Kampf den Datendieben

Mit dem Einstieg in das Internet der Dinge kommt die Angst vor Cyberkriminalität. Wie können wirksame Sicherheitsstrategien aussehen? Ein Überblick. *Von Rainer Böhme*

Es ist bereits absehbar, dass sich im Internet der Dinge ein Teil der IT-Geschichte wiederholt. In den 1980er Jahren eroberten Heimcomputer und PCs die Wohnzimmer und Büros. Zunächst gänzlich ohne Vernetzung, war die Gefahr durch Angriffe bestenfalls aus Hollywood-Filmen bekannt. Für Nutzer unbequeme Sicherheitsmechanismen wurden kaum erprobt und waren dadurch entsprechend fehleranfällig oder fehlten gänzlich. Das böse Erwachen kam mit der weltweiten Vernetzung dieser unsicheren Endgeräte. Selbst ein Austausch der Hardware verbesserte die Sicherheit nicht, denn in der IT-Industrie ist Kompatibilität der Schlüssel zum Erhalt von wertvollen Marktanteilen.

Heute enthält fast jedes produzierte Stück Haushalts- und Gebäudetechnik – von der Kaffeemaschine zum Türschloss – programmierbare Rechner, deren Leistung oft die PCs der 1990er übertrifft. Mit dieser Entwicklung folgen immer mehr Branchen den ungeschriebenen Gesetzen der IT-Industrie: Hersteller schielen auf Marktanteile und verzichten auf Sicherheit, die bei digitalen „Dingen“ noch unbequemer ist. Wenn schon die Eingabe eines Passworts Mühe bereitet, wie soll sich ein Mensch gegenüber einer Vielzahl ihn umgebender Geräte authentifizieren, die keine Tastatur haben?

Erforschung neuer Sicherheitstechniken

Mit der Vernetzung dieser Geräte zum Internet der Dinge eröffnen sich neue Hintertüren für Kriminelle. Sie können ihre Opfer aus der Ferne behindern (Türschloss öffnet nicht), beobachten (Tür lange nicht bedient), Einbrechern Einlass gewähren (Tür öffnet), betrügen (Kaffeemaschine bedient Kreditkarte per Nahfeld-Funk) oder schlecht administrierte Geräte generell so umprogrammieren, dass sie als Plattform für weitere kriminelle Aktivitäten dienen. Strafverfolger werden sich die Zähne ausbeißen, wenn die digitalen Spuren von Tätern über die Geräte Hunderter Unbeteiligter verlaufen.

Trotzdem ist das Internet der Dinge zu verlockend, um aus Angst vor Cyberkriminalität ganz darauf zu verzichten. Umso wichtiger ist es, jetzt wirksame Strategien zu entwickeln. Es müssen neue und an das Internet der Dinge angepasste Sicherheitstechniken erforscht und standardisiert werden. IT-Sicherheit ist jedoch nicht nur ein technisches Problem. Auch die wirtschaftlichen Rahmenbedingungen müssen diejenigen Hersteller belohnen, die sichere Produkte anbieten sowie unvermeidbare Schwachstellen über die Lebenszeit zügig und im besten Interesse ihrer Kunden beheben.

> Die Verantwortung für sicherheitsbewusstes Verhalten können Endnutzer nicht an Hersteller oder Experten delegieren, denn sie allein wissen und entscheiden, wann wer welche „Dinge“ wie nutzen darf.

Damals nur ein Szenario aus Hollywood: Der Schauspieler Matthew Broderick spielt im amerikanischen Kinofilm „War Games“ aus dem Jahr 1983 einen jungen Hacker.

FOTO PICTURE ALLIANCE/DPA

All das ist leichter gesagt als getan, denn jeder einzelne Aspekt benötigt Fachkenntnis und Erfahrung. Trotzdem passieren Fehler: Ein weltweiter Funkstandard für die Heimautomation sieht zwar Verschlüsselung vor, liefert aber einen Ersatzschlüssel, für jedermann einsehbar, in der Spezifikation mit. Es dauerte zwei Jahre, bis dieser offensichtliche Fehler von Sicherheitsforschern öffentlich bemerkt wurde.

Technische Herausforderungen stellen sich beim Einsatz von sicherer Kryptographie auf kleinsten Geräten mit sehr begrenztem Energievorrat. Es herrscht ein inhärentes Ungleichgewicht zwischen den Verteidigern (viele kleine, billige, batteriegespeiste Geräte) und einem Angreifer, der – vom schwächsten Ziel ausgehend – mit Spezialhardware sowie den Rechen- und Energiereserven aus der weltweiten Cloud versucht, kryptographische Sicherungen zu überwinden. Weitere Problemfelder sind die sichere Authentifikation zwischen einem Nutzer und seinen Geräten sowie die Verwaltung der Zugriffsrechte für eine Vielzahl von Nutzern mit unterschiedlichen Rollen und wechselnden Bedürfnissen. Hier passieren Fehler, weil die Materie komplex ist und Endnutzer nicht gleichermaßen mit den digitalen Sicherheitskonzepten vertraut sind, wie sie in der analogen Welt selbst mit komplizierten Sicherheitsmechanismen sozialisiert wurden: Die meisten Menschen können ein Fahrradschloss sicher anbringen oder vermeiden es, Blankoschecks zu unterschreiben. Die Verantwortung für sicherheitsbewusstes Verhalten können Endnutzer nicht an Hersteller oder Experten delegieren, denn sie allein wissen und entscheiden, wann wer welche „Dinge“ wie nutzen darf. Sie müssen es ihren Geräten irgendwie mitteilen, und zwar so, dass Dritte die Berechtigungen nicht eigenmächtig ändern können. Erneut zeigt sich die Bedeutung einer sicheren Authentifikation.

Als technische Lösungsansätze gelten selbstlernende Systeme. Diese verhalten sich jedoch weniger berechenbar als Systeme mit festen Regeln, und es besteht das Risiko, dass Kriminelle die Lernphase zu ihren Gunsten beeinflussen. Ein anderer Ansatz versucht, mehr Sicherheitsmechanismen in die Netze zu verlagern, die Geräte verbinden. Hier ergeben sich Vorteile, wenn pro Person oder Haushalt nur noch ein Netz statt Hunderte von Geräten einzeln verwaltet werden. Die Netze könnten auch Daten filtern, damit neu entdeckte Schwachstellen nicht zum Sicherheitsrisiko werden, solange der Hersteller kein Update bereitstellt. Die Administration dieser Netze bleibt aber anspruchsvoll und somit für Jahrzehnte Fachleuten vorbehalten.

Produkte mit Mindesthaltbarkeitsdatum

Es bleibt die Frage nach den richtigen Rahmenbedingungen. Heutige Software ist oft unsicher, weil es sich für Hersteller nicht lohnt, in Sicherheit zu investieren. Ein erster Schritt wäre, die Haftung für fehlerhafte und unsichere Softwareprodukte eindeutig zu regeln und bei digital vernetzten „Dingen“ konsequent durchzusetzen. Dies schließt sichere Voreinstellungen und eine kostenlose Bereitstellung von Sicherheits-Updates ein. Diese dürfen nicht mit Änderungen der Funktionalität kombiniert werden und müssen die gesamte Lebenszeit der betroffenen Geräte abdecken. Damit Kunden nachhaltige Kaufentscheidungen treffen können, sollten Produkte mit einem Mindesthaltbarkeitsdatum gekennzeichnet werden. Trotzdem nicht vollständig vermeidbare Sicherheitslücken müssen leicht aufspürbar sein und veröffentlicht werden. Eine Erlaubnis zum Reverse Engineering für diesen Zweck würde die Nutzer in Europa schützen und den Standort für Sicherheitsforschung attraktiver machen. Nur eine Kombination aus Technik und Regulierung sowie langfristig die Sozialisation der Nutzer mit der Logik digitaler Sicherheitsmechanismen kann ein kostspieliges Déjà-vu beim Internet der Dinge vermeiden.

Rainer Böhme ist Professor für Sicherheit und Datenschutz am Institut für Informatik der Universität Innsbruck.

Die wichtigsten E-Commerce-Trends 2016

Die fortschreitende Digitalisierung führt zur Integration von Commerce in nahezu alle Lebensbereiche. Leistungsfähige IT-Systeme ermöglichen, dass Ubiquitous-Commerce – also der ständige Austausch von Daten und Informationen zwischen Händlern, Kunden und Systemen – allgegenwärtig wird. Die Trends im Überblick.

VON DIETHELM SIEBUHR

Mega-Omni-Channel

Anbieter können und müssen heute über eine Vielzahl an digitalen Kontaktpunkten mit potentiellen und aktuellen Kunden interagieren. Von der Zahl der genutzten Geräte über Kommunikations-Apps bis hin zu Sensoren: Alle Kontaktpunkte – ob es nun der Konfigurator ist, die „Jetzt kaufen“-Funktion im Messenger oder ein Aktivitätstracker, der einen Sportschuhkauf auslöst – müssen geplant, gemanagt, ja geradezu orchestriert werden auf dem „Path to Purchase“. In diesem Jahr gewinnt, wer die Handhabung von Big Data in noch komplexeren, also Mega-Omni-Channelstrukturen, beherrscht und die richtigen Folgerungen für seinen Shop ableitet.

Online integriert Offline

Eine Erweiterung der Kundenschnittstelle stellt auch der Weg von Online zu Offline dar. Online-Händler erkennen den Wert der physischen Präsenz vor Ort. In den Prozessen bedeutet dies, dass Online-Händler nun auch den Kanal „offline“ in ihre Systeme integrieren müssen. Der traditionelle stationäre Handel wird hingegen zunehmend online: Apple-Stores machen vor, wie mittels Sensoren sowie Check-in- und Check-out-Systemen der Besuch im Laden in der Kundenhistorie abgebildet werden kann. Auch für Click and Collect – also Online-Kauf und Offline-Abholung in der Filiale – sind channelübergreifende Prozesse gefragt.

> Cybercrime-Aktivitäten haben E-Commerce als bevorzugtes Ziel in den Fokus genommen.

Herausforderung Same-Day-Delivery

Im Bereich Lieferung sind die Kundenansprüche in den letzten Jahren enorm gewachsen, was für viele Online-Händler zu einem immer größeren Problem wird: Die Versuche, mit Drohnen oder Paketboxen die Zustellprobleme zu lösen, zeigen, dass es zunehmend auf „Jetzt liefern“ und nicht mehr nur auf „Jetzt bestellen“ ankommt. Wer dieser Herausforderung gewachsen ist und sie mit innovativen Systemen lösen kann, punktet künftig gegenüber Wettbewerbern.

Sicherheit wird wettbewerbsentscheidend

Während Händler bei der Lieferung in erster Linie versuchen, Bequemlichkeit und Zeitaufwand zu optimieren, müssen sie sich in Sachen Sicherheit einem Thema stellen, das zu einer Überlebensfrage werden kann. Cybercrime-Aktivitäten haben E-Commerce als bevorzugtes Ziel in den Fokus genommen. Kunden sind heute weniger denn je bereit, Datenmissbrauch zu akzeptieren. E-Commerce-Anbieter müssen daher ihre Anstrengungen zur Verbesserung der Sicherheit deutlich erhöhen. Nur wer über führende Sicherheitslösungen verfügt, kann im E-Commerce dauerhaft mitspielen.

Commerce geht in die Verlängerung

Mit dem bloßen Kauf der Ware ist der Prozess heute noch nicht zu Ende. Nicht nur angesichts des Nachhaltigkeitsgedankens, der gegen ein Ex-und-Hopp vom veralteten Elektronikgerät spricht: Viele Zielgruppen sind einfach mit den unzähligen Funktionen des Fernsehers überfordert oder wollen sich nicht von der guten alten Waschmaschine trennen. Start-ups wie zum Beispiel Expertiger oder My-Home-Service haben das Potential der „Home-Tech-Services“ erkannt. Physische Güter werden durch Online- oder sensorgestützte Anwendungen wie begleitende Liefer-, Installations- oder Wartungs-Services wertvoller für den Kunden – zum Teil können eigenständige Leistungen, beispielsweise Handwerker-, Raumpflege-, oder Betreuungsservices angeboten werden.

Der Markt setzt auf die Nische

Auch die horizontale Erweiterung der Dimension dessen, was auf innovative Art vertrieben werden kann, nimmt zu. „Food-Commerce“ gewinnt beispielsweise an Popularität. Dabei zeigt sich im Bereich Lebensmittel ein Trend zur Erosion der Mitte, der den gesamten Online-Handel prägt: Im Mainstream konzentriert sich alles auf die Megaplayer, bei Nischenangeboten besteht durchaus die Chance der Kleinen. Bei Lebensmitteln können regionale Anbieter als Online-Bio-Wochenmarkt oder Gourmetanbieter erfolgreich in der Nische bestehen. Sie profitieren davon, dass die Distanz und Unpersönlichkeit aus den Anfangszeiten des Internets im Zuge von Messenger- und Trackingdiensten immer mehr schwindet.

Diethelm Siebuhr ist CEO der Nexinto Holding.