TÜV Rheinland: Cybersecurity entscheidet über die Stabilität von Gesellschaften

10.02.2020 | Köln

Die Entwicklungen im Bereich Cybersecurity sind bedenklich: Die immer größere Zahl von smarten Geräten in privaten Haushalten erhöhen die Angriffsmöglichkeiten für Cyberkriminelle erheblich. Der unkontrollierte Zugriff auf personenbezogene Daten untergräbt das Vertrauen in die digitalisierte Gesellschaft. Logistikbranche und Individualverkehr geraten zunehmend ins Visier von Hackern. Dies sagen die Fachleute von TÜV Rheinland, die ihre Cybersecurity Trends für 2020 veröffentlicht haben. „Besonders schwer wiegt aus unserer Sicht, dass sich Cyberkriminalität zunehmend auf unsere persönliche Sicherheit und die Stabilität der Gesellschaft insgesamt auswirkt“, erklärt Dirk Fenske, Geschäftsführer im Geschäftsfeld Cybersecurity & Functional Safety bei TÜV Rheinland. „Das liegt unter anderem daran, dass digitale Systeme in immer mehr Bereiche unseres täglichen Lebens Einzug halten. Die Digitalisierung bietet viele Vorteile – wichtig ist aber, dass diese Systeme und damit die Menschen vor Angriffen sicher sind.“

Sieben Cybersecurity Trends für 2020 von weltweit führenden Fachleuten

Welche Trends in diesem Jahr besonders wichtig werden, legen die weltweit führenden Expertinnen und Experten für Cybersecurity von TÜV Rheinland in ihrem neuen Bericht dar. Dabei haben die Fachleute sieben wichtige Entwicklungen identifiziert – von Angriffen auf smarte Lieferketten über Gefahren für Medizingeräte bis zu Schwachstellen in Echtzeitbetriebssystemen. Wie in den Vorjahren hat TÜV Rheinland für den Bericht die Einschätzungen der eigenen Fachleute für Cybersecurity weltweit einbezogen.

Der unkontrollierte Zugriff auf personenbezogene Daten birgt die Gefahr der Destabilisierung der digitalen Gesellschaft

Im Jahr 2017 bat die Französin Judith Duportail ein Dating-App-Unternehmen, ihr sämtliche persönlichen Daten zu schicken, die dieses von ihr besaß. Als Antwort erhielt sie ein 800-seitiges Dokument, das ihre Facebook-Likes und -Freunde, das Alter der Männer, an denen sie Interesse bekundet hatte, und jedes einzelne Online-Gespräch enthielt, das sie seit 2013 mit allen 870 passenden Kontakten geführt hatte. Dass Judith Duportail nach mehrjähriger Nutzung einer einzigen App so viele personenbezogene Daten erhielt, unterstreicht: Datenschutz ist mittlerweile sehr herausfordernd. Zudem zeigt dieses Beispiel, wie wenig Transparenz über die

Sicherung und Weiterverarbeitung von Daten herrscht, mit denen sich ein genaues Bild von den Interessen und dem Verhalten einer Person gewinnen lässt.

Smarte Geräte für Verbraucher verbreiten sich schneller als sie abgesichert werden können

Smarte Lautsprecher, Fitnesstracker, smarte Uhren, Thermostate, Energiezähler, smarte Sicherheitskameras für das Zuhause, smarte Schlösser und Leuchten sind die bekanntesten Beispiele für die anscheinend unaufhaltsame Demokratisierung des „Internets vieler Dinge“. Die Anzahl und Leistungsfähigkeit der individuellen „smarten“ Geräte steigt Jahr für Jahr – sie werden mehr und mehr zum festen Bestandteil des Alltags und lassen eine Zukunft vorausahnen, in der Wirtschaft und Gesellschaft von ihnen abhängig werden. Smarte Geräte sind nicht mehr nur Spielzeug oder Technikneuheiten und das macht sie auch zu Zielen für Cyberkriminelle. Bisher bestand die Herausforderung für Cybersecurity darin, eine Milliarde Server und PCs zu schützen. Mit der Verbreitung smarter Geräte könnte sich die Angriffsfläche schnell um das Hundert- oder Tausendfache vergrößern.

Der Trend zum eigenen Medizingerät erhöht das Risiko für eine Internet-

Gesundheitskrise

In den vergangenen zehn Jahren wurden persönliche Medizingeräte wie Insulinpumpen, Herz- und Glukosemonitore, Defibrillatoren und Herzschrittmacher im Zuge des sogenannten „Internets der medizinischen Dinge“ (IoMT) mit dem Internet verbunden. Gleichzeitig haben Forscher eine wachsende Zahl von Softwareschwachstellen festgestellt und die Machbarkeit von Angriffen auf diese Produkte nachgewiesen; dies kann zu gezielten Angriffen auf Einzelpersonen und ganze Produktklassen führen. In einigen Fällen können auch die von den Geräten erzeugten Gesundheitsinformationen abgefangen werden. Bislang tut sich die Gesundheitsbranche schwer damit, auf das Problem zu reagieren – insbesondere, wenn die offizielle Lebensdauer der Geräte bereits abgelaufen ist. Wie bei so vielen IoT-Geräten dieser Generation war die Vernetzung wichtiger als das Bedürfnis nach Cybersecurity. Die komplexe Aufgabe der Wartung und Reparatur von Geräten verläuft unkoordiniert oder mangelhaft – oder fehlt ganz.

Fahrzeuge und die Verkehrsinfrastruktur sind neue Ziele von Cyberangriffen

Durch die Entwicklung eigener Soft- und Hardwareplattformen werden Fahrzeuge und die Verkehrsinfrastruktur zunehmend miteinander verknüpft. Diese Anwendungen bieten Fahrerinnen und Fahrern mehr Flexibilität und Funktionen, potenziell mehr Verkehrssicherheit und scheinen angesichts der Entwicklung selbstfahrender Fahrzeuge unvermeidlich. Der Nachteil ist die zunehmende Anzahl von Schwachstellen, die Angreifende ausnutzen könnten – mit direkten

Auswirkungen auf die Sicherheit. Breit angelegte Cyberangriffe könnten nicht nur die Sicherheit einzelner Verkehrsteilnehmer beeinträchtigen, sondern auch zu weitreichenden Störungen des Verkehrs und der Sicherheit in Städten führen.

Hacker nehmen smarte Lieferketten ins Visier – und machen sie „dumm“

Mit dem Ziel höherer Effizienz und geringerer Kosten nutzen smarte Lieferketten die Automatisierung über das Internet der Dinge (Internet of Things, IoT), Robotik und Big-Data-Management – sowohl innerhalb eines Unternehmens als auch bei Zulieferern. Smarte Lieferketten stellen zunehmend die Lagerhaltung virtuell dar; das Lager ist damit nicht mehr nur ein physisch vorhandenes Gebäude, sondern jeder Ort, an dem sich ein Produkt oder seine Komponenten zu einem beliebigen Zeitpunkt befinden können. Dennoch wächst die Erkenntnis, dass dieses Geschäftsmodell schon bei recht kleinen Störungen die finanziellen Risiken beträchtlich erhöht. Smarte Lieferketten sind dynamisch und effizient, aber auch anfällig für Störungen ihren den Abläufen. Cyberangriffe können Informationen zu Lagerstätten manipulieren. Somit wären Komponenten nicht an den Orten an denen man sie vermutet.

Bedrohungen der Schifffahrt sind nicht mehr nur eine theoretische Gefahr, sondern Realität

Im Jahr 2017 wurden

Waren mit einem geschätzten Gewicht von rund 10,7 Milliarden Tonnen über den Seeweg transportiert. Trotz aktueller geopolitischer und handelspolitischer Spannungen wird allgemein erwartet, dass der Handel weiter zunimmt. Es gibt zahlreiche Belege dafür, dass Staaten mit direkten Angriffen auf Navigationssysteme von Schiffen experimentieren. Auch werden inzwischen Angriffe auf Computernetze von Schiffen gemeldet, mit denen Lösegeld erpresst werden soll. Die Hafenlogistik bietet einen zweiten, sich damit überschneidenden verwundbaren Bereich. Proteste von Cyberaktivisten können sich auf die Schifffahrtsbranche auswirken. Hinter solchen Protesten steht jeweils eine eigene Agenda. Es lässt sich kaum feststellen, wann aus Drohungen durch Aktivisten ein signifikantes Risiko werden könnte. Das macht die Überwachung und das Verständnis von Drohungen zu einem Schlüsselfaktor der modernen maritimen Cybersecurity.

Schwachstellen in Echtzeitbetriebssystemen könnten das Ende des Patch-Zeitalters einläuten

Bis 2025 wird es im Internet der Dinge schätzungsweise über 75 Milliarden vernetzte Geräte geben, die jeweils ein eigenes Softwarepaket verwenden. In diesem befinden sich wiederum viele ausgelagerte und potenziell gefährdete Komponenten. Im Jahr 2019 entdeckte Armis Labs elf schwerwiegende Schwachstellen (genannt „Urgent/11“) im Echtzeitbetriebssystem (Real Time Operating System, RTOS) Wind River VxWorks. Sechs dieser Schwachstellen setzten schätzungsweise 200 Millionen IoT-Geräte dem Risiko von Angriffen durch Codeausführung aus der Ferne (Remote Code Execution, RCE) aus. Diese Ebene der Verwundbarkeit ist eine große Herausforderung, da sie oft tief in einer großen Anzahl von Produkten verborgen ist. Organisationen merken vielleicht nicht einmal, dass es diese Schwachstellen gibt. Angesichts dessen wird die

Vorgehensweise, immer die neuesten Sicherheitsupdates zu installieren, nicht mehr zielführend sein.

Kontakt für Journalisten: Norman Hübner
Telefon: +49 221 806 - 3060
E-Mail: norman.huebner@de.tuv.com

****

TÜV Rheinland ist ein weltweit führender unabhängiger Prüfdienstleister mit fast 150 Jahren Tradition. Im Konzern arbeiten über 20.000 Menschen rund um den Globus. Sie erwirtschaften einen Jahresumsatz von 2 Milliarden Euro. Die unabhängigen Fachleute stehen für Qualität und Sicherheit von Mensch, Technik und Umwelt in fast allen Wirtschafts- und Lebensbereichen. TÜV Rheinland prüft technische Anlagen, Produkte und Dienstleistungen, begleitet Projekte, Prozesse und Informationssicherheit für Unternehmen. Die Experten trainieren Menschen in zahlreichen Berufen und Branchen. Dazu verfügt TÜV Rheinland über ein globales Netz anerkannter Labore, Prüfstellen und Ausbildungszentren. Seit 2006 ist TÜV Rheinland Mitglied im Global Compact der Vereinten Nationen für mehr Nachhaltigkeit und gegen Korruption.

Website www.tuv.com