

Sicherheit Lektion 7

E-Mails und IM

E-Mails

- ✗ Social Engineering
- ✗ Phishing
- ✗ Malware
- ✗ 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

Attachments könnten Malware enthalten. Bei E-Mails könnte beispielsweise beim Öffnen ein Makro ausgeführt oder beim Anklicken eine ausführbare Datei gestartet werden.

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 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 (siehe Abbildung) oder in der E-Mail befindet sich ein Link zum vermeintliche echten Institut. In Wahrheit aber führt der Link nicht auf die Originalseite sondern auf eine Kopie.



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. 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.

Um mehr über die unterschiedlichen Arten der Verschlüsselung zu erfahren, besuchen Sie beispielsweise <http://de.wikipedia.org/wiki/E-Mail-Verschl%C3%BCsslung>.

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 verschlüssele ich eine einzelne Nachricht?

Erstellen sie in Outlook eine neue Nachricht. Klicken Sie auf der Registerkarte NACHRICHT 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.

Wie verschlüssele 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 empfangen Sie eine verschlüsselte Nachricht?

Öffnen Sie eine verschlüsselte Nachricht und erlauben Sie den Zugriff auf den privaten Schlüssel.

2. IM

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.

Falls Sie *ICQ* oder *Windows Live Messenger* nutzen, sollten Sie wissen, dass die Übertragung unverschlüsselt erfolgt! Nutzen Sie darum besser <http://www.skype.com> oder www.pidgin.im zum Chatten.

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