Von Firewalls und Schwarzen Löchern

Es war ein kühler und windiger Aprilmorgen, an dem die Bürger Estlands, und mit ihnen die Nato, in einer neuen Realität aufwachten: Cyberangriffe, die seit Tagen auf die IT-Infrastruktur des kleinen baltischen Staates einhämmerten, hatten einzelne Teile des estnischen Netzwerkes lahmgelegt — und damit Webseiten von Banken, Behörden, Zeitungen und des estnischen Parlaments blockiert.

Wenn auch nicht der erste Angriff auf ein Bündnismitglied im Cyberspace, so war im April 2007 doch das erste Mal auch für den Otto Normalbürger spürbar, dass etwas Großes passiert. Selbst wer an diesem Tag in Estland nicht mit Behörden oder Banken kommunizieren musste, konnte sehen, dass Nachrichtenforen mit Kommentaren zugespammt, Webseiten gekapert und inhaltlich entstellt wurden — Fachleute sprechen von „trolling" und „defacement".

Wer sich schützen will, muss seine Infrastruktur kennen.

Der Februar 2016: Die Nato hat Cyberangriffe mittlerweile zum möglichen Bündnisfall nach Art. 5 des Washingtoner Abkommens erklärt, und nicht erst seit dem Einbruch in die IT-Infrastruktur des Deutschen Bundestages wird auch in der deutschen Sicherheitspolitik diskutiert, wie kritische Infrastruktur gegen Cyberangriffe geschützt werden kann. Dieser Diskussion stellt sich auch der Bundesverband Sicherheitspolitik an Hochschulen (BSH): Die Heidelberger Sektion des BSH und die studentische Gruppe der Netzpolitik-AG, ein interdisziplinärer Zusammenschluss Heidelberger Nachwuchswissenschaftler, luden daher Anfang des Monats beim Frankfurter Internetknotenpunkt DE-CIX zu Fachgesprächen über die deutsche Cyber-Infrastruktur.

Das Rückgrat deutscher IT-Infrastruktur

Der DE-CIX als weltweit größter Internet-Knotenpunkt befördert in Spitzenzeiten 5.1 Terabits pro Sekunde an „traffic" — in E-Mails umgerechnet wären das 5,1 Milliarden digitale Briefe pro Sekunde. Doch nicht nur E-Mails werden hier weitergeleitet: Ein solcher Knotenpunkt ist, bildlich gesprochen, ein Autobahnkreuz für Daten: Videos, Skype, Internetbanking und Facebook. Ist das baltische Szenario damit auch für Deutschland denkbar?

Foto: Lucas Nußbaumer

Besuch im DE-CIX: Die deutsche IT-Infrastruktur ist gut aufgestellt, aber es bleibt ein ewiger Rüstungswettlauf im Cyberspace

Die genauen Sicherheitsvorkehrungen sind aus guten Gründen nicht öffentlich — aber in die grundsätzlichen Techniken gaben die Mitarbeiter von DE-CIX den Teilnehmern der Exkursion einen umfassenden Einblick. Beispiel Estland: Einen Angriff wie im Jahr 2007 würde nicht den DE-CIX treffen, sondern die Zielnetzwerke, z.B. einer Bank oder eines Ministeriums. Zum Schutz des Zielnetzwerks kann der DE-CIX „blackholen": der gesamte Traffic des Angriffs würde ins Nichts — in das sprichwörtliche Schwarze Loch — umgeleitet werden und dort wirkungslos verpuffen. Die Leitungen am Endpunkt blieben somit frei für den digitalen Puls der Bundesrepublik.

Cybersicherheit – gemeinsame Aufgabe aller!

In der angeregten Diskussion mit dem Team des DE-CIX wurde insbesondere auch die Rolle des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik (BSI) diskutiert. Das Team ging auch auf Fragen ein, die nicht zum Kerngeschäft des Internetknotenpunkts gehören, bei denen jedoch technische Expertise sehr gefragt war. So wurden Big Data und die Frage der Souveränität im Cyberspace ebenso angeregt und offen diskutiert wie physische Bedrohungen kritischer IT-Infrastruktur.

Das Fazit der Teilnehmer: Die deutsche Infrastruktur ist gut aufgestellt, aber es bleibt ein ewiger Rüstungswettlauf im Cyberspace. Das zweite Fazit: Die Diskussion über Cybersecurity in Deutschland ist noch lange nicht vorbei. Oder, wie es Dr. Wolf J. Schünemann, Sprecher der wissenschaftlichen Sektion der Netzpolitik AG, ausdrückte: „Wenn eine derart kritische Infrastruktur wie der DE-CIX von einem relativ kleinen Stab junger Mitarbeiter gesteuert, verwaltet und geschützt werden kann, scheinen die Fähigkeiten für IT-Sicherheit in Deutschland vorhanden zu sein. Die neue Herausforderung „Cybersicherheit" im Auge zu behalten und diese Fähigkeiten zur Wirkung zu bringen wird zukünftig eine gemeinsame Aufgabe von Forschung, Privatunternehmen, Politik – und nicht zuletzt unserer Gesellschaft – sein."

Henning Walravens