atsec the information security provider
NEWS 01/14

E-Mail-Sicherheit „Made in Germany“ und noch immer keine verpflichtende Ende-zu-Ende-Verschlüsselung

Das Problembewusstsein der Internet-Nutzer hat sich durch die Snowden-Enthüllungen stark verändert. Selbst mein Vater fragt mich nach dem ominösen „Herzbluten“, ob er auch betroffen sei: sicher hänge da die NSA mit drin. Der „Heartbleed-Bug“ war der Super-GAU für SSL. Ein derartiger Programmierfehler hätte nicht passieren dürfen. Was mich noch viel mehr ärgert als solche unabsichtlichen Fehler ist, wenn Produkte oder Services absichtlich mit Sicherheitsschwächen als sicher verkauft werden und das Label „Made in Germany“ auf der Mogelpackung prangt. Das wirft ein schlechtes Licht auf all die deutschen Hersteller, die bemüht sind, sichere Produkte und Services zu entwickeln. Konkret wird die mediale Aufmerksamkeit durch die NSA-Leaks als PR-Maßnahme genutzt, um unbedarften Privat- und Firmennutzern vermeintlich sichere E-Mail-Services zu verkaufen.

„E-Mail made in Germany“, eine Initiative deutscher E-Mail-Anbieter, verspricht seinen Nutzern die sichere E-Mail. Eine längst überfällige Entscheidung, den Transportweg per SSL abzusichern, wird geschickt als großer technischer Durchbruch beworben. Nur existiert der Standard seit 20 Jahren und ist selbst bei US-amerikanischen E-Mail-Providern schon lange gängige Praxis. Fremdzugriffen auf E-Mails kann nur durch Ende-zu-Ende-Verschlüsselung erfolgreich entgegengewirkt werden. Hierfür müssen die Nutzer aber weiterhin selbst Hand anlegen. Glauben Sie allen Ernstes, dass ich meinem Vater mit über 70 noch zumuten kann, S/MIME oder GPG zu konfigurieren? Dem Großteil der Anwender geht es da vermutlich ähnlich. Viele werden nicht wissen, dass die E-Mails trotz SSL bei dem Provider im Klartext vorliegen. Immerhin steht der Standort Deutschland für sichere innerdeutsche Datenspeicherung, womit zumindest die Five-Eyes für E-Mails innerhalb des Verbundes außen vor bleiben – oder? Aber: Was passiert mit E-Mails, die an einen Empfänger außerhalb des Verbundes gehen?

Wer nun vermutet, dass der von staatlicher Seite geprüfte Service „De-Mail“ besser sei: weit gefehlt – auch hier gibt es keine Ende-zu-Ende-Verschlüsselung, lediglich eine Transportverschlüsselung. Ferner wird hier ein höchst zweifelhaftes Verfahren zur Sicherstellung der Authentizität des Senders und der Nachricht sowie deren Nicht-Abstreitbarkeit eingesetzt. Nicht, wie man vermuten möchte, über elektronische Signaturen beim Sender und Empfänger, sondern über eine „sichere Anmeldung“ der Nutzer und elektronische Signaturen des De-Mail-Diensteanbieters. Immerhin müssen sich diese beim BSI akkreditieren lassen und damit nachweisen, dass sie die im Gesetz verankerten Anforderungen an die organisatorische und technische Sicherheit erfüllen. Dies setzt z. B. einen sicheren Identifikationsprozess der Nutzer bei De-Mail-Kontoeröffnung voraus. Dennoch, die skizzierte Problematik der fehlenden Ende-zu-Ende-Absicherung bleibt bestehen.

Was rate ich nun meinem Vater und anderen E-Mail-Nutzern?

Solange Provider keine Ende-zu-Ende-Verschlüsselung anbieten: bewusster mit E-Mail-Inhalten umgehen. Für sensible Informationen S/MIME oder GPG einsetzen, bei Bedarf hierfür professionelle Hilfe hinzuziehen. Wir bei atsec nutzen übrigens schon seit langem S/MIME und GPG sowohl für die interne, als auch für die Kommunikation mit unseren Kunden.

Herzlichst,
Ihre Isabell Fouquet

Messen und Konferenzen 2014

Die atsec information security wird in diesem Jahr auf folgenden Messen und Konferenzen vertreten sein:

- **15. ICCC Konferenz in Neu Delhi, Indien: 09. bis 11.09.2014**
  Auf der wichtigsten internationalen Common Criteria Konferenz wird atsec auch 2014 wieder vertreten sein.

- **it-sa in Nürnberg: 07. bis 09.10.2014**
  Auf der größten IT-Sicherheitsmesse im deutschsprachigen Raum wird sich atsec auch im Jahr 2014 wieder mit einem eigenen Stand präsentieren.

- **International Cryptographic Module Conference (ICMC) in Washington D.C., USA: 19. bis 21.11.2014**
  Die Experten-Konferenz für kryptografische Module findet auch 2014 wieder mit Unterstützung von atsec statt. Für Details siehe http://icmconference.org/.

atsec it security blog
Verfolgen Sie brandaktuell Diskussionen und Erlebnisse unserer Mitarbeiter auf http://atsec-information-security.blogspot.de

„Secure“ Messenger

Für Privatpersonen und Unternehmen ist die Kommunikation ausschließlich über E-Mail schon lange nicht mehr zeitgemäß. Stellt ein Unternehmen keinen eigenen Messaging-Dienst zur Verfügung, suchen sich viele Mitarbeiter selbst eine für sie adäquate Möglichkeit, private und geschäftliche Informationen auszutauschen. Ende Februar übernahm Facebook für 19 Milliarden Dollar den Messaging-Dienst WhatsApp. Genaue Gründe für den hohen Kaufpreis nannte Mark Zuckerberg nicht, erklärte jedoch mehrfach: „Es gibt mehrere Wege, wie wir damit Geld verdienen können.“

Dies, zusammen mit den konzeptionellen Sicherheitsmängeln von WhatsApp lässt viele Nutzer über einen Wechsel nachdenken. Dies sollten Unternehmen jetzt nutzen und eine sichere Alternative für ihre Businesskommunikation fest legen. Doch welcher der „sicheren“ Messenger ist der Richtige? Zunächst gilt es erst einmal zu überlegen, welche Kriterien ein solcher Messenger erfüllen muss:

- Ein Messenger muss den Übertragungsweg zwischen den Gesprächspartnern absichern können.
- Er muss gewährleisten, dass nur die Gesprächsteilnehmer selbst die für sie bestimmten Nachrichten lesen können (Ende-zu-Ende-Verschlüsselung).
- Er muss eine unabhängige Überprüfung der Implementierung seiner Sicherheitsfunktionen ermöglichen. Dem Schlagwort „Secure“,mit dem sich mehrere Messenger schmücken, sollte nicht blind vertraut werden. Wie Heartbleed zeigt, ist Open Source zwar nicht die Lösung aller Probleme, aber es ermöglicht eine unabhängige Prüfung des Quellcodes und der damit verbundenen Implementierung der Kryptofunktionalität.
- Ein Messenger muss die Kommunikationspartner auf einfachem Weg zusammen bringen. Der komfortabelste Weg ist der Abgleich von Kontakten mit der Nutzerdatenbank des Messengers. Hierbei werden allerdings datenschutzrelevante Informationen an Dritte weitergegeben, ohne zu wissen, wie vertraulich diese damit umgehen. Besser wäre wenn einzelne Kontakte für den Abgleich ausgewählt oder die Datenbank manuell durchsucht werden könnte.
- Er muss die Kommunikationspartner sicher authentifizieren. Dazu müssen initial die öffentlichen Schlüssel so ausgetauscht werden, dass die Verbindung zwischen Person und Schlüssel eindeutig ist. Dies kann zum Beispiel über das Scannen eines QR-Codes bei einem persönlichen Treffen geschehen.
- Er muss den Missbrauch des Benutzerkontos bei Verlust oder Diebstahl des Smartphones verhindern, z. B. durch Sperrung des Kontos. Manche Messenger bieten auch weitergehende Funktionen an, welche die Vertraulichkeit der Nachrichten gewährleisten, z. B. das Löschen aller alten Nachrichten auf dem Smartphone.

Anhand dieser Kriterien haben wir exemplarisch eine Reihe von Messengern auf ihre Sicherheit hin untersucht. Die Ergebnisse für die drei Textmessenger, die dabei am besten abschnitten, werden nachfolgend kurz vorgestellt:

Threema verwendet zur Absicherung des Transportweges und für die Ende-zu-Ende-Verschlüsselung die Krypto-Bibliothek „NaCl“[1] von Daniel J. Bernstein. Threema bietet eine Möglichkeit die Implementierung der Verschlüsselung zu überprüfen. Ein Zugriff auf den Quellcode ist jedoch nicht möglich. Ein weiteres positives Merkmal von Threema ist sein Umgang mit den Kontakten der Benutzer. Threema benötigt keine Synchronisation der Kontaktinformationen, bietet sie aber an. Sofern kein automatischer Abgleich der Kontakte konfiguriert ist, können Kontakte nur durch das gegenseitige Scannen oder die manuelle Eingabe der ID hinzugefügt werden. Für den automatischen Abgleich der Kontakte werden E-Mail-Adressen und Telefonnummern aus dem Adressbuch als Hash und SSL/TLS verschlüsselt an die Threema Server übertragen. Diese halten die Hashes kurzzeitig im Arbeitsspeicher, um die Liste der übereinstimmenden IDs zu ermitteln und löschen sie anschließend wieder. Sollte das Mobiltelefon, auf dem sich Threema befindet, abhanden kommen, gibt es die Möglichkeit, die eigene ID durch ein zuvor erstelltes Backup wieder einzuspielen. Gegen unbefugten Zugriff hilft eine Code-Sperre, die jedoch manuell nach der Installation aktiviert werden muss. Sollte diese nicht aktiviert gewesen sein, muss eine neue ID erstellt, diese mit der bisherigen Rufnummer und E-Mail-Adresse verknüpft und alle bisherigen Gesprächspartner über den Wechsel der ID informiert werden.

sayHEY verwendet für die Verschlüsselung AES 128bit. Entwickelt wurde sayHEY von simyo. SayHEY vereint sicheres Instant Messaging mit der Standard-SMS-Funktionalität und verspricht eine Ende-zu-Ende-Verschlüsselung der Nachrichten. Leider bietet sayHEY bisher keine Möglichkeiten den Quellcode einzusehen oder die Implementierung der Verschlüsselung selbst zu verifizieren, daher bleibt es beim Vertrauen. Die Synchronisierung von Kon-

taktinformationen ist freiwillig. Der Nutzer selbst entscheidet, ob er alle oder nur einzelne Telefonnummern seines Adressbuches mit dem Server abgleichen möchte. Diese Kontaktinformationen werden als Hash übertragen und mit dem privaten Schlüssel des jeweiligen Nutzers verschlüsselt auf dem Server gespeichert. Weiterhin versichert simyo, dass sich alle sayHEY-Server in Deutschland befinden und somit dem deutschen Datenschutzgesetz unterliegen. Als Transportverschlüsselung verwendet sayHEY SSL/TLS. Ein Plus ist der Umgang mit dem Passwort, welches bei der initialen Einrichtung des Messengers vom Benutzer vergeben und zur Verschlüsselung des privaten Nachrichtenschlüssels verwendet wird. Dank „Secure Remote Password (SRP)“ wird dieses Passwort niemals von der Messaging-App im Smartphone an den Server übertragen. Sollte das Smartphone abhanden kommen, kann man sich an die Entwickler wenden um den Zugriff auf den Dienst zu deaktivieren. Somit bleibt die Vertraulichkeit von zukünftigen Nachrichten gewahrt ohne alle Kontakte über den Verlust des Smartphones informieren zu müssen. Ein Mechanismus zur Wahrung der Vertraulichkeit alter Nachrichten existiert nicht.

TextSecure wurde als Open Source Software unter dem Projekt „Open WhisperSystems“ veröffentlicht. Die Ende-zu-Ende-Verschlüsselung basiert auf dem „Off the Record“ (OTR) Protokoll, beinhaltet aber unter anderem Verbesserungen in Bezug auf Forward Secrecy. Gründer und Entwickler von Whisper Systems –Moxie Marlinspike– beschreibt in dem Blog-Artikel „The Difficulty Of Private Contact Discovery“[2] das bisher ungelöste Problem des Abgleichs von Kontaktinformationen, ohne diese an einen Server zu übertragen und dort zu speichern. Sein Resümee ist, dass ein Hash aufgrund der Menge an verfügbaren Zeichen keine adäquate Methode ist, da mit Hilfe einer Hashmap, Rückschlüsse auf die Telefonnummern gezogen werden können. Daher lädt TextSecure zwar Telefonnummern in regelmäßigen Abständen als Hash zum Abgleich mit der Benutzerdatenbank hoch, löscht diese aber direkt nach der Verarbeitung wieder. Um die Authentizität des Absenders zu verifizieren, kann bei TextSecure ebenfalls ein QR-Code gescannt werden. Der Nachrichtenspeicher ist mit einer Passphrase verschlüsselt, welche bei jedem Neustart des Smartphones eingegeben werden muss. Zur Wahrung der Vertraulichkeit von Nachrichten kann dieser Timeout auf bis zu eine Stunde herabgesetzt werden. Sollte das Smartphone abhanden kommen, bietet Textsecure die Möglichkeit ein zuvor erstelltes Backup wieder einzuspielen.

Alle oben aufgeführten Messenger stellen eine sicherere Alternative zu WhatsApp dar. Welche App aber am besten geeignet ist, hängt vom Schutzbedarf und von den eigenen Anforderungen ab. Durch den erhöhten Schutzbedarf in der Unternehmenskommunikation sollte aber auf jeden Fall ein Messenger mit einer adäquaten Implementierung der Ende-zu-Ende-Verschlüsselung gewählt werden. Alle hier vorgestellten Messenger erfüllen diese Anforderung, jedoch werden sie auf den Servern der jeweiligen Anbieter betrieben. Dadurch passieren alle Nachrichten deren Server oder werden sogar auf ihnen gespeichert. Bestehen hinsichtlich der Verfügbarkeit oder trotz der Ende-zu-Ende-Verschlüsselung Bedenken bei der Vertraulichkeit muss auf Alternativen zurückgegriffen werden, welche auf eigenen Servern installiert und betrieben werden können. Aus diesem Grund setzt atsec einen eigenen Jabber-Server für die interne Kommunikation ein.

	Threema	sayHEY	TextSecure
Absicherung des Transportweges	+	++	+
Ende-zu-Ende-Verschlüsselung	+	+	+
Überprüfbarkeit der Implementierung	+	–	++
Verarbeitung von Kontaktinformationen	+	++	–
Sicherstellung der Authentizität	++	–	+
Maßnahmen bei Verlust des Smartphones	+	++	+

[1] *http://cr.yp.to/highspeed/naclcrypto-20090310.pdf*
[2] *https://whispersystems.org/blog/contact-discovery/*

DevOps

Ein klassisches Problem in der IT ist die Schnittstelle zwischen Softwareentwicklung und Betrieb. Meist sind diese Tätigkeitsbereiche in getrennten Teams organisiert, ziehen unterschiedliche Persönlichkeiten an und weisen eine gewisse, mehr oder weniger freundschaftliche, Rivalität auf. Die Sensibilisierung für dieses Problems hat zur sog. DevOps-Bewegung geführt, die beide Gruppen stärker integriert und die Entwicklungsdauer von Software erheblich beschleunigen kann. Neben wirtschaftlichen Einsparungen kann dies auch positive Aspekte für die Software-Sicherheit haben.

Wer mit dem Begriff „DevOps“ nicht näher vertraut ist, der findet hier eine kurze Einführung. DevOps hat seine Wurzeln in der agilen Softwareentwicklung mit ihren stark iterativen Entwicklungszyklen. Bestes Beispiel dafür ist heute die Entwicklung mit SCRUM. Führt man den iterativen Ansatz konsequent zu Ende, möchte man letztendlich seine Software regelmäßig, am besten permanent, releasen und dabei gleich testen. Dies alles soll idealerweise vollautomatisch geschehen, auf verschiedenen Umgebungen, die ebenfalls automatisch ausgerollt werden können. Durch die permanenten, automatischen Releases baut man die typischen Spannungsfelder zwischen Entwicklung und Betrieb ab: Gerade bei der Übernahme von Software aus der Testumgebung in eine Produktivumgebung kommt es meist zu vielen unliebsamen Überraschungen und damit zu Problemen zwischen beiden Abteilungen. In der Regeln sind Testumgebungen und Produktivumgebungen zwar „ähnlich“ aufgebaut, aber dann doch nicht identisch. In der Hektik des Moments beginnen dann Entwickler, die Software auf dem Produktivsystem anzupassen, Hauptsache, „es läuft irgendwie“. Die Spätfolgen zeigen sich dann im laufenden Betrieb, wenn sich nach und nach die Probleme dieser „Fixes“ und „Workarounds“ herauskristallisieren.
Bei der Umstellung der Entwicklungsmethode auf DevOps bieten sich gute Chancen, auch gleich die Gesamtsicherheit des Produkts zu verbessern.

Automatisiertes Testing

Idealerweise nutzt man für die Durchführung von Tests ein sog. Continuous Integration (CI) Testing System. Dabei wird sämtlicher Code aus dem Code-Repository eines Projekts automatisch in eine Testumgebung integriert bevor die vordefinierten Testsets gestartet werden. Dies erfolgt i.d.R. mehrmals am Tag zu festen Zeiten. Neben den rein funktionalen Tests eignet sich das CI-System auch, um ein Set von Security-Tests ablaufen zu lassen. Insbesondere sollten hier auch Tests auf alle bekannten Sicherheitsschwachstellen der Vergangenheit enthalten sein, die das Produkt betroffen haben. Dies verhindert das bekannte Phänomen, dass Schwachstellen, die längst als beseitigt gelten, durch Import von alten Codeteilen wieder zum Leben erweckt werden.

Automatisierte Erstellung von Umgebungen

Umgebungen sollten komplett automatisiert erstellt werden. Natürlich wird es vermutlich weiterhin einige Unterschiede zwischen den verschiedenen Umgebungen (Produktion, Testing, Entwicklung ...) geben. Allerdings sind diese Unterschiede dann bekannt und kontrollierbar. Mehrere Umgebungen des selben Typs sind identisch, was dafür sorgt, dass verschiedene Entwickler auf identischen Umgebungen arbeiten. Das CI Testing findet dann ebenfalls auf einer kontrollierten Umgebung statt, die bei Bedarf auch jedes mal komplett neu erstellt werden kann. Aus Sicherheitssicht hat dies den Vorteil, dass die Versionen von Bibliotheken und Hilfsprogrammen in den Umgebungen zentral gesteuert werden können. Sollte eine dieser Komponenten Schwachstellen aufweisen, kann durch eine zentrale Anpassung eine neue Version in alle Umgebungen eingespielt werden. Das CI-System erlaubt dann sofort einen zeitnahen Test, ob die neue Version Nebenwirkungen beim Build-Prozess aufweist.

Automatisierte Konfiguration von Umgebungen

Neben der reinen Erstellung von standardisierten Umgebungen ist es auch sinnvoll, diese zentral zu konfigurieren. Hier kommt ein Configuration Management (CM) System ins Spiel. Auch wenn Umgebungen vom selben Typ sind (z. B. die „Entwicklungsumgebung“), wird es einen Satz gemeinsamer Konfigurationsparameter und einen Satz individueller Parameter (IP-Adresse, lokale User ...) geben. Das zentrale CM sorgt dafür, dass diese Parameter automatisch auf die Umgebungen ausgerollt werden. Durch die zentrale Steuerung ergeben sich Vorteile für die Gesamtsicherheit der Systeme, da menschliche Fehler reduziert werden und Security-Experten sich auf ein zentrales System konzentrieren können.

Fazit

Die Einführung eines hochiterativen Entwicklungszyklus auf Basis von DevOps erfordert einige Ressourcen, motivierte Mitarbeiter in Entwicklung und Betrieb, sowie ganz allgemein einen großen Durchhaltewillen. Wenn die Methode einmal umgesetzt ist, dann ergeben sich langfristig neben finanziellen Vorteilen und deutlich schnelleren Release-Zyklen auch Vorteile für die Sicherheit der Produkte. Dies muss allerdings von Anfang an in der Planung eines DevOps-Ansatzes berücksichtigt werden.

IMPRESSUM

atsec information security GmbH
Steinstraße 70
81667 München
Deutschland
Telefon: +49-89-442-49-830
Telefax: +49-89-442-49-831
E-Mail: info@atsec.com

Vertretungsberechtigte Geschäftsführer:
Salvatore la Pietra
Staffan Persson
Registernummer: HRB 129439
Registergericht: Amtsgericht München
UST-ID-Nr. gemäß § 27a UStG:
DE205370914
Verantwortlich für den Inhalt:
Staffan Persson (Anschrift s.o.)