Schulungseinheiten zum Schutz Ihrer Benutzerkonten

Die folgenden Schulungseinheiten wurden innerhalb des vom **Bundesministerium für Wirtschaft und Energie** im Rahmen der **Initiative IT-Sicherheit in der Wirtschaft** geförderten Projekts **KMU Aware** entwickelt.

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

IT-Sicherheit
IN DER WIRTSCHAFT

KMU AWARE
AWARENESS IM MITTELSTAND

Inhalt dieser Schulung

Diese Schulung besteht aus zwei Modulen:

1. **Angriffe auf Benutzerkonten:**

   In diesem Modul wird erklärt, wie Angreifer Zugriff auf Ihre Benutzerkonten im Internet und an Ihren Geräten erlangen können und was Sie dagegen unternehmen können

2. **Technologien im Kontext Ihrer Benutzerkonten**

   In diesem Modul wird erklärt auf welche Technologien Sie beim Schutz Ihrer Benutzerkonten treffen können

Hinweis: Bitte beachten Sie, dass mache pdf-Betrachter (z.B. Apple Preview) die Links zu Webseiten mit weiteren Informationen nicht korrekt verarbeiten. Sollte Ihr pdf-Betrachter davon betroffen sein und Sie die Seiten besuchen wollen, markieren Sie bitte die Links im Dokument und kopieren Sie diese manuell in Ihren Browser.

Modul 1

Angriffe auf Benutzerkonten

In diesem Modul wird erklärt, wie Angreifer Zugriff auf Ihre Benutzerkonten im Internet und an Ihren Geräten erlangen können und was Sie dagegen unternehmen können.

Aufbau dieses Moduls

Dieses Modul erklärt Ihnen in drei aufeinanderfolgenden Teilen, wie Sie Ihre Benutzerkonten (z.B. bei Webdiensten, am PC, am Smartphone, etc.) vor Angriffen schützen können:

1. Wer mögliche Angreifer sind, die auf Ihre Benutzerkonten Zugriff erhalten möchten, und an welchen Stellen diese ansetzen können
2. Welche Konsequenzen eintreten können, wenn jemand Zugriff auf Ihre Benutzerkonten erhält
3. Welche Angriffe genutzt werden können, um Zugriff auf Ihre Benutzerkonten zu erhalten

Im Zuge der Schulung werden auch 25 weit verbreitete Missverständnisse in Bezug auf Passwörter aufgeklärt. Diese sind farblich in blau hervorgehoben und mit dem folgenden Symbol gekennzeichnet:

Teil 1:

Wer mögliche Angreifer sind, die auf Ihre Benutzerkonten Zugriff erhalten möchten, und an welchen Stellen diese ansetzen können

Wer Sie angreift

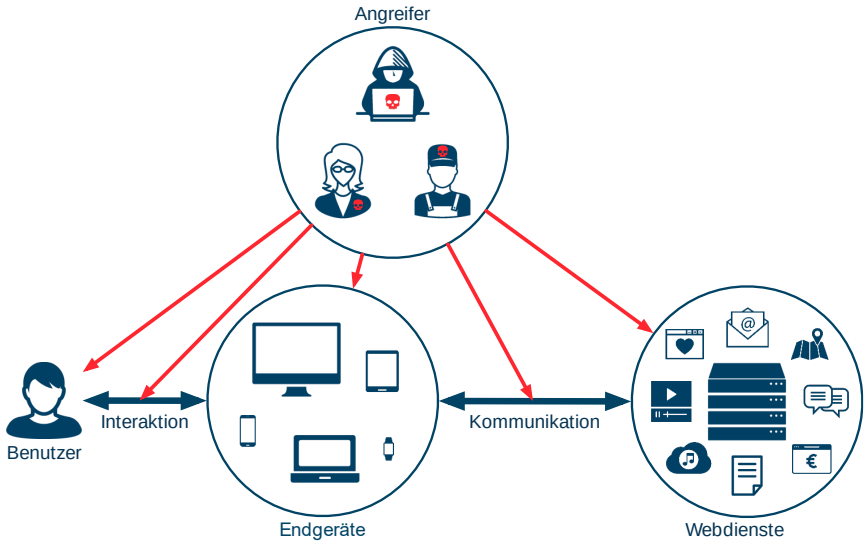
Angreifer ist jeder, vor dem Sie sich schützen möchten oder müssen:

- Ein krimineller Hacker der z.B. Ihr Bankkonto plündern möchte.
- Eine Person, die sich z.B. als Mitarbeiter einer anderen Firma ausgibt, um Zutritt zu Ihrem Büro zu erhalten.
- Ein Arbeitskollege, der z.B. möchte, dass Änderungen an offiziellen Projektdokumenten nicht zu ihm zurückverfolgt werden können.
- Ein neugieriger Partner, der z.B. Zugriff auf Ihre Kommunikation mit anderen Personen erhalten möchte.
- Ein Mitarbeiter eines Cloud-Dienstes, der z.B. seine Position ausnutzt, um illegal Profit zu schlagen.

Missverständnis #1: Sie sollten nicht glauben, dass Angreifer nur kriminelle Hacker vom anderen Ende der Welt sein können. Genauso falsch ist es jedoch anzunehmen, dass nur Personen, die Sie kennen, versuchen werden Ihre Passwörter zu erraten. Angreifer können aus beiden Personengruppen stammen.

Wo angegriffen wird

Angreifer können an vielen Stellen ansetzen:



- Bei Ihnen selbst als Benutzer der Endgeräte
- Bei Ihrer Interaktion mit Ihren Endgeräten
- Bei Ihren Endgeräten
- Bei der Kommunikation zwischen Ihren Endgeräten und Webdiensten
- Bei den Webdiensten, die Sie verwenden

Missverständnis #2: Einige Menschen glauben, sie seien nicht wichtig genug, um überhaupt ins Visier eines Angreifers geraten zu können. Dies ist eine Fehleinschätzung, die schwerwiegende Folgen nach sich ziehen kann. Wie Sie im dritten Teil dieser Schulung sehen werden, gibt es Angriffe, die alle Benutzer eines Webdienstes betreffen. Geben Sie sich also nicht der Illusion hin, Sie seien nicht betroffen, und beschäftigen Sie sich mit Abwehrstrategien. Sonst werden Sie zum Opfer eines Angreifers.

Teil 2:

Welche Konsequenzen eintreten können, wenn jemand Zugriff auf Ihre Benutzerkonten erhält

Konsequenzen

Haben Angreifer Zugriff auf eines Ihrer Benutzerkonten, kann dies die verschiedensten Konsequenzen zur Folge haben.

- Angreifern geht es nicht vorrangig darum Zugriff auf Ihr Benutzerkonto zu erhalten.
- Angreifer sind interessiert an
  - den Daten, die in Ihren Benutzerkonten gespeichert sind (z.B. private Fotos).
  - den Aktionen, die mit Ihren Benutzerkonten ausgeführt werden können (z.B. Nachrichten an Freunde und Bekannte verschicken).
- Es ist wichtig sich klar zu machen, dass Angreifer jedes Ihrer Benutzerkonten, auf welches sie Zugriff erlangen, für eigene Zwecke nutzen können.
- Auf der nächsten Seite finden Sie eine Übersicht, die Ihnen als Anhaltspunkt dienen kann, wie Angreifer Schaden anrichten können.

Missverständnis #3: Der Sicherheitsbedarf Ihrer Benutzerkonten hängt nicht davon ab, wie häufig Sie diese verwenden. Es hängt einzig von den darin zugänglichen Daten und Aktionen, die damit ausgeführt werden können, ab.

Missverständnis #4: Für die Sicherheit Ihrer Benutzerkonten und Endgeräte sind auch im Arbeitsumfeld Sie und nicht alleine die IT-Abteilung zuständig.

Beispiele für Konsequenzen

Aktionen		Mögliche Konsequenzen die durch einen erfolgreichen Angriff entstehen können (z.B.)
Was Sie mit Ihren Benutzerkonten tun	**Was der Angreifer mit Ihren Benutzerkonten tun kann (z.B.)**	
E-Mails versenden / Nachrichten in sozialen Netzwerken posten	• Betrügerische Nachrichten in Ihrem Namen an Freunde und Bekannte schicken • Spam versenden • Private/sensible Informationen (z.B. Fotos) öffentlich posten • Diffamierung durch Nachrichten, die in Ihrem Namen gepostet werden	• Familie und Freunde fallen auf betrügerische Links herein oder installieren Schadsoftware, da sie denen in Ihrem Namen verschickten Nachrichten vertrauen • Verlust von Ansehen/Vertrauen bei Kollegen, Freunden und Familie • Das Benutzerkonto wird wegen Verstößen gegen die Nutzungsrichtlinien gesperrt
Auf den Cloud-Speicher zugreifen	• Private/sensible Informationen mitlesen oder kopieren • Daten im Cloud-Speicher manipulieren oder löschen	• Erpressung mit der Drohung private Daten zu veröffentlichen • Verlust der Daten im Cloud-Speicher • Ihnen kann Schadsoftware (in andere Dateien integriert) untergeschoben werden
Zugriff auf Bank-Daten	• Einsehen von Zahlungs- und Bankdaten	• Bezahlen von Waren oder Dienstleistungen über das Konto • Abziehen aller Geldreserven bis zum Limit des Dispo-Kredites • Privatsphäre-Verletzungen durch Einsehen der Transaktionen • Erpressung durch Drohung von Veröffentlichung der Finanzsituation

Missverständnis #5: Geld ist nicht die einzige Wertsache, die mit Ihrem Bankkonto verbunden ist. Über das Online-Banking kann ein Angreifer häufig auch einsehen, wo Sie einkaufen, wann Sie Ihren Urlaub buchen, wann und was Sie im Ausland bezahlen, Ihre Adresse, Ihre Telefonnummer … Dazu braucht er nur das Passwort und keine TANs.

Teil 3:

Welche Angriffe genutzt werden können, um Zugriff auf Ihre Benutzerkonten zu erhalten

Überblick

Im Folgenden werden Ihnen die Angriffe vorgestellt, die von Angreifern genutzt werden:

- Angriffe, die bei Ihnen oder bei der Interaktion mit Ihren Geräten ansetzen
  - Angriff (1/11): „Gefährliche Nachricht“
  - Angriff (2/11): „Unsicher aufbewahrte Notiz“
  - Angriff (3/11): „Über die Schulter blicken“
- Angriffe, die bei Ihren Endgeräten ansetzen
  - Angriff (4/11): „Endgerät kompromittieren“
- Angriffe, die bei der Kommunikation Ihrer Endgeräte mit Webdiensten ansetzen
  - Angriff (5/11): „Unverschlüsselte Kommunikation abhören“
  - Angriff (6/11): „Verschlüsselte Kommunikation abhören“
- Angriffe, die sowohl bei Ihren Endgeräten als auch bei Webdiensten ansetzen
  - Angriff (7/11): „Gezieltes Raten“
  - Angriff (8/11): „Ungezieltes Raten“
  - Angriff (9/11): „Raten nach Einbruch ins System“
  - Angriff (10/11): „Unverschlüsselte elektronische Notiz“
- Angriffe, die bei Webdiensten ansetzen
  - Angriff (11/11): „Schwachen Reset-Mechanismus ausnutzen“

Einleitung

Es wird jeweils zunächst der Angriff vorgestellt und dann erklärt, wie Sie den Angriff abwehren können. Zu manchen Angriffen erhalten Sie weitere Hinweise, welche über die einfache Abwehr des Angriffes hinausgehen. Damit Sie immer den Überblick behalten, sind die drei Arten von Information jeweils durch entsprechende Symbole gekennzeichnet:

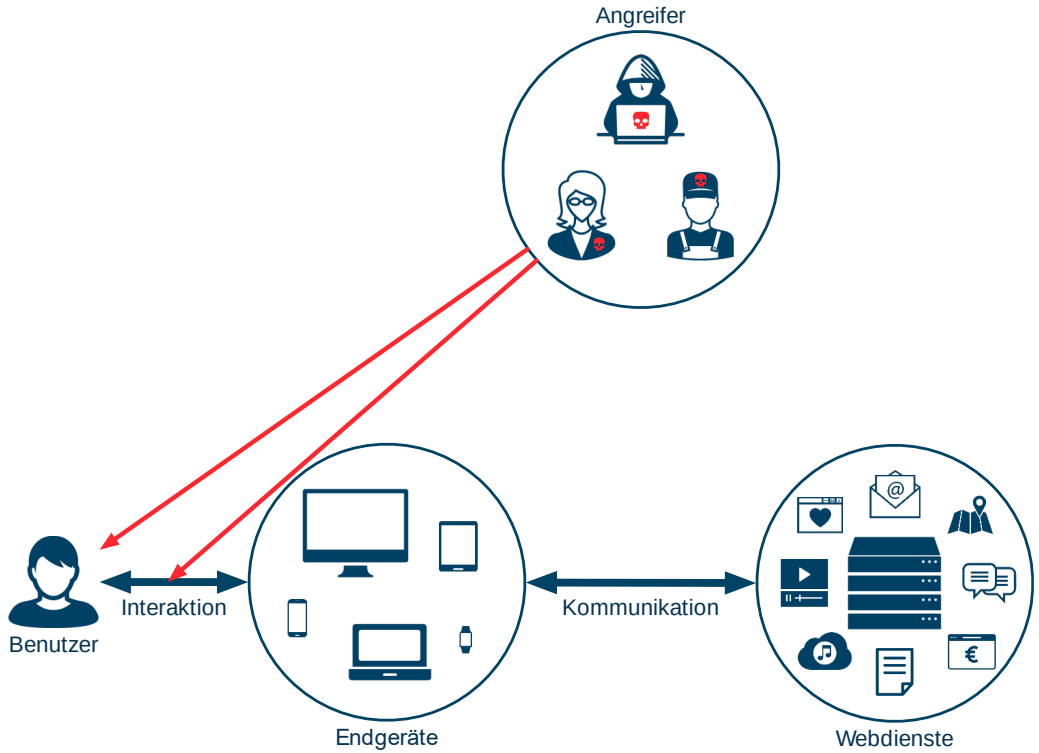
 Beschreibung der Angriffsstrategie

 Beschreibung der Abwehrstrategie

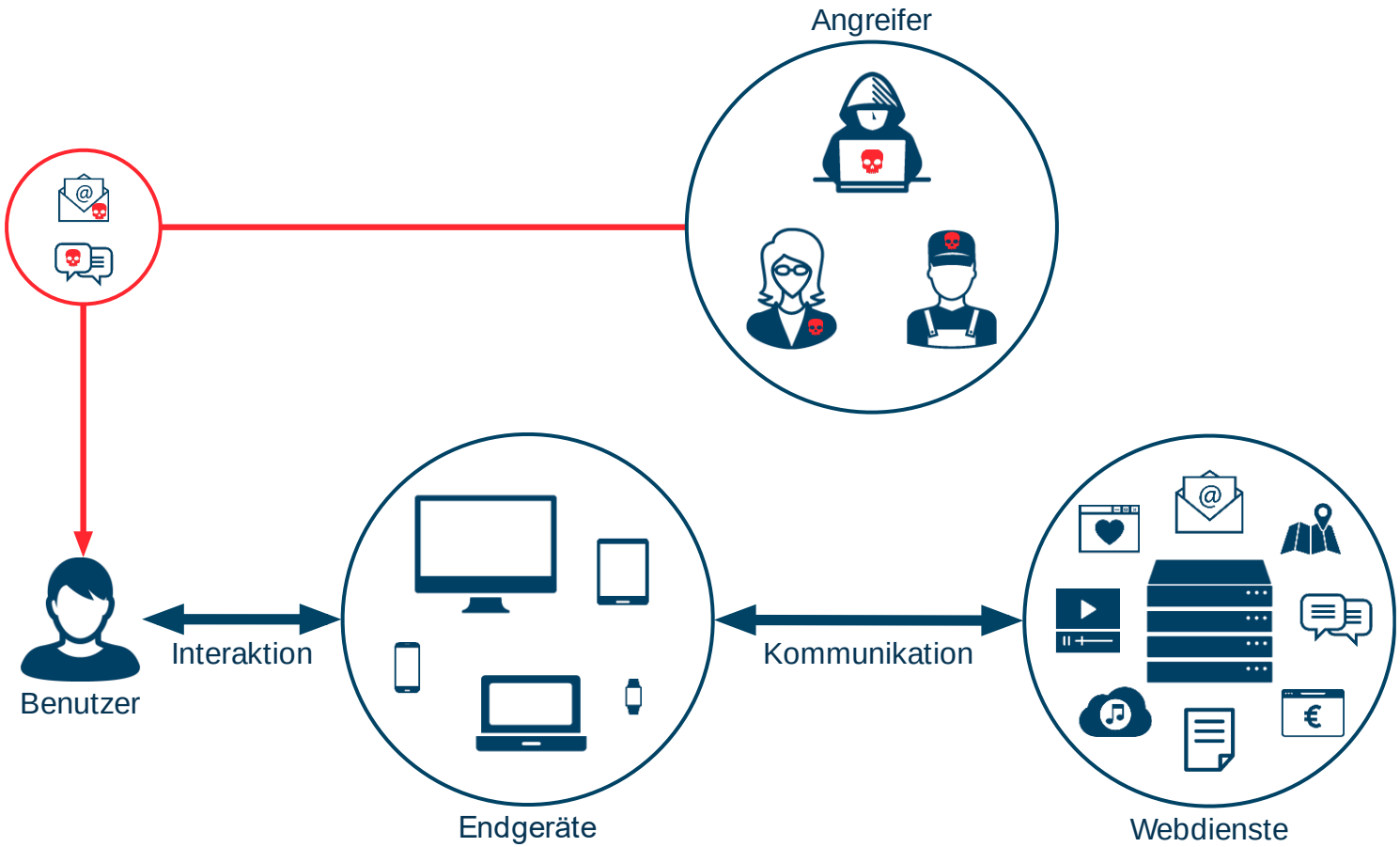
 Weitere Hinweise

Angriffe, die bei Ihnen und Ihrer Interaktion mit Endgeräten ansetzen

Zunächst werden Ihnen die Angriffe vorgestellt, bei denen der Angreifer versucht über Sie als Benutzer oder Ihre Interaktion mit Ihren Endgeräten Zugriff auf Ihre Benutzerkonten zu erhalten.



Angriff (1/11): „Gefährliche Nachricht“



Beschreibung des Angriffs „Gefährliche Nachricht“

Der Angreifer versucht über eine gefährliche Nachricht (z.B. Phishing E-Mail oder auch Anruf eines vorgeblichen Service-Mitarbeiters)

- entweder Sie dazu zu bewegen ihm die gewünschten Daten direkt zuzusenden (z.B. Benutzername und das zugehörige Passwort),
- oder Sie dazu zu bewegen auf einen gefährlichen Link zu klicken (der auf eine betrügerische Webseite führt, die der Angreifer kontrolliert und auf der er alle Ihre Handlungen und alle eingegebenen Daten beobachten kann).

Schon das Klicken auf einen gefährlichen Link kann problematisch sein, da schon der Besuch einer gefährlichen Webseite zu einer Infektion Ihres Endgerätes führen kann, ohne dass Sie dort etwas herunterladen oder anklicken müssen.

Abwehr des Angriffs „Gefährliche Nachricht“

Hier kurz und knapp die wichtigsten Tipps zu Erkennung und Umgang mit gefährlichen Nachrichten:

- Sollten Sie eine gefährliche Nachricht als solche erkannt haben, dann sollten Sie diese direkt löschen.
- Prüfen Sie Absender und Inhalt jeder empfangenen Nachricht auf Plausibilität.
- Prüfen Sie, welche Webadresse tatsächlich hinter einem Link in der Mail steckt, und prüfen Sie, ob der Link einen Bezug zu dem (vermeintlichen) Absender und/oder dem Inhalt der Nachricht hat.
- Prüfen Sie Anhänge an E-Mails hinsichtlich Ihrer Gefährlichkeit.
- Detaillierte Informationen zu den vorgenannten Schritten erhalten Sie in der Schulung[1] zum Thema „gefährliche Nachrichten“.

Weitere Informationen zum Vorgehen der Betrüger, der Erkennung betrügerischer Nachrichten und dem Umgang mit solchen Nachrichten, erfahren Sie in unserer entsprechenden Schulung[1].

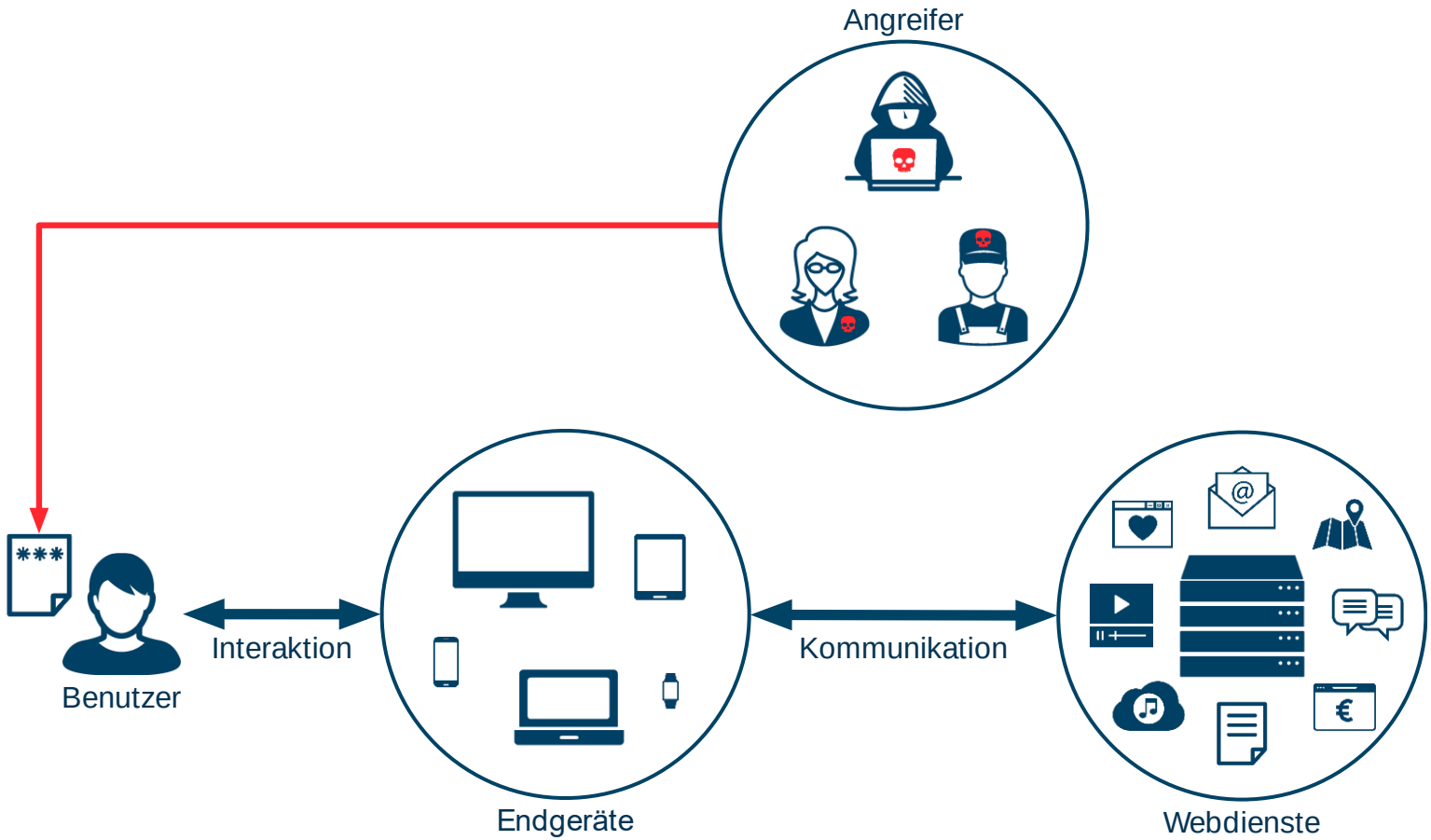
[1] https://www.secuso.org/schulung

Weitere Hinweise zum Angriff „Gefährliche Nachricht“

Es gibt ein Video, welches die Problematik von verschlüsselten Verbindungen noch einmal anschaulich erklärt:

https://www.youtube.com/watch?v=4xIU1lPJs_4

Angriff (2/11): „Unsicher aufbewahrte Notiz entwenden“



Beschreibung des Angriffs „Unsicher aufbewahrte Notiz entwenden“

Der Angreifer nutzt aus, wenn Passwörter auf einen Zettel oder in ein Notizbuch aufgeschrieben werden (physische Aufzeichnungen).

- Werden diese Aufzeichnungen nicht sicher verwahrt, kann ein Angreifer sie entwenden oder kopieren.
- Wird eine Aufzeichnung z.B. auf dem Schreibtisch im Unternehmen (oder unter der Tastatur oder gar am Monitor) aufbewahrt, ist es ein Leichtes für einen Angreifer sich z.B. als Reinigungskraft auszugeben und sich früh morgens oder spät abends Zugang zum Büro zu verschaffen, um die Aufzeichnung zu stehlen oder kopieren.
- Wird ein Passwort im privaten Umfeld aufgeschrieben und in der eigenen Wohnung verwahrt und es schützt private Daten (z.B. private Photos in der Cloud oder Bankdaten) kann es eine nützliche Überlegung sein, sie wie ähnlich wertvolle Sachgegenstände (z.B. Photoalben oder Kontoauszüge) zu verwahren.

Abwehr des Angriffs „Unsicher aufbewahrte Notiz entwenden“

Der Angriff kann durch einfache Maßnahmen abgewehrt werden

- Physische Aufzeichnungen zu Passwörtern müssen Sie stets so sicher verwahren, dass nur Sie selbst Zugriff darauf haben (z.B. auch wenn sie den Arbeitsplatz kurz verlassen, um etwas zu kopieren).
- Insbesondere ist eine sicher verwahrte Notiz dem Wiederverwenden von Passwörtern bei verschiedenen Benutzerkonten vorzuziehen.
- Eine gute Alternative zu physischen Aufzeichnungen von Passwörtern ist die Nutzung eines Passwortmanagers[2].

Missverständnis #6: Wird die Notiz sicher verwahrt, kann das Aufschreiben von Passwörtern sogar eine gute Sache sein (z.B. nach einem Wechsel des Passwortes, bis Sie es oft genug eingegeben haben, um es sich zu merken). Allerdings sollten Sie die Notiz dann vernichten, sobald Sie sich das Passwort merken können. Halten Sie sich daran, ist dies ein deutlich sichereres Vorgehen als Passwörter wiederzuverwenden: Wählen Sie ein angemessen sicheres Passwort, ist es viel schwerer für den Angreifer ein neues Passwort zu erraten als eines, das evtl. an anderer Stelle abhandengekommen sein könnte.

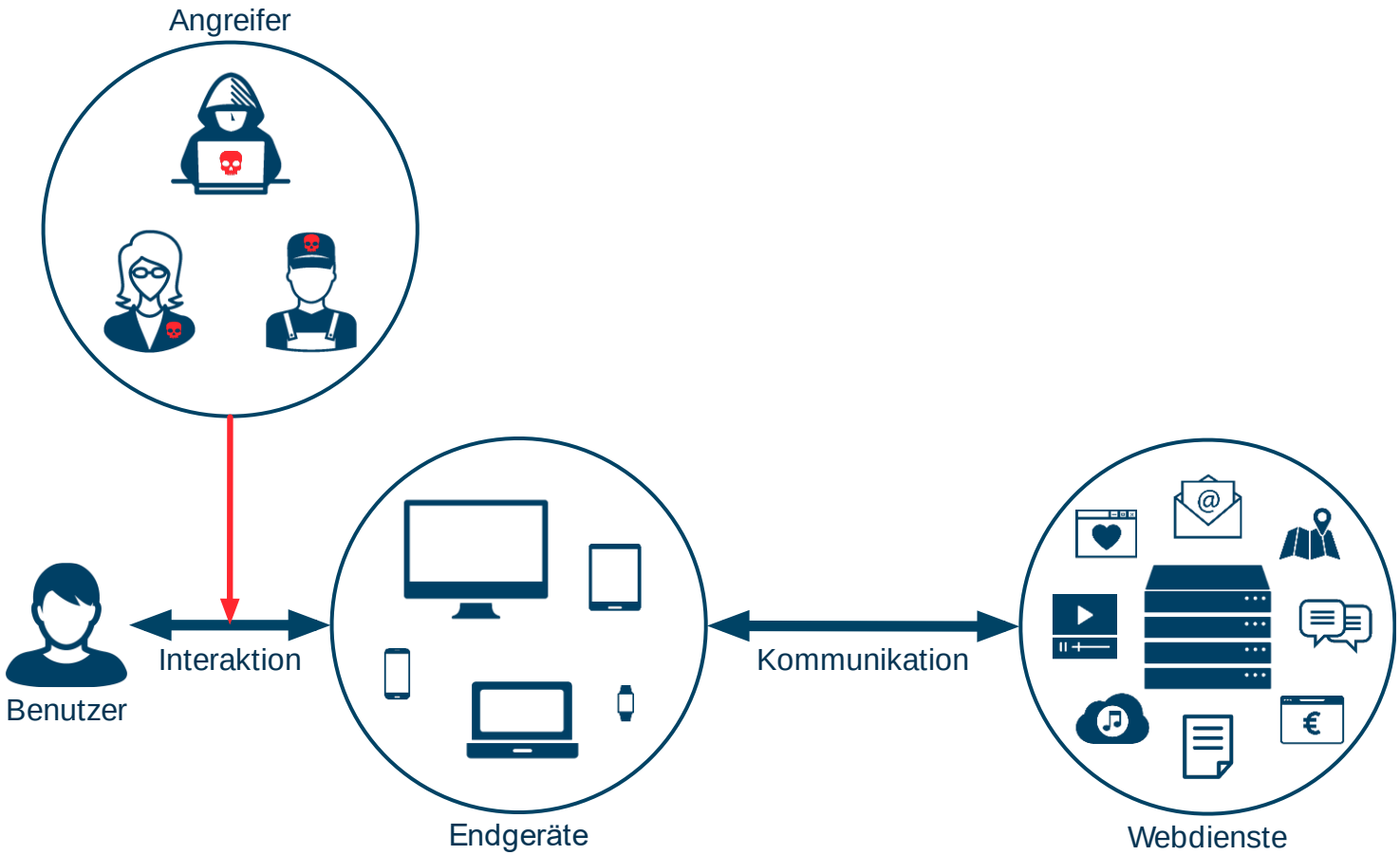
[2] Nähere Informationen hierzu erhalten Sie im zweiten Modul dieser Passwort-Schulung.

Weitere Hinweise zum Angriff „Unsicher aufbewahrte Notiz entwenden“

Seien Sie vorsichtig, wenn Sie Passwörter bereits als Notiz erhalten (z.B. Brief mit Online-Banking-Passwort).

- Angreifer können sogar schon zuschlagen, solange der Brief noch unterwegs ist (also bevor Sie Gelegenheit hatten den Brief sicher zu verwahren).
- Achten Sie darauf, ob Briefe mit Passwörtern unversehrt bei Ihnen angekommen sind.
- Kommt ein solcher Brief geöffnet oder beschädigt bei Ihnen an, sollten Sie
  - das Passwort nicht verwenden,
  - direkt den Absender kontaktieren, ihn darüber informieren und ein neues Passwort anfordern.

Angriff (3/11): „Über die Schulter blicken“



Beschreibung des Angriffs „Über die Schulter blicken“

Der Angreifer versucht den Benutzer bei der Passworteingabe zu beobachten, um eines seiner Passwörter zu erspähen. Fachbegriff: Shoulder-Surfing (über die Schulter blicken).

- Der Angreifer positioniert sich so, dass er alle Aktionen des Benutzers während der Eingabe des Passwortes beobachten kann (z.B. Fingerbewegungen oder Eingaben).
- Der Angreifer kann auf technische Hilfsmittel zurückgreifen, um
  - den Vorgang zu filmen,
  - Tastendrücke durch Wärmebilder oder Spuren auf Touchscreens im Nachhinein nachzuvollziehen.
- Passwörter können oftmals mit nur einer einzigen Beobachtung rekonstruiert werden. Dies gilt auch für alternative Passwort-Verfahren (z.B. die Android-Gesten-Sperre) und an Tastenfeldern (z.B. von Geldautomaten oder Alarmanlagen).
- Bei Smartphones und Tablets ist es zudem üblich, dass der zuletzt eingegebene Buchstabe eines Passwortes kurz im Klartext sichtbar ist. Dies macht eine direkte Beobachtung besonders einfach.
- Bei Touchscreens hinterlassen die Finger bei der Eingabe schmierige Abdrücke. Auch diese könnten genutzt werden, um Ihre Eingabe zu rekonstruieren.

Abwehr des Angriffs „Über die Schulter blicken“

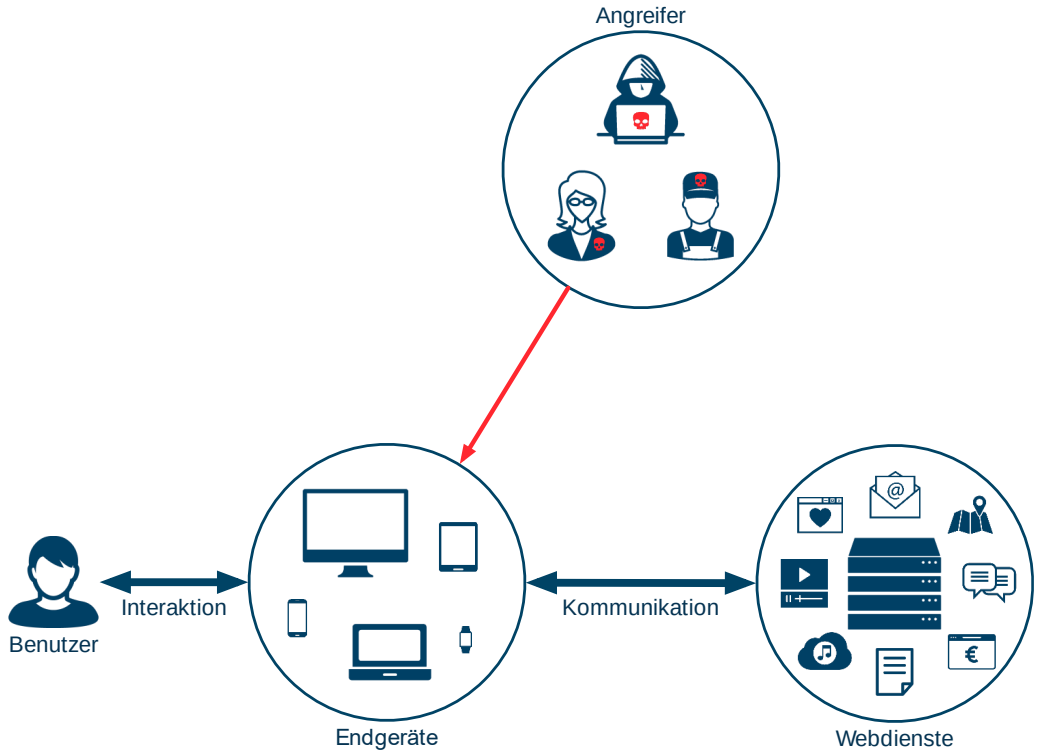
Um sich vor Shoulder-Surfing zu schützen, sollten Sie immer wissen, ob sich gerade jemand in Ihrer Umgebung aufhält, wenn Sie ein Passwort eingeben.

- Aus sozialem Druck kann es dazu kommen, dass Sie überlegen Ihr Passwort in Gegenwart einer Person einzugeben, die es nicht erfahren soll (z.B. ein Arbeitskollege, wenn im Team gearbeitet wird, oder ein Service-Mitarbeiter, wenn der Laptop oder das Smartphone zur Reparatur muss). Haben Sie keine Scheu die Person zu bitten kurz wegzuschauen.
- Seien Sie in öffentlichen Räumen besonders vorsichtig (z.B. in der Bahn oder am Flughafen).
- Haben Sie das Gefühl beobachtet zu werden, reicht es oft aus, den Körper so zu platzieren, dass der Bildschirm des Gerätes nicht einzusehen ist. Aber Achtung: Einfaches Wegdrehen des Gerätes ist wenig effektiv, um z.B. PINs während der Eingabe zu schützen.
- Die Display-Helligkeit während der Passworteingabe herunterzuregeln und das Aufbringen einer speziellen Sichtschutzfolie[3] auf dem Display können das Risiko zu verringern.
- Touchscreens sollten Sie diesen regelmäßig von schmierigen Abdrücken reinigen.
- Die Nutzung eines Passwortmanagers[3] kann das Risiko verringern.

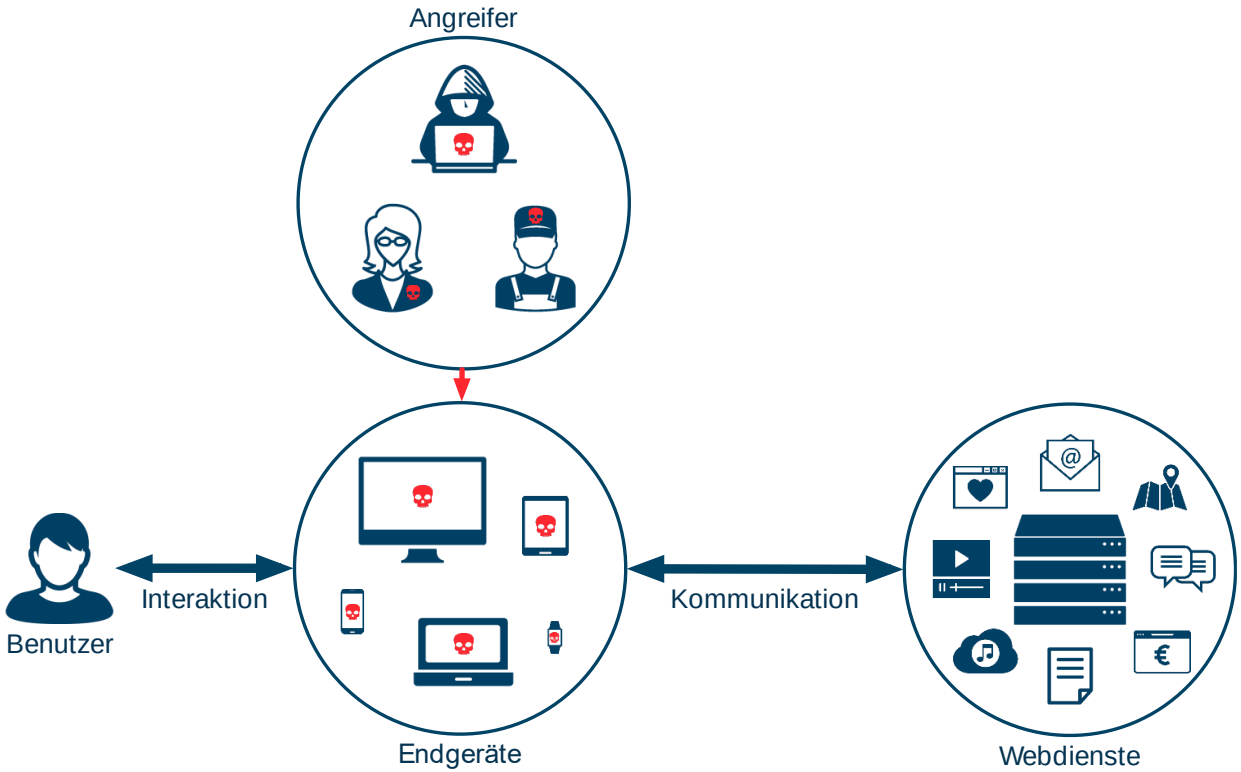
[3] Nähere Informationen hierzu erhalten Sie im zweiten Modul dieser Passwort-Schulung.

Angriffe, die bei Ihren Endgeräten ansetzen

Im Folgenden werden Ihnen die Angriffe vorgestellt, bei denen der Angreifer versucht ausschließlich über Ihre Endgeräte Zugriff auf Ihre Benutzerkonten zu erhalten.



Angriff (4/11): „Endgerät kompromittieren“



Beschreibung des Angriffs „Endgerät kompromittieren“

Der Angreifer versucht eines Ihrer Endgeräte (z.B. Laptop, Desktop-Rechner, Smartphone, Tablet, etc.) mit Schadsoftware (z.B. Virus) zu infizieren.

- Dadurch erhält der Angreifer Zugriff auf alle Ihre Passwörter.
- Wenn erfolgreich, ist es einer der verheerendsten Angriffe.
- Der Angreifer muss die Schadsoftware
  - entweder selbst installieren (z.B. indem er Zugriff auf Ihr ungesperrtes Endgerät erhält, wenn Sie es unbeaufsichtigt lassen),
  - oder Sie hereinlegen, damit Sie diese installieren (z.B. im Zuge eines automatisierten Angriffes beim Besuchen einer infizierten Webseite).
- Seien Sie auch bei mobilen Endgeräten vorsichtig. Immer wieder schleusen Angreifer verschiedene Arten von Schadsoftware in die Stores der Hersteller (Apple, Google, etc.) ein und versuchen Ihre Daten zu stehlen oder Kosten zu erzeugen.

Abwehr des Angriffs „Endgerät kompromittieren“

Ein kompromittiertes Endgerät ist nicht nur eine Gefahr für Ihre Passwörter, sondern für alle Daten auf Ihrem Endgerät. Mit den folgenden Regeln können Sie die Wahrscheinlichkeit eines erfolgreichen Angriffs „Endgerät kompromittieren“ auf ein Minimum reduzieren:

- Installieren Sie stets Updates für jede Software und das Betriebssystem.
- Installieren Sie soweit vorhanden auf Desktop-PCs und Laptops Anti-Viren Software und aktualisieren Sie diese stets. Je nachdem, welches Betriebssystem Ihre mobilen Geräte verwenden, kann auch dort Anti-Viren-Software installiert werden.

Missverständnis #7: Updates der Software und des Betriebssystems sind einer der Grundpfeiler zum Schutz Ihrer Endgeräte. Diese Updates stopfen Sicherheits-Löcher. Bleiben diese Sicherheits-Löcher offen (z.B. weil Updates nicht zeitnah eingespielt werden), können Angreifer durch diese eindringen und Ihr Endgerät übernehmen. Am einfachsten ist es, wenn Sie die automatische Installation von Updates aktivieren. So müssen Sie sich nicht selbst darum kümmern, ob Updates verfügbar sind.

Abwehr des Angriffs „Endgerät kompromittieren“ - *Fortsetzung*

- Sichern Sie alle Ihre Endgeräte (Smartphone, PC, etc.) mit einer Passwort-Sperre (oder vergleichbarem, z.B. Fingerabdrucksensor), geben Sie dieses Passwort nicht weiter und lassen Sie Endgeräte nur in gesperrtem Zustand unbeaufsichtigt. Mobile Geräte sollten Sie nur im Notfall unbeaufsichtigt lassen, da manche Aktionen auch ohne ein Entsperren möglich sind (z.B. Anruf entgegennehmen, der einen Einmal-Code durchgibt).
- Verschlüsseln Sie die Festplatte Ihrer Laptops/PCs. Dazu ist heutzutage meist nur ein Klick auf den richtigen Knopf nötig. Andernfalls kann ein Angreifer mit physischem Zugriff auf Ihr Endgerät dessen Festplatte ausbauen und die Daten direkt auslesen.

Missverständnis #8: Die SIM-PIN müssen Sie eingeben, um die Telefoniefunktion Ihres Handys freizuschalten. Diese PIN reicht nicht für die Sicherung eines Smartphones aus, da die SIM-Karte entnommen und so die Abfrage der SIM-PIN umgangen werden kann. Eine SIM-PIN schützt nur Ihre Telefonrechnung, nicht die Daten auf Ihrem Telefon.

Missverständnis #9: Sie sollten jedes Endgerät sperren, wenn Sie es unbeaufsichtigt lassen – selbst dann, wenn andere Mitarbeiter im gleichen Büro bzw. Freunde/Bekannte im gleichen Raum sind. Wenn diese in Ihrer Abwesenheit auch kurz den Arbeitsplatz verlassen (z.B. Toilette, Kaffee holen, „kurz mal telefonieren“, etc.) kann Ihr Endgerät vollkommen ungeschützt sein.

Abwehr des Angriffs „Endgerät kompromittieren“ - *Fortsetzung*

- Stecken Sie keine USB-Sticks (oder andere externen Speichermedien) aus unbekannten oder bekannten nicht-vertrauenswürdigen Quellen in Ihre Endgeräte (z.B. auf dem Weg zur Arbeit gefunden). Diese können automatisiert Schadsoftware installieren.
- Installieren Sie keine Software aus unbekannten oder bekannten nicht-vertrauenswürdigen Quellen, wie z.B. Download von dubiosen Webseiten, Anhänge aus betrügerischen Nachrichten oder Installation von Apps außerhalb der Stores ihres Mobilgerätes (Google Play Store, iOS App Store, Amazon App Shop, etc.). Weitere Informationen zur Erkennung betrügerischer Nachrichten mit gefährlichen Anhängen können Sie in unserer entsprechenden Schulung unter https://secuso.org/schulung finden.
- Soweit vorhanden, sollten Sie Android-Geräte nicht „rooten“ und iOS- sowie Windows Phone/Mobile-Geräte nicht „jailbreaken“. Zusätzliche Informationen hierzu finden Sie in den weiteren Hinweisen.

Weitere Hinweise zum Angriff „Endgerät kompromittieren“

Manche Anleitungen im Internet empfehlen das eigene Android-Gerät zu „rooten“ (z.B. um vorinstallierte Apps zu löschen, die Sie nicht nutzen). Dies ist nicht zu empfehlen:

- Manche Hersteller bieten Möglichkeiten das eigene Telefon sehr einfach zu „rooten“, bei anderen Herstellern ist dies nicht vorgesehen.
- Dabei werden Schutzmechanismen des Telefons deaktiviert, um tiefgreifende Änderungen am System des Telefons durchzuführen.
- Dabei entsteht ein Sicherheitsrisiko: Das Abschalten der Schutzmaßnahmen ermöglicht ungewünschte Nebenwirkungen, z.B. dass Apps auf Daten anderer Apps zugreifen können. Daher verweigern einige Banking-Apps auf gerooteten Geräten komplett den Dienst.
- Ohne diese Schutzmechanismen kann Malware Ihr Endgerät einfacher befallen.
- Ein weiterer Fall in dem das Smartphone gerootet wird, ist wenn der Hersteller keine Updates mehr für das Telefon anbietet. Mit alternativen Android-Varianten kann ein Update trotzdem möglich sein. Diese Alternativen sind häufig von Hause aus gerootet. Mittlerweile gibt es jedoch ungerootete Alternativen.

Weitere Hinweise zum Angriff „Endgerät kompromittieren“ - *Fortsetzung*

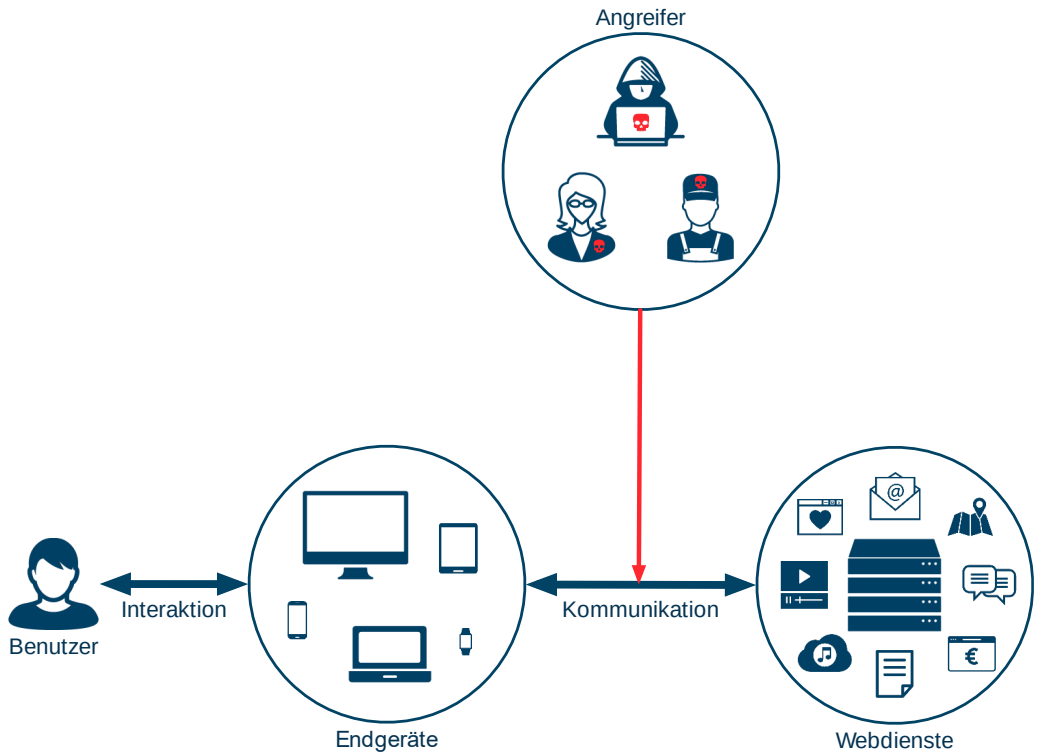
Ähnliche Anleitungen gibt es für iOS und Windows Phone/Mobile. Auf diesen Plattformen spricht man von einem sogenannten „Jailbreak“. Auch beim Jailbreak ist das Ziel Funktionalität freizuschalten, die vom Hersteller nicht vorgesehen ist. Doch auch dies ist nicht zu empfehlen:

- Bei iOS (also auf iPhones aber auch iPods/iPads) und Windows Phone/Mobile ist die Entfernung der Schutzmechanismen grundsätzlich nicht vorgesehen.
- Im Internet kursieren Anleitungen für sogenannte „Jailbreaks“ (engl: Gefängnisausbruch).
- So kann aus den Schutzmaßnahmen ausgebrochen werden, indem Schwachstellen im Betriebssystem des Telefons ausgenutzt werden.
- Jailbreaks funktionieren im Grunde wie Schadsoftware und nehmen dieser den Job ab, die Schutzmechanismen Ihrer Geräte auszuhebeln.
- Trotz unterschiedlicher Begriffe sind die Konsequenzen die gleichen wie beim „rooten“: Das Deaktivieren der Schutzmechanismen erlaubt tiefgreifende Eingriffe ins System des Geräts durch den Benutzer, eröffnet aber auch Angreifern zusätzliche Möglichkeiten.

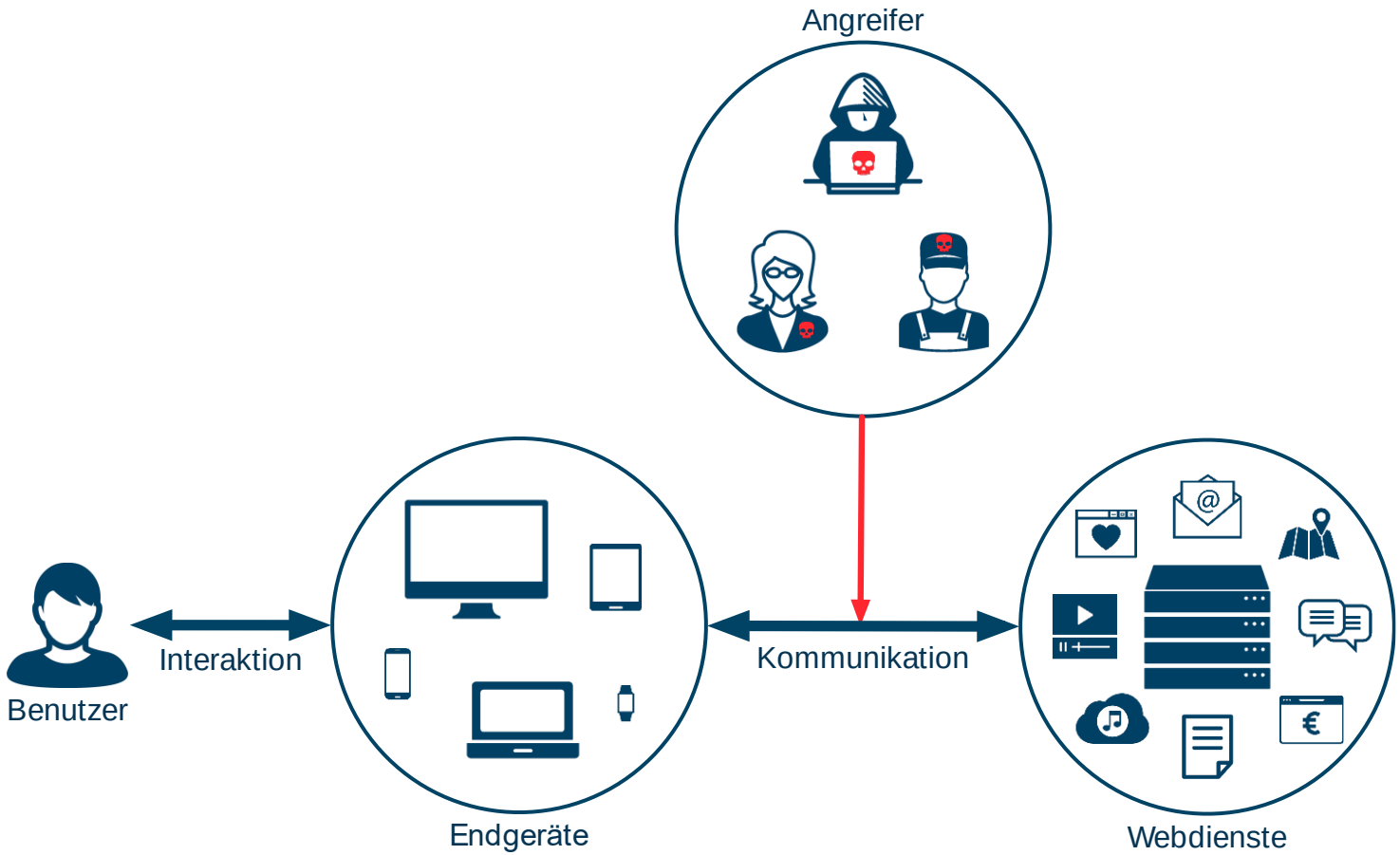
Bei Gebrauchtgeräten kann es nützlich sein sich diesbezüglich beim Vorbesitzer zu erkundigen.

Angriffe, die bei der Kommunikation Ihrer Endgeräte mit Webdiensten ansetzen

Im Folgenden werden Ihnen die Angriffe vorgestellt, bei denen der Angreifer versucht bei der Kommunikation Ihrer Endgeräte mit Webdiensten anzusetzen, um Zugriff auf Ihre Benutzerkonten zu erhalten.



Angriff (5/11): „Unverschlüsselte Kommunikation abhören“



Beschreibung des Angriffs „Unverschlüsselte Kommunikation abhören“

Der Angreifer versucht sich in die Kommunikation zwischen Ihrem Endgerät und dem Webdienst einzuklinken und Ihre Passwörter (oder andere sensible Informationen) mitzuschneiden.

- Besonders kritisch sind unverschlüsselte Verbindungen in ungesicherten WLANs (z.B. in Cafés oder Hotels). Dabei wird das Passwort unverschlüsselt vom Endgerät drahtlos versendet und jeder in der Umgebung (auch ein Angreifer, der gar nicht mit dem WLAN verbunden ist) kann diese Information ohne Probleme mitschneiden.
- Problematisch kann dabei z.B. auch schon die „Anmeldung“ an ein ungesichertes WLAN sein, wenn diese über eine Webseite (ein sogenanntes Captive Portal) unverschlüsselt erfolgt (d.h. keine HTTPS-Verbindung).
- Verschlüsselte Verbindungen können hingegen selbst in offenen WLANs nicht abgehört werden.

Beschreibung des Angriffs „Unverschlüsselte Kommunikation abhören“ - *Fortsetzung*

- Leider können nicht nur Ihre Passwörter abhandenkommen, sondern auch sogenannte „sekundäre Login-Informationen“ (z.B. Cookies). Sie wird vom Webdienst benötigt, um Sie wiederzuerkennen und festzustellen, ob Sie eingeloggt sind. Dies passiert vollautomatisch im Hintergrund. Sie bekommen davon nichts mit. Geraten sekundäre Login-Informationen in die Hände eines Angreifers, kann er dem Server vortäuschen eingeloggt zu sein.

Missverständnis #10: Diese Angriffe mögen sich kompliziert anhören, können jedoch sehr einfach mit Spezialsoftware automatisiert werden (z.B. um alle Benutzer in einem ungesicherten WLAN automatisiert anzugreifen).

Abwehr des Angriffs „Unverschlüsselte Kommunikation abhören“

Um zu verhindern, dass sich ein Angreifer in die Kommunikation einklinken kann, sollte diese stets verschlüsselt sein.

- Eine verschlüsselte Verbindung erkennen Sie bei Webdiensten im Browser daran, dass der Webadresse ein **https://** vorangestellt ist.
- Dies wird in den meisten Browsern auch farblich und mit Symbolen dargestellt. Daher sollten Sie, wann immer dies möglich ist (einige Webseiten bieten leider keine Kommunikation per https an), auf eine sichere Verbindung wechseln, indem sie das http in der Adresszeile des Browsers durch ein https ersetzen.
- Sekundäre Login-Information ist nur bis zu Ihrem nächsten Logout gültig und daher kann ein Angriff darauf nur in dem Zeitfenster zwischen Login und Logout durchgeführt werden.
- Das Risiko kann reduziert werden, indem Sie sich auf Webseiten regulär ausloggen anstatt nur den Browser (oder den Browser-Tab) zu schließen. Warten Sie dabei immer, bis die Webseite anzeigt, dass Sie ausgeloggt wurden.

Weitere Hinweise zum Angriff „Unverschlüsselte Kommunikation abhören“

Die Darstellung der Verschlüsselung der Kommunikation ist von Browser zu Browser unterschiedlich. Informationen dazu, wie Ihr Browser dies darstellt, finden Sie jedoch auf den Webseiten des BSI

- https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/EinrichtungBrowser/Sicherheitsmassnahmen/Verschluesselung/verschluesselung.html

Zu diesem Thema gibt es ein Video, welches die Problematik von verschlüsselten Verbindungen noch einmal anschaulich erklärt und weitere Informationen bietet:

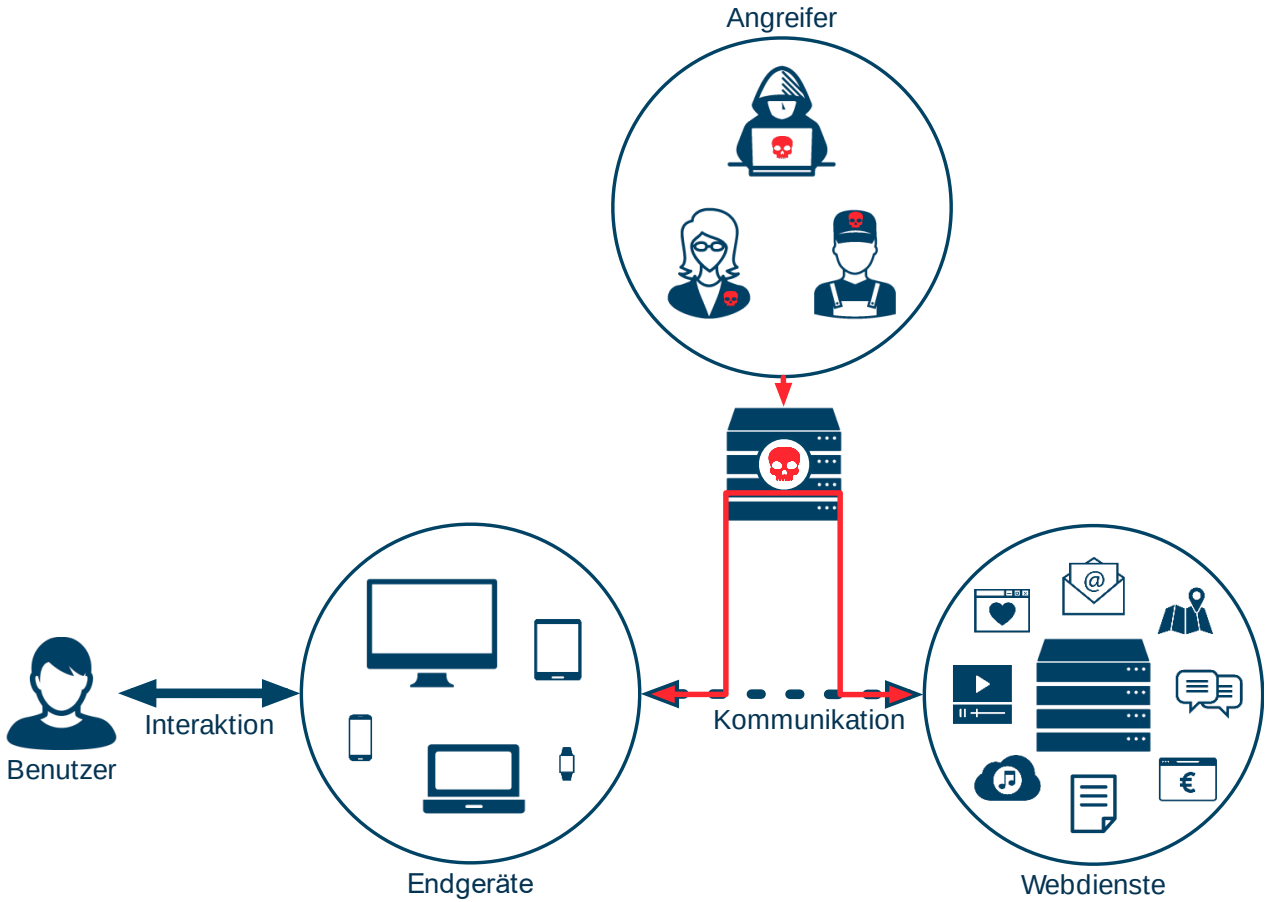
- https://www.youtube.com/watch?v=tW1-CmggG9s

Weitere Hinweise zum Angriff „Unverschlüsselte Kommunikation abhören“ - *Fortsetzung*

Manche Browser zeigen es Ihnen bereits heute an, wenn Sie Passwörter auf einer unverschlüsselten Webseite eingeben. Darüber hinaus gibt es auch Erweiterungen für Ihren Browser, die Sie beim Abwehren des Angriffes unterstützen:

- **PassSec+** unterstützt Sie bei der Erkennung von unsicheren Verbindungen, indem es Sie warnt, wenn Sie möglicherweise sensible Daten über eine unsichere Verbindung übertragen. Weitere Informationen zu PassSec+ erhalten Sie unter: https://www.secuso.org/passsec
- **HTTPS-Everywhere** (zu deutsch: HTTPS Überall) unterstützt Sie dabei immer eine verschlüsselte Verbindung aufzubauen, wo dies möglich ist. Weiterführende Informationen zu diesem Add-On können (nur auf Englisch) auf der folgenden Webseite eingesehen werden: https://www.eff.org/https-everywhere

Angriff (6/11): „Verschlüsselte Kommunikation abhören“



Beschreibung des Angriffs „Verschlüsselte Kommunikation abhören“

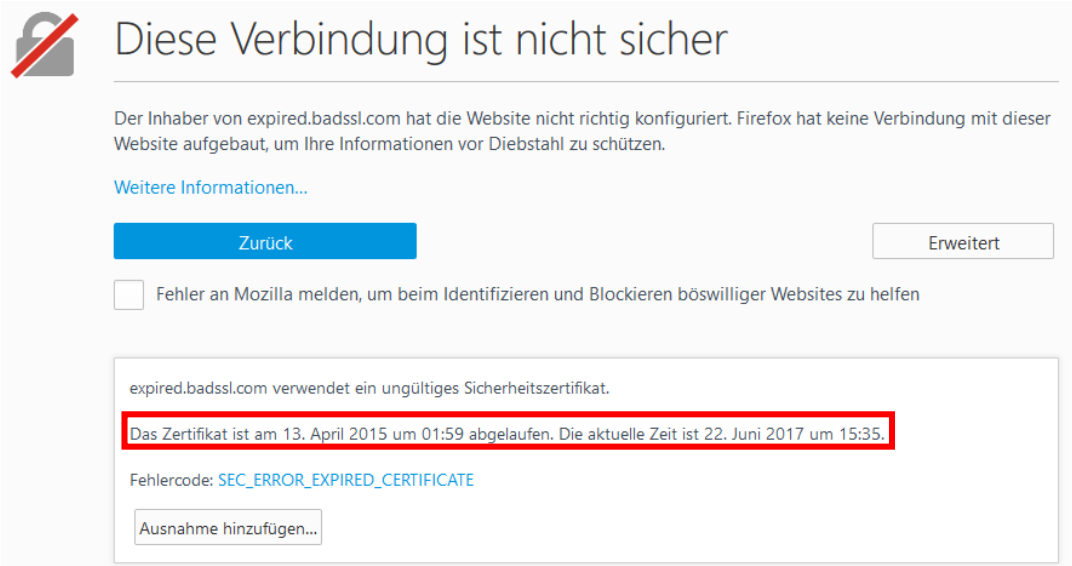
Der Angreifer versucht sich in die verschlüsselte Kommunikation zwischen Ihren Geräten und den Webdiensten einzuklinken:

- Angreifer können verschlüsselte Kommunikation nicht abhören.
- Ein technisch versierter Angreifer kann aber versuchen Sie zu täuschen, indem er versucht sich als der passende Webdienst auszugeben.
- Fallen Sie auf diesen Täuschungsversuch hinein, ist die Verbindung zwar verschlüsselt, aber anstatt mit der richtigen Webseite kommunizieren Sie mit dem Angreifer.

Abwehr des Angriffs „Verschlüsselte Kommunikation abhören“

Diesen Angriff können Sie in Browsern durch eine Warnmeldung erkennen.

- Sollten Sie auf eine solche Warnung stoßen, geben Sie Ihr Passwort nicht einfach ein.
- Weist Sie die Warnung nur auf ein kürzlich abgelaufenes Gültigkeitsdatum des Serverzertifikats hin, ist es in der Regel sicher fortzufahren (leider passiert dies so häufig, dass die überwiegende Anzahl dieser Warnungen Fehl-Alarme sind).
- Wie eine solche Warnung (in diesem Beispiel in Firefox) aussieht, sehen Sie auf dem folgenden Screenshot (der wichtige Teil ist in rot markiert):



Abwehr des Angriffs „Verschlüsselte Kommunikation abhören“ - *Fortsetzung*

- Wird eine andere Warnung angezeigt und Sie müssen den Dienst trotzdem dringend verwenden, dann überprüfen Sie, ob der Fehler an einem anderen Endgerät auch auftritt.
  - Tritt der Fehler dort nicht auf, ist es oftmals sicher über diese neu aufgebaute Verbindung fortzufahren.
  - Tritt er auch am anderen Gerät (oder mit VPN[3]) auf, sollten Sie beim Betreiber des Webdienstes nachfragen, ob eine Fehlkonfiguration vorliegt (schicken sie diesem dazu am besten einen Screenshot, der die Fehlermeldung wie auf der vorigen Seite zeigt). Nutzen Sie dazu Kontaktdaten aus z.B. vergangenen E-Mails und nicht von der möglicherweise vom Angreifer kontrollierten Webseite.
- Falls Sie unterwegs sind und Ihre Firma bietet Ihnen eine VPN-Verbindung[4] an, können Sie auch versuchen diese zu aktivieren und schauen ob der Fehler damit auftritt.
- Kann der Webseitenbetreiber einen Fehler ausschließen, versucht mit sehr hoher Wahrscheinlichkeit ein Angreifer sich in Ihre Kommunikation einzuklinken.

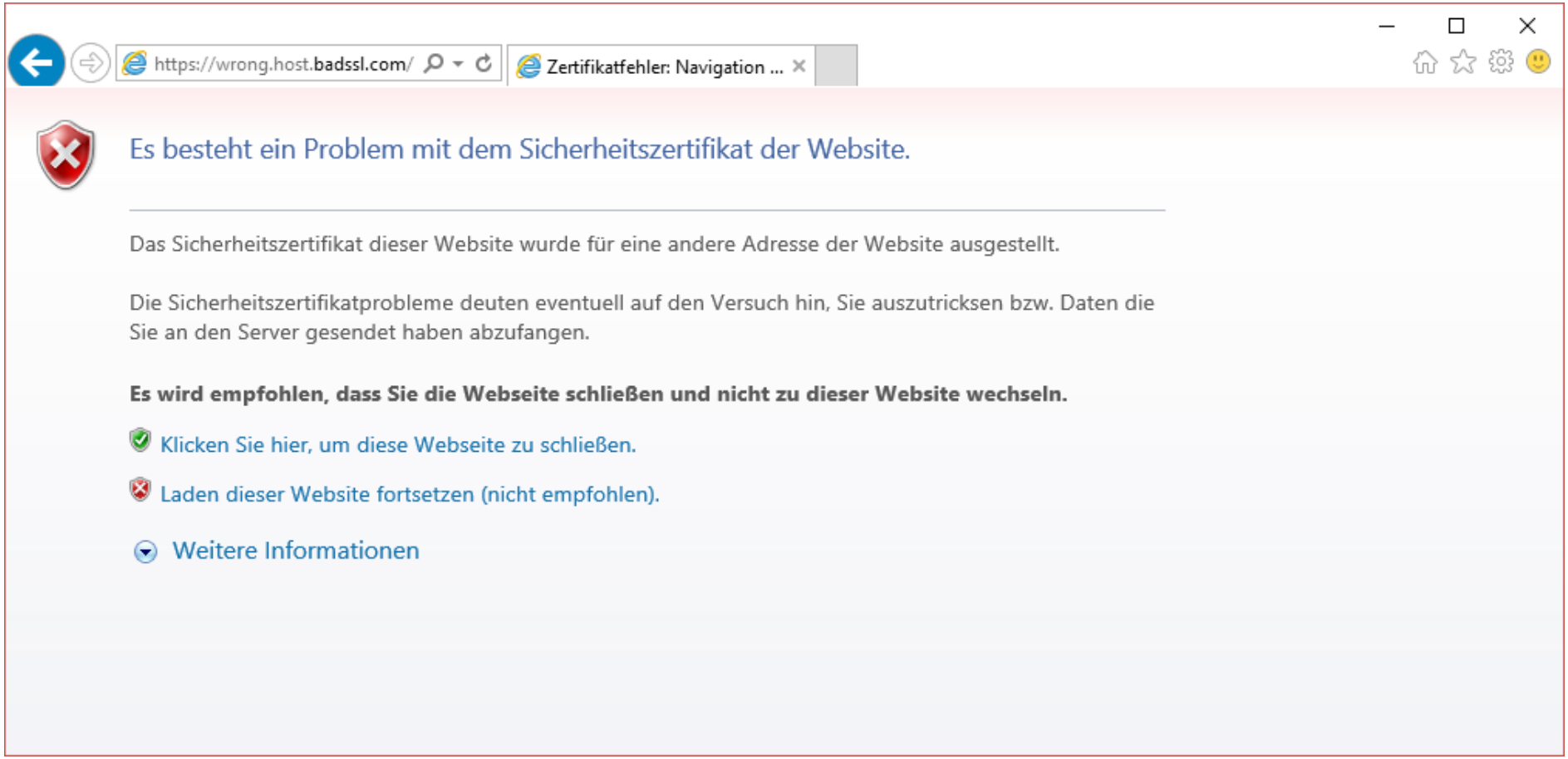
[4] Wenn Sie nicht wissen, was eine VPN-Verbindung ist, ignorieren Sie diese Alternative.

Abwehr des Angriffs „Verschlüsselte Kommunikation abhören“ - *Fortsetzung*

- Umgehen Sie solche Fehlermeldungen nie durch das ersetzen von „https“ durch „http“.
- Daten, die über eine unverschlüsselte Verbindung oder eine verschlüsselte Verbindung, in die sich ein Angreifer eingeklinkt hat, übertragen werden, können nicht mehr als geheim angesehen werden.
- Daher hilft es in diesem Falle nichts, sich auszuloggen oder den Browser zu schließen.
- Haben Sie das Gefühl, dass eines Ihrer Passwörter in die Hände von Angreifern geraten ist, dann versuchen sie dieses so schnell wie möglich (über eine sichere verschlüsselte Verbindung) zu ändern.

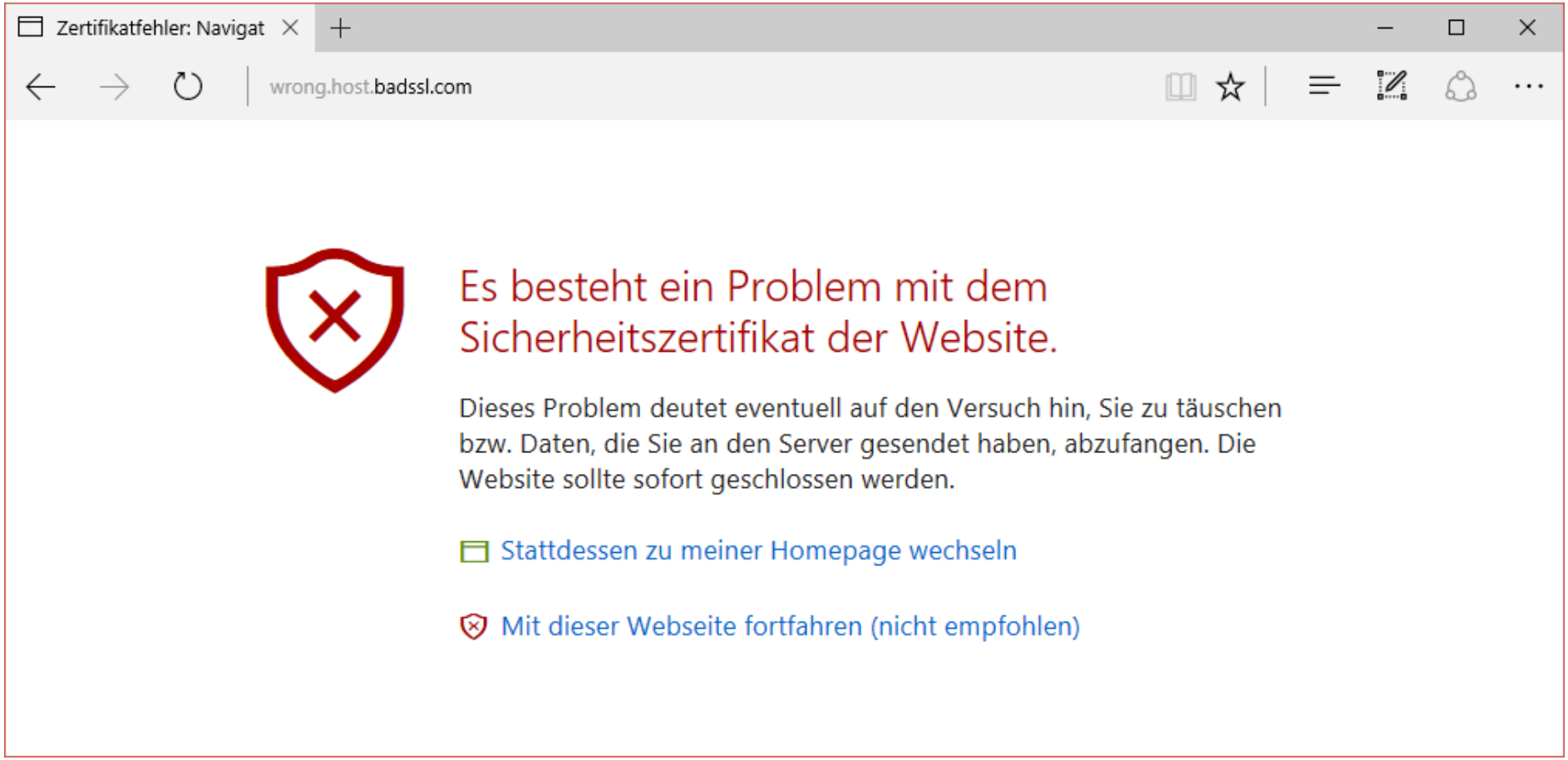
Weitere Hinweise zum Angriff „Verschlüsselte Kommunikation abhören“

Das folgende Bild zeigt eine gefährliche Warnung in Internet Explorer:



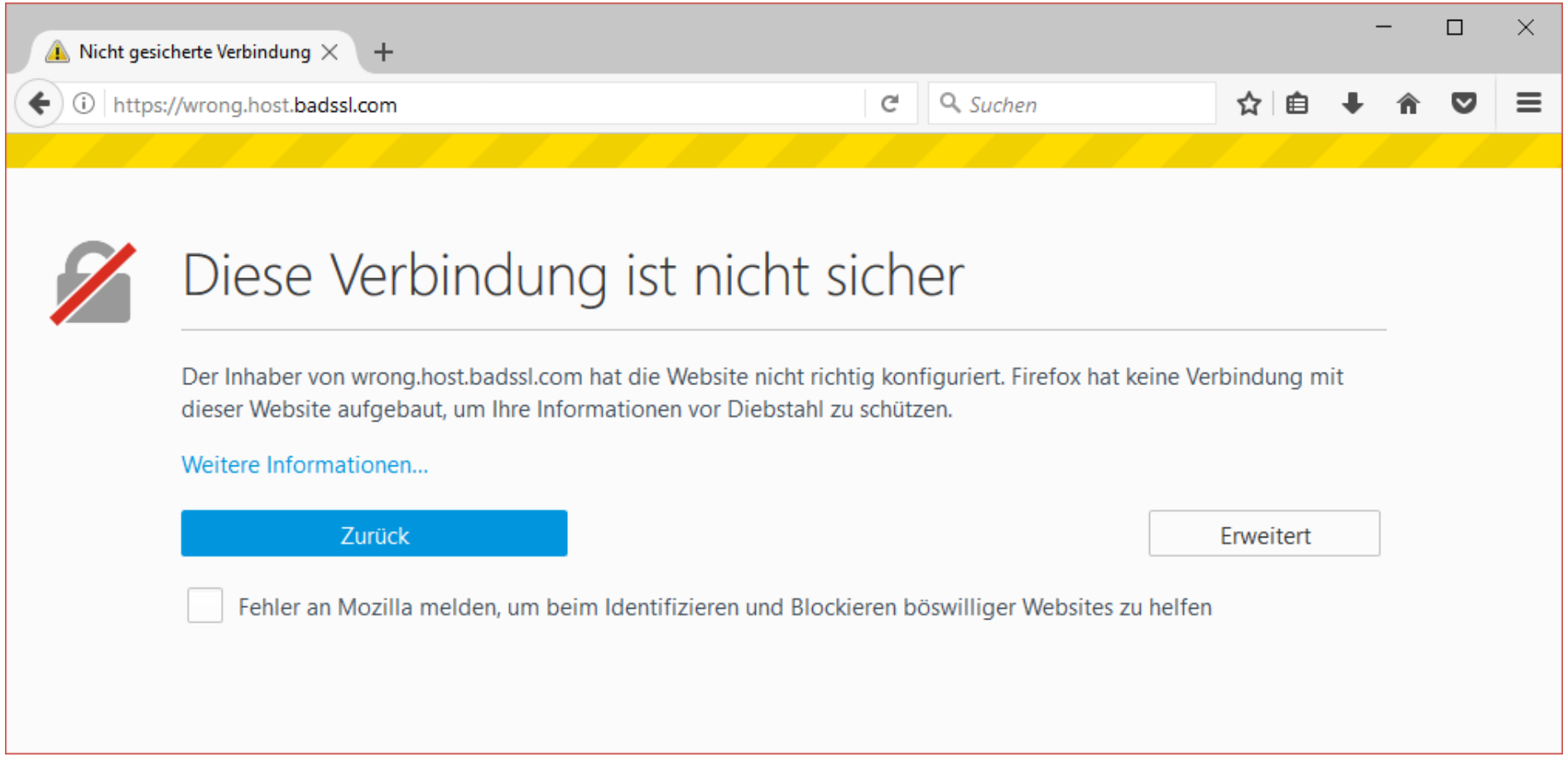
Weitere Hinweise zum Angriff „Verschlüsselte Kommunikation abhören“

Das folgende Bild zeigt eine gefährliche Warnung in Edge:



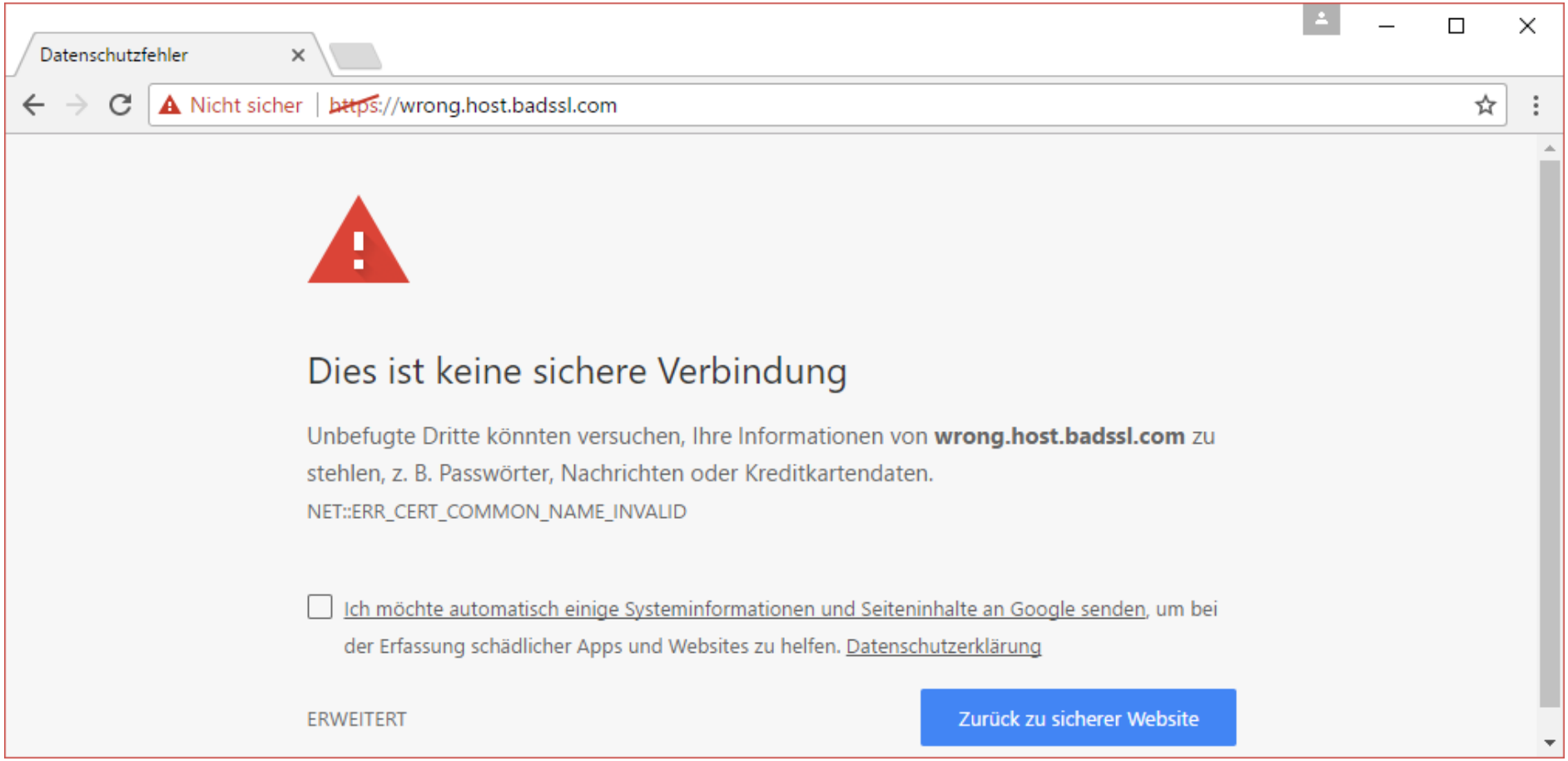
Weitere Hinweise zum Angriff „Verschlüsselte Kommunikation abhören“

Das folgende Bild zeigt eine gefährliche Warnung in Firefox:



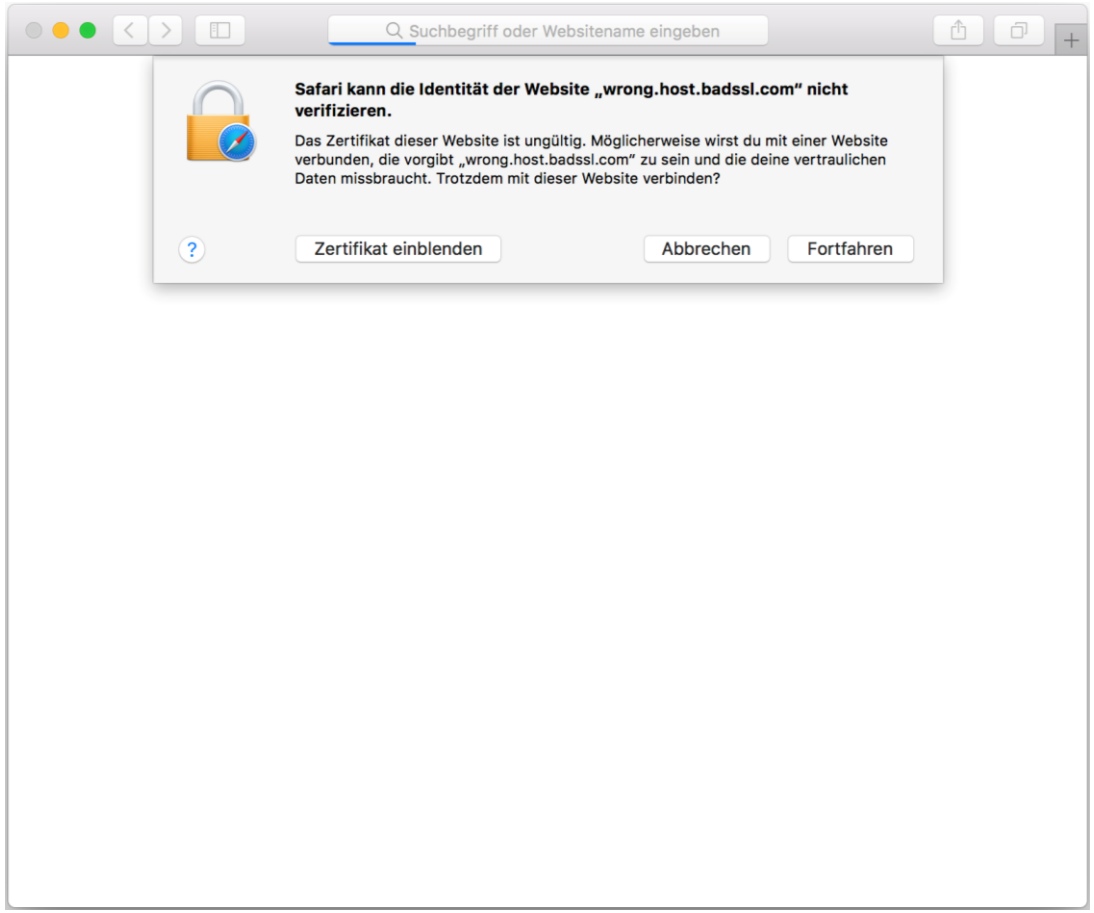
Weitere Hinweise zum Angriff „Verschlüsselte Kommunikation abhören“

Das folgende Bild zeigt eine gefährliche Warnung in Chrome:



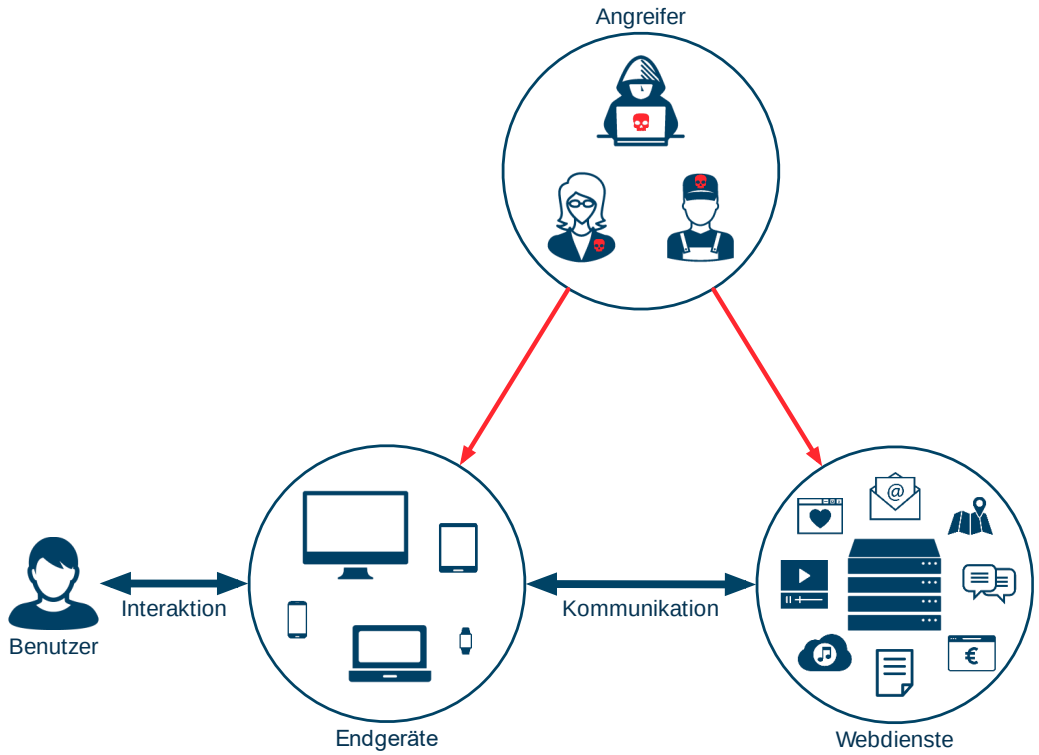
Weitere Hinweise zum Angriff „Verschlüsselte Kommunikation abhören“

Das folgende Bild zeigt eine gefährliche Warnung in Safari:

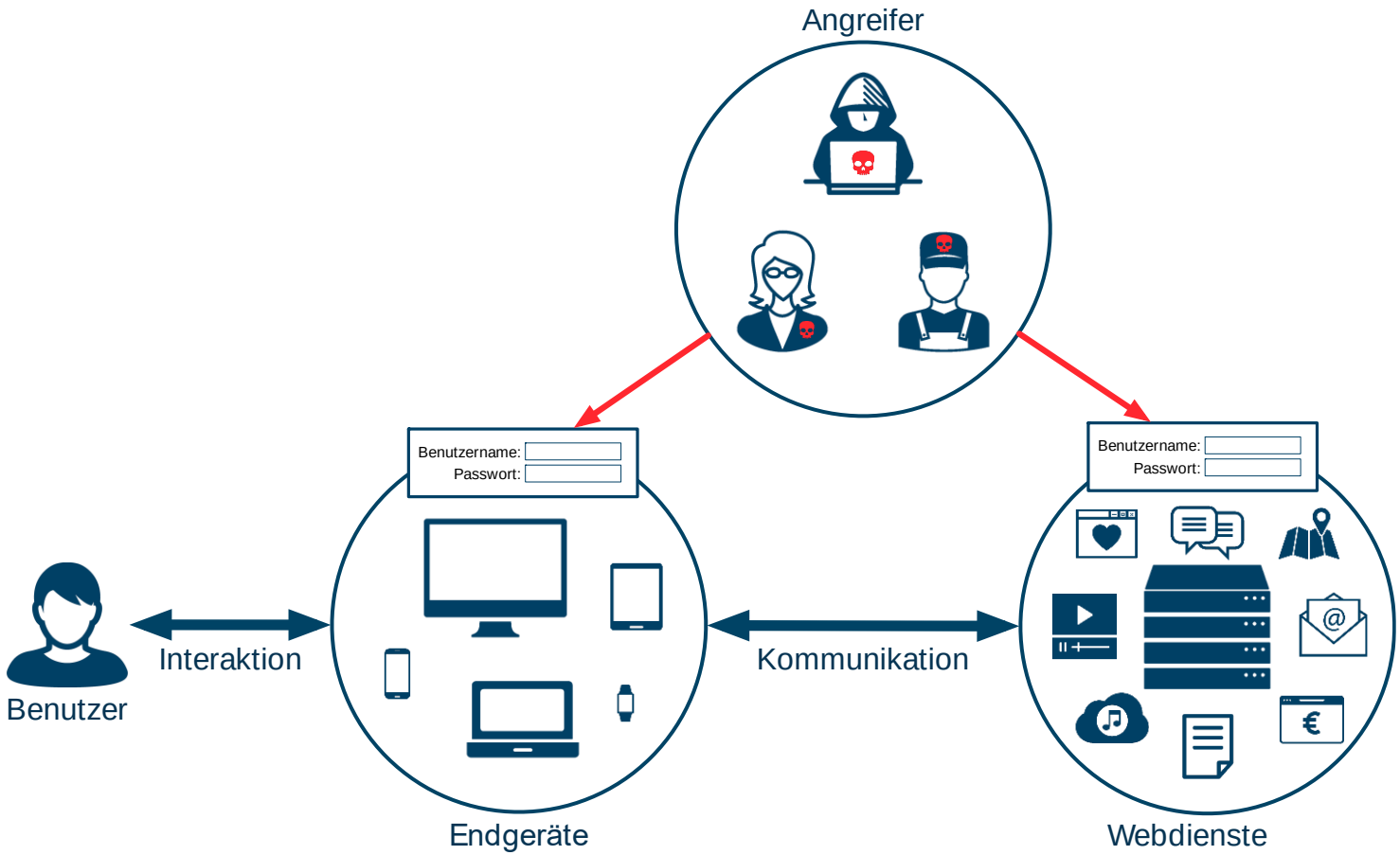


Angriffe, die sowohl bei Ihren Endgeräten als auch bei Webdiensten ansetzen

Im Folgenden werden Ihnen die Angriffe vorgestellt, bei denen der Angreifer sowohl bei Ihren Endgeräten als auch bei den von Ihnen verwendeten Webdiensten ansetzen kann.



Angriff (7/11): „Gezieltes Raten“



Beschreibung des Angriffs „Gezieltes Raten“

Der Angreifer versucht das Passwort des Benutzers zu erraten und nutzt den normalen Login-Mechanismus, um zu überprüfen, ob es das richtige Passwort ist.

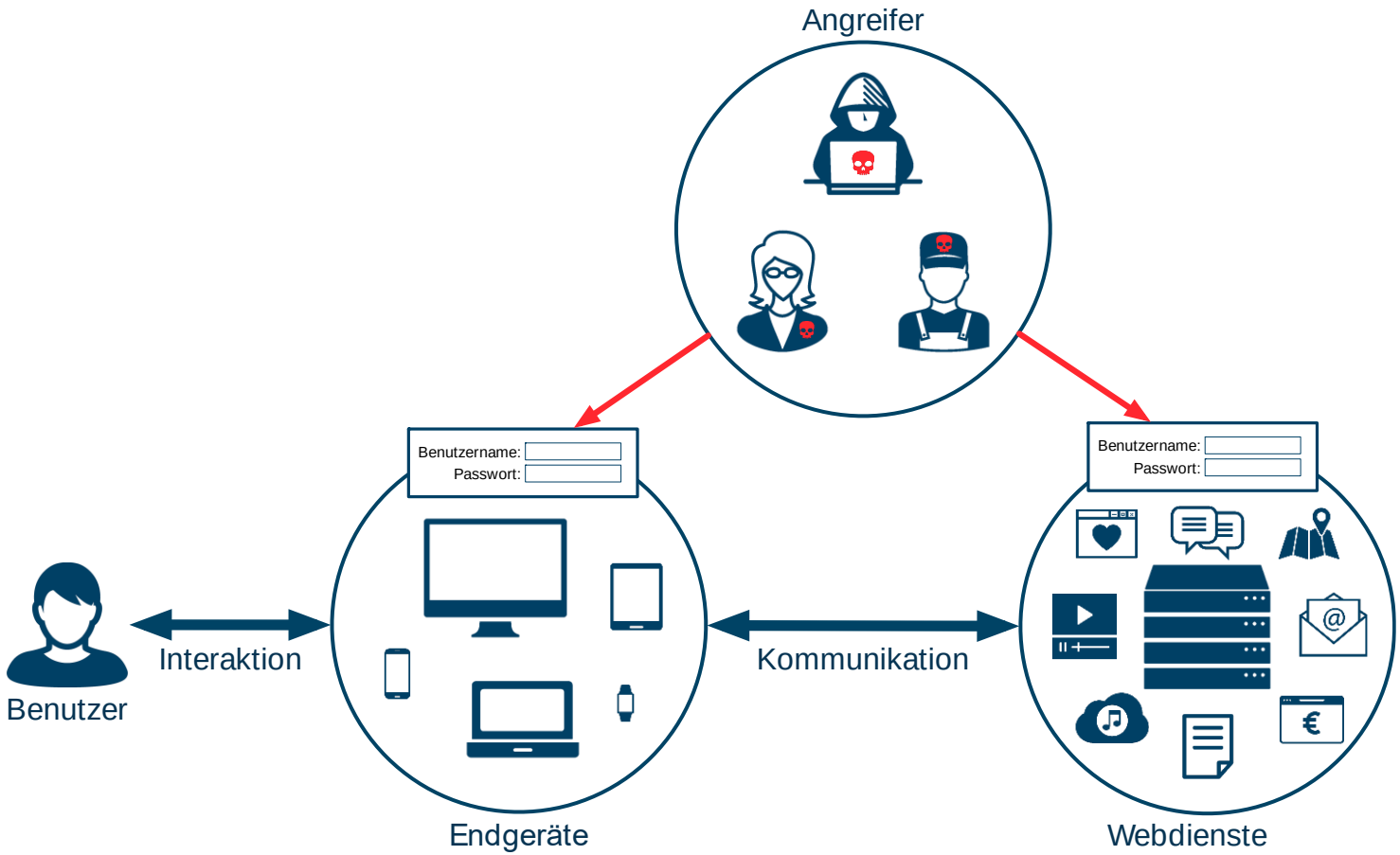
- Der Angreifer probiert gezielt Passwörter, die ganz genau auf das Opfer zugeschnitten sind, in Verbindung mit dem bekannten Benutzernamen.
- Dazu versetzt er sich gezielt in die Rolle des Opfers, um so dessen Prozess zur Passwort-Generierung nachzuahmen. Dies setzt intimes Wissen über das Opfer voraus (z.B. Hobbies, Lieblingstier, Vorliebe für bestimmte Rätsel, Geburtstage, etc.).
- Durch den offenherzigen Einsatz von sozialen Medien haben auch fremde Angreifer immer bessere Chancen mit einer solchen Strategie erfolgreich zu sein.
- Technisch versierte Angreifer können sich eine Liste der relevanten Informationen erstellen und diese dann mit Spezialsoftware automatisiert durchprobieren.
- Besonders einfach ist dieser Angriff, wenn Sie Passwörter wiederverwenden. Kennt der Angreifer eines Ihrer Passwörter, kann er dieses und Variationen davon ausprobieren.
- Standard-Passwörter bei Geräten wie z.B. netzwerkfähigen Kameras, etc. stellen ein Risiko dar. Standard-Passwörter können von Angreifern einfach in Erfahrung gebracht werden.

Abwehr des Angriffs „Gezieltes Raten“

Um vor gezieltem Raten geschützt zu sein, sollte Ihr Passwort keine persönlichen Daten nutzen.

- Machen Sie sich klar, welche persönlichen Daten dem Angreifer bekannt sein könnten. Ihre Arbeitskollegen können leichter inhaltliche Details und Assoziationen im Arbeitskontext herstellen. Die Fußballfreunde wissen genau, gegen welche Mannschaft man das Eigentor geschossen hat. Der Partner kennt den Ort, an dem man sich das erste Mal getroffen hat und das Geburtsdatum des gemeinsamen Hundes.
- Je nachdem, gegen wen Sie sich schützen möchten, sollten Informationen gemieden werden, welche den betreffenden Personen bekannt sind. Solche Informationen können auch von Person zu Person weitergegeben werden, ohne dass Sie dies wissen oder merken.
- Standard-Passwörter bei Geräten wie Netzwerk-Druckern oder Routern sollten unbedingt geändert werden. Diese sind üblicherweise in den Handbüchern zu den entsprechenden Geräten vermerkt und können so von Angreifern sehr einfach genutzt werden.
- Teils ist es möglich Passwörter mit sogenannten Sicherheitsfragen zurückzusetzen und so Zugriff auf ein Benutzerkonto zu erlangen. Dies betrifft jedoch nicht das Passwort selbst und wird daher an späterer Stelle dieses Moduls genauer behandelt (Angriff 11).
- Zufällig generierte Passwörter (z.B. von Passwortmanager) schützen vor gezieltem Raten.

Angriff (8/11): „Ungezieltes Raten“



Beschreibung des Angriffs „Ungezieltes Raten“

Beim „ungezielten Raten“ nutzt der Angreifer den normalen Login-Mechanismus, um zu überprüfen, ob das geratene Passwort das richtige ist. Im Gegensatz zum „gezielten Raten“ ist es nicht Ziel des Angreifers in ein bestimmtes Benutzerkonto einzudringen.

- Der Angreifer versucht stattdessen ungezielt möglichst viele Benutzerkonten bei einem bestimmten Dienst (z.B. E-Mail-Anbieter) zu knacken und für die eigenen Zwecke zu nutzen.
- Der Angreifer schickt jeden Passwort-Kandidaten (also das Passwort, das er ausprobieren möchte) für jeden Benutzernamen den er kennt, einzeln an den Webdienst oder an das Gerät.

Missverständnis #11: Alle Benutzer des Webdienstes oder Endgerätes sind gleichermaßen betroffen. Daher sollten Sie nie das Gefühl haben, dass Sie zu unwichtig sein könnten.

Missverständnis #12: Spezielle Software erlaubt es dem Angreifer diesen Angriff zu automatisieren. Er muss nicht jedes Passwort einzeln eingeben. Dies übernimmt die Software für ihn.

Beschreibung des Angriffs „Ungezieltes Raten“ - *Fortsetzung*

- Die Server von Webdiensten erlauben häufig nur eine sehr eingeschränkte Anzahl von fehlgeschlagenen Logins in kurzer Zeit.
- Einige Webdienste haben einen Blockierungs-Mechanismus, der das Benutzerkonto nach einer gewissen Anzahl an Versuchen für eine gewisse Zeit sperrt (ähnlich zu den drei Versuchen bei der PIN-Eingabe einer Bankkarte). Auch mobile Geräte haben oftmals solche Beschränkungen (wenn eine Sperre gesetzt ist).
- Der Angreifer nutzt daher eine Wörterliste der am weitesten verbreiteten Passwort-Kandidaten, um diese mithilfe spezieller Software automatisiert zu testen.
- Der Angreifer ist auf die Kenntnis gültiger Benutzernamen angewiesen. Daher ist dieser Angriff bei Webseiten mit öffentlichen Benutzernamen (z.B. Auktionsseiten oder Foren) und auch bei E-Mail-Konten besonders relevant.
- E-Mail-Konten sind deshalb gefährdet, weil Angreifer E-Mail-Adressen auf dem Schwarzmarkt im Internet in großer Stückzahl und zu sehr geringen Preisen erwerben können. Jede E-Mail-Adresse, an die Spam versendet wird, ist im Internet schon einmal über die „schwarze Ladentheke“ gewandert.

Abwehr des Angriffs „Ungezieltes Raten“

Der Angreifer testet bei diesem Angriff nur die häufigsten Passwörter. Diese sollten Sie auf keinen Fall verwenden! Im Folgenden finden Sie eine kleine Auswahl der häufigsten Passwörter von 2016, die in jeder Wörterliste zu finden sein werden:

123456	1234567	monkey	Fussball	123456789
password	Passwort	letmein	1234	111111
passwort	willkommen	sesam	1QAY2WSX	qwertzuiop
qwerty	1234567890	login	dragon	master
qwertz	abc123	princess	starwars	internet

Diese Liste hat natürlich keinen Anspruch auf Vollständigkeit! Die Wörterbücher der Angreifer sind meist deutlich umfangreicher und werden immer wieder angepasst.

Missverständnis #13: Auch Tastenverläufe auf der Tastatur, die auf den ersten Blick noch zufällig aussehen (z.B. 1QAY2WSX oder qwertz) sind in den Wörterlisten der Angreifer zu finden, da sie von vielen Benutzern als Passwort gewählt werden. Daher stellen Tastenverläufe auf der Tastatur unsichere Passwörter dar, selbst wenn sie Sonderzeichen und Zahlen enthalten.

Abwehr des Angriffs „Ungezieltes Raten“ - *Fortsetzung*

Der Angreifer weiß natürlich, welche Seite er angreift. Daher sind zusätzlich auch andere Passwörter zu vermeiden. Die folgenden Passwörter sind Beispiele, die nach dem Hack von Adobe im Jahr 2013 sehr einfach geknackt werden konnten. Es gab viele Passwörter, die mit dem Namen Adobe direkt zusammenhingen oder an Produkte der Firma angelehnt waren:

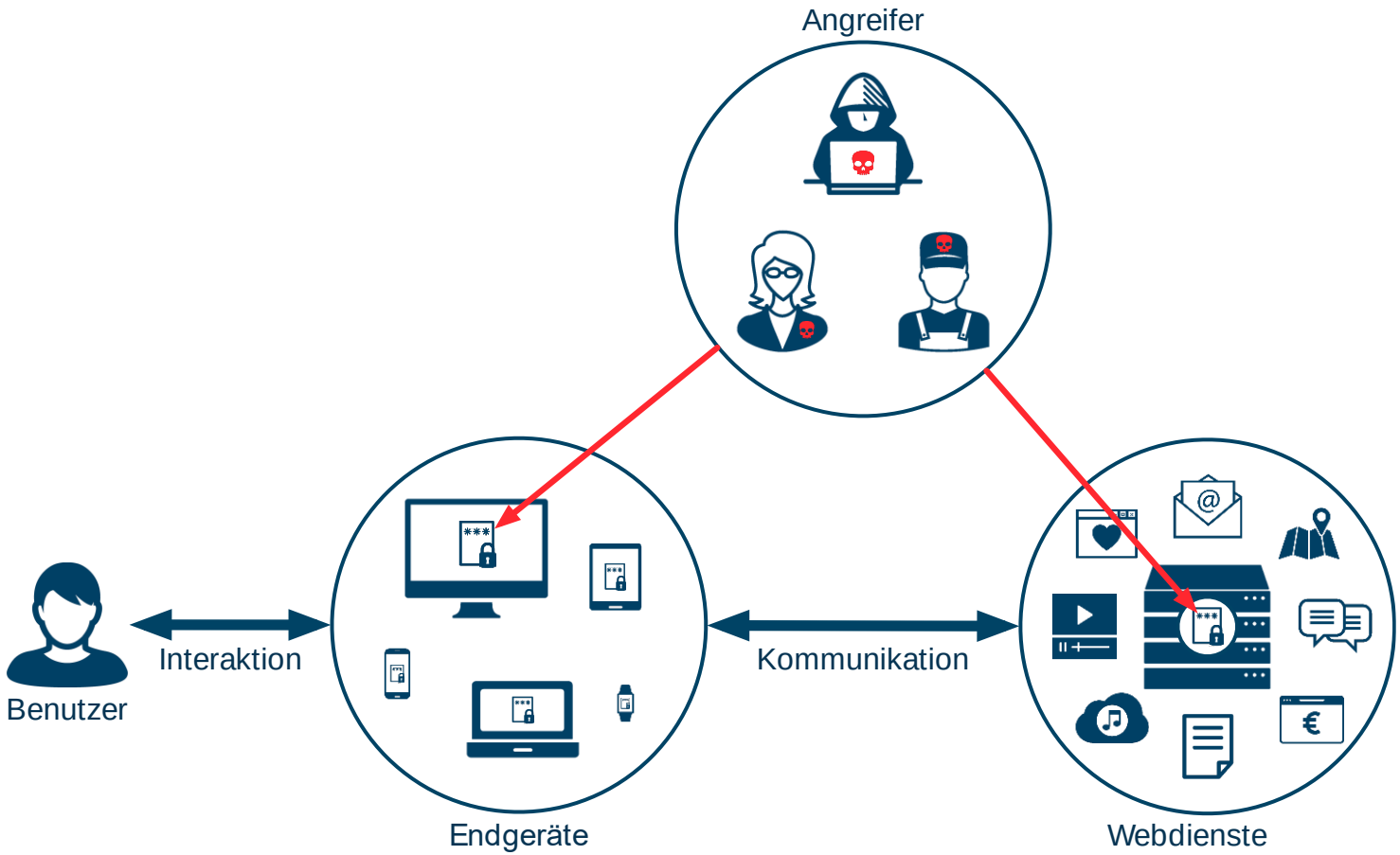
adobe123	adobeadobe	photoshop
adobe1	macromedia	flashplayer

Missverständnis #14: Angreifer probieren nicht immer die gleichen Wörterlisten. Sie passen sie an die Gegebenheiten an (z.B. welcher Webdienst das Ziel ist). Diese Anpassung beinhaltet auch das Aufnehmen von Wörtern aus verschiedenen Sprachen.

Eine einfache Möglichkeit sich vor ungezieltem Raten zu schützen ist die Nutzung eines Passwortmanagers[5] oder von Zwei-Faktor-Authentifizierung[5].

[5] Nähere Informationen hierzu erhalten Sie im zweiten Modul dieser Passwort-Schulung.

Angriff (9/11): „Raten nach Einbruch ins System“



Beschreibung des Angriffs „Raten nach Einbruch ins System“

Der mächtigste Rate-Angriff besteht darin, nicht den normalen Login-Mechanismus zu nutzen, sondern zunächst die Passwortdaten aller Nutzer aus einem System zu entwenden (z.B. durch einen Einbruch bei einem Webdienst).

- Für diesen Angriff muss ein technik-versierter Angreifer zunächst in den Webservice oder das gesperrte System eindringen.
- Folgen Webdienste und Gerätehersteller der empfohlenen Praxis, sind Passwörter immer in einer verschleierten Form (als sogenannter Hashwert) gespeichert. Daher muss der Angreifer auch im Falle eines erfolgreichen Einbruches einen Rate-Angriff durchführen.
- Die Benutzernamen sind in den entwendeten Passwortdaten enthalten.

Missverständnis #15: Alle Benutzer des Webdienstes oder Endgerätes sind gleichermaßen betroffen. Daher sollten Sie nie das Gefühl haben, dass Sie zu unwichtig sein könnten.

Beschreibung des Angriffs „Raten nach Einbruch ins System“ - *Fortsetzung*

Der eigentliche Rate-Angriff wird mit den entwendeten Daten durchgeführt.

- Es wird Spezialsoftware eingesetzt, die automatisiert mithilfe der entwendeten Daten enorm viele Passwort-Kandidaten in kurzer Zeit ausprobiert.
- Technisch-versierte Angreifer nutzen nacheinander zwei verschiedene Strategien.
  1. Zunächst eine sogenannte „Brute Force“-Strategie (Angriff mit roher Gewalt):
     - Es werden alle möglichen Passwort-Kandidaten durchprobiert.
     - Theoretisch kann so jedes Passwort erraten werden, auch komplett zufällige mit Zahlen und Sonderzeichen.
     - Der Aufwand dieser Strategie steigt sehr stark mit der Länge des Passworts an.
     - Ab einer Länge von 8 Zeichen bei Passwörtern ist diese Strategie für Angreifer in der Regel nicht mehr rentabel.

Missverständnis #16: Passwörter werden durch das Einfügen von Großbuchstaben, Zahlen und Sonderzeichen nicht automatisch sicherer. Dies gilt insbesondere für kurze Passwörter. Sind Passwörter kurz, kann ein Angreifer einfach alle Möglichkeiten durchprobieren. Eine gute Möglichkeit lange Passwörter zu generieren ist es mehrere Wörter aneinanderzuhängen, sodass das Gesamt-Passwort möglichst lang ist. Dies ist eine Strategie, die auch von Edward Snowden empfohlen wird.

Beschreibung des Angriffs „Raten nach Einbruch ins System“ - *Fortsetzung*

2. Kann das Passwort mit der „Brute Force“-Strategie nicht erraten werden, wechselt der Angreifer zu einem „Wörterbuch-Angriff“:
   - Wie beim „ungezielten Raten“ testet er häufig von Benutzern gewählte Passwörter.
   - Die Wörterliste ist deutlich größer und aus verschiedenen Quellen erstellt, z.B. Wörterbücher verschiedener Sprachen, Buchstabenketten wie „qaywsx“, die auf der Tastatur ein Muster ergeben, und bekannte Passwörter aus vergangenen Einbrüchen.

Missverständnis #17: Die eingesetzte Software erzeugt aus jedem Eintrag der Wörterliste mehrere weitere Einträge und testet auch diese. Dabei wird menschliches Verhalten nachgeahmt:

- Anhängen von Zahlen/Sonderzeichen (insbesondere “!“) an das Ende oder den Anfang des Passwortes
- Ersetzen von Buchstaben durch Zahlen (z.B. E→3) und durch Sonderzeichen (z.B. a→@)
- Ersetzen von Kleinbuchstaben durch Großbuchstaben (insbesondere am Anfang des Passwortes).

Daher werden Passwörter durch Großbuchstaben, Zahlen und Sonderzeichen nicht automatisch sicherer.

Missverständnis #18: Ein Angreifer wird mit der eingesetzten Spezialsoftware alle Kombinationen aus Jahr, Monat und Tag (oder nur einem Teil davon) als Zahlen zusammensetzen und ausprobieren. Wer also das Geburtsdatum seines Hundes oder Lieblingsschauspielers anstatt des eigenen verwendet, verändert die Stärke des Passwortes gegen einen solchen Angriff nicht. Dies gilt sowohl für das Raten nach Einbruch ins System, als auch bei ungezielten Rate-Angriffen, wenn viele Rate-Versuche möglich sind, bevor der Angriff vom Betreiber unterbunden wird.

Abwehr des Angriffs „Raten nach Einbruch ins System“

Die Abwehr eines solchen Angriffes liegt vornehmlich bei den Sicherheits-Experten der Webdienste und Gerätehersteller, die ihre Systeme entsprechend absichern und zuverlässige Mechanismen einsetzen sollten, um zu bemerken, wenn ein Angreifer in ein System eindringt.

- Sollte ein Webdienst, bei dem Sie ein Benutzerkonto haben, Ziel eines Angriffes werden, sollten Sie schnellstmöglich handeln und das Passwort ändern.
- Ein vorsorgliches Ändern von Passwörtern hingegen ist nicht nötig, auch wenn dies leider einige Standards immer noch vorsehen, denen manche Unternehmen entsprechen müssen (z.B. PCI-DSS der Kreditkartenindustrie).

Missverständnis #19: Das vorsorgliche Ändern von Passwörtern, die man sich merken muss, wird von der Wissenschaft als nicht hilfreich angesehen. Der immense Mehraufwand für Benutzer steht in keinem Verhältnis zur Schutzwirkung. Auch staatliche Stellen wie das amerikanische NIST oder das britische NCSC passen bereits Ihre Empfehlungen an. Sie empfehlen nur ein neues Passwort zu wählen, wenn das alte in die Hände eines Angreifers gerät anstatt es vorsorglich zu wechseln. Die Behörden empfehlen Webdiensten stattdessen eine rigorose Überwachung der eigenen Server und den Einsatz von sogenannten Lockout-Mechanismen (z.B. die Begrenzung der Anzahl der Versuche beim Login oder zusätzliche Überprüfungen bei Logins aus Ländern, von denen aus sich der Benutzer noch nie eingeloggt hat). Passwörter häufig zu wechseln ist daher eine überholte Praxis und sollte nicht angewendet werden.

Abwehr des Angriffs „Raten nach Einbruch ins System“ - *Fortsetzung*

Um sich vor Rate-Angriffen nach einem Einbruch ins System zu schützen, sollten Sie ein langes Passwort wählen (für sehr sichere Passwörter mindestens 20 Zeichen).

- Vermeiden Sie Passwörter, die in der Wörterliste des Angreifers vorkommen können oder aus deren Einträgen generiert werden können.
- Diese Passwörter müssen Rate-Angriffen nach Einbruch ins System widerstehen können:
  - Ihr Login am PC/Laptop
  - Das Master-Passwort Ihres Passwortmanagers[6]
  - Das Passwort Ihres E-Mail-Benutzerkontos
  - Ihre Passwörter Benutzerkonten bei Single-Sign-On-Diensten[6]

Missverständnis #20: Oftmals verlangen Webdienste, dass Zahlen und Sonderzeichen in das Passwort integriert werden. Die aktuelle Forschung zeigt jedoch, dass Großbuchstaben, Zahlen und Sonderzeichen Passwörter nicht automatisch sicherer machen. Ziehen Sie lange Passwörter (z.B. durch Aneinanderreihen mehrerer Wörter) dem Einfügen von Zahlen und Sonderzeichen vor. Lange Passwörter bieten meist deutlich mehr Sicherheit und können zudem einfacher zu merken sein. Das Aneinanderreihen mehrerer Wörter ist hierbei eine besonders wirksame Strategie, die Angreifern das Erraten von Passwörtern erschwert.

[6] Mehr Informationen zu diesen Technologien erhalten Sie im zweiten Modul dieser Schulung.

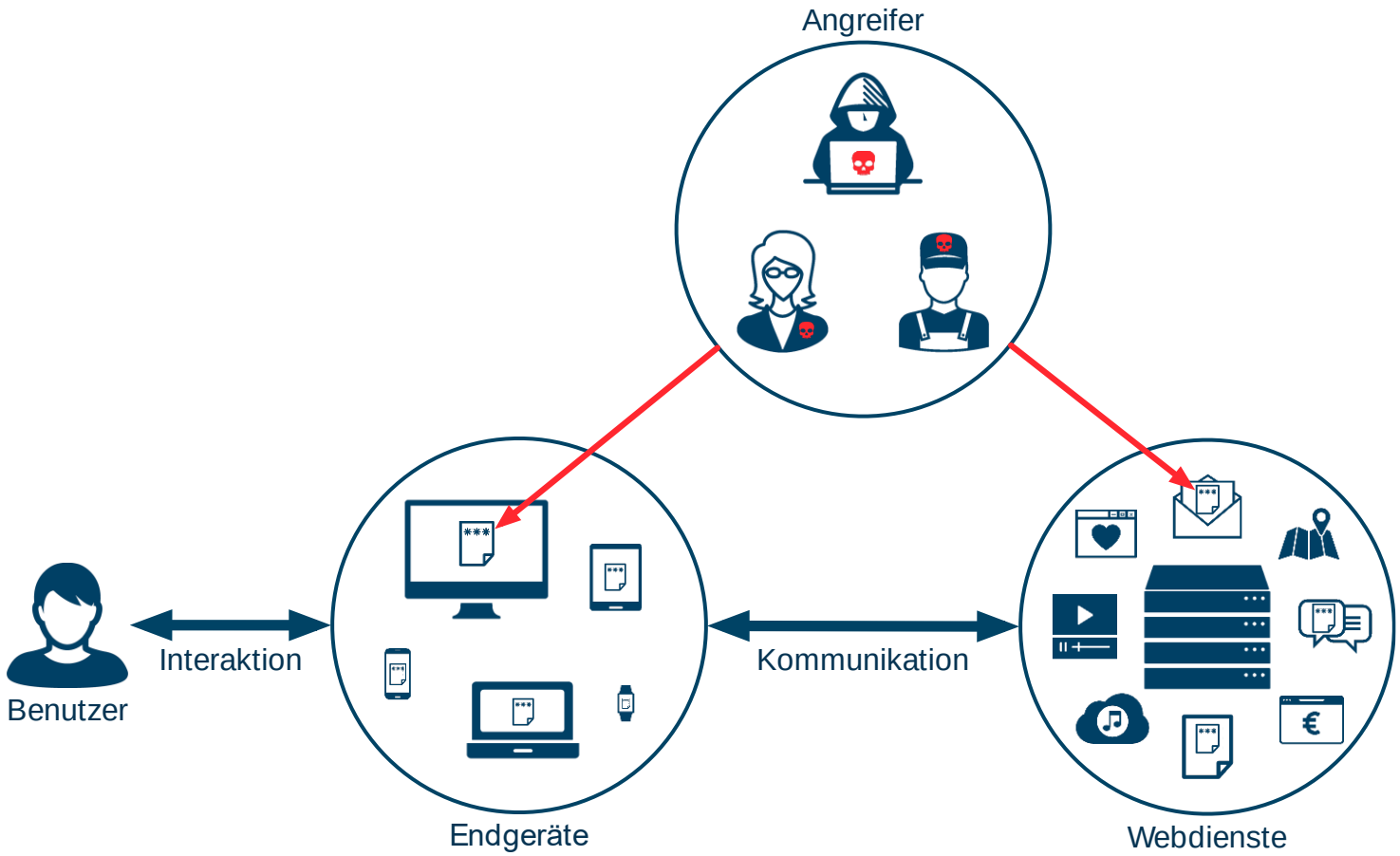
Weitere Hinweise zum Angriff „Raten nach Einbruch ins System“

- Wenn Sie Passwörter wiederverwenden, birgt ein Einbruch in nur einen Dienst den sie nutzen das Potential, dass auch Ihre Benutzerkonten bei anderen Diensten in Gefahr geraten.

Missverständnis #21: Auch besonders starke Passwörter sollten nicht mehrfach verwendet werden. Tatsächlich ist die Gefahr sich in ungerechtfertigter Sicherheit zu wiegen hierbei hoch. Je öfter Sie ein Passwort wiederverwenden (egal wie stark es ist), desto größer ist das Risiko. Auch Passwörter, die sie häufig eingeben, sollten Sie nicht für andere Benutzerkonten wiederverwenden. Es gibt immer wieder auch große Webdienste, die sorglos mit den Passwortdaten Ihrer Benutzer umgehen und so können auch komplexe Passwörter abhandenkommen und Angreifern in die Hände fallen.

- Auf der Webseite https://haveibeenpwned.com (nur in Englisch verfügbar) können Sie überprüfen, ob Sie von einem bekannten Hacker-Einbruch betroffen sind und eines Ihres Passwörter abhandengekommen ist. Wenn Sie dort nichts finden, heißt dies jedoch nicht, dass Sie nicht doch von einem kleineren oder weniger bekannten Hacker-Einbruch betroffen sein könnten.

Angriff (10/11): „Unverschlüsselte elektronische Notiz entwenden“



Beschreibung des Angriffs „Unverschlüsselte elektronische Notiz entwenden“

Der Angreifer versucht Passwörter, die Sie „elektronisch aufgeschrieben“ haben (z.B. in Office-Dokumenten auf einer unverschlüsselten Festplatte) zu entwenden.

- Unverschlüsselte Notizen sind unsicher aufbewahrten physischen Notizen gleichzusetzen, egal ob auf Ihrem Gerät, externen Speichermedien (z.B. USB-Stick) oder in der Cloud. Jeder mit Zugriff auf das Gerät (bzw. Speichermedium/Cloud) erhält Zugriff auf Ihre Passwörter.
- Werden solche Notizen bei Backups auf externe Speichermedien (z.B. USB-Stick, etc.) kopiert, sind sie umso einfacher zu entwenden oder verlieren.
- Werden Sie in der Cloud abgelegt, (z.B. Office-Dokument in der Dropbox, etc. oder als Notiz in Evernote bzw. ähnlichen Notizprogrammen), haben Administratoren des Cloud-Dienstes Zugriff darauf und Angreifer erbeuten bei einem Einbruch in die Server alle Ihre Passwörter.

Missverständnis #22: Browser haben meist einen integrierten Passwortmanager, der es erlaubt Passwörter zu speichern. Das Speichern von Passwörtern im Browser ist das Gleiche wie das Speichern von Passwörtern in einem Passwortmanager. Ist die Festplatte Ihres Gerätes nicht verschlüsselt und Ihre Passwörter sind in einem Passwortmanager gespeichert (egal ob Browser oder eigenständiges Programm), der nicht durch ein Masterpasswort geschützt ist, ist dies einer unverschlüsselten elektronischen Notiz gleichzusetzen.

Abwehr des Angriffs „Unverschlüsselte elektronische Notiz entwenden“

Unverschlüsselte elektronische Notizen von Passwörtern sollten Sie immer vermeiden, egal ob auf Ihrem Gerät, externen Speichermedien wie USB-Sticks oder in der Cloud.

- Verschlüsselt gespeicherte Passwörter sind unkritisch und werden empfohlen.
- Im Falle eines Verkaufs oder der Weitergabe eines Ihrer Geräte sind unverschlüsselte Informationen auch nach dem Löschen von dem neuen Besitzer wiederherstellbar, bei verschlüsselten Informationen dagegen hat er keine Chance. Passwortdaten sollten Sie beim Verkauf oder der Weitergabe Ihrer Geräte stets löschen, selbst wenn ein Freund der neue Besitzer ist. Sie wissen nie, wen er an das Gerät lässt und was genau damit passiert.

Missverständnis #23: Gespeicherte Passwörter dürfen nur auf verschlüsselten Speichermedien aufbewahrt werden. Sind alle vier der folgenden Kriterien erfüllt, ist es immer noch sehr ratsam ein Masterpasswort für Ihren Passwortmanager zu wählen, in Ausnahmefällen jedoch weniger kritisch:

1. Nur Sie verwenden Ihre Geräte
2. Sie haben die Festplatte Ihres Endgerätes verschlüsselt
3. Sie synchronisieren Ihre Passwörter nicht auf andere Endgeräte
4. Sie sperren Ihr Endgerät immer, wenn Sie es nicht verwenden

Andernfalls müssen Sie im Passwortmanager immer ein Masterpasswort setzen. Dies sollte so gewählt sein, dass es auch dem Angriff „Raten nach Einbruch ins System“ standhalten kann.

Abwehr des Angriffs „Unverschlüsselte elektronische Notiz entwenden“ - *Fortsetzung*

- Wenn Sie Ihre Passwörter auf mehrere Geräte synchronisieren oder auch andere Personen Ihre Geräte verwenden, ist es erforderlich Ihre Passwörter durch einen zusätzlichen Zugangsschutz (z.B. Master-Passwort) zu sichern.
- Eine sichere Synchronisierung kann mit Passwortmanagern durchgeführt werden, die mit einem Master-Passwort geschützt sind (sowohl eigenständige Programme als auch in Browsern integrierte).

Missverständnis #24: Die meisten IT-Sicherheits-Experten nutzen Passwortmanager und vertrauen diesen ihre Passwörter an. Der Einsatz von Passwortmanagern erlaubt eine sichere Verwaltung von Passwörtern und hilft Ihnen vielen Angriffen vorzubeugen und entgegenzuwirken. Weitere Informationen dazu erhalten Sie im zweiten Modul dieser Schulung.

Abwehr des Angriffs „Unverschlüsselte elektronische Notiz entwenden“ - *Fortsetzung*

Erfordert es ein Notfall, dass Sie ein Passwort elektronisch an eine andere Person senden, sollten Sie diese Nachricht (E-Mail, etc.) unbedingt verschlüsseln, um sicherzustellen, dass nur der rechtmäßige Empfänger Zugriff auf das Passwort erhält.

- Ist dies nicht möglich, suchen Sie nach einer anderen Möglichkeit das Passwort verschlüsselt zu übertragen (wenn Ihre Firma dies erlaubt z.B. durch die Verwendung eines sicheren Kurznachrichtendienstes wie etwa Threema, Signal, etc.).
- Im Arbeitskontext verwenden Sie soweit möglich dafür nur Geräte, die Ihnen Ihr Arbeitgeber zur Verfügung stellt.
- Teilen Sie ein Passwort mit einer anderen Person, sollten Sie es in jedem Fall ändern sobald der Notfall abgeschlossen ist.

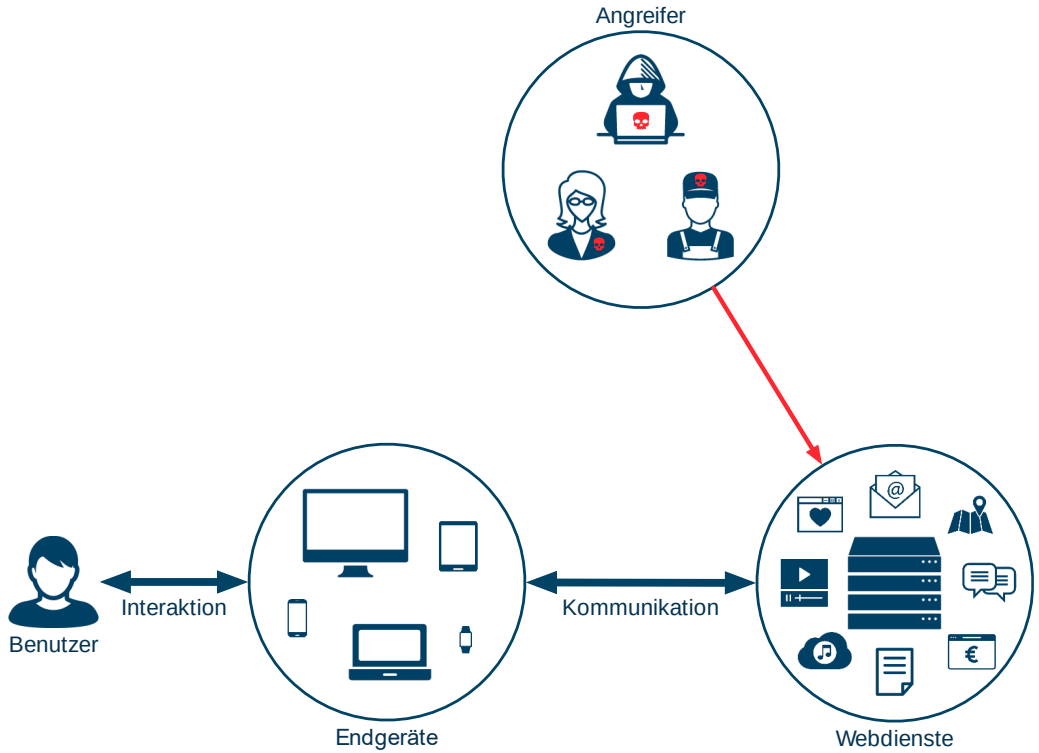
Weitere Hinweise zum Angriff „Unverschlüsselte elektronische Notiz entwenden“

Analog zum Brief kann es vorkommen, dass Ihnen Passwörter per elektronischer Nachricht (z.B. E-Mail) zugestellt werden.

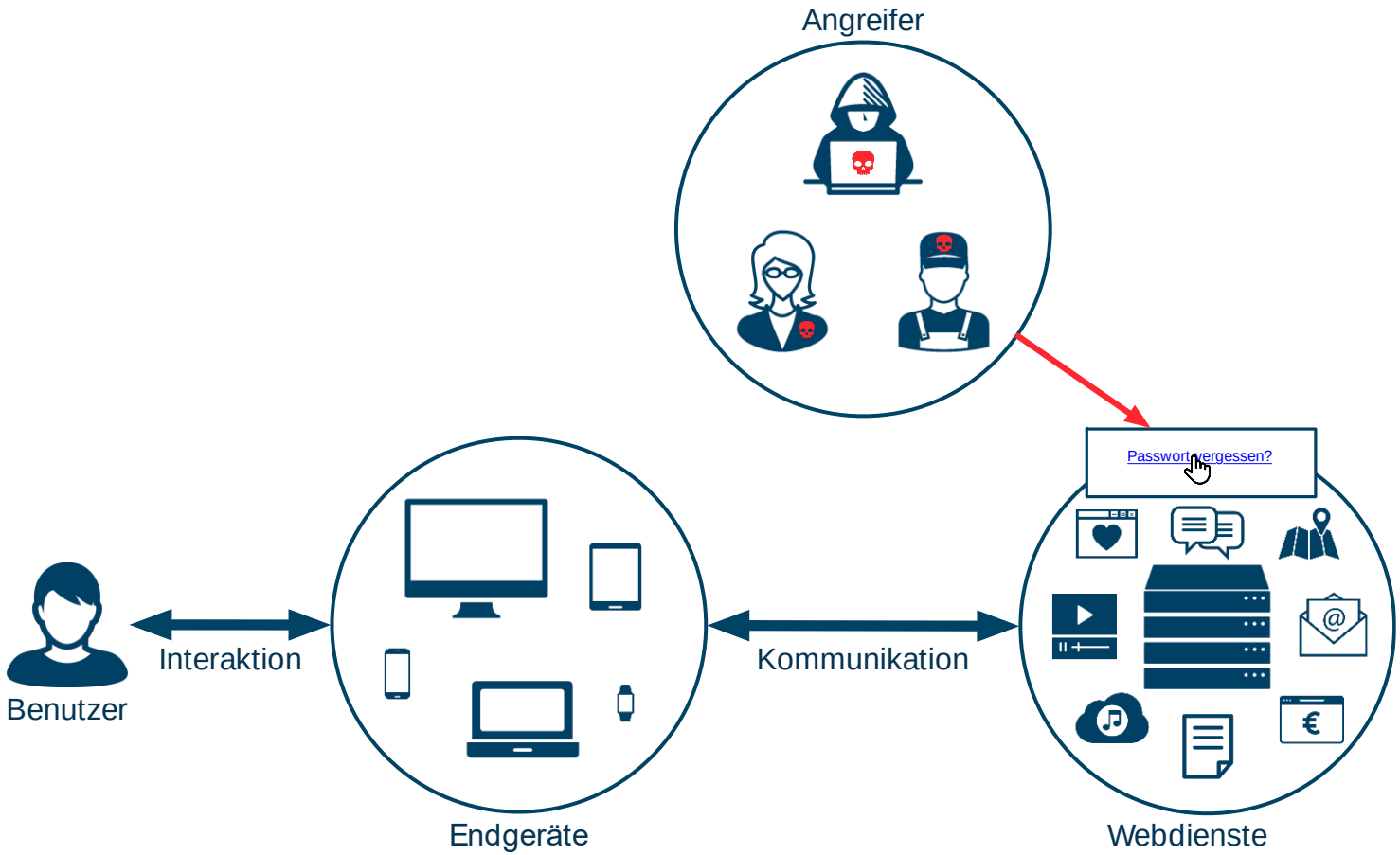
- Werden E-Mails unverschlüsselt versendet, kann der Angreifer schon unterwegs zuschlagen, ohne dass Sie dies merken.
- Unverschlüsselt versendete Passwörter sollten Sie stets schnellstmöglich ändern.

Angriffe, die bei Webdiensten ansetzen

Im Folgenden werden Ihnen die Angriffe vorgestellt, bei denen der Angreifer ausschließlich bei den von Ihnen verwendeten Webdiensten ansetzt.



Angriff (11/11): „Schwachen Reset-Mechanismus ausnutzen“



Beschreibung des Angriffs „Schwachen Reset-Mechanismus ausnutzen“

Der Angreifer versucht einen unsicheren Reset-Mechanismus auszunutzen.

- Wurde ein Passwort vergessen, kann oftmals mittels eines sogenannten Reset-Mechanismus der Zugang zum entsprechenden Benutzerkonto wiederhergestellt werden.
- Bietet der Reset-Mechanismus keinen angemessenen Schutz, hilft das beste Passwort nichts, da die Gesamtsicherheit Ihres Benutzerkontos auf das Sicherheitsniveau des Reset-Mechanismus heruntergesetzt wird.
- Der Angreifer erhält auf diese Weise Zugriff auf Ihr Benutzerkonto, ohne dass er das Passwort kennt.

Abwehr des Angriffs „Schwachen Reset-Mechanismus ausnutzen“

Um diesen Angriff abzuwehren, müssen Sie sich zunächst darüber im Klaren sein, welche Reset-Mechanismen verwendet werden. Häufig anzutreffende Möglichkeiten sind

1. Zuschicken eines Links oder Passworts per E-Mail
   - Das Passwort zum E-Mail-Account stellt den Grundpfeiler der Sicherheit dieses Accounts dar.
   - Ist es nicht angemessen sicher gewählt, kann ein Angreifer durch den Reset-Mechanismus Zugriff auf andere Accounts erlangen.
   - Sollte Ihnen ein Webdienst ein neues Passwort in einer unverschlüsselten E-Mail zuschicken, sollten sie dieses sofort beim nächsten Login ändern.

Missverständnis #25: Selbst wenn Sie es nur nutzen, um Nachrichten zu verschicken, stellt Ihr E-Mail-Benutzerkonto in vielerlei Hinsicht ein lohnendes Ziel für Angreifer dar. Das Ausnutzen der Fähigkeit Passwörter zurückzusetzen ist hierbei besonders relevant. In ihrem E-Mail-Benutzerkonto liegen Nachrichten von allen Webdiensten, bei denen Sie sich registriert haben. So kann der Angreifer alle Webdienste im Konto durchgehen und darauf zugreifen.

Abwehr des Angriffs „Schwachen Reset-Mechanismus ausnutzen“

2. Sicherheitsfragen
   - In diesem Fall werden häufig Fragen zur Auswahl gestellt, die persönliche Daten abfragen (z.B. Mädchenname der Mutter).
   - Dies stellt einen besonders problematischen Reset-Mechanismus dar.
   - Sie sollten stets große Vorsicht walten lassen, welche Fragen Sie wählen und wie Sie diese beantworten.
   - Machen Sie sich klar, ob die Antworten zu den Fragen womöglich an anderer Stelle im Internet verfügbar sind oder welche Personen aus Ihrem Umfeld die Antworten zu diesen Fragen kennen.
   - Die beste Lösung, um mit Sicherheitsfragen umzugehen ist es, sich zufällige Antworten ausdenken und diese für den Fall, dass Sie das Passwort zurücksetzen müssen, sicher zu Hause zu verwahren oder in einem Passwortmanager zu speichern.

Modul 2

Technologien im Kontext Ihrer Benutzerkonten

In diesem Modul wird erklärt, auf welche Technologien Sie beim Schutz Ihrer Benutzerkonten treffen können

Aufbau dieses Moduls

Es gibt einige Technologien, die Sie beim Schutz Ihrer Benutzerkonten unterstützen können. In diesem zweiten Modul der Schulung werden Ihnen Technologien mit den jeweiligen Vor- und Nachteilen vorgestellt. Die Reihenfolge der Technologien ist kein Indikator für deren Wichtigkeit, die Technologien sind alphabetisch geordnet:

1. Fingerabdrucksensoren
2. Graphische Passwörter
3. Hardware Tokens
4. Passwortmanager
5. Sichtschutzfolien
6. Single-Sign-On
7. Zwei-Faktor-Authentifizierung

Wenn Sie das Gefühl haben mit einer Technologie bereits ausreichend vertraut zu sein, können Sie deren Beschreibung überspringen.

Technologie 1: Fingerabdrucksensoren

Fingerabdrucksensoren erlauben es ein reguläres Text-Passwort mit Ihrem Fingerabdruck als biometrischem Merkmal zu ersetzen.

- Immer mehr Geräte (insbesondere Smartphones) werden mit einem Fingerabdrucksensor ausgeliefert.
- Ein Fingerabdrucksensor kann die Abdrücke Ihrer Finger im Sensor speichern und erlaubt es die Eingabe Ihres Passwortes durch das Berühren des Sensors oder Wischen über den Sensor mit einem Finger zu ersetzen.
- Oftmals (z.B. bei Touch ID, dem Fingerabdrucksensor in Geräten der Firma Apple) wird das Passwort jedoch nicht vollständig ersetzt, sondern beibehalten, um ein Einloggen auch dann zu ermöglichen, wenn der Sensor einen Defekt aufweisen sollte oder Sie sich am entsprechenden Finger verletzen.

Vorteile und Nachteile der Technologie „Fingerabdrucksensoren“

Vorteile

- Die Benutzung eines Fingerabdrucksensors kann deutlich schneller sein als die Eingabe eines Passwortes, wodurch im Alltag Zeit gespart werden kann.
- Ein Fingerabdrucksensor schützt vor Beobachtungsangriffen, da sich ein Angreifer auch nach dem Beobachten (oder sogar Aufzeichnen) des Vorgangs nicht anmelden kann.

Nachteile

- Fingerabdrucksensoren vereinfachen Kopier-Angriffe. In der Regel hinterlassen Sie auf allen Dingen, die Sie mit Ihren Fingern berühren, Ihre Abdrücke. Auch hochauflösende Photos reichen aus, um eine Kopie Ihres Fingerabdrucks zu erstellen. Mit einer solchen Kopie kann der Angreifer sehr effizient gezielte „Rate“-Angriffe durchführen.
- Das Ändern des eigenen Fingerabdruckes ist nicht möglich, wenn er in die Hände eines Angreifers fällt.
- Ihre Fingerabdrücke müssen im Gerät gespeichert werden.
- Kann ein Angreifer Ihr Endgerät stehlen, erhält er potentiell Ihre Fingerabdrücke auf der Oberfläche des Geräts direkt mit dazu.

Hinweise zum Anwenden der Technologie „Fingerabdrucksensoren“

Fingerabdrucksensoren sind besonders dann einfach einzusetzen, wenn Sie bereits in Geräte integriert sind.

- Häufig haben neuere Smartphones heutzutage integrierte Fingerabdrucksensoren.
- Auch Laptops sind mit Fingerabdrucksensoren verfügbar.
- Die Einrichtung unterscheidet sich von Hersteller zu Hersteller und von Gerät zu Gerät, ist aber in der Regel einfach möglich und im Zweifelsfall auch in den Handbüchern bzw. auf den Hilfe-Seiten des Herstellers beschrieben.
- Je nach Umsetzung des Fingerabdrucksensors im Gerät kann dieser auch andere Passwörter auf Ihrem Gerät ersetzen (z.B. die Anmeldung am PC/Laptop, das Smartphone entsperren oder auf die Passwörter in einem Passwortmanager zugreifen).
- Vorsicht ist bei anderen biometrischen Verfahren (wie z.B. der Gesichtserkennung und Iris-Scannern) geboten. Die Varianten dieser Technologien in für Verbraucher vorgesehener Hardware (z.B. Smartphones) bieten oftmals nur einen ungenügenden Schutz.
- Wenn Sie einen Fingerabdrucksensor bei einem Gerät im Unternehmen einsetzen möchten, klären Sie dies zunächst mit der IT-Abteilung ab.

Technologie 2: Graphische Passwörter

Graphische Passwörter sind eine Alternative zu Text-Passwörtern und können diese ersetzen:

- Graphische Passwörter sind anstatt aus Buchstaben aus graphischer Information aufgebaut.
- Die bekanntesten Vertreter dieser Technologie sind
  - die Muster-Sperre in Android, bei der ein Muster in einem Raster von Punkten eingegeben werden muss.
  - das graphische Passwortsystem in Windows (ab Windows 8 verfügbar), bei dem bestimmte Punkte auf einem Bild angeklickt werden müssen, um das Passwort einzugeben.
- Graphische Passwörter ändern das Sicherheitsniveau nicht. Sie sind genauso anfällig bzw. widerstandsfähig gegen die verschiedenen Angriffe wie Text-Passwörter.

Vorteile und Nachteile der Technologie „Graphische Passwörter“

Vorteile

- Graphische Information wird im menschlichen Gehirn anders gespeichert als Text und andere abstrakte Informationen. Daher sind graphische Passwörter im Allgemeinen deutlich einfach zu merken und erinnern.

Nachteile

- Je nach verwendetem graphischen Passwortsystem kann die Eingabe deutlich länger dauern als bei normalen Passwörtern, was das Beobachten der Eingabe für einen Angreifer vereinfachen kann.
- Graphische Passwörter sind in der Regel nicht mit Passwortmanagern kompatibel.

Hinweise zum Anwenden der Technologie „Graphische Passwörter“

Graphische Passwörter sind dort, wo sie verfügbar sind, sehr einfach einzurichten. Zusätzlich sollten Sie aber folgende Hinweise beachten:

- Ein Wechsel zwischen Text-Passwörtern und graphischen Passwörtern ist in der Regel problemlos möglich.
- Auch bei graphischen Passwörtern ist es möglich einfach zu ratende Passwörter zu erstellen
  - Bei der Android Mustersperre sollten Sie möglichst keine symmetrischen Muster wählen und nicht in einer der Ecken (insbesondere der linken oberen) anfangen.
  - Bei Passwortverfahren, wie dem in Windows 8 eingebauten, sollten Sie es vermeiden folgende Dinge als Klickpunkte zu wählen, da diese von Benutzern besonders häufig gewählt werden und somit auch von Angreifern zuerst probiert werden:
    - Gesichter von Personen auf den Bildern
    - Rote Gegenstände
    - Ecken und die Mitte von Gegenständen

Technologie 2: Hardware Tokens

Hardware Tokens sind eine weitere Alternative zu Text-Passwörtern und können diese ersetzen:

- Anstatt ein Textpasswort einzugeben, müssen Sie bei der Benutzung eines Hardware Tokens diesen mit sich führen und für den Login nutzen.
- Hardware Tokens ersetzen Ihr bisheriges Passwort, aber nicht etwaige Reset-Mechanismen, die auch Zugriff auf Ihr Benutzerkonto ermöglichen (folglich Angriff 11 im Modul „Angriffe auf Benutzerkonten“)
- Hardware Tokens werden in verschiedenen Formaten angeboten, z.B.:
  - Als USB-Stick, der zum Login eingesteckt werden muss. Solche Hardware Tokens sehen aus wie USB-Speicher-Sticks, bieten aber keine Möglichkeit Daten zu speichern. Sie dienen ausschließlich als Ersatz für das Text-Passwort und werden in einen USB-Port gesteckt, wenn Sie normalerweise das Passwort eingeben müssten.
  - Integriert in andere Geräte (z.B. Smartwatches). Diese Lösung nutzt Hardware, die Sie sowieso mit sich führen.
  - Spezielle Chipkarten. Diese Lösungen benötigen spezielle Chipkarten-Lesegeräte und werden vornehmlich in Unternehmen eingesetzt.

Vorteile und Nachteile der Technologie „Hardware Tokens“

Vorteile

- Ein Hardware Token schützt Sie vor Beobachtungsangriffen, da sich ein Angreifer auch nach dem Beobachten (oder sogar Aufzeichnen) des Vorgangs nicht anmelden kann.
- Rate-Angriffe werden durch die Benutzung eines Hardware Tokens deutlich erschwert, da der Token das Textpasswort durch ein langes und vollkommen zufälliges Geheimnis ersetzt, das auf dem Token gespeichert ist und nicht ohne weiteres ausgelesen werden kann.
- Je nach Konfiguration ersetzt der Token das Textpasswort vollständig und Sie müssen es sich nicht merken oder es erinnern.

Nachteile

- Wird Ihnen der Hardware Token gestohlen, kann der Angreifer sich in Ihrem Namen einloggen. Mache Hardware Tokens können so konfiguriert werden, dass zusätzlich auch eine PIN oder ein Textpasswort eingegeben werden muss. Diese müssen Sie sich dann aber merken und für das Einloggen eingeben.
- Den Hardware Token müssen Sie beim Einsatz unterwegs (z.B. Laptop auf Reisen) stets mitführen.

Hinweise zum Anwenden der Technologie „Hardware Tokens“

Hardware Tokens bedürfen häufig etwas Aufwand in der Einrichtung. Im Unternehmen wird dies aber die IT-Abteilung für Sie übernehmen:

- Wenn Ihr Unternehmen die Nutzung eines Hardware Tokens nicht vorschreibt, klären Sie zunächst mit der IT-Abteilung die Nutzung ab.
- Je nach Betriebssystem und verwendetem Hardware Token kann es nötig sein zusätzliche Software für die Einrichtung des Hardware Tokens zu installieren. Im Unternehmen wenden Sie sich dazu an die IT-Abteilung. Im privaten Kontext finden Sie umfangreiche Dokumentation auf den Webseiten der Hersteller.
- Neben dem Login am PC/Laptop bieten viele Hardware Tokens auch die Möglichkeit Sie im Zuge von Zwei-Faktor-Authentifizierung zu nutzen (diese Technologie wird später in diesem Modul beschrieben).

Technologie 3: Passwortmanager

Passwortmanager sind Software, die Ihnen bei der Erstellung und der Verwaltung Ihrer Passwörter helfen kann.

- Passwortmanager können für Sie die Wahl und Verwaltung Ihrer Passwörter übernehmen.
- Sie stellen eine einfache Möglichkeit dar Passwörter verschlüsselt zu speichern.
- Es gibt sie als eigenständige Software oder integriert in Browser (wenn dieser Ihnen anbietet Passwörter zu speichern).
- Es gibt sie sowohl für Desktop-Plattformen (Windows, Mac OS, Linux, etc.) als auch für mobile Plattformen (Android, iOS, Windows Phone/Mobile, etc.).
- Oftmals ist es auch möglich Ihre Passwörter auf mehreren Geräten zu synchronisieren.
- Passwortmanager sind eine der effektivsten Möglichkeiten, um der Vielzahl von Angriffen auf Passwörter und Benutzerkonten zu begegnen.
- Die meisten IT-Sicherheits-Experten vertrauen Passwortmanagern ihre Passwörter an, um diese sicher zu verwalten.

Vorteile und Nachteile der Technologie „Passwortmanager“

Vorteile

- Ein Passwortmanager erlaubt es Ihnen für jedes Benutzerkonto ein neues und sicheres Passwort zu wählen. Er nimmt Ihnen das Merken der Passwörter ab. Viele Passwortmanager bieten zudem die Möglichkeit beliebig lange, sichere Passwörter zu generieren und für Ihre Benutzerkonten zu nutzen. Wird diese Möglichkeit genutzt, sind alle diese Benutzerkonten gegen Rate-Angriffe (d.h. Gezieltes Raten, Ungezieltes Raten, Raten nach Einbruch ins System) geschützt.
- Es oft auch möglich ein Add-On in Ihrem Internet-Browser (Firefox, Chrome, Safari, Internet Explorer, Opera, etc.) zu installieren. Dies ist ein kleines zusätzliches Programm, welches Ihren Browser erweitert und die Passwörter automatisch auf bekannten Webseiten eintragen kann. Dies schützt Sie gegen den Angriff „Über die Schulter blicken“.
- Zudem werden auf betrügerischen Webseiten die Passwörter nicht eingetragen, da zu den Passwörtern die entsprechende Webadresse gespeichert wird. Dies hilft beim Erkennen und Abwehren von Angriffen mit gefährlichen Nachrichten und Links (z.B. Phishing).

Vorteile und Nachteile der Technologie „Passwortmanager“ - *Fortsetzung*

Nachteile

- Passwörter müssen immer verschlüsselt gespeichert werden. Sind nicht alle der folgenden Kriterien erfüllt, müssen Sie unbedingt ein starkes Master-Passwort setzen:
  - Nur Sie verwenden Ihre Endgeräte (auf denen der Passwortmanager installiert ist).
  - Sie haben die Festplatte Ihres Endgerätes verschlüsselt.
  - Sie synchronisieren Ihre Passwörter nicht auf andere Endgeräte.
  - Sie sperren Ihr Endgerät, wenn Sie es nicht verwenden.

  Sind diese Kriterien erfüllt, sollten Sie ein Master-Passwort setzen, müssen es aber nicht zwangsläufig tun. Die meisten Passwortmanager erfordern jedoch immer ein Master-Passwort vom Benutzer.
- Müssen Sie ein Master-Passwort setzen und vergessen es, können Sie auf Ihre Passwörter eventuell nicht mehr zugreifen.

Hinweise zum Anwenden der Technologie „Passwortmanager“

Beim Einsatz eines Passwortmanagers sollten Sie die folgenden Dinge beachten:

- Sie müssen sich für einen geeigneten Passwortmanager entscheiden. Testberichte und Einschätzungen zu verschiedenen Passwortmanagern finden Sie in der Fachpresse. Da sich Passwortmanager in Ihren Funktionen und dem Aussehen teils stark unterscheiden, sollten Sie sich Zeit nehmen, um den für Sie passenden zu finden.
- Wenn für Sie vornehmlich Passwörter von Benutzerkonten auf Webseiten relevant sind, können Sie auch in Betracht ziehen die Passwörter in Ihrem Browser zu speichern. Andernfalls kann ein eigenständiges Passwortmanager-Programm mit einem passenden Browser-Add-On die bessere Wahl sein.
- Wenn Sie ein Master-Passwort wählen müssen, sollten Sie hier ein Passwort wählen, welches mindestens 20 Zeichen lang ist, z.B. durch das Aneinanderreihen mehrerer Wörter.

Hinweise zum Anwenden der Technologie „Passwortmanager“ *- Fortsetzung*

- Sollten Sie beim Hinzufügen auf Passwörter stoßen, die einfach geraten werden können, ersetzen Sie diese gleich. Bietet der Passwortmanager einen Passwortgenerator, verwenden Sie diesen.
- Sollten Sie ein neues Benutzerkonto bei einem Dienst eröffnen, nutzen Sie am besten den Passwort-Generator des Passwortmanagers, um ein angemessen sicheres Passwort zu erzeugen.
- Wenn Sie ein im Passwortmanager gespeichertes Passwort benötigen, um es auf einer Webseite oder in einem Programm einzugeben, können Sie es aus dem Passwortmanager herauskopieren. Einige Passwortmanager bieten sogar die Möglichkeit als Tastatur zu fungieren und Ihre Passwörter direkt in beliebige Programme einzutippen.
- Wenn Sie Ihre Passwörter direkt im Internet-Browser speichern oder ein zu Ihrem Passwortmanager passendes Add-On installiert haben, werden die Passwörter zu den entsprechenden Webseiten noch bequemer zugänglich.
- Sollten Sie einmal ein Benutzerkonto schließen, müssen Sie dieses auch aus dem Passwortmanager löschen.

Technologie 4: Sichtschutzfolien

Sichtschutzfolien können helfen sensible Inhalte auf dem Display Ihres Endgerätes zu schützen:

- Sichtschutzfolien werden an Laptop-Bildschirmen oder auf Displays von Mobilgeräten (Smartphone, Tablet, etc.) angebracht.
- Sie verringern den Sichtwinkel, aus dem Inhalte auf dem Bildschirm bzw. Display einsehbar sind.
- Sie reduzieren die Gefahr, dass Personen, die neben Ihnen stehen oder sitzen (z.B. im Zug), sehen, was gerade auf Ihrem Gerät angezeigt wird.
- Bei mobilen Geräten werden die einzelnen Buchstaben bei der Passworteingabe kurz im Klartext angezeigt, bevor sie durch ein anderes Symbol (meistens Stern oder Kreis) ersetzt werden. Mit einer guten Sichtschutzfolie ist die Gefahr, dass ein Sitznachbar im Zug das Passwort erspähen kann, deutlich geringer.

Vorteile und Nachteile der Technologie „Sichtschutzfolien“

Vorteile

- Sichtschutzfolien verringern die Gefahr von Shoulder-Surfing-Angriffen (über die Schulter blicken).

Nachteile

- Sichtschutzfolien können (je nach Hersteller und Produktart) insgesamt zu einer dunkleren Darstellung von Inhalten auf dem Bildschirm bzw. Display Ihres Gerätes führen.
- Sichtschutzfolien können (je nach Hersteller und Produktart) das Gefühl beim Bedienen von Touchscreens verändern.
- Wird eine dunklere Darstellung mit einer höheren Bildschirm-Helligkeit kompensiert, kann dies zu einem erhöhten Stromverbrauch (und entsprechend einer geringeren Akkulaufzeit) führen.

Hinweise zum Anwenden der Technologie „Sichtschutzfolien“

Sichtschutzfolien für verschiedene Geräte erhalten Sie im gut sortierten Fachhandel und in Online-Shops.

- Achten Sie genau darauf, dass die Sichtschutzfolie auch zu Ihrem Gerät passt, sonst können Teile des Bildschirms ungeschützt bleiben.
- Es gibt zwischen Herstellern teils große Unterschiede bezüglich der Schutzwirkung (d.h. des Winkels aus dem der Bildschirm unter Einsatz der Folie noch einsehbar ist). Informieren Sie sich hier in der Fachpresse oder im Fachhandel.
- Es gibt zwei Typen von Sichtschutzfolien, jedoch sind nicht immer beide Typen für alle Endgeräte verfügbar:
  1. Der erste Typ ist selbsthaftend und wird komplett auf den Bildschirm geklebt.
  2. Dem zweiten Typ liegen spezielle doppelseitige Klebestreifen zur Befestigung bei, sodass die Folie ohne Probleme entfernt und wieder befestigt werden kann.
- Wenn Sie eine Sichtschutzfolie für ein Gerät im Unternehmen einsetzen möchten, klären Sie dies zunächst mit der IT-Abteilung ab.

Technologie 5: Single-Sign-On

Single-Sign-On beschreibt die Möglichkeit sich nicht mithilfe eines Passwortes bei einem Webdienst anzumelden, sondern durch ein Benutzerkonto bei einem anderen, sogenannten Single-Sign-On-Dienst.

- Der Single-Sign-On-Dienst bürgt bei anderen Webdiensten für Ihre Identität.
- Einloggen müssen Sie sich nur noch beim Single-Sign-On-Dienst. Dieser gibt ihr Passwort nicht an andere Webdienste weiter, sondern loggt Sie direkt beim anderen Webdienst ein.
- Diese Art des Logins findet man häufig im betrieblichen Umfeld, ist aber auch im privaten Kontext möglich.
- Viele soziale Netzwerke bieten Single-Sign-On-Dienste für den privaten Kontext an (z.B. Facebook Connect oder Google+ Login).
- Eine Vielzahl an Webseiten bieten die Option an Single-Sign-On im privaten Umfeld zu nutzen (z.B. Airbnb, Pinterest und viele weitere).
- Beim Nutzen von Single-Sign-On-Diensten ist es umso wichtiger, dass das Passwort für den Single-Sign-On-Dienst sicher gewählt ist, da es Zugriff auf andere Konten gewährt.

Vorteile und Nachteile der Technologie „Single-Sign-On“

Vorteile

- Durch die Nutzung von Single-Sign-On entfällt die Wahl und das Verwalten der Passwörter für Benutzerkonten, bei denen Sie sich über einen Single-Sign-On-Dienst anmelden.
- Single-Sign-On spart Ihnen beim Einloggen potentiell Zeit, da Sie sich nur noch beim Single-Sign-On-Dienst einloggen müssen. Sind Sie dort bereits eingeloggt, nimmt der Login bei anderen Webdiensten keine zusätzliche Zeit in Anspruch.
- Die Erstellung von Benutzerkonten bei neuen Diensten kann schneller gehen, wenn man die dafür benötigten Daten (z.B. E-Mail-Adresse, o.ä.) nicht erst einzeln eingeben muss, sondern diese aus dem Single-Sign-On-Dienst übernommen werden können.

Vorteile und Nachteile der Technologie „Single-Sign-On“ - *Fortsetzung*

Vorteile

- Nur beim Single-Sign-On-Anbieter wird ein Passwort gewählt und gespeichert. Daher sind Ihre Benutzerkonten bei anderen Webdiensten, bei denen Sie Single-Sign-On zum Anmelden nutzen, automatisch vor verschiedenen Angriffen geschützt:
  - Rate-Angriffe (d.h. Gezieltes Raten, Ungezieltes Raten, Raten nach Einbruch ins System) sind nicht möglich, da es bei den Webdiensten kein Passwort gibt, dass erraten werden könnte. Hinweis: Das Passwort beim Single-Sign-On-Dienst kann jedoch weiterhin erraten werden und sollte besonders sicher gewählt werden.
  - Da es kein Passwort gibt, dass zurückgesetzt werden könnte, sind auch Angriffe auf den Reset-Mechanismus nicht möglich.

Vorteile und Nachteile der Technologie „Single-Sign-On“ - *Fortsetzung*

Nachteile

- Nutzen Sie Single-Sign-On, sind Sie auf den entsprechenden Single-Sign-On-Dienst angewiesen, um sich einzuloggen. Fällt der Single-Sign-On-Dienst aus, können Sie sich bei keinem anderen Benutzerkonto einloggen, für das Sie diesen Single-Sign-On-Dienst nutzen. Gleiches gilt, wenn ihr Benutzerkonto beim Single-Sign-On-Dienst gesperrt wird.
- Bei den meisten Single-Sign-On-Diensten können Sie immer nur dieselben Daten bei der Erstellung eines neuen Benutzerkontos nutzen (d.h. es ist nicht möglich verschiedene E-Mail-Adressen für verschiedene Benutzerkonten zu verwenden, wenn Sie für diese den gleichen Single-Sign-On-Dienst verwenden).
- Der Single-Sign-On-Dienst kann Ihre Online-Aktivität nachvollziehen, da er weiß, wann Sie sich wo einloggen (solange der Login über den Single-Sign-On-Dienst geschieht).
- Ist der Single-Sign-On-Dienst Opfer eines Einbruchs in die Systeme, kann ein Angreifer potentiell auf alle Ihre Benutzerkonten zugreifen, bei denen Sie den Single-Sign-On-Dienst nutzen.

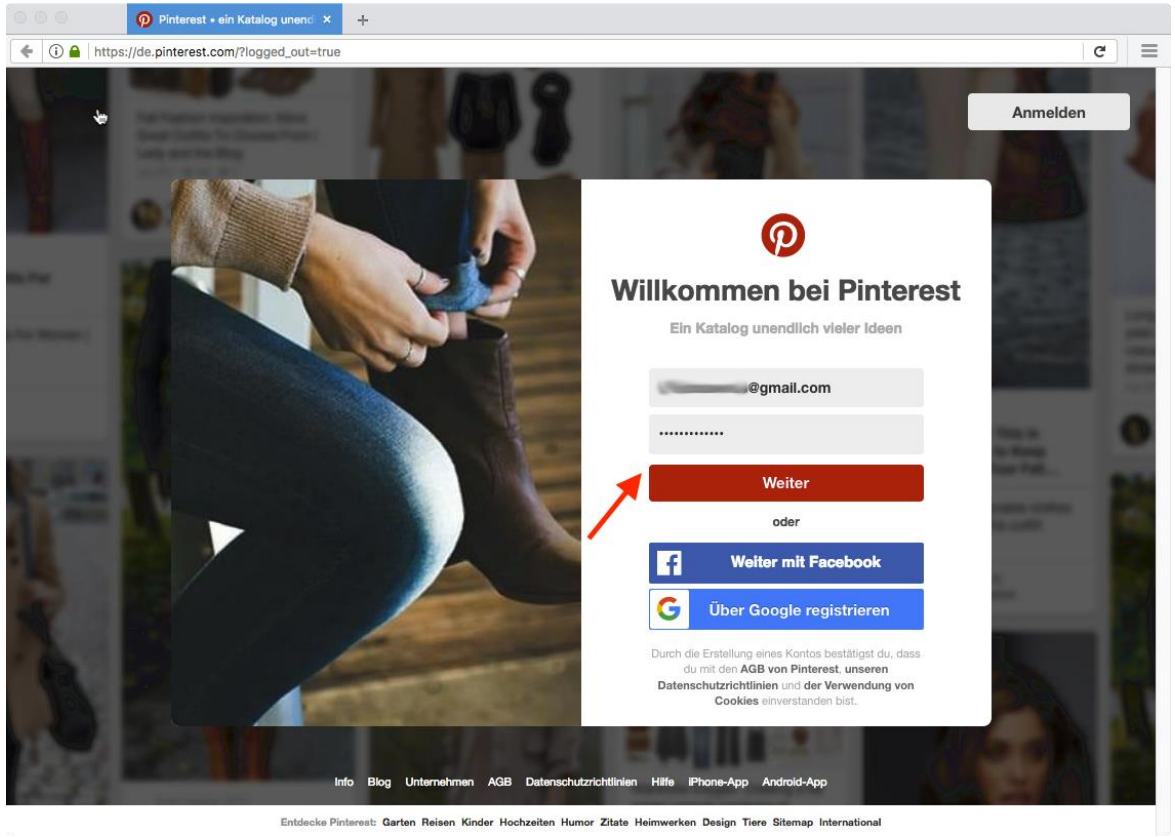
Hinweise zum Anwenden der Technologie „Single-Sign-On“

Ist Single-Sign-On erst einmal eingerichtet, kann es eine sehr bequeme Technologie darstellen.

- Wird Single-Sign-On in Unternehmen eingesetzt, ist dessen Nutzung vorgeschrieben und sie haben häufig nicht die Wahl es einzusetzen oder nicht. Dann übernimmt die IT-Abteilung die Einrichtung für Sie.
- Wenn Sie Fragen zu Single-Sign-On im Unternehmens-Kontext haben, sollten Sie sich an die IT-Abteilung Ihres Unternehmens wenden.
- Im privaten Umfeld können Sie selbst entscheiden, ob Sie einen Single-Sign-On-Dienst nutzen möchten.
- Viele Webseiten bieten diese Möglichkeit mittlerweile an. Die am häufigsten unterstützten Single-Sign-On-Dienste sind Facebook und Google.
- Häufig ist ein Umstieg auf Single-Sign-On nachträglich möglich. Dazu müssen Sie das Benutzerkonto, für welches Sie Single-Sign-On nutzen möchten, mit Ihrem Benutzerkonto beim gewünschten Single-Sign-On Dienst verbinden. Dies können Sie über die Einstellungen zu Ihrem Benutzerkonto durchführen. Es kann sinnvoll sein das Passwort, welches Sie mit Single-Sign-On ersetzen, zunächst auf einen zufälligen Wert zu setzen (und eine Notiz davon sicher zu verwahren), falls der Webdienst es nicht aus Ihrem Benutzerkonto löscht.

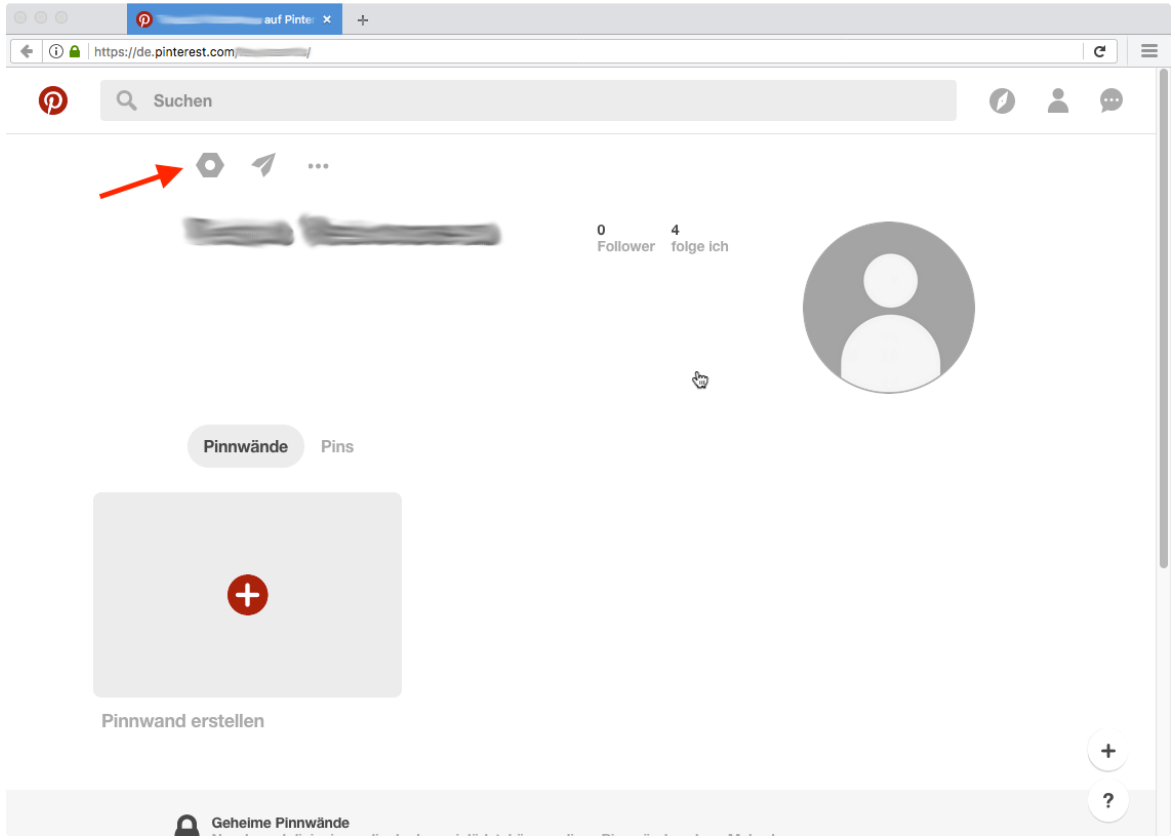
Hinweise zum Anwenden der Technologie „Single-Sign-On“ - *Fortsetzung*

Die Screenshots auf den folgenden sechs Seiten zeigen den Vorgang eines nachträglichen Einrichtens von Single-Sign-On beispielhaft für den Webdienst „Pinterest“, wobei Google als Single-Sign-On-Dienst eingerichtet wird. Schritt 1 – Login bei Pinterest:



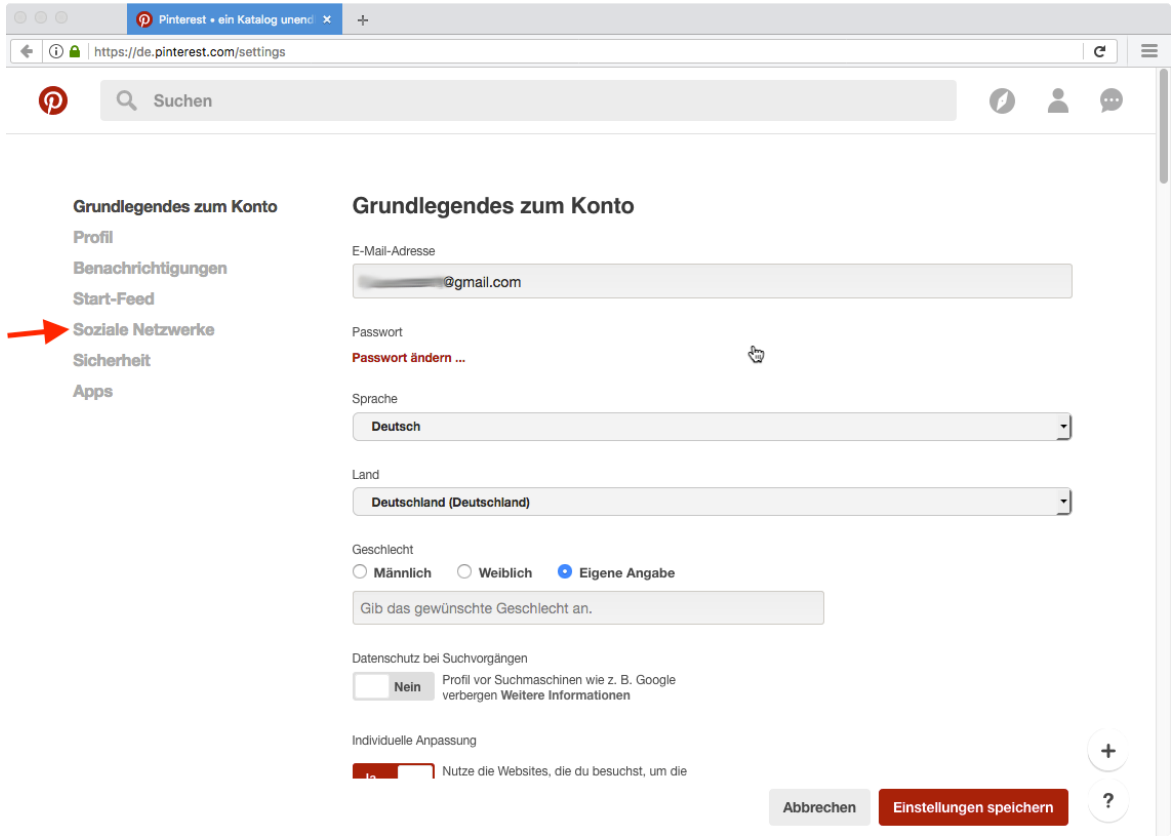
Hinweise zum Anwenden der Technologie „Single-Sign-On“ - *Fortsetzung*

Schritt 2 – Navigation in die Einstellungen:



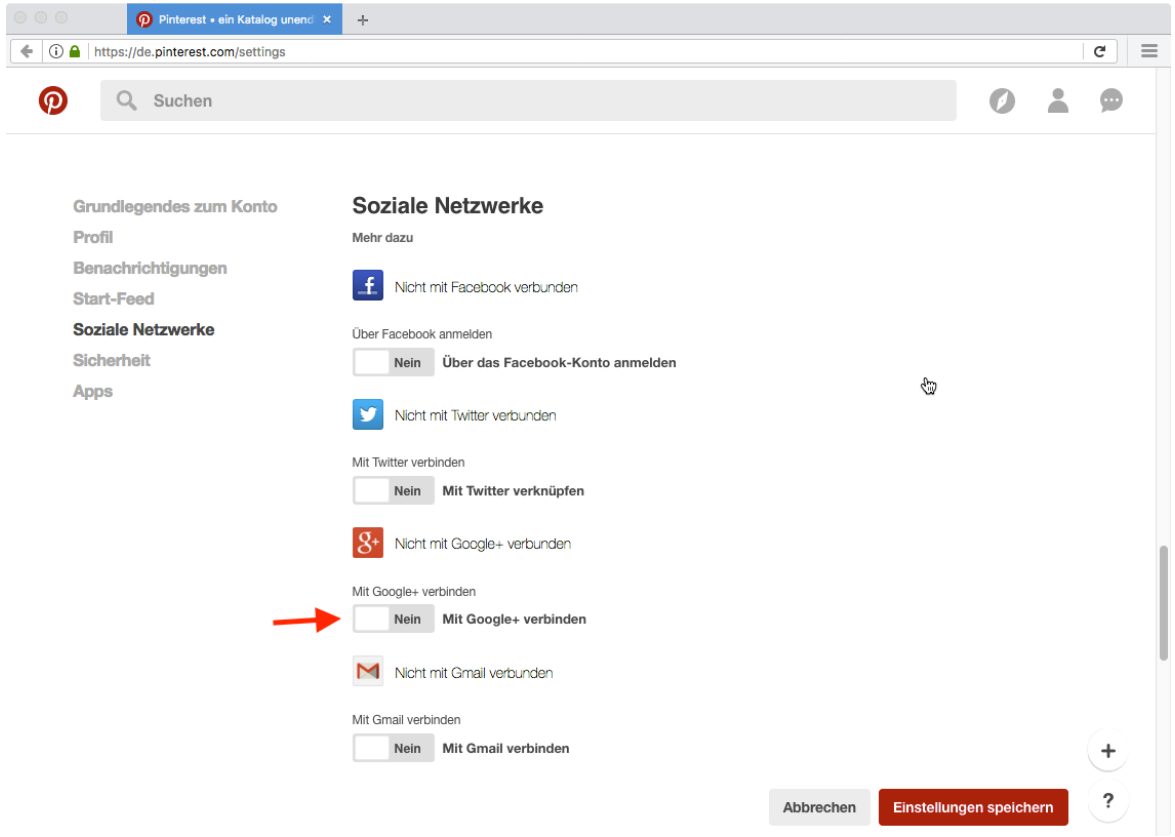
Hinweise zum Anwenden der Technologie „Single-Sign-On“ - *Fortsetzung*

Schritt 3 – Navigation zu den Single-Sign-On Optionen (diese werden teilweise auch als „Social Login“ bezeichnet, wenn ein soziales Netzwerk als Single-Sign-On-Dienst dient):



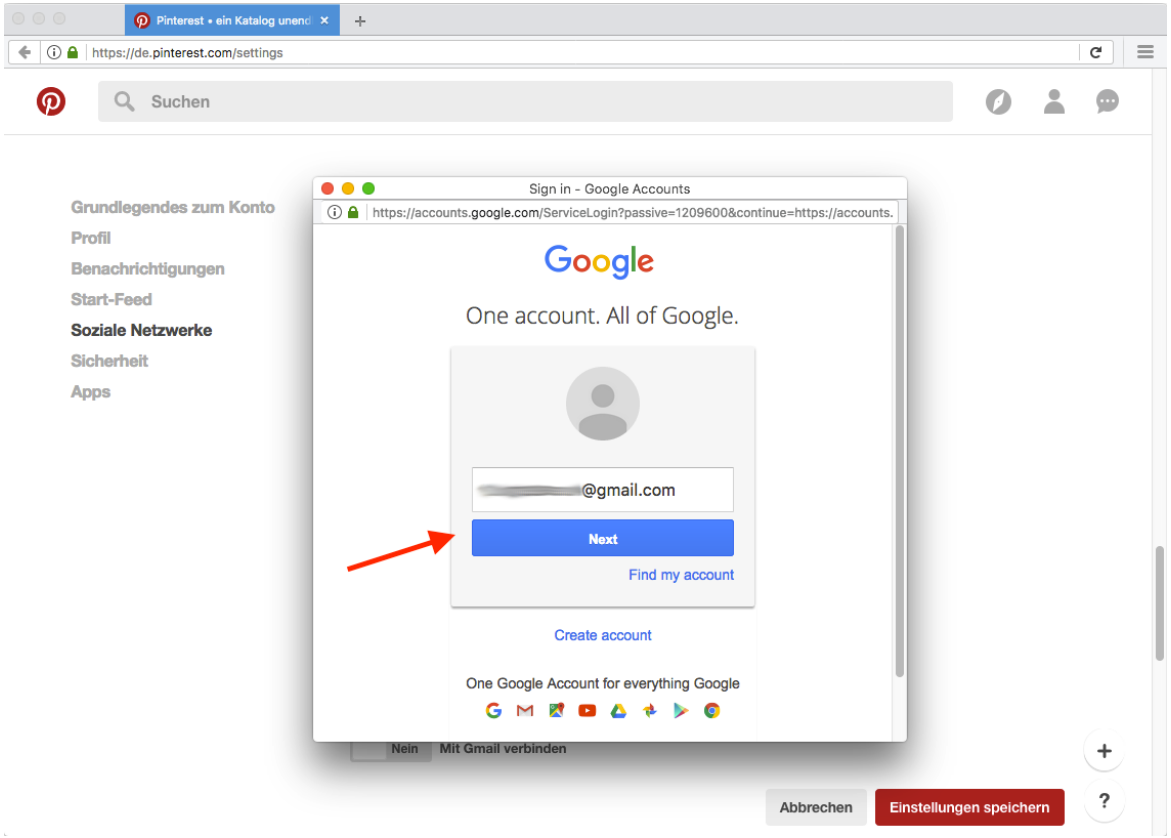
Hinweise zum Anwenden der Technologie „Single-Sign-On“ - *Fortsetzung*

Schritt 4 – Aktivieren des Logins per Google-Account:



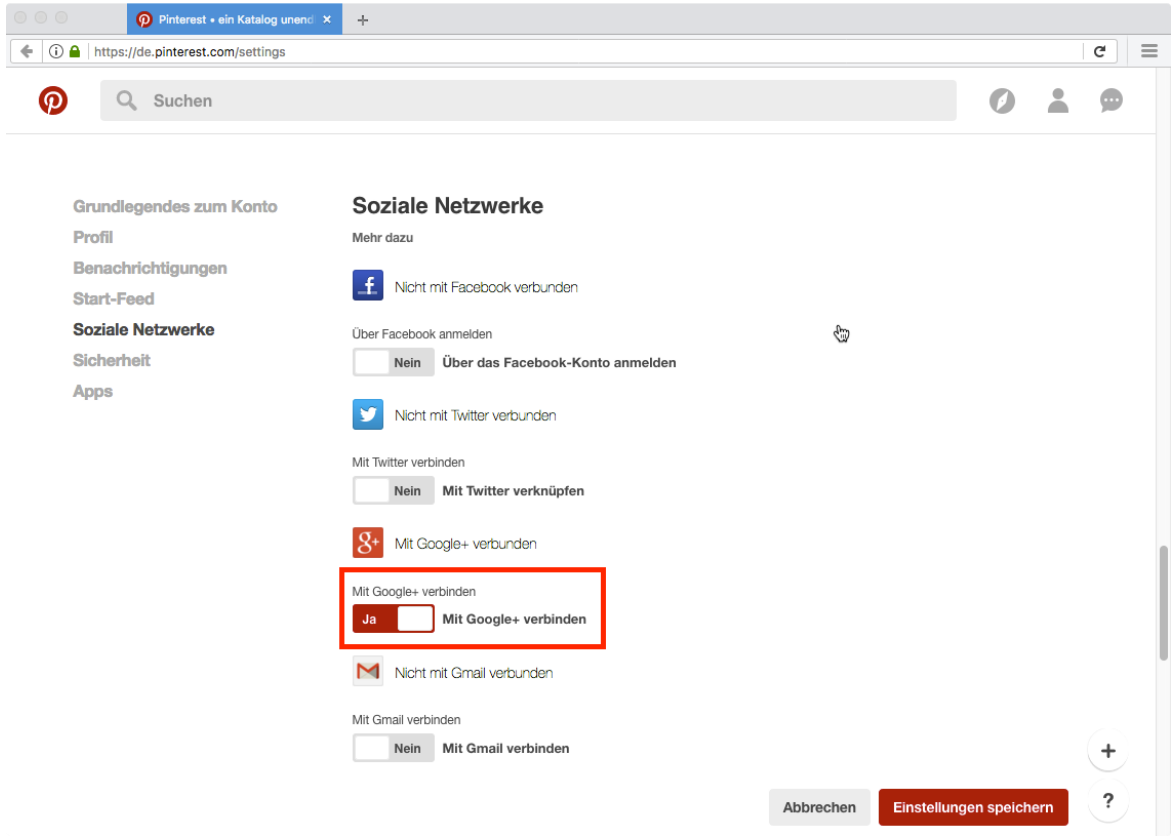
Hinweise zum Anwenden der Technologie „Single-Sign-On“ - *Fortsetzung*

Schritt 5 – Login bei Google, um zu bestätigen, dass Sie sich in Zukunft über Ihr Google-Benutzerkonto bei Pinterest einloggen möchten:



Hinweise zum Anwenden der Technologie „Single-Sign-On“ - *Fortsetzung*

Schritt 6 – Ihre Einstellungen bei Pinterest zeigen nun, dass Sie sich mit Google einloggen können:



Technologie 6: Zwei-Faktor-Authentifizierung

Zwei-Faktor-Authentifizierung ist eine Technologie, mit der Sie Ihre Benutzerkonten zusätzlich zum regulären Passwort absichern können.

- Im Bereich der Authentifizierung (also dem Beweisen der eigenen Identität) unterscheidet man drei verschiedene „Faktoren“:
    1. wissensbasierte (etwas, das Sie wissen, z.B. ein reguläres Text-Passwort)
    2. biometrische (etwas, das Sie sind, z.B. Ihr Fingerabdruck)
    3. besitzbezogene (etwas, das Sie besitzen, z.B. ein zusätzliches Gerät).
- Bei der Nutzung von Zwei-Faktor-Authentifizierung werden nicht nur einer, sondern zwei Faktoren für das Anmelden im entsprechend geschützten Benutzerkonto benötigt.
- Ein ähnliches Prinzip kennen Sie vermutlich aus dem Online-Banking, wo Sie neben dem Passwort noch TANs brauchen.
- Viele Firmen bieten Zwei-Faktor-Authentifizierung mittlerweile für ihre Webdienste an (z.B. Amazon, Google, Microsoft, Apple, Dropbox, Evernote, Yahoo, Ebay, Paypal, Facebook und viele andere), und es werden immer mehr.
- Theoretisch könnte es auch Drei-Faktor-Authentifizierung geben, aber dies ist sehr selten.

Vorteile und Nachteile der Technologie „Zwei-Faktor-Authentifizierung“

Vorteile

- Wenn Sie Zwei-Faktor-Authentifizierung nutzen, kann niemand auf Ihr Benutzerkonto zugreifen, der nur das Passwort besitzt.
- Experten sehen Zwei-Faktor-Authentifizierung als eine der effektivsten Methoden an, sich vor jedem der im ersten Modul vorgestellten Angriffe zu schützen.

Vorteile und Nachteile der Technologie „Zwei-Faktor-Authentifizierung“

Nachteile

- Der zweite Faktor (und/oder ein passendes Lesegerät für z.B. Fingerabdrücke oder Chipkarten) muss stets mitgeführt werden.
- Bei den meisten Lösungen für Webseiten wird ein Telefon für den Empfang von SMS oder ein Smartphone für die Installation einer App benötigt.
- Bei Unternehmenslösungen wird oftmals ein zusätzliches Gerät (z.B. RSA SecurID Token) benötigt.
- Zweit-Faktor-Authentifizierung schützt nicht vor Angriffen auf unsicher verwahrte Notizen (egal ob auf Papier oder elektronisch), wenn der zweite Faktor auch als Notiz verwahrt wird (Z.B. TAN-Liste) die unsicher verwahrte Notiz auf dem gleichen Gerät liegt wie der zweite Faktor (z.B. Login im Browser des Smartphones mit Code aus App als zweitem Faktor).
- Ist der zweite Faktor gestohlen oder verloren (oder wenn der zweite Faktor ein Smartphone ist, der Akku leer) kann nicht ohne zusätzlichen Aufwand auf das Konto zugegriffen werden.

Hinweise zum Anwenden der Technologie „Zwei-Faktor-Authentifizierung“

Wenn Sie Zwei-Faktor-Authentifizierung einsetzen wollen, sollten Sie die folgenden Punkte beachten:

- Schauen Sie zunächst, ob der gewünschte Dienst Zwei-Faktor-Authentifizierung anbietet. Eine einfache Websuche hilft hier weiter. Ein Verzeichnis mit vielen Webseiten, die Zwei-Faktor-Authentifizierung anbieten, stellt die Webseite https://twofactorauth.org/ (nur in Englisch verfügbar) dar.
- Im privaten Kontext werden Sie zur Einrichtung von Zwei-Faktor-Authentifizierung oftmals ein Smartphone benötigen. Halten Sie dieses bereit.
- Sollten Sie die Wahl zwischen Zwei-Faktor-Authentifizierung per SMS und per ChipTAN oder App haben, dann sollten Sie immer die anderen Methoden der Nutzung von SMS vorziehen. Die Nutzung von SMS Methoden ist weniger sicher.
- Sollte Ihnen der zweite Faktor einmal abhandenkommen ist dies in der Regel nur mit erhöhtem Aufwand verbunden aber kein Problem. Die genaue Prozedur hängt jedoch im Detail von der eingesetzten Variante ab (App auf dem Smartphone versus dem von Ihrem Arbeitgeber bereitgestellten Token).

Abschließende Hinweise

Zum guten Schluss ☺

Als Letztes möchten wir Ihnen noch etwas mit auf den Weg geben: einen guten Vorsatz. Im Folgenden haben wir einige Vorschläge für Ziele, die Sie sich für die Zukunft setzen können, um das Gelernte im Alltag umzusetzen. Versuchen Sie es doch einfach: Wählen Sie die Ziele aus, welche Sie am meisten ansprechen, und schauen Sie, wie gut Sie es umsetzen können:

- Ich werde in Zukunft einen Passwortmanager verwenden.
- Ich werde überprüfen, ob ich Passwörter mehrfach verwende und gegebenenfalls ändern.
- Ich werde regelmäßig überprüfen, ob Webanwendungen, die ich nutze, kompromittiert worden sind und gegebenenfalls Passwörter ändern.
- Ich werde für mein E-Mail-Benutzerkonto Zwei-Faktor-Authentifizierung einrichten und nutzen.
- Ich werde prüfen, dass bei der Passworteingabe keine unberechtigten Personen zusehen.
- Ich werde eine Sichtschutzfolie auf meinem Gerät anbringen.
- Ich werde eine Sperre auf meinem mobilen Gerät einrichten.

Möchten Sie Dinge aus der Schulung umsetzen, die hier nicht genannt sind, dann können Sie natürlich auch ein eigenes Ziel definieren.

Rechtliches

Alle in dieser Schulung verwendeten Icons stammen von thenounproject.org und sind entweder gemeinfrei oder unter einer Creative Commons Lizenz vom Typ Namensnennung 3.0 Vereinigte Staaten von Amerika zugänglich. Um eine Kopie dieser Lizenz einzusehen, konsultieren Sie http://creativecommons.org/licenses/by/3.0/us/ oder wenden Sie sich brieflich an Creative Commons, Postfach 1866, Mountain View, California, 94042, USA.

Die Icons stammen von folgenden Künstlern: Andrew Forester, Daniela Baptista, il Capitano, anbileru abileru, Nikhil Dev, Alfa Design, Numero Uno, Arthur Shlain, IconsGhost, jayati bandyopadhyay, Andrew, Hopkins, Carin Marzaro, Hector, Gregor Cresnar, Adrien Coquet, b farias, Adrien Coquet, corpus delicti, Nicolas Vicent, Oliviu Stoian, Lorena Salagre, myladkings, Nikita Kozin, Joel Wisneski, Pedro Santos, Sandra, Ruslan Design, Aaron K. Kim, Edward Boatman, Vladimir Belochkin, Michael Finlay, Peter van Driel