Mehrstufige Sicherheitsarchitektur

Wirtschafts- und Industriespionage ist nicht erst seit den Enthüllungen von Edward Snowden für die Unternehmen ein hoch brisantes Sicherheitsthema. Die Gefahr, dass unternehmenswichtige Daten ausgespäht, gegebenenfalls Daten manipuliert und Systeme oder Anlagen sabotiert werden, war allerdings für die Unternehmen noch nie so groß wie heute.

Bild: Twinsec

Christian Ehlen,
Senior Consultant IT-Security bei Twinsec

Abgesehen haben es Wirtschafts- und Industriespione unter anderem auf geschäftliche Kerninformationen sowie Informationen aus Forschung & Entwicklung, zu Planungen, Firmenaufkäufen, Patenten und Ausschreibungen. Was also tun, um sich besser vor Spionageattacken zu schützen? Eines steht außer Frage: Was das Einschleusen von unternehmensspezifischer Ausspähungs-Software betrifft, helfen allein die klassischen, auf Signaturen basierende Lösungen wie (Next-Generation-) Firewalls, Intrusion-Prevention-Systeme, Webproxies/ Viruswalls und Antispam-Systeme, den Unternehmen häufig nicht weiter. Diese erkennen technologiebedingt nur die zumeist auf breite Angriffe ausgelegte, bereits bekannte Malware und Angriffsanatomie, die der Scanner anhand ihres digitalen Fingerabdrucks per Mustererkennung identifiziert. Dies macht sie aber keinesfalls überflüssig, sondern zu einem funktional erprobten Teil einer mehrstufigen Sicherheitsarchitektur. Um gezielte Angriffe zu erkennen und anzugehen, bedarf es eines zweiten Walls hinter der bestehenden Verteidigungslinie, der die risikobehafteten Kommunikationsbeziehungen und Daten abschöpft und detailliert untersucht.

Geheimdienste und Industriespione investieren viel Zeit, Intelligenz und Geld, um die individuellen Schwachstellen eines Unternehmens aufzuspüren und auszunutzen. Die Kenntnis über Schwachstellen innerhalb der vom Zielobjekt eingesetzten Software und den dazugehörigen programmatischen Exploit-Code erarbeiten sie in Eigenregie. Oder sie kaufen diese Kenntnis am Grau- beziehungsweise Schwarzmarkt ein. So wie es aussieht, kann zudem davon ausgegangen werden, dass viele der installierten IT-Systeme bereits im manipulierten Zustand, versehen mit Back- beziehungsweise Bugdoors, sind. Doch oft sind diese Systeme, die dadurch per se als nicht vertrauenswürdig gelten, für das Unternehmen aus wirtschaftlichen und funktionalen Gründen ohne Alternative. Nicht überall wird quelloffene Software eingesetzt. Dort, wo sie eingesetzt wird, wird sie meist nicht durch professionelle Verfahren untersucht, entwickelt und eingebunden. Damit die Angreifer innerhalb der zielgerichteten Operationen auf Unternehmen unentdeckt bleiben, verwenden sie Methoden wie Polymorphie, Verschlüsselung und Binär-Packer. Die daraus resultierende Dynamik und Einzigartigkeit ist schwierig als maliziös zu identifizieren. Zudem machen sich Wirtschafts- und Industriespione auf Basis von öffentlichen Quellen über bestimmte Personen im Unternehmen schlau, die für sie aufgrund ihrer Funktionen besonders lukrative Angriffsziele darstellen. Dabei muss der Angreifer nicht einmal im Besitz von erweiterten Angriffs- und Auswertungstechnologien wie die von der NSA verwendeten „Quantum Insert“ und „XKeyscore“ sein. Oftmals reichen eine Analyse von sozialen Netzwerken, wie Xing, Face book oder Linkedin oder die Ergebnisse einer Suchmaschinenabfrage aus. Danach werden diese Personen per E-Mail adressiert, die genau auf ihre Hobbys und Neigungen abzielen, um auf diesem Weg Ausspähprogramme einzuschleusen und einzunisten.

Dass die infiltrierten Programme vom Unternehmen nicht entdeckt werden sollen, hat aus Sicht der Angreifer einen weiteren Grund: Die Schadprogramme sollen solange wie möglich, dort, wo sie eingenistet wurden, ausspionieren. Somit wissen die Unternehmen ohne geeignete Abwehrmechanismen nicht einmal, ob sie bereits Opfer von gezielten Angriffen geworden sind und wie lange sie schon ausgespäht werden. Die Erfolgsaussicht auf Seiten des Angreifers ist hoch, die Situation für die Angegriffenen dennoch nicht aussichtslos. Denn erste Sicherheitslösungen im Markt gibt es bereits, die den existenten Schutzwall aus klassischen Maßnahmen im Rahmen einer mehrstufigen Sicherheitsstrategie auch gegen gezielte Spionageangriffe verstärken. Dazu werden die potenziellen maliziösen Programme in eine virtuellen Laborumgebung (Sandbox) umgelenkt. Sie stellt ein möglichst nahes Abbild des Backend mit den daran angeschlossenen Endgeräten dar. Innerhalb dieser ausbruchssicheren Laborumgebung wird in Parallelanalyse für jede extrahierte, potenzielle Attacke untersucht, was im einzelnen passiert: Dringen die Programme tiefer in Systeme ein? Werden Anwendungen und Datenbestände infiltriert, wenn ja, welche? Werden Einstellungen gemacht beziehungsweise verändert? Darüber hinaus werden die Kommunikationsverbindungen, ein- und ausgehend, von den neuen Abwehrlösungen gründlich inspiziert.

Leistungsfähige Lösungen sind schon heute dazu in der Lage, über zahlreiche betriebssystem- und applikationsabhängige Merkmale auf mögliche Infiltrationen und Korruptionen hin zu untersuchen und bei Gefahr zu alarmieren. Noch kommen für die Paralleluntersuchungen strukturierte Raster zum Einsatz, die marktwichtige Betriebssysteme und Applikationen repräsentieren. Noch besser würde allerdings der Abwehrschutz gegenüber solchen Angriffen funktionieren, wenn die betroffenen Unternehmen selbst ein exaktes 1:1-Abbild ihrer Backend-Umgebung als abgesetzte Laborumgebung erstellen würden.