IT-SICHERHEIT

Angriffsziel Kraftwerk

Von Uwe Sievers | 5. Februar 2016 | Ausgabe 05

Cyberangriffe werden verstärkt politisch eingesetzt. Der Kampf im digitalen Untergrund richtet sich häufig gegen Staaten, wichtige Industrien und Bürger. Wenn als Ziel kritische Versorgungseinrichtungen wie Stromnetze ausgewählt werden, ist die Bevölkerung unmittelbar betroffen.

Foto: PantherMedia/Jens Ickler

Kraftwerke, wie hier in Berlin, aber auch Verkehrsknotenpunkte zählen zu den kritischen und damit sensiblen Infrastrukturen.

Während in Israel letzte Woche wegen einer ungewöhnlich heftigen Kaltfront der Stromverbrauch auf Rekordhöhe stieg, haben Angreifer Steuersysteme der israelischen Energieversorgung lahmgelegt. Es sei einer der schwersten Cyberangriffe, den das Land je erlebt habe, erklärte Israels Energieminister Yuval Steinitz auf der Cybertech Conference in Tel Aviv. Dabei zählt die Nation nach eigenen Angaben zu den fünf großen Playern der IT-Security-Branche.

Die im Cyberspace ausgetragenen politischen Konflikte richten sich primär gegen wichtige Versorgungseinrichtungen wie Kraftwerke, Wasserbetriebe, Strom- und Telekommunikationsnetze oder für die Wirtschaft bedeutende Produktionsstätten. Große Gefahren sehen Experten wie der TÜV Rheinland auf Industrie-4.0-Anlagen zukommen.

Stehen politische Einrichtungen im Fokus, geht es dagegen um Spionage: Hacker hatten sich im Mai letzten Jahres Zugriff auf 14 Server des deutschen Bundestags verschafft, darunter war auch einer mit sämtlichen Zugangsdaten für Parlamentsrechner. Der Angriff soll nach Überzeugung deutscher Sicherheitsbehörden im Auftrag der russischen Regierung erfolgt sein, berichtet der Spiegel. Gegenüber klassischen Sabotage- und Spionagemethoden bieten die digitalen Pendants Vorteile: Sie lassen sich problemlos aus der Ferne anwenden, ohne Agenten vor Ort der Gefahr von Entdeckung auszusetzen. Die Verursacher sind kaum auszumachen.

Deshalb besäßen alle großen Nationen „Cyberwaffen“, berichtete Eugene Kaspersky, Gründer des russischen Herstellers von Sicherheitssoftware, letzte Woche auf der Sicherheitstagung IT-Defense in Mainz. Waffen, die ständige Nachrüstung verlangten. „Cyberwaffen kann man nur einmal benutzen. Danach sind die anvisierten Systeme davor

Foto: Uwe Sievers

„Ziele werden nicht nur vernetzte Autos sein, sondern auch vernetzte Züge, Schiffe und Flugzeuge.“ Eugene Kaspersky, Gründer des gleichnamigen IT-Sicherheitsunternehmens.

geschützt – oder tot“, erklärt Kaspersky.

Staaten setzen für Angriffe auch Hackergruppen ein. Diese „Söldner des Cyberspace“ könnten jedoch genauso gut von Terroristen angeheuert werden, befürchtet Kaspersky. Denn sie zielten wie das Militär auf kritische Infrastruktur. „Methoden und Ziele sind die gleichen, nur die Motivation ist eine andere“, so der Russe.

Die Leidtragenden dieser politischen Auseinandersetzungen im Cyberspace sind allzu oft die Bürger, wie unlängst ein großer Stromausfall in der Ukraine zeigte. Das ruft auch die europäische Sicherheitsbehörde Enisa auf den Plan. Doch die internationalen Bemühungen stecken noch in den Kinderschuhen. Kaspersky rät dagegen, die Vorfälle ernst zu nehmen und warnt vor kommenden Gefahren: „Ziele werden nicht nur vernetzte Autos, sondern auch vernetzte Züge, Schiffe und Flugzeuge sein.“ -Seiten 12 und 13