Dieser Professor erklärt Cyber-Sicherheit zur Chefsache

Verwaltungsrat erklärt Thomas R. Köhler ist Verwaltungsratsmitglied bei der Firma Juice Technology AG in Bachenbülach. Jetzt liegt sein Buch «Chefsache Cyber-Sicherheit» auf.

Ruth Hafner Dackermann

Thomas R. Köhler ist Verwaltungsratsmitglied bei der Juice Technology AG. Und er hat ein Buch geschrieben zur Cyber-Sicherheit. Foto: PD

Professor Köhler, beinahe täglich liest oder hört man, dass Cyberkriminelle am Werk sind. Firmen sind ebenso betroffen wie Privatpersonen. Wie gross ist die Chance, dass ein Start-up-Unternehmen wie Juice Technology durch Cyberangriffe gefährdet ist?
Jedes Unternehmen ist heutzutage durch Cyberangriffe gefährdet. Die breite Masse sieht sich eher ungezielten Angriffen ausgesetzt. Phishing-Mails kommen millionenfach vor. Sie wollen eine Person dazu animieren, auf einen mit Schadsoftware verseuchten Mailanhang oder Link zu klicken. Das ist aber meist relativ einfach zu erkennen. Schwieriger wird es, wenn Unternehmen gezielt attackiert werden. Diese Art der Attacke muss bei einem Technologieführer wie Juice Technology erwartet werden. Hier beobachten wir, dass Unternehmen erst in ihren Strukturen ausgespäht und dann gezielt einzelne Mitarbeiter angegangen werden. Derartiges ist viel schwieriger zu erkennen. Das Ziel dieser aufwendigen Attacken ist meist der Diebstahl von Informationen, insbesondere Geschäftsgeheimnissen und Entwicklungsergebnissen. Informationen, die Gold wert sein können in einem hochkompetitiven Markt wie dem der Elektromobilität.

Die Sicherheit von Ladeinfrastrukturen ist eines der grossen Themen, die mit dem Durchbruch der E-Mobilität immer wichtiger werden. Wie gross ist die Gefahr in der Schweiz?
Wenn man an Ladeinfrastrukturen denkt, denken wohl die meisten zunächst an Stecker und Kabel. Dabei ist der wesentliche Bestandteil einer Ladestation längst die Software, die den Ladevorgang steuert – oft als Lastmanagement über mehrere Stationen hinweg. Angreifer, die hier erfolgreich attackieren, können nicht nur Stromdiebstahl begehen, sondern unter Umständen auch Gefahren für die Stromversorgung heraufbeschwören. Dass dies kein theoretisches Problem ist, hat Anfang August dieses Jahres eine Studie in Grossbritannien gezeigt. Untersucht wurde die Sicherheit der Wallboxen lokaler Hersteller. Gleich bei mehreren Modellen gab es Sicherheitslücken. In einem Fall konnte man auch auf das interne Netzwerk des Gebäudes Zugriff nehmen – mit unabsehbaren Folgen. Für die Schweiz lassen sich ähnliche Szenarien nicht ganz ausschliessen, denn nicht alle Hersteller nehmen es so genau mit der Software. Das muss und wird sich ändern. Juice ist – mit seinem starken Fokus auf Software und Vernetzung – hier der Vorreiter für ein neues Bewusstsein in Sachen Cybersicherheit für die Ladeinfrastruktur.

Früher waren es vor allem Computerviren oder Trojaner, welche als Gefahr angesehen wurden. Inzwischen reden Sie in Ihrem Buch von E-Mail-Scams, Phishing-Mails, Enkeltrick für Unternehmen durch CEO-Fraud sowie Erpressung und Datendiebstahl in einem dank Ransomware. Leben wir wirklich in einer so gefährlichen Welt?
Die Cyberkriminalität hat längst den Drogenhandel in Sachen Umsatz abgelöst. Mit der umfassenden Vernetzung unserer Welt ist es auch ein weitgehend risikoloses Verbrechen, denn die Cybergangster sitzen oft in Ländern, deren Behörden es nicht so genau nehmen, insbesondere wenn die Verbrecher – wie oft – die eigene Bevölkerung schonen. Was wir in den letzten Jahren beobachten und was ich in meinem neuen Buch im Detail beschreibe, ist nun die Professionalisierung der Szene. Es gibt regelrechte Cybercrime-Start-ups, und das in verschiedenen Teilen der Welt. Das macht das Ganze so gefährlich.

Während der Corona-Pandemie wurde vermehrt im Homeoffice gearbeitet. Lauern hier zusätzliche Gefahren?
Ja, und das gleich in mehrfacher Hinsicht. Zum einen wurden von vielen Unternehmen hier Fehler bei der Einrichtung der dafür notwendigen Technologien gemacht, es musste ja alles schnell gehen. Die so unbeabsichtigt geschaffenen Lücken und Konfigurationsfehler nutzen Cyberkriminelle nun Zug um Zug aus. Dazu kommt, dass es häufig nicht gelingt, Privates und Geschäftliches sauber zu trennen. Da werden schon mal Unternehmensrechner von Familienangehörigen mitbenutzt, oder man erlaubt den Mitarbeiterinnen und Mitarbeitern im Homeoffice den Einsatz privater Geräte im Unternehmensnetz. Da sind Sicherheitsprobleme fast schon garantiert. Ein dritter Punkt ist die Vereinsamung der Menschen im Homeoffice. Wenn ich keine Kolleginnen und Kollegen habe, die ich mal eben was fragen kann, dann klicke ich vielleicht doch eher auf den Link, der mir irgendwie seltsam vorkommt.

In Ihrem Buch schreiben Sie, dass Insiderbedrohungen als der am meisten unterschätzte Bereich der IT-Sicherheit angesehen werden. Könnte dies auch auf ein Unternehmen wie Juice Technology zutreffen?
Insiderbedrohungen sind immer eine Frage der Unternehmenskultur. Unzufriedene Mitarbeiterinnen und Mitarbeiter neigen zu kriminellen Aktivitäten. Akute Geldnot liefert ebenfalls häufig einen Anstoss. Selbst Tesla war schon im Fokus einer Attacke, die dazu dienen sollte, einen Mitarbeiter als Spion anzuwerben. Doch das wurde aufgedeckt. Ich halte es für extrem unwahrscheinlich, dass Juice Technology hier Opfer eines solchen Vorfalls werden kann. Ausschliessen kann man es nicht.

Welche Massnahmen empfehlen Sie KMU generell, um mit den Gefahren aus dem Internet besser umzugehen und sich schützen zu können?
Die Mitarbeiter über die Risiken aufklären ist ebenso wichtig wie laufende Back-ups, die dann getrennt vom Unternehmensnetz gelagert werden. Ausserdem sollte man einen Notfallplan haben. Ich empfehle zudem, durch eine unabhängige Fachfirma eine Sicherheitsanalyse machen zu lassen. Hier gibt es auch verschiedene Anbieter, die das kostengünstig und weitgehend automatisch machen, sodass man sich auch als KMU dies leisten kann.

Ein Satz in Ihrem Buch lautet: «Es gibt nur zwei Arten von Unternehmen – die, die gehackt wurden, und die, die es noch nicht wissen.» Braucht bald jede Firma ihren eigenen IT-Sicherheitsexperten und lohnt sich der finanzielle Aufwand in Bezug auf den möglichen Schaden?
In jedem Fall sollte man sich fachlichen Rat holen. Das Problem bei jeder Investition in Sicherheit ist aber, dass man das nicht wirklich rechnen kann, denn im besten Fall passiert ja gerade nichts. Firewall und Virenschutz sollte jedes Unternehmen haben, ebenso wie eine Back-up-Strategie. Der Rest hängt dann davon ab, was genau das Unternehmen macht.

Neben Firmen sind auch Privatpersonen gefährdet. Was soll man machen, wenn man auf Facebook Freundschaftsanfragen aus aller Welt erhält? Wie gelangen solche Personen überhaupt an mein Profil?
Anfragen von Unbekannten sind häufig ein Einfallstor für kriminelle Aktivitäten. Man erschleicht sich so das Vertrauen einer einzelnen Person oder einer ganzen Gruppe als Basis für weitere Aktivitäten. Am besten beantwortet man keine Anfragen von Menschen, die man nicht im wahren Leben kennt, und stellt sein eigenes Profil so ein, dass es nicht jeder einsehen kann. Die grossen Social-Media-Plattformbetreiber machen es den Kriminellen leider zu leicht, an Profile Dritter zu kommen. Hier hilft – wie so oft bei Cybersicherheit – nur der «gesunde Menschenverstand».

Zur Person

Der in Deutschland wohnhafte Thomas R. Köhler ist einer der profiliertesten Vordenker zum Thema Cybersicherheit und Verfasser mehrerer Bücher zur Sicherheit im Netz. Seit vier Jahren ist der 52-Jährige Verwaltungsratsmitglied bei der Zürcher Unterländer Firma Juice Technology, welche hochwertige Ladestationen für Elektroautos anbietet und ihr Hauptquartier in Bachenbülach hat. Köhler ist seit 2019 Research Professor am Center for International Innovation der Hankou University in China. *(rh)*

Das sagt der CEO von Juice Technology

Christoph Erni ist CEO von Juice Technology AG. Zum Buch «Chefsache Cyber-Sicherheit» sagt er: «Bezüglich Cyberangriffen wie Phishing-Mails wollen wir unsere 113 Mitarbeitenden am Hauptsitz in Bachenbülach sensibilisieren, indem wir demnächst einen internen Testlauf durchführen. Wer fällt auf solche Mails herein? Totale Sicherheit gibt es nie, doch den Leuten ist viel zu wenig bewusst, wie viel Schaden angerichtet werden kann. Cybersicherheit ist tatsächlich Chefsache. Wir müssen Firmen- und Kundendaten seriös schützen – dies gehört zum strategischen Teil der Firma.

Sollte ein komplexes System wie unseres gehackt werden, würde schlimmstenfalls das ganze Gebäude durch Stromausfall lahmgelegt. Wir wären somit erpressbar. Unsere Firma ist international erfolgreich – wir könnten ein attraktives Ziel für Hackerangriffe sein. Doch dank unserer IT-Abteilung und speziellen Beratern sind wir gut aufgestellt. Allerdings darf man sich niemals in falscher Sicherheit wähnen.

Während der Corona-Krise waren unsere Mitarbeitenden oft im Homeoffice beschäftigt. Das ist brutal gefährlich, denn sehr schnell können Viren über andere PC aufgelesen werden. Ich persönlich bin kein Fan von Homeoffice. Eine Firma lebt davon, dass man sich gegenseitig austauscht. Interagieren ist äusserst wichtig.
Vor Insiderbedrohungen habe ich persönlich keine Angst. Wir vertrauen unseren Mitarbeitenden rundum. Bei Juice Technology versuchen wir immer, ein gutes Arbeitsklima zu schaffen. Zudem erstellen wir regelmässig eine Bedrohungs-Matrix: Wie gross sind die Gefahren? Mit welchem Risiko leben wir?

Totale Sicherheit ist nicht bezahlbar. Kosten für Cybersicherheit müssen in einem vernünftigen Rahmen bleiben, und auch die betrieblichen Abläufe dürfen aufgrund von Sicherheitsvorschriften nicht negativ beeinflusst werden. In Zahlen ist dies momentan nicht bezifferbar. Doch wir nehmen unsere Verantwortung wahr in Bezug auf interne Datensicherheit und sind Vorreiter bezüglich Sicherheit von Ladeinfrastrukturen.» *(rh)*