Sensible Informationen : welche Sicherheit leiste ich mir?

Autor(en): **Stocker, Axel / Müller, Peter**

Objekttyp: **Article**

Zeitschrift: **ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift**

Band (Jahr): **181 (2015)**

Heft 4

PDF erstellt am: **22.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-513487

Sensible Informationen – Welche Sicherheit leiste ich mir?

Unser Alltag ist geprägt von einer Flut an Informations- und Datenaustausch. Die damit verbundenen Sicherheitsrisiken werden häufig verkannt. Handelt es sich nur um ein Thema für Militärkreise und Regierungsstellen («Feind hört mit»)? Wie schütze ich mich nachhaltig und ohne Administrationsaufwand? Oberst Axel Stocker, Regional Operations Manager der Omnisec AG, stellt sich diesen Fragen.

Interview: Peter Müller, Redaktor ASMZ

Peter Müller: Mit Geschäftspartnern telefoniert, einen Berichtsentwurf per E-Mail weitergeleitet, ein vertrauliches Dokument im firmeninternen Netzwerk fertiggestellt, per MMS eine Geburtstagsfesteinladung verteilt und im Internet mittels Kreditkarte die Ferien gebucht: Unser Alltag ist geprägt von Informationsaustausch und Datenbearbeitung. Welche Sicherheitsüberlegungen hätten mir dabei durch den Kopf gehen sollen?

Axel Stocker: Die erste Überlegung muss immer sein, «was will ich gegen wen, wie sicher und warum schützen?». Aufgrund dieser Lagebeurteilung müssen dann die entsprechenden Massnahmen ergriffen werden. Heute kann keiner mehr sagen, er hätte nicht vermutet, dass Informationen abgehört werden oder Hintertüren die Sicherheitssysteme ad absurdum führen. Der «Snowden-Bericht» ist nicht der erste und wird nicht der letzte sein. Als Nachrichtenoffizier stelle ich fest, dass die Gegenseite mehr kann als vermutet wird und der Datenhunger weiterhin sehr gross ist.

Im Ereignisfall wird oft entschuldigend festgehalten: Eine absolute Sicherheit gibt es nicht. Umgekehrt werben spezialisierte Sicherheitsfirmen – wie die Omnisec AG – beispielsweise mit einer 100 % sicheren kryptologischen Verschlüsselung während Jahren. Wie lässt sich dieses Versprechen in der Praxis umsetzen?

Eigentlich sehr einfach: Man braucht nur die zentralen Elemente in der eigenen Hand zu haben. Alle unsere Lösungen basieren auf einem einzigen, eigenen Konzept: OmniCrypt. Das beginnt bei der Generierung der Zufallszahlen für die Schlüsselerstellung und geht über Schlüsselverteilung, Hardware, Software, Algorithmen und Protokolle bis hin zur Integration.

Ein Hochsicherheitshandy – erkennen Sie die Unterschiede?
Bild: Omnisec

Warum soll eine proprietäre Lösung wie OmniCrypt besser sein als eine Standardlösung, welche weit verbreitet ist?

Gehen wir davon aus, dass die Aussagen zur Einflussnahme der Geheimdienste betreffend Nachrichtenbeschaffung keine Gerüchte sind. Die Basis für alle Verschlüsselungen sind Zufallszahlen. Es gibt Hinweise auf eine Einflussnahme, als entsprechende Standards definiert wurden. OmniCrypt basiert auf einem physikalischen Phänomen, nämlich dem thermischen Diodenrauschen. Die Physik kann nicht beeinflusst werden. Standardverschlüsselungen wie AES (Advanced Encryption Standard) sind öffentlich beschrieben, werden als Turngerät an der Universität verwendet und zwei Bit sind schon gelöst. Anbieter einer AES-Lösung differenzieren sich oft durch eine nicht offengelegte Software-Blackbox von der Konkurrenz. OmniCrypt ist gegenüber dem Kunden transparent, dadurch hat er eine 100 %-Kontrolle über seine Lösung.

Sicherheit bei sensiblen Informationen ist vor allem für das Militär, Regierungsstellen und Unternehmen von zentraler Bedeutung. Wer ist der Haupttreiber hinter den verschiedenen Sicherheitsangeboten im Informationsbereich? Muss sich der Laie darunter eher ein Dual-Use-Produkt vorstellen oder gibt es typische Unterschiede für diese Hauptkunden?

In der Presse konnte man genügend über die Sicherheit von Dual-Use-Telefonen lesen, die durch eine App oder einen Chip «geschützt» wurden. Es gibt keine eierlegende Wollmilchsau. Bei unserem Telefon wurde das Betriebssystem umgeschrieben, viele Funktionen entfernt und wir geben das Modell vor. Hochsicherheit verlangt gewisse Auflagen. Nachrichtendienste haben Nachrichtenbeschaffung als Regierungsauftrag. Einige Nationen weiten das bis in den Wirtschaftsbereich aus. Als Firma in einem Schlüsselbereich (Finanzen, High-Tech, Rohstoffe usw.) muss ich davon ausgehen, ein Ziel zu werden. Auch ein Schulterschluss von Regierungen und kriminellen Gruppen kommt vor. Schlimm wird es, wenn der Benutzer glaubt, seine Kommunikation sei sicher und er sich entsprechend sorglos verhält.

Was verstehen Sie unter «falschem Verhalten»?

Erinnern wir uns an TOZZA: Wenn ich über einen unsicheren Kanal kommuni-

ziere, verschleiere ich die sensitiven Aussagen. Bei einem sicheren Kanal, kann ich alles klar benennen. Ist dieser «sichere Kanal» aber kompromittiert, gebe ich unwillentlich alles preis. Dieser Fall tritt leider häufig bei Dual-Use-Geräten auf. Entweder durch einen Benutzerfehler oder weil der ungeschützte Teil des Gerätes kompromittiert wurde.

Festnetz, Mobilfunk, Fax oder Internet bieten unterschiedliche Sicherheitsherausforderungen. Und schliesslich ist den verschiedenen Klassifizierungen der Informationen Rechnung zu tragen. Wie löst man diese vielfältigen Anforderungen in der Praxis getreu dem Firmenmotto von Omnisec AG «keep your secrets secret» – vor allem auch unter risikoorientierten und ökonomischen Überlegungen?

Innerhalb der eigenen Organisation sind es vor allem organisatorische Massnahmen wie z.B. keine Speicherung auf privaten Datenträgern, Zutrittsschutz usw. Will ich Informationen austauschen, müssen sie meinen Perimeter verlassen und geschützt werden. Wenn ich nur einen «single point of entry» vom und zum Internet habe, kann ich diesen besser schützen und überwachen (Konzentration der Kräfte). Ökonomisch ist es sinnvoll, wenn ich nur ein System beschaffen und betreiben muss. Alle unsere Lösungen sind für die höchsten Sicherheitsanforderungen zugelassen.Wenn ich eine für GEHEIM zugelassene Lösung verwende, ist VERTRAULICH automatisch auch erlaubt. Die Kosten, welche durch Informationsverlust entstehen, sind enorm und werden leider oft nicht berücksichtigt. Sie sind ein Mehrfaches der Einsparungen einer billigen Lösung, welche oft schwächer ist. Die indirekten Kosten wie Recovery, Reputation usw. sind dabei noch gar nicht berücksichtigt.

Ältere Armeeangehörige können sich noch gut an die Funkverschlüsslung vor rund 30 Jahren erinnern: Sperrige, schwere Zusatzgeräte, aufwendige Chiffrierschlüsselverwaltung und geheime Geräteklassifikation bei eingestelltem Schlüssel. In der Verwaltung und in der Privatwirtschaft stöhnen manche noch heute über das mühsame Handling unterschiedlicher Passwörter für unterschiedliche Zwecke und mit unterschiedlicher Gültigkeitsdauer. Ist die Sicherheitshandhabung sensibler Informationen heute benutzerfreundlicher geworden?

Mein Rücken kennt das SVZ-B auch noch. Wir unterscheiden Vorgaben, Bereitstellung und Bedienung. Eine Vorgabe ist zum Beispiel das seriöse Handling, welches ein Hochsicherheitshandy fordert: Man lässt es im Hotel nicht offen herumliegen. Das System- und Usermanagement erfolgt im aktiven Netz zentral über einen verschlüsselten Kanal. Und auch hier werden das Vier-Augen- sowie Need-to-know-Prinzip konsequent umgesetzt. Das Handling ist einfach und damit fehlerrobust. Bei unseren Lösungen kann die Verschlüsselung nicht deaktiviert werden, deshalb ist man mit unserem Handy immer auf der sicheren Seite. Das Handling soll ähnlich sein wie bei einem «normalen» Gerät.

Omnisec AG ist ein unabhängiges, rein schweizerisches Unternehmen mit Sitz in Dällikon ZH. Omnisec steht für rund 70 Jahre Erfahrung auf dem Gebiet des kryptologisch verschlüsselten Informationsaustausches. Sicherheitslösungen von Omnisec stehen weltweit bei militärischen Organisationen und Regierungsbehörden erfolgreich im Einsatz, um Informationen bis zur Stufe STRENG GEHEIM sicher auszutauschen.
Das Angebot von Omnisec geht über die Entwicklung, Herstellung und Implementierung von Lösungen für einen abhör- und manipulationssicheren Informationsaustausch hinaus. Die umfassenden, skalierbaren Lösungen von Omnisec basieren auf OmnyCrypt™, einer einzigartigen, inhouse entwickelten Sicherheitsarchitektur.
Die kompromisslosen Qualitätsstandards und die hohe Innovationskraft von Omnisec manifestieren sich unter anderem in einer erfolgreichen Zusammenarbeit mit der auf dem Gebiet der Kryptologie weltweit führenden Eidgenössischen Technischen Hochschule (ETH) in Zürich. Omnisec ist nach ISO 9001:2008 zertifiziert.

Der Mensch selber stellt bekanntlich immer noch das grösste Sicherheitsrisiko dar, besonders wenn er die Gefahren verkennt, in Eile handelt oder sich Routine einstellt. Ein Produkt kann aber auch in falsche Hände geraten (z.B. Werkspionage durch Diebstahl) oder für andere Zwecke eingesetzt werden (z.B. Eindringen in geschützte fremde Netze). Welche Massnahmen ergreift Omnisec, um solche Risiken zu umgehen oder zumindest zu minimieren?

Die kritischen Bereiche sind: Werkspionage, Fehlmanipulation, Diebstahl. Alle Mitarbeiter von Omnisec sind IOS-überprüft und wir nutzen unsere Lösungen. Die Besitzverhältnisse von Omnisec sind transparent. Dem Kunden gegenüber legen wir seine Lösung vollständig offen. In unseren rund 70 Jahren gab es keine seriösen Anschuldigungen bezüglich Spionage oder Backdoors. Unsere Lösungen sind benutzerfreundlich und stressresistent: Die Verschlüsselung ist immer aktiviert, das verhindert Fehlmanipulation. Selbst gegen bewusste Fehlmanipulation wurden Massnahmen ergriffen und die praxiserprobten Lösungen unterstützen den Betreiber beim Umsetzen seiner Sicherheitsvorgaben. Alle Daten auf den Geräten sind verschlüsselt und damit sicher. Beim Handy hat der User die Möglichkeit, das Gerät mit einem «Stresscode» zu löschen: Wird ein Gerät gestohlen, kann es der Kunde aus der Ferne («remote») neutralisieren.

Die technologischen Quantensprünge folgen sich teilweise Schlag auf Schlag. Wie sieht die Entwicklung bei der Informationssicherheit aus? Zeichnen sich kurz- und mittelfristig wesentliche Änderungen ab und wie soll diesen Herausforderungen begegnet werden?

Ich bin weder Wahrsager noch Kryptologe. Glaubt man aber den Kryptologen, so ist das Rennen gegen Angriffe auf eine korrekt implementierte und saubere Verschlüsselung gewonnen. Ein staatlicher Angreifer hat zusätzliche Möglichkeiten. Seien es Forderungen von Backdoors, Meta-Daten-Auswertungen bis hin zu rechtlichen Auflagen. Besonders die rechtlichen Auflagen werden weiter zunehmen und dürfen oft nicht kommuniziert werden. Hat ein Anbieter Verbindung zu einem Land mit einem starken und offensiven Nachrichtendienst, so muss ich davon ausgehen, dass alle Daten gegenüber dem Geheimdienst offengelegt werden müssen. Der Anbieter darf seine Kunden darüber nicht informieren. Hier verweise ich erneut auf den «Snowden-Bericht». Mit der steigenden Mobilität werden Gegenmassnahmen wie zum Beispiel SIM-Karten-Wechsel schwieriger. Bei unserem Handy kann ich eine lokale SIM-Karte verwenden, ohne dass sich meine Rufnummer ändert. Metadatenauswertungen sind sinnlos, da ich in einem Sternnetz kommuniziere: Von aussen kann nicht erkannt werden, mit wem ich telefoniere. Als Nof aber auch als Betriebswirtschafter sage ich, dass die Angriffe zunehmen werden: Information ist das neue Gold. Der wichtigste Schutz sind eine erhöhte Wachsamkeit und der kompromisslose Schutz meiner Informationen, sobald sie meinen physischen Perimeter verlassen. ■