

Audit von Authentifizierungsverfahren

Abendseminar «Innovative Alternativen zum Passwort»
26.10.2010, Hotel Novotel, Zürich

Walter Sprenger
Compass Security AG

Audit eines Authentifizierungsverfahrens

- ◆ Pre-Audit
 - ◆ Evaluation der geeigneten Authentisierungslösung
- ◆ Post-Audit
 - ◆ Audit der Integration in die Infrastruktur/Applikation



Wert der Daten (Information Assets)?

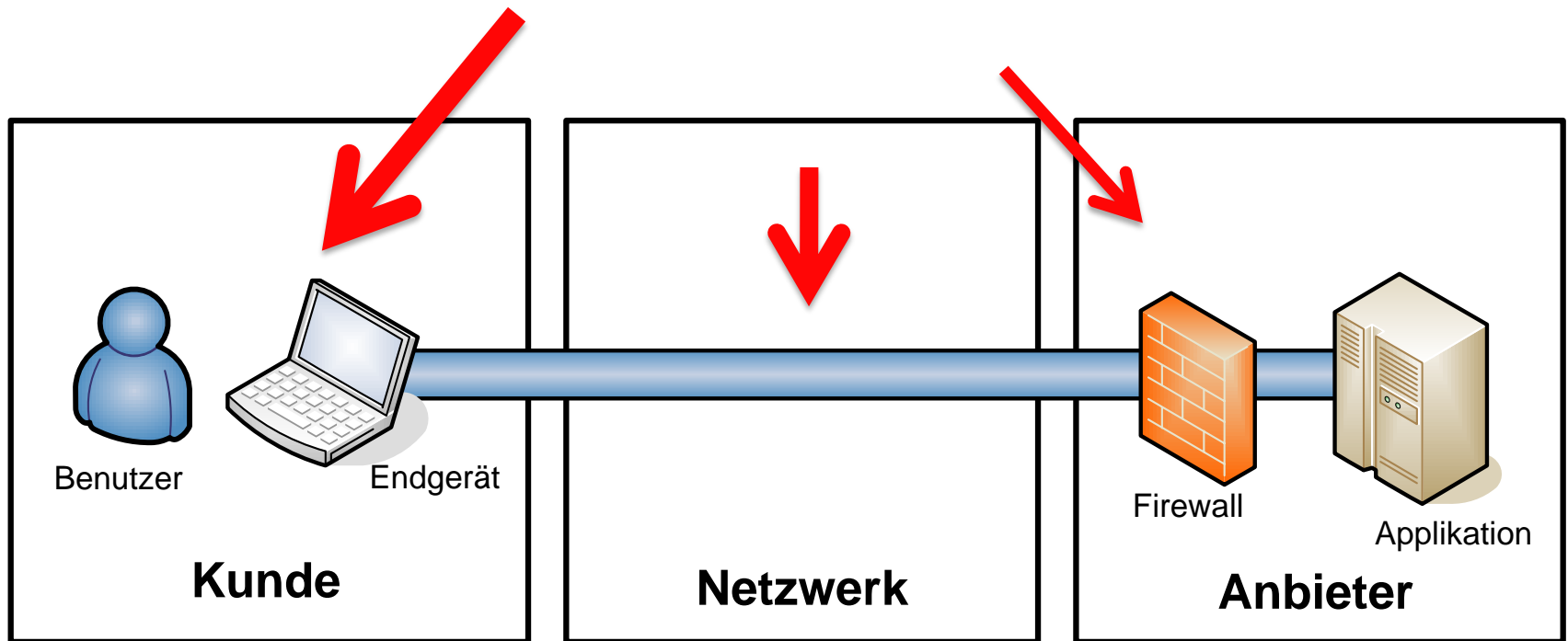
Vertraulichkeit der Daten?

Rechtliche Anforderungen?

Schutzbedarf?

- ✦ Zugangsschutz
- ✦ Identifikation von Benutzern
- ✦ Verhinderung von Account Lockouts
- ✦ Verhinderung unerlaubter Aenderungen / Transaktionen
- ✦ Schutz vor Einsicht persönlicher Daten / Firmengeheimnisse
- ✦ Schutz vor Identitätsdiebstahl / Schutz vor falschen Signaturen

Wo wird der Angriff erwartet?



Anbieter

- ✦ Authentisierungsinformationen erraten
- ✦ Authentisierungsinformationen wiederverwenden
- ✦ Schwachstellen in der Authentifizierung ausnutzen
- ✦ Schwachstellen in der Applikation (z.B. Cross Site Scripting)

Netzwerk

- ✦ Datenverkehr umleiten (Pharming, Routing)
- ✦ Datenverkehr belauschen (Man in the Middle)
- ✦ Datenverkehr verändern
- ✦ Protokollschwächen

Kunde

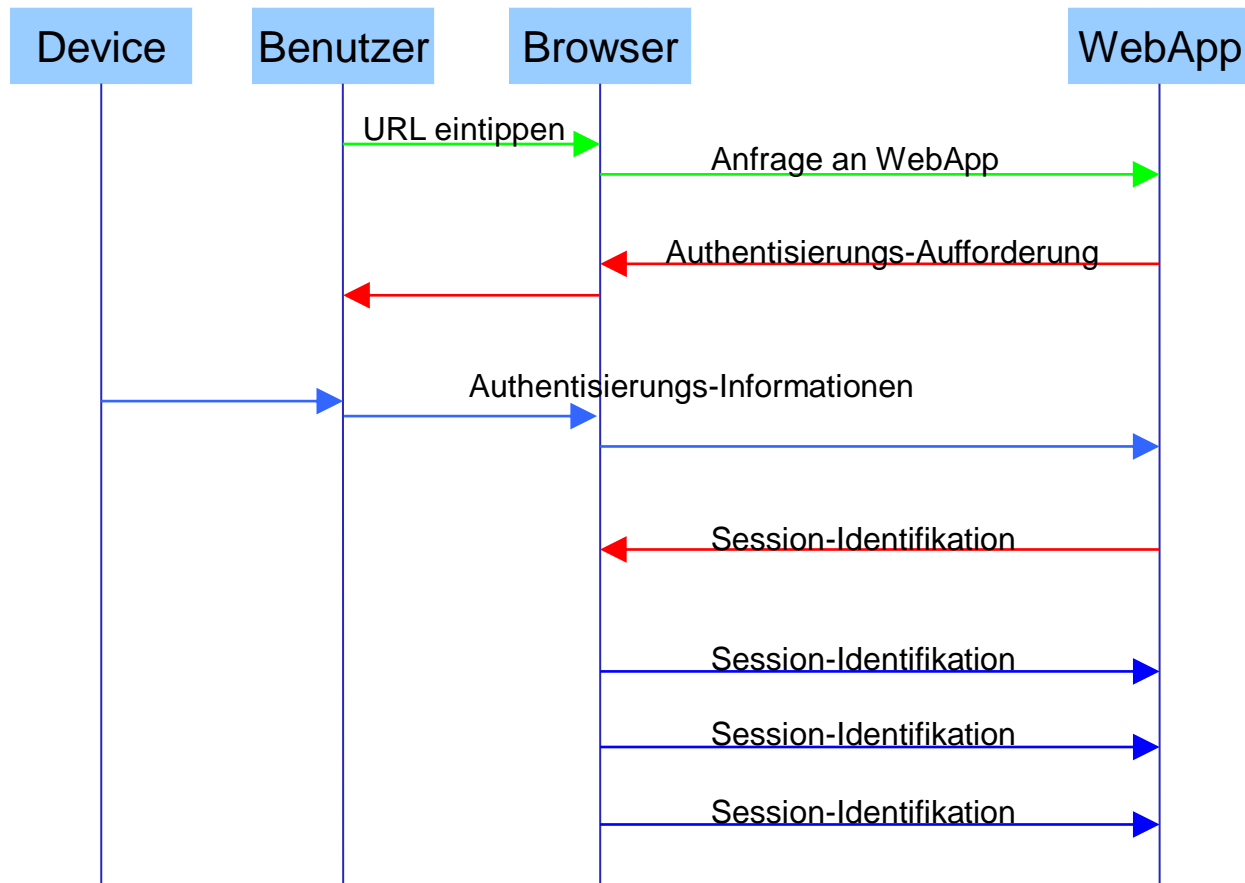
- ✦ Social Engineering / Phishing
- ✦ Trojaner im Browser
- ✦ Trojaner auf dem Endgerät
 - ✦ Session Cookie Stealing bis Fernsteuerung des Computers

Evaluationskriterien aus Business Sicht

- ✦ Benutzerfreundlichkeit
 - ✦ Benutzer arbeitet wie gewohnt
 - ✦ Benutzer muss etwas neues lernen
 - ✦ Benutzer muss etwas eintippen
 - ✦ Benutzer muss etwas vergleichen
- ✦ Plattform (definiert / unabhängig)
- ✦ Grösse / Mobilität
- ✦ Installation von Software / Hardware
- ✦ Generische Lösung / Einzellösung
- ✦ Einsatzzweck: Authentifizierung/ Zahlungsfreigabe / Signatur / Sicherer Speicher / Zeitstempel
- ✦ Kosten Anschaffung / Betrieb
- ✦ Anzahl Benutzer
- ✦ Auslieferung / Registration
- ✦ Aktualisierungsmöglichkeit
- ✦ Barrierefreiheit / Gesundheitsrisiken

Die **AUTHENTIFIZIERUNG** ist nur die halbe Miete.

Genauso wichtig ist das **SESSION HANDLING** !!



Session Stealing / Hijacking (z.B. mit Trojaner)

- ✦ Der Angreifer wartet, bis sich der Benutzer eingeloggt hat und erspart sich die Mühe, die Authentisierungsinformationen in Erfahrung zu bringen
- ✦ Der Angreifer liest die Session aus dem Browser aus und übermittelt diese zu sich
- ✦ Der Angreifer kann die Session gleichzeitig von einem anderen Browser aus nutzen

Authentifizierungs Audit

- ✦ Stärke der Authentifizierung
- ✦ Analyse von Protokollschwächen
- ✦ Security Evaluation des Device
- ✦ Analyse Verwundbarkeiten auf Attacken (Phishing, MITM, Guessing)
- ✦ Account Lockout / Account Enumeration
- ✦ Fehlermeldungen („Password falsch“)
- ✦ Replay Möglichkeiten („Back Button“)
- ✦ Speicherung Authentisierungsinformationen / Caching
- ✦ Uebermittlung der Authentisierungsinformationen (URL, POST)
- ✦ Logout Möglichkeit
- ✦ Parameter Prüfung (SQL Injection, Cross Site Scripting, LDAP, XPATH)
- ✦ „Passwort vergessen“ Funktionalität
- ✦ Passwort Aenderung / History
- ✦ Passwort Komplexitätsanforderungen

Session Handling Audit

- ✦ Session Sniffing
- ✦ Session Guessing
- ✦ Session Fixation
- ✦ Session Stealing Prevention
- ✦ Session Binding (TLS/SSL)
- ✦ Session Terminierung
- ✦ Session Soft/Hard-Timeouts
- ✦ Cookie Einstellungen

- ✦ Attack Detection
- ✦ Browser Fingerprinting

Beispiel Attack Detection

- ✦ Detektion von Session Hijacking Attacken
 - ✦ Request Parameter vergleichen
 - ✦ Ueberwachen von SSL Session ID und IP-Adresse
 - ✦ Vergleich von Browser spezifischen Parametern

- ✦ Transaktionsprüfung / Benutzerverhalten
 - ✦ Statistiken zu jedem Benutzer ermitteln
 - ✦ Aktuelle Transaktion mit dem normalen Benutzerverhalten vergleichen
 - ✦ White Listing von Zielkonten
 - ✦ Limiten bei Transaktionen

Beispiel Browser Fingerprinting

- ✦ Mittels JavaScript und Request-Parametern wird ein Fingerprint des Browsers ermittelt
- ✦ Veränderungen im Browser können möglicherweise detektiert werden
- ✦ Der Benutzer kann identifiziert werden, bevor er sich authentisiert

- ✦ Beispiel: <https://panopticlick.eff.org/>

A screenshot of the Panopticlick website. The word "Panopticlick" is written in a large, grey, sans-serif font, with a fingerprint icon replacing the letter "o". Below it, the text "How Unique – and Trackable – Is Your Browser?" is displayed in a smaller, black, sans-serif font. The background of the screenshot is a light grey fingerprint pattern.

Panopticlick
How Unique – and Trackable – Is Your Browser?

Your browser fingerprint **appears to be unique** among the 1,192,056 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 20.19 bits of identifying information.**

Die meisten Firmen wählen die Authentifizierungs-Lösungen vorwiegend aufgrund von Business-Anforderungen und nicht aufgrund der Sicherheits-Anforderungen.

Eine gute Authentisierungslösung bringt wenig zusätzliche Sicherheit, wenn dem Session Handling zu wenig Beachtung geschenkt wird.

Die meisten Authentifizierungs-Lösungen sind nicht in der Lage, die Bedrohung durch verseuchte Endgeräte zu adressieren. Der einfachste und wahrscheinlichste Angriff läuft schon seit längerem über das Endgerät des Benutzers.

Compass Security Network Computing AG

Postfach 1628
Glärnischstrasse 7
CH - 8640 Rapperswil

team@csnc.ch | www.csnc.ch | +41 55 214 41 60

Secure File Exchange: www.filebox-solution.com

