

ZWISCHENRUF

Die Gefahr, die aus dem Rechner kommt: Computerviren und Cyber-Attacks

Wir alle wissen: Ohne IT, die Informationstechnologie, läuft fast nichts mehr. Die meisten Geschäftsvorgänge, wie auch viele Produktionsprozesse, unser Verkehrswesen, die weltweite Kommunikation, aber ebenso kleine Arbeitshilfen im Haushalt, sie alle basieren immer mehr auf IT – und werden damit anfälliger für Computerviren, für Spionage und für Sabotage. Vor kurzem gab es einen Angriff in neuem Maßstab durch einen Computer-Virus mit dem Namen STUXNET. Mit ihm wurde erstmals in der Geschichte die Steuerung ganzer Industrieanlagen von einem Virus befallen. Der Angriff konnte weder von Microsoft noch von irgendeinem gängigen Antivirus-Programm abgewehrt werden. Stuxnet hat seitdem weltweit bereits einige Industrieanlagen infiziert, unter anderem ein Kernkraftwerk im iranischen Bushere (auch wenn dieses noch nicht hochgefahren war, signalisierte das ein kaum zu unterschätzendes Risiko mit globalem Gefährdungspotenzial). Stuxnet ist das Beispiel eines Sabotage-Angriffs in Cyber-Form. Wer dahintersteckte und welche genauen Ziele verfolgt wurden, ist nur wenigen genauer bekannt. Es ist aber wohl davon auszugehen, dass es ein Nationalstaat war, der eine neue Form des Angriffs erprobt.

Mit dem Siegeszug der Informationstechnologie in unserem Alltag ist der Cyber-Terrorismus zu einem sicherheitspolitischen Thema von großer Bedeutung geworden. Denn Rechner und Netzwerke können von irgendwo und vielfach binnen Sekunden manipuliert oder sogar ausgeschaltet werden. Somit müssen auch unsere lebenswichtigen Netze – unter anderem für die Energie- und Rohstoffversorgung, das Transportwesen, Finanzsysteme, IT- und Telekommunikationsnetze, aber auch unsere Verteidigung – noch besser geschützt und



abgesichert werden. Längst berät man daher in der NATO über Strategien im Umgang mit Angriffen aus dem Cyber-Space. Englands Verteidigungsministerium hat sich der Sache ebenfalls angenommen und das Thema Cyber-Attacks in sein Nationales Sicherheitskonzept integriert. Auch in Kanada gab es kürzlich ein „IT-Problem“ im Bereich der Atomkraftwerke, das politischen Handlungsbedarf deutlich machte.

Terrorismus ist keine militärische Strategie im traditionellen Sinn, sondern primär eine Kommunikationsstrategie. Cyber-Terrorismus ist wiederum eine spezielle Form des Terrorismus, der mit Hilfe von Internet-Technologien Angriffe auf Computersysteme verübt. Die eingesetzten Waffen sind Werkzeuge aus dem Bereich der Informatik. Im einfachsten Fall zielen Angriffe auf rechnergestützte Verbindungen, um die Kommunikation auf diesem Wege zu vereiteln. Ein Beispiel für einen erfolgreichen Cyberangriff findet sich 2007 in Estland, wo nach einem konzertierten „Denial of Service-Angriff“ Regierungs- und Verwaltungsstellen sowie die größte Bank des Landes nicht mehr erreichbar waren. Zudem wirkte sich der Angriff auf Krankenhäuser, Energieversorgungssysteme und Notrufnummern aus.

Der Unterschied zum „klassischen“ Terrorismus: Für Cyber-Attacks und Cyber-Crimes braucht man keine Armeen, Raketen oder Flotten, sie sind ganz einfach von heimischen Laptops aus vorzunehmen. Stuxnet ist nicht über das Internet, sondern von Menschenhand über einen USB-Stick oder Laptop eingeschleust worden. Damit kommen als potenzielle Cyber-Terroristen auch „Leute wie du und ich“ in Betracht. Vielleicht sogar der geschasste und daher illoyale Mitarbeiter?

Sind Viren wie Stuxnet Waffen? Fest steht, dass die virtuellen Attacken realen Schaden anrichten und man sich deshalb noch intensiver mit diesem Thema auseinandersetzen muss – die Politik und die Unternehmen! Cyber-Terrorismus muss Bestandteil eines Konzepts zur vernetzten Sicherheit sein. Die neuen Kommunikationsformen machen vieles praktischer, aber die Systeme sind sehr verwundbar.



Ludolf von Löwenstern

Der Zwischenruf gibt die Auffassung des Verfassers wieder. Persönlich haftend der CC HOLDING Verwaltungs- und Beteiligungsgesellschaft. Er ist ehrenamtlich in verschiedenen Institutionen engagiert, unter anderem im Wirtschaftsrat Deutschland als Mitglied des Bundesvorstandes und Vorsitzender der Landesfachkommission ITK Informations- und Telekommunikationstechnologie (gegr. 1994), Deutsches Marine Institut (DMI), E-Business-Ausschuss der Handelskammer Hamburg.