Zeitschrift: LANline Heft: 014 Jahrgang: 2001 Seite: 76

Sichere E-Mail erfordert kompetente Nutzer

For your eyes only

E-Mail ist heute einer der wichtigsten Kommunikationsdienste in Wirtschaft, Verwaltung und im privaten Bereich. Verstärkt werden auch sensible Daten über diesen elektronischen Dienst verteilt. Der Schutz solcher Informationen vor unbefugtem Zugriff sowie der Schutz vor Verbreitung von "Malicious Code" ist allerdings noch nicht in der gleichen Weise entwickelt wie die Nutzung zugenommen hat, obwohl die nötige Technik durchaus zur Verfügung steht. Hier können zielgruppenspezifische Schulungsmaßnahmen Wissen vermitteln und vor allem Bewusstsein schaffen. Seminare sind damit ein wichtiger Bestandteil eines E-Mail-Sicherheitskonzepts.

Mit der öffentlichen Verfügbarkeit des Internets hat sich die Kommunikationskultur in Unternehmen und Behörden weltweit revolutioniert. Informationen, die noch vor zehn Jahren ausschließlich per Post, Telefon oder Fax transportiert wurden, werden heute zum großen Teil per E-Mail versandt. Neben der Beschleunigung des Informationsflusses haben sich auch Qualität und Quantität der Information grundlegend verändert. Das Dokument hat sich vom klassischen Brief in Textform zu einem multimedialen Datenpaket entwickelt, das den Empfänger mit riesigen Datenmengen, Videos, Bildern und Musik versorgen kann.

Der Übertragungsweg einer E-Mail besitzt im Vergleich zu den "alten" Kommunikationswegen einige neue Eigenschaften. So wurde der lineare Informationsfluss von Sender zum Empfänger über definierte und gesicherte Wege gegen ein vom Sender nicht steuerbares Hin und Her der Daten durch die verzweigten Bahnen des Internets eingetauscht. Auf diesem Weg können Informationen verändert, repliziert, umgeleitet und abgefangen werden. Diese erhebliche Unsicherheit des Informationsflusses ist allerdings noch nicht mit der gleichen Intensität in das Bewusstsein der Anwender gedrungen, wie die vielen Vorteile, welche die neue Technik bietet. Noch immer werden von Unternehmen und Privatpersonen massenhaft sensible Daten ungeschützt per E-Mail verschickt.

Was für das Internet gilt, gilt ebenso für das Intranet, das interne Firmennetz. Verschiedenen Untersuchungen zufolge kommen mehr als die Hälfte aller Angriffe aus der Reihe der eigenen Mitarbeiter. Ein schlagendes Argument, die Information auch in den "eigenen vier Wänden" vor unberechtigtem Zugriff zuverlässig zu schützen.

Auch die Entwicklung von Computer-viren hat in den letzten Jahren von der zunehmenden Nutzung von E-Mail profitiert. Wegen der zahlreichen Spielarten von Viren und virenähnlichen Programmen wurde der Begriff "Malicious Code" geprägt. Er umfasst alle Programme, die mit der Fähigkeit ausgestattet sind, Systeme in irgendeiner Weise zu manipulieren, zu beeinträchtigen oder zu schädigen. Die Hauptausbreitung über Diskette wurde abgelöst von der E-Mail-Kommunikation und hat ebenfalls eine neue Qualität erlangt wie es der "I-Love-You-Worm" im Jahr 2000, beziehungsweise sein etwas harmloserer Nachfolger Anfang 2001 eindrücklicher nicht hätten demonstrieren können. Bei der Diskussion des Themas E-Mail-Sicherheit darf der Aspekt des Virenschutzes deshalb nicht fehlen.

Technik der E-Mail-Sicherheit

Das Gefährdungspotenzial im Informationsaustausch via E-Mail wurde schon früh erkannt. Als effizientes Sicherheitsszenario wurde das Konzept der "Ende-zu-Ende-Sicherheit" entwickelt und in zahlreichen Produkten umgesetzt. Das bedeutet, dass die digitale Nachricht, bevor sie den PC des Autors verlässt, kryptografisch verschlüsselt wird und auch digital signiert werden kann. So verpackt und unterschrieben gehen die Daten auf die Reise. Erst im PC des Empfängers werden sie wieder entschlüsselt und damit lesbar. Durch dieses Vorgehen sind wichtige Sicherheitsziele erreicht:

a) Vertraulichkeit: Die Nachricht wird durch die Verschlüsselung mit starken kryptografischen Verfahren für alle Personen außer dem Adressaten unlesbar.

b) Authentizität: Die digitale Signatur bestätigt die Identität des Absenders.

c) Integrität: Über die digitale Signatur kann sichergestellt werden, dass die Information während des Transports nicht unbemerkt verändert werden kann.

Es existieren unterschiedliche Verfahren, deren kombinierter Einsatz eine sichere und schnelle Verschlüsselung und Signatur beziehungsweise Entschlüsselung und Verifikation erlauben. Sie hier alle zu erläutern, würde den Rahmen dieses Artikels sprengen. Daher an dieser Stelle eine kurze Skizze der Funktionsweise.

Jeder Anwender benötigt einen privaten Schlüssel, den nur er kennt und den er vor unerlaubtem Zugriff sichern muss sowie einen öffentlichen Schlüssel, den er seinen Kommunikationspartnern zur Verfügung stellt. Er selbst besitzt von allen seinen Kommunikationspartnern den individuellen öffentlichen Schlüssel. Mathematische Algorithmen wandeln die Daten mit Hilfe des öffentlichen Schlüssels des Empfängers in einen unverständlichen Zeichenhaufen um. Nur der Besitzer des passenden privaten Schlüssels ist in der Lage, die ursprünglichen Daten wiederherzustellen.

Bild 2 zeigt, wie die sichere E-Mail-Kommunikation konkret abläuft: Die Senderin Alice möchte an den Empfänger Bob eine Nachricht senden. Alice ist der öffentliche Schlüssel von Bob bekannt. Alice verschlüsselt die Nachricht mit Hilfe des öffentlichen Schlüssels von Bob und verschickt sie über das Internet. Bob kann die Nachricht mit Hilfe seines privaten Schlüssels wieder entschlüsseln. Zusätzlich kann Alice die Nachricht auch digital signieren, sodass sie eindeutig als Absenderin ausgewiesen wird. Dies tut sie mit ihrem privaten Schlüssel. Die digitale Signatur kann von Bob mit dem öffentlichen Schlüssel von Alice verifiziert werden. Bob ist damit außerdem sicher, dass die Nachricht nicht manipuliert wurde.

Es wird deutlich, dass der Schutz der E-Mail die Mitwirkung des Benutzers erfordert. Auch bei einer sehr anwenderfreundlichen Software ist ein Grundverständnis der Funktionsweise notwendig.

Technik des Virenschutzes

Bei der Umsetzung der Ende-zu-Ende-Sicherheit in Unternehmen ist zu beachten, dass eine zentrale Überprüfung von verschlüsselten E-Mails auf Malicous Code nicht möglich ist. Genau wie die eigentliche Nachricht wird auch der "Schädling" verschlüsselt und kann von Virenscannern nicht geprüft werden. Der allgemein übliche Viren-Check an der Firewall ist damit wirkungslos. Deswegen ist es unumgänglich, Virenschutzprogramme auf den PCs zu installieren und regelmäßig zu aktualisieren. Hier sind komfortable Programme auf dem Markt, die es erlauben, den Virenschutz zentral zu installieren, ohne den Endanwender mit irgendwelchen Aufgaben zu behelligen.

Doch auch bei aktuellstem Stand bleibt selbst der beste Virenschutz immer einen Schritt hinter dem Angreifer zurück. Erst wenn ein Virus entdeckt wurde, kann ein wirkungsvolles Schutzprogramm geschrieben werden. Deswegen ist die Sensibilität des Nutzers ein wichtiges und entscheidendes Element des Virenschutzes. Er muss entscheiden können, wann eine E-Mail mit Vorsicht zu genießen und welches Attachment lieber nicht zu öffnen ist. Hier können Schulungen helfen, zum anderen ist aber auch das Design der Sicherheitsprodukte entscheidend. Wenn Verschlüsselung und digitale Signatur mit zeitraubenden und komplexen Abläufen verbunden sind, ist die Gefahr groß, dass viele Nutzer die Lust verlieren und die Sicherheitstechnik einfach nicht anwenden. Im Normalfall sollten mit einem Maus-klick und der Eingabe des Passworts Verschlüsselung und Signatur erfolgreich durchgeführt werden können. In Ausnahmesituationen, die nicht automatisiert abgearbeitet werden können, muss dem Nutzer eine eindeutige Definition des Handlungsablaufs vorliegen.

Bewusstsein und Know-how

Für einen erfolgreichen Schutz von E-Mails müssen neben der Installation der Technik drei Voraussetzungen erfüllt sein:

a) Die Anwender sind für die Problematik sensibilisiert und sehen E-Mail-Sicherheit als Notwendigkeit an.

b) Sie sind motiviert, die Sicherheitstechnik einzusetzen.

c) Sie verfügen über das notwendige Wissen, dies zuverlässig zu tun. Dazu gehören vor allem Sicherheitsregeln und eindeutig definierte Handlungsabläufe.

Um diese Voraussetzungen zu erfül-len, sind Schulungen ein unverzichtbares Instrument. Der Schulungsbedarf beschränkt sich allerdings nicht allein auf die Anwender. Wie bereits im vorhergehenden Beitrag dieses Heftes erläutert, brauchen Systemverwalter, die Sicherheitskonzepte mitgestalten und die für die Erweiterung der Systeme um die Sicherheitsfunktionen verantwortlich sind, übergreifendes Wissen und detaillierte Produktkenntnis, um das Zusammenspiel der Systeme steuern zu können. Unternehmensinterne Multiplikatoren, seien es Ausbilder oder "Super-User", müssen mit der Sicherheitstechnologie vertraut sein, um Kollegen und Mitarbeiter effizient schulen zu können. Schließlich gilt es auch, den für die Einführung von Sicherheitsmechanismen in Unternehmen Verantwortlichen Sensibilität und technisches Grundverständnis zu vermitteln.

Der richtige Anbieter für den richtigen Zweck

Bei der Auswahl der Schulungsmaßnahmen müssen bereits im Vorfeld Inhalte und Zielgruppen genau definiert werden. Grundsätzlich sind drei Arten von Schulungsanbietern denkbar:

1. Hersteller der Sicherheitsprodukte

Vom Hersteller kann man erwarten, dass er seine Produkte gut kennt und entsprechende Schulungsangebote vorhält. Ein Herstellerseminar erscheint sinnvoll, um Systemverwalter, Multiplikatoren und Endanwender zielgruppenspezifisch mit dem Produkt vertraut zu machen. Es sollte darauf geachtet werden, dass der Sensibilisierung und Motivation der Mitarbeiter für E-Mail-Sicherheit in den Konzepten des Schulungsanbieters angemessen Platz eingeräumt wurde.

2. "Hausinterne" Multiplikatoren

Oft entstehen Sicherheitslösungen aus individuellen Konzepten, die den Anforderungen des jeweiligen Unternehmens gerecht werden. Hier kann es Sinn machen, intern die Ausbildung der Endanwender zu übernehmen. Die Einführung in das Produkt sollte sich auf die wesentlichen technischen Vorgänge beschränken. Der Schwerpunkt sollte auch hier in der Sensibilisierung und Motivation der Anwender liegen.

3. Herstellerunabhängige Schulungsunternehmen

In der konzeptionellen Phase bieten herstellerunabhängige Schulungen den Vorteil, die Fragestellung produktneutral behandeln zu können. Um zu einer tragfähigen individuellen Lösung zu kommen, ist es wesentlich, alle technischen und organisatorischen Aspekte der E-Mail-Sicherheit aufzufächern. Daraus lässt sich ein Anforderungsprofil generieren, an dem sich die vorhandenen Produkte messen lassen müssen. Diese Schulungen richten sich in erster Linie an Entscheider, Projektleiter und Systemverwalter.

Das Beratungsunternehmen Secorvo Security Consulting beispielsweise hat mit Secorvo College eine Institution geschaffen, die mit ihren Seminaren wichtige Grundlagen für ein solides Sicherheitskonzept legt. Die Teilnehmer profitieren von der Nähe zum Beratungsgeschäft. Secorvo berät ausschließlich in IT-Sicherheitsfragen. Die Schulungen werden von den eigenen Consultants durchgeführt. Pro Tag agieren durchschnittlich vier verschiedene Referenten. So fließen die vielfältigen Erfahrungen von Secorvo ein und machen das Seminar abwechslungsreich.

Zum Thema E-Mail-Sicherheit werden zwei Seminare angeboten. Ein eintägiges Seminar vermittelt einen Überblick; das zweitägige Seminar "E-Mail-Sicherheit - Grundlagen, Konzepte, Lösungen" erlaubt den Teilnehmern, einzelne Gebiete zu vertiefen. Ergänzend kann das Grundlagenseminar "IT-Sicherheit heute" besucht werden. Es gibt denjenigen, die sich neu in das Thema IT-Sicherheit einarbeiten, einen umfassenden Einblick in die Grundlagen. Bei Sicherheitsfragen spielt auch in der Informationstechnik der Mensch immer eine zentrale Rolle, da sein Verhalten entscheidend für den Erfolg der Sicherheitsmaßnahmen ist. Somit sollten Schulungen immer ein fester Bestandteil eines erfolgreichen E-Mail-Sicherheitskonzepts sein.

(Christoph Weinmann/sm)

Christoph Weinmann ist bei Secorvo Security Consulting in Karlsruhe verantwortlich für den Seminar- und Schulungsbereich "Secorvo College".

Weitere Informationen

Zu Verfahren, deren kombinierter Einsatz eine sichere und schnelle Verschlüsselung und Signatur beziehungsweise Entschlüsselung und Verifikation erlauben, sei auf ein Secorvo White Paper vom 23. Juni 2000 verwiesen: Fox, Dirk: "E-Mail-Sicherheitslösungen", abzurufen unter www.secorvo.de

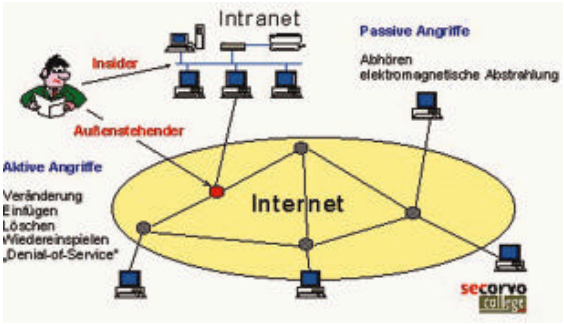

Bild 1. Angriffe auf vertrauliche E-Mail-Nachrichten können sowohl aus dem öffentlichen Internet als auch dem firmeninternen Intranet kommen

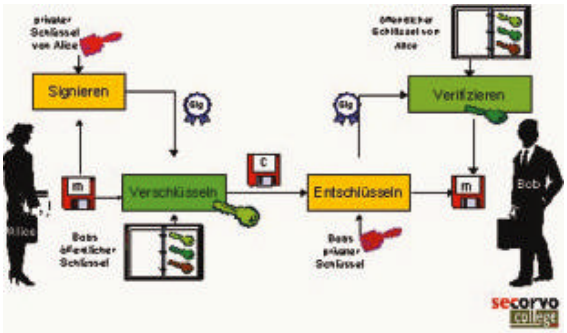

Bild 2. Ablauf einer sicheren E-Mail-Kommunikation

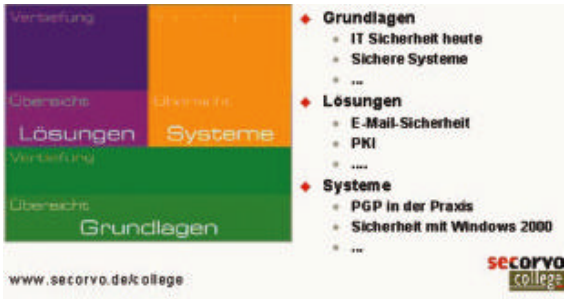

Bild 3. Aufbau des Secorvo-College-Seminarangebots zum Thema IT- und E-Mail-Sicherheit

voriger Artikel nächster Artikel Trefferliste neue Suche