Die großen Lügen der IT-Sicherheit

Es gibt jede Menge Thesen, Patentrezepte und andere Aussagen, die im IT-Umfeld versprechen, für Sicherheit zu sorgen. Für sich alleine genommen, entpuppen sich viele davon jedoch als glatt gelogen oder zumindest nicht „allein seligmachend", meint unser Autor und plädiert für einen umfassenden Ansatz jenseits von „Buzzword-Security".

Von Ramon Mörl, München

Angriffsvektoren werden immer komplexer, treten an bekannten, erwarteten, aber auch an völlig unerwarteten Stellen auf – es gibt Aussagen, dass bei bestimmten Angriffen kein Schutz möglich oder der Angriff noch nicht einmal erkennbar ist (vgl. [1]). Es ist also an der Zeit, traditionelle Verfahren und Handlungsmuster daraufhin zu prüfen, wie zeitgemäß sie sind. Dabei fällt auf, dass einige der Strategien und Thesen, die aktuell als valide Lösungsszenarien gehandelt werden, an dem Ziel einer adäquaten IT-Sicherheit mehr oder weniger vorbei gehen und das Ziel, einen optimalen Schutz mit den vorhandenen Mitteln umzusetzen, nicht erfüllen.

Dieser Artikel will gängige Thesen – für sich genommen und als alleiniges Ziel verfolgt – als „Lüge" entlarven und in den richtigen Kontext setzen. Dazu dient exemplarisch ein Angriffsmuster als Referenz, das auf einer Tagung der Allianz für Cyber-Security (www.allianz-fuer-cybersicherheit.de), durch zwei Mitarbeiter des Fraunhofer SIT vorgestellt wurde – es könnten aber hier auch viele andere Angriffe (Conficker, Stuxnet, Flame, ...) auf die Integrität eines Rechners als Beispiel fungieren.

Referenz-Angriff

Ein Angreifer übernimmt einen Standard-Client nur auf der Basis, dass beide Rechner im gleichen WLAN aktiv sind und der angegriffene Rechner einen Browser mit einer Softwareschwachstelle gestartet hat (und welcher Browser hat keine Schwachstelle?). Der angegriffene Anwender muss in diesem Szenario keinen „Ok"-Knopf drücken oder irgendeine kritische Aktion durchführen.

In der Konsequenz erlangt der Angreifer über Schadsoftware (z. B. Keylogger), die er installiert hat, alle Daten des Rechners, den Usernamen und dessen Passwort – kann also nicht nur alle Daten von dem angegriffenen System abgreifen, sondern auch selbst in das Firmennetz eindringen.

Thesen und Gegenrede

„Security-Awareness macht sicher!"

Einer der kostengünstigsten Wege IT-Sicherheit zu erreichen: Der gut geschulte Anwender handelt immer sicher! Technisch bleibt also nichts zu tun...?! Unabhängig davon, dass es immer gut ist, gut geschulte Anwender zu haben, lautet die wesentliche Frage, welchen Kernaufgaben mit welcher Wertschöpfung für das Unternehmen die einzelnen Anwender nachgehen. IT und besonders die Sicherheit der IT werden in professionell geführten Umgebungen gerne als Service wahrgenommen, der einfach gegeben ist, ohne dass Anwender Zeit damit verbringen müssten, bestimmte Risiken einzuschätzen.

Klar ist auch, dass der Anwender in dem eingangs beschriebenen „Referenzangriff" überhaupt keine Chance hat, sich gegen die Attacke zu verteidigen – außer vielleicht, am Flughafen, im Hotel oder unterwegs eben nicht zu arbeiten, was natürlich wieder eine produktivitätssenkende Lösung ist.

Besonders perfide an einer Schutztechnik, die sich nur auf die Security-Awareness der Anwender verlässt, ist die Schuldfrage: Denn wenn etwas passiert ist, dann ist logischerweise der Anwender schuld – eine schon aus sozialer Sicht nicht anstrebenswerte Lösung. Juristisch ist diese „Schuld" dann auch nicht in eine Haftung umsetzbar und entbindet den Vorstand oder die Geschäftsführung überdies nicht von der gesetzlich zugeordneten Verantwortung für Datenschutz und IT-Sicherheit.

Optimal ist es, jeden Mitarbeiter über die Risiken seines Wirkungsbereichs zu informieren und ihm – am besten technisch unterstützt – sichere Handlungsmöglichkeiten aufzuzeigen.

„Höchste Anti-Virus-Erkennungsrate ist wertvoll!"

Am Beispiel der am weitesten verbreiteten IT-Sicherheitsfunktion, den Anti-Virus-(AV)-Mechanismen, kann man gut eine andere Problematik erkennen: AV wird heute als 100% notwendig angesehen und

ist deshalb in jeder professionell betriebenen IT-Umgebung vorhanden. In vielen Entscheidungsprozessen wird der Kostenpunkt für die Virenabwehr entlang der Erkennungsrate des AV entschieden – je höher die Erkennungsrate des AV-Systems ist, umso mehr Geld ist sie wert. Allgemein bekannt ist, dass die Erkennungsraten aufgrund verschiedener Faktoren weit unter 100 % liegen.

Im Sinne eines sinnvollen 360-Grad-Schutzes und angesichts der leider immer gegebenen Begrenzung der Gesamtmittel für die IT-Sicherheit sollte man sich aber die Frage stellen, welche Budgets man gegen Schadsoftware richtet, die nicht von dem AV-System erkannt wird. Für den Entscheider ist dabei wichtig, dass jedem Angreifer im Internet Prüfroutinen zur Verfügung stehen, die verifizieren, ob und wenn ja von welchen AV-Systemen ein bestimmter Angriff erkannt wird – professionelle Angreifer verwenden natürlich nur solche, die kein AV erkennt.

Es ist also eine mögliche Strategie, durch Einsparung auf traditionellen AV-Systemen Geld freizuschaufeln, das in IT-Architekturen (z. B. virtuelle Schleusen, ReCoBS, ...) investiert wird, mit denen sich die blinden Flecke der AV-Systeme schützen lassen.

„Durchgängige Verschlüsselung ist wesentlich!“

Nach Snowden sind die Forderungen nach einer Ende-zu-Ende-Verschlüsselung zu Recht lauter geworden, um herauszustellen, dass dadurch die einfache Massendatensammlung erschwert wird (vgl. [2]). Beim geschilderten Referenzangriff stellt man aber fest, dass die Ende-zu-Ende-Verschlüsselung gegen eine Übernahme des Clients nicht schützt (für Verfeinerungen des Problembilds siehe etwa [3]). Im Gegenteil: Hat ein Angreifer den Client übernommen oder sogar eine Möglichkeit gefunden, ein Benutzerlogin zu erschleichen, so hilft ihm eine Ende-zu-Ende-Verschlüsselung eher sich zu verstecken, da bisherige Investitionen in IDS/IPS, Firewall, netzzentrierte Sicherheit und viele weitere Verfahren dadurch entweder nutzlos werden oder die Sicherheit der genutzten Kryptografie reduziert wird, weil die verwendeten Schlüssel an zu vielen Stellen bekannt und nutzbar sind.

Statt für Ende-zu-Ende-Verschlüsselung sollte die Energie besser in eine durchgehende Vertrauenskette investiert werden: Diese reicht technisch von den Ein-/Ausgabe-Geräten des Anwenders (Maus, Tastatur, Authentifizierungsdevices, ...) über die genutzten Services bis zu den Daten *und* berücksichtigt auch organisatorische Anforderungen an die Vertrauenswürdigkeit der Lösungen. Ähnlich wie das in der Nahrungsmittelindustrie zum Schutz der Bürger schon gängig ist, bedeutete das einen Herkunftsnachweis aller Bauelemente und die jeweiligen Erklärungen zu Datenschutz und -sicherheit der beteiligten Lieferantenkette.

„Komplexe Passwörter schützen Daten und Systeme!“

Vorwiegend aus der Smartphonewelt kommt die Idee, dass es für alles eine eigene App gibt: Braucht man etwa Licht, greift man zur Taschenlampen-App. Jeder prüft, ob diese App auch leuchtet, also ihre angekündigte Funktionalität erfüllt. Wenige stellen sich die Frage, was sie womöglich sonst noch macht – beziehungsweise: nicht machen darf. In dieser Einschätzungs-Welt kommen dann Apps, die Sicherheit versprechen gerade recht – der Anwender kennt ja bestimmte Sicherheitsmaßnahmen: Je komplexer das Passwort ist und je öfter ich das Passwort wechsle, desto sicherer bin ich.

Peter Schaar hatte auf der Fraunhofer-Konferenz „Future Security 2012 – Für eine sichere Zukunft“ als damals agierender Datenschutzbeauftragter Deutschlands gesagt: „Eine Anwendung kann nur so sicher sein wie das Betriebssystem, auf dem sie läuft.“ Die Sicherheitsanalyse von Android- oder iOS-Sicherheits-Apps muss das berücksichtigen und deshalb bis in die Analyse der AGB und die gültigen Rechtsketten sowie deren Durchsetzbarkeit reichen.

Zudem ist technisch zu beachten, dass andere Anwendungen das System ausspähen (z. B. alle Tastatureingaben) und dadurch Passwörter ebenfalls im Klartext erhalten können. Der Schutz von Daten, die etwa in einer Public Cloud liegen, ist dadurch also nicht gegeben und die Eingabe des Passworts nur ein Feigenblatt-Schutz.

Besonders tragisch ist es, wenn an sich gut funktionierende Sicherheitssysteme der „traditionellen Welt“ (z. B. Desktops, PCs, Notebooks) dadurch gefährdet werden, dass die Mechanismusstärke auf mobilen Systemen für die gleichen Datenbestände mit einer weit niedrigeren Stufe akzeptiert wird. Der Angreifer kann am „schwächsten Punkt“, hier dem Smartphone, das Passwort ausspähen und womöglich in verschlüsselte Daten einen dann auch verschlüsselten Schadcode infiltrieren, der anschließend einem Innentäter-Angriff auf die klassischen Clients gleichkommt.

Es gilt also, die Mechanismusstärke und den Wirkungsgrad der gesamten Lösung zu verstehen, um bewerten zu können, ob diese Lösung adäquat für die Services und Daten ist, auf denen sie operiert. Im Beispiel der Passworteingabe auf einem Smartphone war der schwache Schutzgrad für den Profi einfach erkennbar. Man stelle sich nun vor, ein Hard-/Softwarehersteller hätte mehrere Millionen Euro zur Verfügung und überlegt, ob er diese eher in die Sicherheit seines Produkts oder in die gute Vermarktung einer schwächeren Sicherheit investiert,

die dem Endkunden jedoch eine hohe Sicherheit vortäuscht. Leider ist die Mechanismusstärke einer komplexen Lösung heute auch für Profis nicht mehr einfach zu analysieren – der Konsument bleibt zunehmend alleine.

Den Blick dafür, ganze Systeme nach ihrem Schutzgrad und der Toleranz für fehleranfällige Produkte zu untersuchen, gibt es aktuell nur in der Hochsicherheit. Trotzdem täte es aber not, auch in anderen Umgebungen einfache Kochrezepte für ein sicheres Gesamtsystem zu entwickeln – leider findet sich im Moment kein Akteur, der diese Aufgabe ganzheitlich übernehmen will.

Ein erster Schritt könnte darin bestehen, vertrauenswürdige Produkte, Lieferanten, Betreiber und Dienstleister in langen Listen zu führen – doch auch diese verantwortungsvolle Tätigkeit will aktuell niemand wirklich übernehmen, der über die Sachkompetenz zur Beurteilung der komplexen Zusammenhänge verfügt *und* das Vertrauen des Marktes als neutrale Instanz genießt.

„Die Klassifikation von Daten bringt Sicherheit!“

In einigen der global tätigen Unternehmen ist aus dem Wunsch, sich vor unerwünschten Datenabfluss zu schützen, ein isoliertes Projekt zum Klassifizieren gespeicherter Daten (alias „Identifikation der Kronjuwelen“) übrig geblieben. Lösungen zu einer solchen Klassifikation haben aber nicht unbedingt auch Schutzfunktionen eingebaut: So haben einige gängige Systeme die Klassifikationsdaten einfach im Klartext als Attribut der Daten untergebracht – im schlimmsten Fall im so genannten Alternate-Data-Stream (ADS), wodurch die Klassifikationsattribute beim Kopieren auf andere Filesysteme (USB-Stick) oder beim Versand per E-Mail einfach verloren gehen.

Echte (zusätzliche) Sicherheit bringen nur Lösungen, die verifizieren, dass die Klassifikation an den Netzgrenzen (IP-Netze, aber auch asynchrone Übergänge an USB, Bluetooth etc.) ausgewertet werden, und einen Zugriff auf die Daten nur ermöglichen, wenn die Klassifikationsdaten von vertrauenswürdigen Instanzen ausgewertet und der intendierte Zugriff durch diese genehmigt wurden.

„Zum Schutz vor Datenklau (DLP) genügt es, abfließende Daten zu überwachen.“

Zur Erinnerung: Der oben skizzierte Referenzangriff zeigt, dass es ohne Zutun eines böswilligen Mitarbeiters, trotz guter Schulung möglich ist, dass ein Angreifer das Login des Anwenders simuliert – jeder Datenzugriff dieses illegalen Benutzers lässt nun Daten abfließen. Insofern ist es Pflicht in einem DLP-Projekt, auch vor Schadcode und Standardangriffen zu schützen, um zu vermeiden, dass fremder Code die Passwörter und Logindaten der Anwender ausspäht!

Mit Lösungen zu Besitz und Wissen (Two Factor Authentication) ist man möglicherweise eine Spur besser, wenn der „Besitz“ gegenüber der zentralen Authentifizierungsautorität direkt etwas nachweist, was nicht multiplizierbar ist.

„Wenn jeder alles richtig macht,...“

Nicht selten wird angenommen oder unterstellt, dass der Schutzgrad der Kommunikationspartner mindestens so hoch ist wie der eigene. In der IT-Sicherheit gilt jedoch: „Wer nicht Teil der Lösung ist, der ist Teil des Problems.“ Von außen lässt sich die Qualität, mit der eine Organisation den Schutz der eigenen IT durchsetzt, nur schwer beurteilen. Betrachtet man zusätzlich noch das Statement eines Mitglieds der Piraten-Partei, der das Recht auf Infektion seiner IT-Systeme mit Schadcode als Grundrecht forderte, dann erlangt man einen ersten Blick darauf, dass es bei diesem Thema längst nicht nur um technische Kompetenz oder Handlungswillen geht.

„Das Internet – in Deutschland ein rechtssicherer Raum“

Das Ansehen eines Films per Streaming wird in Deutschland rechtlich anders gewertet als das Ansehen eines Filmes nach einem Download beziehungsweise der Download selbst. Für Konsumenten schafft das die Notwendigkeit, sich nicht nur mit IT, sondern auch mit Rechtsfragen zu beschäftigen und diese in die richtige Beziehung zu setzen, um rechtskonform zu handeln.

Auf der anderen Seite: Die Diskussionen um die immer restriktiveren nationalen Datenschutzrichtlinien und die häufig vertretene Rechtsauffassung, dass dieses Datenschutzrecht per Gesetz für alle Daten aus Deutschland weltweit gültig ist, verstellt den Blick auf die Durchsetzbarkeit dieses Rechts. Nach wie vor gibt es Länder, in denen andere Gesetze gelten und in deren Rechtssystem weder die Exekutive noch die Legislative mit deutschen Behörden kooperieren. Bei der Durchsetzung nationaler Gesetze ist häufig auch die Frage der Beweislast und die Zugänglichkeit von Beweisen so organisiert, dass für das Opfer von Internetbetrügereien keine Chance besteht, den oder die Täter dingfest zu machen.

Wo rechtliche Probleme zum Durchgriff auf ausländische Akteure ungeklärt sind, kann es wichtig sein, den Raum, in welchem zulässig und sicher gehandelt werden kann, adäquat einzuschränken. Das Bundesministerium des Innern hat hier mit dem Erlass einer „No-Spy“-Klausel als Geschäftsbedingung bereits richtungsweisend agiert (vgl. www.tagesschau.de/inland/csc106.html).

„Wenn ich mich nicht vollständig schützen kann, dann nutze ich mein Geld lieber für andere Dinge."

Ein gutes Risikomanagement wird *nie* einen vollständigen Schutz anvisieren, sondern die für die Wertschöpfung und Existenz der Organisation wesentlichen Prozesse, Services, Daten et cetera adäquat absichern. Diese Absicherung wird dann als adäquater Schutz definiert und definiert das subjektive „100%-Schutzziel", das sich in dieser Definition natürlich immer erreichen lässt.

„Die Rahmenbedingungen sind offensichtlich."

Eine der schwierigsten Herausforderungen ist es, den demokratisch und kulturell optimalen Punkt in dem Dreieck Zensur/Regulierung, Freiheit von Information und den Möglichkeiten großer Datensammlungen zu finden. Leider genügt der Rahmen dieses Artikels nicht, um dieses Thema ausreichend zu ergründen. Zu beobachten und festzuhalten ist jedoch, dass sehr viele – vor allem internationale – Akteure hier mit versteckten (also nicht offen ausgesprochenen) Zielen arbeiten, so genannten Hidden Agendas.

Verblüffenderweise gehen aber alle gängigen Strategien davon aus, dass alle Akteure alle ihre Ziele offen ansprechen und nur diese verfolgen würden. Einer der großen (nötigen!) Umdenkprozesse, der Gott sei Dank in kleinen Teilen jetzt wahrnehmbar wird, ist es, Strategien aufzusetzen, die es ermöglichen, die eigenen Ziele unabhängig von den Hidden Agendas weiterer Diskussionspartner zu verfolgen – ein spieltheoretisch hochinteressantes und bereits vielfach untersuchtes Problem.

Komplexität

Auf einer Konferenz zum Thema IT-Sicherheit mit Industrieteilnehmern und verschiedenen Ministeriumsmitarbeitern aus den Ressorts Inneres sowie Wirtschaft und Finanzen wurde der Security vorgehalten, generell zu kompliziert zu sein. Das Beispiel aus der Politik: „Ich kann jederzeit an jeder Ecke eine Bratwurst kaufen – IT-Sicherheit ist da immer schwierig." Die Diskussion danach zeigte, dass auch der Kauf der Bratwurst in ein ganzes Szenario von Überprüfungen eingebettet ist, das so weit geht, dass lückenlose Nachweise von Aufzucht und Transport der lebenden Tiere bis hin zur Verarbeitung rückverfolgbar sein müssen, damit die Sicherheit der Bevölkerung vor gesundheitsschädlichen Waren gegeben ist.

Dieser Beitrag verfolgt die These, dass die IT-Sicherheit deshalb als so kompliziert wahrgenommen wird, weil sie gerade *nicht* als nachweisbare Vertrauenskette unter Berücksichtigung *aller* Facetten betrachtet wird.

Statt die Unsicherheit einer Technik (im Referenzangriff z. B. „der Browser") durch das „Bekleben mit einem Pflaster" zu lösen und dabei im schlimmsten Fall den Bock zum Gärtner zu machen, sei hier dazu angeregt, den Blick darauf zu lenken, stabile und nachweisbare Vertrauensketten zu etablieren. Denn erst durch die vollständigen Vertrauensketten, die bei einer „sicheren Tastatur" beginnen und über zertifizierte Services, deren Herkunft und Veränderung (wie bei dem Fleisch in einer Bratwurst) nachgewiesen ist, bis hin zu adäquat geschützten Daten reichen, wird eine nachhaltige Sicherheit möglich.

Insofern ist das Arbeiten an sicheren Standards zwar ein wichtiger Schritt, gleichzeitig muss man aber auf Architekturen setzen, die schon heute möglich sind und gegenüber bestimmten unsicheren Bestandteilen (Hardware, Betriebssysteme, Anwendungen, Netzkomponenten ...) fehlertolerant agieren.

Bei der Erstellung der Vertrauensketten ist auch die Einsicht unabdingbar, dass Kryptografie nur eins von vielen wesentlichen Mitteln ist: Systeme, deren gesamtes Vertrauen nur auf kryptografischen Verfahren beruht, können sich Standardsystemen – wie beispielsweise Browsern – nicht öffnen. Erst wenn zu den kryptografischen Verfahren andere (etwa o. g.) Kontrollmechanismen in geeigneter Qualität dazu kommen, entstehen Vertrauensketten, die auch Browser oder unsichere Kommunikationsanwendungen fehlertolerant mit einbeziehen können.

Interessant ist, dass man dann auch Exploits wie den USB-Hack, der als „BadUSB" auf der Black Hat 2014 in Las Vegas von Karsten Nohl und Jakob Lell beschrieben wurde [1], ein adäquates Schutzprofil entgegensetzen kann – und damit etwas, was bis dato als „nicht erkennbar" angenommen wurde, trotzdem unterbinden kann. ■

Ramon Mörl ist Geschäftsführer der itWatch GmbH.

Literatur

[1] Karsten Nohl, Jakob Lehl, BadUSB – On Accessories that Turn Evil, www.blackhat.com/us-14/briefings.html#badusb-on-accessories-that-turn-evil

[2] Ramon Mörl, Ein Jahr danach – IT-Sicherheit im „Jahr 1" nach Snowden, <kes> 2014#3, S. 6

[3] Hilde von Waldenfels, Wie (un-) durchsichtig?! <kes> 2010#5, S. 6