Security Lektion 7
E-Mails und IM

- E-Mails
  Social Engineering
  Malware
  Phishing
  Verschlüsseln und digitale Signatur
- IM
  Begriff
  Sicherheit, Gefahren und Vertraulichkeit

✓ Elektronische Nachrichten werden sekundenschnell und unkompliziert versandt. Ihr Vorteil ist nach wie vor die Unabhängigkeit von einer Plattform. Mit Verteilerlisten erreicht man schnell viele Personen, Darum wird dieses Medium gerne für betrügerische Zwecke missbraucht.
Weil E-Mails zudem so geheim sind wie Postkarten, sollten Sie Nachrichten verschlüsselt senden.

Aufgabe

1. E-Mails

Online Social Engineering durch betrügerische und unerwünschte Nachrichten

Für betrügerische Aktionen gibt es mittlerweile den Fachbegriff *Online Social Engineering*. Dabei wird das Internet verwendet, um an Informationen zu kommen. Der „gratis Antivirus-Download" oder „100 MB kostenloser Webspace" entpuppen sich als Hacker-Werkzeuge (vgl. dazu Sicherheit / Lektion 1).

Unter SPAM bzw. JUNK E-Mails fallen unerwünschte Werbemails, meist für zweifelhafte Zwecke (vorgetäuschte Gewinne, Hilfe für in Not Geratene, etc.).

Malware

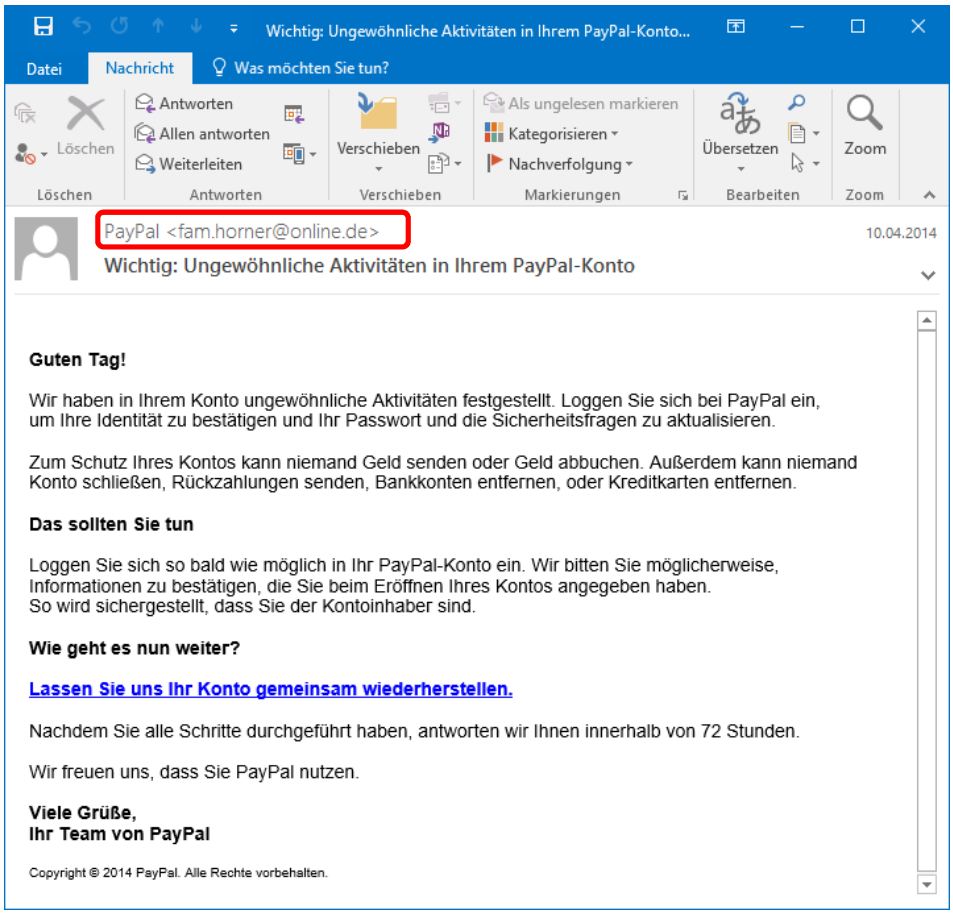
Wenn Sie auf Ihrem PC oder mobilem Gerät, E-Mails senden und empfangen, werden Sie immer wieder im Anhang Dateien mitgesendet erhalten. Das könnte die Telefonrechnung sein, ein Vertrag oder ein Angebot. Wichtig ist, dass in Attachments auch Malware enthalten sein kann. Bei E-Mails könnte beispielsweise beim Öffnen ein Makro ausgeführt oder beim Anklicken eine ausführbare Datei gestartet werden. In der ersten Lektion haben Sie zum Schutz vor Makroviren Sie bereits die Makroeinstellungen geändert.

Nutzen Sie auf jeden Fall ein Antiviren-Programm, bevor Sie Dateien mit der Endung **.exe* öffnen. Auch **.bat* oder **.dot* oder **.scr* sind heikel. Auch stimmt etwas nicht, wenn die Dateinamen aus scheinbar zwei Endungen bestehen. Besser gar nicht öffnen.

Phishing

Das in diesem Training schon erwähnte Kurzwort für Password und Fishing bedeutet, dass jemand eine falsche Identität annimmt, um an persönliche Zugangsdaten zu kommen. Dabei werden entweder E-Mails mit einer Aufforderung verschickt, die

Zugangsdaten zurückzumailen oder in der E-Mail befindet sich ein Link zum vermeintlich echten Institut (siehe Abbildung auf der nächsten Seite). In Wahrheit aber führt der Link nicht auf die Originalseite, sondern auf eine Fälschung.



Von Phishing-Attacken betroffen sind mittlerweile alle Firmen. Ich habe vermeintliche E-Mails von PayPal, Internet-Providern, Kreditkaren-Firmen, Amazon und auch von Microsoft erhalten. Manchmal ist es schwierig, die Fälschung zu erkennen. Banken senden sicher keine E-Mails, bei den Rechnungen vom Internet-Provider stimmt mit der Absender-Adresse etwas nicht und die Zahlungsaufforderung von Amazon hat nichts mit einer wirklichen Bestellung zu tun. Sehen Sie in der Abbildung oben nach, von wem die Nachricht kam. In der roten Umrandung steht:

PayPal <fam.horner@online.de>.

Den Benutzernamen kann man in den Kontoeinstellungen nach Belieben ändern, die E-Mail-Adresse aber bleibt. So erkennen Sie die Fälschung. Außerdem fehlt eine persönliche Anrede. Auch in der Grußformel fehlen Informationen über das Unternehmen. Und wenn mit der Maus auf den vermeintlichen Link gezeigt wird, erscheint eine Infobox mit der Webadresse, die geöffnet wird, wenn man darauf klickt. Diese angezeigte Adresse (siehe Abbildung auf der nächsten Seite) kann von keinem seriösen Unternehmen sein. Also gar nicht erst draufklicken.

Informieren Sie die echten Firmen auf jeden Fall über den Phishing-Versuch. So können diese Unternehmen Ihre Kundschaft wenigstens warnen.

Verschlüsseln und digitale Signatur

Man sagt gemeinhin, E-Mails sind so sicher wie Postkarten. Nicht ganz: denn auf Postkarten befindet sich wenigstens die persönliche Unterschrift. E-Mails verfügen nicht über diesen Urheber-Beweis. Erst mit einer digitalen Signatur wird sichergestellt, dass ein E-Mail nicht gefälscht wurde. Optimal ist, wenn zusätzlich eine verschlüsselte Übertragung stattfindet. (Websites verfügen zB über digitale Zertifikate, wenn Waren verkauft oder persönliche Daten eingegeben werden. Einerseits haben Sie als Kunde oder Kundin die Garantie, dass die Identität der Website gewährleistet ist und andererseits haben Sie die Sicherheit, dass Ihre Daten verschlüsselt übertragen werden.)

Wie funktioniert das?

Persönliche Zertifikate bestehen aus drei Komponenten: Einer *digitalen Signatur*, einem *privaten* und einem *öffentlichen Schlüssel*. Die Digitale Signatur ist eine kryptische Zeichenfolge. Der Empfänger oder die Empfängerin verfügt über den privaten Schlüssel. Der geheime Schlüssel, der auf dem Computer des Absenders beibehalten wird und vom Absender verwendet wird, um Nachrichten an Empfänger mit einer digitalen Signatur zu versehen und um Nachrichten von Empfängern zu entschlüsseln. Private Schlüssel sollten kennwortgeschützt sein. Stimmt dieser Schlüssel mit dem verwendeten öffentlichen Schlüssel überein, kann die Nachricht entschlüsselt und gelesen werden. Ohne den entsprechenden privaten Schlüssel wird lediglich verstümmelter Text angezeigt.[1]

Wo fordere ich ein persönliches Zertifikat an?

Ein persönliches Zertifikat, auch digitale ID genannt, wird von einer unabhängigen Zertifizierungsstelle, einem sogenannten Trust Center, ausgestellt.

Wie verschlüssle ich eine einzelne Nachricht?

Erstellen Sie in Outlook eine neue Nachricht. Klicken Sie auf der Registerkarte OPTIONEN in der Gruppe BERECHTIGUNG auf NACHRICHTENINHALTE UND ANLAGEN VERSCHLÜSSELN.

Wird diese Schaltfläche nicht angezeigt, so öffnen Sie im Register OPTIONEN das Dialogfeld der Gruppe WEITERE OPTIONEN. Ändern Sie die SICHERHEITSEINSTELLUNGEN und aktivieren Sie das Kontrollkästchen NACHRICHTEN UND ANLAGEN VERSCHLÜSSELN.

[1] *Um mehr über die unterschiedlichen Arten der Verschlüsselung zu erfahren, besuchen Sie beispielsweise http://de.wikipedia.org/wiki/E-Mail-Verschl%C3%BCsselung.*

Wie verschlüssle ich alle ausgehenden Nachrichten?
Wählen Sie DATEI | OPTIONEN. Wählen Sie in der Kategorie SICHERHEITSCENTER die Schaltfläche EINSTELLUNGEN FÜR DAS SICHERHEITSCENTER. Aktivieren Sie die gewünschten Kontrollkästchen und bestätigen Sie mit **OK**.

Wie empfange ich eine verschlüsselte Nachricht?
Öffnen Sie eine verschlüsselte Nachricht und erlauben Sie den Zugriff auf den privaten Schlüssel.

2. IM

Begriff

Instant Messaging bedeutet die sofortige Nachrichtenübermittlung, bei der sich zwei oder mehrere Teilnehmende Textnachrichten übermitteln. Diese Texte werden sofort übermittelt. Besser bekannt ist diese Technik unter dem Namen *Chatten* (englisch für *plaudern, sich unterhalten*).

Zum Chat müssen Sie sich erst registrieren. Im Chatroom sehen Sie, wer aus Ihrer Kontaktliste online ist. Tippen Sie Ihre Nachricht in den Eingabebereich und bestätigen Sie mit der Enter-Taste. Der Beitrag wird für die anderen Teilnehmenden sichtbar.

Sicherheit, Gefahren und Vertraulichkeit

Es ist üblich, sich in Chatrooms mit einem *Nickname* anzumelden. Das bedeutet, man weiß nicht, wer sich hinter einem Namen wirklich verbirgt. Also Vorsicht bei der Preisgabe von vertraulichen Informationen. Weil aber die Gefahr eines Missbrauchs von personenbezogenen Daten groß wäre, bleibt man bei der Verwendung von Nicknames.

Höflichkeit ist jedoch auch im Chatroom angebracht, nicht nur im direkten Kontakt mit anderen Menschen. Der Fachbegriff für Verhaltensregeln im Chat lautet *Chatiquette*.

Gibt es im Chatprogramm zusätzliche Möglichkeiten zur Übermittlung von Dateien, lassen Sie wieder Ihre Vorsicht walten – starten Sie keine fremden Dateien, da sie Malware enthalten könnten.

Diese Vorkehrungen können Sie treffen:

- Nachrichten verschlüsseln
- Teilnehmer, die nicht vertrauenswürdig oder unbekannt sind, blockieren
- Daten, die persönlich sind, nicht weitergeben
- Vorsicht ist geboten, wenn jemand Hilfe anbietet und auf Ihren Rechner zugreifen möchte, zum Beispiel über Fernwartung
- Beim Download von Apps auf ein mobiles Gerät achten Sie bitte auf seriöse Plattformen. Einerseits könnten Keylogger und andere Malware installiert werden, andererseits könnten Kosten entstehen oder sogar Ihre persönlichen Daten ausgelesen werden. Auch verlangen manche Apps Zugriff auf Einstellungen, damit die Software installiert werden kann. Dabei wird unter Umständen weitreichender Zugriff gewährt, beispielsweise auf

  Kontakte
  Standort
  Bilder
  etc.

Haben Sie Ihr mobiles Gerät verloren oder wurde es gestohlen, dann können Sie eine *Geräteortung* vornehmen, eine *Fernsperre* setzen und als letzte Maßnahme auch eine *Fernlöschung* Ihrer Daten vornehmen. So können Sie dem Missbrauch Ihrer Daten zuvorkommen – unter der Voraussetzung, dass Sie dabei schnell vorgehen und dem Dieb nicht genug Zeit geben, die Daten auszulesen!

Auch wenn Sie über das Internet telefonieren – der Fachbegriff lautet VoIP – sind Sie weder vor Lauschangriffen noch vor Malware gefeit. Nutzen Sie darum einen vertrauenswürdigen Anbieter wie https://www.teamviewer.com/de/ oder http://www.skype.com.

Sicherheit Schritt sieben
Sichere Kommunikation online

Übung und Selbststudium

1. Finden Sie heraus, wie in Ihrem Land die Rechtslage zu unerwünschten Werbemails aussieht.
2. Wo erhalten Sie ein persönliches Zertifikat? Was kostet es?
3. Wie installieren Sie den privaten Schlüssel?
4. Wie senden Sie ein persönliches Zertifikat?
5. Woran erkennen Sie eine ausführbare Datei?
6. Recherchieren Sie zum Thema Chatiquette.

Testen Sie Ihr Wissen

1. Wie sicher sind E-Mails?
2. Was können Sie tun, um die Echtheit Ihres E-Mails zu garantieren?
3. Welche persönlichen Daten können missbräuchlich verwendet werden?

Notizen

Wussten Sie, dass es einen Unterschied zwischen dem Löschen und dem Vernichten von Dateien gibt? Damit beschäftigt sich unter anderem die nächste Lektion.