Leseprobe

IT-Sicherheit

Studienheft

IT-Sicherheit

Autorin

Florian Jörgens (M.Sc.)

Überarbeitung:

Prof. Dr. Carsten Lang

IT-Sicherheit

Verfasser:
Florian Jörgens (M.Sc.)

Überarbeitung:
Prof. Dr. Carsten Lang

Merke

Datensicherungen sollten regelmäßig durchgeführt werden. Oftmals wird das Thema erst behandelt, wenn es bereits zu einem Datenverlust gekommen ist.

Online-Campus

Eine Onlinevorlesung hierzu findest Du in Deinem Online-Campus.

3.6 Sei skeptisch gegenüber E-Mails aus unbekannter Quelle

Die Globalisierung und die stetig wachsende Digitalisierung haben neben einer Vielzahl an Vorteilen auch diverse Schattenseiten mit sich gebracht. Durch das Medium E-Mail ist die Kommunikation mit einer schier unendlichen Anzahl an Menschen machbar. Dies eröffnet kriminellen Einzelpersonen, Institutionen sowie Organisationen neue Geschäftsmodelle, um sich Geld oder Informationen auf betrügerische Art und Weise zu beschaffen.

Der technologische Fortschritt hat dazu geführt, dass technische Maßnahmen der IT-Sicherheit immer besser geworden sind. Dies haben auch die Angreifer festgestellt und die Angriffsmuster angepasst.

Da sich ein Mensch leichter hacken lässt als ein System, sind es vor allem Attacken aus dem Bereich Social Engineering, die in Kombination mit klassischer Schadsoftware ihre Opfer treffen.

Beim **Social Engineerings** nehmen Angreifer durch zwischenmenschliche Interaktionen Personen ins Visier und versuchen, ihr Verhalten dahingehend zu beeinflussen, dass sensible Daten oder Informationen freiwillig herausgegeben werden, oder dass sie ein anderes nicht regelkonformes Verhalten (z. B. Vornahme von nicht korrekt geprüften und freigegebenen Überweisungen) zeigen. Diese Ausnutzung menschlicher „Schwächen" baut auf den Elementen Vertrauensaufbau, Mitleid oder Mitgefühl sowie auf dem Eindruck, zwischenmenschliche Hilfe zu leisten, oder anderen psychologischen Mechanismen (z. B. Angst, Einschüchterung) auf.

Dies muss nicht einmal auf hoch technisierte Art und Weise passieren: Ein einfacher Telefonanruf einer vermeintlich verzweifelten Mutter mit Babygeschrei im Hintergrund mag schon ausreichen, um an die ein oder andere Information zu gelangen. Dabei sind viele Adressaten im Unternehmen denkbar: Der CEO hat wenig Zeit und ist vielleicht schneller geneigt, ohne großartige Prüfung auf persönlich formulierte, detailreiche Anfragen einzugehen. Aushilfskräfte möchten sich profilieren und legen deswegen ein hohes Maß an Hilfsbereitschaft an den Tag. Assistenten haben oftmals umfassenden Zugang und möchten ihrem Vorgesetzten Arbeit abnehmen. Nimmt ein Angreifer die Identität des Vorgesetzten an (sogenannter CEO-Fraud), traut sich ein Assistent gegebenenfalls nicht, dies zu hinterfragen. So sind viele weitere Beispiele denkbar.

Klassische Szenarien sind hierbei zum Beispiel der vermeintliche Anruf eines falschen Administrators, der Zugangsdaten wie Passwörter oder Bankdaten abfragen möchte.

Phishing

Ein anderes gängiges Beispiel für Social Engineering ist Phishing (Neologismus aus password und fishing). Hierbei werden Nachrichten, Webseiten oder E-Mails täuschend echt gefälscht, an das Opfer geschickt und darauf vertraut, dass das Opfer die entsprechenden Links in der E-Mail anklickt, Benutzername und Passwort einträgt, Dateianhänge runterlädt o. Ä.

Hierzu kopieren Angreifer die originalen Webseiten und manipulieren diese so, dass Eingaben nicht an den eigentlichen Server, sondern an die Angreifer geschickt werden. Dadurch können Zugangsdaten, Bankdaten usw. abgefangen werden.

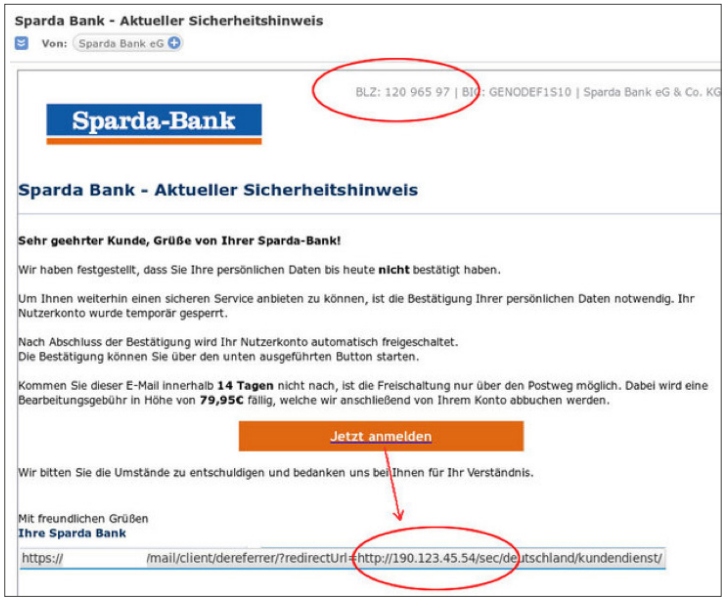

Abb. 11 Phishing
(entnommen aus BSI-fuer-Buerger.de o. J.)

Abb. 12 Phishing
(entnommen aus BSI-fuer-Buerger.de o. J.)

Am Beispiel der letzten Abbildung kann man sehen, wie perfide diese Masche ist. Nicht nur, dass die E-Mail im Corporate Design erstellt wurde, Ralf Hoßbach ist tatsächlich Leiter des Kundenservice.

Abb. 13 Phishing Telekom 2
(eigene Darstellung)

Eine Möglichkeit, um diesen Betrug als Empfänger zu entdecken, ist, mit der Maus über den Link zu fahren und somit das Vorschaufenster zum eigentlichen Link aufzuklappen. Daran erkennt man, dass die tatsächliche Webseite eine andere ist, als angegeben.

Weitere Anhaltspunkte, an denen man Phishing erkennen kann, sind:

- gefälschte Absenderadressen
- unpersönliche Anrede
- Hinweis auf dringenden Handlungsbedarf
- Drohungen
- Abfrage vertraulicher Daten
- Aufforderung zum Öffnen von Anhängen oder Anklicken von Links

CEO-Fraud

In eine ähnliche Richtung agiert die Betrugsmethode „Chef-Masche“ (oder auch: CEO-Fraud), bei der Angreifer durch die Verwendung falscher oder gestohlener Identitäten zur Überweisung von Geld auffordern.

CEO steht hierbei für Chief Executive Officer, da sich die Angreifer oftmals als Geschäftsführer des Unternehmens ausgeben. Über soziale Netzwerke wie Xing oder LinkedIn werden befugte Mitarbeiter aus Finanzbuchhaltung und Rechnungswesen sowie deren Vorgesetzte identifiziert. Durch die Nutzung bestimmter Tools und Webseiten mit denen man E-Mail-Absender fälschen kann, bekommen diese Mitarbeiter dann Aufforderungen vom vermeintlichen Vorgesetzten, Geld auf bestimmte Konten zu überweisen. Zusätzlich werden die Mitarbeiter unter Zeitdruck gesetzt.

Das FBI geht davon aus, dass Business Email Compromise/Email Account Compromise, zu dem CEO-Fraud und Phishing zählen, in den USA in 2021 einen Schaden von 2,4 Milliarden US-Dollar verursacht hat (FBI 2021, S. 9).

Das Bundesamt für Sicherheit in der Informationstechnik rät hier zu besonderer Vorsicht und gibt bestimmte Handlungsempfehlungen (BSI.bund.de o. V. 2017):

- öffentliche Kontaktdaten sollten sich auf allgemeine Adressen beschränken
- Schulung der Mitarbeiter
- Aufbau eines internen Kontrollsystems, was ungewöhnliche Zahlungsanweisungen verhindert
- Absenderadresse verifizieren, Inhalt der E-Mail auf Plausibilität überprüfen
- beim Auftraggeber vorher nachfragen

Grundsätzlich gilt bei E-Mails aus unbekannter Quelle oder Nachrichten mit zweifelhaftem Inhalt, eine gesunde Skepsis zu haben und sich zu fragen:

- Habe ich etwas mit dem Absender oder Inhalt zu tun?
- Kann der Absender meine E-Mail-Adresse haben? (vor allem bei gefälschten Telefon-Rechnungen oder Lieferbenachrichtigungen auf die berufliche E-Mail-Adresse auffällig)
- Ist die Absender-E-Mail-Adresse echt?

Die Phishing-Angriffe müssen hierbei nicht zwingend per Mail erfolgen, sondern können grundsätzlich auch per SMS oder WhatsApp geschehen.

Im Zweifelsfall sorgt ein kurzes Telefonat bei dem eigentlichen Unternehmen oder Absender für Klarheit und vermeidet mögliche Schadensszenarien. Ansonsten kann auch der IT-Support unterstützen.

Auch gehen viele Nutzer von der Annahme aus, dass nichts passieren könne, wenn E-Mails nur gelesen, aber keine Anhänge angeklickt werden. Dem ist leider nicht so. Viele E-Mails werden heute im HTML-Format verschickt. Dies ermöglicht u.a. die Formatierung der Texte oder das Einfügen von Grafiken. Im Kern stellt HTML eine Programmiersprache dar. In den Quellcode des entsprechenden Programms können damit auch schädliche Anweisungen eingefügt werden. Außerdem ist es möglich, mittels HTML-Code die Gültigkeit der E-Mail-Adresse des Empfängers zu bestätigen (BSI 2023).

Merke

Verdächtige E-Mails sollten nicht gelesen, sondern sofort gelöscht werden. Die Anzeige im HTML-Format sollte deaktiviert werden. Wird eine E-Mail geöffnet und man ist sicher unsicher, sollte die E-Mail stets auf Inhalt, Absender und Seriosität geprüft werden, bevor Anhänge geöffnet oder Links angeklickt werden. Falls Zweifel bzgl. der Korrektheit des Absenders bestehen, sollte dieser über einen anderen Kommunikationskanal kontaktiert werden, um die tatsächliche Herkunft der E-Mail vor dem Öffnen zu klären.

Online-Campus

Eine Onlinevorlesung hierzu findest Du in Deinem Online-Campus.

3.7 Sichere Nutzung des Internets

Für viele ist das Internet zum alltäglichen Begleiter und Unterstützer im beruflichen als auch privaten Umfeld geworden. Dabei wird neben dem Komfort und der Erleichterung vieler Dinge übersehen, welche Gefahren hinsichtlich der eigenen Daten dort lauern.

Unabhängig davon sollte stets eine strikte Trennung privater und beruflicher Daten erfolgen.

Dies bedeutet, dass für beide Bereiche unterschiedliche Passwörter verwendet werden und diese nicht im Browser, zwecks Möglichkeit des Auslesens, gespeichert werden sollten.

Weiterhin ist es wichtig, sich darüber im Klaren zu sein, dass Informationen, die im Internet stehen, nicht mehr verschwinden. Dies gilt vor allem für Foren, Boards und soziale Netzwerke. Auch wenn Daten durch den Benutzer gelöscht werden, speichern Suchmaschinen wie Google diese noch in einer Art Zwischenablage (Cache) für unbestimmte Zeit.

In vielen Fällen greifen wir über **Browser** auf das Internet zu (z. B. Microsoft Edge, Google Chrome oder Mozilla Firefox). Eine ausreichende Sicherheit kann nur erreicht werden, wenn der Browser in geeigneter Weise konfiguriert ist (vgl. dazu und im Folgenden BSI 2023). Vor allem die folgenden Aspekte sollten berücksichtigt werden:

- nicht notwendige Add-ons/Plug-ins sollten deinstalliert oder deaktiviert werden,
- über die Datenschutzeinstellungen können u. a. bestimmte Zugriffe blockiert, Browser-Daten gelöscht und Cookies von Drittanbietern gesperrt werden,
- Adressen für sicherheitskritische Anwendungen (z. B. Online-Banking) sollten manuell eingegeben und nicht aus mehr oder weniger dubiosen Quellen kopiert werden.

Viele Programme werden heute aus dem Internet heruntergeladen. Prüfen Sie vor jedem **Download eines Programms,** ob die Quelle vertrauenswürdig ist. Idealweise werden Programme nur von der Web-Page des Herstellers heruntergeladen. Nicht selten haben sich Nutzer über das Herunterladen eines vermeintlich nützlichen Programms einen Trojaner installiert.

Geben Sie persönliche oder vertrauliche Daten nur auf Internet-Seiten ein, die über eine Verschlüsselung verfügen. Sie erkennen diese Seiten an dem Kommunikationsprotokoll https in der Adresszeile oder dem Symbol für ein geschlossenes Schloss. Beim Rückgriff auf Wireless LAN sollte der Router so konfiguriert sein, dass er den Standard WPA3 unterstützt.

Seit einiger Zeit weit verbreitet ist die Nutzung sogenannter Cloud-Dienste wie z. B. Dropbox, Google Drive, Microsoft Azure oder Amazon Web Services, also der Nutzung von digitalem Speicherplatz im Internet zur Ablage von Dateien. Hier muss sich der Anwender bewusst machen, dass die Daten nicht in einer risikofreien „Wolke" liegen, sondern de facto auf dem Computer eines fremden Unternehmens, dass genauso den Gefährdungsszenarien der IT-Sicherheit (vgl. Kapitel 2 „Gefährdungen der IT-Sicherheit") ausgesetzt ist wie das eigene.

QV

Grundsätzlich gilt diese Vorsicht auch bei der Nutzung von Kommunikationsdiensten wie WhatsApp oder Filesharing-Diensten wie WeTransfer. Der Benutzer kann nicht wissen, wer sonst noch Zugriff auf diese Systeme hat und wo diese Daten tatsächlich liegen. Je nach Land, in dem die Daten effektiv gespeichert sind, können z. B. komplett andere Datenschutzbestimmungen gelten, als sie für die europäische Union zutreffen. Unternehmen sollten die Nutzung auf bestimmte Dienste beschränken oder eigene zur Verfügung stellen, da die Nutzung nicht genehmigter Dienste zu einem Datenverlust führen kann.

WhatsApp verfügt zwar, wie in der nachfolgenden Abbildung zu sehen, über eine sogenannte Ende-zu-Ende-Verschlüsselung, also der Verschlüsselung während der Übermittlung, allerdings werden die Chat-Verläufe unverschlüsselt auf dem jeweiligen Smartphone abgelegt, sobald diese empfangen wurden, und sind somit dort angreifbar. Ebenso werden Back-ups unverschlüsselt auf dem Smartphone abgelegt. Einige Daten werden darüber hinaus auf den Servern des Anbieters (z. B. eigene Telefonnummer und Kontakte) abgelegt. Ferner wurden in der Vergangenheit wiederholt Schwächen bei der End-to-End-Verschlüsselung bekannt.

Abb. 14 Ende-zu-Ende-Verschlüsselung
(entnommen aus WANNENMACHER 2016)

Sobald sich im Internet bewegt wird, stellt Schadsoftware eine omnipräsente Bedrohung dar. Dabei existiert ein Katz-und-Maus-Spiel zwischen Anbietern von Software, die versuchen ihre Sicherheitslücken zu schließen, und Angreifern, die diese ausnutzen wollen.

Schadsoftware

Es gibt im Bereich der Schadsoftware eine Vielzahl an unterschiedlichen technischen Varianten. Zu den bekanntesten zählen:

Viren

Hierbei handelt es sich um ein Programm, welches sich lokal auf einem Rechner selbstständig verbreitet und kopiert, indem es sich an bestimmte Dateien hängt, also den Code verändert oder in Sektoren der Festplatte (insbesondere Boot-Sektoren) schreibt. Viren können nur dann von einem auf den anderen Computer übergreifen, wenn sie z. B. per USB-Stick übertragen werden. Natürlich können sie auch per E-Mail mit infiziertem Anhang verschickt werden. Viren können Dateien zerstören oder Systemfehler verursachen. Ein Virus ist also wie eine Art Infektion, die andere Computer ansteckt.

Würmer

Würmer verbreiten sich, ähnlich wie Viren, selbstständig, befallen hierbei allerdings keine anderen Programme. Die Ziele sind stattdessen das Eindringen in fremde Geräte sowie die anschließende Ausführung der eigenen Kopie. Typische Übertragungswege sind hierbei Anhänge in E-Mails, da viele Würmer sich automatisch an sämtliche Adressaten in E-Mail-Adressbüchern weiterleiten.

Trojaner

Trojaner tarnen sich als harmloses Programm, um Zugriff auf einen Rechner zu bekommen. Der Nutzer startet die Anwendung und ermöglicht somit dem Unbefugten über eine in dem Programm versteckte Schadensroutine z. B. die Kontrolle über das System. Trojaner verbreiten sich nicht wie beispielsweise Viren oder Würmer, sind allerdings aufgrund der Möglichkeit des Systemzugriffs riskant. Zur Kategorie der Trojaner gehören unter anderem auch Spyware, also Software, die Daten über das System sammelt und diese verschickt, sowie Keylogger, die Tastatureingaben protokollieren.

Ransomware

In dem vergangenen Jahren hat außerdem der Schaden durch Ransomware starkt zugenommen. Hierbei handelt es sich um Schadprogramme, die über Eigenschaften von Würmern und Trojanern verfügen und diese nutzen, um einzelne Dateien oder ganze Verzeichnisse einer Festplatte zu verschlüsseln, so dass der eigentliche Nutzer auf diese Daten nicht mehr zugreifen kann. Dieser wird aufgefordert ein Lösegeld (‚ransom') zu zahlen, damit die Daten wieder entschlüsselt werden. Der entsprechende Geldbetrag ist in der Regel über ein Online-Zahlsystem oder über Bitcoins bzw. eine andere Kryptowährung zu zahlen, damit die Nachverfolgung der Zahlung erschwert wird. In einigen Fällen wurden die verschlüsselten Daten auch nach Zahlung des Lösegelds nicht wieder entschlüsselt.

Der beste Schutz gegen Malware, neben einer erhöht Aufmerksamkeit, ist das regemäßige Aktualisieren der eigenen Geräte. Patches für das Betriebssystem und Updates für Apps und Software sollten zeitnah eingespielt werden, um bekannte Sicherheitslücken schließen zu können. Außerdem sollten die Malware-Tabellen und die eigentliche Software der Antivirenprogramme regelmäßig (idealerweise automatisch) aktualisiert werden. Dies gilt insbesondere vor dem Hintergrund des permanenten Wettbewerbs zwischen Angreifern und Herstellern. Bisher unbekannte Sicherheitslücken (sogenannte Zero-Day Exploits) werden von Angreifern genutzt, zeitgleich versuchen die Hersteller, diese zu schließen. Der Anwender muss hierbei schnell reagieren, um die Updates einzuspielen, bevor diese Lücken ausgenutzt werden können.

Merke

Ein aktuelles Antiviren-Programm ist auf jedem Computer Pflicht, da Malware ständig weiterentwickelt wird und sich schnell verbreitet. Ebenso sollte jedes andere Gerät (u. a. Router, Laptops, Smartphones und Tablets) durch eine Firewall und Virenschutz geschützt werden. Geeignete Sicherheitseinstellungen sind auch für alle übrigen internetfähigen Endgeräte erforderlich (z. B. Kameras, Drohnen, Roboter).

Online-Campus

Eine Onlinevorlesung hierzu findest Du in Deinem Online-Campus.