IT-Sicherheit

Angreifer im Visier

[05.11.2015] Massenattacken, gezielte Angriffe oder so genannte Advanced Persistent Threats zielen auf die IT-Infrastrukturen von Regierungsstellen und Kommunen. Der Cyber-Schutz für IT-Netzwerke im öffentlichen Bereich ist deshalb für alle Verwaltungsebenen essenziell.

Im Mai 2015 konnten Hacker das interne Datennetz des Deutschen Bundestags erfolgreich attackieren. Experten bezeichnen den Vorfall als schwerwiegend, die Netzwerke des Bundestags wurden heruntergefahren und mussten erneuert werden. Der Verfassungsschutz, die Bundestagsverwaltung und das Bundesamt für Sicherheit in der Informationstechnik (BSI) sind mit der Aufklärung beschäftigt. Werden sensible Informationen bei einer staatlichen Stelle entwendet, kann nicht zuletzt das Vertrauen der Bürger nachhaltig erschüttert werden. Zudem gilt es, kritische Infrastrukturen vor Cyber-Angriffen zu schützen. Die Experten des Unternehmens Kaspersky Lab entdecken täglich mehr als 325.000 neue Schadprogramme. Trojaner, Würmer, Rootkits und Keylogger bedrohen die IT-Sicherheit und finden ihren Weg ins Netzwerk. Es gilt also grundsätzlich, die eigene IT-Infrastruktur und alle innerhalb dieser Umgebungen genutzten Geräte, auch Smartphones und Tablets, professionell vor der Flut an Schädlingen zu schützen.

Cyber-Spionage-Kampagnen

Zudem muss sich der öffentliche Bereich vor zielgerichteten Attacken schützen. Vor allem Cyber-Spionage-Kampagnen richten sich auch gegen Organisationen der öffentlichen Hand. Bei den so genannten Advanced Persistend Threats (APTs) handelt es sich beispielsweise um hoch professionelle, andauernde und äußerst präzise Cyber-Attacken. Vermutlich von Nationalstaaten unterstützt, werden sie immer raffinierter. Sie nehmen mit komplexen, modularen Werkzeugen sorgfältig ausgewählte Nutzer ins Visier und verbergen sich vor effektiven Detektionssystemen. Ein häufiger Angriffsvektor ist das so genannte Spear-Phishing. Dabei wird eine personalisierte E-Mail an eine bestimmte Person in einer Organisation versendet, in der Hoffnung, dass diese auf einen in der E-Mail enthaltenen gefährlichen Link klickt oder einen Anhang öffnet, der den Code der Angreifer ausführt und ihnen Einlass in das anvisierte Netzwerk gewährt.

Gefährlicher Bedrohungsakteur

Im Februar dieses Jahres enttarnte Kaspersky Lab einen Bedrohungsakteur, der hinsichtlich technischer Komplexität und Raffinesse alles bislang Bekannte in den Schatten stellte – die so genannte Equation Group. Bei ihrer APT-Attacke wurden zum Beispiel Werkzeuge verwendet, die sehr kompliziert und kostenintensiv zu entwickeln sind. Ihre Aktionen verbergen sie in einer außergewöhnlich professionellen Weise. Seit dem Jahr 2001 hat die Equation-Gruppe Opfer in über 30 Ländern weltweit aus folgenden Bereichen infiziert: Regierungs- und diplomatische Institutionen, Telekommunikation, Luft- und Raumfahrt, Energie, Nuklearforschung, Öl- und Gasindustrie, Militär, Nanotechnologie, islamische Aktivisten und Gelehrte, Massenmedien, Transport, Finanzinstitute sowie Unternehmen, die Verschlüsselungstechnologien entwickeln. Es gibt zuverlässige Hinweise darauf, dass die Equation Group mit anderen einflussreichen Gruppen, beispielsweise mit den Betreibern von Stuxnet und Flame interagierte – wobei die Equation Group offenbar eine führende Position innehatte.

Sicherheit auf neuestem Stand

Software Updates sind für alle genutzten Anwendungen Pflicht. Nicht nur IT-Sicherheitslösungen wie AV-Komponenten oder Spam-Filter, sondern auch Betriebssysteme oder Programme wie Java, Microsoft und Adobe sollten auf dem neuesten Stand sein. Dabei helfen aktuelle Patch- und System-Management-Lösungen. Zudem bieten adäquate IT-Sicherheitslösungen dedizierten Echtzeitschutz – auch vor neu auftauchenden Gefahren wie Zero-Day-Exploits. Zu den führenden Plattformen zählt hier Kaspersky Endpoint Security for Business. Sie bietet nicht nur eine zentrale Verwaltung, sondern auch weitere Sicherheitstechnologien wie Verschlüsselung oder den Schutz für mobile Geräte. In einem sehr sensiblen Umfeld wie dem öffentlichen Bereich reichen rein technische Sicherheitsmaßnahmen allerdings nicht aus. Es gilt, gezielte Angriffe und die Schwachstelle Mensch so gering wie möglich zu halten. Mit professioneller Unterstützung kann das gelingen. Die Zauberworte lauten hier Schulungen und Intelligenz – und zwar für IT-Fachleute ebenso wie für das Sekretariat.

Schulungsmaßnahmen und Services

Dabei geht es um die Vermittlung klassischer Cyber-Sicherheitsgrundsätze, aber auch um Spezialkenntnisse, beispielsweise über digitale Forensik, Malware-Analyse oder Reverse-Engineering. Für unterschiedliche Bereiche werden zwischenzeitlich spezielle Services angeboten. Beispielsweise wurden für kritische Infrastrukturen spezielle Systeme und Dienstleistungen entwickelt. Malware- oder Vorfalluntersuchungen sowie Reporting-Dienstleistungen vom Botnetz-Tracking bis zu Cybersecurity-Reports unterstützen ebenfalls im Bereich der IT-Sicherheit. Zusammen mit den Mitarbeiterschulungen und der in einem Sicherheitsunternehmen vorhandenen Thread Intelligence lässt sich durchaus von einer Security Intelligence sprechen. Werden diese Basisschutzkomponenten mit für die eigene Organisation passenden Zusatzmaßnahmen angereichert, lässt sich ein mächtiger und mehrschichtiger Anti-APT-Schutzwall für Endpoints und Netzwerke errichten.

()

Dieser Beitrag ist im Spezial der November-Ausgabe von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Kaspersky, BSI, Cyber-Schutz, Kaspersky Endpoint Security