Konzeption der sicheren E-Mail-Nutzung

HERBERT FIDESSER

Geschäftsführender Obmann der pSIT rea.GenmbH. die sich mit Schulungen und Beratungen im Bereich der IT-Sicherheit beschäftigt.
fidesser@psit.at

Bevor E-Mailsysteme für die Nutzung freigeben werden, sollte festgelegt werden, für welchen Einsatzzweck und welche Informationen E-Mail vorgesehen ist. Abhängig davon, wofür E-Mail eingesetzt werden soll, unterscheiden sich auch die Ansprüche an Vertraulichkeit, Verfügbarkeit, Integrität und Verbindlichkeit der zu übertragenden Daten sowie des eingesetzten E-Mail-Programms. Es muss geklärt werden, ob über E-Mail **ausschließlich unverbindliche oder informelle Informationen** weitergegeben werden sollen oder ob einige oder sogar alle der bisher schriftlich bearbeiteten **Geschäftsvorfälle** nun per E-Mail durchgeführt werden sollen. Bei letzterem ist zu klären, wie Anmerkungen an Vorgängen wie Verfügungen, Abzeichnungen oder Schlusszeichnungen, die bisher handschriftlich angebracht wurden, elektronisch abgebildet werden sollen.

▶ Digitale Signatur und Verschlüsselung

Bei der Konzeption der E-Mail-Nutzung muss auch festgelegt werden, ob und wie kryptografische Sicherungsmechanismen zu implementieren sind (digitale Signatur, Verschlüsselung).
Ein Unternehmen muss darauf aufbauend eine E-Mail-Richtlinie festlegen, die folgende Punkte enthält:

- wer erhält einen E-Mail-Anschluss,
- die Regelungen, die von den E-Mail-Administratoren und den E-Mail-Benutzern zu beachten sind,
- bis zu welchem Anspruch an Vertraulichkeit oder Integrität dürfen Informationen per E-Mail versandt werden,
- welche Handbücher beschafft werden,
- wie die Benutzer geschult werden und
- wie jederzeit technische Hilfestellung für die Benutzer gewährleistet wird.

▶ Sicherheit des Datentransfers

Durch organisatorische Regelungen oder durch die technische Umsetzung sind dabei insbesondere die folgenden Punkte zum ordnungsgemäßen Dateitransfer zu gewährleisten:

- Die E-Mail-Programme der Benutzer müssen durch den Administrator so vorkonfiguriert sein, dass ohne weiteres Zutun der Benutzer maximale Sicherheit erreicht wird.

- Die Übermittlung von Daten darf erst nach erfolgreicher Identifizierung und Authentisierung des Senders beim Übertragungssystem möglich sein.

- Die Benutzer müssen vor erstmaliger Nutzung von E-Mail in die Handhabung der relevanten Applikationen eingewiesen werden. Die organisationsinternen Benutzerregelungen zur Dateiübermittlung muss ihnen bekannt sein.

- Zur Beschreibung des Absenders werden bei E-Mails so oft genannte Signatures (Absenderangaben) an das Ende der E-Mail angefügt[1]. Der Inhalt einer Signature sollte dem eines Briefkopfs ähneln, also Name, Organisationsbezeichnung und Telefonnummer und Ähnliches enthalten. Diese Signature darf jedoch weder mit einer Signatur im Sinne einer (eingescannten) Unterschrift noch mit einer elektronischen Signatur, die die Korrektheit und Authentizität des Textinhaltes belegt, verwechselt werden. Eine Signature sollte nicht zu umfangreich sein. Die Behörde bzw. das Unternehmen sollte einen Standard für die einheitliche Gestaltung von Signatures festlegen.

- Von den eingesetzten Sicherheitsmechanismen hängt es ab, bis zu welchem Vertraulichkeits- bzw. Integritätsanspruch Dateien per E-Mail versandt werden dürfen. Es sollte geregelt werden, ob und wann übertragene Dateien verschlüsselt bzw. digital signiert werden. Es ist zentral festzulegen, welche Applikationen für die Verschlüsselung bzw. den Einsatz von digitalen Signaturen von den Benutzern zu verwenden sind. Diese müssen den Benutzern zur Verfügung gestellt werden, die wiederum in deren Anwendung unterwiesen werden müssen.

- Es sollte vor der Einführung elektronischer Kommunikationssysteme festgelegt werden, unter welchen Bedingungen ein- oder ausgehende E-Mails zusätzlich ausgedruckt werden müssen.

- Die Dateiübertragung kann (optional) dokumentiert werden. Für jede stattgefundene Übermittlung ist dann in einem Protokoll festzuhalten, wer wann welche Informationen erhalten hat. Bei der Übertragung personenbezogener Daten sind die gesetzlichen Vorgaben zur Protokollierung zu beachten.

▶ Interne E-Mails

E-Mails, die intern versandt werden, dürfen das interne Netz nicht verlassen. Dies ist durch entsprechende administrative Maßnahmen sicherzustellen. Beispielsweise sollte die Übertragung von E-Mails zwischen verschiedenen Liegenschaften einer Organisation über eigene Standleitungen und nicht über das Internet erfolgen.
Grundsätzlich sollten Nachrichten, die an interne Adressen verschickt wurden, nicht an externe Adressen weitergeleitet werden. Sollen hiervon Ausnahmen gemacht werden, sind alle Mitarbeiter darüber zu informieren. Beispielsweise kann für Außendienstmitarbeiter oder andere Mitarbeiter, die viel unterwegs sind, die E-Mail an externe Zugriffspunkte weitergeleitet werden.

▶ Private E-Mail-Nutzung

Es wird immer wieder diskutiert, ob und in wieweit dienstliche E-Mail-Zugänge für private Zwecke benutzt werden dürfen. Solange die private Nutzung sich in Grenzen hält, wird dies sogar von vielen Organisationen unterstützt, da die Mitarbeiter dadurch eine positivere Einstellung zu E-Mail bekommen. Generell empfiehlt es sich aber, hierzu in der E-Mail-Richtlinie zu vereinbaren, welche Spielregeln bei der E-Mail-Nutzung allgemein und auch hinsichtlich privater Nutzung einzuhalten sind.
Bei der Nutzung von E-Mail in Institutionen sollte auch festgelegt werden, welche E-Mail-Programme eingesetzt werden sollen. Neben unterschiedlicher Funktionalität hat die Auswahl der E-Mail-Clients und -Server auch Einfluss auf die Benutzungsfreundlichkeit und den Administrationsaufwand, aber auch auf die Sicherheit der gesamten IT-Umgebung. Neben eigenständigen Client-Programmen kann auch auf Webmail zurückgegriffen werden.

▶ Webmail

Als Webmail werden Angebote bezeichnet, bei denen über einen Browser auf webbasierte E-Mail-Dienste zugegriffen wird. Verschiedene Anbieter von Mailservern bieten entsprechende Erweiterungen entweder direkt in ihr Produkt integriert oder als Zusatzmodule an. Webmail hat den Vorteil, dass hierbei von jedem Rechner mit Internet-Anschluss weltweit auf die E-Mail-Postfächer zugegriffen werden kann, ohne dass hierfür in aufwendige Infrastruktur investiert werden muss. Es ist allerdings schwieriger als beim Transport über die internen E-Mail-Server, die organisationsweit gültigen Sicherheitsrichtlinien durchzusetzen, beispielsweise im Hinblick auf Virenschutz oder Verschlüsselung. Außerdem ist die Gefahr, dass vertrauliche E-Mails mitgelesen oder Passwörter abgehört werden, beim externen Zugriff auf Webmailzugänge wesentlich höher.
Bei der Nutzung von Webmail aus einem Behörden- bzw. Unternehmensnetz heraus muss unbedingt der Virenschutz beachtet werden. Bei aktuellen Virenwarnungen kann es einige Zeit in Anspruch nehmen, die neuen Virenschutz-Updates auf alle Clients aufzuspielen. In einer solchen Situation kann es sinnvoll sein, den Zugriff auf Webmail zumindest solange zu verhindern, bis die Verantwortlichen für Virenschutz sicher sind, dass ein ausreichender Schutz besteht.
Der Umgang mit Webmail im Unternehmen sollte daher geregelt sein. Hierbei gibt es mehrere Varianten:
Unternehmen können beschließen, die Nutzung von Webmail generell zu verbieten. Dies muss dann natürlich den Mitarbeitern bekannt gegeben werden. Das Verbot kann außerdem technisch durch Filterung bezüglich der bekannten Anbieter unterstützt werden, wobei man sich hier darüber klar sein sollte, dass Benutzer immer neue Wege finden können, um auf solche Dienste zuzugreifen.
Es kann die Empfehlung ausgesprochen werden, Webmail für private E-Mails, die aus dem internen LAN verschickt werden sollen, zu nutzen. Damit kann vermieden werden, dass Mitarbeiter trotz entsprechender Verbote dienstliche E-Mail-Zugänge für private Zwecke nutzen - beispielsweise, weil es dringend oder einfach praktisch ist.
Es gibt auch Unternehmen, in denen Webmail offiziell für dienstliche E-Mails freigegeben ist. Die Gründe hierfür sind unterschiedlich. So gibt es z. B. eine Reihe kleinerer Organisationen, die keinen eigenen E-Mail-Server haben und Webmail für Kommunikation nach außen einsetzen. Webmail kann auch für Mitarbeiter praktisch sein, die auf Dienstreisen auf ihre E-Mail zugreifen müssen, für die aber kein Zugang über Remote Access eingerichtet ist. Ein weiterer Grund für die Nutzung von Webmail kann darin bestehen, dass die jeweilige Organisation bei bestimmten E-Mails nicht nach außen in Erscheinung treten will oder dass Webmail-Adressen dort angegeben werden, wo Spam erwartet wird, also bei bestimmten Downloads, Newsgruppen etc. ■

Ouelle: Grundschutzkatalog des deutschen Bundesamts für sichere Informationstechnologie.

***Herbert Fidesser**, der Verfasser dieses Beitrages ist geschäftsführender Obmann der vSIT reg.GenmbH, die sich mit Schulungen und Beratungen im Bereich der IT-Sicherheit beschäftigt. Weitere Informationen: fidesser@vsit.at*

Anmerkung:

[1] Bitte verwechseln Sie diese Signature, die eine reine Textinformation darstellt, nicht mit der digitalen Signatur, die die Identität der Absenderin, des Absenders tatsächlich nachweist.