Quo vadis Internetsicherzeit – eine Bestandsaufnahme

Nie war das Internet so sicher wie heute, sagt Chester Wisniewski. Der Weg war lang und es ist noch immer viel zu tun.

Von Chester Wisniewski, Principal Research Scientist bei Sophos

Wir leben in einer Zeit, da die Schlagzeilen suggerieren, dass alles immer nur schlimmer und bedrohlicher geworden ist. Das gilt auch für die Sicherheit der Internetnutzer:innen. Ich bin überzeugt, dass hier schon vieles erreicht wurde. Hier ein Rückblick auf die Entwicklungen:

Sicherheit in den Anfangstagen
Das heutige World Wide Web unterscheidet sich stark von dem, was Sir Tim Berners-Lee 1990 erdacht hat. Das frühe Web war zwar frei und offen, aber eben auch ein wenig zu offen. Es gab weder Datenschutz noch Verschlüsselung, um die Informationen zu schützen, die zwischen den zahlreichen Servern und Routern übertragen wurden, die an der Vernetzung der Welt beteiligt waren.
Netscape trug zur Lösung dieses Problems bei, indem es die Verschlüsselung durch Secure Sockets Layer (SSL) einführte, die später zu einer offiziellen Spezifikation, Transport Layer Security (TLS), aktualisiert wurde. Damals war TLS dazu gedacht, digitale Einkaufswagen, die Kreditkartendaten und gelegentlich auch Anmelde-IDs und Passwörter zu schützen.

Snowden war der Startschuss: Sicherheit als Standard
Seltsamerweise blieb dies bis 2013 so, als der NSA-Mitarbeiter Edward Snowden beschloss, der Welt mitzuteilen, wie viele Online-Informationen die Vereinigten Staaten über fast jeden Menschen auf der Welt sammelten - und sammeln konnten.
Trotzdem wurden noch im Oktober 2013, wenige Monate nach Snowdens Enthüllungen, nur 27,5 Prozent der von Mozilla Firefox geladenen Webseiten in irgendeiner Form verschlüsselt. Dies veranlasste die Menschen in der Sicherheitsbranche, sich für die Verbesserung der Sicherheit und des Datenschutzes von Internetnutzer:innen weltweit zu interessieren und zu arbeiten.
Der Gedanke war: Die einzige Möglichkeit, dieses Problem zu lösen, besteht darin, alles zu verschlüsseln. Dies spornte die Einführung neuer Technologien und Standards an, um zu gewährleisten, dass die Dinge standardmäßig sicher sind. Die neuen Technologien und Standards haben das Risiko jedoch nicht gänzlich beseitigt. Wenn Kriminelle immer noch in Netzwerkverbindungen eindringen können, sind sie auch in der Lage, Nutzer:innen einfach auf eine gefälschte Website umzuleiten, um ihre privaten Daten zu stehlen. Dies ist ein so genannter Machine-in-the-Middle-Angriff (MitM), der durch die Bereitstellung falscher DNS-Antworten (Domain Name System), den Betrieb eines bösartigen Zwillings-Wi-Fi-Zugangspunkts oder auch direkt durch ISPs (Internet Service Provider), Regierungen, Strafverfolgungsbehörden und andere durchgeführt werden kann. Unternehmen können sogar den TLS-Verkehr abfangen, indem sie Middleboxen einsetzen, die den geschützten Verkehr untersuchen.

Schritte zur Behebung des Problems
Selbst wenn eine Website HTTPS verwendet, muss sie wahrscheinlich zunächst checken, ob das unsichere HTTP (Hypertext Transfer Protocol) verwendet wird und die Benutzer:innen auf die sichere Website umleiten, da Webbrowser in der Regel standardmäßig zuerst HTTP versuchen.

2012 schlug Google einen neuen HTTP-Header vor, um den Browser anzuweisen, die erste Verbindung über HTTPS herzustellen: HSTS (HTTP Strict Transport Security). Mit diesem HTTP-Header konnten Website-Administrator:innen angeben, dass ihre Webseite nur über HTTPS geladen werden sollte und dass Browser niemals versuchen sollten, Verbindungen über HTTP an Port 80 herzustellen.

Ende 2013 kündigte Google an, dass sein Chrome-Browser beim Zugriff auf unsichere Webseiten eine Warnung ausgeben und unverschlüsselte Websites in den Suchergebnissen niedriger einstufen würde, um alle Websites zu ermutigen, TLS-Verschlüsselung einzusetzen. Dank der Politik von Google und der intensiven Bemühungen der gesamten Sicherheitsgemeinschaft hat sich die Zahl der Websites, die sichere Verbindungen unterstützen, in nur drei Jahren verdoppelt. Aus den Google-Statistiken geht hervor, dass die von Chrome-Nutzern besuchten Websites in den meisten Ländern in 95 Prozent der Fälle verschlüsselt sind.

Im November 2020 begann der jüngste Schritt der Browserhersteller, uns in eine immer verschlüsselte und damit sicherere Internetwelt zu führen, als Mozilla eine reine HTTPS-Option in Firefox einführte. Wenn diese Funktion aktiviert ist, versucht sie, alle Verbindungen sicher über HTTPS herzustellen, und gibt eine Warnung aus, wenn HTTPS nicht verfügbar ist. **Im April 2021** fügte Chrome eine ähnliche Option hinzu und aktivierte sie standardmäßig. Große Fortschritte.
.....

Fazit: Das Internet war noch nie so sicher wie heute.
Da 95 Prozent der Webseiten verschlüsselt sind und diejenigen, die nicht verschlüsselt sind, in der Regel kein großes Risiko darstellen, ist dies eine gute Nachricht, vor allem in der Zeit des regen Online-Shoppings.

Nach und nach hat die Sicherheitsgemeinschaft zusammengearbeitet, um die Standards zu verbessern, Druck auf Nachzügler auszuüben und die Kosten für die sichere Kommunikation über das Internet zu senken. Die erzielten Fortschritte sind beeindruckend, wenn man bedenkt, welches Ausmaß das Problem einst hatte.

Die Arbeit ist jedoch noch lange nicht abgeschlossen. Die Tatsache, dass nur 31,6 Prozent der Webseiten HSTS verwenden, zeigt, dass selbst Funktionen, die kostenlos sind und die Sicherheit erheblich verbessern, nicht so weit verbreitet sind, wie sie sein sollten.

Die Sicherung der Anwendungsschicht hat massive Auswirkungen auf die Nutzer:innen und die Sicherheit. Es besteht immer noch die Gefahr, dass die Anbieter der von uns genutzten Netze Spionage betreiben und unsere Daten an Werbenetze zu verkaufen oder von Cyberkriminellen kompromittiert werden.

Aber dank HSTS und TLS können Internetnutzer:innen so gut wie ungehindert surfen und kommunizieren, ohne dass ein nennenswertes Risiko besteht, dass etwas schief geht – selbst über nicht vertrauenswürdige WiFi- und Mobilfunknetze.

Die gesamte, ausführliche Analyse in englischer Sprache mit Detailbeschreibung und Grafiken gibt es hier:

https://news.sophos.com/en-us/2021/11/22/the-state-of-world-wide-web-security-in-2021/

Neu: Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de