bild 1). Das heisst, die Nachricht wird vom Sender mit dem gleichen Schlüssel verschlüsselt, mit dem sie der Empfänger wieder entschlüsselt. Eine einfache – und aus heutiger Sicht sehr unsichere – Variante der symmetrischen Verschlüsselung hat schon Julius Cäsar benutzt: Er hat einfach die Buchstaben des Alphabets verschoben und die Nachricht einem Boten übergeben. Der Empfänger hat das Alphabet dann wieder zurückverschoben; er musste jedoch wissen, um wie viel Buchstaben das Alphabet verschoben wurde, brauchte also denselben Schlüssel wie Cäsar.

Eine einfache, aber sehr sichere symmetrische Verschlüsselung ist der so genannte One-Time-Pad (Kasten). Er besteht aus einer einfachen XOR-Operation (Exklusiv-Oder-Operation) zwischen Nachricht und Schlüssel. Der Sender nimmt die Nachricht, wandelt sie in eine Bit-Folge um und führt ein einfaches XOR mit dem Schlüssel aus. Den so verschlüsselten Text kann er nun über einen unsicheren Kanal (z.B. das Internet) dem Empfänger schicken. Dieser führt mit dem verschlüsselten Text und dem gleichen Schlüssel wieder eine XOR-Operation durch und erhält als Resultat die ursprüngliche Nachricht (Bild 2).

Man kann beweisen, dass man ohne Kenntnis des Schlüssels die Nachricht nie aus dem verschlüsselten Text ableiten kann, wenn der Schlüssel gleich lang wie die Nachricht selbst ist und nur einmal benutzt wird. Der Schlüssel muss über

One-Time-Pad: Verschlüsselung mittels XOR

Beweis mittels boolscher Algebra

x = Nachricht
y = Schlüssel
z = verschlüsselter Text
r = Text nach der Entschlüsselung

Verschlüsselung (XOR):
(1) $z = x \cdot \bar{y} + \bar{x} \cdot y$
Entschlüsselung (XOR):
(2) $r = z \cdot \bar{y} + \bar{z} \cdot y$
Behauptung:
(3) $r = x$

Nach den Regeln der boolschen Algebra folgt aus (1):

(4) $\bar{z} = x \cdot y + \bar{x} \cdot \bar{y}$

(5) $r = (x \cdot \bar{y} + \bar{x} \cdot y) \cdot \bar{y} + (x \cdot y + \bar{x} \cdot \bar{y}) \cdot y$
$= x \cdot \bar{y} \cdot \bar{y} + \bar{x} \cdot y \cdot \bar{y} + x \cdot y \cdot y + \bar{x} \cdot \bar{y} \cdot y$
$= x \cdot \bar{y} + x \cdot y$
$= x \cdot (\bar{y} + y)$
$= x$

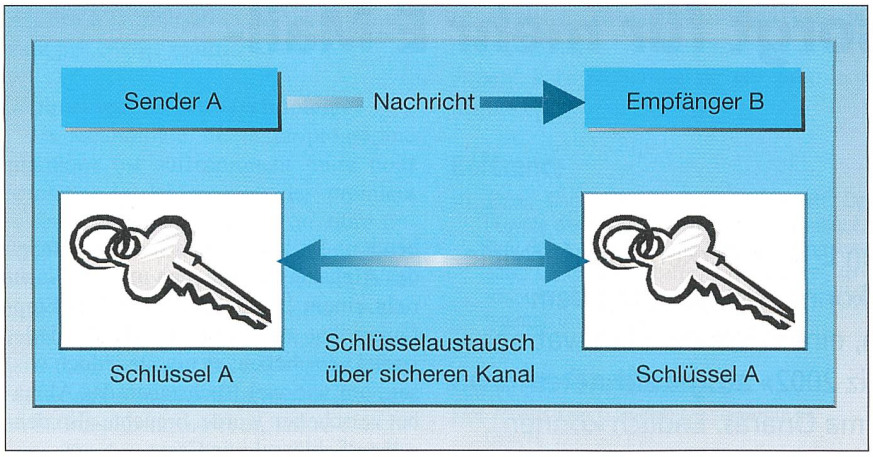

Bild 1 Schematische Darstellung eines symmetrischen Verschlüsselungsverfahrens

einen sicheren Kanal ausgetauscht werden, was das Problem allerdings nur verschiebt: Statt der Nachricht müsste nun dieser Schlüssel verschlüsselt übertragen werden. In der Praxis wird die symmetrische Verschlüsselung vor allem für die Sicherung von lokalen Daten (Harddisk-Verschlüsselung) angewendet, kommt aber auch bei der verschlüsselten Datenübertragung zum Einsatz, wobei der verwendete symmetrische Schlüssel dann durch Public-Key-Verfahren übertragen wird.

Mit der asymmetrischen Verschlüsselung (Public-Key-Verschlüsselung) lassen sich Schlüssel sicher übertragen. Dabei besitzt jeder Teilnehmer zwei Schlüssel. Den einen, den privaten (oder geheimen) Schlüssel, behält er für sich, den zweiten, den öffentlichen Schlüssel (Public Key), kann er öffentlich verteilen. Jeder beliebige Dritte kann mit diesem öffentlichen Schlüssel eine Nachricht verschlüsseln, doch nur der Besitzer des privaten Schlüssels kann die Nachricht wieder lesbar machen. Bildlich kann man sich den öffentlichen Schlüssel als Vorhängeschloss mit Schnappverschluss und den privaten Schlüssel als den zum Schloss passenden Schlüssel vorstellen (Bild 3).

Der Besitzer der beiden Schlüssel kann irgendjemandem, der ihm eine Nachricht verschlüsselt zuschicken will, seinen öffentlichen Schlüssel über einen unsicheren Kanal wie das Internet zusenden, da niemand mit diesem Schlüssel eine Nachricht entschlüsseln kann. Der Absender (A in Bild 3) verschlüsselt seine Nachricht mit dem öffentlichen Schlüssel (Vorhängeschloss), und nur der Empfänger (B in Bild 3) wird mit seinem entsprechenden privaten Schlüssel die ursprüngliche Nachricht aus der Sendung decodieren können.

Technologisch basiert die Public-Key-Verschlüsselung auf einer mathematisch schwierig zu berechnenden Problemstellung, wie zum Beispiel der Primfaktorzerlegung: Aus zwei sehr grossen Primzahlen kann man zwar ohne Probleme und rasch das Produkt berechnen; es ist aber – zumindest zurzeit – noch sehr schwierig, dieses Produkt wieder in die zwei Primzahlen zu faktorisieren. Diesen Umstand nutzt das wohl bekannteste Public-Key-Verfahren, das so genannte RSA-Verfahren[4)].

Es gibt heute mehrere Public-Key-Security-Verfahren (PKS), die sich bezüglich Algorithmus und Schlüssellänge voneinander unterscheiden. Um einen derartigen Code zu knacken, kann man natürlich alle möglichen Schlüssel durchprobieren. So hat ein Hacker vielleicht das (sehr grosse) Glück und er findet nach den ersten paar Versuchen den richtigen Schlüssel. Ansonsten muss er bei den heute üblichen 128-Bit-Schlüsseln 2^{128} Schlüssel durchprobieren. Nehmen wir an, es gibt Computer, die eine Milliarde Schlüssel pro Sekunde durchprobieren (noch weit von den heutigen Möglichkeiten entfernt) und ein Hacker hätte Zugriff auf 1 Milliarde dieser Computer, so würde es immer noch etwa 1000-mal das Alter des Universums in Anspruch nehmen, um alle Möglichkeiten zu prüfen.

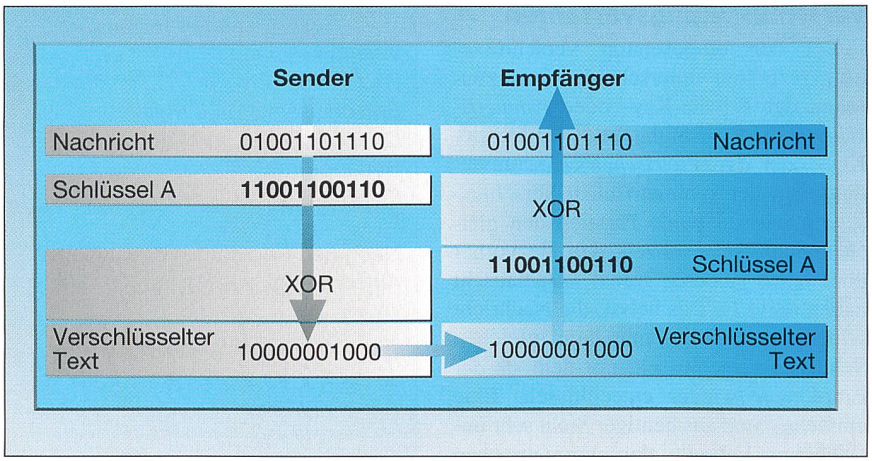

Bild 2 Ver- und Entschlüsselung mittels XOR-Operation

Bisherige Prävention

Einer der Gründe dafür, dass gegen diese grossen Sicherheitslöcher viel zu wenig unternommen wird, ist, dass sich die Verfasser der E-Mail-Nachricht des Risikos meist nicht bewusst sind. Das Schreiben einer E-Mail ist eine persönliche Angelegenheit, die der Absender auf seinem eigenen Computer ausführt, wo er sich sicher fühlt. Des Weiteren werden Vorfälle von unberechtigtem Zugriff auf E-Mails, sofern sie überhaupt bemerkt werden, von den betroffenen Unternehmungen aus Furcht vor negativer Publicity schnell unter den Teppich gekehrt. Es kann somit angenommen werden, dass nur ein verschwindend kleiner Teil aller E-Mail-Hacking-Vorfälle je an die Öffentlichkeit gelangt.

Der Hauptgrund für die ungenügende Prävention dürfte jedoch sein, dass Sicherheits-Softwarelösungen und Sicherheits-Plugins viel zu kompliziert zu bedienen sind und einen grossen Installations- und Schulungsaufwand verlangen, was viele IT-Verantwortliche bisher vor durchgreifenden Massnahmen abgeschreckt hat.

Secure-E-Mail-Server SEPP

Die auf Internet-Security spezialisierte Firma Onaras bringt nun ein interessantes System zur Lösung des geschilderten Problems auf den Markt: den Secure-E-Mail-Server SEPP. SEPP ist eine Hardware-Box im Firmennetzwerk, die den E-Mail-Verkehr automatisch, das heisst

ohne jegliches Zutun der Benutzer, verschlüsselt. Er stellt sicher, dass E-Mails an Filialen, Kunden, Lieferanten und andere nur vom Empfänger gelesen werden können und unverändert bei ihm ankommen. Zusätzlich werden alle E-Mails und Attachments automatisch auf Viren und ausführbare Dateien überprüft.

Die Benutzer von SEPP verschicken dabei ihre E-Mails wie gewohnt mit ihrem E-Mail-Programm (Outlook, Netscape usw.). SEPP ver- und entschlüsselt für die ganze Firma die aus- und eingehenden E-Mails und deren Attachments automatisch im Hintergrund. Der Kommunikationspartner benötigt zum Lesen selber keinen SEPP und auch kein spezielles Produkt von Onaras. Er kann eine normale Verschlüsselungs-Software einsetzen oder z.B. Outlook-Plugins benutzen, da SEPP äusserst sichere und weltweit verbreitete Public-Key-Verschlüsselungs-Standards (PGP, SSL, S/MIME) [3] verwendet, die alle eine Schlüssellänge von mindestens 128 Bit verwenden.

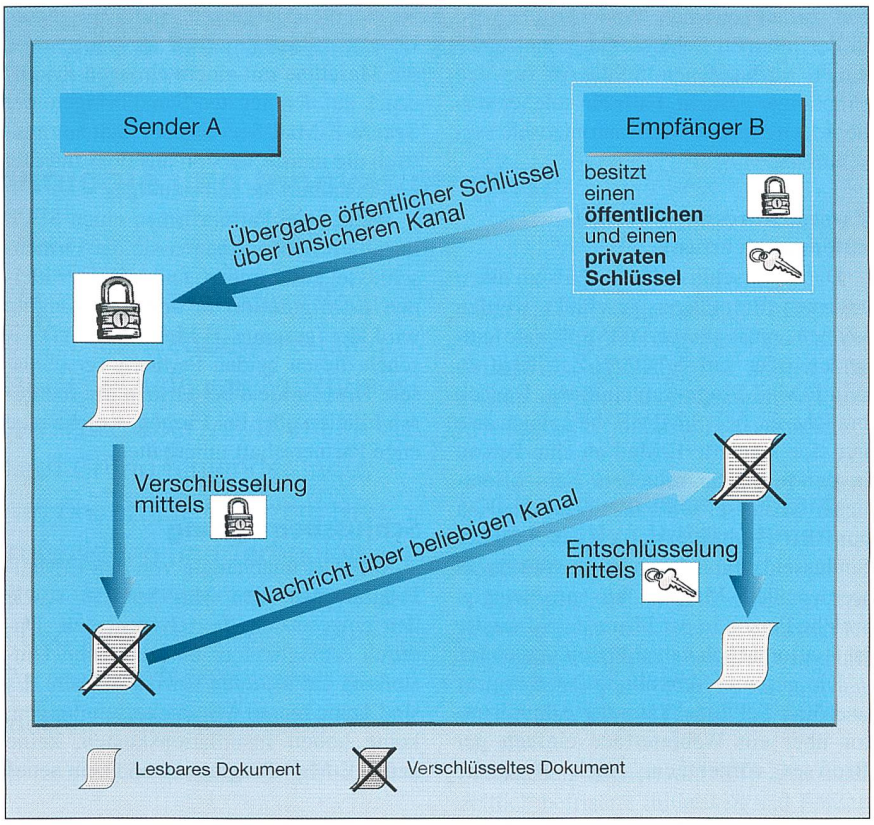

Bild 3 Schematische Darstellung einer asymmetrischen Verschlüsselung

Aufbau

SEPP ist ein Appliance Server, das heisst, ein Produkt, das aus Hard- und Software besteht. Ein Vorteil liegt darin, dass man das Gerät einfach ins Firmennetzwerk stellen kann, ohne auf den bestehenden Servern Software oder Plugins zu installieren. Damit ist SEPP auch unabhängig von eingesetzten Betriebssystemen, Mail-Servern und anderen Software-Komponenten. Man muss keine neue Version kaufen, wenn man auf eine neue Netzwerkumgebung wechselt oder das Betriebssystem updated.

Der Hauptvorteil aber liegt darin, dass Onaras sicherstellen kann, dass von der Hardware über das Betriebssystem bis zur Service-Software alles reibungslos zusammenpasst und auf Sicherheit optimiert ist. Mit OpenBSD[5] benutzt SEPP ein Betriebssystem, das im Hinblick auf Sicherheitsanwendungen entwickelt worden ist. OpenBSD ist ein Berkley Unix Derivat mit kryptologischen und Firewall-Funktionalitäten.

Der Secure-E-Mail-Server SEPP benutzt zwei Betriebsmodi. Je nach Bedarf lässt er sich im Intranet oder in der De-Militarized Zone (DMZ) betreiben. Der DMZ-Betriebsmodus ist eher für grössere Firmen gedacht, bei denen das interne Netzwerk schon durch entsprechende Sicherheitsmechanismen abgesichert ist. Der Intranet-Betriebsmodus ist für kleinere Firmen ohne eigenen Mailserver oder für Firmen mit sehr hohem Sicherheitsbedürfnis geeignet. Dieser Modus erlaubt Verschlüsselung bis an den einzelnen Arbeitsplatz, zudem sind die E-Mails auch verschlüsselt auf dem Mailserver abgelegt.

Funktionsweise

Um die Funktionsweise des Secure-E-Mail-Servers SEPP zu erläutern, verfolgt man am besten eine E-Mail auf ihrem Weg durch die Maschine. SEPP besitzt einen Listener, der auf Port 25 hört und die E-Mails in Empfang nimmt. Zuerst wird geprüft, ob es sich um eine eingehende oder eine ausgehende E-Mail handelt. Dann wird die E-Mail in ihre Einzelteile (also Header, Body und Attachment) zerlegt, die anschliessend das eigentliche Herzstück des Secure-E-Mail-Servers SEPP durchlaufen: die Rule Engine.

Die eingebaute Rule Engine erlaubt, das Verhalten von SEPP an die individuellen Bedürfnisse der Unternehmung anzupassen. Sie besteht aus einem Regelbaum mit vielen Regeln, die der Reihe nach durchlaufen werden. Eine Regel ist dabei eine Aktion, die ausgeführt wird, wenn gewisse Bedingungen zutreffen. Als Bedingungen kann man den Absender prüfen, den Empfänger, den Inhalt der E-Mail, ob sie verschlüsselt oder signiert ist, einen Virus enthält usw. Auf Grund dieser Überprüfung kann die E-Mail gesendet, gelöscht, zurückgewiesen, verbzw. entschlüsselt oder mit einem Disclaimer versehen werden. Zudem kann beispielsweise der Postmaster informiert oder andere Aktionen ausgelöst werden.

Die Regeln können so gestaltet werden, dass sie die firmeneigene Security Policy genau abbilden.

E-Mail-Check am Beispiel des Standard Rule Set

Ablauf bei eingehender E-Mail

Beim Standard Rule Set wird bei einer eingehenden E-Mail zuerst geprüft, ob sie mit PGP oder S/MIME verschlüsselt ist; falls dies zutrifft, wird sie entschlüsselt. Anschliessend wird geprüft, ob sie signiert ist, und die Signatur gegebenenfalls überprüft. Zuletzt wird die E-Mail nach Viren durchsucht und – falls irgendwelche Besonderheiten aufgetreten sind – ein Report mit allen notwendigen Informationen an die E-Mail angehängt. Bei vorhandenen Viren wird zusätzlich auch der Administrator benachrichtigt. Die E-Mail wird wieder zusammengesetzt und an den internen Empfänger weitergeleitet.

Ablauf bei ausgehender E-Mail

In diesem Fall wird die E-Mail im Standard Rule Set zuerst nach Viren überprüft. Sind solche vorhanden, wird sie so-

fort zurückgewiesen. Anderenfalls wird in der internen Schlüsseldatenbank nach einem vorhandenen Schlüssel für den Empfänger gesucht. Falls ein solcher vorliegt, wird die E-Mail automatisch verschlüsselt.

Externe Adressaten werden automatisch erfasst

Damit verschlüsselte E-Mails an einen externen Empfänger geschickt werden können, muss dieser PGP-Software einsetzen oder ein S/MIME-Zertifikat in sein E-Mail-Programm einfügen. Danach braucht er bei S/MIME beispielsweise nur eine signierte E-Mail an eine Person in der Firma zu schicken. Sein öffentlicher Schlüssel wird dabei automatisch aus der E-Mail extrahiert und in die Schlüsseldatenbank integriert. Von da an werden alle E-Mails an ihn – unabhängig, welche Person in der Firma der Absender ist – automatisch verschlüsselt versendet.

Die gesamte Verwaltung der Benutzer und ihrer Schlüssel kann der Administrator über ein Webinterface einfach per Browser vornehmen. Auch sämtliche Netzwerkeinstellungen sind über dieses Interface konfigurierbar. Er kann sogar die Maschine mit einem einzigen Knopfdruck auf den neusten Stand bringen: der Secure-E-Mail-Server SEPP lädt automatisch die neuste Version aus dem Internet und installiert sie selbständig[6].

Wenn zwei Partnerfirmen einen SEPP installiert haben, können sie die Firmenschlüssel austauschen, und mit einer kleinen Konfiguration in der Rule Engine wird der gesamte E-Mail-Verkehr zwischen diesen beiden Partnern verschlüsselt. Dies ist ideal bei Firmen mit mehreren Filialen oder bei Firmen, welche eine enge Partnerschaft unterhalten.

Schlussbemerkung

SEPP ist unabhängig von den E-Mail-Programmen, den Mail-Servern sowie den eingesetzten Betriebssystemen. Dadurch ermöglicht er eine einfache Umstellung auf sicheren E-Mail-Verkehr. Es sind keine teuren Mitarbeiterschulungen, keine hohen Installationskosten, keine neuen E-Mail-Programme und kein neues Firmennetzwerk nötig, da sich SEPP nahtlos in bestehende Netzwerkinfrastrukturen einfügt.

Nach Wissen des Autors ist SEPP zurzeit der einzige erhältliche Hardware-basierte E-Mail-Verschlüsselungs-Server. Da er von der Hardware über das Betriebssystem bis hin zur Software auf Sicherheit und Zuverlässigkeit optimiert ist und zudem Mechanismen wie automatisches Virenscanning besitzt, bietet er höchstmögliche Sicherheit für sensible Daten.

Hardware-box pour plus de sécurité e-mail

Jusqu'à présent, beaucoup de sociétés considéraient le cryptage du trafic e-mail comme trop compliqué. Cela pourrait changer avec le Secure-E-Mail-Server SEPP (Secure E-Mail PGP Proxy), un produit de la société suisse de systèmes de sécurité Onaras, qui a reçu le prix de l'innovation «Site technologique Suisse 2002». Les informations confidentielles comme les données financières, contrats ou offres, peuvent désormais être expédiées et reçues par e-mail sans inquiétude. Le SEPP est un Hardware-box installé dans le réseau de la société et qui codifie le trafic e-mail automatiquement, sans que les utilisateurs doivent faire quoi que ce soit. Le SEPP fait en sorte que les e-mails ne puissent vraiment être lus que par le destinataire et lui parviennent sans modification. En outre, tous les e-mails et annexes sont passés automatiquement au test antivirus. Le Rule Engine perfectionné permet une adaptation sans problème à la politique de sécurité de la société.

Literatur

Guter Kryptographie Überblick: Spektrum der Wissenschaft. Dossier 4/2001, «Kryptographie», www.spektrum.com

W. Diffie, M. Hellmann: New Directions in Cryptography. IEEE Transactions on Information Theory, Bd. IT-22, Heft 6, November 1976 (Erste Veröffentlichung von Public-Key-Verfahren)

Links

Integrierter Virusscanner: www.sophos.de
Glossar: www.ciphersbyritter.com/glossary.htm
Krypto-Gruppe der ETH: www.crypto.ethz.ch
RSA-Verfahren:
http://world.std.com/~franl/crypto/rsa-guts.html;
www.rsasecurity.com

Adresse des Autors

Faby Honegger, Onaras AG, 5408 Ennetbaden
honegger@onaras.ch

[1] SEPP: Secure E-Mail PGP Proxy (die aktuelle Version versteht zudem auch S/MIME. PGP steht dabei für Pretty Good Privacy)
[2] Gemäss International Data Corp. wird die Zahl der versendeten E-Mails weltweit von 2,6 Billionen im Jahr 2000 auf 9,2 Billionen im Jahr 2005 steigen (www.boss-it.com/scripts/full_new.asp?story-id=46, Sept. 2001).
[3] PGP: Pretty Good Privacy, www.pgpi.com; SSL: Secure Sockets Layer; S/MIME: Secure/Multipurpose Internet Mail Extensions
[4] RSA-Verfahren: Nach seinen Erfindern Rivest, Shamir und Adleman benanntes Verfahren
[5] www.openbsd.org
[6] Von der Homepage onaras.ch holt sich der Rechner einen Link zu einem bestimmten Server, von welchem er dann die neusten Packages und Scripts lädt und selbständig installiert.