16. März 2016 20 Minuten

«Was, wenn ein Stausee fremdgesteuert wird?»

Sicherheitspolitiker verurteilen die Mega-Attacken auf Schweizer Webshops. Sie sehen die Firmen und den Staat in der Verantwortung.

«Was, wenn plötzlich ein Stausee fremdgesteuert ist oder ein Trafo ausgeschaltet wird?», fragt Balthasar Glättli (Grüne). Er fordert eine klarere Regelung der Verantwortlichkeiten bei der Informatiksicherheit. Im Bild: die Staumauer am Lac des Dix.

Bild: Keystone/Alessandro Della Bella

Die neue Qualität der Attacken beunruhigt Sicherheitspolitiker von links bis rechts. Für CVP-Nationalrat Jakob Büchler etwa zeigen die Ereignisse schmerzhaft, wie «verletzlich unsere Gesellschaft für Cyberkriminalität geworden ist». Die Schweiz habe eine nationalen Strategie gegen Cyber-Risiken beschlossen und mache vieles richtig. Doch der Kampf gegen die Kriminellen müsse noch entschlossener geführt werden als bis anhin.

«Attacke ist ein Warnschuss»

Patentrezepte, wie man den Cyberkriminellen das Handwerk legen könnte, haben die Parlamentarier keine. So sagt FDP-Nationalrat und Digitec-Co-Gründer Marcel Dobler, dass der Staat Privaten kaum helfen könne. «Die Angriffe sind strafbar, allerdings ist es fast ein Ding der Unmöglichkeit, herauszufinden, wer dahinter steckt.»

Firmen sähen sich immer wieder mit Erpressungen konfrontiert. Wie viel man in die Abwehr der Attacken investiere, müsse jedes Unternehmen abwägen. «Um eine DDoS-Attacke abzuwehren, braucht es enorme Rechenleistungen, was sehr kostspielig ist», sagt Dobler. Auf der anderen Seite könne eine solche Attacke für einen Online-Händler wie Digitec teuer werden. «Besonders schlimm sind Attacken, die nicht nur den Webshop lahmlegen, sondern auch das interne System.» Ein solcher Stillstand, der 500 Mitarbeiter am Arbeiten hindere, koste schnell hunderttausende Franken pro Tag.

Auch SVP-Sicherheitspolitiker Thomas Hurter sieht die Wirtschaft in der Verantwortung. «Bei der IT-Sicherheit ist wie beim Sport: Man muss ständig trainieren, damit Muskeln vorhanden sind.» Die Attacke sei ein Warnschuss, die Dispositive zu überprüfen. Mit der Meldestelle Melani gebe es zudem eine staatliche Anlaufstelle, wenn Firmen Hilfe bräuchten. Dort, wo ein öffentliches Interesse bestehe oder die Schweiz bedroht sein könnte, erlaube zudem das neue Nachrichtendienstgesetz, Aktivitäten Cyberkrimineller besser zu überwachen.

Kritische Infrastrukturen genügend geschützt?

In seinem Sicherheitspolitischen Bericht warnt der Bundesrat aber auch vor Cyber-Angriffen auf kritische Infrastrukturen wie die Stromversorgung und die Telekommunikation. Ein Angriff könne «einen grossräumigen Stromausfall zur Folge haben, der seinerseits die meisten Funktionen von Wirtschaft und Gesellschaft zum Erliegen bringen würde», heisst es im Papier.

Laut dem Grünen Balthasar Glättli ist die Schweiz ungenügend auf solche Gefahren vorbereitet: «Wenn ich ein paar Stunden kein SBB-Ticket lösen oder keinen TV bestellen kann, ist das verkraftbar.» Sei aber die Stromversorgung betroffen, gehe es an das Eingemachte. «Was, wenn plötzlich ein Stausee fremdgesteuert ist oder ein Trafo ausgeschaltet wird?», fragt Glättli. Das Eidgenössisches Starkstrominspektorat Esti definiere heute, wie hoch ein Zaun um eine Anlage sein müssen, überprüfe die IT-Sicherheit aber nicht. «Die Verantwortung für die Informatiksicherheit muss klar geregelt werden.»

Mit dem Thema wird sich demnächst die Sicherheitspolitische Kommission befassen, wie Präsidentin Corina Eichenberger (FDP) bestätigt. Eichenberger selbst sieht die Lösung weniger in einem strengeren Gesetz, als in der Sensibilisierung und Ausbildung. «Zudem müssen wir die internationale Zusammenarbeit stärken, um Cyberdelikte besser ahnden zu können.»

(daw)