Spezialthema: Praktikabler Datenschutz / Datensicherheit im Emailverkehr und beim Surfen
Referent: Michael Steinacker

Angriffe im Email-Verkehr und Abwehrmaßnahmen:

Angriffe erfolgen über (sogenannte) Spam-Emails, die glücklicherweise zum größten Teil (90%) durch ein Anti-Spam-Programm der Email-Provider (t-online, gmx, gmail (Google), hotmail/outlook (Microsoft), yahoo, aol, freemail, etc.) erkannt und gelöscht werden, bevor wir (der Empfänger) sie sehen.

Spam-Emails haben vor allem zwei Ziele(siehe unten → Angriffe/Fallen beim Surfen im Internet):

- Entweder soll der Empfänger auf eine gefälschte /gefährliche Web-Seite gelockt werden
- oder der Empfänger soll eine angehängte Datei – ein Viren-Programm - auf seinem Rechner öffnen (und es damit auf seinen Rechner herunter laden).

Bei fragwürdigen Inhalten sollte man also nie auf einen eingebetteten Link klicken und nie eine angehängte Datei direkt in der Email öffnen. Die Datei muss erst gespeichert und auf ihre Endung geprüft werden. Keine Datei öffnen, die auf „.exe“ oder „.msi“ endet, also z.B. (angebliche) Fotodateien mit „jpg.exe“ oder (angebliche) Textdateien mit „doc.exe“ oder „docx.exe“.

Dateien, die einen Virus enthalten, werden typischerweise von den Antivirus-Programmen auf dem PC (Norton, Kaspersky, Avira o.ä.) erkannt.

Spam-Emails lassen sich sehr häufig an folgenden Indizien erkennen: Ich (der Empfänger) bin nicht als der Empfänger erkennbar / der Absender ist mysteriös / die Email hat keine „Unterschrift“.

Verdächtige Spam-Emails missbrauchen auch den Ruf seriöser Absender. Beispiele: Versandbenachrichtigung von Amazon / Postbank – Security-Update-App / Gefälschte DHL-Paketankündigungen / Gefälschte UPS-Paketankündigungen / Vodafone-Rechnungen (Telekom, O2) / Zahlungsaufforderungen von eBay und PayPal / Falsche Ikea-Rechnungen /Ermittlungsverfahren mit Bundeskriminalamt (BKA) als Absender / Virenwarnung vom BSI.

Email-Adressen sind analog wie Post-Adressen auf einem Brief nach einem festen Schema aufgebaut. Um die Angriffe über gefälschte Adressen zu verstehen, folgt hier eine kurze Erklärung der Struktur einer Email-Adresse. Email-Adressen sind immer von hinten zu lesen (so wie Post-Adressen auf einem Brief von der Post bei der Zustellung immer von unter „abgearbeitet“ werden). Als Letztes steht die „Landeskennung“

- .de steht z.B. für „Deutschland, .ch für die Schweiz und .com wurde ursprünglich für USA (als der erste „Adressen-Bereich“ überhaupt im Internet) verwendet und wird daher heute von allen international tätigen Firmen verwendet. (Daraus hat sich die merkwürdige Situation entwickelt, dass die USA als einzige große Nation kein „eigenes“ Landeskennzeichen im Internet hat !)
- davor steht bis zum Zeichen „@“ der Email-Provider/Firma innerhalb des „Landes“. Dieser Teil kann auch noch durch „.“ strukturiert werden (das Finanzamt München hat beispielsweise die email-Adresse: xxxx@famuc.bayern.de)
- vor dem „@“-Zeichen steht typischerweise der Name/Gruppe/Funktion des Empfängers/Senders:

Angreifer arbeiten häufig sehr „kreativ“ mit „gefälschten“ Email-Adressen, die einen seriösen Absender vorgaukeln sollen. Großunternehmen wie Amazon, Banken/Sparkassen, Finanzamt, etc. benutzen (praktisch immer) in ihrer Email-Adresse (nur) den eigene Namen nach dem @-Zeichen, z.B. "@amazon.com" oder "@amazon.de

Die Überprüfung des Absenders beginnt ja von hinten, also mit der Endung für das Land:
daher nie Emails mit Absendern öffnen wie z.B.:
@amazon .com**.ru** / @amazon .com.**izb.ru**/ @**payment-**amazon.de / @amazon**e**.de / @a**n**azon.de/
amazon-security@**hotmail.com** / amazon-payments@**gmx.de**.

Abwehr weiterer Email-Angriffsvarianten:
Keine „HOAX-Mails“ (HOAX : engl. für Jux, Scherz) weitergeben. Diese Mails enthalten beispielsweise eine Warnung vor einem besonders gefährlichen Virus im Internet und man wird gebeten, an alle Freunde diese Email sofort weiter zu leiten. Normalerweise ist dies auch schon der „Haupteffekt“: eine totale Überflutung der Email-Server. Es kommt selten vor, dass in der Email ein Virus steckt.

Reagieren Sie nicht auf Aufforderungen zum Abmelden ("Unsubscribe") von der Verteilerliste einer Spam-Email. Durch die Antwort weiß der Angreifer, dass ihre Email-Adresse „echt“ ist oder er verkauft die Email-Adresse (noch teurer) an weitere „Spam-Emailer“ und wer sich irrtümlich in eine „Spam-Email-Liste“ eingetragen hat, hat ein echtes Problem!

Verschlüsselung (für vertraulichen Email-Anhang)

Zum Sichern von vertraulichen Anhängen ist es sinnvoll, diese Anhänge vor dem Versand (symmetrisch) zu verschlüsseln. Dann kann während des Versendens kein Angreifer diese Information lesen. Für eine (symmetrische) Verschlüsselung vereinbaren alle Beteiligten vorher gemeinsam einen „Schlüssel“ und ein (Verschlüsselungs-) Verfahren. Eine praktische Methode für das „Verfahren“ ist heute die Verwendung von (sogenannten) „Zip“-Programmen. Zip-Programme sind eigentlich Programme, um Daten zu komprimieren, und erzeugen eine Datei mit der Endung „.zip“ – wenn sie sich an bestehende „Standards“ halten. Sie sind also zum Versenden von (großen) Anhängen in einer Email sehr sinnvoll. Glücklicherweise hat sich bei den „Standard“ Zip-Programmen auch eine zuverlässige Verschlüsselung durchgesetzt, die man für diesen Zweck nun gut nutzen kann.
Im Internet ist das Programm „7-Zip“ kostenlos aus „sicheren“ Quellen erhältlich. Dies benötigt jeder Anwender, der Dateien verschlüsseln will. Anwender, die nur diese Dateien empfangen und lesen möchten, kommen mit einer „Standard-Microsoft-Installation“ aus, und müssen natürlich den gemeinsamen Schlüssel kennen und beim Öffnen der Datei eingeben.

Angriffe/Fallen beim Surfen im Internet:

Viren:
Manche Web-Seiten laden automatisch Viren auf den Rechner. Viren sind Schad-Programme, die auf den PC unerlaubte Aktionen durchführen sollen. Typische Aktionen sind

- das Sammeln und Versenden von Passwörtern an den „Viren-Angreifer“. Mit Passwörtern von Internet-Shops kann der Angreifer möglicherweise auf Kosten des Opfers dann einkaufen.
- beim Online-Banking: Änderung der Überweisungen, sodass eine große Geldmenge auf das Konto des Angreifers überwiesen wird.
- Verschlüsseln der (privaten) Daten auf dem PC; der Schlüssel wird erst nach der Zahlung einer gewissen Geldmenge auf dem PC wieder zur Verfügung gestellt (häufig 500 €, siehe Süddeutsche Zeitung vom 28/29.11.2015 Seite 31).

Phishing:
durch gefälschte Web-Seiten, die beispielsweise eine Bank oder einen Internet-Shop vortäuschen, werden Ihre Anmeldedaten und andere vertrauliche Informationen gestohlen (Identitätsdiebstahl)

„Neu anmelden“:
Webseiten, die zum Herunterladen von Kochrezepten, „kostenloser“ Software, Treibern, Musik, Bildern etc. eine Neuanmeldung, häufig mit Adresse, verlangen, stellen sich dann als kostenpflichtig heraus: man erwirbt eine Mitgliedschaft, ein Abonnement, o.ä.

Meldung: „Virenscanner downloaden“:
Die Meldung „ein Virus wurde entdeckt, dringend einen zusätzlichen Virenscanner downloaden“ nicht befolgen – der „Download“ ist selbst der Virus

Abwehrmaßnahmen beim Surfen:

Kaufen und Downloads nur aus vertrauenswürdigen Quellen (dazu nach Bewertungen im Internet suchen, ist aber leider speziell für ungeübte Anwender recht schwierig).

Keine „betrügerischen" Web-Seiten aufrufen.

Adressenname: Die (letzten) Teile vor dem ersten „/" prüfen z.B. http://www.name.com/entry/cc/de/ und dann die Interpretation immer von hinten starten – wie bei Email-Adressen:
Ein „Angreifer" ist z. B. zu erkennen an: http://www.name.com.**ru**/entry/cc/de

Bei wichtigen Aktivitäten(Online-Banking, Einkauf mit Konto oder Kreditkarte, etc.) sollte die Adresse im Browser oben mit https://.... beginnen. Zusätzlich ist im Browser (meistens neben der Adresse) ein Symbol eines geschlossenen Schlosses. Die Adresse ist jetzt bei Banken grün unterlegt. (eigentlich sollte das auch bei jedem Login und jeder Bezahlung sein, ist es aber leider nicht!)

Spezielle Sicherheitsmaßnahmen beim Online-Banking

Überweisung und mTan auf demselben Gerät zu speichern, ist extrem gefährlich. Die Virusgefahr ist in diesem Fall besonders hoch. Banken machen die Gerätetrennung zur Sicherheitsvorgabe, die Nicht-Beachtung stellt eine grobe Verletzung der Sorgfaltspflicht dar.

Banken fragen nie nach login-Daten oder mTan „zum Testen"

Nie PINs, TANs, Passwörter, Telefonnummern oder andere Sicherheitsinformationen (Geburtsort, Geburtsname der Mutter, Name des Haustieres, etc.) auf Email/Telefon-Nachfrage bekanntgeben! Seriöse Firmen machen so etwas nicht.

Keine „vermeintlichen" Sicherheitsupdates der Bank herunterladen (besonders bei Smartphones)

Fazit:

Technisch

Aktuelle Sicherheitssoftware (Virenscanner)auf dem PC installieren
Regelmäßig Updates einspielen lassen von Microsoft, Adobe (Acrobat-Reader + Flash-Player), Java etc.
Wichtige private Dateien regelmäßig auch extern sichern, damit sie zweimal vorhanden sind
Alle Endungen anzeigen lassen! Einzelschritte dazu bei Microsoft: Extra - Ordneroptionen - Ansicht - *kein* Häkchen bei „Erweiterungen bei Bekannten Datentypen ausblenden"

Menschlich

Viel wichtiger allerdings als all das ist es, sich bewusst zu werden, was man tut und was man besser lässt. Vieles lässt sich mit gesundem Menschenverstand vermeiden, wenn man ein Verständnis fürs Internet entwickelt, d.h. eine gesunde Mischung aus Vertrauen und Misstrauen.
Kaufen und Downloads nur aus vertrauenswürdigen Quellen (dazu nach Bewertungen suchen).

Im Zweifelsfall ist es immer günstiger, vertrauensvolle Personen (Freunde, bekannte) zu fragen, als hinterher den Schaden zu beseitigen/bezahlen.

Zuverlässige Quellen für die Sicherheit im Internet:

https://www.sicher-im-netz.de/

https://www.bsi-fuer-buerger.de/BSIFB/DE/Home/home_node.html

http://www.sicher-online-gehen.de/ (Kinderschutz im Internet)

www.bsi.de (Bundesamt für Sicherheit in der Informationstechnik)