Passwort - Ausspioniert

Das beste Passwort nützt nichts, wenn es ein Angreifer mitlesen kann, oder der User es ihm sogar freiwillig mitteilt.
Passiert mir nicht? Dann lies weiter!

Ich hab mir nur schnell einen Kaffee geholt

Hat ein Hacker direkten Zugang zu einem System oder einer offenen Session, genügt eine halbe Minute, um die benötigten Login-Daten zu erhalten. Falls die Passwörter in dieser Zeit nicht schon geknackt sind, kann er sie zumindest zum Knacken mit nach Hause nehmen. Dann kann er mit schnellen Rechnern oder - wie auch üblich - mit tausenden geklauten Rechnern (= Botnets) an der Dekodierung Deines Passwortes arbeiten. Das ergibt dann viele Milliarden Versuche pro Sekunde (mehr als 2 Milliarden Versuche pro Sekunde pro PC).

Shoulder Surfing

heißt - über die Schulter ausspionieren, z.B.

- zuschauen, wie jemand den Bankomat Pin oder das Passwort eintippt
- Mini-Kameras / Spiegel / Fernglas aus dem gegenüberliegenden Haus
- oder für die Paranoiker die gehoben Spionage-Variante: Abhören der Tastatur (da die Tastenanschläge mit passender Analyse-Software unterschiedlich klingen), z.B. über einen Laserstrahl, der die Schwingungen der Fensterscheibe wieder hörbar macht

Zurück zur Praxis:

Achtung: Geübte User lesen nicht mehr genau, was am Bildschirm steht und vertun sich manchmal in den Eingabefeldern, z.B:

- der User will wie gewohnt den Bildschirm durch Passworteingabe entsperren, aber
- Windows zeigt diesmal die normale Login Maske
- der User, der ohne Lesen das Passwort eintippt, schreibt es im Klartext in das Feld Username
- **peinlich, wenn das bei einer Präsentation auf der Großleinwand passiert**
- und der User dasselbe Passwort für all seine Internet Logins verwendet

Gegenmaßnahmen:

- Hand am Bankomat verdecken (Kamera über Tastaturfeld)
- bei Passworteingabe nicht zuschauen lassen; notfalls Zuschauer/Kollegen auffordern: “Bitte - ich möchte mein Passwort eingeben!”
- Passwort so wählen, daß es schnell getippt und nicht einfach durch Zusehen mitgelesen werden kann
- erst schauen, dann tippen: prüfen, ob man auch wirklich im richtigen Eingabefeld ist, bevor man das Passwort tippt

Phishing

Beim Phishing werden den Zugangsinformationen über Softwareanwendungen des Anwenders “geangelt” (Online Banking, Facebook Login, ...). Beispiele sind gefälschte Webseiten, E-Mails, Mitteilungen oder Anwendungen, die den Nutzer beispielsweise zur Angabe seines Passwortes und Benutzernamens auffordert.

Gegenmaßnahmen:

Schutz bietet nur eine entsprechende Software und ein aufmerksamer Anwender.

Wer sich aufgrund einer E-Mail auf eine Webseite begibt und dort seine geheimsten Daten eingibt, sollte sich fragen:

Würde ich auf der Straße einem Unbekannten, der mich dazu auffordert, meine Kontodaten oder Hausschlüssel geben? Auch wenn der Vorwand gut oder dringend ist und der Ausweis offiziell aussieht?

- Schauen, Denken, Tippen
- Ist das überhaupt die Webseite meiner Bank? - URL genau checken!
- Ist die Verbindung verschlüsselt? - Browser Symbole checken
- Lieber bei der Hotline anrufen und fragen, ob das richtig und wirklich nötig ist
  - Aber Achtung: NICHT bei der Betrugs-Nummer, die in der E-Mail steht, sondern bei der offiziellen Hotline aus dem Telefonbuch!

Social Engineering

In den meisten Fällen ist der User selbst das schwache Glied ! Oft ist es der Nutzer, der, aus Unwissenheit oder vorsätzlich, eine Lücke im System öffnet, indem er Informationen (zum Beispiel Passwörter) an den Hacker weitergibt oder E-Mail-Anhänge ausführt.

Der Angreifer bricht durch Vortäuschung einer falschen Identität in das soziale Umfeld des Benutzers ein, um unberechtigt Daten zu erlangen. Das Opfer fühlt sich sicher und gibt die Daten frei. Man möchte meinen, daß das viel Geschick erfordert, aber es ist erschreckend, wie bereitwillg Nutzer alles glauben was auf dem Bildschirm steht.

Scareware ist ein eingeschleustes Schadprogramm, das den Benutzer durch Vorspielen von Bedrohungen verängstigt und so zu bestimmten Handlungen bewegen soll, wie Eintippen von Administrator Passwörtern oder zum Kauf einer bestimmten Bereinigungs-Software (die dann meist auch nur ein weiteres Schadprogramm ist).

Gegenmaßnahmen:

Es gibt keine Sicherheitsvorkehrungen, die den User vor Betrug bewahren können, nur gesunder Menschenverstand, Vernunft und ein wenig Kenntnis über verschiedene Vorgehensweisen können ihn davor bewahren, in die Falle zu treten !

- Schauen, Denken, Tippen
- gesundes Mißtrauen gegenüber jedem E-Mail-/SMS-Inhalt
  - E-Mail ist eine Klartext Postkarte, die durch viele Hände geht
  - der Dir bekannte Absender kann gefälscht sein
  - der ursprüngliche Inhalt und Attachments können verändert worden sein

- auch SMS können einen vertrauten Absender vortäuschen
- wenn die natürlichen Authentifizierungs-Möglichkeiten Blick-Kontakt und Stimme fehlen, sollte man sehr genau überlegen und prüfen, wer der andere ist und welche Daten man weitergibt
- Gute Virensoftware blockiert bekannten Pishing-Seiten

Apps

Schon mal überlegt, warum die tolle App nichts oder fast nichts kostet?
Weil sehr viele Apps nur ein kleiner Servicevorwand sind um deine Daten zu verkaufen.

Schön, wenn die User sich die Wanzen selbst installieren.
Wer Apps (auch aus Apple/Google Store) ohne gute Recherche und ohne Einschränken der unnötig voreingestellten vollen Zugriffsrechte installiert, darf sich nicht wundern, wenn seine Zugangs-, Kommunikations-, Kontakt- und Positionsdaten am freien Markt verkauft werden.

Key Logging

Key Logging verwendet Hard- oder Software Hilfsmittel (z.B. Trojaner) um die Eingaben eines Nutzers zu protokollieren. Ziel ist die Spionage von geheimen Zugangsdaten.

Das bekannteste Beispiel in den Medien ist der EC-Kartendaten Diebstahl. Dabei werden die Daten der EC-Karte mit einem vorgelagerten Lesegerät aufgezeichnet. Die PIN erhält der Angreifer durch ein übergelagertes Eingabefeld.

Man in the Middle − Attacke

Der Angreifer steht logisch oder physikalisch zwischen den kommunizierenden Parteien und hat Zugriff auf den Datentransfer. Dabei kann er Daten einsehen, um wichtige Informationen zu erhalten oder Daten manipulieren um ein gewünschtes Verhalten beim Opfer hervorzurufen, z.B:

- die Netzwerkrouter des Hauseigentümers (zwischen mir und dem Internet)
- Daten-Recorder/Abzweigung im Keller beim Telekabel-Anschluß
- Daten-Recorder an Bankomat Lesegeräten (Tankstelle, Supermarkt)
- ARP-Spoofing: Abhören des Datenverkehrs und IP-Telefonie
  - der Angreifer sendet verfälschte ARP-Pakete (zur Identifikation von Rechnern im Netzwerk) und weist sich damit als anderer (interner) Computer aus
  - er kann den Datenverkehr zum eigentlichen Empfänger damit auf sich umleiten und damit die gesamte Kommunikation mitschneiden
  - Trotz der Bekanntheit und des Alters des Angriffes bieten gängige Betriebssysteme keinen Schutz vor ARP-Spoofing an. Dieser muss in der Regel nachgerüstet werden.

- Banking-Trojaner
  - Ein Trojaner dupliziert die Bank-Webseite und leitet alle Eingaben an den Hacker
  - die eingegebene TAN ist ja nur einmal gültig; daher gibt der Trojaner an die Bank eine falsche TAN Nummer weiter und fängt die zurückgegebene Fehlermeldung ab

    - der Kunde wird vom getarntenTrojaner aufgefordert, eine andere TAN-Nummer einzugeben, usw, bis er aufgibt
    - inzwischen wird mit den eingegebenen TANs fleißig abgebucht
    - alternativ wird auch ein Rechnerabsturz ausgelöst, weil es dann plausibler ist, daß die vorher eingegeben TAN nicht mehr gültig ist und man eine neue TAN eintippen muß

Gegenmaßnahmen:

Kommunikation verschlüsseln bevor sensible Daten die eigene Umgebung verlassen, z.B:

- VPN
- HTTPS
- Up-to-date Virenschutz
- 2-way Online Banking, d.h. für jede Transaktion werden 2 unterschiedliche Kommunikationswege benötigt
    - für eine Transaktion fordert der Benutzer bei der Bank eine TAN an,
    - diese wird umgehend per SMS zugeschickt und dann
    - vom Benutzer im Browser eingetippt

Replay-Attacke

Bei der Replay Attacke sendet der Angreifer zuvor aufgezeichnete Daten, um etwa eine fremde Identität vorzutäuschen (siehe Man in the Middle − Attacke).

- geklauter Fingerabdruck bei biometrischer Authentifizierung
    - Versuche, die Bürgerkarten mit Fingerabdruck-Scans sicherer zu machen
    - Hat ein Hacker den Scan-Datenstrom einmal kopiert (z.B. durch einen Trojaner), kann er ihn einfach abspielen um Deine Identität vorzutäuschen
- alle Systeme, die immer dieselben Daten erfordern, um Benutzer/Absender zu authentifizieren, sind anfällig für Aufzeichnung und Replay Attacken

Gegenmaßnahmen:

- häufige Situationen der Man-in-the Middle und Replay-Attacken in der Datenübertragung werden durch IPSec, VPN, und andere Systeme unterbunden

Spoofing

Verschleierung der eigenen Identität und Vortäuschen eines bekannten Gegenübers

- Mail-Spoofing: vorgetäuschter Absender
- URL-Spoofing: vorgetäuschte, nachgebaute Webseite; sieht aus wie ein Facebook Login oder meine Online-Banking-Seite - ist es aber nicht
- Call ID Spoofing: Anrufe und SMS unter einer vorgetäuschten Nummer
    - Hauptsächlich bei IP-Telefonie
- GPS-Spoofing: ist eine Methode, GPS-Empfänger zu einer falschen Positionsbestimmung zu verleiten.
- Netzwerk-Spoofing: vorgetäuschte Adressen und Services können den gesamten Datenstrom umleiten, kompromittieren, und abhören, z.B.
    - ARP-Spoofing
    - DHCP-Spoofing

- DNS-Spoofing
- IP-Spoofing
- MAC-Spoofing

Hijacking

Entführung, Diebstahl, gewaltsame Übernahme, z.B:

- Session Hijacking: Entführung einer Kommunikationssitzung, z.B. eines Wiki Logins oder MyFiles Logins bei ungesicherter Kommunikation oder schlecht programmierten Systemen
- History-Hijacking: Erfolgreiche Übernahme der Browser-History: Durch eine bekannte Sicherheitslücke wird es Seitenbetreibern ermöglicht, das bisherige Surfverhalten ihrer Besucher auszuspionieren.
- Network-Hijacking: Übernahme eines schlecht geschützten Servers im Internet bzw. in einem WLAN, dabei wird oft der eigentliche Besitzer des Servers ausgesperrt