Das WEF im Zeichen der IT: Cybersecurity unter globalen Top-5-Risiken

Gabriel Gabriel

Auf dem Weltwirtschaftsforum (WEF) letzte Woche in Davos standen bemerkenswert viele IT-bezogene Veranstaltungen auf dem Konferenzprogramm. Dementsprechend prominente Vertreter namhafter Firmen, Organisationen und Forschungseinrichtungen referierten daher auch über Belange der IT, welche heute und in Zukunft auf die Wirtschaft und unsere Gesellschaft Einfluss haben. Eines der ganz zentralen Themen war dabei die vierte industrielle Revolution und damit die Frage, wie sichergestellt werden kann, dass Technologien von morgen unser Leben besser und nicht schlechter machen.

Konzernchefs wie Satya Nadella (Microsoft), Ginni Rometty (IBM), Hiroaki Nakanishi (Hitachi), Bill McDermont (SAP) oder Michael Dell (Dell Technologies) – um nur einige zu nennen – beschäftigten sich in ihren Vorträgen und Diskussionsbeiträgen bei Podiumsgesprächen denn auch mit (digitaler) Globalisierung, Industrie 4.0 und selbstverständlich auch mit Künstlicher Intelligenz (KI). Microsoft-Schweiz-Chefin Marianne Janik meinte in einem Beitrag der Tagesschau des Schweizer Fernsehens

SRF, viele Menschen fragten sich, ob das WEF eigentlich eine Technologie-Konferenz sei. Gleichzeitig begrüsste sie den Hype um KI. Denn er fördere die Diskussion darüber, wie wir Menschen damit umgehen wollen.

Cybersecurity fünfgrösstes Risiko der Welt

Ein weiteres vieldisk

utiertes IT-Thema war Cybersicherheit. Nicht zuletzt, weil der Ausfall kritischer Informationsinfrastrukturen, Datendiebstahl und Cyberattacken – neben Ereignissen wie Naturkatastrophen, ungewollter Migration, Massenvernichtungswaffen, übertragbarer Krankheiten oder Scheitern des Klimaschutzes – im aktuellen Global Risks Report des WEF zu den zehn wahrscheinlichsten und folgeschwersten Risiken zählen. Interessant dabei: Internetangriffe rangieren überhaupt erst seit 2014 unter den Top-5-Risiken. Das Risiko von Datendiebstahl und -missbrauch liegt in Bezug auf die Eintrittswahrscheinlichkeit sogar noch vor den Cyberangriffen.

Cyber-Sicherheit zu komplex für einzelne Unternehmen

Nicht umsonst hat das WEF erst kürzlich die Neugründung des Center of Cybersecurity bekanntgegeben, welches Verträge mit Europol, Interpol, der Nationalen Cyber-Behörde Israels, der Organisation Amerikanischer Staaten, dem Nationalen Cyber-Sicherheitszentrum des Vereinigten Königreichs, dem UC Berkeley Center für langfristige Cybersicherheit sowie mit der Global Cyber Alliance unterzeichnete. Das Center for Cybersecurity hat wie viele Staaten, Organisationen und Firmen den «Pariser Aufruf für Vertrauen und Sicherheit im

Cyberraum» unterzeichnet. Unlängst gab auch die Zürich Versicherung bekannt, bei der neuen WEF-Organisation dabei zu sein. Der Konzern geht davon aus, dass in den nächsten fünf Jahren die Kosten aufgrund von Attacken auf Unternehmen weltweit auf acht Billionen Dollar ansteigen werden. Die neue WEF-Initiative lud in Davos zu einem offenen Forum ein.

Kernaussage der Diskussion: Einzelne Organisationen, Länder und Unternehmen können heutzutage die Probleme – wie etwa vor zwei Jahren die verheerenden Auswirkungen der Schadsoftware Wannacry – nicht mehr allein in den Griff bekommen. Da weltweit Informationen geteilt würden, stünden alle vor denselben Herausforderungen. Diese seien aber bei den Betroffenen nach wie vor ein Tabuthema. Unternehmen würden kriminalisiert, wenn Daten verloren gehen und fürchten Imageverluste, während die Täter meistens unerkannt und unbestraft bleiben. Ins selbe Horn stösst UN-Generalsekretär Antonio Gutierres, welcher statt harten Massnahmen weiche Mechanismen fordert. Alle Beteiligten – IT-Anbieter, Wissenschaft, Wirtschaft und zivilrechtliche Organisationen – müssten gemeinsame Normen und Protokolle entwickeln, um dem Problem Herr zu werden.

Mitarbeiter sensibilisieren und sichere Werkzeuge anbieten

Walter Bohnmayr, bei der Boston Consulting Group weltweit für IT-Sicherheit zuständig, warnt, Mitarbeiter seien viel zu wenig geschult. Cybersecurity sei ein ganzheitliches Problem der Unternehmen, nicht ein IT-Problem. Fakt ist: die mit Risiken hinsichtlich der Informationssicherheit behaftete Verwendung von privaten Geräten im Geschäftsleben (Bring Your Own Device) ist heute beim Grossteil der Unternehmen nicht mehr zu verhindern. Unternehmen müssen allerdings auch beim Einsatz von Unternehmensgeräten sicherstellen, dass Mitarbeitende Regeln beachten und keine private Tools wie Dropbox oder

Whatsapp für den geschäftlichen Gebrauch verwenden, die Unternehmensanforderungen an Compliance, Sicherheit und Datenschutz nicht genügen. Das funktioniert allerdings nur, wenn für das Teilen und Bearbeiten von vertraulichen Informationen Werkzeuge verwendet werden, die nicht nur durch den neuesten Stand entsprechende technologische Vorkehrungen garantieren, sondern diese auch mit anerkannten Zertifizierungen nachweisen können. Darüber hinaus müssen diese Lösungen einfach bedienbar und benutzerfreundlich sein. Denn ebenfalls klar ist: Ohne eine hohe Akzeptanz und Nutzerzufriedenheit werden die Mitarbeiter die Lösungen nicht einsetzen, sondern weiter auf unsichere Wege ausweichen und den Verlust vertraulicher Informationen, Know-how, die Wettbewerbsfähigkeit und das Überleben des Unternehmens riskieren.