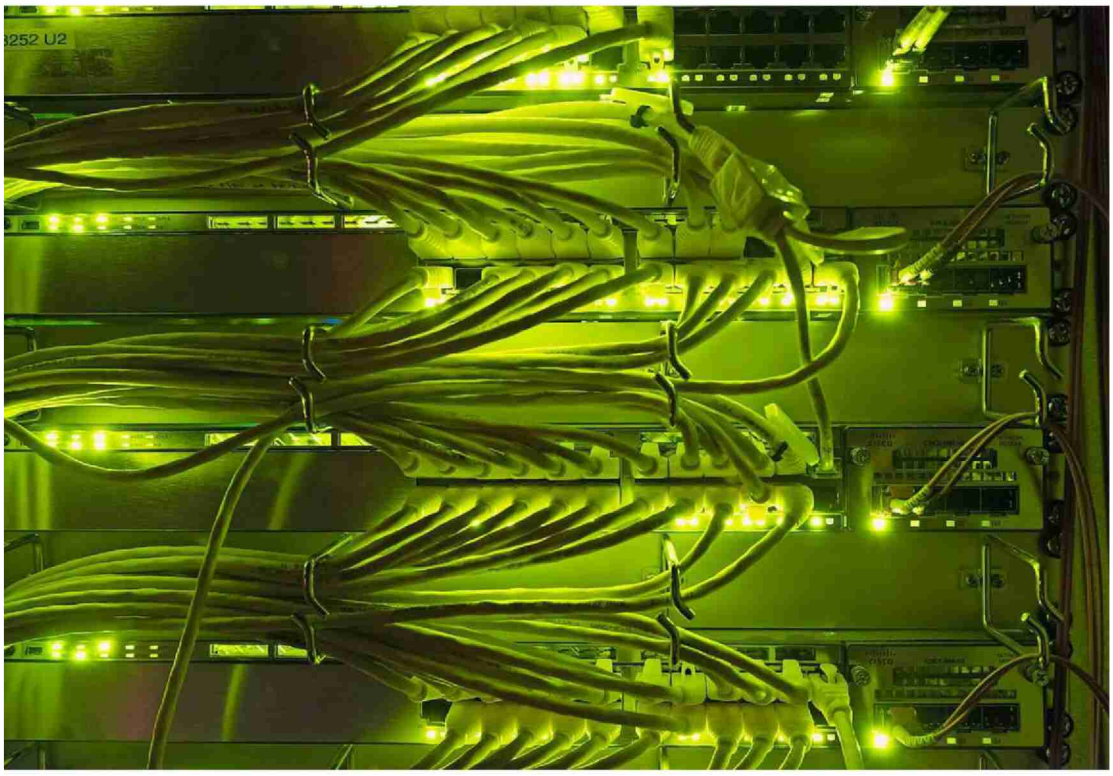
Der Bund

Datum: 28.08.2018

Uneinigkeit bei der Cyberabwehr

Sicherheit Viele Unternehmen sind ungenügend gegen Attacken aus dem Internet geschützt. Der Bund will ihnen helfen – mit freiwilligen Massnahmen. Politiker zweifeln, dass das reicht.



Minimalstandards sollen Infrastrukturen besser vor Cyberangriffen schützen. Foto: Urs Jaudas

Christoph Lenz

Hört man Experten in Sachen Cybersicherheit zu, so wähnt man sich bisweilen inmitten eines Science-Fiction-Abenteuers: Der Cyberkrieg ist längst Realität. Täglich, wenn nicht stündlich, werden Grossunternehmen, staatliche Stellen und kritische Infrastrukturen angegriffen. Ja, auch in der Schweiz. Und man muss von Glück sprechen, dass die Attacken nur selten so erfolgreich sind wie im Fall der bundeseigenen Rüstungsschmiede Ruag 2016.

Umso alarmierender sind die Antworten auf die Frage, wie gut Schweizer Unternehmen für Cyberangriffe gerüstet sind. «Die meisten Schweizer Firmen sind blind», sagt etwa Reto Häni, Chef der IT-Sicherheit bei der Beratungsfirma PWC. Die Firmen erkennen also nicht, wer sie attackiert. Sie merken vielleicht nicht einmal, dass sie angegriffen werden (so wie die Ruag).

Eigene Lösungen gefragt

Diesem Problem wollen Reto Häni und das Bundesamt für wirtschaftliche Landesversorgung (BWL) entgegenwirken. Gestern haben sie in Bern einen Minimalstandard für Informations- und Kommunikationsrisiken in Schweizer Unternehmen vorgestellt. Über hundert konkrete Handlungsanweisungen sollen Firmen helfen, ihre Resilienz gegenüber Cyberrisiken zu verbessern. Die Massnahmen reichen von der Analyse von Bedrohungen über die Schulung der Mitarbeiter bis hin zu anspruchsvollen Verifikationen der benutzten Software.

Der Bund

Datum: 28.08.2018

Muss jetzt jeder Bäcker und jede Taxi-Unternehmerin die Mitarbeiter zur IT-Schulung schicken? Natürlich nicht. Der Bund setzt bei seinem Massnahmenpaket auf Freiwilligkeit. Selbst den Betreibern von kritischen Infrastrukturen, etwa Stromnetzen oder der Wasserversorgung, wollen die Beamten nicht vorschreiben, welche Sicherheitsvorkehrungen sie einhalten müssen. Man vertraue darauf, dass bei den besonders schützenswerten Infrastrukturen die Branchenverbände eigene Lösungen entwickelten, erklärte gestern Werner Meier, der BWL-Delegierte. «Falls diese Vereinbarungen nicht greifen, können Massnahmen für verbindlich erklärt werden.»

Jeder Vorfall eine Meldung?

Die Zurückhaltung des Bundes irritiert die Politik. Nationalrätin Edith Graf-Litscher (SP, TG) sieht im gestern vorgestellten Minimalstandard zwar einen Schritt in die richtige Richtung. Bei kritischen Infrastrukturen sei eine Meldepflicht für Cybervorfälle aber überfällig, sagt sie, die schon 2017 einen Vorstoss für eine Meldepflicht durchs Parlament brachte. «Wenn etwas passiert, müssen die Experten vom Bund das erfahren. Nur so können sie die Gefahrenlage richtig einschätzen, vor Bedrohungen warnen und mögliche Folgeschäden von Attacken eingrenzen.» Ihr schwebe eine möglichst unbürokratische Meldepflicht vor. Zudem müsse sichergestellt sein, dass Unternehmen ihre Meldungen auch anonym eingeben könnten. «Aber dass der Bund hier vorwärtsmachen muss, ist für mich absolut klar.»

Auch Nationalrat Marcel Dobler (FDP, SG) fordert, dass der Bundesrat eine Meldepflicht ausarbeitet für die sehr kritische Infrastruktur. Diese müsse jedoch differenziert ausgestaltet sein: «Bei schweren Cyberattacken auf AKW und die Trinkwasserversorgung ist klar, dass eine harte Meldepflicht angezeigt ist. Bei weniger kritischen Infrastrukturen sollten die Auflagen weniger streng sein», so Dobler.

Im BWL sieht man derweil eher die Nachteile: Die Meldepflicht berge auch Risiken, sagte gestern der BWL-Delegierte Werner Meier. «Vielleicht erfahren wir aufgrund unserer informellen Gespräche heute mehr über die Vorfälle in der Wirtschaft, als wenn eine starre Meldepflicht eingeführt wird.»

Verfahren gegen Hacker eingestellt

Ruag Die Bundesanwaltschaft hat das Strafverfahren zum Cyberangriff auf den Rüstungskonzern Ruag sistiert. Die Täterschaft habe nicht eruiert werden können, sagte Sprecher André Marty am Montag zu Radio SRF. Zweieinhalb Jahre hat die Bundesanwaltschaft ermittelt wegen wirtschaftlichen Nachrichtendiensts, also wegen Spionage gegen die Ruag. Beim Angriff, der über ein Jahr gedauert hatte und erst im Januar 2016 entdeckt wurde, waren grosse Datenmengen entwendet worden.

Gemäss früheren Medienberichten gab es deutliche Hinweise darauf, dass der Angriff auf die Ruag von Russland ausging. Offiziell bestätigen will das die Bundesanwaltschaft aber nicht. Sprecher Marty sagte lediglich: «Ganz grundsätzlich und nicht direkt bezogen auf ein konkretes Strafverfahren kann man sagen, dass natürlich bei dermassen komplexen Realitäten meistens nur staatliche Akteure infrage kommen: Das kostet zu viel Geld und braucht enormes Know-how – das ist in der Regel staatliches Hacking.»

Erfahrungsgemäss bittet die Schweiz bei politischen Delikten wie Spionage mögliche Täterstaaten gar nicht erst um Rechtshilfe. Sprecher Marty lässt offen, ob die Bundesanwaltschaft im Fall Ruag Russland oder andere Staaten um Hilfe gebeten hat – er sagt aber: «Rechtshilfe macht dann Sinn, wenn ich davon ausgehen darf, dass eine Behörde im Ausland auch ein Interesse daran hat, meine Fragen zu beantworten. Sonst macht das relativ wenig Sinn.» *(sda/red)*