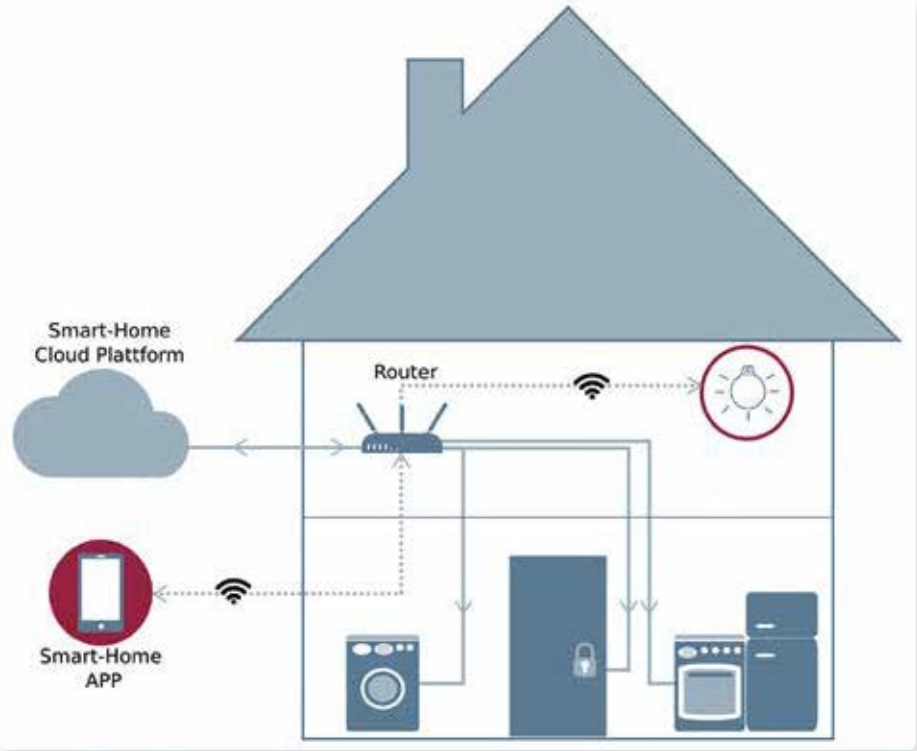
Internet of Things (IoT)

Herausforderung für die IT-Sicherheit

Das Internet of Things (IoT) gehört gegenwärtig zu den wohl meistdiskutierten und vielversprechendsten Technologien. Immer mehr Unternehmen aus unterschiedlichsten Branchen gehen dazu über, ihre Produkte internetfähig zu machen, um neue Dienste und Funktionen anbieten zu können. Auf diesem Wege werden immer mehr Bereiche des täglichen Lebens vernetzt. So soll, Erwartungen entsprechend, die Anzahl der weltweit vernetzten Objekte im IoT bis 2020 auf 20 Milliarden ansteigen.[1] Andere Prognosen gehen von bis zu 50 Milliarden Objekten aus. Ob das IoT die großen Erwartungen wirklich erfüllen kann, hängt nicht zuletzt von einem adäquaten Sicherheitslevel für alle Objekte, Dienste, Prozesse sowie Soft- und Hardware ab. Es stellen sich die Fragen, welche Sicherheitsanforderungen kommen im IoT auf uns zu und wie ist es aktuell um die Sicherheit des IoT bestellt?

Ständige Verfügbarkeit, Kommunikation unter vernetzten Objekten und Datenverarbeitung in Echtzeit sind Eigenschaften, die das IoT ausmachen. Die IoT-Technologie hat das Potenzial, viele Lebensbereiche positiv zu beeinflussen. Die Risiken und Probleme dieser IoT-Technologien sind zurzeit aber eine sehr große Herausforderung. Es entstehen neue Anforderungen an die vorhandene Infrastruktur des Internets und deren Sicherheit. Zusätzlich entstehen neue Gefahren für die Objekte selbst, da sie potenziell physischer Gefahr ausgesetzt werden können. Sensoren und Aktoren können in Umgebungen zum Einsatz kommen, in denen sie



Smart-Home

Opfer von Vandalismus und unbefugten Zugriffen werden. Folglich ist es für die Hersteller notwendig, die Objekte physisch robust und sicher zu gestalten.

Ein Großteil des Datenaufkommens im Internet wird heutzutage durch Nutzerinteraktionen generiert. Doch was passiert, wenn immer mehr Objekte mit dem Internet vernetzt werden und anfangen, untereinander autonom zu kommunizieren? Die Anzahl der intelligenten IoT-Geräte nimmt Jahr für Jahr stark zu. Die Herausforderung besteht nicht nur darin, den steigenden Datenverkehr und die große Menge an IoT-Geräte in einem effizienten und sicheren Objekt- und Identitätsmanagement zu bewältigen, sondern auch die Kommunikation und die IoT-Geräte selbst sicher zu gestalten. Mit dem IoT entstehen neue Möglichkeiten zur Datenaggregation. Das stellt Datenschützer vor die neuen Herausforderungen, die Privatsphäre der Nutzer zu schützen. Sensoren und Aktoren, die variabel angebracht werden können und ubiquitär Daten sammeln, erfassen eine Vielzahl an Informationen über die Nutzer und deren Umfeld. Darunter sind auch hochsensible Daten. Diese sensiblen Daten sollten nur für Berechtigte zugänglich sein. Die Aggregation von Daten geschieht für die Nutzer in der Regel unbemerkt, sodass diese sich nicht bewusst sind, welche sensiblen Daten wann und wo gesammelt werden.

Was verrät meine Waage wem?

Bereits heute führt der Einsatz von IoT-Technologie dazu, dass immer mehr sensible Daten aus den unterschiedlichsten Anwendungsbereichen generiert werden. Der Haushalts- oder Gesundheits-/Fitnessbereich sind Branchen, in denen die gesammelten Informationen einen hohen Persönlichkeitswert genießen. Im Umfeld eines Smart-Home-Systems werden sehr viele Daten wie Temperatur, Wasser- und Stromverbrauch etc. von einer Vielzahl an Sensoren generiert und erfasst. Mithilfe solcher Daten könnten Angreifer ganze Bewegungs- und Verhaltensprofile von Menschen erstellen, aus denen sich zum Beispiel ableiten lässt, wann die Bewohner das Haus verlassen oder im Urlaub sind. Gleichzeitig lassen sich viele Komponenten fernsteuern und können durch ihre Verbindung zum Internet angegriffen werden.

Im Fitnessbereich bieten sich ebenfalls große Einsatzmöglichkeiten für das IoT. So sammeln und analysieren zum Beispiel intelligente Körperwaagen oder Fitnessarmbänder, die häufig über eine App steuerbar sind, Daten der Nutzer. Mit diesen IoT-Geräten lassen sich Messwerte wie Körpergewicht, Herzfrequenz und der prozentuale Anteil des Fettgewebes messen. Die sensiblen Daten werden in der Regel in der Cloud der Hersteller gespeichert und zum Beispiel mithilfe von Algorithmen der Künstlichen Intelligenz verarbeitet. Das heißt, der Kunde gibt seine sensiblen Daten aus der eigenen Obhut und muss dem Unternehmen vertrauen, dass die sensiblen Daten in den IoT-Geräten, in der Cloud und bei der Übertragung dazwischen angemessen geschützt werden.

Die Erfahrung zeigt jedoch, dass einige Hersteller dieser Verantwortung zurzeit nicht gerecht werden und häufig auf die Imple-

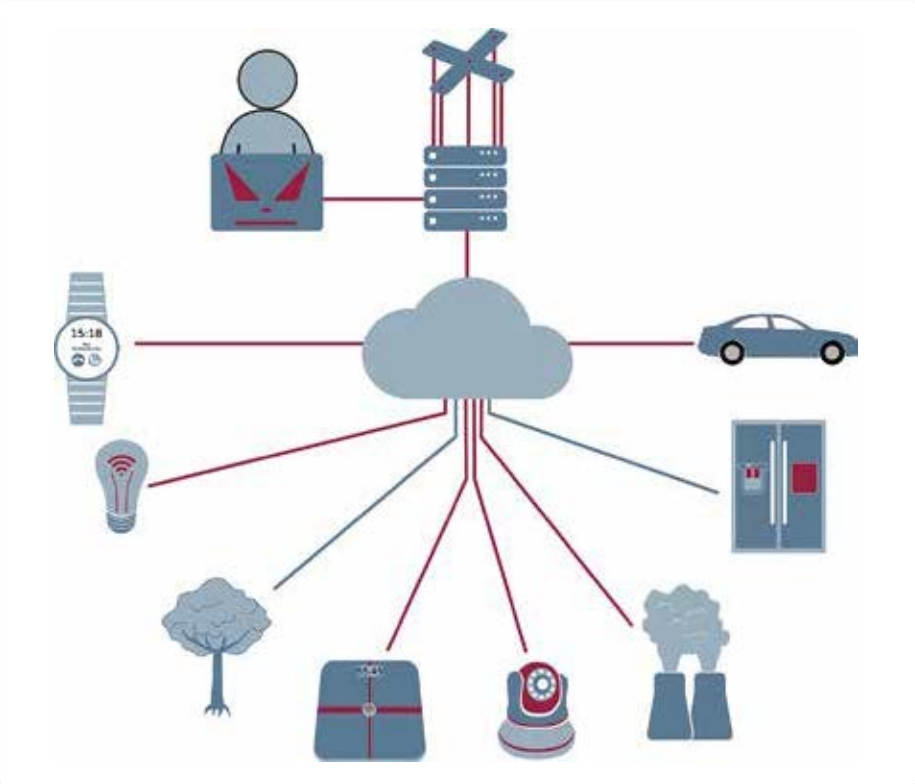
mentierung von Sicherheitsfeatures verzichten. So gab es Fälle, in denen die gesamte Kommunikation im Klartext übertragen wurde.[2] Aufgrund dieser unverschlüsselten Übertragung ist es für Hacker/Kriminelle ein Leichtes, Informationen abzufangen. IoT findet auch im medizinischen Bereich und im Gesundheitswesen großes Anwendungspotenzial. Hier werden sensible Daten der Patienten digital erfasst und online verfügbar gemacht. Vitalparameter oder die Krankenhistorie eines Menschen sind hochsensible Daten, die nicht in die Hände Dritter gehören.

Durch die industrielle Nutzung des IoT – in Deutschland prägte unter anderem die Bundesregierung den Begriff Industrie 4.0 – entstehen digitale Wertschöpfungsnetzwerke. Entlang der Wertschöpfungsketten, die Zulieferer, Hersteller, Logistik bis hin zu den Händlern umfassen, werden ebenfalls große Mengen Daten generiert und ausgetauscht. Dies erzeugt neue Angriffsvektoren, die Angreifer nutzen können, um Zugang zu unternehmenskritischen Daten, etwa Forschungs- und Fabrikationsdaten, zu bekommen. Die Folge eines solchen Datendiebstahls kann von einem Imageschaden, aus dem finanzielle Schäden oder der Verlust von Kundenvertrauen resultieren können, bis zu einer Beeinträchtigung der Wettbewerbsfähigkeit durch den Verlust von Wissensvorsprung reichen.

Die Gefahr und Durchschlagskraft von IoT-Botnetzen!

Botnetze sind schon länger als Bedrohung bekannt. IoT-Botnetze stellen eine neue Stufe der Gefahr für die Infrastruktur des Internets dar. Im Unterschied zu konventionellen Botnetzen bestehen IoT-Botnetze hauptsächlich aus kompromittierten IoT-Geräten. Diese haben die Eigenschaft, dauerhaft und mit guter Bandbreite online verfügbar zu sein. Dadurch stehen sie, einmal unter der Kontrolle eines Angreifers, immer für einen Angriff bereit. Welches Gefahrenpotenzial die schiere Masse an ungesicherten IoT-Geräten mit sich bringt, zeigten die massiven DDoS-Angriffe im September 2016 auf den Blog des Journalisten und Sicherheitsforscher Brian Krebs[3] und auf die Server des französischen Hosters OVH[4].

Das Botnetz Mirai, das für die Angriffe verantwortlich war, bestand angeblich aus mehr als einer Million[5] kompromittierter IoT-Geräte. Brian Krebs[7] Blog stand bis dahin unter dem Schutz von CDN-Betreiber Akamai und durfte dessen Anti-DDoS-Dienst kostenfrei nutzen. Die DDoS-Angriffe waren so stark, dass sich Akamai dazu gezwungen sah, den Blog vom Netz zu nehmen.[6] Die Intensität der DDoS-Angriffe erreichte eine bis dahin nicht dagewesene Dimension, mit einem durch die Anfragen erzeugten Traffic von 665 Gigabit[7] bis zu 1,5 Terabit pro Sekunde.[3] Die Menge der kompromittierten IoT-Geräte bestand hauptsächlich aus ungesicherten, mit dem Internet verbundenen Sicherheitskameras, digitalen Videorekordern und Haushaltsgeräten.



IoT-Botnetz

Anfang Oktober wurde der Quellcode von Mirai veröffentlicht. Die Analyse des Quellcodes zeigte deutlich, mit welch simpler, auf menschlicher Schwäche basierender Strategie die Malware agierte. Sie durchsuchte das Internet nach IoT-Geräten, testete, ob diese noch auf das Default-Passwort des Herstellers konfiguriert waren, und brachte sie dann unter ihre Kontrolle. Gegenüber den üblichen Methoden wie „Social Engineering" oder „E-Mail-Poisoning" ermöglichte diese Herangehensweise eine enorme Senkung des Aufwands. Stattdessen können die meist schlecht gesicherten IoT-Geräte über die Ports 22 (SSH) oder 23 (Telnet) direkt angegriffen werden. Die ständige Verfügbarkeit der IoT-Geräte macht sie zu sehr attraktiven Bots. Basierend auf dem offenen Quellcode von Mirai entstanden viele Ableger des Botnetzes.

Lahmgelegte Internetriesen

Am 21. Oktober 2016 wurde erneut ein schwerer DDoS-Angriff bekannt. Das Opfer war diesmal die Infrastruktur des Internetdienstleister DynDNS.[8] Der Angriff lief in Angriffswellen ab, an denen mehrere Botnetze

beteiligt waren. Die Folge war, dass viele große Internetdienste wie Twitter, Paypal, Spotify, Netflix und Amazon stundenlang nicht zu erreichen waren. Der strategisch gut platzierte Angriff auf DynDNS zeigt nicht nur die Gefahr durch IoT-Botnetze, sondern auch deutliche Schwächen großer Internetdienstleister, welche sich ausschließlich auf einen DNS-Anbieter verlassen. Der Schaden dürfte für die Internetdienste, die offline waren, nicht unerheblich gewesen sein. Über die Urheber des Angriffs wird viel spekuliert. Erste Vermutungen waren Hackergruppen oder gar Geheimdienste, die Quelle könnte aber auch ganz woanders liegen. So soll ein Gamer, mit persönlichem Groll gegen das Sony Playstation Network, Urheber des Angriffs gewesen sein. Das eigentliche Ziel war demnach das Playstation Network. Ein eigenes Botnetz ist dafür nicht nötig. Das Geschäftsmodell „Botnet-as-a-Service" hat sich im Darknet längst etabliert.[9]

Die Meldungen über Angriffe von IoT-Botnetzen halten weiterhin an. Am 27. November 2016 verärgerte eine Großstörung des Telekomnetzes zahlreiche Telekom-Kunden, da diese zeitweise nicht auf Internet-Dienste zugreifen konnten. Dabei soll eine Variante des Mirai-Botnetzes gezielt Speedport-Router der Telekom angegriffen und versucht haben, diese mit Malware zu infizieren, um sie in ein Botnetz zu integrieren. Die Angreifer hatten versucht, über den Port 7547 auf die Geräte zuzugreifen. Dieser ist Teil des Fernwartungsprotokolls TR-069, welches wiederum das Protokoll TR-064 verwendet. Das Protokoll TR-064 wird für die LAN-Side CPE Configuration verwendet. Mit dieser Schnittstelle lassen sich internetfähige Geräte aus dem lokalen Netzwerk konfigurieren. Dabei sollte das Protokoll nur aus dem lokalen Netzwerk verfügbar sein.

Hacker konnten, ohne sich vorher einer erfolgreichen Authentifizierung unterziehen zu müssen, auf Geräte zugreifen. Diese Sicherheitslücke war offenbar schon vorher bekannt.[10] Der Malware gelang es zwar nicht, die Kontrolle über die Router übernehmen, sie legte mit dieser Attacke aber ca. 900.000 Router lahm.[11] Die Störung des Telekom-Netzes war nicht beabsichtigt und ist deshalb als „Kollateralschaden" zu klassifizieren. Als Reaktion sperrte die Telekom den Internet-Verkehr für Port 7547 und verteilte später ein Software-Update an die Router. Bei einer erfolgreichen Attacke hätten Besitzer der befallenen Router keine spürbaren Auswirkungen wahrnehmen können. Es war Glück im Unglück, dass die Router stattdessen ausfielen. Welch enormen Schaden die kompromittierten 900.000 Router hätten anrichten können, kann nur spekuliert werden.

Es gibt keine einheitliche Plattform für das Internet of Things

Der Begriff „Internet of Things" suggeriert ein Internet-ähnliches Konstrukt, in das netzwerkfähige Geräte eingebunden werden, untereinander kommunizieren und von jedem Ort, zu jeder Zeit erreichbar sind. Grenzenlos sind die Kommunikationsmöglichkeiten im IoT aber nicht. Tatsächlich ist das IoT heutzutage eher ein Netzwerk von Plattformen, auf denen IoT-Geräte, die denselben Standard nutzen, kommunizieren können. Gewachsen aus dem Druck, schnell Lösungen für das IoT anbieten zu können, haben viele Hersteller IoT-Plattformen entwickelt, die ausschließlich Unterstützung für die eigenen Geräte bieten.

Diese Entstehung von IoT-Insellösungen widerstrebt nicht nur dem Gedanken von einem Netzwerk aus IoT-Geräten, sie hat auch direkte Auswirkungen auf die Verfügbarkeit von Diensten und Systemen und damit auf die Nutzer. Weiterhin existiert auch eine gewisse Update-Problematik. Nicht jedes IoT-Gerät verfügt über einen automatischen Update-Service und kann folglich nicht auf entdeckte Sicherheitslücken in der Firmware reagieren. Die IoT-Geräte bleiben ungesichert und bieten ein ständiges Ziel für Hacker. Stellt ein Hersteller die Unterstützung einer IoT-Plattform ein, sind die Geräte de facto unbrauchbar. So zum Beispiel geschehen mit einem Hausautomatisierungs-Hub, der für die Ansteuerung von Smart Home Devices via Smartphone-App zuständig war. Nachdem die betreibende Firma die Server vom Netz genommen hatte, konnten die Nutzer nicht mehr auf ihren Hub und damit auf die Steuerung ihres Hauses zugreifen.[12]

Durch die Diversifikation der IoT-Plattformen ist eine unübersichtliche Sicherheitslage entstanden. Das Sicherheitslevel variiert

von Plattform zu Plattform und von Gerät zu Gerät, abhängig von eingesetzten Protokollen und Sicherheitsmechanismen. Nutzer, die Wert auf IT-Sicherheit legen, dürften es schwer haben, den Überblick zu behalten, welche IoT-Produkte sicher eingesetzt werden können. Unübersichtlich kann sich auch das IoT-Gerätemanagement gestalten, wenn unterschiedliche IoT-Plattformen innerhalb einer IT-Umgebung zum Einsatz kommen. Das IoT-Gerätemanagement ist für gewöhnlich innerhalb einer IoT-Plattform implementiert. Ein zentrales, plattformübergreifendes Rechte- und Zugriffsmanagement ist dadurch nicht einfach realisierbar.

Unterschiedliche Anwendungsprotokolle für das Internet of Things

Die Vielzahl unterschiedlicher IoT-Plattformen spiegelt sich in der Anzahl der möglichen Protokolle wider. Die Plattformen verwenden auf Anwendungsebene Protokolle wie MQTT, CoAP, HTTPS oder Lemonbeat, um Informationen auszutauschen. Für die Verarbeitung hingegen wird überwiegend mit TCP oder UDP gearbeitet. Das ermöglicht den Einsatz von Sicherheitsprotokollen wie TSL/DTLS oder IPSec, um die Kommunikation zu verschlüsseln. Der Einsatz dieser bewährten Sicherheitsprotokolle ist notwendig, da die auf Leichtgewichtigkeit ausgelegten IoT-Protokolle kaum ausreichende Sicherheitsmechanismen mitbringen. Eine Analyse dieser Zusammenarbeit von IoT- und Sicherheitsprotokollen zeigte jedoch Schwachstellen. Einige Sicherheitsanforderungen, etwa eine Ende-zu-Ende-Verschlüsselung der Knoten, wurden nicht erfüllt. Außerdem ist die Benutzbarkeit der Sicherheitsprotokolle in Verbindung mit ressourcenbeschränkten oder mobilen Geräten nicht ohne weiteres umzusetzen.[6] Ein normales Endgerät (Desktop, Notebook, …) kann starke kryptographische Verfahren ohne Performanceverluste umsetzen. Für ressourcenbeschränkte Geräte ist die Berechnung dieser Verfahren eine Herausforderung.

Verpflichtung der Hersteller

IT Security by Design ist ein Entwicklungsparadigma, welches für die Sicherheit im IoT von großer Bedeutung ist. Die Umsetzung dieses Designgrundsatzes ist für Hersteller, durch den Mehraufwand, mit zusätzlichen Kosten verbunden. Bei der Betrachtung der bereits erwähnten Angriffe konnte der Großteil der IoT-Geräte jedoch nur kompromittiert werden, da die zu überwindenden Hürden für Angreifer zu gering waren. Viele Hersteller scheinen das Entwicklungsparadigma noch nicht zu berücksichtigen. Die Aufforderung, ein Standardpasswort ändern zu müssen, hätte die großflächige Übernahme zahlreicher Geräte bereits verhindert. Hersteller stehen deshalb in der Verantwortung, Sicherheitsmaßnahmen von Werk aus zu implementieren. Im Gegensatz zu Desktopsystemen und Notebooks ist es Nutzern oft nicht möglich, einen zuverlässigen Schutz nachträglich zu implementieren.

Hersteller von IoT-Geräten sollten neue und sichere IT-Architekturen, wie Sicherheitskerne, mit Isolierungs- und Separierungstechnologien sowie kryptographische Funktionen, wie vom TPM, verwenden. Damit können die meisten Sicherheitsprobleme einfach und nachhaltig eliminiert werden. Die Anforderungen an Herstellerhaftung, Zertifizierung und Absicherung von Rest-Risiken können mithilfe dieser Technologien einfach erfüllt werden.

Standardisierungsbedarf bei IT-Sicherheit und dem Internet of Things!

Damit die Hersteller wissen, welche IT-Sicherheitsmaßnahmen sie in ihren Design- und Entwicklungsprozessen berücksichtigen müssen, bedarf es Standards, deren Umsetzung ausreichend Schutz bietet. Diese IT-Sicherheitsmaßnahmen müssen für die breite Masse der IoT-Geräte, trotz extremer Diversifikation hinsichtlich technischer Komponenten, der Kommunikationswege, Aufstellungsorte und Einsatzbereiche, interoperabel sein. Das Problem mit den Standards im IoT ist auch hier die Vielzahl an unterschiedlichen Lösungsansätzen. Es gibt eine Menge Konsortien, Unternehmen und Initiativen, die an Lösungen arbeiten. Leider geschehen diese Bemühungen aber parallel nebeneinander her, sodass in näherer Zukunft nicht mit einheitlichen Lösungen gerechnet werden kann. Welche Standards sich letzten Endes durchsetzen werden, wird in erster Linie von den großen Herstellern sowie der Industrie beeinflusst. Sind deren Lösungen auf dem Markt und beim Verbraucher im Einsatz, werden neue, eventuell sicherere Standards nicht mehr berücksichtigt, solange es keine rechtlichen Rahmenbedingungen gibt. Aus diesem Grund sollten die Unternehmen aus Deutschland und Europa bemüht sein, einen gemeinsamen Standard zu definieren und umzusetzen.

Fazit/Empfehlung

Die Vorkommnisse der letzten Monate haben gezeigt, wie anfällig das Internet of Things ist. Die erschreckende Leichtigkeit von Angriffen aus dem IoT – in Kombination mit der Schlagkraft von IoT-Botnetzen – ist ein deutliches Zeichen, dass es schlecht um die aktuelle Sicherheitslage des IoT bestellt ist und der Handlungsbedarf groß ist. Besonders besorgniserregend ist dabei die Tatsache, dass nicht die implementierten Sicherheitsvorkehrungen überwunden wurden, sondern kaum bis gar keine Sicherheitsmaßnahmen existierten. Aus diesem Grund war und ist es möglich, größere Internet-Dienste mithilfe von IoT-Botnetzen anzugreifen und für einen spürbar anhaltenden Zeitraum unerreichbar zu machen. Treffen die Prognosen ein, dann werden bis 2020 bereits 20 Milliarden IoT-Objekte mit dem Internet verbunden sein. Es kann nur erahnt werden, welches Gefahrenpotenzial hinter dem IoT steckt, wenn den aktuellen IT-Sicherheitsproblemen nicht mehr Aufmerksamkeit geschenkt wird. Dabei stehen besonders die Hersteller und Entwickler in der Verantwortung. Die schnelle Produktion von IoT-Geräten, um sich Marktanteile im hart umkämpften Markt zu sichern, geht zu Lasten der Sicherheit. Wenn der Trend anhält, müssen Gesetze, Normen und Richtlinien der EU als regulierende Instanz in Kraft treten.

Den Nutzern selbst bleibt indes nur übrig, sich auf die IT-Sicherheitsmaßnahmen der Hersteller zu verlassen. Einem Standard-Nutzer von IoT-Geräten ist nicht zuzumu-

ten, seine Firewall im Zugangsrouter, zum Beispiel DSL-Router, so zu konfigurieren, dass die Anfragen auf möglicherweise gefährlichen Ports an die IoT-Geräte geblockt werden. Die Vergabe von sicheren Passwörtern, nach Inbetriebnahme der IoT-Geräte, sollte standardmäßig gefordert werden. Werden die vorgestellten Herausforderungen nicht gelöst, stellt das Internet der Dinge den Nährboden für die größte Bedrohung im und für das Internet dar.

Gelingt es hingegen Herstellern und Nutzern, die Hürden zu erhöhen, dann stellt das Internet of Things den nächsten Schritt der Vernetzung dar. Diese birgt neben den bekannten Risiken auch zahlreiche Chancen. Werden die Anforderungen an Sicherheit und Datenschutz erfüllt, so können die Sensoren und Aktuatoren zum Beispiel den Menschen bei zahlreichen Aufgaben unterstützen, Leben retten und dabei helfen, Unfälle zu vermeiden. ■

JOHNNY HOANG
ist wissenschaftliche Hilfskraft am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen im Forschungsbereich Internet-of-Things.

OLE JÖTTEN
ist wissenschaftliche Hilfskraft am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen im Forschungsbereich Internet-of-Things.

PROF. DR. NORBERT POHLMANN
ist Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.

CHRIS WOJZECHOWSKI
ist wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen und leitet den Forschungsbereich Internet-of-Things.

Literatur:

1 *STAMFORD, „Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015," 2015. [Online]. Available: https://www.gartner.com/newsroom/id/3165317. [Accessed: 14-Dec-2016].*

2 *V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, „Network-level security and privacy control for smart-home IoT devices," 2015 IEEE 11th Int. Conf. Wirel. Mob. Comput. Netw. Commun. WiMob 2015, pp. 163–167, 2015.*

3 *F. A. Scherschel, „Massiver DDoS-Angriff auf Secruity-Journalist Brian Krebs," heise.de, 2016. [Online]. Available: https://www.heise.de/security/meldung/Security-Journalist-Brian-Krebs-war-Ziel-eines-massiven-DDoS-Angriffs-3329988.html. [Accessed: 05-Oct-2016].*

4 *D. Schirrmacher, „Rekord-DDoS-Attacke mit 1,1 Terabit pro Sekunde gesichtet," heise.de, 2016. [Online]. Available: http://www.heise.de/newsticker/meldung/Rekord-DDoS-Attacke-mit-1-1-Terabit-pro-Sekunde-gesichtet-3336494.html. [Accessed: 05-Oct-2016].*

5 *F. A. Scherschel, „Project Shield: Google rettet Blogger Krebs vor DDoS per IoT-Botnetz," heise.de, 2016. [Online]. Available: https://www.heise.de/security/meldung/Google-Schutzschild-rettet-Blogger-Krebs-vor-DDoS-per-IoT-Botnetz-3333054.html. [Accessed: 05-Oct-2016].*

6 *F. A. Scherschel, „Akamai kapituliert vor DDoS-Angriff auf Security-Blogger," heise.de, 2016. [Online]. Available: https://www.heise.de/security/meldung/Akamai-kapituliert-vor-DDoS-Angriff-auf-Security-Blogger-3330281.html. [Accessed: 05-Oct-2016].*

7 *F. Greis, „Nach DDoS-Attacken: Akamai nimmt Sicherheitsforscher Krebs vom Netz – Golem.de," 2016. [Online]. Available: http://www.golem.de/news/nach-ddos-attacken-akamai-nimmt-sicherheitsforscher-krebs-vom-netz-1609-123419.html. [Accessed: 16-Nov-2016].*

8 *H. Gierow, „Amazon, Spotify, Twitter, Netflix: Mirai-Botnetz legte zahlreiche Webdienste lahm – Golem.de," golem.de, 2016. [Online]. Available: http://www.golem.de/news/ddos-massiver-angriff-auf-dyndns-beeintraechtigt-github-und-amazon-1610-123966.html. [Accessed: 27-Oct-2016].*

9 *J. Schuster, „Frustrierter PlayStation-Spieler legte Teile des Internets lahm," heise Security, 2016. [Online]. Available: https://www.heise.de/security/meldung/Frustrierter-PlayStation-Spieler-legte-Teile-des-Internets-lahm-3492276.html. [Accessed: 22-Nov-2016].*

10 *F. A. Scherschel, „Großstörung deutsche Telekom: Angreifer nutzten Lücke und Botnetz-Code," heise Security, 2016. [Online]. Available: https://www.heise.de/newsticker/meldung/Grossstoerung-bei-der-Telekom-Angreifer-nutzten-Luecke-und-Botnetz-Code-3507088.html. [Accessed: 01-Dec-2016].*

11 *F. A. Scherschel, „Telekom-Störung: BSI warnt vor weltweitem Hackerangriff auf DSL-Modems," heise Security, 2016. [Online]. Available: https://www.heise.de/security/meldung/Telekom-Stoerung-BSI-warnt-vor-weltweitem-Hackerangriff-auf-DSL-Modems-3506556.html. [Accessed: 01-Dec-2016].*

12 *A. Donath, „Revolv: Google macht Heimautomatisierung kaputt – Golem.de," 2016. [Online]. Available: http://www.golem.de/news/revolv-google-macht-heimautomatisierung-kaputt-1604-120128.html. [Accessed: 12-Sep-2016].*