Risiko im Anhang

Die elektronische Post zählt zu den wichtigsten schriftlichen Kommunikationsmitteln. Um ihre Sicherheit ist es allerdings in mehrfacher Hinsicht schlecht bestellt.

Es beginnt damit, dass Sie bei einer herkömmlichen E-Mail nie sicher sein können, dass sie den Adressaten erreicht. Das Anfordern einer Lese- oder Übermittlungsbestätigung ist nicht überall möglich und auch nur dann hilfreich, wenn der Empfänger die Rückmeldung zulässt bzw. der Server des Mailproviders diese Services überhaupt unterstützt.
Die an sich sinnvollen Spam-Filter (Junk-Mail-Filter) können sich als Falle erweisen und eine anhand der vordefinierten Kriterien falsch eingestufte E-Mail „schlucken". Zum Teil geschieht dies bereits anbieterseitig online. Oder das Postfach des Empfängers ist voll und die E-Mail kann nicht zugestellt werden. Ob in diesem Fall eine Fehlermeldung zurückkommt (meist „Mailer Daemon" oder „Delivery Status Notification"), ist gleichfalls serverabhängig. „Eingeschriebene" E-Mails mit elektronischem Rückschein, wie es sie etwa bei GMX oder Directbox als kostenpflichtige Zusatzleistungen gibt, bieten zumindest etwas mehr Gewissheit über den Verbleib der versandten Mails. Ob das Gegenüber die Nachrichten tatsächlich liest, ist eine andere Geschichte.

Verschlüsselung mit Lücken

Womit wir beim eigentlichen Thema sind: Es kann auch niemand von uns nachvollziehen, ob die Nachricht wirklich nur vom Empfänger gelesen wird. Die von GMX vor einiger Zeit groß beworbenen verschlüsselten Übertragungswege sind eigentlich eine Selbstverständlichkeit und waren bei den meisten Anbietern schon davor Standard. Dies ändert nichts an den drei bis vier Schwachstellen: der Computer des Absenders, der Server des Mailproviders, häufig der Server eines weiteren Providers sowie der Computer des Empfängers. Überall dort liegen die E-Mails im Klartext vor, vergleichbar einer Postkarte. Ende-zu-Ende-Verschlüsselung direkt am Computer ist eine Lösung. Sie ist etwas umständlich einzurichten, aber es existieren brauchbare Anleitungen dazu (nicht zuletzt in KONSUMENT 9/2014). Alternativ gibt es die Möglichkeit, bestimmte Webmaildienste verschlüsselt zu nutzen (siehe z.B. www.mailvelope.com). Das ist aber alles sinnlos, wenn man keinen Zweiten hat, der es mithilfe derselben Technik ebenfalls tut und somit die Mails auch wieder lesbar machen kann. In gewisser Weise ist die Situation ähnlich wie bei den Smartphone-Messengern: Millionen von Nutzern setzten aus Bequemlichkeit seit jeher auf WhatsApp, obwohl dieser Dienst erst seit April 2016 vollständig verschlüsselt.

Noch einmal lesen

Eine herkömmliche E-Mail ist schnell geschrieben, doch Sie sollten vor dem Abschicken aus mehreren Gründen nochmals drüberlesen. Ist die Nachricht dem Sinn nach verständlich? Hat die automatische Korrekturfunktion zugeschlagen und selbsttätig Wörter geändert? Und stehen vor allem keine zu persönlichen Dinge drin?
Natürlich haben nicht alle möglichen Leute von Haus aus Zugriff auf Ihren E-Mail-Verkehr. Wer kommt also infrage? Zunächst einmal diejenigen, die erlaubter- oder unerlaubterweise Zugang zu Ihrem Computer oder Mobilgerät haben. Bitte keine Pauschalverdächtigungen, aber die Erfahrung sagt: Gelegenheit macht neugierig. Es genügt schon, den Raum zu verlassen, ohne den PC zu sperren, oder sich die E-Mail-Vorschau standardmäßig auf dem Sperrbildschirm des Smartphones anzeigen zu lassen, damit quasi im Vorübergehen Informationen an die Öffentlichkeit gelangen können.
Den kompletten E-Mail-Verkehr lesen kann die IT-Abteilung des Arbeitgebers. Das ist freilich ohne Betriebsvereinbarung bzw. die persönliche Zustimmung jedes Betroffenen nicht erlaubt und betrifft ausschließlich dienstliche E-Mails. In private E-Mails darf der Arbeitgeber keine Einsicht nehmen. Was erlaubt ist, ist aber das generelle Verbot von privaten E-Mails am Arbeitsplatz. In einem solchen Fall genügt es, wenn der Arbeit-

Foto: Alhovik / Shutterstock.com

geber die Überwachung des dienstlichen Mailverkehrs ankündigt. Er benötigt dann keine weitere Zustimmung.
Die E-Mails lesen können auch die Internetprovider. Sie tun dies automatisiert für eigene Zwecke, um – wie etwa Google – interessenbasierte Werbung schalten zu können. Auf behördliche Anfrage geben sie freilich auch die E-Mails im Wortlaut heraus. Wie einfach das geht, hängt von den Gesetzen jenes Staates ab, in dem der Provider angesiedelt ist. Die NSA-Affäre hat gezeigt, dass die Gesetzeslage etwa in den USA sehr überwachungsfreundlich ist.

Betrugsversuch nicht ausgeschlossen

Bleibt noch die Möglichkeit, dass man Opfer eines Betrugsversuches wird. Im Zuge einer sogenannten Man-in-the-middle-Attacke kann sich ein Dritter, der ein privates oder – was wahrscheinlicher ist – ein öffentliches WLAN manipuliert, in die Kommunikation einschalten. Damit kann er nicht nur den Datenstrom zwischen Ihrem Gerät und dem Internet auslesen, sondern auch die E-Mails umleiten, damit sie nicht den vorgesehenen sicheren Transportweg nehmen. Womit wir wieder beim Thema wären, welche Informationen man in unverschlüsselten Mails weitergeben kann und welche besser nicht.
Der in Bezug auf die Sicherheit relevanteste Aspekt ist der Umgang mit empfangenen Mails. Das betrifft nicht nur solche von unbekannten Absendern, die man am besten ungelesen löscht, sondern auch solche von bekannten Personen. Accounts werden unbemerkt gekapert, Adressen missbräuchlich verwendet, Programme durch Schadsoftware dazu veranlasst, selbige per E-Mail an alle gespeicherten Kontakte weiterzuleiten. Kurz: Nur weil Maria Musterfrau Ihre beste Freundin ist, bürgt ihr Name im Absender noch nicht für hundertprozentige Sicherheit – genauso wenig wie Ihr eigener.

Phishing boomt

Wenn Ihre Bank oder ein bekanntes Unternehmen schreibt und Daten von Ihnen haben möchte oder Sie dazu auffordert, einen Internetlink oder ein im Anhang befindliches Dokument zu öffnen, dann ist sowieso Vorsicht angebracht. Ziel solcher Phishing-Mails ist oft, an Ihre Bank- oder Kreditkartendaten zu gelangen. Oder es handelt sich um versuchten Identitätsdiebstahl, um dann unter Ihrem Namen im Internet illegale Handlungen zu setzen. Immerhin: Viele Phishing-Mails sind daran zu erkennen, dass der Absendername – wenn überhaupt – nur auf den ersten Blick dem Original entspricht und dass sie sprachliche Mängel aufweisen.
Trotzdem ist es nicht immer ganz einfach, gefälschte von echten E-Mails zu unterscheiden – was die Frage aufwirft, was man im Zweifelsfall mit Attachments (E-Mail-Anhängen) tun soll. Theoretisch kann in jedem davon ein Virus enthalten sein; in der Praxis sind .zip- und .exe-Dateien besonders kritisch, aber in letzter Zeit auch Word- und Excel-Dokumente (.doc/.docx bzw. .xls/.xlsx). PDF-Dateien sind ebenfalls nicht immer harmlos, und auch HTML-Mails, also formatierte E-Mails mit Grafiken und Bildern, stellen eine Bedrohung dar.

Vorsichtsmaßnahmen

Die nachfolgend beschriebenen Vorkehrungen berücksichtigen die eben genannten Fälle. Manches ist in den gängigen Programmen und Betriebssystemen mittlerweile standardmäßig voreingestellt, Sie sollten sich aber sicherheitshalber davon überzeugen. Und grundsätzlich gilt: Halten Sie die gesamte Software immer auf dem aktuellen Stand und installieren Sie einen Virenschutz.

1. Verhindern Sie, dass Bilder und Grafiken automatisch heruntergeladen werden.

Outlook: »Datei/Optionen/Trust Center (früher: Sicherheitscenter)/Einstellungen für das Trust Center/Automatischer Download«. „Bilder in HTML-Mails oder RSS-Elementen nicht automatisch herunterladen" aktivieren. Ebenfalls im Trust Center unter »E-Mail-Sicherheit« die Option „Standard-Nachrichten im Nur-Text-Format lesen" anhaken. Unter »Datei/Optionen/E-Mail« ganz unten bei „Nach dem Verschieben oder Löschen eines geöffneten Elements" die Option „Zurück zum aktuellen Ordner" einstellen.
Windows Live Mail: »Datei/Optionen/Sicherheitsoptionen/Sicherheit«. „Bilder und andere externe Inhalte in HTML-E-Mails blockieren". Außerdem unter »Optionen/E-Mail« vor „Nachrichten im Vorschaufenster automatisch herunterladen" sowie vor „Alle Nachrichten als Nur-Text lesen" Haken setzen.
Mail-App (Windows 10): »(Zahnradsymbol)/Lesen«. „Nächstes Element automatisch öffnen": Aus; „Externe Bilder und Formate automatisch herunterladen": Aus.
Apple Mail: »Mail/Einstellungen/Darstellung«. Hier muss „Entfernte Inhalte in Nachrichten laden" deaktiviert sein.

2. Verzichten Sie auf das Vorschaufenster (Lesebereich) und auf die Nachrichtenvorschau, denn auch so können bestimmte Viren auf Ihren Computer gelangen.

Outlook: Unter dem Karteireiter »Ansicht« können Sie für jeden Ordner einzeln die Optionen festlegen. Besser keine Vorschau verwenden Sie für: Posteingang, Junk-E-Mail (Spam) und Gelöschte Elemente.
Windows Live Mail: Unter »Ansicht« lässt sich der Lesebereich für sämtliche Ordner ein- und ausblenden.
Mail-App (Windows 10): Die Vorschau lässt sich zwar nicht ausblenden, aber E-Mails lassen sich ungeöffnet löschen.
Apple-Mail: Das Vorschaufenster lässt sich mit dem Mauszeiger nach links bzw. rechts ziehen, also öffnen und schließen. Unter »Mail/Einstellungen/Darstellung« setzen Sie die Listenansicht (= Nachrichtenvorschau) auf „Keine".

3. Aktivieren Sie auf Ihrem privaten Account keinesfalls automatische Antworten oder Abwesenheitsnotizen. Sie bestätigen dadurch lediglich den Absendern von Spam-Mails, dass Ihre E-Mail-Adresse gültig ist.
4. Makros sollten in den Office-Programmen von Microsoft standardmäßig blockiert sein. Kontrollieren Sie unter »Datei/Optionen/Trust Center/Einstellungen/Einstellungen für das Trust Center«, ob die Option „Alle Makros mit Benachrichtigung deaktivieren" markiert ist.
5. Eine Möglichkeit zum relativ sicheren Öffnen unbekannter Anhänge ist Sandboxie (siehe Computertipp auf Seite 13).

Rat und Hilfe für Verbraucher in Europa ECC-Net
Co-funded by the European Union

Dieser Artikel entstand im Rahmen der „Action 670702 – ECC-NET AT FPA", für welche das Europäische Verbraucherzentrum Österreich Förderungen aus den Mitteln des Verbraucherprogramms der Europäischen Union (2014–2020) erhält.

Mehr zum Thema

Bisher in KONSUMENT erschienen:

Browser	1/16
Browser-Erweiterungen	3/16
Flash-Cookies und Skripte	4/16