

Cyber-Terrorismus ist im Aufwind

06.09.2011 | 13:45 | Stefan Mey (wirtschaftsblatt.at)

Nach 9/11 gab es Änderungen im Flugverkehr, aber kaum in der IT-Security. Dabei zeigen jüngste Fälle, dass Angriffe starken Schaden anrichten.

Als im Jahr 2009 der Virus "Conficker" 3000 PCs der Kärntner Landesregierung lahmlegte, kostete die Wiederherstellung 2500 Personalstunden, es fielen sieben Arbeitsjahre aus, da die Bediensteten ohne PC nicht arbeiten konnten. Ein ähnliches Bild 2007 in Estland: Politische Spannungen um die russische Minderheit führten zu Cyber-Attacken gegen das Land - Internet-Provider wurden lahmgelegt, die beiden größten Banken des Landes angegriffen, die Regierungskommunikation versagte. Im Jahr 2003 wiederum waren von einem Stromausfall in den USA und Kanada 50 Millionen Menschen betroffen - Telefone und Wasserversorgung fielen aus, der öffentliche Verkehr brach zusammen. Auch hier wird der Zusammenhang mit einem Cyber-Angriff nicht ausgeschlossen.

Cyber-Terrorismus ist im Aufwind - nicht zuletzt auf Grund der vergleichsweise geringen notwendigen Mittel: Einem Vortrag des Abwehramts auf der FH Hagenberg zufolge reichen für einen Angriff über Würmer und Botnetze eine Vorlaufzeit von 18 bis 24 Monaten und Finanzmittel von zehn Millionen €. Durch den Angriff auf die IT-Infrastruktur eines Landes kann alles geschädigt werden, was digital kommuniziert.

Und die Zuliefernden Unternehmen haben nicht selten einen daraus resultierenden Image-Schaden: Nachdem im Herbst 2010 ein iranisches Atomkraftwerk Opfer eines Cyber-Angriffs über den Wurm Stuxnet geworden war, stand die Firma Siemens im Zentrum der Kritik: Verschiedene Institutionen warnten vor Sicherheitslecks im Siemens-System, der Konzern wies die Vorwürfe zurück.

Nicht genug geschützt

Eine weitere Bedrohung für Unternehmen: Sie könnten Kollateralschaden bei einem Cyberangriff davon tragen, obwohl sie gar nicht Primärziel des Angreifers waren, sagt Josef Pichlmayr, Geschäftsführer des österreichischen Sicherheitssoftware-Unternehmens Ikarus: In der Schusslinie steht etwa, wer Zulieferer ist, für das Opfer Hosting betreibt oder einfach nur an der gleichen Leitung hängt.

"Unternehmen sollten für solche Fälle daher einen Business Continuity Plan haben", sagt Pichlmayr. Einige wenige Unternehmen seien gut abgesichert, aber viele würden nicht genug Ressourcen dafür haben - dabei ließe sich bereits mit 20 Prozent Mehraufwand die Sicherheit um 80 Prozent erhöhen. Etwa setzen viele Angreifer auf Social Engineering, also das Ausnützen menschlicher Schwachstellen: Nicht selten geben Mitarbeiter heikle Informationen im Web preis - und oft sind die Plaudertaschen nicht mal die Primärziele des Angriffs.

Auf staatlicher Ebene sieht Pichlmayr ebenfalls starken Nachholbedarf: "Die Verantwortlichen bräuchten ein Hundertfaches jener Ressourcen, die sie heute kriegen", sagt der Experte. Der politische Wille fehle aber - während nach 9/11 im Bereich der Flugsicherheit viel passiert ist, gebe es bei der IT-Security kaum ernsthafte Ansätze. Die USA kommunizierten viel und passen auch ihre Gesetzgebung an das neue Bedrohungsszenario an - auch sie würden aber auf Konferenzen einräumen, dass sie sich nur bedingt schützen können. "Der Vorteil Österreichs bleibt noch, dass wir kein bevorzugtes Ziel für Terroranschläge darstellen", relativiert Pichlmayr. Wenn es aber zu einem gezielten Angriff auf die entsprechenden Strukturen käme, wäre das ein ernsthaftes Problem - schließlich gibt es auch bei uns noch keinen Bereich des Lebens, der noch nicht digitalisiert ist.