Das lange Ende des Perimeters

Hätte vor einem Monat jemand nach vier Begriffen gefragt, deren gemeinsames Vorkommen in einem einzigen Satz maximal unwahrscheinlich ist, wären „Hochschule des Bundes für öffentliche Verwaltung, Open-Source-Software, russischer Geheimdienst und Brexit“ keine schlechten Kandidaten gewesen. Einen „veritablen Cyberangriff“ später, und es wissen jetzt immerhin (fast) alle, was der IVBB* ist. Am neusten Hack auf das Auswärtige Amt ist einiges erstaunlich – und vieles auch nicht.

Nicht überraschend, sondern ein Zeichen der momentanen Aufgeladenheit sowohl des Cyber-Themas als auch der aktuellen Beziehungen zu Russland war die Stärke des medialen Echos auf einen Vorfall, der so oder ähnlich in den meisten Ländern mehrere Male im Jahr stattfinden dürfte und hier zudem eine vergleichsweise magere Ausbeute ergab.

Schon rein statistisch vorhersagbar war der lange Zeitraum zwischen Infektion und Detektion. Nicht überraschend war auch, dass selbst der fortgeschrittenste Angriff unter den fortgeschrittenen Angriffen (Advanced Persistent Threats) mit Wasser kocht, wo Wasser genügt. Dass die Infektion über eine an sich unkritische Lernsoftware erfolgen konnte, wirft allerdings Fragen nach fehlender Gründlichkeit beim Sicherheitskonzept auf.

Grundsätzlich zu erwarten waren darüber hinaus die Spekulationen über die Täter, obwohl in Fachkreisen „Attribution“, also die Zuschreibung eines Angriffs, nach wie vor als schwer bis unmöglich gilt.

Die eigentliche Überraschung liegt im Infektionsweg, der im Nebeneinander von „hochsicherem Netz für die obersten Bundesbehörden und Verfassungsorgane“ und „Open-Source-Lernsoftware mit Sicherheitslücken“ anklingt. Hier scheint etwas nicht zusammenzupassen.

In anderen IT-Einsatzbereichen wurde der „Perimeter“, die ehemals starre Netzwerkgrenze, schon vor rund 10 Jahren für tot erklärt und siecht seitdem dank zyklischer Verjüngungskuren à la Next-Generation-Firewalls, Anomalieerkennung oder Intrusion Detection fröhlich vor sich hin.

Konzerne wie Google haben akzeptiert, dass der Perimeter heute immer weniger zu schützen ist, und ihn konsequenterweise aufgegeben. An seine Stelle sind neue Konzepte getreten, die der veränderten Bedrohungslage durch die Mobilität der Daten und Mitarbeiter besser gerecht werden. Gleichzeitig musste die IT unterwegs zwangsweise einfacher und verlässlicher werden.

Mehr Cyberwehr plus Gegen-Hacks sind jedoch kein Schlüssel zum Erfolg. Vielmehr sind die besten Köpfe gefragt, moderne Methoden wie Googles Unternehmenssicherheitsmodell BeyondCorp (siehe ix.de/ix1804003), automatisierte Hardware-Inventarisierung, zentrale Access Proxies und DFIR (Digital Forensics, Incident Response) einzuführen.

Damit dies Erfolg haben kann, fehlt nur noch eines: An die Stelle des Jammerns über den Fachkräftemangel müsste die Begeisterung treten, dieses spannende technische Projekt – Arbeitstitel „BeyondGov“ – mit aller Kraft umzusetzen.

DAVID FUHR

ist Head of Research beim IT-Sicherheitsberatungsunternehmen HiSolutions.

Alle Links: ix.de/ix1804003

* Informationsverbund Berlin-Bonn