«Cybersicherheit ist ein zentraler Bestandteil von Innovation»

Reto Häni leitet seit 2016 den Bereich Cybersicherheit bei PwC Schweiz. Im Interview erläutert er, wie Unternehmen im Kontext von Digitalisierung, Vernetzung und Globalisierung ihre Denkweise ändern und ihre Systeme dosiert und möglichst sicher öffnen können.

Interview: Fridel Rickenbacher, Mitglied Redaktion swissICT, Mitbegründer und Partner MIT-GROUP

Wie diverse Studien aufzeigen, ist Cybersicherheit nicht mehr eine rein technische Angelegenheit, sondern ein strategisches Risiko und eine der drei grössten Herausforderungen für CEOs und Verwaltungsräte weltweit. Wie sehen Sie das?
Ja, das ist korrekt. Dabei umfasst die Cybersicherheit weit mehr als Technologie. Der «Global Risk Report» des World Economic Forum von 2017 führt Datendiebstahl und Cyberattacken als zwei der sechs grössten Hauptrisiken auf. Cyberrisiken sind sogar noch weiter verbreitet und eine Schlüsselkomponente bei mehr als der Hälfte der 25 wichtigsten Treiber von Risiken von neuen Technologien. In der Folge werden Cyberrisiken und damit die Cybersicherheit immer häufiger auch auf der Stufe CEO und Verwaltungsrat betrachtet. Sie gelten als Erfolgskomponenten eines Unternehmens.

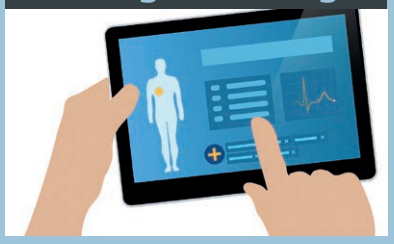
Sicherheit zu 100 Prozent gibt es bekanntlich nicht. 99 Prozent der Sicherheit wird getragen von Technologien, Prozessen und Menschen. Der Rest ist Sache des Risikomanagements. Wie ist Ihre Erfahrung?
Prozentuale Anteile zu nennen, ist hier schwierig. Doch Sicherheitsrisiken und -chancen werden heute mehr denn je Bestandteil des Risikomanagements und Restrisiken müssen entweder getragen oder auf Versicherungen transferiert werden. Dabei geht es aus meiner Sicht um mehr als nur ein Prozent. Mit der zunehmenden Professionalisierung der Gefahren ist der Mensch immer stärker überfordert. Darum müssen die Unternehmen mehr Prozesse, Technologien und Services finden, die diese wachsende Lücke schliessen.

Wo steht die Schweiz – als Land und Standort von Managed-Services-Providern – jetzt und in Zukunft im internationalen Vergleich von Cybersecurity/Cloud-Sicherheit und Resilienz, zum Beispiel von kritischen Infrastrukturen?
Es existiert eine Diskrepanz zwischen der Wahrnehmung von dem, was in der Schweiz im Cyberspace vorfällt, und den Bereichen, in denen wir in Incident-Response-Aktivitäten involviert sind. Hier stehen wir im internationalen Vergleich meines Erachtens viel schlechter da, als allgemein angenommen wird. Da hilft es auch nicht, dass wir über Probleme und Herausforderungen wenig sprechen. Hinzu kommt, dass wir in der Schweiz keine allgemeine Meldepflicht bei Vorfällen haben. Es gibt auch keine zentrale Stelle, die überhaupt eine Übersicht hat. Während die Resilienz von kritischen Infrastrukturen bezüglich traditioneller Risiken recht gross ist, haben viele Unternehmen bei der Cybersecurity noch immer einen grossen Nachholbedarf. Wie sich das in Zukunft entwickelt, hängt wohl davon ab, wann (also weniger ob) es zu einem signifikanten Cybervorfall kommt und ob dann die entsprechenden Investitionen getätigt werden.

Bis jetzt blieben wir vor signifikanten Ausfällen, wie sie zum Beispiel in Grossbritannien bei WannaCry im Gesundheitswesen vorfielen, verschont. Das wird kaum so bleiben. Die Cloud-Sicherheit ist in diesem Zusammenhang übrigens nicht nur ein Risiko, sondern auch eine wichtige Chance. Die grossen Cloud-Provider investieren überproportional viel in die Sicherheit und bieten heute Dienstleistungen an, die viel sicherer sind als das, was eine Firma selber gewähren könnte. Die Umsetzung des Datenschutzes muss allerdings seriös betrachtet werden.

«Cybersicherheit ist nicht nur Risikoreduktion, sondern ein zentrales Element, damit disruptive digitale Geschäftsmodelle gefunden, eingeführt und betrieben werden können.»

Serie Digitalisierung



In den letzten Jahren wurden einige wichtige Gesetzesvernehmlassungen, Bundesvorstösse und Standortbestimmungen für neue oder überarbeitete Gesetze wie das EPDG, DSG oder die E-ID in Angriff genommen. Diese stellen grundlegende Weichen für die Digitalisierung des Wirtschaftsstandortes Schweiz und von Fachbereichen wie dem Datenschutz, dem Schweizer Gesundheitswesen (E-Health) und der elektronischen Identität. Das swissICT Magazin beleuchtet diese Entwicklungen in einer Serie aus unterschiedlichen Blickwinkeln.

Wie beurteilen Sie die Regulierungsdichte, insbesondere auch neue, in Vernehmlassung stehende Gesetze wie das neue Datenschutzgesetz DSG und die elektronische Identität E-ID, und ihre Auswirkungen auf Schweizer Firmen?
Die Regulierungsdichte zu Datenschutz und -sicherheit war in der Schweiz in vielen Bereichen bisher gering. Mit der Revision des Datenschutzgesetzes und vielleicht fast noch wichtiger mit der neuen EU-Datenschutz-Grundverordnung (EU-DSGVO) – die übrigens auch für die meisten Schweizer Firmen zum Tragen kommt – gelten für Unternehmen in der Schweiz neue und griffigere Regeln. Zum Beispiel schreibt die EU-DSGVO «Privacy by Design» und eine Meldepflicht bei Datenverlusten vor. Das zwingt viele Firmen, ihren Umgang mit Personendaten grundsätzlich zu überprüfen. Dazu bleibt ihnen nicht mehr viel Zeit. Sie sollten möglichst schnell zumindest eine Gap-Analyse durchführen, damit sie wissen, wo sie stehen. Interessant zu wissen wäre, wie man die kommenden Regulierungen als Geschäftsvorteil nutzen kann. Ich bin überzeugt, dass sich durchdachte und transparente Datenschutzgrundlagen und -massnahmen positiv für Kommunikation und Kundenbindung nutzen lassen. Solche Überlegungen werden noch viel zu selten gemacht.

Es ist absehbar, dass das kombinierte Universum von Digitalisierung, künstlicher Intelligenz, Internet der Dinge, Clouds und Bots für die Sicherheit und den Datenschutz grosse Herausforderungen mit sich bringt. Wo sehen Sie speziellen Handlungsbedarf in einem zunehmend «analysierten» Lebens- und Arbeitsraum?
Stimmt, diese Herausforderungen bestehen. Aber die Chancen sind auch sehr gross. Cloud, Bots, künstliche Intelligenz bedeuten nicht automatisch, dass die Sicherheit abnimmt. Im Gegenteil – mit der Wahl der richtigen Plattformen kann ein Unternehmen die Sicherheit sogar erhöhen, wenn es moderne Technologien einsetzt. Eine besondere Herausforderung stellt in fast jedem Fall der Datenschutz dar. Darum muss eine Organisation bei jedem neuen Projekt und Produkt von Beginn weg beide Aspekte mit einbeziehen und neben dem Datenschutz auch die Sicherheit gleich einbauen. Dies ist speziell beim Internet der Dinge wichtig. Hier geht es um eine Vielzahl von Geräten, bei denen die Sicherheit oft kaum berücksichtigt wurde. Zudem fallen immense Datenmengen an, die von diesen Geräten zurückgemeldet werden. Das ist doppelt anspruchsvoll für die Konzeption industrieller und privater Lösungen! Hier sind auch die Benutzer dieser Endgeräte in der Pflicht. Sie dürfen nicht jede Datenschutzdeklaration einfach wegklicken, sondern sollten sich überlegen, ob sie ihre Daten wirklich preisgeben wollen und unter welchen Umständen diese verwendet werden dürfen.

«Cybersicherheit ist es nicht nur ein Technologiethema, sondern ein wichtiges Traktandum für die Geschäftsleitung und den VR.»

Wenn der Wirtschaftsstandort Schweiz an der Digitalisierung teilnehmen und diese so mitgestalten will, fehlen uns gerade Cybersecurity-Fachkräfte. Wie schätzen Sie diese Lage ein?
Ich meine, dass die Nachfrage nach Cybersecurity- und Datenschutzspezialisten in den nächsten paar Jahren deutlich ansteigen wird. Allerdings zeigt sich der Mangel nicht nur bei den individuellen Spezialisten. Auch die Breite und Tiefe der Anforderungen wächst laufend. Dadurch können einzelne Personen die gesamten Anforderungen gar nicht mehr abdecken. Dieser Herausforderungen muss sich ein ganzes Team mit einem breiten Mix von Fähigkeiten annehmen. Viele Unternehmen können schlicht kein solches Sicherheitsteam anstellen und sinnvoll einsetzen. Darum werden Firmen Sicherheitsbereiche immer häufiger direkt als Managed Service beziehen. Der Trend geht sogar so weit, dass ganze Sicherheitsbereiche ausgelagert werden. Wir sehen dies ganz praktisch sogar in Kernbereichen wie Identity und Access Management – noch vor wenigen Jahren wäre das ein Tabuthema gewesen. Solche Managed Services haben viele Vorteile. Richtig definiert und mit den richtigen Partnern bestückt, muss sich der Kunde nicht mehr um den Mix von Menschen und Talenten kümmern. Der Sicherheitsprovider stellt ihm zur richtigen Zeit und am richtigen Ort die richtigen Skills zur Verfügung. Der Provider selbst kann Synergien nutzen und effiziente Teams bilden. Das wiederum schlägt sich in der Zufriedenheit und Weiterentwicklung der Mitarbeiter nieder und der Provider kann hoch qualifizierte Mitarbeiter finden. Viele unserer Sicherheitsspezialisten motivieren sich nämlich nicht nur über die Anstellungsbedingungen, sondern weil sie in einem hoch performanten Team arbeiten können und an spannenden Aufgaben mit hohem Abwechslungsreichtum gemessen werden.

Dies ist eine gekürzte Fassung des Interviews. Das gesamte Gespräch lesen Sie unter: **www.swissict.ch/interview-haeni**

Reto Häni

Reto Häni ist seit 2016 Partner bei PwC Schweiz, Mitglied des PwC-Digital-Services-Führungsteams und leitet den Bereich Cybersicherheit, eine multidisziplinäre Gruppe von Spezialisten in den Bereichen Cybersicherheit, Technologierisiko und Forensik. Diese bieten das komplette Spektrum von Cyberrisiko- und Resilienzdienstleistungen an, von der Strategie über das Design und die Umsetzung bis zum Betrieb.
Zuletzt war Häni als Chief Security Officer Western Europe für Microsoft tätig. Davor arbeitete er unter anderem als Gruppen Chief Information Officer (CIO) für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport sowie für die ETH in Zürich. Während der letzten 17 Jahre spezialisierte er sich auf Cybersicherheit, Datenschutz, Cloud-Sicherheit und Compliance sowie Unternehmens- und IT-Risk-Management.