Stets bemüht um Sicherheit?! (1)

Beispiele, Fragen und Gedanken dazu, warum in Sachen Security so viel schiefgeht

Security-Know-how ist heute fast überall gefragt, aber Spezialisten sind selten. So kommt es trotz guten Willens verbreitet zu vordergründigen oder halbgaren Betrachtungen und in der Folge „hakt" es mit der Sicherheit – auch dort, wo man es eigentlich nicht erwarten würde. Unser Autor legt anhand von Beispielen aus der Praxis den sprichwörtlichen Finger in die Wunden, um den Weg für Lösungen zu bereiten.

Von Ramon Mörl, München

Wenn man sich einmal anschaut, was an wie vielen Stellen in Sachen Security immer wieder schiefgeht, könnte man sich fast schon fragen: Sind wir eigentlich zu dumm für IT-Sicherheit? Zumindest zeigen sich an etlichen Stellen über den gesamten Lebenszyklus von IT-Lösungen erhebliche Know-how-Defizite – und zwar auch in Organisationen, bei denen man das eigentlich nicht erwarten würde. Umso stärker trifft es Unternehmen, die (noch) weniger Know-how zu IT und IT-Sicherheit besitzen.

Verschiedenste – anonymisierte – Beispiele und Überlegungen aus der Praxis sollen im Folgenden zeigen, wo es überall hapert. Nur wenn man um die Defizite weiß, kann man ja mittelfristig für entsprechende Fortbildung oder Abhilfe sorgen und gegebenenfalls kurzfristig nach Workarounds Ausschau halten – langfristig sind ohnehin „größere" Lösungen gefragt.

Kulturelle Defizite

Denn letztlich scheinen wir heute noch ein gesamtgesellschaftliches Problem mit der IT-Sicherheit zu haben: zu wenig Ausbildung, zu wenig Bewusstsein, zu wenig Stellenwert et cetera. Ein Mitarbeiter der Inneren Sicherheit, der leider ungenannt bleiben muss, forderte einmal in kleiner Runde, dass wir uns *als Kultur* damit auseinandersetzen müssten, welche Abbildung gesellschaftlich etablierte Schutzmechanismen der traditionellen Welt in der IT-Sicherheit finden könnten und sollten.

Doch auch dazu braucht es Know-how an allen möglichen Stellen. Denn ein adäquater Schutz entsteht ja erst durch die Robustheit eingesetzter, passender Verfahren – und schon, um das richtige Schutzniveau und die benötigte Robustheit richtig einschätzen zu können, braucht es gute Kenntnisse.

In der „analogen" Welt glaubt sich jeder hierzulande gut geschützt – Deutschland gilt als sehr sicher, was ein positiver Aspekt für den Standort ist. Zweifelsohne wäre es ein Wettbewerbsvorteil, wenn Deutschland und in der Folge auch Europa die Sicherheit in der digitalen Welt ebenfalls als attraktiven Standortfaktor besetzen könnten.

Doch wie soll das gehen, wenn es „überall" an Know-how um die IT-Sicherheit fehlt? Dieser Mangel ist an sich bekannt und an vielen Stellen bemerkbar (s. u.) – aktuelle Zahlen gehen davon aus, dass nur rund 1 % der Beschäftigten in der Informations- und Telekommunikationstechnik (ITK) Spezialwissen in IT-Sicherheit besitzen. IT-Sicherheit ist überall notwendig, passendes Know-how aber längst nicht überall vorhanden.

Wissens-Defizite

Bevor man auf die gesellschaftliche Breite abzielt, sollte man den Blick zunächst auf die „Avantgarde" richten – auf Unternehmen und Organisationen, die bereits in Sachen Sicherheit aktiv sind, wo Einsicht und Wille vorliegen und auch schon gehandelt wird. Und selbst bei dieser Gruppe und ihren Partnern, die doch eigentlich als Vorbild dienen müssten, findet man noch mehr als genug Defizite. Denn auch dort, bei sicherheitssensitiven KMU und auch vielen größeren Organisationen, sind jede Menge Stakeholder daran beteiligt, die IT wirklich sicherer zu machen – oder bei diesem Versuch ins Stolpern zu geraten oder gar zu scheitern.

Dabei gilt es, den gesamten Lebenszyklus und die gesamte Handlungskette von der Bedarfsermittlung über Ausschreibung, Herstellung, Marketing, Vertrieb, Kauf, Installation und Betrieb zu betrachten. Entlang eben dieser Handlungskette soll im Folgenden anhand realer Beispiele aus jüngerer Zeit aufgezeigt werden, wo Akteure spezifisches Know-how benötigen, das in den beschriebenen Fällen eben nicht verfügbar war oder aus anderen Gründen nicht „zum Tragen kam".

Zusammenstellen der Anforderungen

Beispiele für „Scheitern auf hohem Niveau“ findet man bisweilen bereits in den Anforderungen für neue Lösungen. So wird für moderne IT-Systeme – auch getrieben durch die ISO-27000er-Normen – die Klassifikation von Daten gefordert. Das Ziel dieser Klassifikation oder des „Labelings“ ist es, eine bestimmte Information (dauerhaft) mit einem Sicherheitsmerkmal wie „firmenvertraulich – Nur für den Dienstgebrauch“ oder „vertraulich“ zu verbinden.

Viele Lösungen auf dem Markt binden Klassifikationsinformationen jedoch in den so genannten „Alternate Data Stream“ (ADS) ein – eine Art Attribut einer Datei, den das zugrunde liegende Dateisystem (z. B. NTFS) als Standard kennt. Diese Eigenschaft einer Datei geht jedoch bei der Übertragung per E-Mail oder auf bestimmte andere Dateisysteme (z. B. auf USB-Sticks), die ADS nicht unterstützen, einfach verloren.

In Anforderungslisten zur Klassifikation von Daten findet sich dennoch das „sichere, nachhaltige und dauerhafte Koppeln der Klassifikationsinformation“ nur selten, auch wenn die Klassifikation später als Sicherheitsmerkmal verwendet werden soll. Auf konkrete Nachfrage erfährt man dann meist, dass dieser Zusammenhang entweder unbekannt war oder dass man eine ohnehin komplexe Projektierung nicht noch schwieriger gestalten wollte.

Solche Antworten zeugen von Know-how-Defizit, das in der frühen Phase der Anforderungen eventuell bereits durch eine Marktsichtung hätte behoben werden können – wenn es denn Vorlagen gäbe, was aus einem bloßen Labeling eine echte Sicherheitsfunktion macht, die man später auch als Grundlage für DLP-Projekte einsetzen kann.

Mangel an Metrik

Zweifelsohne handelt es sich bei der IT-Sicherheit um ein komplexes Thema. Nur selten geht es um sichtbare, einfach prüfbare Funktionen und hübsche, ergonomische Oberflächen – viel öfter darum, höhere Robustheit und verbesserten Schutz gegen aktuell bekannte und zukünftig vorstellbare Angriffe zu erreichen.

Dieser Schutz sollte von allen Beteiligten als komfortabel und selbstverständlich wahrgenommen werden. Doch weder für den Schutz noch für den Komfort gibt es eine Metrik, um diese Parameter fundiert zu vergleichen. Zertifizierungen bieten zwar eine Hilfestellung, aber man muss ihre Verfahrensweise genau verstehen können, um die Ergebnisse zu beurteilen – wieder braucht es Wissen.

Lieferketten von IT-Sicherheitsprodukten

Viele IT-Sicherheitsprodukte greifen auf weit verbreitete De-facto-Standards zurück und integrieren diese – etwa bei SSL und TLS. Mit Heartbleed gab es plötzlich einen Angriff, der auf eine Schwachstelle in einer gängigen SSL-Implementierung aufgesetzt hat. Diese war häufig auch in Drittprodukten enthalten, ohne dass dies den Endkunden bekannt war. Zum großen Teil wird auch gar nicht erst danach gefragt, welche Technik real in einem angebotenen Produkt „verbaut“ ist.

Spätestens Heartbleed hat aber gezeigt, dass es sinnvoll sein kann, zu wissen, in welchem System welche Open Source oder welche Bibliothek von Dritten (z. B. als OEM) enthalten ist: Ein Grund, schneller handeln zu können, wenn neue Angriffe auf diese Elemente bekannt werden. Ein weiterer Grund ist, bereits beim Kauf besser einschätzen zu können, auf was man sich einlässt. Dieser Punkt ist mehrdimensional, denn sowohl die rechtlichen Abhängigkeiten, Fragen der Haftung als auch technische wie juristische Hintertüren können die eigene Einschätzung der „digitalen Souveränität“ des Käufers beeinflussen.

Insofern sollte man sich zugekaufte oder mitgenutzte Komponenten in einem Produkt per Herstellererklärung auflisten und den Lieferanten für die Korrektheit dieser Eigenerklärung Haftung übernehmen lassen – dabei ist die Offenlegung der gesamten Lieferkette bedeutsam. Neben dem grundlegenden Know-how um die positiven Auswirkungen solcher Transparenz in der Lieferkette fehlt es häufig auch am Bewusstsein zu entsprechenden K.-o.-Kriterien für den Einsatz bestimmter Lösungen.

Die Fähigkeit, Informationen zur Lieferkette aller eingesetzten Produkte im Sinne einer Gesamtsicherheit im Unternahmen zu managen, erfordert weiteres Know-how, das ebenfalls selten ist. Erst wenn eine flächige Aufmerksamkeit entsteht und die haftungsunterlegte Angabe der vollständigen Lieferkette in großen Beschaffungen berücksichtigt würde, könnte dieser Punkt jedoch zum gelebten Standard werden – und so auch (mit einfachen Kriterien unterlegt) eine Entscheidungshilfe darstellen. Eine von neutraler Stelle kommentierte Vorlage für einen „Lieferketten-Fragenkatalog“ würde helfen, derartiges Know-how zu bündeln.

Ausgestaltung von Ausschreibungen

Eine Ausschreibung für eine Verschlüsselungslösung, die der Autor gesehen hat, umfasste weit über einhundert funktionale und ergonomische Kriterien, die eine potenzielle Lösung zur Verschlüsselung von Dateien erbringen musste; insgesamt ließen sich 1000 Punkte erreichen. Eine Frage lautete: „Kann das kryptografische

System umgangen oder gebrochen werden?“ – die möglichen Ergebnisse: „mit einfachen Mitteln“ = 0 Punkte und „nicht möglich“ = 10 Punkte (also 1 % der erreichbaren Gesamtpunktzahl für die Vergabe). So hätte also ein Produkt, das zu umgehen oder zu brechen ist, im Prinzip 990 von 1000 Punkten erzielen und die Ausschreibung gewinnen können – ein Produkt, das Geld und Aufwand sicher nicht wert gewesen wäre.

Ausschreibungen müssen offensichtlich anders aussehen, wenn sie die Sicherheit verbessern sollen: Zuerst hätte man einen unteren Schwellenwert der Robustheit definieren müssen – und nur Produkte, die diesen Wert nachweislich überschreiten, dürfte man später anhand von Standardkriterien (z. B. Funktionalität, Preis usw.) vergleichen.

Bei der Robustheit von Verschlüsselungsverfahren ist aber auch zu berücksichtigen, dass es nicht nur um die Kryptografie geht – gute Zufallszahlen, Schlüsselgenerierung, -verwaltung und -lagerung, ein starker Algorithmus et cetera sind nicht alles. Vielmehr geht es auch um die Einbettung in das Zielsystem: Denn wenn beispielsweise in einer transparenten Verschlüsselungslösung jeder laufende Prozess (auch „remote“) die Entschlüsselung anfordern kann, dann ist zwar möglicherweise das Kryptosystem in sich robust, aber das Gesamtsystem hat dennoch keinen oder nur geringen Schutz (vgl. [1]).

Ein großes Problem stellt hier bereits die Definition des unteren Schwellenwertes für die Robustheit des Gesamtverfahrens dar, denn es gibt dazu keine Maßeinheit oder Metrik. Hier ist vielfältiges Know-how nötig, das nur sehr spärlich in der ITK anzutreffen ist. Hilfreich wäre es, wenn Organisationen mit höherem Schutzbedarf ihre Ergebnisse zur Robustheit von Produkten und ihre Erfahrungen bei deren Betrieb detailliert beschreiben und veröffentlichen würden, sodass Dritte hiervon profitieren könnten – bis hin zu einer Liste von Produkten mit geeigneten Betriebskonzepten und Integratoren.

Organisationen mit höherem Schutzbedarf möchten jedoch verständlicherweise nicht offenlegen, welche Produkte mit welchen Betriebskonzepten bei ihnen im Einsatz sind. Deshalb benötigte man eine Art Tauschbörse, die es einerseits ermöglicht, praktische Erfahrungen zu kommunizieren, ohne dass deren Urheber publik wird – andererseits müsste aber dennoch sichergestellt sein, dass Qualität und Integrität der transportierten Informationen überprüfbar und nachvollziehbar bleiben. So würde man etwa sicherlich einen eintägigen Kurztest anders berücksichtigen als eine umfassende Marktuntersuchung mit praktischen Tests auf Basis etlicher Manntage, die parallel in kurzer Zeit durch ein großes Team eines namhaften Marktteilnehmers erstellt wurde. Weitere Hindernisse eines solchen Erfahrungstransfers blieben aber dennoch

Fragestellungen der Haftung und möglicher Wettbewerbsverzerrungen.

Bewertung von IT-Sicherheitslösungen

Die praktische Nutzbarkeit einer Lösung ist von wesentlicher Bedeutung. Trotzdem bleibt es noch wichtiger, dass eine implementierte Lösung tatsächlich einen besseren Schutz verwirklicht als es ihn ohne sie gegeben hat – sonst sollte man besser gar nicht investieren.

Man stelle sich eine Organisation vor, die ihre Mitarbeiter zum wöchentlichen Wechsel eines 12 Zeichen langen Passworts für den Systemzugang (natürlich mit komplexen Nebenanforderungen) zwingt, ohne dafür Sorge zu tragen, dass die vergebenen Passwörter gegen ein Ausspähen mit Keyloggern geschützt sind. Die Mitarbeiter würden sich zu Recht gegängelt vorkommen und der betriebene Aufwand, der zu signifikanten Kosten im Helpdesk führen dürfte, wäre nicht gerechtfertigt. Eine parallele Maßnahme zum technischen Passwort-Schutz gegen Ausspähen würde die Maßnahme hingegen sinnvoll begleiten und man könnte die Wechselfrequenz reduzieren, was zu einer höheren Benutzerakzeptanz führt.

In verschiedenen Bewertungen wird eine „All-in-One"-Lösung mit komfortablem Remote-Management aus praktischen Erwägungen heraus favorisiert – zumeist, da so etwas aus Fachanwendungen heraus als State-of-the-Art betrachtet wird. Dass ein Remote-Management aller Systemeigenschaften von außerhalb (evtl. sogar über unsichere Betriebssysteme oder BYOD-Elemente) praktische Vorteile in der Handhabung hat, ist evident – aber Nachteile für die IT-Sicherheit sollten ebenso evident sein: Remote-Interfaces zur Verwaltung von beliebigen Drittsystemen senken die Sicherheit und müssen selbst wieder aufwändig überwacht werden. Der zusätzliche Aufwand, den man in den Schutz der Konfigurationsdaten und administrativen Einstellungen solcher Sicherheitssysteme steckt, muss in der Gesamtkalkulation Berücksichtigung finden.

Weitere Betrachtungen dieser Art sind die Entwicklungswerkzeuge, mit den ein IT-Sicherheitsprodukt programmiert wurde, und seine Verankerung im System: C# ist beispielsweise leichter angreifbar als auf gut geprüften Compilern erstellter C-Code – und Systeme, die im Applikationskontext oder als Dienste laufen, sind leichter angreifbar als solche, die mit einem im Betriebssystem-Kern verankerten Treiber arbeiten (Kernel-Mode-Driver).

Diese Problematik wird noch komplexer, weil man ein Defizit (z. B. geringe Robustheit des Compilers gegen Angriffe) auch durch andere Sicherheitsmaßnahmen wieder wettmachen kann (z. B. Isolation des Produkts auf einem gehärteten System). Betriebskonzepte können ebenso positive wie negative Auswirkungen auf die Sicherheit des Gesamtsystems haben. Das benötigte Know-how: IT-Risiken entschärfen (Mitigation), neue Risiken durch neue Produkte erkennen und reduzieren.

Auch hier sind all diese Aspekte (und noch mehr) für hochsichere Umgebungen schon vorgedacht, aber keine einfachen Checklisten und prüfbaren Kriterien, Auswahl-Listen oder gar fertige Prüfberichte verfügbar. Bestätigungen über Herstellungsprozesse erweitern die Fähigkeiten zur Sicherheitseinschätzung und könnten zusammen mit dem Fragenkatalog zur Lieferkette als Fragen an die Hersteller/Anbieter in die Beschaffung mit aufgenommen werden. Doch sowohl für das Erstellen der richtigen Fragen (ein einfaches Kopieren der ISO 27001 ist hier nicht zielführend) als auch für deren Auswertung ist spezifisches Know-how erforderlich. Und darüber hinaus möchten (oder dürfen) Hersteller auch längst nicht jedem potenziellen Kunden tiefe Einblicke, etwa in die Sicherheitsüberprüfung ihres Personals und ihrer Prozesse, geben.

Auch hier wäre deshalb eine Vertrauensbörse wichtig, welche die Ergebnisse von Prüfungen verbindlich darstellt, ohne die Anonymität der handelnden Personen und die Vertraulichkeit von Herstellungsprozessen zu gefährden. In Verschlusssache-Umgebungen existiert zu diesem Zweck die Sicherheitsüberprüfung des Herstellers oder relevanter Teile von Hersteller und Lieferant. Doch diese Unternehmen unterliegen dem Geheimschutz: Hat ein Hersteller eine solche Prüfung positiv hinter sich gebracht, darf darüber nicht öffentlich gesprochen werden – wesentliche (bereits geleistete) Anstrengungen zur Identifikation vertrauenswürdiger IT-Systeme und Unternehmen bleiben somit weithin ungenutzt. Wieder wäre es hilfreich, einen Weg zur breiteren Nutzung zu finden, der die Interessen aller Stakeholder – also auch der öffentlichen Hand, die den Aufwand des Geheimschutzes betreibt – geeignet berücksichtigt, aber dennoch Dritte von den Ergebnissen profitieren lässt.

Marketing, Vertrieb und Marktmacht

Kaum ein potenzieller Kunde interessiert sich für die Kostenverteilung zwischen Forschung, Entwicklung, Marketing und Vertrieb. Dabei könnten diese Strukturen Anhaltspunkte dafür geben, dass Produkte mit den teuersten Marketingprozessen und den meisten Vertriebsstandorten nicht unbedingt die robustesten IT-Sicherheitsverfahren implementieren, weil womöglich weniger Ressourcen in die Forschung und Entwicklung von Schutzmechanismen fließen.

Auch bei den Produkten, die unter IT-Sicherheits-Flagge vertrieben werden, verbergen sich bisweilen schwarze Schafe – sogar wenn legitimerweise „IT-Security made in Germany" als Label verwendet wird [2]. Um

solche schwarzen Schafe zu erkennen, ist erheblicher investigativer Rechercheaufwand nötig – den kann natürlich längst nicht jeder Beschaffer betreiben. Der Endkunde kann meist mangels geeigneter Informationen nicht einmal beurteilen, welche Komponenten wo programmiert oder gebaut wurden und welche Beteiligten eventuell sogar nachrichtendienstlichen Hintergrund haben (vgl. den Abschnitt zur Lieferkette).

Natürlich kann ein Produkt nur dann gekauft werden, wenn es beworben und vermarktet wird – Ausgaben in Marketing und Vertrieb sind zwingend notwendig. Nicht selten sind solche Ausgaben aber gerade bei Lösungen, die stark auf Sicherheit setzen, so gering, dass diese für viele Marktteilnehmer quasi unsichtbar bleiben.

Auf der anderen Seite könnte man denken, dass große Firmen, weil sie überall bekannt und präsent sind, auch besonders stabile und sichere Produkte mit nachhaltigen Strategien anbieten. Dass das nicht der Fall sein muss, zeigen jedoch viele reale Beispiele: der Cisco Security Agent wurde aufgekündigt, Check Point hat seine nach dem Kauf von pointsec und DiskNetPro entwickelte Endpoint-Strategie mehr oder weniger ganz aufgegeben, die in Deutschland recht bekannten Produkte von utimaco sind nach der Übernahme durch Sophos zum Teil aufgekündigt worden, zum Teil durch ein Wechselbad der Strategien gegangen ...

Wo das nötige Know-how zur exakten Beurteilung fehlt, wird man eher zu einer vom Marketing gepushten Lösung greifen, anstatt sich für eine eventuell noch unbekanntere, aber womöglich nachhaltig robuste Lösung mit strategischen Vorteilen zu entscheiden. Denn die handelnden Marktteilnehmer sind notwendigerweise umsatzgetrieben. Ähnlich wie beim Umweltschutz wird aber ein völlig frei entwickelter Markt wenig in echte IT-Sicherheit und mehr in gut verkaufte Scheinsicherheit investieren!

Literatur

[1] Hilde von Waldenfels, Wie (un-)durchsichtig?!, Wie viel Transparenz Verschlüsselung braucht und erträgt, <kes> 2010#5, S. 6

[2] Dirk Banse, ПОЛИЦИЯ, WELT am Sonntag, 29. November 2015, Ausgabe 48, S. 8, online verfügbar unter www.welt.de/print/wams/wirtschaft/article149394820/O-N-N.html.

[3] Ramon Mörl, Gemeinsam stark gegen Cyber-Angriffe, <kes> Special IT-Sicherheit in Kommunen und Behörden (Verlagsbeilage), Mai 2013, S. 38, online verfügbar über www.kes.info/archiv/specials/kommunen-und-behoerden (Registrierung erforderlich)

Im Markt fehlen heute Dirigenten, die das gesamte Orchester mit der geeigneten Information versorgen und so auch Unternehmen mit weniger IT-/IT-Security-Know-how den Zugang zu wichtigen Informationen barrierefrei und leicht konsumierbar (also frei von Fachbegriffen und langen Detailtexten), dafür aber von vertrauenswürdiger neutraler Stelle beglaubigt ermöglichen. Wie schon beschrieben, wäre eine geeignete Vertrauenskette oder Vertrauensbörse ein mögliches Medium, um Erfahrungen und Erkenntnisse zu transportieren und dann auch in die geeigneten, konsumierbaren Informationspakete zu übersetzen.

Eine Umfrage zum KMU-Markt auf der it-sa 2014 hat beispielsweise ergeben, dass viele Unternehmen gerne in IT-Sicherheit investieren würden, wenn der Zugang für sie barrierefrei und kalkulierbar wäre – man wünscht sich offenbar eine von neutraler Stelle befürwortete Zusammenstellung verschiedener Produkte mit einem geeigneten Betriebskonzept, zusammengefasst zu einem einzigen „Mach-mich-sicher"-Paket, zu einem festen Preis. Natürlich dürfen Verfügbarkeit und Ergonomie des Gesamtsystems nicht leiden und der Anbieter muss für dieses Paket auch in diesen Aspekten eine Haftung übernehmen (die ggf. an die Hersteller durchzureichen ist). Integratoren und Beratern fehlt aber eine verlässliche Information, mit welchen Lösungen sie solche Pakete aus welchen Gründen für welche Märkte schnüren sollten – Zusammenstellungen sind daher auf eigene Untersuchungen angewiesen, die sich wiederum auch kommerziell tragen müssen, was eine klare Begrenzung von Ressourcen bedeutet.

Zu guter Letzt ist auch an anderer Stelle die Frage nach dem Geld wesentlich: Ein Händler wird Produkte, bei denen er einen höheren Anteil vom Verkaufserlös erhält, aus einsichtigen Gründen lieber verkaufen als andere – Produkte mit geringer Marge oder kleinen Absatzmärkten werden häufig gar nicht erst ins Portfolio genommen. Jeder an der Handelskette Beteiligte muss naturgemäß entweder über die Quantität der abgenommenen Stückzahlen oder über eine hohe Marge beim einzelnen Verkauf seine internen Kosten decken. Beides spricht dagegen, dass so genannte Best-of-Breed-Lösungen in weit verbreiteten Handelsketten landen, da hierbei (zumindest zu Beginn der Vermarktung) für gewöhnlich geringe Margen und kleine Absatzmärkte die Regel sind. Hilfe verspricht dem Anbieter dann Venture-Capital (VC) – doch VC-Gesellschaften geben Kapital meist nur gegen Beteiligung an Patenten und „Intellectual Property" (IP) der Unternehmen, wodurch die Eigenständigkeit und zum Teil auch die Innovationskraft der Geförderten leidet.

Die Fortsetzung dieses Beitrags folgt in der nächsten <kes>.

Ramon Mörl ist Geschäftsführer der itWatch GmbH.

Stets bemüht um Sicherheit?! (2)

Beispiele, Fragen und Gedanken dazu, warum in Sachen Sicherheit so viel schiefgeht

Security-Know-how ist heute fast überall gefragt, aber Spezialisten sind selten. So kommt es trotz guten Willens verbreitet zu vordergründigen oder halbgaren Betrachtungen und in der Folge „hakt" es mit der Sicherheit – auch dort, wo man es eigentlich nicht erwarten würde. Unser Autor legt anhand von Beispielen aus der Praxis den sprichwörtlichen Finger in die Wunden, um den Weg für Lösungen zu bereiten.

Von Ramon Mörl, München

Wenn man sich einmal anschaut, was an wie vielen Stellen in Sachen Security immer wieder schiefgeht, könnte man sich fast schon fragen: Sind wir eigentlich zu dumm für IT-Sicherheit? Zumindest zeigen sich an etlichen Stellen über den gesamten Lebenszyklus von IT-Lösungen erhebliche Know-how-Defizite – und zwar auch in Organisationen, bei denen man das eigentlich nicht erwarten würde. Umso stärker trifft es Unternehmen, die (noch) weniger Know-how zu IT und IT-Sicherheit besitzen.

Verschiedenste – anonymisierte – Beispiele und Überlegungen aus der Praxis sollen im Folgenden zunächst zeigen, wo es überall hapert – wie bereits im ersten Teil dieses Beitrags [1]. Nur wenn man um die Defizite weiß, kann man ja mittelfristig für entsprechende Fortbildung oder Abhilfe sorgen und gegebenenfalls kurzfristig nach Workarounds Ausschau halten – Lösungsansätze liefern die letzten Abschnitte dieses Artikels.

Wissens-Defizite (Fortsetzung)

Im ersten Teil ging es bereits um Anforderungen und Ausschreibungen, die Bewertung von IT-Sicherheitslösungen, Lieferketten sowie Marketing, Vertrieb und Marktmacht der Anbieter. Im weiteren Verlauf des Lebenszyklus schließen sich Herstellung, Kauf, Installation und Betrieb an. Weitere reale Beispiele aus jüngerer Zeit sollen entlang dieser Handlungskette zeigen, wo Akteure spezifisches Know-how benötigen, das in den beschriebenen Fällen eben nicht verfügbar war oder aus anderen Gründen nicht „zum Tragen kam".

Herstellung

Beim Entwickeln von Schutzverfahren stehen viele Unternehmen vor der Frage „make or buy?". Idealerweise wird in beiden Fällen gemäß der Doktrin „Security by Design" die IT-Sicherheit bereits im Produktdesign berücksichtigt, also einer sehr frühen Phase der Produktplanung. Diese Doktrin ist sehr wünschenswert: Sie führt zu Ende gedacht jedoch dazu, dass jeder Softwarehersteller und jedes Systemhaus auch IT-Security-Know-how benötigen – und zwar eines der teuersten und seltensten Form, das nämlich in der Planung von Architekturen und in deren Umsetzung zum Tragen kommt. Prinzipiell lässt sich diese Expertise natürlich auch zukaufen – man steht also wieder vor der Entscheidung „make or buy".

Am konkreten Beispiel aus der Vergangenheit stellt sich das etwa so dar: Die Analysten von Gartner empfahlen in ihren Strategieberatungen für die Hersteller von Softwareverteilverfahren, einzelne Komponenten der Endpoint-Security mitzuliefern – in diesem Fall vor allem Device-Control-Software. Deshalb begannen Firmen wie Materna und Matrix 42, eigene „Sicherheitslösungen" herzustellen. Vor der Frage „make or buy?" stehend, entschieden sich die meisten Unternehmen natürlich für „make", da hier die Wertschöpfungstiefe größer und die Handlungsgeschwindigkeit am fertigen Produkt höher ist – allerdings muss ein Produkt erst einmal fertig werden.

In der Konsequenz haben sich Hersteller von „Non-IT-Security"-Produkten in den IT-Security-Markt bewegt, weil „das ja auch nur IT ist – und so schwer kann das nicht sein". IT-Architekten werden dann zu Security-Architekten und Entwickler zu „IT-Security-Entwicklern" umdefiniert. Wesentlich ist, hier zu erkennen, dass im Entscheidungsverfahren um „make or buy" die Robustheit der Lösungen kein wesentliches Ziel dargestellt hat – mangels Metrik und mangels Awareness. „Time to Market" und Produktionskosten stellen hingegen durchaus wesentliche Entscheidungsparameter dar, die auch aus der klassischen IT bekannt sind. Als Resultat gibt es dann Produkterweiterungen und Sicherheitsfunktionen mit fraglicher Robustheit, weil eben kein langjähriges Know-how zur IT-Sicherheit in den „make or buy"-Entscheidungsprozess eingeflossen war.

In den beispielhaft genannten Fällen hat Matrix 42 die Entwicklung übrigens nach vielen Monaten wieder aufgegeben und Materna ein Produkt mit dem Namen „Device Inspector“ auf den Markt gebracht, das zum Beispiel immer dann, wenn eine neue Richtlinie gerade geladen wird, weder die alte noch die neue durchsetzt – also im IT-Sicherheitsjargon einfach „offen“ ist und überhaupt keinen Schutz bietet.

Die resultierende Problematik ist mehrdimensional: Zum einen „verbrennt“ ein Hersteller Geld für Produkte, die letztlich ihre Marktziele häufig nicht erfüllen. Viel schlimmer sind aber Verwerfungen im Markt, die dadurch entstehen, dass der Vertrieb natürlich versucht, die neuen Produkte, die womöglich nur eine Scheinsicherheit herstellen, zu verkaufen – und dabei auch den einen oder anderen Käufer findet, denn die wünschenswerte Robustheit lässt sich ja eben nicht leicht messen. Die angebotenen Funktionen kann indessen jeder einander gegenüberstellen – meist allerdings ohne sich darüber im Klaren zu sein, dass man die berühmten Äpfel und Birnen vergleicht, wenn man ein nicht-robustes Produkt einem robusten Produkt mit den (vordergründig) gleichen Funktionen gegenüberstellt.

Hier wäre der Rückgriff auf neutrale Vertrauensketten zu jedem Zeitpunkt in der Planung, der Herstellung und der Markteinführung extrem wertvoll – leider stehen jedoch auch für diese Phase keine neutralen Institutionen bereit.

„Security by Design“ multipliziert diese Problem noch, denn unter dieser Prämisse sollen ja alle Produkte die Sicherheit schon von Anfang an berücksichtigen. Während man beispielsweise beim Herstellen einer Applikation zur Berechnung der individuellen Steuerschuld recht offenkundig mit sensiblen Daten umgeht, gibt es sicher viele andere Anwendungen, bei denen sich die Berücksichtigung adäquater Sicherheit weniger deutlich

Robustheit von IT-Sicherheits-Mechanismen

In einer Diskussion um die beste Robustheit von IT-Sicherheitsverfahren wurde deutlich, dass sich die Ziele von Verfügbarkeit auf der einen Seite und Integrität und Vertraulichkeit auf der anderen Seite zum Teil entgegenstehen: Für die Verfügbarkeit von Systemen ist es prinzipiell gut, alle Verfahren von möglichst verschiedenen Herstellern auf möglichst unterschiedlichen Betriebssystemen und Hardwareplattformen parallel zu betreiben und dadurch redundant zu halten. Bei einem erfolgreichen Angriff würden dann nicht alle Systeme gleichzeitig befallen – die verteilte Plattform reduziert die Ausfallwahrscheinlichkeit.

Andererseits nutzt ein Angreifer aber natürlich die am schwächsten geschützte Plattform, um Integrität und Vertraulichkeit zu überwinden – die Schwächen der parallel eingesetzten Systeme addieren sich sozusagen. Hiergegen wäre es also sinnvoll, die verschiedenen Systeme hintereinanderzuschalten, sodass ein erfolgreicher Angriff auf das erste System im zweiten oder dritten hängenbleibt.

Weil sich die drei Grundziele der IT-Sicherheit teils schon grundsätzlich widersprechen, ist es wesentlich, diese Anforderungen subjektiv und in feiner Granularität zu definieren. Dieser Vorgang ist zeitintensiv und kann längst nicht von allen KMU gemeistert werden. Deshalb ist es wichtig, Best Practices für verschiedene Branchen zu erarbeiten – hier ist immerhin über die im KRITIS-Bereich diskutierten Mindeststandards schon Bewegung im Markt zu beobachten. Darüber hinaus könnten Branchenverbände in der Vertrauenskette gute Arbeit leisten, um die komplexen Themen der IT-Sicherheit für ihre jeweilige Klientel zu vereinfachen.

aufdrängt. Und wie der vormalige Bundesbeauftrage für den Datenschutz Peter Schaar schon mehrfach öffentlich betonte, kann eine Anwendung letztlich nur so sicher sein wie das Betriebssystem, auf dem sie läuft.

So kommen also auf viele Hersteller reichlich „fachfremde" Aufgaben zu – und häufig greift man dann zum Beispiel auf „IT-Sicherheitsbaukästen" als Software-Development-Kits (SDKs) oder Bibliotheken zu, die man in die eigenen Programme einbinden kann (vgl. auch den Abschnitt zu Lieferketten in [1]). Es wäre nun wünschenswert, wenn dieser Markt tatsächlich orchestriert würde, da sich ja auch die Qualität und Robustheit so eines SDK nicht einfach erkennen lässt. Erneut scheint eine sehr plausible Lösung in einer Art Sicherheits-Börse und den zugehörigen Vertrauensketten liegen zu können.

Kauf

Angriffe auf IT-Systeme sieht man nicht. Verfahren der IT-Sicherheit werden oft als Verhinderer wahrgenommen – im besten Fall sind sie ebenfalls unsichtbar. Was also motiviert ein Unternehmen, Geld in etwas zu investieren, das es potenziell behindert und vor unsichtbaren Dingen in der Zukunft potenziell bewahrt – wo man doch das Geld heute in sinnvolle Dinge investieren kann, mit denen man morgen mehr Umsatz macht?!

Das ist im Wesentlichen eine häufige Argumentation der im Kasten „Marktteilnehmer" erwähnten dritten Gruppe, die an IT-Sicherheit nicht interessiert ist – hinzu kommen noch Argumente wie „100 % Sicherheit gibt es ohnehin nicht, also brauche ich doch gar nicht erst in 50 % oder 80 % investieren, wenn ich dann immer noch nicht geschützt bin".

Es ist ein langer Weg, der auch sanktionierte Regulierung mit einbeziehen muss, um in solchen Umgebungen zumindest eine Basissicherheit zu etablieren, damit Kommunikationspartner und Dritte nicht durch solche ungeschützten Unternehmen gefährdet werden. Das von einem Mitglied der Piratenpartei einmal gefor-

Marktteilnehmer

Bereits 2004 erzählte der Hersteller einer zugelassenen Verschlüsselungslösung, dass es zunehmend komplizierter werde, die höhere Robustheit seiner Lösung im Markt darzustellen, weil auf Kundenseite auch bei großen Unternehmen kaum jemand die Unterschiede der im Markt verfügbaren Produkte und ihre Auswirkungen auf die Sicherheit des Gesamtsystems verstehe.

Bei Entscheidern ist das Know-how, eine höhere Robustheit der gleichen Funktion (z. B. bei einem Firewall-System) zu erkennen, nicht vorauszusetzen. Die Bundesregierung möchte letztlich sogar Bürger sowie kleinere und mittlere Unternehmen (KMU) in die Lage versetzen, im Internet und den digitalen Welten sicher zu handeln. Doch wenn schon in großen Unternehmen kaum Kompetenz vorhanden ist, um zu unterscheiden, welche Lösung besser schützt – wie soll das dann für KMU und Privatleute klappen?

Generell lassen sich im Wesentlichen drei Gruppen von Marktteilnehmern unterscheiden:

_____ Teilnehmer, die bereits etwas für ihre Sicherheit tun und auch willens sind, mehr zu tun, wenn sie die richtigen Möglichkeiten dazu aufgezeigt bekommen

_____ Teilnehmer, denen die Thematik eigentlich egal ist und die eher als „Mitläufer" handeln (sog. Follower), wenn und wo es ihnen nicht „weh tut"

_____ Teilnehmer, die aus konkreten Gründen, also absichtlich, keine oder nur geringe Sicherheit umsetzen möchten

Die IT-Sicherheit funktioniert ähnlich wie der Umweltschutz: Einzelne und ihr richtiges, nachhaltiges Handeln bilden eine Keimzelle, die unbedingt erforderlich ist. Wesentliche Schwellwerte kann man aber nur überschreiten, wenn viele oder sogar alle in einer „Community" ihre ähnlichen Schutzziele vergleichbar robust umsetzen, da sich Kommunikation und Prozesse in solchen Handlungsgemeinschaften immer enger aufeinander abstützen.

Für das Ziel einer verbesserten Gesamtsicherheit gilt es also, für die erste der genannten Gruppen gute Lösungen bereitzustellen und vor allem über verlässliche Sekundärindikatoren neutraler Stellen Entscheidungssicherheit herzustellen (siehe Haupttext). Die Follower werden dann nachziehen, sobald keine Einbußen im Komfort festzustellen und die Preise annehmbar sind – oder größere Schäden in der Presse so angesprochen werden, dass sich die Handelnden persönlich angesprochen fühlen.

Die dritte Gruppe wird vermutlich nur handeln, wenn eine mit Sanktionen belegte Regulierung für sie greift. Doch selbst dann können freiwerdende Kapazitäten und Investitionen nur in echte Sicherheitsverbesserungen fließen, wenn Blaupausen mit Vorbildcharakter existieren – also Lösungen real in Betrieb sind, denen neutrale Stellen bestätigen, dass sie die regulatorischen Anforderungen sanktionsbefreiend erfüllen.

derte freie Recht, sich selbst mit Schadcode zu infizieren, muss auf seinen demokratischen Konsens hin überprüft werden. Gibt es den nicht, dann muss der Markt sich so weiterentwickeln, dass die Marktdurchdringung eines Basisschutzes ähnlich nahe an 100 % liegt wie heute schon die Durchdringung mit Anti-Viren-Software.

Der einfache Zugang zu schützender Technologie ist eine wesentliche Voraussetzung hierfür: Diese Technologie ist in Ansätzen schon erkennbar. So hat beispielsweise Microsoft in Windows 10 das automatische (Wieder-) Anschalten des plattformeigenen Anti-Virus-Programms implementiert, wenn ein potenziell installiertes Zusatzprodukt nicht mehr lizenziert ist oder aus anderen Gründen seinen Dienst einstellt.

Installation

Eine sichere Organisation nützt nichts, wenn sie nicht „gelebt" wird – und ein Produkt nützt nichts, wenn es nicht „richtig" installiert beziehungsweise (sicher) konfiguriert ist. Nahezu jedes IT-Sicherheitsverfahren kann man auch so einrichten, dass es keine Sicherheitsziele erfüllt. Es empfiehlt sich also, vor der Installation zu untersuchen, welche Schutzziele man eigentlich damit erreichen will und wie der Einsatz des neuen Werkzeugs eventuell mit den Schutzzielen von bereits etablierten Produkten harmonisiert werden muss. Dabei handelt es sich um eine sehr herausfordernde Aufgabe: „Mal eben schnell" nebenbei geht das nicht. Unter Fehlern der Installation kann man jedoch gegebenenfalls lange leiden – oft sogar eine geraume Zeit, ohne es zu bemerken.

Auch hier wäre es sehr hilfreich, wenn die Expertise großer IT-Organisationen beim sicheren Betrieb auch interessierten KMU zugänglich gemacht würde. Solche Versuche sind sogar bereits unterwegs: So haben einige DAX-Unternehmen mit der DCSO eine IT-Security-Firma gegründet, die auch Dritten mit gebündelten Erfahrungen helfen soll. Der CIO-Verband VOICE hat ebenfalls eine Anlaufstelle für seine Mitglieder organisiert. Optimal wäre es, wenn hier auch die Expertise des Bundes – nicht zuletzt aus der Konsolidierung seiner IT – mit eingesteuert und dadurch multipliziert werden könnte.

Betrieb

Bei Systemen, die dem Schutz dienen, sollte man vorsichtig mit Möglichkeiten umgehen, sie in Echtzeit umzukonfigurieren oder ihre durch die Installation einmal erreichten Sicherheitsziele in Echtzeit manuell zu reduzieren. Eine Remote-Administration vom Urlaubsort aus, wie sie verschiedene Werbebroschüren visualisieren, ist mehr als bedenklich.

Vielmehr ist es notwendig, ein die erreichte Sicherheit erhaltendes Betriebskonzept zu entwickeln, das auch geprüft oder – noch besser – mittels technischer Maßnahmen erzwungen („enforced") wird. Zusätzlich gilt: Je mehr unterschiedliche Systeme man betreibt, umso wahrscheinlicher sind menschliche Fehler. Insofern ist es zwar manchmal sinnvoll, zwei Verfahren oder Produkte für ein Thema zu nutzen, Kosten für zusätzliches Know-how und abgestimmtes Betriebskonzept müssen dabei aber ebenfalls berücksichtigt werden.

Damit keine Defizite an den Schnittstellen zu anderen Produkten entstehen, empfiehlt es sich, vorab in einem „Proof of Concept" (PoC) sowohl die Installation als auch den korrekten Betrieb zu testen und gegebenenfalls nachzubessern.

All diese Verfahren kosten Zeit und Geld – viele KMU können sich das nicht leisten. Optimal wäre deshalb eine generische Blaupause für eine Sicherheitsarchitektur, die in mehreren Implementierungen (also unterschiedlichen Produktzusammenstellungen) mit dieser Schnittstellenproblematik im Betrieb beschrieben wird. Diese Produktzusammenstellungen ergeben dann im besten Fall eine Gesamtlösung, die man per monatlicher Miete beziehen kann – ohne das Erfordernis, innerhalb des KMU eigene Expertise aufzubauen. Bereits erfolgte Investitionen des KMU könnte man dabei berücksichtigen, indem deren einzelne Komponenten in die Architektur integriert werden, wodurch wiederum neue Produktzusammenstellungen entstehen, deren Robustheit dann im Echtbetrieb überprüft werden könnte.

Mangel an Menschen

IT-Sicherheitshersteller in Deutschland beklagen einen Fachkräftemangel bei vielen Positionen in der Herstellung sicherer IT-Produkte von der Planung über Produktion, Qualitätssicherung und Marketing bis in den Vertrieb. Diesem Fachkräftemangel will man offenbar zunehmend durch neue Ausbildungsprogramme begegnen – doch das braucht Zeit.

Unabhängig davon kann es sich längst nicht jedes KMU leisten, eine eigene IT-Security-Abteilung zu unterhalten, die Leistungen des BSI, eines TÜV oder anderer Organisationen nachbildet, um die Robustheit von IT-Sicherheit entlang akzeptierter Standardverfahren zu beurteilen. Auch heute schon existierende Zertifikate, etwa nach Common Criteria, lösen dieses Problem nicht, weil die Evaluierung nur gegen die für die Prüfung definierten „Protection Profiles" erfolgt – und bereits das Verständnis für deren Inhalte und damit die „Aussagekraft des Zertifikates für die eigene IT" ein Know-how erfordert, das in KMU nicht vorhanden ist.

Zusammenfassung

Know-how und Fachleute zur Bewertung der Robustheit und des Schutzgrades von Lösungen sind prinzipiell vorhanden – es handelt sich aber um ein Spezial-Know-how, das nicht beliebig multiplizierbar ist. Die Frage der Fragen lautet daher: Wie kann man dieses Spezial-Know-how so einsetzen, dass möglichst alle darauf zugreifen können und die Ergebnisse selbst verbindlich und vertrauenswürdig sind?

Es wird kein Weg daran vorbeiführen, die aufgezeigten Liefer- und Handlungsketten vollständig transparent und vertrauenswürdig zu gestalten. So sind in der klassischen Sicherheit etwa Listen von vertrauenswürdigen Alarmanlagen und Listen mit Unternehmen üblich, welche diese adäquat verarbeiten und einbauen können. In Sachen IT-Sicherheit lassen wir jedoch – Stand heute – Bürger und KMU bezüglich der Auswahl von Prozessen, kommerziellen Produkten auf Basis ihrer Robustheit sowie hinsichtlich ihrer Integration und ihrem sicheren Betrieb gänzlich alleine, obwohl dazu fundierte Kenntnisse vorliegen. Und größere Unternehmen sind darauf angewiesen, aufwändige Analysen jeweils selbst durchzuführen – das mag gehen, bindet aber zumindest teilweise auch unnötig wertvolle (Fach-)Kräfte.

Selbst die Annahme, dass sich Behörden und Kommunen – allein schon, um durch die Abnahme großer Mengen die Kosten zu senken – auf wenige standardisierte Produkte einigen und die Erfahrungen bei Installation und Betrieb in User-Communities austauschen könnten, ist deutlich zu optimistisch. So gibt es zwar beispielsweise bei der Bundeswehr durch die so genannte „Technische Architektur der Bundeswehr“ (TA-Bw) Standards, die bis auf Produktniveau reichen – diese haben aber keine Auswirkung in anderen Ressorts. Und für viele Organisationen der öffentlichen Hand sind sie gar nicht sichtbar, weil die TA-Bw selbst eingestuft ist.

Blockaden auflösen

Häufig ist zu hören: „IT-Sicherheit ist nicht alles, aber ohne IT-Sicherheit ist alles nichts.“ In der Tat werden

Medienkompetenz und Wertewandel

Galt es im letzten Jahrhundert noch als Inbegriff von Freiheit, wenn ein 18-jähriger sein erstes Auto kaufte, so gibt es heute Gesellschaftsgruppen, die sich durch ein eigenes Auto zu stark angebunden fühlen. Sie nehmen es vielmehr als Freiheit wahr, am Carsharing teilzunehmen und eben keine Verantwortung für ein eigenes Auto zu tragen.

In einigen Communities ist bezüglich des geltenden beziehungsweise „gelebten“ Datenschutzes und des Wunsches nach Schutz in der digitalen Umgebung in Deutschland ebenfalls ein Wertewandel wahrzunehmen, sodass ein bewegliches Ziel bezüglich der zu schützenden Information und vieler anderer Parameter entsteht.

Dieser Wertewandel führt auch dazu, dass die gesellschaftlichen Ziele bezüglich der Vertraulichkeit beispielsweise von personenbezogenen Daten auf der einen Seite und den Möglichkeiten von „Big Data“ auf der anderen Seite aktuell keiner klaren demokratisch (bzw. gesamtgesellschaftlich) anerkannten Linie unterliegen, wodurch natürlich auch der Transport von Lerninhalten an Schulen „weichen“ und teilweise persönlichen Auslegungen unterliegt.

Für die besondere Problematik des Datenschutzes und vor allem des Bundesdatenschutzgesetzes (BDSG) findet man viele Beispiele:

_____ Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hat in einem Bericht festgestellt, dass die AGB von iPhone und iPad in mehreren Punkten gegen das BDSG verstoßen, was niemanden wirklich verblüfft hat. Interessant ist, dass diese formale Feststellung keine Reaktion auslöst, die Apple dazu zwingt, dieses Problem zu beheben.

_____ Mit deutschen Steuergeldern finanzierte Projekte in Entwicklungsländern nutzen immer auch IT und bauen zum Teil auch IT-Infrastruktur auf. Das BDSG wird dabei jedoch nicht verpflichtend mit implementiert – weder in den eigenen Systemen noch in den Systemen vor Ort.

Während man einen Verlust an Verfügbarkeit von Informationen meist sofort bemerkt, wird der Verlust der Integrität erst im Problemfall und der Verlust der Vertraulichkeit spät oder sogar nie bemerkt. Die Beweisbarkeit von Schutzverletzungen, also erfolgreichen Angriffen, folgt ebenfalls dieser Reihenfolge – in der IT-Sicherheit ist dieser Zusammenhang seit Langem bekannt.

Solche einfachen Erkenntnisse (hier gibt es ja noch viel mehr wesentliche Entscheidungsfaktoren) und ihre Konsequenzen in die gesamte Bevölkerung zu transportieren, um eine so genannte Medienkompetenz herzustellen, scheitert aber aus verschiedenen Gründen:

_____ Die Communities mit reduziertem Datenschutzempfinden ziehen sich durch alle Bevölkerungsgruppen und alle Altersstrukturen, weshalb es nicht den „einen“

bei vielen Themen und Innovationen wie Cloud, Industrie 4.0, Outsourcing und sogar dem Abschluss von Außenhandelsvereinbarungen Belange der Datensicherheit und des Datenschutzes als blockierende Faktoren genannt.

Unbestritten gibt es täglich viele Angriffe – die Tendenz ist in Quantität und Qualität zunehmend. Viele hundert Seiten Text über intendierte Sicherheitsarchitekturen, gesetzte Sicherheitsziele, das Commitment von CXOs zu diesen Zielen und verabschiedete Sicherheitsregeln werden die Cyber-Attacken nicht abwehren, sind aber – wenn sie professionell gemanagt werden – eine notwendige Voraussetzung für sinnstiftendes Handeln.

Betreiber von IT-Systemen, Beschaffer von IT-Produkten, IT-Dienstleister und Anwender stehen dabei jedoch vor dem Problem, ihren Schutzbedarf (oder den ihrer Kunden) gegen Bedrohungen durchzusetzen, die ihnen allzu oft unverständlich sind. Dazu wählen sie Vorgehensmodelle und Lösungen und müssen sichere von weniger sicheren oder sogar unsicheren Lösungen unterscheiden, um den individuell als adäquat betrachteten Schutzbedarf umzusetzen und das investierte Geld zielorientiert einzusetzen.

Softwareprojekte sollen nur noch unter dem Credo „Security by Design“ arbeiten und so sicherstellen, dass die Implementierungen von Anfang an sicher sind – und scheitern am hierzu benötigten Know-how. Medienkompetenz (vgl. Kasten) soll schon im frühen Kindesalter geschult werden – Lehrer und Professoren mit geeigneten Fähigkeiten sind jedoch Mangelware. Trainingsmodelle und Lerninhalte bleiben überdies meist unscharf, da beispielsweise die Diskussion um einen sinnvollen Datenschutz gegenüber den Vorteilen großer Datensammlungen noch keinen gesellschaftlichen Konsens erbracht hat.

Wege zur Abhilfe

Während Politik und Gesellschaft der Frage nachgehen, wie wir in 10 oder 20 Jahren die geschilderten Know-how-Engpässe überwinden können, bleibt es zwingend notwendig, Strategien zu entwickeln und

definierten Kommunikations-Kanal gibt, um die Hintergründe und Vorteile von „der Privatheit von Daten“ zu kommunizieren. Ziel müsste es ja sein, dass jeder Bürger seine Entscheidung über die Privatheit beziehungsweise Vertraulichkeit seiner Daten selbst treffen kann, sobald er ein geeignetes Alter beziehungsweise Kompetenz erreicht.

_____ Für Ausbildungseinrichtungen wie Schule, Universität, Erwachsenenbildung et cetera lässt sich kein klarer Lerninhalt erkennen, der wirklich demokratisch konsolidiert ist, da die gesellschaftliche Diskussion noch offen ist. Insofern bleibt nur der praktische Umgang nach bestem Wissen und Gewissen der Lehrer und Ausbilder im digitalen Wandel – was im Normalfall deren persönlicher Meinung entspricht. Die persönlichen Meinungen zu den sinnvollen Datenschutz-Zielen unterliegen aber auch bei Lehrern und Ausbildern der bereits erwähnten breiten Varianz.

_____ Werden in der Ausbildung hohe Datenschutz-Ziele als wertvolle Inhalte transportiert, so müssen diese Ziele natürlich auch praktisch umsetzbar sein. Es gälte also, die Robustheit des hierzu vorgesehenen Schutzes ebenso zu unterrichten. Das würde aber dazu führen, dass entweder jeder Bürger ein IT-Sicherheitsexperte wird oder klare, einfache Aussagen zu der Robustheit von Produkten und Lösungen von einer geeigneten neutralen Stelle gemacht werden müssten.

Mit der Seite „BSI für Bürger“ gibt es zwar schon eine entsprechende Informationsquelle, diese beschäftigt sich aber nur mit kostenfreien Lösungen, nicht mit Kaufprodukten. Konkrete Angaben zu konkreten Lösungen von neutralen anerkannten Stellen scheinen jedoch der einzige Weg zu sein, der es ermöglicht, der Komplexität des Themas und vorliegenden Know-how-Engpässen gerecht zu werden. In vielen Produktlandschaften sind schriftlich belegte Qualitätskriterien ein wesentlicher Faktor im Markt – in der IT-Sicherheit jedoch (noch) nicht.

Albert Einstein wird zugeschrieben, dass er die Dummheit darin sah, bei dauerhaft gleichbleibender Handlungsweise andere Ergebnisse zu erwarten. In vielen Branchen (z. B. Automotive, Gesundheit und Ernährung) hat man nach dem Erkennen von Problemen gehandelt, indem striktere Kontrollen, geforderte Merkmale, Nachweise über Lieferketten, Nachweise über verwendetes Material et cetera sowie eine darauf basierende Haftung eingeführt wurden.

Es bleibt zu hoffen, dass auch in der IT-Sicherheit bald adäquate Mechanismen etabliert werden, dank derer sich jeder Lehrer, jeder Bürger, jedes KMU und jedes Unternehmen auf seine Kernkompetenzen und -aktivitäten im digitalen Raum konzentrieren kann. Die Robustheit des Schutzes von IT-Systemen müsste dann nach klaren, einfachen Mechanismen für jeden Teilnehmer durch belegte, neutrale Aussagen nachgewiesen werden. Dann wären Kauf und Nutzung von IT-Sicherheit ähnlich einfach, standardisiert und selbstverständlich wie die TÜV-Prüfung und -Plakette an jedem Auto in Deutschland.

umzusetzen, die trotz dieser Engpässe echten Schutz ermöglichen. Eine der wenigen Möglichkeiten ist es, das vorhandene Know-how zu bündeln und vertrauenswürdige Kommunikationskanäle zu möglichst standardisierten, konsolidierten Ergebnissen zu etablieren – keine einfache Aufgabe.

Es wird wohl keine andere Möglichkeit geben, als gute und verlässliche Sekundärindikatoren einzurichten. Solche Sekundärindikatoren können aber trügerisch sein: So haben Einkäufer zum Teil sehr komplexe Mechanismen erarbeitet, um sicherzustellen, dass sie immer nur von Unternehmen beziehen, die in den verschiedensten IT-Produkten über längere Zeiträume hinweg die günstigsten Preise und Konditionen bieten – der Transferschluss, dass diese Lieferanten auch die sichersten Produkte liefern, ist aber natürlich unzulässig.

Vertrauensketten

Geeignete Vertrauensketten sind indes eine gute Lösung für den aktuellen Engpass der Know-how-Ressourcen. Um das Vertrauen in eine solche Kette und ihre Handlungsträger herzustellen, muss der Endabnehmer allerdings nicht nur überzeugt werden, hierüber die von ihm gewünschte Robustheit zu erhalten, sondern der eingekaufte Schutz muss auch unter dem Aspekt „State of the Art“ sein Geld wert sein und darf keine Mogelpackung darstellen.

In klassischen („analogen“) Märkten haben sich verschiedene Organisationen wie beispielsweise die Stiftung Warentest, die TÜVs und viele andere dem Aufdecken solcher Mogelpackungen gewidmet. In der IT-Sicherheit funktioniert das noch nicht so gut, da die Schutzziele nicht einfach zu artikulieren sind und das Know-how für geeignete Verfahren (z. B. Penetrationstests und White-Hat-Hacking) nicht so verbreitet verfügbar ist.

Um es einem Fachmann zu ermöglichen, sich von ihrer eigenen Robustheit zu überzeugen, muss eine Vertrauenskette zumindest in fünf „Dimensionen“ vollständig und nachweisbar sein: Technik, Organisation, Rechtssicherheit, Haftung und Lieferkette.

_____ Technik wird bereits häufig diskutiert und ist eigenständig schon sehr komplex. Neu in der Betrachtung sind hauptsächlich der „letzte Meter“ und die Betrachtung der Schnittstellen zwischen den Sicherheitslösungen.

_____ Unter Organisation ist regelmäßig mehr zu verstehen als nur eine Sicherheitsrichtlinie, die aufgeschrieben wird und mit asynchronen Security-Awareness-Maßnahmen versucht, den Anwender mit in die Verantwortung einzubinden. Die Organisationseinbindung muss vielmehr alle Elemente einer Sicherheitsrichtlinie entweder technisch umsetzen oder in Echtzeit in konkrete Handlungsanweisungen übersetzen, die der Anwender auch versteht. Zwingend gehört auch ein Monitoring des Verbotenen zur organisatorischen Einbettung, wenn sich Verbotenes aus anderen Gründen nicht vollständig blockieren lässt.

_____ Rechtssicherheit entsteht erst, wenn die verschiedenen Rechtsräume, die Anwendung finden, sich in den wesentlichen Fragen widerspruchsfrei überlagern. Diese Überlagerung kann durch verschiedene Orte der Datenhaltung, aber auch durch unterschiedliche Produktionsorte von verschiedenen Teilen einer Lösung herbeigeführt werden.

_____ Zurzeit ist kaum eine Haftung für die Robustheit der Einsatzziele gegeben – die vorherrschende Überlagerung der Rechtsräume erschwert die Durchsetzbarkeit einer eventuell bestehenden Haftung zusätzlich.

_____ Lieferketten sind nicht nur bezüglich der Rechtssicherheit und Haftung eine wesentliche Komponente zur Einschätzung der Robustheit: Soft- und Hardware setzt sich zumeist aus verschiedensten Komponenten mit unterschiedlichen Lieferwegen zusammen, was etliche Schwierigkeiten bewirken kann, die im Folgenden näher erläutert werden.

Lieferketten

Zum einen könnten auf diesen Wegen Hintertüren oder zusätzliche Komponenten eingebaut worden sein, die für den Einsatz in schützenswerter Umgebung hinderlich wären (z. B. Fernwartungsfunktionen).

Zum anderen muss vor allem bei Produkten, die direkt die IT-Sicherheit fördern sollen, aber auch bei Produkten, die Cyber-Angriffen ausgesetzt sind, die Handlungsgeschwindigkeit gegenüber neuen Angriffen als eine wesentliche Qualität gelten: Besteht eine Lösung aus vielen verschiedenen Komponenten, die Open Source und Drittanbietern entstammen, dauert es meist wesentlich länger, die gesamte integrierte Liefereinheit gegen aktuelle Angriffe zu prüfen und – noch wesentlicher – die verbauten Komponenten im Falle einer Verletzbarkeit verlässlich nachbessern zu lassen. Denn diese Nachbesserung kann in der Regel ja nicht in Eigenregie durchgeführt werden, sondern hierzu müssen eventuell sogar mehrere Teilnehmer der Lieferkette koordiniert aktiv werden.

Heute sind dabei noch nicht einmal alle verbauten Komponenten mit ihrer jeweiligen Lieferkette auszuweisen – weder der letztendliche Nutzer noch die Akteure innerhalb einer Lieferkette haben notwendigerweise Kenntnis über alle verbauten und mitgelieferten Komponenten. Das ist einer Sicherheitseinschätzung wenig dienlich und

verhindert die benötigte Transparenz. Denn transparente Lieferketten dienen Käufern nicht nur zur Einschätzung der damit verbundenen digitalen Souveränität, sondern auch hinsichtlich der möglichen Handlungsgeschwindigkeit gegenüber Angriffen.

Fazit

In einem Umfeld mit beweglichen Schutzzielen und fehlenden Vertrauensketten ist es für viele Marktteilnehmer heute nahezu unmöglich, echte, robuste IT-Sicherheit zu kaufen und zu implementieren.

Viele Unternehmen und Anwender benötigen dazu einfach befolgbare Handlungsabläufe und konkrete Empfehlungen für vertrauenswürdige Integratoren, Berater und Produkte sowie Sekundärindikatoren (z. B. in Form von Hersteller-Erklärungen über Lieferketten mit Haftungsübernahme bei Fehlinformation), entlang derer sie prüfen können, ob die dargestellten Vertrauensketten und Lösungen für sie adäquat sind.

Die Empfehlung, dass jeder einzelne Anwender selbst so viel „Security-Awareness" entwickeln sollte, dass alle an der Informationsverarbeitung Beteiligten – im privaten wie im geschäftlichen Umfeld – sicher handeln könnten, geht teilweise am Thema vorbei, denn gute Angriffe sind immer unsichtbar.

Wenn wir uns allerdings als Gesellschaft und Markt intelligent aufstellen und bei einzelnen Marktteilnehmern durchgeführte Analysen und bereits erreichte Schutzziele in adäquaten, verlässlichen Vertrauensketten kommunizieren könnten, dann ließen sich diese Maßnahmen mit geringerem Aufwand multiplizieren – und so mit geringeren Kosten und vor allem geringerem Know-how auch einführen und betreiben.

Wir sind also eigentlich doch nicht „zu dumm" für die IT-Sicherheit. Aber wir nutzen die verfügbaren Ressourcen – unser kollektives Know-how – nicht effizient, weil wir den wirklichen und nachgewiesenen Experten nicht den geeigneten Glauben schenken und die hierzu notwendige vertrauenswürdige Infrastruktur nicht anlegen.

Es gibt zwar viele Gründe, warum sich das in den letzten 20 Jahren so entwickelt hat, wie es nun einmal ist – wichtig ist aber, dass wir die Chancen, die gerade durch zentralisierte Organisationen wie DCSO, VOICE, ITZB und viele andere entstehen, und die aktuellen Konsolidierungsvorhaben in diesen Organisationen wirklich nutzen.

Die Konsolidierung der Bundes-IT im ITZB könnte hier Vorbild werden, wenn die Aussagen von Frau Dr. Suder, Herrn Engelke und Herrn Vitt in die Tat umgesetzt werden und nicht in Organisation, Papier und „Willen" hängen bleiben, sondern bis in die Konsolidierung von Plattformen und Lösungen durchgreifen – und die Ergebnisse dann auch so kommuniziert werden, dass sie für andere Teilnehmer ebenfalls nutzbar werden. Zum Beispiel könnten Branchenverbände diese für ihre jeweilige Branche „übersetzen".

So würden Vertrauensketten entstehen, welche die Erfahrungen aus unterschiedlichen Umgebungen bündeln und über vertrauenswürdige Informationsketten bis in die KMU weiterleiten – und dabei ein für den jeweiligen Nutzer / Marktteilnehmer „konsumierbares" Format zur Verfügung stellen. ■

Ramon Mörl ist Geschäftsführer der itWatch GmbH.

Literatur

[1] Ramon Mörl, Stets bemüht um Sicherheit?! (1), Beispiele, Fragen und Gedanken dazu, warum in Sachen Sicherheit so viel schiefgeht, <kes> 2016#2, S. 19