www.think-ing.de

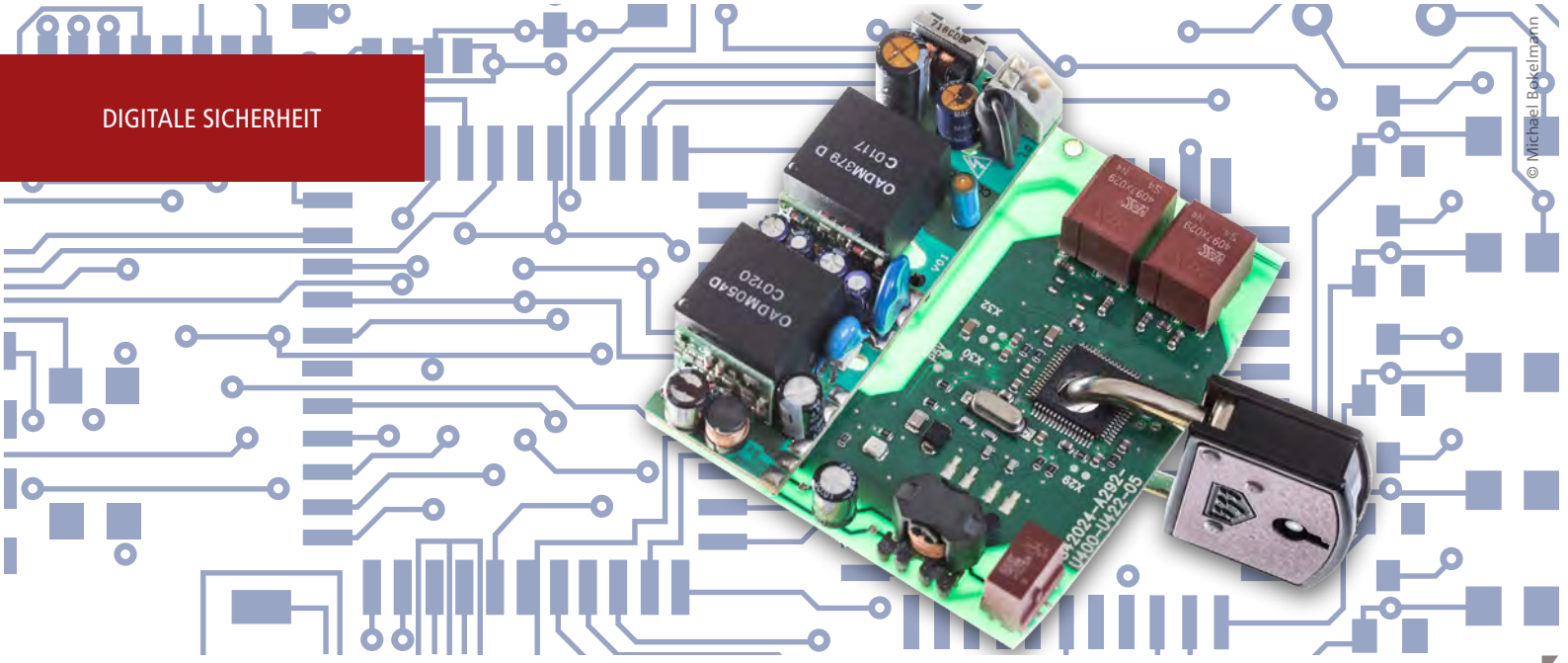
think ING.

kompakt

Neues aus der Welt der Ingenieure

03|2016

DIGITALE SICHERHEIT



INTRO

Digitales Wettrüsten

Beim BMI gibt es ein Nationales Cyberabwehrzentrum und bei der Bundeswehr ein Betriebszentrum für IT-Systeme. Befürchtungen um die Sicherheit sensibler Daten nehmen immer mehr zu. Schlagzeilen über Cyberangriffe, eine Attacke auf die IT des Bundestages und die globale Abhöraffäre der nationalen Sicherheitsbehörde der USA lassen uns alle als Nutzer von Onlineshopping, sozialen Netzwerken, Messengern oder Onlinebanking aufhorchen. Besonders sensibel reagieren Unternehmen, die ihre Geschäftsdaten vor Zugriffen schützen müssen. Das führt zu einem Wettrüsten der anonymen Angreifer mit IT-Sicherheitsingenieuren, die für unsere zunehmend vernetzte Infrastruktur und Wirtschaft unentbehrlich sind.

DATENSICHERHEIT

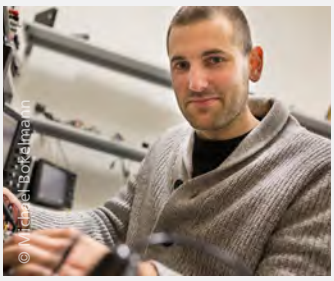
IT-Experten sind gefragt

Mittlerweile weiß beinahe jeder, dass das Internet ohne digitale Bodyguards eine No-Go-Area ist. Ohne diesen Schutz läuft man dort Gefahr, viel Geld, wichtige Daten, Freunde oder sogar seine Identität zu verlieren. Das Internet ist aber nach wie vor auch eine große Chance für die Wirtschaft, bei steigendem Sicherheitsaufwand.

Um die Gefahren für digitale Prozesse von Unternehmen besser einschätzen zu können, lockte der TÜV Süd potenzielle Nutzer mit einem nur virtuell existierenden Wasserkraftwerk an. IT-Experten stellten das angebliche Kraftwerk, das in einer deutschen Kleinstadt angesiedelt sein sollte, ins Internet und beobachteten acht Monate lang sämtliche Attacken auf diesen digitalen Köder. Geschützt war das virtuelle Wasserkraftwerk durch industrieübliche Schutzmaßnahmen. Die Ergebnisse zeigten deutlich, dass schon ein verhältnismäßig unbedeutendes kleines Kraftwerk viele Angreifer anlockt. Am Ende der Versuchszeit verzeichneten die Experten über 60.000 Zugriffe aus über 150 Ländern. Beinahe zeitgleich mit der Einstellung ins Netz schlug ein Angreifer zu, als hätte er bereits auf der Lauer gelegen. 2.995 Attacken kamen allein aus China, 2.318 aus den USA und 366 aus Deutschland, selbstverständlich mit verschleierter IP-Adresse.

Bedenkt man, dass Unternehmen zunehmend Maschinen und Produktionsstätten über das Internet vernetzen, liefert dieses

weiter auf S. 2



PORTRÄT

Die Schlüsselmacher

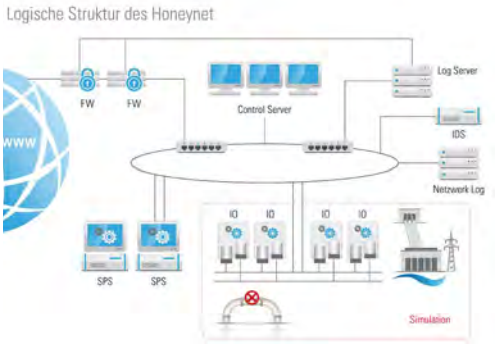
Beim Start-up PHYSEC entwickeln Forscher und Studenten Konzepte zur Verschlüsselung von Daten für das Internet der Dinge. Das Bundesministerium für Wirtschaft und Energie förderte die Gründungsidee mit 650.000 Euro. weiter auf S. 2–4

MOBIL UND DIGITAL

kompakt als App abonnieren

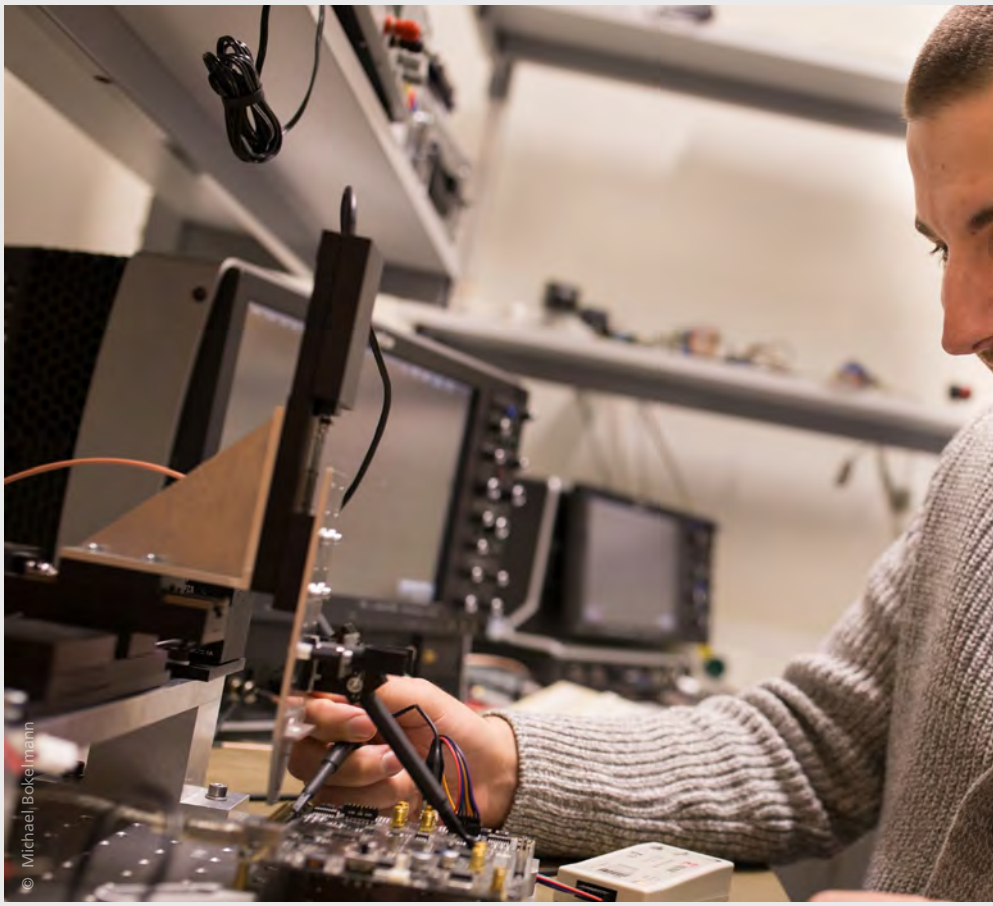
kompakt kann man sich auch mit vielen Zusatzinfos und Filmen als App fürs Tablet abonnieren. Einfach den QR-Code scannen oder unter s.think-ing.de/kompakt-digital dem Link zum entsprechenden Store folgen.

sogenannte Honeynet-Experiment ein klares Signal, mehr Aufwand und Ressourcen in IT-Sicherheit zu stecken.
Die Tricks im Netz werden immer raffinierter. So wurde unlängst der Cloud-Dienst Dropbox von einer perfiden Phishing-Attacke (Fischen nach Passwörtern) heimgesucht. Die Fake-Seite befand sich im echten Dropbox-Dienst. Über einen Link landete der Kunde auf einer täuschend echt aussehenden Dropbox-Seite und loggte sich mit E-Mail und Passwort ein. Kurz vor Weihnachten erlebten einige Smartphone-Nutzer mit Android-Betriebssystem eine böse Überraschung. WhatsApp forderte sie auf, ein Upgrade herunterzuladen, mit dessen Hilfe sie ihre Freunde beim Chatten beobachten können. Das ist zwar nicht die feine Art, die folgende Strafe war aber doch zu hart, das Handy begann sofort zu vibrieren und war danach unbrauchbar. Der Absender war offenbar doch nicht WhatsApp.



Honeynet-Struktur für ein virtuelles Wasserkraftwerk in der deutschen Provinz

Verursachen solche teuren Späße schon im Privatbereich große Schäden, so schlagen sie bei Unternehmen erst recht zu Buche (nach Untersuchungen des Ponemon-Instituts (USA) pro Attacke durchschnittlich 3,5 Millionen Dollar). Im Januar 2015 waren laut Softwarehersteller Symantec über ein Drittel aller Angriffe auf Unternehmen mit bis zu 250 Mitarbeitern gerichtet. Das heißt: Jedes Unternehmen ist im Visier und muss sich entsprechend wappnen. Vor diesem Hintergrund warten auf IT-Experten eine Menge Aufgaben. Einer aktuellen Umfrage des VDI zufolge wird die Nachfrage nach IT-Ingenieuren für Softwareentwicklung und IT-Sicherheit in den kommenden Jahren stetig steigen. Diese müssen dann beispielsweise auch die Frage klären, welche Clouddienste die entsprechende Sicherheit für die Auslagerung von sensiblen Unternehmensdaten gewährleisten können.



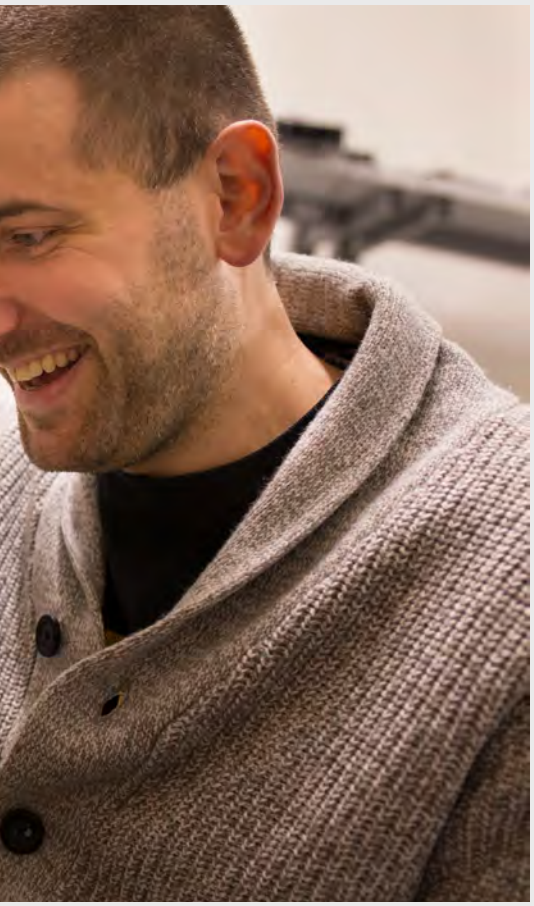
Mit Spaß bei der Sache: Benedikt Driessen, CTO des Start-ups PHYSEC, misst die elektromagnetische Abstrahlung eines Hardwarebausteins

DIE SCHLÜSSELMACHER

Das Start-up PHYSEC entwickelt Sicherheit für das Internet der Dinge

Der Mensch ist ein kommunikationsfähiges Tier. Das ist ein wesentlicher Teil seiner Erfolgsgeschichte. Und auch seine Maschinen werden zunehmend gesprächiger. Sie kommunizieren diskret und unhörbar über das vielzitierte Internet der Dinge. Im Produktionsprozess der sogenannten Industrie 4.0 tauschen sich Maschinen und Materialien permanent über den Stand der Produktion, ihren Bedarf und mögliche Störungen aus. So soll die Produktion schlanker, karbonarmer und effizienter werden und sich weit-

Auf vier ZigBee-Modulen, auf Basis von 8051 Prozessoren, wird die Software entwickelt und getestet



gehend selber regulieren. Auch Autos und Haushaltsgeräte in sogenannten Smart Homes sind zunehmend online und versenden Daten. Alles schön und gut. Aber ist das auch sicher?

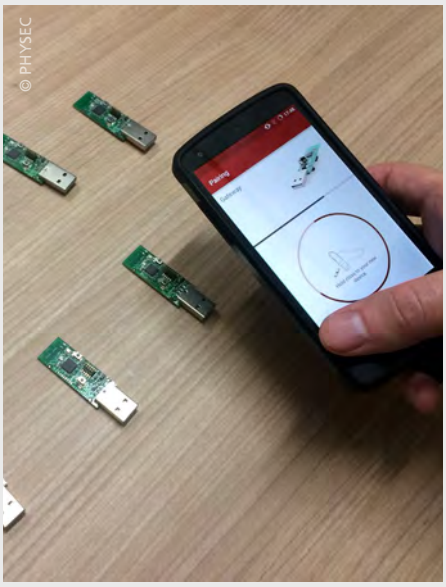
Darüber denken einige Forscher und Studenten des Horst Görtz Instituts für IT-Sicherheit an der Bochumer Ruhr-Universität intensiv nach. Sie entwickeln Konzepte zur Verschlüsselung dieser Daten, die möglichen digitalen Angreifern die rote Karte zeigen sollen. Offenbar mit Erfolg. Im Juni vergangenen Jahres wurde ihre Gründungsidee vom Bundesministerium für Wirtschaft und Energie im Rahmen des Programms EXIST Forschungstransfer mit rund 650.000 Euro gefördert. Das Start-up PHYSEC war geboren.

Fußwege

Der Fußweg zum frisch gebackenen Unternehmen führt durch neonbeleuchtete Gänge, die nach Putzmittel riechen, tief in den Bauch des architektonischen Walfisches Ruhr-Universität hinein. Hier sitzen die drei Jungunternehmer und ihre teilweise studentischen Mitarbeiter inmitten hoher Stapel von Kisten, Rechnern, Kabeln und allerlei elektronischen Geräten. Die Ruhr-Universität Bochum stellt als Partner des EXIST-Programms die Räume zur Verfügung und die Mitarbeiter von PHYSEC sind Angestellte der Hochschule. Im Rahmen des Unternehmensstarts mussten sich die drei Gründer Christian Zenger, Heiko Koepke und Benedikt Driessen auch mit zahlreichen geschäftlichen Fragen beschäftigen und beispielsweise die Geschäftsbedingungen im Detail mit der Hochschule aushandeln.

Kerngeschäft Schlüssel

Das Kerngeschäft von PHYSEC sind Schlüssel, nicht die analogen aus Metall, sondern immaterielle und digitale. Zur Verschlüsselung der Kommunikation unter Systemen gibt es unterschiedliche Ansätze, wie Benedikt Driessen erläutert. Weit verbreitet ist die Lösung, auf eine vertrauenswürdige Partei zu setzen, die vor jeder Kommunikation zweier Systeme entscheidet, ob die Adresse sauber ist, ob Schlüssel und Absender auch wirklich zusammenpassen. Dazu kann man auf einen Server in den USA zurückgreifen oder sich die erforderliche, aber sehr teure Hardware selbst beschaffen. PHYSEC bietet zu diesem Verfahren zwei Alternativen an: „Bei unserem System braucht man weder diese zentrale Instanz noch die teure Infrastruktur. Die Geräte verteilen die Schlüssel autonom und diversifizieren sie. Die Schlüssel können, wenn gewünscht, sehr oft wechseln. Wenn dann ein Schlüssel gehackt wird, hat dieser eine extrem kurze Lebensdauer." Es lohnt sich also nicht, den großen Aufwand zu betreiben.



Neue Geräte lassen sich sicher per Handy-App in das Netz der Dinge integrieren

Eine weitere Sicherheitslösung des jungen Start-ups hilft bei der Authentifikation von Geräten, die in ein mithilfe der digitalen Schlüssel gesichertes Netzwerk aufgenommen werden möchten. Dazu benötigt man ein Smartphone, eine App und das PHYSEC-ProPair Modul. Mann hält das Mobiltelefon einfach nah an das Gerät, um festzustellen, ob der Kommunikationspartner, der am Netz teilhaben möchte, auch der ist, für den er sich ausgibt. So können mögliche Angreifer sich nicht als legitime Kommunikationspartner einschleichen.

Raspberry PIs mit WLAN-Modulen für Entwicklungen und Tests

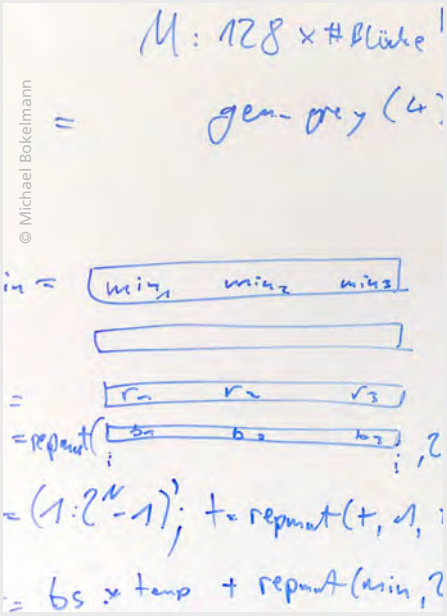
Mitdenken ist angesagt

Der Arbeitsalltag bei PHYSEC erfordert Im-

provisationsvermögen und Ausdauer. „Die Arbeitszeiten variieren sehr stark. Wer einen geregelten Arbeitsalltag erwartet, ist hier leider nicht richtig. Selbstmotivation und Teamwork sind gefragt. Da wir drei Gründer die Augen nicht überall haben können und wollen, muss jeder einzelne das Team kennen und mitdenken. Meist funktioniert das sehr gut und macht dann automatisch einen Riesenspaß."

Das Hacker-Mindset

Benedikt Driessen selbst studierte IT-Sicherheit in Bochum, arbeitete in einer Bochumer Sicherheitsfirma, promovierte über Sicherheitsanalysen von Satellitentelefonen und landete anschließend bei Infineon in München. Für seine Promotionsarbeit mussten Sicherheitssoftware analysiert und



Brainstormingergebnisse werden auch handschriftlich festgehalten

Verschlüsselungsalgorithmen geknackt werden. Nennt man das nicht Hacken? Muss man als guter IT-Sicherheitsmann ein Hacker sein? „Ich denke, das ist sicher von Vorteil. Bei der IT-Sicherheit braucht man dieses Mindset, sich zu fragen: Wie könnte ich dieses System jetzt angreifen?" Und wie hält man sich bei diesem Wettrüsten ständig auf dem Laufenden? „Die Dynamik bei der IT-Sicherheit kann so verdeutlicht werden: Die einen entwickeln beispielsweise einen neuen Verschlüsselungsalgorithmus und dann kommen die anderen und sagen, geht so nicht, da habt Ihr einen Fehler gemacht. Wir zeigen Euch mal, wie wir das kaputtmachen können. Dann wird umgedacht. Das ist ein kontinuierlicher Prozess und der Motor des Ganzen. Aus diesem Grund sind Systeme, die feste Schlüssel einsetzen, auch prinzipiell benachteiligt."

INTERVIEW

Schwieriger Umgang mit Spionen

Marco Ghiglieri, 32, ist Master of Science in Informatik, wissenschaftlicher Mitarbeiter an der TU Darmstadt und promoviert derzeit am dortigen Lehrstuhl Sicherheit in der Informationstechnik. Dieser gehört einem der größten europäischen Forschungszentren für IT-Sicherheit, Center for Research in Security and Privacy (CRISP), an.

Woran arbeiten Sie momentan?
Zurzeit bin ich an einer empirischen Forschungsarbeit beteiligt, in der wir 200 Menschen danach befragen, ob sie wissen, was bei der Installation und Nutzung eines Smart-TVs passiert.

Was passiert denn dabei?
Nun, als Smart-TV definieren wir zunächst mal einen Fernseher, der mit dem Internet verbunden werden kann. Das tun die meisten Nutzer auch, wenn sie das Gerät erstmalig anschließen und dazu aufgefordert werden, ihr WLAN-Passwort einzugeben. Dank dieser Internetverbindung empfängt und sendet der Fernseher fortan Daten, wie zum Beispiel Infos über empfangene Sendungen, Verweilzeiten etc. Man muss also damit rechnen, dass die Hersteller und Sender die auf diesem Weg übertragenen Daten analysieren. Oder anders ausgedrückt: Solange der Fernseher am Strom hängt, kann man nicht davon ausgehen, dass diese Informationen nicht weitergeleitet werden. Viel spannender ist aber, dass viele Fernseher heute Mikrofone zur Sprachsteuerung und manche sogar eine Kamera zum großformatigen Skypen besitzen. Und wo Daten reingehen, können auch Daten rausgehen. Es ist möglicherweise furchtbar spannend zu wissen, was die Zuschauer vor dem Fernseher eigentlich so tun.

Der Fernseher als Spion, ist das wirklich möglich oder pure Spekulation?
Das ist leider keine Spekulation. 2015 hat ein Forscher aus Berlin gezeigt, dass es absolut möglich ist, Personen vor ihrem Smart-TV zu filmen und die Bilder von einem x-beliebigen Standort aus anzusehen. Und schon ein Jahr zuvor konnten wir im Rahmen unserer Forschung belegen, dass beim Onlinebanking via Smart-TV alle Daten manipuliert werden konnten, weil ein Verschlüsselungsverfahren des Fernsehers nicht richtig funktionierte. Wenn die Software der Smart-TVs nicht immer auf dem neuesten Stand ist, können Sicherheitsprobleme auftreten, die man leicht ausnutzen kann. Das grundsätzliche Problem hierbei ist eben die Möglichkeit, in Privatsphäre und Datenschutz einzugreifen. Das andere Problem ist, dass viele Nutzer überhaupt nicht wissen, dass es derartige Gefahren gibt. Das zeigt auch meine Befragung.

Marco Ghiglieri

Wie gehen Sie mit diesen Problemen um?
Wir brauchen vor allem Aufklärung, was den Datenschutz und die Privatsphäre angeht. Im nächsten Schritt müssen wir dann ein System entwickeln, das Privathaushalte vor derartigen Sicherheitsproblemen schützt. Meine Vision ist ein Router, der nicht nur die übliche Verbindung zwischen Provider und Nutzer herstellt, sondern auch sortiert, welche Daten gesendet werden dürfen und welche nicht. Grundsätzlich ist das gar nichts Neues, allerdings sind die bisherigen Verfahren auf einem konsumentenunfreundlichen Niveau. Es ist schlichtweg zu kompliziert, sich hier einzuarbeiten. Gut für Hersteller und Sender: Sie wollen möglichst lange unentdeckt bleiben und werden nach immer neuen Lücken suchen und diese auch finden. Einen 100-prozentigen Schutz wird es daher für normale Benutzer auch zukünftig nicht geben.

Ist das nicht eine ziemlich resignierte Blickweise?
Eigentlich nicht. Ich sehe kein Problem, solange der Nutzer sein Risiko kennt. Wenn man Ski fährt oder auf die Straße geht, lebt man ja auch mit dem Risiko, sich zu verletzen. Jeder weiß das, passt auf und geht mit den Gefahren bewusst um. Dahin müssen wir auch in der digitalen Welt kommen. Nur wenn jeder die Schwachstellen und Gefahren im System kennt, ist er mündig, sich dafür oder dagegen zu entscheiden.

Im Kampf gegen Quantencomputerangriffe sind Forscher ihrer Zeit voraus. Noch gibt es diese Supercomputer nicht, trotzdem sind ihre Verschlüsselungen – zum Beispiel für die personenbezogenen Daten auf Gesundheitskarten – gerüstet für Angriffe in der Zukunft.

ANWENDUNGSBEISPIELE

Alles sicher! Oder nicht?

Sichere Nutzung von Clouds

Cloud-Dienste sind praktisch und werden immer beliebter. Dass deren Verschlüsselungstechniken zumindest undurchsichtig sind, stört die wenigsten Nutzer, obwohl die dort abgelegten Dateien durchaus angreifbar sind, oder der Betreiber umgekehrt die Daten in seinem Interesse auslesen kann.

Die Lösung für dieses Problem liefert die Open-Source-Anwendung PanBox, die Cloud-Dienste um eine spezielle Verschlüsselung ergänzt. Diese Software wurde von der Sirrix AG, einem Spezialisten in Kryptographie, Informationssicherheit und Trusted Computing und dem Fraunhofer-Institut für Sicherheit und Informationstechnologie entwickelt. Dabei haben die Entwickler ein dezentrales Schlüsselmanagement errichtet, wodurch die volle Kontrolle über die eigenen Daten ausschließlich bei den Nutzern von PanBox liegt. Private Anwender können die Software PanBox kostenfrei unter der Domain www.panbox.org herunterladen.

Die Anwendung PanBox erweitert die Cloud-Dienste um eine spezielle Verschlüsselung

Sicherheitslücken beim Log-in

Guido Schmitz, Daniel Fett und Ralf Küsters (von links) haben Sicherheitslücken im weitverbreiteten Log-in-System OAuth 2.0 offengelegt

Wer kennt diese Buttons nicht: „Mit Facebook anmelden“ oder „Google-Log-in verwenden“. Diese sogenannten Single Sign-Ons (SSO) ersparen ein neues Passwort und sind für User besonders bequem. Leider waren sie bislang aber auch besonders unsicher, fanden die Informatiker Guido Schmitz, Daniel Fett und Ralf Küsters der Universität Trier heraus. In dem für SSO am häufigsten verwendeten System OAuth 2.0 entdeckten sie gravierende Sicherheitslücken. Daraufhin war die Internet Engineering Task Force IETF (eine internationale Organisation zur technischen Weiterentwicklung des Internets) alarmiert, worauf sich die zuständige Arbeitsgruppe der Organisation unverzüglich traf. Dabei diskutierten Forscher mit den Entwicklern des Systems über das Problem und behoben es. „Und nun ist es wirklich sicher“, sagen die Trierer Wissenschaftler. Seit Jahren entwickeln sie Verfahren zur Sicherheitsanalyse von Internetanwendungen und lieferten schließlich neben dem Fund der Sicherheitslücken in OAuth 2.0 auch einen mathematischen Beweis, dass das Log-in-System nun wirklich sicher ist.

Schutz für morgen

Weltweit arbeiten Forscher an der Entwicklung von Quantencomputern, die heutige Computer in ihrer Rechenleistung um ein Vielfaches überbieten, um unter anderem auch schwierigste Verschlüsselungen mühelos knacken zu können. Doch dieser Intelligenz von morgen müssen bereits heutige Sicherheitsmechanismen standhalten, da viele aktuelle Kleinstgeräte wie elektrische Türschlösser oder auch Gesundheitskarten eine lange Lebensdauer haben. An der Ruhr-Universität Bochum entwickelte Prof. Dr.-Ing. Tim Güneysu (heute an der Universität Bremen) hierzu – im Rahmen des EU-Projekts Post-Quantum Cryptography – kryptografische Verfahren, die auch den

Im Alltag begegnen uns an vielen Stellen langzeitsichere Kryptoverfahren, zum Beispiel in elektronischen Schließsystemen.

Überrechenoperationen der Quantencomputer mühelos standhalten. Seine Grundidee setzt bei den Verschlüsselungen auf sehr lange Codes. Prinzipiell lassen sich diese mit den leistungsschwachen Prozessoren kleiner gegenwärtiger Geräte nur schlecht handhaben. Um diesem Problem zu begegnen, entwickelte Tim Güneysu Möglichkeiten, den Schlüssel zu verkleinern, ohne die Sicherheit zu gefährden.

Sicherheitsforschung

Welche persönlichen Daten hinterlasse ich im Internet, und wer kann sie sehen? Niemand weiß das so genau, und selbst den Profis ist es kaum möglich, die Wege ihrer Onlinedaten nachzuvollziehen, weiß auch Michael Backes, Professor für IT-Sicherheit und Kryptografie der Universität

Prof. Dr. Michael Backes ist IT-Sicherheitsforscher und untersucht, wie es um die Privatsphäre im Internet beschaffen ist

des Saarlandes. Er ist der Sprecher einer internationalen, von der Deutschen Forschungsgemeinschaft (DFG) geförderten Forschungsgruppe, die sich dem Thema Methoden und Instrumente zum Verständnis und zur Kontrolle von Datenschutz widmet. Tatsächlich geht es darum, wissenschaftliche Grundlagen auf diesem Gebiet zu schaffen. Daher wird die Forschergruppe in einem ersten Schritt zunächst analysieren, inwieweit private Daten abgegriffen und verwertet werden können. Die Wissenschaftler wollen beispielsweise herausfinden, ob Menschen an einer Handbewegung oder Ähnlichem in ihren Youtube-Videos identifiziert werden können oder welche Informationen sich aus Beziehungen in sozialen Netzwerken ableiten lassen. Darauf aufbauend sollen in einem zweiten Schritt Mechanismen entwickelt werden, die dem einzelnen Nutzer helfen, seine Daten zu schützen und selbst zu bestimmen, welche Informationen er preisgibt und welche nicht.

Awareness mit AVARE

Eine Forschergruppe unter Federführung des Karlsruher Instituts für Technologie (KIT) entwickelt bereits eine Anwendung zum Schutz persönlicher Daten. Das Programm mit dem Namen AVARE soll es Nutzern ermöglichen, ihre Datenschutzeinstellungen selbst zu definieren und global – sowohl in allen Anwendungen als auch auf allen Endgeräten – anzuwenden. Wenn Datenschutzrichtlinien einer Anwendung im Widerspruch zu den durch den Nutzer festgelegten Präferenzen stehen, weist das System seinen Nutzer darauf hin und stellt ihm drei Verfahrensmöglichkeiten zur Wahl: 1) Der Benutzer kann die betroffene Anwendung von seinen Datenschutzeinstellungen ausschließen. 2) AVARE kann den Zugriff auf bestimmte Daten definieren, zum Beispiel auf bestimmte Kontakte des Adressbuchs. 3) AVARE kann Ersatzdaten erzeugen und beispielsweise anstelle des wirklichen Standorts einen zufälligen Ort angeben.
Schließlich bleibt zum Schluss noch die Frage, wie es um die Sicherheit des Präferenzprofils steht, schließlich gehört es auch zu den persönlichen Daten. Die Antwort: alles sicher. Die Übermittlung erfolgt verschlüsselt und den Schlüssel kennt nur der Benutzer, der ihn auch selbst überträgt.

AVARE kapselt eine Anwendung und kontrolliert ihre Interaktion mit der Umwelt. Ein AVARE-Server verteilt die Einstellungen an alle Endgeräte.

Links FÜR STUDIERENDE

Wer in der IT-Sicherheit arbeiten möchte, findet an deutschen Hochschulen zahlreiche Studiengänge, die in Programmiersprachen, Kryptologie und diskreter Mathematik ausbilden.

Eingebettete Systeme
Bachelor und Master an der TU Kaiserslautern
s.think-ing.de/angewandte-info-kaisersl-bachelor
s.think-ing.de/angewandte-info-kaisersl-master

Cyber-Sicherheit
Bachelor an der Universität des Saarlandes
s.think-ing.de/cybersicherheit-saarland

IT-Sicherheit
Master am der TU Darmstadt
s.think-ing.de/it-sicherheit-darmstadt

Weitere Studiengänge unter: search-ing.de

IT-Sicherheit/Informationstechnik
Bachelor an der Ruhr-Universität Bochum
s.think-ing.de/it-sicherheit-bochum

Informatik
Bachelor und Master an der TU München
s.think-ing.de/informatik-tum-bachelor
s.think-ing.de/informatik-tum-master

IT-Systems Engineering
Bachelor am HPI (Hasso-Plattner-Institut) in Potsdam
s.think-ing.de/it-systems-hpi

OpenHPI bietet offene Onlinekurse zu IT-Sicherheit, an denen jeder übers Netz teilnehmen kann:
open.hpi.de/courses

think IND.
Die Initiative für Ingenieurnachwuchs

IMPRESSUM

Herausgeber: Gesamtmetall

Gesamtverband der Arbeitgeberverbände der Metall- und Elektro-Industrie e.V.
Voßstraße 16 - 10117 Berlin

Objektleitung: Wolfgang Gollub (verantw.)

Druck: color-offset-wälter GmbH & Co. KG, Dortmund

Redaktion und Gestaltung: concedra GmbH, Bochum

www.think-ing.de