«Aktuelle Technik» hat drei hochkarätige Experten zu einem Round Table geladen, um mit ihnen über die Themen Cyber-Kriminalität, Datenschutz und die Auswirkungen auf das Engineering von Projekten zu diskutieren.
Interview: Andreas Leu
Fotos: Holger Jacob

«Cyber-Security im Engineering»

Dem Thema Schutz vor Cyber-Kriminalität wird in vielen Unternehmen leider oft noch zu wenig Beachtung geschenkt. Warum ist das so und welche verheerenden Auswirkung diese Einstellung haben kann – dazu äussern sich folgende Experten:

Prof. Dr. Hannes Lubich, Dozent für Informatik an der Fachhochschule Nordwestschweiz (FHNW). Er beschäftigt sich seit über 35 Jahren mit Betriebssystemen, Netzwerk- und Kooperationstechnologien, IT-Architekturen, Informationssicherheit und Risikomanagement. Während zehn Jahren war er Forscher und Dozent an der ETH Zürich und war zudem am Aufbau und Betrieb des Schweizer Hochschulnetzes Switch und des Sicherheitszentrums Switch-Cert beteiligt.
Seit April 2009 ist er als Professor für Informatik am Institut für Mobile und Verteilte Systeme an der FHNW in Brugg-Windisch tätig und vertritt das Gebiet ICT System & Service Management in der akademischen Ausbildung, der beruflichen Weiterbildung und der angewandten Forschung und Entwicklung.

Michael Rey, CEO bei Rey Automation. Nach dem erfolgreichen Lehrabschluss als Elektromonteur studierte er an der ZHAW Kommunikation und Informatik An-schliessend arbeitete er bei Kindlimann AG Informatik (Europe) und stieg beim Familienunternehmen Rey Automation ein. Er gründete Rey Informatik und absolvierte parallel das NDA in Automation Management an der FHNW. Seit 2016 ist er CEO der Rey Automation.

Roger Hiestand, Head of IT Security bei Siemens Schweiz AG. Er beschäftigt sich seit mehr als 15 Jahren mit IT-Sicherheitssystemen und spezialisierte sich auf den Cyber-Security-Bereich bei Industrieanlagen – Operational Technology (OT). Bei Siemens Schweiz AG verantwortet er das komplette Cyber-Security-Portfolio für den Bereich Building Technologies.
Das erfolgreich abgeschlossene Studium mit dem Bachelor of Science in Information Technology gibt ihm die Möglichkeit, nebst dem technischen Wissen auch die wirtschaftlichen Faktoren mit einzubeziehen, sodass perfekt integrierte Sicherheitslösungen vor allem im Bereich OT erstellt werden können.

Mark Twain sagte einst: «Prognosen sind schwierig, besonders wenn sie die Zukunft betreffen.» Es gab in der Vergangenheit viele Irrtümer. Auch dieser von Bill Gates, als er 2004 meinte: «Spam wird in zwei Jahren ein Ding der Vergangenheit sein.» Warum lag er damals falsch? Warum sind wir heute so weit, und was wurde bezüglich Kriminalität im Netz verpasst beziehungsweise was lief falsch? Lassen sich Lehren für die Zukunft ableiten, oder muss hier Cyber-Security immer wieder neu erfunden oder angepasst werden?
Lubich: Die Aussage von Bill Gates hatte seinerzeit einen ganz bestimmten Hintergrund. Er propagierte damals, dass Microsoft weltweit eine sichere E-Mail-Umgebung anbieten würde, die Spam in ihrer eigenen Umgebung vollständig ausgeschlossen hätte. Dieser Vorschlag fand aber keine ausreichende Unterstützung im Markt. Dass wir heute über Sicherheitsthemen diskutieren, von denen wir gehofft haben, dass sie längst abgehakt wären, liegt unter anderem auch daran, dass wir bei der Sicherheit im Netz ein sehr bewegliches Spielfeld haben, in dem neue Probleme permanent hinzukommen, alte aber nicht eliminiert sind. Damit steigt die Gesamtkomplexität eines Systems dermassen, dass wir nicht mehr in der Lage sind, Sicherheit zu garantieren, und dazu gehören natürlich auch E-Mail-Sicherheit und Ähnliches. Hinzu kommt, dass wir bei der Cyber-Security ein Nachgedanke des Engineerings sind. Die Unternehmen wollen die Ersten auf dem Markt sein. Sie überbewerten daher die Opportunitäten, und die Sicherheit steht dem Verkauf sowie dem Marketing beim Time-to-Market im Weg. Das führt dazu, dass sich hier eine Schere immer weiter öffnet. Es herrscht klar ein Interessenkonflikt. Natürlich wäre es schön, wenn «Security by Design» im Engineering verstanden würde, aber der Marktdruck lässt das in vielen Fällen so nicht zu.
Rey: Wir als Engineering-Unternehmen sind natürlich direkt betroffen, denn wir «dürfen» die Produkte einsetzen, die uns die Hersteller zur Verfügung stellen. Die Situation hat sich in den letzten Jahren insofern geändert, dass heute alles vernetzt wird. Früher war eine Steuerung nicht dazu vorgesehen, mit einer Cloud zu kommunizieren. Heute werden diese älteren Steuerungen ohne weitere Massnahmen in eine neue Infrastruktur eingebunden. Hinzu kommt, dass alles sehr schnelllebig geworden ist, denn die Firmen und der Markt stehen unter Druck. Die Kunden möchten möglichst schnell ihre Maschinen vernetzen, jedoch ist die Basis dazu oft nicht vorhanden. Der Gedanke an die Security wird verdrängt, denn die Kosten dafür sind zu hoch. In solchen Situationen geht man schnell den einfachen Weg und bindet rasch ein I/O-Link-Gateway oder einen Lora-Sensor in die Anlage ein und fragt nicht, was mit der Verschlüsselung sei und wie die Daten kommuniziert würden. Und schon haben wir ein Sicherheitsproblem.
Hiestand: Als Hersteller stehen wir bei dieser Thematik mittendrin. Siemens ist einerseits Hersteller, andererseits auch Lösungsanbieter. Wir haben diese Problematik klar erkannt, und es ist ein Bereich, bei dem wir feststellen, dass der Security-Gedanke im Engineering noch nicht genügend angekommen ist. Und wenn wir beim Thema Entwicklung von neuen Produkten sind, sehen wir, dass der Markt dort ebenfalls Schwierigkeiten hat. Die grundsätzliche Basis fehlt teilweise in den Industrien, auch im OT-Bereich. Das Bewusstsein über das, was alles dazugehört, ist vielfach nicht vorhanden. Nicht nur bei der Entwicklung der einzelnen Produkte, sondern auch bei deren Implementierung. Viele Produkte bieten

«Es besteht ein Interessenkonflikt zwischen Cyber-Security und Time-to-Market.»
Roger Hiestand

«Die heutige Informatikausbildung ist auf agile Softwareentwicklung ohne langwierige Spezifikationen ausgelegt.»

Hannes Lubich

Ansatzmöglichkeiten, eine Security zu verwenden. Weil das Thema in den Industrien noch so fern ist, herrscht immer noch oft die Auffassung, dass es sich um eine Insellösung und somit um eine sichere Lösung handelt. Diese Denkweise ist auch im Jahr 2019 bei den Planern, den Herstellern und in den Engineering-Abteilungen nach wie vor vorhanden. Das ist aus unserer Sicht die ganz grosse Baustelle. Früher wurde das Thema Security noch vermehrt von der Compliance getrieben. Und heute, es wurde bereits angedeutet, spielt Time-to-Market eine wesentlich grössere Rolle. Die Industrieunternehmen wägen schlicht und einfach das Restrisiko ab und entscheiden sich aus wirtschaftlichen Gründen unter Umständen gegen wirksame Sicherheitsvorkehrungen.

Ich unterhielt mich an einer Tischmesse mit einem Geschäftsleitungsmitglied eines grösseren Beratungs- und Engineering-Unternehmens im IT-Bereich. Auf die Frage, wie seine Firma das Thema Cyber-Security bei der Beratung und im Engineering angehe, gab er folgende Antwort: «Das ist nicht unsere Sache, dafür gibt es spezielle Unternehmen.» Da war ich doch ziemlich verblüfft. Was halten Sie von dieser Aussage?

Lubich: Das ist schon eine eigenartige Antwort, aber leider nicht unüblich.
Rey: Wir stellen das oft fest. In unserem Unternehmen legen wir den Fokus auf eine 360-Grad-Digitalisierung, welche die Sicherheit mit einschliesst. Wir haben Informatik- und Datenbankspezialisten, aber auch Automatikspezialisten. Wenn wir eine PC-basierte Steuerung mit einer Windows-Plattform einsetzen, ist unser Automatikprogrammierer glücklich und legt mit seiner Automatisierungsapplikation sofort los. Alles andere interessiert ihn in diesem Moment nicht. Wenn dann unser Netzwerkspezialist bezüglich Sicherheit die ersten Fragen stellt, bekommt dieser vom Programmierer die Antwort, dass das nicht seine Welt sei. Dabei ist das System offen wie ein Scheunentor. Ich kenne Kunden, bei denen eine Steuerung mit einer Windows-Plattform über 20 Jahre am Netz hängt und das Betriebssystem in all den Jahren nie «gepatcht» wurde. Hier stellen wir eine grosse Diskrepanz fest. Als Engineering-Firma ist es unsere Pflicht, den Kunden darauf aufmerksam zu machen, welche Risiken er eingeht, welche gravierenden Folgen entstehen können und welche Lösungen sinnvoll wären.
Hiestand: Ein Grund dafür könnte sein, dass das Gedankengut noch nicht vorhanden ist. Der Programmierer sieht seine Aufgabe darin, die Anlage zum Funktionieren zu bringen. Die vor- und nachgelagerten Prozesse sind nicht definiert, oder es ist den Programmierern nicht klar, wie sie bei der Security vorgehen müssten.
Rey: Man erkennt an dieser Stelle einen Konflikt zwischen IT und OT. Die Informatik «kämpft» gegen den Automationsbereich, denn das ist jeweils nicht ihre Welt. Oft verstehen die Informatiker nicht, was bei der Anlagenautomatisierung benötigt wird, denn in diesem Bereich gibt es andere Protokolle, und es handelt sich um ganz andere Prozesse. Und generell gilt, wenn man etwas nicht versteht, will man am liebsten nichts damit zu tun haben. Also installiert der IT-Ingenieur ein grosses Class-C-Netz und definiert dann: Das ist das Automationsnetz, und es interessiert mich nicht, was ihr daran anschliesst. Deshalb haben wir zusätzlich eine IT-Abteilung aufgebaut und Personen ausgebildet, die mit den Prinzipien der Automation vertraut sind.
Lubich: Wir stellen fest, dass hier Ingenieurdisziplinen unterschiedlich agieren. Ein Informatikingenieur ist sich gewohnt, mehr oder weniger täglich Softwareänderungen vorzunehmen, auch wenn diese, organisatorisch gesehen, nur einmal im Monat eingespielt werden. Spreche ich mit einem Kraftwerkingenieur, dann ist für ihn ein Change-Zyklus von 30 Jahren oder sogar länger normal. Hier prallen zwei Ingenieurwelten aufeinander, die wenig voneinander wissen. Sie reden oft mehr übereinander als miteinander. Auf der anderen Seite besteht auch das Problem, wem delegiere ich was. Wenn die andere Partei etwas macht, heisst das noch lang nicht, dass sie die Aufgabe richtig verstanden hat. Fairerweise muss man hinzufügen, dass die Informatik diesbezüglich keine besonders gute Historie vorweist. Das Internet per se wurde nie designt, um sicher zu sein. Es wurden einfach immer mehr Funktionen auf eine schwache Basis gepackt. Für mich ist es manchmal erstaunlich, dass es überhaupt noch funktioniert. Ich hatte Mitte der 80er-Jahre dabei mitgewirkt, das Internet in die Schweiz zu bringen, und damals ging man davon aus, dass es sich um ein kleines Netz für ein paar Hochschullehrer handelt. Das Internet war ursprünglich nicht für den Massenmarkt gedacht und designt, aber jetzt verwenden wir es für viele Dinge, für die es zu Beginn nicht vorgesehen war. Nun kommen nicht nur die Anwender, die glauben, dass es sich beim Internetzugang um ein Menschenrecht handelt, sondern nun kommen auch Infrastrukturspezialisten, die behaupten, dass sie diese Konnektivität ebenfalls brauchten. Einer der Gründe für das «Pushen» auf schnelle Vernetzung mit 5G und auf schnelles Internet ist nicht, dass Netflix auf dem Mobile schneller laufen muss, sondern weil der Markt Anlagen erschliessen will und diese mit Netzwerkadressen versehen muss. Dafür brauche ich eine Infrastruktur, auf die beide Seiten nicht vorbereitet sind. Für die IT-Ingenieure ist das immer noch ein bisschen ein Versuch mit Irrtum. Dazu muss man fairerweise sagen, dass wir in der IT nicht die gleichen Gewährleistungen haben wie für ein industrielles Produkt. Die klassischen IT-Unternehmen können sich mit AGB zum grossen Teil gegenüber den Kunden absichern. Wenn jemand Software installiert, akzeptiert er die AGB des Anbieters, klickt auf OK, ohne den Inhalt wirklich gelesen zu haben. Die Informatik ist deshalb,

rechtlich gesehen, von den Konsequenzen «enthaftet». Würde ich heute eine Maschine oder Anlage kaufen, würde das nicht so funktionieren. Hier gilt nicht dieselbe Art der Produkthaftung. Das hat die IT-Branche bis anhin ausgenutzt, denn sie ist gewohnt, dass sie Fehler macht und diese nachträglich repariert werden müssen. Das gilt, solange keine physischen Schäden entstehen, die irgendwann nicht mehr reversibel sind, weil jemand verunfallt oder eine Maschine physisch defekt ist. In der Informatik lässt sich ein Fehler im Nachhinein immer mit einem Softwarepatch reparieren. Diese Denkweise ist bei den klassischen IT-Programmierern noch sehr stark verankert.

Hiestand: Dieses Verhalten wird auch nach wie vor von der Gesellschaft toleriert, wenn nicht sogar unterstützt, egal ob es sich um eine Privatperson oder um ein Unternehmen handelt. In der IT-Welt ist es völlig normal, dass ich ein Betriebssystem mehrmals im Jahr update. Zu diesem Zeitpunkt kann ich mit meinem Rechner nicht arbeiten, das ist bekannt und wird auch so akzeptiert. Wenn es sich um eine produzierende Maschine handelt, die zur Produktionszeit gewartet wird, und wenn der Unterbruch zehn Minuten dauert, wird das nicht gebilligt. Handelt es sich um eine Maschine aus Zeiten ohne Elektronik, wurde diese eingesteckt und lief 10 bis 15 Jahre praktisch ohne Unterbruch. Auch beim Wechsel zur Digitalisierung besteht immer noch dieselbe Erwartungshaltung, obwohl mittlerweile Komponenten installiert sind, die auch in der IT verwendet werden und deren Lebenszyklus nun rund fünf Jahre ist, was der Normalität entspricht.

Lubich: Wenn ich diese Verhaltensweise beispielsweise auf Fahrzeuge und auf produzierende Anlagen hochrechne, dann klafft für mich eine Lücke in der Wahrnehmung, was mit dem Begriff Sicherheit bezeichnet wird. Dazu kommt, dass wir im Deutschen das Wort Sicherheit für zwei Dinge verwenden. Im angelsächsischen Raum werden Safety und Security klar voneinander getrennt.

Hiestand: Eine Problematik besteht auch darin, dass die Arbeitskräfte immer noch die gleiche Ausbildung aufweisen. Wir stellen das auch bei uns fest. Als ich bei Siemens anfing, waren die Kameras noch alle analog mit einem Videokabel verbunden. Dann kam der Wechsel zur Digitalvideotechnik, die Personen, die diese anwendeten, waren jedoch nach wie vor die Spezialisten für die analoge Videotechnik. Nun soll der gleiche Mitarbeiter eine Kamera in eine Netzwerkinfrastruktur eines Gebäudes installieren. Dazu fehlt ihm jedoch einfach das Know-how, welche Auswirkungen das auf die Security haben kann. An diesem Beispiel erkennt man, dass hier zwei Welten verschmelzen.

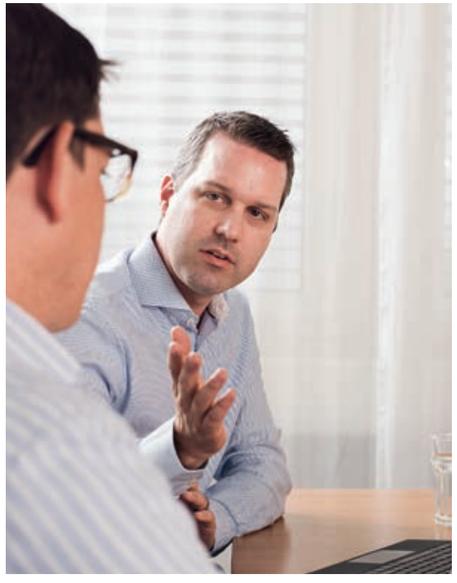
Agiert die Industrie bei Cyber-Security überhaupt noch, oder kann sie nur reagieren? In welchem Umfang ist es sinnvoll, aktiv zu agieren, wann und wo kann oder muss man es sich leisten, angemessen zu reagieren? Gibt es technische Möglichkeiten wie künstliche Intelligenz (KI), die Cyber-Security (Beispiel Instagram) auch lernen kann?

Lubich: In diesem Bereich existiert inzwischen relativ viel. Dabei muss aber berücksichtigt werden, dass die Technologie nur einen Teil der Lösung sein kann. Diese muss auch gesteuert, überwacht und ausgewertet werden. Auch dieses Wissen ist nicht überall vorhanden. Weiter muss man berücksichtigen, dass solche Werkzeuge beiden Kontrahenten zur Verfügung stehen, sowohl den «Angreifern» als auch den «Verteidigern». Die Angreifer sind oft wesentlich agiler, solch neue Werkzeuge einzusetzen. Ich bin Moment habe ich ein Beratungsmandat bei einem grossen Polizeikorps, um das Thema Cyber-Kriminalität zu bearbeiten. Dabei stellen wir fest, dass kriminelle Organisationen gegenüber den angegriffenen oft schneller und ohne einen speziellen Businessplan agieren können. Zudem sind die Angreifer durchaus bereit, Vorinvestitionen in erfolgreiche Übergriffe zu tätigen. Das war bis vor einigen Jahren die Domäne der Nachrichtendienste. Der sehr erfolgreiche Angriff auf die iranische Nuklearaufbereitung war seinerzeit ein Angriff der westlichen Nachrichtendienste. Die Vorbereitung dazu dauerte circa zwei bis drei Jahre und kostete wohl mehr als 15 Millionen US-Dollar. Erstaunlicherweise erkennen wir nun, dass kriminelle Organisationen bereit sind, in vergleichbarem finanziellem und zeitlichem Umfang Angriffe vorzufinanzieren, ohne dass eine Garantie auf Erfolg besteht. Sie tun das, weil dahinter Gewinn durch Erpressung oder Schädigung eines wirtschaftlich Beteiligten steckt. Aus meiner Sicht öffnet sich so, was die einsetzbaren Mittel angeht, eine weitere Schere. Ich bin früher gegen Cyber-Kriminelle angetreten, das waren meistens Einzeltäter. Heute sind es ganze Organisationen. Wir treten gegen Nachrichtendienste an, die Wirtschaftsspionage betreiben. Diesen stehen Mittel in einem Masse zur Verfügung, bei denen wir schlichtweg nicht mithalten können.

Rey: Es besteht höchstens die Möglichkeit, die Hürde etwas höher zu setzen. Wir können versuchen, es bis zu einem gewissen Grad zu verhindern.

Hiestand: Bei diesem Punkt ist es wichtig, zu verstehen, dass das auch mit der Interessenlage zu tun hat. Warum hat die Angreiferseite dieses Interesse? Diese Partei kann oder darf das machen, während die defensive Seite es machen muss. Der Angreifer muss nur eine Sicherheitslücke finden, während der Verteidiger möglichst alle schützen sollte. Der Punkt, die Hürde höher zu setzen, ist gerade in der Industrie extrem wichtig. Die Erfolgsquote der Angreifer ist deshalb so hoch, weil sie wissen, dass viele Anlagen einfach nicht geschützt sind.

Lubich: Die entsprechenden Werkzeuge dafür sind im Internet oft frei verfügbar. Allein die Suchmaschine Shodan sucht speziell nach industriellen Steuerungsanlagen, die über das Internet erreichbar sind. Das geht von Verkehrskameras bis zu Spitalinfrastrukturen. Das kann man auch als «Laie» auf einer eigenen Suchmaschine beobachten. Dort erkennt man zum Beispiel, dass ein Standardpasswort seit längerer Zeit vom Hersteller nicht mehr verändert wurde. Die Angreifer sind zudem in der Lage, dieses Wissen innerhalb ihrer Community besser zu teilen. Im Darknet existieren Plattformen für solche Informationen, die auch jemand findet, der selbst keine kriminelle Energie hat. Die Protagonisten auf der Darknet-Seite arbeiten sehr gut zusammen und sind auch in der Lage, die notwendigen Mittel bereitzustellen. Dadurch wurden die Angriffe sehr professionell. Wir sehen oft, dass das über Länder geschieht, mit denen wir kein Rechtshilfeabkommen haben, um die Täter effizient zu verfolgen. Das bedeutet auch, dass sich eine Staatsanwaltschaft nicht allzu sehr für solche Straftaten interessiert, weil die Erfolgschancen bei den Ermittlungen nahe bei null liegen. Dadurch ist die Dunkelziffer der Übergriffe sehr hoch. Es gibt beispielsweise Länder, bei denen die Zahlung von Lösegeldern eine Straftat oder zumindest meldepflichtig ist. Das trifft für



«Der Programmierer sieht seine Aufgabe in erster Linie darin, die Anlage zum Funktionieren zu bringen.»

Roger Hiestand

«Unternehmen vernachlässigen aus Kostengründen die Wichtigkeit der Cyber-Security. Das kann allerdings sehr gefährlich sein.»

Michael Rey

die Schweiz nicht zu. Natürlich sagt die Polizei, dass die Unternehmen nicht bezahlen sollen, wenn sie angegriffen werden. Ist eine Firma auf die Produktion angewiesen, kommt sie schnell in Versuchung, das Lösegeld zu bezahlen. Das funktioniert in der Praxis erstaunlich oft
Rey: Ein Beispiel dazu: Bei einem grossen Unternehmen wurden die Arbeitsstationen, wir sprechen von mehr als 1000 Geräten, durch eine Cyber-Attacke verschlüsselt. Die Angestellten konnten nicht mehr arbeiten. Das ERP hat zwar einwandfrei funktioniert, allerdings konnte niemand mehr darauf zugreifen. Das heisst, die gesamte Produktion, die über das ERP abgewickelt wurde, war stillgelegt. Praktisch jeder Mitarbeiter musste sein privates Notebook organisieren, um mit diesem über einen speziell eingerichteten Kanal auf die Daten zuzugreifen. Der monetäre Schaden dürfte sich in Millionenhöhe bewegt haben.
Lubich: Auch im Spitalbereich funktioniert das ziemlich gut. Es gab in Deutschland eine Klinik, bei der die ganze Infrastruktur nicht mehr funktioniert hat, und dann kamen Probleme auf, an welche die Ingenieure nicht gedacht hatten. Was passiert, wenn eine Operation verschoben werden muss, weil man zum Beispiel auf die Krankenakte keinen Zugriff mehr hat und man nun die Blutgruppe oder andere Daten des Patienten nicht kennt. Dann entsteht ein nicht kalkulierbares Risiko, wenn man den Patienten operiert, aber gegebenenfalls auch, wenn man nicht operiert. Wer soll dann die Verantwortung tragen? Denn das ist kein Entscheid, den das Engineering fällen wird. Wir sind auf jeden Fall weder gesellschaftlich noch juristisch auf solche Begebenheiten vorbereitet.
Hiestand: Wir hatten einen Fall, bei dem eine Lüftungsteuerung verschlüsselt worden war. Es wurde zwar bei der Installation eine Software in Form eines VPN-Client eingebaut, der für die Datensicherheit zuständig war. Dieser Client jedoch war inzwischen völlig veraltet und deshalb angreifbar. Über diesen konnte man nun problemlos zugreifen, und man erhielt im Nu Zugang auf das gesamte System.
Lubich: Für den Verkauf solcher Schwachstellen gibt es inzwischen sogar einen Markt, und es handelt sich an dieser Stelle um ein handelsübliches Verfahren. Jedes grössere Softwareunternehmen bietet heute ein Rückkaufprogramm für Softwarefehler an, die neu bekannt gewordenen sind. Wenn ich also einen neuen Softwarefehler finde, kann ich das dem Hersteller melden. Bin ich tatsächlich der Erste, der einen gravierenden Fehler gefunden hat, zahlt mir das Unternehmen inzwischen für eine solche Schwachstelle gegen 20 000 US-Dollar. Wenn ich dasselbe im Darknet anbiete, erhalte ich mitunter das Zehnfache. Das steuerfrei und in einer von mir gewählten Kryptowährung. Das ist inzwischen ein ganz normaler Markt.
Rey: Wir erleben praktisch wöchentlich, dass wir auf Anlagen stossen, die noch mit Betriebssystemen wie Windows XP oder Windows NT ausgerüstet sind. Das letzte Update wurde vielleicht vor zwei oder drei Jahren durchgeführt. Das Argument der Kunden für diese Nachlässigkeit ist jeweils: Wir schliessen die Anlage ja nicht oft ans Internet an.

Diese Verhaltensweise erstaunt doch sehr, denn man liest heute sehr viel über Cyber-Kriminalität in den Medien. Warum kommt diese Botschaft nicht an?
Lubich: Ich traf auf eine Anlage, bei der noch Windows XP auf dem Steuerungssystem installiert war. Ich ging zur Business-Unit und fragte, ob wir auf Windows 10 upgraden könnten. Daraufhin wurde ich gefragt, ob die Anlage danach schneller und besser laufe oder ob sie über mehr Funktionalitäten verfüge. Ich musste zur Antwort geben: «Nein, sie ist anschliessend nur moderner und damit auch sicherer.» Damit war die Angelegenheit vom Tisch, denn dafür war kein Geld vorhanden. Und genau hier liegt das Problem, dass wir heute Nachrüstungen für die Security durchführen sollten, die im Angebot nie vorgesehen waren.

Ist es möglich, dass die Ingenieure, was die Cyber-Security betrifft, oft alleingelassen werden? In vielen Unternehmen gibt es doch auch eine Qualitätssicherung, die von Fall zu Fall eingreifen müsste. Das Risiko ist doch ab einem gewissen Zeitpunkt einfach zu hoch.
Hiestand: Die Problematik ist nicht nur, dass die Ingenieure alleingelassen werden, sie ist auch durch den Lebenszyklus der Produkte bedingt. Es ist von der Historie gar nicht möglich, die Produkte sicher zu machen, denn, wie anfangs erwähnt wurde, ist das Internet per se nicht sicher. Genau gleich verhält es sich mit einer Steuerungssoftware. Diese wurde seinerzeit nicht dafür ausgelegt, dass sie Daten über das Netzwerk austauscht. Deshalb besteht gerade bei den neuen Anlagen die grosse Herausforderung darin, diese Systeme nun auch wirklich sicher zu machen. Den Fokus gilt es also darauf zu legen, dass, wenn wirklich neue Produkte entwickelt werden, die IT-Security ein integrierter Bestandteil der Entwicklung darstellt. Der zweite Schritt besteht darin, diese Entwicklungen in bestehende Infrastrukturen einzubinden.
Lubich: Ein tragisches Beispiel sind die beiden in diesem Jahr abgestürzten Boeing-737-Max-Flugzeuge. Die Vermutung liegt nahe, dass sich das Problem auf Softwareschwachstellen zurückführen lässt. Aufgrund dieses Beispiels erkennt man, wie hoch der Einführungsdruck des Marktes auf die Ingenieure war. So etwas passiert sogar in einem stark regulierten Umfeld wie in der Flugzeugindustrie. Kritisch wird es also immer dann, wenn bei einem Schaden Leib und Leben betroffen sind. Es handelt sich dabei in der Regel um Fahrzeuge oder um krisenrelevante, lebenserhaltende Infrastrukturen. Dadurch entsteht inzwischen ein ganz anderer politischer und gesellschaftlicher Druck. Wir spüren auch, dass in der Politik das Interesse an solchen Vorkommnissen immer dann steigt, wenn etwas Tragisches passiert. Wenn also die Schädigung nicht nur virtuell, sondern physisch und möglicherweise irreversibel ist. Diese typische Reaktion auf solche Vorkommnisse halte ich jedoch für keinen gangbaren Weg. Im Regelfall wird jeweils ein Gesetz oder eine Verordnung verabschiedet, die Technologie ist inzwischen aber schon weiter fortgeschritten. Die Gesetzgebung und die Regulation sind eben nur die eine Hälfte der Wahrheit, die andere Hälfte ist die Einschätzung der wirtschaftlichen und gesellschaftlichen Folgen. Die Frage, die man sich aber ebenfalls stellen sollte, ist, wie die Problematik der Cyber-Security zum Beispiel versicherungstechnisch aussieht. Dieses Thema beschäftigt die Versicherungsbranche heute sehr stark. Ist zum Beispiel ein selbst lernendes Produktionssystem überhaupt versicherbar, wenn sich seine Handlungen weder vom Hersteller noch vom Betreiber genau genug vorhersagen oder im Schadenfall nachstellen lassen? Das ist inzwischen für Versicherungsinstitute ein grosses Thema. Hier stossen aber deren momentan vorhandene Überprüfungsmechanismen an ihre Grenzen.
Hiestand: Ich denke, dass es heute wichtig ist, dass man sich dieser Problematik bewusst ist und überhaupt eine Risikoabschätzung vornimmt. Man muss heute auf solche Fälle vorbereitet sein. Klar, es ist reaktiv, aber wenigstens bis zu einem gewissen Grad kontrollierbar.
Was wir bei Siemens derzeit machen, ist, ab einer gewissen Grösse eines Projektes eine Art Zwischenschicht einzubauen. Wir haben inzwischen eine eigene Security-Abteilung, die zusammen mit dem Kunden die Sicherheitsbelange eines Systems in Form einer Thread-and-Risk-Analyse genauer unter die Lupe nimmt. Wir wollen damit den Kunden besser verstehen, was er mit den Anlagen am Ende genau machen will. Wenn wir ihm explizit aufzeigen, dass der Hintergrund darin besteht, seine Anlagen besser zu schützen, ist er auch eher dazu bereit, Geld dafür auszugeben.
Lubich: Die zweite Massnahme, die wir dann ergreifen, ist, dass wir den

Die Gesprächsrunde v. l. n. r.: Michael Rey, Roger Hiestand, Andreas Leu und Prof. Hannes Lubich.

«Anlagen werden in der Industrie zwar regelmässig gewartet, das Aufspielen von Sicherheits-Updates bei der IT-Infrastruktur wird aber bewusst oder unbewusst vernachlässigt.»

Michael Rey

Ingenieuren sagen: «Seid euch bewusst, es gibt eine Qualitätsabnahme.» Diese umfasst auch Punkte aus der IT und der Cyber-Security. Was bedeutet, dass es zum Beispiel auch einen Penetrationstest auf das Gerät gibt, das sie gerade gebaut oder integriert haben. Dabei betrachten wir ihre Lösung als eine «Blackbox», und es ist völlig egal, welche Komponente für was zuständig ist. Wir müssten also die Qualitätssicherung insofern ergänzen, dass sie die Möglichkeit hat, gegebenenfalls auch mit externen, spezialisierten Firmen solche Penetrationstests durchzuführen. Da die Infrastruktur vor Ort oft unbekannt ist, kann natürlich auch zu einem späteren Zeitpunkt ein versteckter Fehler entdeckt werden. Es ist allerdings peinlich, wenn es sich um eine offensichtliche Sicherheitslücke handelt, die schon in der Entwicklungsphase hätte entdeckt werden müssen. Zusammen gefasst braucht es beides. Einerseits eine Änderung im Ingenieurdenken, andererseits auch eine konsequente Nachkontrolle. Letzteres ist vielfach schwerer durchzusetzen, da es Prozesse verzögert und Geld kostet.

Hiestand: Für uns als Hersteller ist die Situation insofern schwierig, dass unsere Produkte oft auch von externen Unternehmen eingesetzt werden. Das bedeutet, diese kaufen die Produkte und verbinden sie als eigene Lösung irgendwo beim Kunden mit dem Internet. Für die IT-Infrastruktur vor Ort ist jeweils das Floor-Management beim Kunden zuständig. Es muss also im Interesse des Herstellers liegen, bereits bei der Entwicklung der Produkte der Sicherheit genügend Platz einzuräumen. Denn er weiss nicht, in welcher Umgebung seine Produkte am Schluss eingesetzt werden.

Lubich: In der Schweiz sind oft die kleinen und mittleren Unternehmen die Innovationstreiber. Diese sind allerdings bei einem erfolgreichen Angriff wesentlich verwundbarer, da sie im Unterschied zu grossen Konzernen keine zweite Geschäftseinheit haben oder aufbauen können, welche die Verluste kompensiert. Das betrifft innovationsstarke Länder wie die Schweiz ganz besonders. Diese KMU verlieren durch einen Angriff ihr einziges Geschäftsgeheimnis oder sind finanziell durch Umsatzausfall schneller ruiniert.

Rey: Ein KMU hat gegenüber einem Grossunternehmen auch nicht die finanziellen Mittel, solche Analysen und Tests durchzuführen. Es muss gezwungenermassen diese Dienstleistungen extern beziehen. Das ist für Start-up-Unternehmen oft nicht finanzierbar.

Hiestand: In der Schweiz herrscht zwar ein gewisses Versicherungsdenken wie zum Beispiel bei Krankheit vor. Man hofft aber, dass man die Versicherung nicht braucht. Auf Geschäftsleitungsebene ist diese Denkweise bei der Cyber-Security noch nicht angekommen, dass man auch in diesem Bereich in etwas investieren muss, das man hoffentlich gar nie braucht.

Lubich: Dazu kommen als weiterer Risikofaktor auch die modernen Engineering-Methoden. In der Informatik ist im Moment alles dem Schlagwort Agilität untergeordnet: also agile Softwareentwicklung ohne langwierige Spezifikationen. Man fängt also einfach mal an und macht danach kleine iterative Änderungen. Diese Vorgehensweise widerspricht unserer Haltung in der Cyber-Security, weil wir gern wissen möchten, was der Kunde überhaupt will. Wir wollen das Gesamtsystem verstehen, damit wir das geeignete Sicherheitssystem implementieren können. Die Softwareentwickler driften im Moment von der klassischen Vorgehensweise ab, dass sie eine Spezifikation erhalten und sie danach umsetzen. Anschliessend wird die Software nach dieser Spezifikation getestet. Alles soll heute agil und wenn möglich in der Cloud funktionieren, aber am Ende versteht keiner mehr, wie das Tool überhaupt programmiert wurde. Ich habe heute oft das Problem, die wirkliche Ursache eines Schadens festzustellen, da der Code sehr undurchsichtig und ohne Design erstellt wurde. Die heutigen Informatiker verstehen gar nicht mehr, dass ihre Software zwar virtuell in der Cloud läuft, jedoch auch physische Auswirkungen haben kann. Wenn wir daran denken, dass wir gerade bei KI bereits zu Beginn gar nicht wissen, was am Ende ein System genau macht, dann wird es schon sehr schwierig, die Auswirkungen richtig zu beurteilen.

Bekommt die Industrie die Sicherheit bei KI und IoT in den Griff? Was kann sie dabei selbst steuern, und wo ist sie von der IT (zu) abhängig? Wie lässt sich das Risiko systematisch erkennen und auf ein akzeptables Mass reduzieren?

Welchen zusätzlichen Effort müsste die Industrie leisten, und welche anderen Instanzen müssen in diesem Bereich ebenfalls mitziehen?

Hiestand: Ich bin der Meinung, dass für die Cyber-Security die KI eventuell sogar unterstützend sein kann, weil diese Sicherheit als solches gesehen auch statisch ist. Wir können uns auch selbstkritisch reflektieren und uns fragen, ob die aktuelle Herangehensweise überhaupt noch richtig ist. Gerade bei der agilen Entwicklung könnte KI helfen, die Systeme besser zu schützen. Das trifft zumindest im Moment noch am wenigstens auf die Industrie zu, da hier eher noch abgeschlossene Systeme zu finden sind.

Lubich: In der Logistik wird KI, was zum Beispiel Lagerbewirtschaftung, Transportoptimierung und so weiter betrifft, schon häufig eingesetzt. Der Mensch wird in diesem Regelkreis praktisch ausgeschlossen. Es ist schwierig, in eine solche Infrastruktur überhaupt noch einzugreifen, weil der Mensch vom System als zu langsam wahrgenommen wird. Das autonome Fahrzeuge fragt mich nicht, ob es das ABS aktivieren darf, wenn es bremsen soll, denn ich wäre in diesem Fall der langsamere und unzuverlässige Teil. Zukünftig wird es auch nicht fragen, ob es eine andere Route wählen soll. Ich kann mir durchaus vorstellen, dass sich in der Industrie je länger, je mehr Anwendungen mit KI finden. Die Problematik wird sein, dass wir viele Auswirkungen wegen der hohen Komplexität von KI nicht mehr vorhersagen können.

Inwiefern sind der Gesetzgeber und die Verbände gefordert, neue Regulatoren zu erstellen, und wie soll die Einhaltung der entsprechenden Vorgaben überprüft werden? Im E-Government-Bereich gibt es mit eCH einen Verein, der die Kommunikation mit der öffentlichen Hand standardisiert. Private Unternehmen, die E-Government-Lösungen anbieten, müssen also das Rad nicht immer neu erfinden, sondern können auf bewährte Standards zurückgreifen. Wäre ein solches Modell für die Industrie nicht auch sinnvoll?

Rey: Ein «gutes» Beispiel für eine solche Zusammenarbeit ist eben leider das Darknet selbst. Die Teilnehmer kommunizieren miteinander und helfen einander sogar. In der Industrie herrscht immer noch die Angst vor der Konkurrenz. Wir versuchen schon, einander zu unterstützen und voneinander zu lernen. Die Problematik der Cyber-Security ist inzwischen so komplex, dass wir aufeinander angewiesen sind. Die Kommunikation zu fördern, stellt jedoch eine hohe Hürde dar. Ein übergeordneter Verein wäre sicher der richtige Ansatz. Die Industrie sollte schon selbst den ersten Schritt in diese Richtung machen, nicht die Politik.

Lubich: Man muss an dieser Stelle noch zwei Dinge differenzieren, nämlich Recht und Regulation. Recht ist immer nachgeordnet, und Rechtssicherheit bekommt man nicht durch ein neues Gesetz. Denn es referenziert auf Technologien, die sich inzwischen bereits wieder verändert haben. Rechtssicherheit erhält man erst durch eine juristische Auslegung. Das dauert allerdings so lange, dass es für die Industrie kaum mehr eine Wirkung hat. Regulationen, die sich eine Branche selbst gibt, existieren nicht nur beim E-Government. Die Banken haben es vorgemacht und haben nach der Finanzkrise selbst Regulatorien entwickelt. Es war allerdings auch ein grosser Druck von der Öffentlichkeit und der Politik vorhanden, die Banken wurden praktisch dazu gezwungen. Die Behörden und die Gemeinden können als Monopolisten die Standards von eCH gar nicht ignorieren. In einem völlig freien Markt wie in der Industrie herrscht allerdings nach wie vor der Gedanke der Differenzierung gegenüber den Wettbewerbern. Dadurch wird es schwieriger, aber hier könnten die Branchenverbände wie die Handelskammern durchaus eine tragende Rolle spielen. Diese haben allerdings Bedenken, wenn sie in den freien Markt eingreifen. Wartet man auf die Politik, wird es zu lange dauern, und möglicherweise wird nur ein partielles Problem gelöst. Zudem wird die Frage der ausreichenden Verfolgung der Internetkriminalität versus die Freiheiten im Internet auch bereits parteipolitisch zerrieben, da die Parteien hier unterschiedliche Interessenlagen verfolgen. Die Politik reagiert aber oft erst auf öffentliche Empörung, wenn wieder etwas passiert ist. Erfahrungsgemäss hält danach dieser Druck nicht lange Zeit an. Wenn wir also eine ganze Industrie dazu bringen wollen, sich selbst Standards für die Informationssicherheit zu geben, dann ist das ein langer gesellschaftlicher Prozess.

«Bis ein Gesetz oder eine Verordnung verabschiedet wird, ist die Technologie inzwischen aber schon weiter fortgeschritten.»

Hannes Lubich