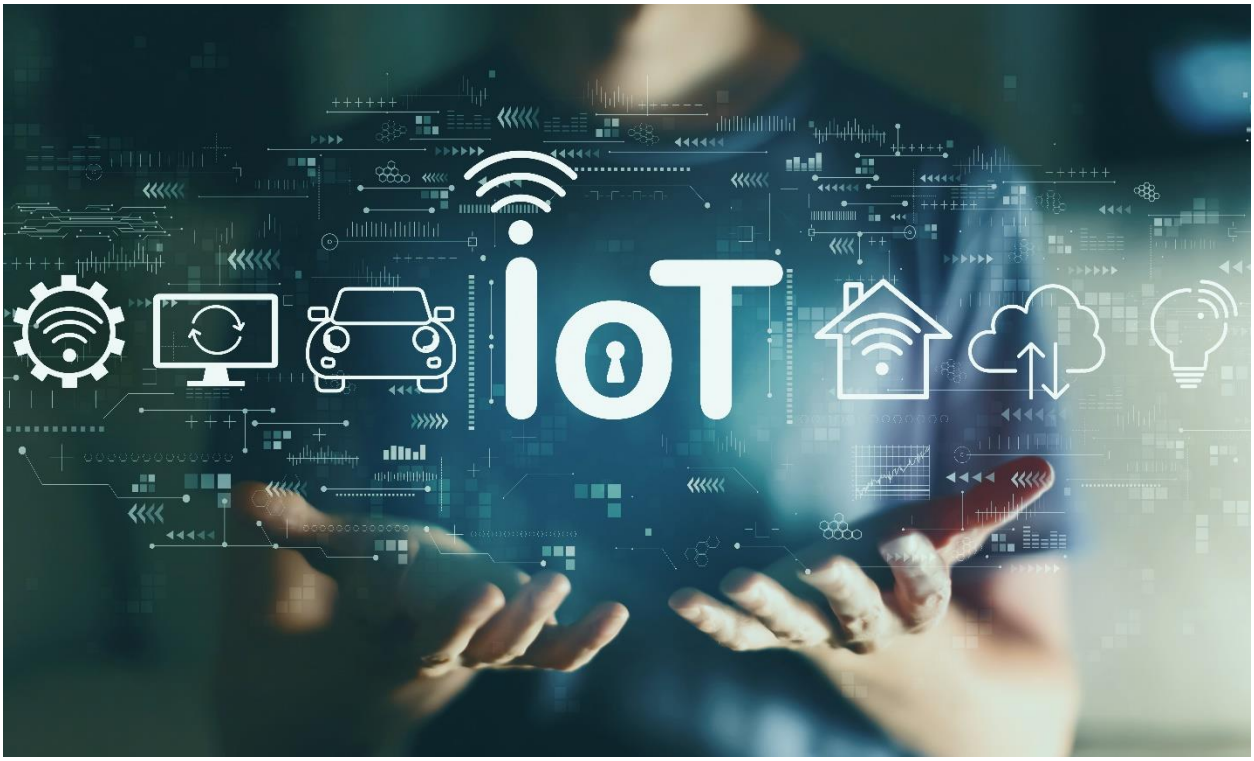
IoT Security-Spezialisten: Pioniere einer sicheren Industrie 4.0

Geschrieben von Joshua Bucheli, KI Ethik Forscher und Fellow beim ForHumanity Center, in Zusammenarbeit mit Tobias Schläpfer, Cryptography Engineer bei NatWest Services, und Peter Kosel, Gründer von cyberunity



2017 schockierte eine EU-US-Untersuchung Millionen von Eltern, als diese eine Schwachstelle in der Bluetooth-Schnittstelle einer deutschen Smart-Doll aufdeckte, die es Hackern ermöglichte, die mit ihr spielenden Kinder abzuhören und mit ihnen zu sprechen. So schrecklich sich das auch anhört, sind wahre Chuckies das geringste unserer Probleme, wenn das Internet of Things (IoT) nicht eher früher als später richtig abgesichert wird.

Das Internet steckte die Summe des menschlichen Wissens in die Tasche praktisch jedes Individuums auf dem Planeten, indem es Computer miteinander verband und Innovationen hervorbrachte, von denen Alan Turing nur träumen konnte. Das IoT wendet dieses Konzept auf den Rest unserer Umgebung an und stattet die Objekte, die uns umgeben, mit den Vernetzungsfähigkeiten aus, die unsere Welt schon einmal revolutioniert haben.

Für diejenigen, die sich wünschen, sie hätten in den frühen Tagen der Internetrevolution die Nase vorn gehabt, stellt das IoT eine zweite Chance dar... solange sie bereit sind, in die richtigen Leute zu investieren, die ihnen dabei helfen, die Art von Missgeschicken zu verhindern, die einen Reboot der Chucky-Franchise inspirieren könnten.

Wo steht das Thema IoT heute?

Das Internet verbindet Computer miteinander und ermöglicht es ihnen, Informationen aufzuzeichnen und auszutauschen. Das IoT verbindet so ziemlich alles andere mit dem Netz. Von smart-Uhren und Toiletten bis hin zu Ampeln und Atomkraftwerken - alles, was einen Ein/Aus-Schalter hat, ist leichte Beute.

Mit über 15 Milliarden neuen Geräten, die innerhalb des nächsten Jahrzehnts online gehen sollen, und Innovationen wie Quanten-Computer und Cloud-Computing, stellt das IoT eine der bedeutendsten Revolutionen der Technik dar. Doch mit den neuen Möglichkeiten kommen auch neue Risiken – in einer vollständig digitalisierten Welt wird so ziemlich alles um uns herum anfällig für digitale Bedrohungen.

«Der Unterschied zwischen IT- und IoT-Sicherheit beginnt damit, dass IoT-Geräte in viel grösserer Zahl existieren und viel offener zugänglich sind. Das IoT ist an die 'Dinge' selbst gebunden und nicht an gesicherte Orte wie Rechenzentren oder Serverräume. Das macht es viel schwieriger, sie zu sichern, zu verschlüsseln, zu patchen und zu aktualisieren», sagt Tobias Schläpfer, Cryptography Engineer bei NatWest Services.

In den Anfängen des IoT verbanden dedizierte Geräte, sogenannte ‘Gateways’, die ‘Dinge’ mit einer zentralen Cloud und ermöglichten deren Fernsteuerung auf Basis der von ihnen gesammelten und ausgetauschten Daten. Heute entwickelt sich das IoT weg von den geschlossenen Systemen, auf denen es ursprünglich eingeführt wurde, wodurch die Gateways nicht mehr gebraucht werden und die Security direkt vom IoT-Gerät selbst übernommen werden muss.

Wohin bewegt sich das Thema IoT?

«Wie die GDPR und Initiativen wie das ENISA Security-Label zeigen, erkennen sogar die Regulierungsbehörden, dass das IoT eine hohe Priorität in der Gesetzgebung einnehmen muss», sagt Tobias.

Angesichts von vielbeachteten Vorfällen wie dem Hack eines Casino-Aquariums in Las Vegas werden sich Firmen bewusst, dass sie etwas tun müssen. Dazu beginnen auch ihre Kunden zunehmend die Gefahren zu verstehen, die damit verbunden sind, dass jedes ‘Ding’ online gestellt wird. Sie stellen mehr Fragen, und es ist wichtig, dass Unternehmen mit Antworten bereitstehen.

‘Future-Proofing’ ist eine ganzheitliche Angelegenheit, die proaktiv und gemäss den Zero-Trust-Standards integriert werden muss, die die Cybersicherheit im Allgemeinen untermauern – etwas, das OEMs, die IoT-Geräte herstellen, noch nicht vollständig erkannt haben:

«Unternehmen müssen sich die Frage stellen, wie sie sicherstellen, dass die Geräte nicht nur smart, sondern auch *sicher* sind. Stattdessen führen sie das Thema Sicherheit oft erst in späteren Phasen des Design- und Produktionsprozesses ein», warnt Tobias.

Ein erheblicher 'pain-point', der bei der IoT-Sicherheit speziell beachtet werden muss, ist, dass diese Geräte in Bezug auf Rechenleistung, Speicherplatz und Akkulaufzeit weitaus begrenzter sind als Smartphones und Computer – Schlüsseleigenschaften, auf die sich robuste Cybersicherheitslösungen wie RSA-Schlüssel üblicherweise verlassen.

«Hier müssen Unternehmen anfangen, neue Lösungen zu erforschen. So sollten sie beispielsweise Token- oder Claim-basierte Authentifizierungslösungen in Betracht ziehen, die auf zeitabhängigen Berechtigungsnachweisen statt auf herkömmlichen PKI-Authentifizierung basieren», empfiehlt Tobias.

Glücklicherweise werden die Sicherheitsbedürfnisse des IoT in der Branche immer deutlicher, und Tools wie die OAuth Standardprotokolle ermöglichen vermehrt eine sichere und offene API-Autorisierung.

Für diejenigen, die sich für die Feinheiten der PKI-Authentifizierung, RSA-Schlüssel und das IoT interessieren, bietet das folgende Video einen sehr guten technischen Überblick.

IoT Security-Spezialisten: Gefragte Fähigkeiten und Ausbildungen

Beim IoT geht es darum, Geräte ('things') mit den Vernetzungsmöglichkeiten der digitalen Welt zu vereinen. Um es abzusichern, braucht es daher Personen, die eine Balance zwischen software- und hardwarebezogenen Fähigkeiten finden und die Überschneidungen zwischen beiden verstehen.

«An der Verbindungsstelle von Hardware und Software müssen sich IoT-Sicherheitsspezialisten bewusst sein, dass eher die Firmware als die Software im Fokus steht, und sie müssen im Hinterkopf behalten, dass die Absicherung des IoT sogar eine Frage der Entwicklung neuer Hardware sein kann», betont Tobias.

Das bedeutet zum einen, dass Personen gefragt sind, die sich mit den Grundlagen von Sicherheitsalgorithmen und -methoden, PKI-Authentifizierung, Access-Management und Netzwerktechnik auskennen. Es braucht Menschen, die den Unterschied zwischen RSA- und elliptischer Kryptografie sowie deren jeweiligen Einflüssen auf IoT-Systeme verstehen.

Andererseits profitieren starke IoT-Sicherheitsspezialisten auch von Erfahrungen in der Elektrotechnik und müssen die limitierten Ressourcen und Kommunikationsprotokolle, die diese Geräte einschränken, praktisch und innovativ umgehen können.

Dank der Interdisziplinarität der IoT-Sicherheit werden auch Quereinsteiger sehr gefragt sein. Elektroingenieure, Embedded-Systems Ingenieure, Netzwerksicherheitsingenieure und Kryptographie-Spezialisten mit einem Hang zur praktischen Arbeit und einem Interesse an Softwareentwicklung sind gut aufgestellt, um bei der Entwicklung sicherer Firmware für das IoT mitzuwirken.

Was die Qualifikationen angeht, «ist es wichtig zu bedenken, dass Arbeitserfahrung und nachgewiesenes praktisches Verständnis gegenüber Zertifikaten oder Diplomen bei weitem bevorzugt wird», sagt Tobias.

Der Nachweis einer akademischen Ausbildung wie das MAS-Programm des ZHAW Institute of Embedded Systems oder das Internet of Things MAS-Programm der Universität Genf verschafft den Bewerbern dennoch einen deutlichen Vorsprung. Auch Qualifikationen in sicherheitsrelevanter Embedded C-Programmierung, der Nachweis von Workshops, wie das kommende IoT SECFOR 2021 von Ares, und Weiterbildungen wie Foundations of IoT Security der IoTSF oder Certified IoT Security Practitioner von Certnexus heben Bewerber von der Konkurrenz ab.

Was die spannenden Beschäftigungsmöglichkeiten an der Front der IoT-Sicherheit angeht, so spriessen täglich neue Unternehmen wie Sensiron, Kistler, Duagon und Qiio aus dem Boden. Auch Chip-Hersteller wie NXP, Renesas und WISeKey bieten interessante Optionen für angehende IoT-Sicherheitsspezialisten.

Wer sich für den Einstieg in die Welt der IoT-Security interessiert, kann sich bei Prof. Dr. Andreas Rüst, Leiter des Studiengangs IoT an der ZHAW, Jonas Conrad, Leitender Forscher des pd|z an der ETH Zürich oder Prof. Dr. Willenbacher des KIT, informieren.

Personality: über technisches Know-How hinaus

Wenn es um IoT-Sicherheitsspezialisten geht, ist es klar, dass Ingenieure in der gesamten IT-Branche sehr gefragt sein werden. Aber es braucht mehr als nur technische Fähigkeiten, um eine Technologie dieser Grössenordnung zukunftssicher zu machen.

Es braucht Fleiss und Ausdauer, wenn es um langwieriges Troubleshooting geht. Gut ausgeprägte analytische Fähigkeiten zur Identifizierung von Sicherheitsrisiken und möglichen Lösungen sind ebenfalls unerlässlich.

Schliesslich, und das wird oft unterschätzt, sind auch Kommunikationsfähigkeiten für effektive IoT-Sicherheitsspezialisten unerlässlich. Ein entscheidender Teil ihrer Arbeit wird darin bestehen, das Management auf die Risiken des IoT aufmerksam zu machen. Daher ist die Fähigkeit, das Bewusstsein zu schärfen und Probleme, Lösungen und die jeweiligen Vorteile der verschiedenen Handlungsoptionen aufzuzeigen, absolut entscheidend.

In unserem heutigen Artikel steht die technologische Vernetzung der Dinge im Mittelpunkt. Die Relevanz und die Attraktivität der Möglichkeiten ist unbestritten. Wenn es jedoch darum geht, die richtigen Menschen zu gewinnen, die diese Technologien erfolgreich vorantreiben, dann ist ebenfalls Vernetzung gefragt – menschliche Vernetzung.

Auch hier könnte man wieder technologiegetrieben mittels künstlicher Intelligenz versuchen über Algorithmen die passenden Spezialisten zu identifizieren. Das ist bereits heute möglich und wird sich auch in Zukunft weiter auf höherem Niveau etablieren. Was in jedem Fall von bedeutender Wichtigkeit sein wird, um die entscheidende Nasenlänge voraus zu sein, sind echte sehr gut gepflegte Beziehungen, die es möglich machen unkompliziert mit potentiellen Kandidaten in Kontakt zu kommen und rasch eine Zusammenarbeit zu initialisieren.

Bei aller Liebe zur Technologie werden sich nur die Unternehmen im Markt langfristig durchsetzen können, die die richtigen Persönlichkeiten noch weit vor deren Anstellung kennen, kontinuierlich pflegen und dann für sich gewinnen. Time to **candidate market** ist ein heute vielfach diskutiertes jedoch noch zu wenig strategisch ausgeprägtes Element innerhalb der Key-Success-Drivers von Unternehmen. Peter Kosel beobachtet in seinem täglichen Geschäft wie wenig Aufmerksamkeit das Thema **Pflege zukünftiger Leistungsträger** geniesst.

Der KNOW YOUR TALENTS approach von cyberunity unterstützt Unternehmen genau auf dieser Reise - Peter Kosel begleitet Unternehmen aktiv in eine erfolgreiche Zukunft und ist gerne für Gespräche offen. Sie erreichen ihn ganz unkompliziert unter pk@cyberunity.io.