IT-Sicherheit – ein Überblick

Version 1.0, 16.09.2014

Dieses Dokument soll Ihnen einen groben Überblick darüber geben, worauf es beim Thema IT-Sicherheit ankommt, damit Sie das, was Sie in einer Schulung lernen, besser einsortieren können: Was bringt Ihnen die Technik, wo sind ihre Grenzen? Was brauchen Sie, und was müssen Sie lernen, um dieses Ziel zu erreichen?

Aspekte

Die Software, die Ihnen auf der Schulung nähergebracht wird, soll einen oder mehrere dieser drei Aspekte leisten:

1. *Vertraulichkeit (Verschlüsselung)*

   Das Ziel: Die Daten werden so verändert, dass niemand außer den legitimen Empfängern in der Lage ist, auf direktem Weg die Ursprungsdaten wiederherzustellen. Verschlüsselung ist die einfachste der drei Techniken (damit gibt es die wenigsten Sicherheitsprobleme).

   Ein wichtiger Unterschied verbreiteter Verfahren ist die Dauer der Entschlüsselbarkeit. Abgeschlossene Datenpakete (asynchrone Kommunikation), etwa E-Mail, werden zumeist für langlebige Schlüssel verschlüsselt; das heißt, dass sie immer wieder entschlüsselt werden können. Das hat natürlich Vorteile, kann aber zum Problem werden, wenn Schlüssel in die falschen Hände geraten, weil dann womöglich die gesamte Kommunikation eines langen Zeitraums entschlüsselt werden kann. Bei synchroner Kommunikation – also etwa dem Zugriff auf Web- und Mailserver (Transportverschlüsselung) oder bei Chats – kann man (ohne Tricks) eine andere Art der Verschlüsselung verwenden, bei der die Schlüssel nur kurz gespeichert werden. Gelangt ein Schlüssel in die falschen Hände, kann damit (im Idealfall) nur sehr wenig entschlüsselt werden. Diese Funktion nennt man *(Perfect) Forward Secrecy ((P)FS)*. Die offensichtlichen Grenzen dieser Technik liegen darin, dass dort, wo man die langlebigen Schlüssel klauen kann, meistens auch die unverschlüsselten Daten liegen. Wer (im laufenden Betrieb) in Ihren Rechner einbricht, muss nicht mehr entschlüsseln.

   Bedenken muss man aber, dass reine Verschlüsselung (ohne ergänzende Maßnahmen) kein Allheilmittel ist. Bei Informationen, die dem Angreifer nicht zugänglich sind, gibt es kein Problem, aber wenn es nur darum geht festzustellen, welche Inhalte Sie z.B. auf einer Website gelesen haben oder welche von mehreren bekannten Dateien Ihnen jemand verschlüsselt geschickt hat (oder ob überhaupt eine Datei oder welche Art von Datei), dann mag es ausreichen, die Menge der übertragenen Daten zu kennen. Von größerer praktischer Bedeutung ist, dass bei E-Mail aus historischen Gründen der Betreff nicht verschlüsselt wird, sondern nur der Text und eventuelle Anhänge. Neuere Systeme haben dieses Problem nicht.

2. *Authentizität (Signaturen)*

   Bei verschlüsselten und unverschlüsselten Daten ist gleichermaßen von Interesse, von wem sie stammen. Dafür gibt es digitale Unterschriften. Durch den Vergleich der Daten mit der Unterschrift wird die Integrität der Daten gesichert (d.h., dass die Daten nach dem Unterschreiben nicht verändert wurden); die Unterschrift kann einem Schlüssel zugeordnet werden und der (allerdings nicht automatisch) einer Person oder Organisation.

   Die wichtigste Unterscheidung bei Signaturen ist, ob man sie gegenüber Dritten nutzen kann. Bei einer Signatur für asynchrone Daten (E-Mail) können Sie z.B. vor Gericht die Daten und die Unterschrift vorlegen und damit nachweisen, dass der Absender (bzw. jemand mit Zugriff auf seinen Schlüssel...) wirklich diese Daten geschickt hat (ob er die an Sie geschickt hat, ist damit nicht automatisch klar). Ob diese (aufwendigere) Möglichkeit gewünscht ist, hängt von den Umständen ab. Bei synchroner Übertragung (z.B. Webserver, Chat) wird zumeist so verfahren, dass die Authentizität des Kommunikationspartners zu Beginn sichergestellt wird und danach nur noch ein Verfahren verwendet wird, das die Integrität sichert. Das heißt, Sie haben während der Verbindung die Gewissheit, dass der andere die Daten genau so geschickt hat, können dies aber nicht dafür verwenden, hinterher Dritten gegenüber nachzuweisen, was der andere geschickt hat. Diese Funktion nennt man *plausible deniability*.

   Ein notwendiger Zwischenschritt bei der Erzeugung von Signaturen (die Hashwerte) ist viel komplizierter als Verschlüsselung, so dass dort immer wieder Fehler gefunden werden und Signaturen eine "permanente" Baustelle sind. Unsicherheiten dieser Technik haben zur Folge, dass Unterschriften missbraucht werden können; es sieht dann so aus, als hätte man andere Daten unterschrieben.

3. *Vermeidung von Metadaten (Anonymisierung)*

   Mit dem Begriff Metadaten bezeichnet man die Umstände eines Kommunikationsvorgangs, also etwa den Absender, den Empfänger und den Zeitpunkt (bei E-Mail) oder die Adresse der übertragenen Daten (die URL bei Zugriffen auf Webserver). Gemeint ist damit sowohl ein rein technischer Empfänger (also etwa eine E-Mail- oder IP-Adresse oder Telefonnummer) als auch die Zuordnung dieser Adresse zu einer Person oder Organisation. Auch wenn man nicht weiß, zu wem eine Adresse gehört, kann es aufschlussreich sein, mit wer mit dieser Adresse kommuniziert. Das kann auch bei Verschlüsselung aller Daten die Zuordnung ermöglichen.

   Anonymisierung ist die komplizierteste der drei Techniken – und damit die fehleranfälligste. Sie wird auf Netzebene dadurch angestrebt, dass die Datenströme auf Umwegen durchs Internet geleitet werden (was sie zwangsläufig verlangsamt), so dass keiner der beteiligten Rechner sowohl Anfangs- als auch Endpunkt der Verbindung weiß. Anonymisierung auf Netzebene funktioniert mit ganz normalen Internetanwendungen.

   Außerdem gibt es Anonymisierung auf Anwendungsebene. Dies wird dadurch realisiert, dass für E-Mail, Chat, Webserver, Foren, Filesharing usw. neue Protokolle und Anwendungen entwickelt werden, die Anonymität ermöglichen sollen. Die beiden Ansätze dafür sind, dass es gar keine Server mehr gibt (reines Peer-to-Peer-System) und dass die Server selber anonym sind ("versteckt" in der Netzebene-Anonymisierung).

Sicherheit vs. Bequemlichkeit

Es wird oft gefordert, die Sicherheitssoftware müsse einfacher werden. Zweifellos ist bei der Benutzerfreundlichkeit noch Luft nach oben. Das darf aber nicht über eine harte Tatsache hinwegtäuschen:

Bequemlichkeit geht auf Kosten der Sicherheit

Aus u.a. folgenden Gründen:

- *Fingerprints*
  Die eindeutige Identifizierung der Kommunikationspartner (und Server) ist unerlässlich. Dafür muss man lange Hashwerte vergleichen, niedliche Zeichenketten dieser Art:
  `7D82 FB9F D25A 2CE4 5241 6C37 BF4B 8EEF 1A57 1DF5`
  Die müssen so lang sein (und aus einer sicheren Quelle – Papier!), weil nur eine ausreichende Länge verhindert, dass ein Angreifer die zugehörigen Daten (Schlüssel) fälscht. Es wurden bequeme Systeme geschaffen, die diese Prüfung automatisieren, aber damit gibt man die Kontrolle aus der Hand.
- *Sachkenntnis*
  Wenn man nicht weiß, was man gerade tut, hat man sowieso verloren – wenn man nicht von der Technik völlig entmündigt werden will. Gegen unbekannte Bedrohungen kann man sich nicht sinnvoll schützen. Folgender Richtwert: Die Sicherheit, die unterm Strich steht, ergibt sich
  zu 10% aus der Technik – zu 60% daraus, dass man (immer!) weiß, was man tut – zu 30% aus Disziplin
- *Rechnersicherheit*
  Normale Computer sind nicht zu schützen. Jede relevante Software hat Fehler, auch Sicherheitssoftware. Die Erkennungsrate von Virenscannern gegen Schadsoftware, die erst wenige Stunden alt ist, geht gegen null.
  Da Verschlüsselung (gegen gezielte Angriffe) wenig bringt, wenn man die Daten im Klartext einfach vom Rechner kopieren kann, haben sensible Daten auf normalen Computern schon mal gar nichts zu suchen. Die sichere Verschlüsselung der Laufwerke mit relevanten Daten sollte selbstverständlich sein.
- *verbindliche Absprachen*
  Die Technik setzt bestensfalls das um, was man möchte. Sie verhindert nicht, dass die Kommunikationspartner Unterschiedliches wollen. Das betrifft die Sicherheit der Verschlüsselung (also vor allem die der Rechner hinter der Verschlüsselung), aber auch die Bedeutung von Signaturen. Was heißt es, wenn eine Nachricht signiert ist? Ist das nur ein Schutz gegen Adressfälschung, oder hat die dadurch eine höhere Verbindlichkeit?

Sicherheitsniveaus: Wie viel braucht man?

Es ist wichtig, dass man sich klar macht, dass die eigenen Daten sehr unterschiedlich schutzbedürftig sind und man sie jeweils angemessen schützen muss – nicht zu wenig, aber auch nicht zu viel.

- *Vertraulichkeit (Verschlüsselung)*
  Entgegen verbreiteten Gerüchten kommt es nicht darauf an, dass alles verschlüsselt wird. Jeder muss im Bedarfsfall in der Lage sein, verschlüsselt zu kommunizieren – und zwar auf dem angebrachten Sicherheitsniveau. Die meisten Leute haben leider nur einen – schlechten – Schlüssel.
- *Authentizität (Signaturen)*
  Wofür verwendet man Signaturen – als Schutz vor trivialer Adressfälschung oder zur Sicherung von Informationen, deren Manipulation sehr peinlich und / oder sehr teuer wäre?
- *Vermeidung von Metadaten (Anonymisierung)*
  Ein weiteres Gerücht ist, dass Metadaten genauso viel wert seien wie die Daten selber. Das ist in dieser Allgemeinheit natürlich falsch. Dass man mit seiner Familie und seinen Freunden kommuniziert ist klar und nicht schutzbedürftig. Wer die Freunde sind, ist zumeist auch klar (Facebook, Telefonate). Bei E-Mail o.Ä. einen Kontakt zu verschleiern, der anderswo (für einen Geheimdienst) offensichtlich ist, bringt wenig.
  Gegenbeispiele: Wenn man regelmäßig verschlüsselt mit Prostituierten oder Leuten aus dem organisierten Verbrechen kommuniziert, dann mag man das Problem haben, dass man auch ohne Kenntnis des Inhalts erpressbar wird. Aber auch hier gilt: Auch die Handys sehr spezieller Dienstleister werden getrackt, und wenn die regelmäßig im selben Raum sind wie das eigene und diese Ereignisse eine auffällige Korrelation zu Besuchen bei Geldautomaten haben, dann rettet einen die anonymisierte E-Mail auch nicht mehr.
  Man sollte deshalb die eigenen Kontakte nüchtern danach bewerten, ob die Kommunikation mit ihnen verschleiert werden muss. Die meisten Leute werden keine kritischen Kontakte haben. Neue Technik wirkt sich sowieso nur auf neue Kontakte aus – denn über die vorhandenen wissen **DIE** ja schon alles. Der typische Anwender sollte sich erst mit Kryptografie vertraut machen und dann mit Anonymisierung.

Was ist zu tun?

- über Jahre beständig dazulernen; keine Hektik, sondern durchhalten
- sich mit Open-Source-Software vertraut machen (Linux, LibreOffice)
- (auch) offene, langlebige Systeme nutzen (XMPP mit z.B. OTR)
- mehr Sichtbarkeit des Themas → neue Nutzer: http://www.openpgp-schulungen.de/fuer/unterstuetzer/