WhatsApp führt Ende-zu-Ende-Verschlüsselung ein

WhatsApp hat damit begonnen, die über den eigenen Dienst versendeten Kurznachrichten besser zu verschlüsseln. Dazu kommt nicht irgendeine, sondern die renommierte Ende-zu-Ende-Verschlüsselung des von Experten und Datenschützern hoch geschätzten Messengers TextSecure zum Einsatz. Diese stammt von Open Whisper Systems und schnitt im Vergleich verschiedener Verschlüsselungssysteme für Messenger in c't 8/14 in puncto Sicherheit als sehr empfehlenswert ab. In Kombination mit der einfachen Benutzbarkeit und der Anwenderbasis von WhatsApp ergibt das ein Dream-Team.

WhatsApp ist wohl die meistgenutzte Messaging-App auf Smartphones und auf dem besten Weg, die SMS aufs verdiente Altenteil zu schicken. In Bezug auf Sicherheit und Privatsphäre geriet WhatsApp allerdings immer wieder in die Kritik. Insbesondere die fehlende Verschlüsselung der Kommunikation war Datenschützern und Sicherheitsexperten stets ein Dorn im Auge. Das soll sich jetzt ändern. Bereits seit einem halben Jahr arbeitet WhatsApp mit Open Whisper Systems zusammen, um die Krypto-Infrastruktur von TextSecure zu integrieren. Die Android-Versionen sollen dessen Ende-zu-Ende-Verschlüsselung schon jetzt beherrschen und bereits Milliarden verschlüsselte Nachrichten am Tag austauschen. In weiteren Ausbaustufen sollen verschlüsselte Gruppen-Chats und die anderen unterstützten Betriebssysteme folgen. Ebenso will WhatsApp den Nutzern die Möglichkeit geben, gegenseitig die Schlüssel zu überprüfen, wie man es bereits von anderen verschlüsselnden Messengern wie Threema kennt. (ju)

Spezial-Scanner spürt Staatstrojaner auf

Die Software „Detekt" des Vereins Digitale Gesellschaft e. V. soll acht verschiedene Staatstrojaner aufspüren können. Das Entfernen der Schädlinge ist nicht vorgesehen. Stattdessen empfehlen die Entwickler, sich die Unterstützung eines Experten zu sichern, falls das Tool tatsächlich Alarm schlägt – im schlimmsten Fall solle man den betroffenen Rechner entsorgen. Amnesty International und die EFF sind bei der Initiative mit im Boot; Amnesty legt den eigenen Aktivisten bereits nahe, die Software einzusetzen. Das quelloffene Python-Programm wurde von Claudio Guarnieri von der Sicherheitsfirma Rapid 7 programmiert, der sich bereits mit der Cuckoo-Sandbox und einer Analyse von FinFisher einen Namen machte.

Es nutzt die Pattern Matching Engine Yara, um Hinweise auf Staatstrojaner zu erschnüffeln. Die Software soll FinFisher/FinSpy, Gh0st, das Remote-ControlSystem des Hacking-Teams, BlackShades und weitere Schadsoftware entdecken. In einem kurzen Test bei heise Security gelang es der Software, bekannte Muster des FinSpy-Trojaners erfolgreich zu entdecken. (fab)

Detekt soll bekannte Staatstrojaner entdecken, etwa die Software der deutschen Firma FinFisher.

Microsoft kritisiert Anti-Viren-Hersteller

Auf der AVAR-2014-Konferenz in Sydney hat Dennis Batchelder von Microsoft einen Vortrag über die Entwicklung des Anti-Malware-Ökosystems gehalten. Dabei kritisierte er die Hersteller von Anti-Virus-Programmen. Für ihn sieht es so aus, als würden die AV-Firmen den Kampf gegen professionelle Virenschreiber verlieren, da immer mehr Malware auf den Markt drängt. Das hängt seiner Meinung nach auch damit zusammen, dass die AV-Hersteller sich momentan stark untereinander bekriegen und somit wertvolle Ressourcen verschenken. Die Firmen würden weniger zusammenarbeiten und Viren-Samples erst spät untereinander teilen, sodass Kunden erst mit Verzögerung geschützt werden.

Insbesondere denken AV-Hersteller laut Batchelder zu stark an die Umsätze statt an die Kunden. So meinte er, dass bei einigen AV-Programmen eine ganze Menge Software mit auf der Platte installiert wird, die eigentlich schon als „potenziell unerwünscht" klassifiziert werden könnte; darunter Browser-Toolbars. Außerdem gäbe es zu viele Probleme mit dem Freemium-Modell: Viele AV-Programme verbreiten seiner Meinung nach zu viel Werbung und nerven den Benutzer. Letztlich zum Nachteil des Kunden: Der deinstalliert seine AV-Lösung lieber und bleibt ungeschützt, so das Worst-Case-Szenario.

(Andreas Marx/fab)

Bild: Andreas Marx, AV-TEST

Dennis Batchelder von Microsoft geht hart mit den AV-Herstellern ins Gericht.

Sicherheits-Notizen

Avast 2015 hatte Probleme mit dem Rollup-Update für Windows 8.1 vom 18. November (KB3000850). Wer das Patch-Paket bei laufendem Virenwächter einspielte, musste danach mit Abstürzen des Internet Explorer, der Systemsteuerung und des Windows-Explorers rechnen. Manche Systeme fuhren nicht mehr herunter, andere hingen in einer Boot-Schleife fest. Avast hat seine Software inzwischen aktualisiert und das Problem behoben.

Microsoft musste das **Windows-Update** vom November-Patchday, welches eine kritische Lücke in der Krypto-Infrastruktur SChannel gestopft hatte, nachbessern und erneut ausliefern. Es hatte in Zusammenhang mit SQL Server zu schweren Performance-Problemen geführt und die TLS-Verschlüsselung auf Windows Server 2008 R2 und Server 2012 teilweise unbrauchbar gemacht. Betroffene Administratoren müssen das Update (KB2992611) von Hand neu installieren, um die verbesserte Version zu bekommen.

Außerdem hat Microsoft eine kritische Lücke in Windows außer der Reihe geschlossen: Über das Authentifizierungssystem **Kerberos** kann sich ein angemeldeter Benutzer auf allen unterstützten Versionen von Windows Server Administrator-Rechte auf sämtlichen Rechnern in einer Domäne verschaffen. Das öffnet dem Angreifer das gesamte LAN für weitere Attacken. Alle unterstützten Desktop-Versionen von Windows wurden ebenfalls gepatcht; dort stuft Microsoft das Update jedoch nur als vorbeugende Verteidigungsmaßnahme ein.

SSL-Zertifikate von Mozilla und der EFF

Unter dem Namen „Let's Encrypt" wollen Mozilla, Akamai, Cisco und die EFF eine kostenlose Zertifizierungsstelle für SSL/TLS-Zertifikate einrichten. Die neue Certificate Authority (CA) soll ab Sommer 2015 an den Start gehen und dann kostenlose Zertifikate an Administratoren verteilen. Anders als bei selbstsignierten Zertifikaten sollen Browser diesen Zertifikaten vertrauen, ohne dass der Anwender mit einer Fehlermeldung konfrontiert würde. Neu entwickelte Software soll es wesentlich einfacher machen, Zertifikate anzufordern und zu erneuern. Die Organisatoren wollen den Großteil der Software als Open Source öffentlich zur Verfügung stellen.

Wenn die Software fertig ist, soll man seinen Linux-Server mit zwei einfachen Zeilen entsprechend konfigurieren und die Seite über HTTPS verfügbar machen können. Alles weitere, wie die Verifizierung der Domain und die Einstellungen am Webserver, sollen automatisch vonstattengehen. Nicht mal eine E-Mail-Bestätigung soll nötig sein, da das Tool automatisch gegenüber Let's Encrypt bestätigt, dass man Kontrolle über den entsprechenden Server hat. Die Software kümmert sich auch um eine Verlängerung des Zertifikats, wodurch Fehlermeldungen wegen versäumter Zertifikatsverlängerungen der Vergangenheit angehören sollen.

Die Idee, durch kostenlose Zertifikate mehr Server-Betreiber zum Verschlüsseln zu bewegen, ist nicht neu. In der Vergangenheit hatten Anbieter wie CAcert allerdings immer wieder Probleme, in die Listen gängiger Browser aufgenommen zu werden. Unter anderem hatte sich hier Mozilla verweigert. Eine Alternative bietet die israelische Firma StartSSL, die ebenfalls seit Jahren kostenlose Zertifikate anbietet. Diese funktionieren auch mit den meisten Browsern. Geld macht StartSSL mit Extended-Validation- und Wildcard-Zertifikaten. Im Gegensatz dazu wird die von Mozilla & Co. gegründete Internet Security Research Group (ISRG) rein gemeinnützig auftreten. (fab)

Zero-Day-Politik des BSI wird zum Streitpunkt

Die Gesellschaft für Informatik (GI) hat den Umgang der Regierung mit sogenannten Zero Day Exploits, bisher unveröffentlichten Sicherheitslücken, angeprangert. Nach dem Entwurf für das neue IT-Sicherheitsgesetz soll das Bundesamt für Sicherheit in der Informationstechnik (BSI) diese Sicherheitslücken zwar sammeln, muss sie aber nicht veröffentlichen. Das ermöglicht es mutmaßlich anderen Behörden, Nutzer mit Hilfe dieses Wissens anzugreifen – etwa um deren Computer zum Zwecke der Quellen-TKÜ mit Staatstrojanern zu infizieren.

Hartmut Pohl, Sprecher des Arbeitskreises für Datenschutz und IT-Sicherheit bei der GI, sieht in diesem Vorgehen der Behörde eine unnötige Belastung für die Wirtschaft. Die Veröffentlichung von bis dato unbekannten Lücken sei unverzichtbar, um diese zu schließen und sich so nachhaltig gegen Angriffe schützen zu können. Kriminelle verdienten durch das Ausnutzen solcher Lücken Milliarden, während deutsche Firmen die Verluste schultern müssten. (fab)