Sehr geehrte Damen und Herren,

Ist das Internet noch sicher?

Ob am Flughafen, in der Schule, im Café, bei der Zugfahrt oder im Hotel – öffentliche WLANs stellen Oasen der Netzanbindung dar und gehören mittlerweile zum Alltag eines jeden Laptop- oder Smartphone-Besitzers. Es stellt sich jedoch die Frage, wie sicher die öffentlichen WLANs tatsächlich sind und wie sich Nutzer vor Gefahren schützen können. Ralf Schmitz zeigt es live in den Vorträgen, wie einfach er in ein Netzwerk einbrechen kann.

Als die ersten kostenlosen WLAN-Hotspots auf den Laptops und Handys erschienen, war das Vertrauen in die Sicherheit der Netze sehr gering. Die Angst vor Viren, Malware und dem Ausspähen von Daten war groß und bis heute nicht ganz unberechtigt. Rechner, die sich im selben Netzwerk befinden, kommunizieren gemäß den Vorgaben des Layer 2 (Data Link Layer) des TCP/IP-Protokoll-Stacks. Ob es ein Laptop ist oder ein Smartphone ist egal. Hacker nutzen das Verfahren aus, um sich in die Kommunikation zwischenzuschalten – die gefürchteten MITM-Angriffe (Man in the Middle).

Das 1999 von dem Hacker Dug Sonof vorgestellte Tool arpspoof beispielsweise bietet dem Rechner kontinuierlich mögliche Verbindung zum System eines Angreifers an. Einmal angenommen, läuft der gesamte Datenverkehr über diese „Verkehrsumleitung“. Angreifer könnten DNS-Antworten fälschen, den Datenverkehr nach Log-in-Informationen ausspähen und im nächsten Schritt weitere Hacking-Tools einsetzen, zum Beispiel sslstrip.

Das vom Kryptografen und Sicherheitsforscher Moxie Marlinspike erstmals auf der Black Hat 2009 vorgestellte sslstrip entwickelte sich schnell zum Lieblingsspielzeug von Hackern. Es erlaubte Angreifern, eine Zielperson beim Browsen im Web abzufangen und die SSL-Verschlüsselung zu umgehen.

Denn sslstrip greift Websites an, die HTTP für die Bereitstellung von Inhalten und HTTPS lediglich für „geheime“ Informationen wie Kennwörter oder Schlüssel verwenden. Das ist fatal und gefährlich weiß Schmitz zu berichten. Das sslstrip-Tool fängt den HTTP-Verkehr ab, schreibt alle darin befindlichen HTTPS-URLs in HTTP neu um und schickt sie wieder auf den Weg.

Durch diesen Trick können sich Hacker in den Datenstrom einklinken und Daten auslesen.

Standard für sichere Kommunikation: TLS

„Seit arpspoof und sslstrip sind über 15 Jahre vergangen. Es hat sich aber einiges getan“, weiß Ralf Schmitz zu berichten.

TLS (Transport Layer Security) ist die neue Verschlüsselung. Das Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet hat sich mittlerweile zum Standard entwickelt.

Mit steigender Leistungsfähigkeit der Geräte, einschließlich der mobilen Endgeräte, kommt TLS nicht nur bei der Übertragung von Anmeldeinformationen, sondern auch beim gesamten Datenverkehr zum Einsatz. Folglich können Angreifer Daten während der Übertragung weder lesen noch verändern.

Darüber hinaus nutzen Websites heute in der Regel HSTS (HTTP Strict Transport Security), das den Clients die Verbindung über HTTP verbietet. Viele Browser verfügen über eine Vorladeliste von HSTS-Sites, was bedeutet, dass der Verbindungsaufbau zu diesen Seiten niemals über HTTP erfolgt. Dadurch lassen sich Downgrade-Angriffe von HTTPS auf HTTP verhindern. Auch HTTP/2 und HTTP/3, die Nachfolger von HTTP/1.1, laufen nur noch über TLS.

Das Problem der Nachahmung von Zertifikaten

Sicher konfigurierte Websites und Anwendungen nutzen TLS für die gesamte Kommunikation, um Daten zu schützen. Wie sieht es aber mit der Authentifizierung aus? Woher weiß ein Web-Browser, dass er mit der richtigen Website spricht? Websites müssen gemäß X.509-Standard über ein Zertifikat verfügen, um sich gegenüber einem Web-Browser oder einer Anwendung zu identifizieren. Ein Angreifer, der diese Sicherheitsvorkehrung umgehen will, kann das auf unterschiedliche Art und Weise versuchen: Er erstellt ein eigenes Zertifikat, ahmt ein legitimes Zertifikat nach, oder er stiehlt es einfach, denn Hacker sind faul.

Ein eigenes Zertifikat zu erstellen ist einfach. Allerdings stehen die Chancen eher schlecht, dass moderne Web-Browser oder Apps dieses Zertifikat als gültig akzeptieren.

Nur technisch sehr versierte Angreifer schaffen es, ihre Zertifikate als vertrauenswürdig einstufen zu lassen. Mit einem Netzwerk-Sniffer wie Wireshark lässt sich einsehen, wie ein Browser die Authentifizierung mit einer betrügerischen Webseite untersagt und eine entsprechende TLS-Warnmeldung ausgibt.

Windows-Angriffsfläche verkleinern

Es gibt jedoch ein Problem, das insbesondere Windows-Systeme betrifft: Legacy-Authentifizierungs- und Erkennungsmechanismen, insbesondere LLMNR (Link-Local Multicast Name Resolution) und NBT-NS (NetBios over TCP/IP – Name Service). Ein gerissener Angreifer kann diese Dienste missbrauchen und Windows-Betriebssysteme dazu bringen, sich mit einem bösartigen Server zu verbinden. Das bekannte Responder-Tool automatisiert solche Angriffe. Ganz wichtig: Hier empfiehlt es sich, die Legacy-Systeme zu deaktivieren, sofern sie nicht nötig sind.

Eine weitere Schwachstelle von Windows ist die in Browsern integrierte Proxy-Authentifizierungsfunktion über WPAD (Web Proxy Auto-Discovery). WPAD ist unter Windows standardmäßig aktiviert. Auch in macOS und Linux ist die Funktion zu finden, dort aber nicht als Standard hinterlegt. WPAD sendet den NTLMv2-Hash des Benutzerkennworts über das Netzwerk, sobald ein Web-Proxy eine WPAD-Datei bereitstellt. Diese weist den Browser an, sich über NTLM zu authentifizieren. Ein Angreifer kann sich so den NTLMv2-Hash seines Angriffsziels verschaffen und offline knacken. So kann er entweder den Klartext wiederherstellen oder den Hash mit einer „Pass the Hash“-Attacke wiederverwenden.

Diese Angriffsarten setzen aber voraus, dass entweder Active-Directory-Zugangsdaten aus dem Internet (etwa über RDP und einige SSO-Provider) oder Hashes akzeptiert werden (beispielsweise über psexec oder WMI). Es gehört damit zu den dringlichsten Sicherheitsvorkehrungen, die Angriffsfläche für Windows-Systeme möglichst klein zu halten.

Folgende Tipps gibt Ralf Schmitz weiter:

Ist das WPAD-Protokoll aktiv, können Anwender einen statischen DNS-Eintrag verwenden, um sicherzustellen, dass niemand den Host-Namen des Proxys fälscht.

Bei der automatischen Proxy-Erkennung empfiehlt es sich, in allen installierten Browsern das Hakchen auf „deaktiviert“ zu stellen, sofern diese nicht zum Einsatz kommt.

LLMNR: Wenn nicht im Einsatz, lässt sich diese Funktion über Gruppenrichtlinien (GPOs) deaktivieren.

NBT-NS: Auch diese Funktion lässt sich über Gruppenrichtlinien ausschalten.

NTLM-Authentifizierung: Um die Verwendung durch den Browser zu deaktivieren, gehen Anwender am besten schrittweise vor. Anstatt die Windows-Anmeldeinformationen automatisch zu übermitteln, fordert der Browser nun nach jedem Schritt eine Authentifizierung an, um die Anmeldeinformationen zu erfassen.

Firewalls: Die Sicherheitssysteme sind und bleiben essenziell, um öffentliche WLANs ruhigen Gewissens nutzen zu können. Selbst wenn Hacker Log-in-Daten abfangen, verhindern Firewalls in den meisten Fällen ihre Wiederverwendung. Deshalb auch regelmäßig Updates machen, am Besten automatisiert.

VPN bringt als Sicherheitsvorkehrung wiederum ein Sicherheitsrisiko mit. VPNs führen oft zu Problemen, zum Beispiel bei der Verbindung mit unternehmenseigenen Portalen. Daher lohnt es sich, das Kosten-/Nutzen-Verhältnis von VPNs genau abzuwägen. Eine Alternative zur richtigen Konfiguration sind sie keinesfalls.

Mit freundlichen Grüßen

Celina Nowak

P.S.: Bitte setzen Sie uns auf die White-Liste in Ihrem Postfach, damit die Zustellung der Mails gewährleistet ist. Gerne dürfen Sie diese Mail an Freunde, Kollegen, Bekannte weiterleiten.

Kontaktformular: http://www.sicher-stark-team.de/kontakt.cfm

Herausgeber:
Bundespressestelle Sicher-Stark:
Dr. Axel Schäfer (V.i.S.d.P.)
Service-Tel.: 0180-5550133-2*

Rückfragen und Anmerkungen bitte an:
****
Bundespressestelle Sicher - Stark
Hofpfad 11, D-53879 Euskirchen
Service-Tel.: 0180-5550133-2*
Service-Fax: 0180-5 550133-0*
*0,14 Euro/Minute aus dem deutschen Festnetz;
Mobilfunkhöchstpreis 0,42 Euro/Minute

Bitte haben Sie Verständnis dafür, dass wir als soziale Einrichtung auf eine Teilfinanzierung über Telefonkosten angewiesen sind. Wir rufen Sie gern zurück.
Kontakt: presse@sicher-stark.de
****