Handelszeitung Nr. 21, 23. Mai 2019

Cybercrime Kein Generalverdacht!

«Blosses Hoffen auf Vertrauen wäre fahrlässig.»

Christoph Hilber
Managing Partner, P-Connect

Unsere Welt wird unsicherer – auf vielen Ebenen. Die Internationale Sicherheitskonferenz in München zeigte auf, dass diplomatische Politik einer aggressiven Diplomatie weicht und im Hintergrund die Messer gewetzt werden. Konventionelle Waffen werden vorgeführt, während unsichtbar für mögliche Cyber-Angriffe aufgerüstet wird. Mit dem Internet der Dinge dürfte die Cyber-Option zunehmend effektiv und vor allem viel schneller werden.

Immerhin: Auf Cyber-Angriffe sind viele Unternehmen vorbereitet. In einer Umfrage bei Verwaltungsräten antworteten 70 Prozent, dass ihre Firmen schon einmal angegriffen wurden. Jedoch sind nur 40 Prozent der Unternehmen überzeugt, einen Angriff rechtzeitig zu entdecken. Wer noch nie gehackt wurde, hat es vielleicht einfach nicht gemerkt. Wer über lukrative Geheimnisse verfügt wie Patente, Innovationen und so weiter tut gut daran, seine IT-Systeme sehr genau unter Kontrolle zu halten. Der wahre Luxus in diesem Zusammenhang, nämlich nichts Interessantes oder Wissenswertes zu besitzen, ist keine interessante Option.

Auf der dritten Ebene der Unsicherheit wird es emotional herausfordernd. Während auf den ersten beiden Ebenen mit logischen oder physischen Gegenmassnahmen reagiert werden kann, spielt in der dritten Vertrauen – oder Misstrauen – eine Rolle. Der «Forensic Fraud Barometer» von KPMG lässt aufhorchen: Kader sind die Haupttäter bei Wirtschaftsdelikten – und es ist mit einer hohen Dunkelziffer zu rechnen. Das müsste vor allem den Verwaltungsräten grosse Sorge bereiten, bedeutet dies doch, gegenüber dem selbst ernannten Management misstraulsch zu sein. Und jeder Mitarbeiter, jede Mitarbeiterin könnte in Versuchung geraten, mit Geheimnissen in die eigene Tasche zu wirtschaften.

Faire Bezahlung und Respekt dienen der inneren Sicherheit

In jedem Manager und jedem Mitarbeitenden einen Wirtschaftskriminellen zu sehen, ist allerdings wohl übertrieben. Leider gibt es für diese Ebene keinen Virenscanner, sondern nur die Kontrolle über konsequent gelebte Prozesse. Über Cyber-Hygiene auf mögliche Bedrohungen oder Diebstähle zu sensibilisieren, dürfte zu kurz gegriffen sein. Eine Kultur der Wertschätzung, der Offenheit, des Respekts und der fairen Bezahlung zu schaffen, ist zwar anspruchsvoller, jedoch ein wirkungsvolles Werkzeug für die innere Sicherheit.

Das Gute ist, dass das Thema Cybersecurity bereits eine Industrie ist, sehr lukrativ und mit stellen Wachstumskurven. Auf einen Hack folgt umgehend ein Update, ein Gegenhack. Das Geschäftsmodell funktioniert allerdings etwas anders als andere. Während die klassische Innovation darauf beruhte, ein Produkt oder eine Dienstleistung schneller, präziser, günstiger zu entwickeln, besteht im Cyberwar ehrliche Innovation in der Geschwindigkeit bei der Identifikation und Bekämpfung einer unehrlichen Innovation.

Wir sollten uns nicht hinreissen lassen, in jedem und jeder einen Feind zu vermuten. Jedoch müssen wir misstrauischer werden. Hoffen auf Vertrauen wäre fahrlässig. Wo es hinter einer offenen Türe etwas zu holen gibt, wird es jemand holen. Wenn unsere Autos selbstständig fahren und die Wertschöpfungskette vernetzt ist, wird Vorsorge besser sein als Heilen, misstrauenbasierte Entwicklung besser als der Glaube an das Gute. Für einige Industrien ist das möglicherweise Neuland.