Swisscom-Studie zu Cyber Security Mit dem permanenten Risiko leben

Wegen der rasenden Geschwindigkeit der Digitalisierung sind sichere IT-Systeme eine Illusion. Wirtschaft und Politik sollten weniger den perfekten Schutz anstreben, als die Handhabung von Gefahren verbessern.

Studien zur IT-Sicherheit gibt es viele, am Dienstagmorgen hat nun auch die Swisscom einen Bericht zu «Cyber Security» herausgegeben. Im Gegensatz zu den Gutachten von Sicherheitsfirmen wie Kaspersky oder Symantec sucht man in der nur rund 24 Seiten dünnen Broschüre des Schweizer Telekomunternehmens vergeblich nach Zahlen. Was einen zuerst etwas enttäuscht, entpuppt sich bei der Präsentation durch Stefan Frei, Sicherheitsexperte bei Swisscom, als willkommene Abwechslung.

Grenzen der Effizienz

In seinem Referat unterscheidet Frei zwei grundsätzlich unterschiedliche Bedrohungsarten. So gebe es zum einen mehr von bestehenden und bekannten Angriffen; in diesem Bereich kommen die quantitativen Studien von Firmen zum Zug, die sich auf Internet-Sicherheit spezialisiert haben. Zum anderen erlaube aber die rasante Entwicklung der Technologie auch immer neue Verknüpfungen, die zu prinzipiell nicht vorhersehbaren Attacken führen könnten.

Ein Beispiel wäre hierzu die Kombination von Drohnen mit modernen Hochfrequenzsendern (Software Defined Radio, SDR): Mit dem unbemannten Fluggerät können physische Zugriffsbeschränkungen wie Zäune umgangen und mit dem SDR-Gerät schliesslich die drahtlose Kommunikation auf bisher unzugänglichem Gelände abgehört oder gestört werden. Solche Geschichten klingen für die meisten nach James-Bond-Filmen, die rasante technologische Entwicklung machen allerdings die dafür notwendigen Geräte für einen immer grösseren Personenkreis erschwinglich und bedienbar.

«Bereits kompromittiert»

Um mit unvorhersehbaren Bedrohungen umzugehen, empfiehlt es sich, bei IT-Systemen eine gewisse Redundanz einzuplanen – keine einfache Aufgabe in einem wirtschaftlichen Umfeld, in dem Effizienzsteigerungen oft überlebenswichtig sind. Doch Redundanz scheint wichtiger zu sein als die Erhöhung von Abwehrmassnahmen. Laut Frei müssen wir nämlich davon ausgehen, dass wichtige Infrastrukturen in der Schweiz – und auch bei seinem Arbeitgeber der Swisscom – bereits kompromittiert sind. Daher sollte es in erster Linie darum gehen, mit diesen Schwachstellen umzugehen. Unternehmen sollten Prozesse definieren, die bei der Aufdeckung einer Sicherheitslücke zum Zug kommen.

Ein Beispiel für ein solches Schwachstellen-Management sind die regelmässigen und teilweise

automatisierten Updates, die Softwarefirmen herausgeben. Hier weist Frei explizit darauf hin, dass bei der Entwicklung des «Internets der Dinge» von diesen früheren Erfahrungen gezehrt werden sollte. Nur so könne verhindert werden, schmerzliche Fehler zu wiederholen.

Überfordernde Geschwindigkeit

Auch wenn der Swisscom-Bericht viele Gefahren aufzeigt und künftige Bedrohungen benennt, als Schwarzseher will sich Frei nicht bezeichnen. Laut ihm wird nicht alles schlechter, sondern es wird alles anders – und das mit rasender Geschwindigkeit. Dies schaffe Möglichkeiten für Kriminelle, die immer etwas schneller als die Behörden seien. Als Beispiel nennt er die Einführung des Automobils: In Frankreich hätten Räuber bereits früh diese Innovation genutzt, um der berittenen Polizei einfacher zu entkommen.

Die Geschwindigkeit der Digitalisierung gibt agilen Kriminellen aber nicht nur einen Vorteil, sondern sie überfordere laut Frei auch die Gesellschaft. Der Umgang mit den neuen Möglichkeiten müsse erst gelernt werden. Teilweise könne dies auch zu Kurzschlusshandlungen in der Politik führen.

Der Sicherheitsexperte erwähnt in der Studie erstaunlicherweise die Gesetzgebung als eine Bedrohung. Darauf angesprochen meint Frei, dass die Politik unter anderem Software verbieten wolle, die dazu genutzt werden könne, in fremde Systeme einzudringen. Die Analogie zu einem Verbot von Waffen ist offensichtlich, weshalb die Gesetzesänderung auf den ersten Blick einleuchtet. Doch auch Firmen wie Swisscom nutzen solche Programme, um ihre eigenen Systeme zu testen. Damit hat die Gesetzesänderung trotz löblichen Absichten das Potenzial, am Ende die IT-Sicherheit sogar zu vermindern. Wie für Unternehmer gilt auf für Politiker: Statt perfekten Schutz anzustreben, sollte die Handhabung von Risiken und bestehender Sicherheitslücken im Vordergrund stehen.