

Schutz kritischer Informationsinfrastrukturen – vier Säulen der Informationssicherheit

Unter den OECD-Staaten gibt die Schweiz am meisten Geld pro Kopf und Jahr für Informations- und Kommunikationstechnologien (IKT) aus. Das verschafft uns Markt- und Standortvorteile, ist aber auch mit Abhängigkeiten und Risiken verbunden. Das Bedrohungsspektrum ist breit und reicht von Erpressungen über Wirtschaftsspionage bis hin zu Funktionsstörungen der kritischen Infrastrukturen eines Landes wie der Energieversorgung, des Finanzwesens, Transports und der Logistik oder des Gesundheitswesens. Die sie unterstützenden so genannten kritischen Informationsinfrastrukturen – das Internet mit eingeschlossen – sind daher zu schützen. Das Konzept der Informationssicherung der Schweiz beruht auf den vier Säulen Prävention, Früherkennung, Bekämpfung von Vorfällen sowie strategisches Krisenmanagement



Wegen ihrer grossen Bedeutung sind Kontrollsysteme – etwa zur Steuerung von Transport und Verkehr – zum Inbegriff kritischer Informationsinfrastrukturen geworden. Entsprechend wichtig sind Massnahmen zu ihrem Schutz. Im Bild: Stellwerk der SBB. Bild: Keystone

Softwarefehler in Verkehrsleitsystemen, Ausfälle von Mobiltelefonnetzen und Betriebsunterbrüche bei Geldausgabeautomaten sind Ereignisse, die uns die Schattenseiten der IKT vor Augen führen. Technische Pannen, aber auch gezielte Angriffe auf die IKT-Infrastrukturen – wie etwa das unbefugte Eindringen in oder das vorsätzliche Schädigen von Systemen – können dazu führen, dass beispielsweise die Strom-, Geld- oder Wasserversorgung massiv gestört werden.



Dr. Ruedi Rytz
Leiter der Geschäftsstellen
Infrastrukturbereiche,
Bundesamt für wirtschaftliche
Landesversorgung
BWL, Bern

Der Fall Estland

Eine Vorahnung, welche Herausforderungen auf moderne Informationsgesellschaften zukommen könnten, gaben vor Jahresfrist die über das Internet ausgeführten Angriffe auf Estland. Die Angriffe standen in Zusammenhang mit der geplanten Versetzung eines russischen Kriegsdenkmals. Als Urheber wurden russische Nationalisten vermutet. Die tatsächliche Herkunft der Angriffe wird aber wohl nie exakt ermittelt werden können. Sicher ist, dass als Folge der Angriffe verschiedene estnische Internetbanken über Tage blockiert waren, was einen massiven Umsatzeinbruch verursachte. Ebenso standen die gut ausgebauten E-Government-Dienstleistungen zeitweise nicht zur Verfügung. Für die Bevölkerung wurde es zunehmend schwierig, sich über Internet-Massenmedien zu informieren; auch die Internet-Kommunikation mit dem Ausland riss teilweise ab. Das Beispiel zeigt, dass Angriffe auf IKT-Infrastrukturen eines Landes durchaus dazu geeignet sind, der Wirtschaft Schaden zuzufügen und Druck auf Regierungen auszuüben.

Botnetze: Angriffe mit Folgen für die Volkswirtschaft

Die beschriebenen Attacken wurden mittels so genannter Botnetze ausgeführt.¹ Botnetze sind eine Ansammlung gehackter Computer, die von einem Angreifer zentral (fern-)gesteuert und zur Durchführung von «Arbeiten» herangezogen werden können. Botnetze umfassen Tausende bis zu 1 Mio. Computer. Das Hacken der Maschinen und deren Eingliederung in ein Botnetz erfolgt automatisiert durch Schadsoftware unter Ausnutzung von bestimmten Sicherheitslücken in Betriebssystemen oder Anwendungen. Bei den so befallenen und in ein Botnetz integrierten Maschinen handelt es sich vielfach um PC von Privatpersonen, welche heute so leistungsstark sind, dass es ihren Besitzern kaum auffällt, wenn ihr Rechner, währenddem sie gerade einen Text bearbeiten, zeitgleich dazu eingesetzt wird, beispielsweise eine Internetbank in Estland lahmzulegen. Es ist bekannt, dass allein in der Schweiz Zehntausende PCs Botnetzen angehören.

Eine Möglichkeit, die geballte Leistung der Botnetze zu nutzen, besteht – wie in Estland geschehen –, darin Webserver (z.B. E-Banking- oder E-Commerce-Server) gleichzeitig mit so vielen Anfragen zu überfluten, bis diese unter der ungeheuren Last zusammenbrechen und so für legitime Kunden nicht mehr verfügbar sind. Solche so genannten Denial-of-Service-Angriffe (DoS) gegen E-Commerce-Server gehen häufig mit der Erpressung von Schutzgeldern einher und können grundsätzlich alle Firmen betreffen, die Dienstleistungen über das Internet anbieten. Die ökonomischen Verluste für Betroffene sind mitunter gross und können im Extremfall gar deren wirtschaftlichen Ruin zur Folge haben. Vor drei Jahren führte eine DoS-Attacke auf die Tochtergesellschaft der Royal Bank of Scotland Worldpay, welche für die Abwicklung von Kreditkartentransaktionen besorgt ist, zum fast vollständigen Erliegen der Finanztransaktionen. Kunden von 30 000 Geschäften in 70 Ländern konnten ihre Kreditkarten nicht mehr zur Bezahlung nutzen und mussten die Ware in den Regalen stehen lassen. Die Umsatzeinbussen während des dreitägigen Angriffs betrugen 50%–80%, was mit entsprechenden Folgen für die Volkswirtschaften verbunden war. Angriffe mit Botnetzen können sich so rasch einmal auf ganze kritische Infrastrukturen – wie hier das Finanzwesen – auswirken.

Neben DoS-Attacken werden Botnetze für viele andere Zwecke eingesetzt. Dazu gehört beispielsweise auch das Versenden von Spam (siehe *Kasten 1*). Botnetze werden von den

Angriffern meist nicht selbst aufgebaut, sondern gemietet. Im Internet-Untergrund existieren Preislisten von Botnetzen – es werden sogar Gratisdemonstrationen ihrer Leistungsfähigkeit angeboten. Leute, die Botnetze aufbauen, verdienen Geld (Jahreseinkünfte von 200 000 US-\$ sind nicht selten) mit deren Vermietung, wobei die «Mieter» diese beispielsweise durch Erpressung oder den Versand von Spam wiederum zu Geld machen. Die Arbeitsteilung im Internet-Untergrund ist also weit fortgeschritten und trägt offensichtlich auch hier zur Steigerung der Produktivität bei. Adam Smith hätte seine wahre Freude.

Beklemmende Vorstellung einer Attacke auf Kontrollsysteme

Trotz der oben beschriebenen – und der grossen Anzahl weiterer – real existierender Bedrohungen, die sich inzwischen fast täglich in Vorfällen manifestieren, hat wohl nichts die Fantasie der Menschen so beflügelt wie Angriffe über IKT-Infrastrukturen auf Kontrollsysteme. Darunter verstehen wir Systeme zur Überwachung, Kontrolle und Steuerung von Industrieanlagen (z.B. Chemie, Kraftwerke), zur Verteilung lebenswichtiger Güter (z.B. Strom, Wasser, Brennstoff) oder zur Steuerung von Transport und Verkehr (Eisenbahnen, Verkehrsleitsysteme, Post). Ihrer Bedeutung entsprechend sind Kontrollsysteme zum Inbegriff kritischer Informationsinfrastrukturen geworden. Die Vorstellung, dass Terroristen in den Bergen von Kabul mit einem Laptop auf den Knien die Lichter in westlichen Grossstädten ausknipsen, ist beklemmend. Um es vorwegzunehmen: Szenarien dieser Art sind – mindestens vorderhand noch – weniger reale Bedrohung denn packendes Material für Kinofilme. Trotzdem ist davor zu warnen, die Problematik auf die leichte Schulter zu nehmen.

Entwicklung und Betrieb von Überwachungs-, Kontroll- und Steuerungssystemen haben lange Tradition. Ursprünglich hatten diese aber nur wenig Ähnlichkeit mit herkömmlichen IKT. Sie waren von den Computernetzwerken (wie das Internet) isoliert, benutzten proprietäre Hard- und Software und setzten zur Kommunikation eigene Protokolle ein. Die breite Verfügbarkeit vergleichsweise günstiger Geräte mit eingebauter Schnittstelle zum Internet hat in den letzten Jahren grosse Veränderungen gebracht. Kurz: Kontrollsysteme ähneln zunehmend PCs und dem Internet. Den Vorteil der kostengünstigen Technologie erkaufte man sich damit, dass Kontrollsysteme nun grundsätzlich den gleichen Bedrohungen ausge-

Kasten 1

Botnetze: Versand von Spam

Über 90% der weltweit versandten Spam (unerwünschte Werbemails) werden über Botnetze verschickt. Seit dem 1. April 2007 ist der Versand von Spam in der Schweiz ausdrücklich untersagt. Das Bundesgesetz über den unlauteren Wettbewerb (UWG) sieht verschiedene Massnahmen gegen Spam vor, und das Fernmeldegesetz (FMG) hält fest, welche Massnahmen die Fernmeldeanbieter ergreifen müssen. Wird der Spam von der Schweiz aus an schweizerische Adressaten verschickt, so muss der Internet Service Provider des Absenders aktiv werden; in den anderen Fällen (Absender in der Schweiz, Empfänger im Ausland und umgekehrt) ist das Staatssekretariat für Wirtschaft (Seco) zuständig.

1 Das Wort Bot hat seinen Ursprung im slawischen robota (Arbeit), daher auch der Begriff Roboter.

setzt sind, wie wir sie vom Internet her kennen. Malware (Viren, Würmer) sowie Hacker halten Einzug.

Bis heute sind nur wenige Fälle von Angriffen auf Kontrollsysteme dokumentiert. Der bekannteste Fall hat sich im Jahr 2000 in Queensland, Australien, zugetragen. Von seinem Laptop aus ist es einem 49-jährigen Mann gelungen, in die computergesteuerte Wasserversorgung einzudringen. Er konnte sich als «Pumpstation 4» anmelden und in der Folge sämtliche Alarmmeldungen unterdrücken. So erlangte er die uneingeschränkte Befehlsgewalt über 300 Kontrollknoten des Trink- und Abwassersystems. Es gelang ihm, Millionen Liter Abwasser in Parks, Flüsse, ja sogar in die Anlage eines Hotels ausfliessen zu lassen. Die Meeresfauna wurde schwer geschädigt; das Flusswasser färbte sich schwarz und der Gestank war über lange Zeit unerträglich. Erst beim 46. Versuch konnte der Mann von der Polizei gefasst werden.

Im Fall Estland sind keine Angriffe auf Kontrollsysteme beobachtet worden. Trotzdem haben sich im Nachgang an diese Ereignisse viele Länder in Untersuchungsberichten Gedanken über solche Angriffe gemacht.²

Anstrengungen von staatlicher Seite in der Schweiz

Die Schweiz als führender Wirtschaftsstandort hat im Falle einer grösseren Störung in der Informationsinfrastruktur viel zu verlieren. Mehrmals hat der Bundesrat seinen Willen bekundet, die IKT-Infrastrukturen unseres Landes vor Missbrauch, Ausfällen und Angriffen zu schützen, so etwa mit der Verabschiedung des Konzepts *Information Assurance* (Informationssicherung) im Jahr 2000, der Schaffung der *Koordinationsstelle zur Bekämpfung der Internetkriminalität (Kobik)* im Jahr 2001 sowie mit dem Aufbau der *Melde- und Analysestelle Informationssicherung (Melani)* im Jahr 2003.

Im Bereich des Schutzes kritischer Informationsinfrastrukturen (Informationssicherung) verfolgt der Bundesrat die von ihm im Konzept «Information Assurance» dargelegte Strategie. Sie beruht auf den vier Säulen Prävention, Früherkennung, Bekämpfung von Vorfällen sowie strategisches Krisenmanagement.

– Bezüglich der *Prävention* erarbeitet der Bereich IKT-Infrastruktur im Bundesamt für wirtschaftliche Landesversorgung (BWL) gemeinsam mit den betroffenen Stellen in der Wirtschaft – d.h. den Betreibern kritischer Informationsinfrastrukturen in den Sektoren Energieversorgung, Transport, Gesundheitswesen usw. – Risi-

koanalysen, in denen die Abhängigkeit dieser Sektoren von den unterstützenden IKT-Infrastrukturen untersucht und wo möglich vorbereitende Massnahmen zu deren Schutz vorgeschlagen werden.

- Die *Früherkennung* sowie die *Bekämpfung von Vorfällen* fallen in den Zuständigkeitsbereich von Melani. Es handelt sich hierbei um eine Kooperation des Informatikstrategieorgans Bund (ISB) mit dem Dienst für Analyse und Prävention im Bundesamt für Polizei (Fedpol). Ziel von Melani ist es, den Betreibern kritischer IKT-Infrastruktur subsidiär Mittel zur Verfügung zu stellen, was nur einer staatlichen Stelle möglich ist. Dies ist insbesondere in den Bereichen des Nachrichtendienstes (Abschätzung von Bedrohungslagen), bei der Strafverfolgung sowie bei den nationalen Computer Emergency Response Teams (Govcert.ch) der Fall. Zu diesem Zweck arbeitet Melani eng mit den Betreibern dieser Infrastrukturen (z.B. Energieversorgern, Banken und Telekommunikationsunternehmen) zusammen.
- *Strategisches Krisenmanagement*: Für den Fall von länger andauernden Störungen in der Informations- und Kommunikationsinfrastruktur, welche sich auf das Funktionieren der kritischen Infrastrukturen auswirken, ist die Einberufung des *Sonderstabs Informationssicherung (Sonia)* vorgesehen. Sonia setzt sich aus Vertretern der Bundesverwaltung sowie erfahrenen Repräsentanten aus der Kaderorganisation des Bereichs IKT-Infrastruktur der Wirtschaftlichen Landesversorgung zusammen.

Durch die enge Zusammenarbeit zwischen Wirtschaft und Staat sowohl im Rahmen der Wirtschaftlichen Landesversorgung als auch bei Melani verfügt die Schweiz über ein umfassendes, flexibles und kostengünstiges Modell zum Schutz der kritischen Informationsinfrastrukturen, welches auch im Ausland als vorbildlich gilt. ■

² Siehe beispielsweise Schweden: www.krisberedskapsmyndigheten.se, «Publications», «Other Documents», «Large Scale Internet Attacks, SEMA's Educational Series 2008:2».