Blick in die Glaskugel

Ein guter Schutz hat immer drei Perspektiven: Die Zukunft, die Gegenwart und die Vergangenheit. Das gilt auch für die IT-Sicherheit: Mit der Vergangenheit beschäftigt sich die IT-Forensik, für einen wirksamen Schutz in der Gegenwart sorgen präventive Sicherheitsmaßnahmen (Firewalls, Malware-Scanner, Verschlüsselung, Passwörter etc.), und die Zukunft ist zumeist Gegenstand des IT-Risikomanagements – sofern man sich überhaupt mit ihr beschäftigt.

Mit der wachsenden Abhängigkeit der Wirtschaft und vieler Versorgungseinrichtungen von einer funktionierenden informationstechnischen Infrastruktur und der gleichzeitigen Zunahme ernst zu nehmender gezielter Angriffe auf Verwaltungs- und Versorgungsnetze grenzt es inzwischen jedoch an Fahrlässigkeit, sich lediglich reaktiv mit neuen Gefahren auseinander zu setzen. Denn kreative kriminelle Geschäftsideen und deren enormes finanzielles Gewinnpotential im Erfolgsfall, ein globalisierter Wettbewerb und terroristische Drohungen machen Angriffe auf IT-Systeme zu einer ernst zu nehmenden Bedrohung, denen herkömmliche Abwehrmechanismen nicht automatisch gewachsen sein müssen.

Und selbst wenn die Flexibilität heutiger IT-Systeme und –Netze einen flächendeckenden Ausfall zumindest kritischer IT-Infrastrukturen unwahrscheinlich macht, tröstet das im Einzelfall wenig – der Schaden für die betroffenen Unternehmen kann auch ohne überregionale Katastrophe existenzbedrohend für einzelne sein.

Der Blick in die Zukunft lässt, wie jüngste Ereignisse wieder zeigten, jedoch vor allem erwarten, dass die bereits seit einigen Jahren zu beobachtenden Tendenzen sich verstärken werden: Unter Ausnutzung von „Zero Day Exploits", die es dank fortgesetzt fehlerträchtiger Software auch weiterhin zahlreich geben wird, werden immer ausgefeiltere Angriffsprogramme entwickelt und in IT-Systeme und Infrastrukturen eingeschleust – auch über bislang selten genutzte Einfallstore wie Smartphones oder USB-Sticks. Tatsächlich ist es jedoch gar nicht so einfach, neue Bedrohungen dieser Art rechtzeitig zu erkennen. Das liegt vor allem an den oft neuen Angriffsmethoden und –wegen sowie der schnellen Verbreitung neuer Angriffssoftware und der daher extrem kurzen Reaktionszeit, die betroffenen Infrastrukturen bleibt.

Die IT-Frühwarnung versucht nun, neue Mechanismen zu entwickeln, die auch bisher unbekannte Angriffe nicht nur möglichst früh erkennen und damit den Schaden minimieren helfen, sondern durch Warnungs- und Alarmierungsmaßnahmen noch nicht betroffenen Systemen eine rechtzeitige Gegenwehr ermöglichen.

Das vorliegende Schwerpunktheft stellt die bisherigen Erkenntnisse und aktuellen Forschungsvorhaben in diesem noch jungen, aber – so ist zu befürchten – wahrscheinlich schon in Bälde besonders wichtigen Gebiet der IT-Sicherheit vor.

Eckehard Hermann, Dirk Fox