Prävention und Detektion im Zeitalter fortgeschrittener Angriffe

Juni, 2015

Klassifikation:
Öffentliche Version

IOprotect GmbH
Huobstrasse 14
8808 Pfäffikon SZ
+41 (0)44 533 00 05
info@ioprotect.ch
www.ioprotect.ch

Einleitung

IOprotect hat sich in den vergangenen Jahren intensiv mit den Auswirkungen von gezielten Angriffen befasst und diverse Aufträge im Bereich von Security Audits, Angriffsanalysen, IT Forensik und Monitoring durchgeführt. Das vorliegende Dokument fasst die von IOprotect gemachten Feststellungen zusammen. Fazit: Der Schutzgrad der Unternehmen ist vielfach ungenügend.

Erkenntnisse

- Client-Systeme sind das Einfallstor Nr. 1, werden jedoch nicht als das wahrgenommen. Überprüfungen in diesem Bereich werden gar nicht oder nicht in der notwendigen Tiefe und Periodizität durchgeführt.
- Die Infektion eines Client-Systems via Internet ist relativ einfach möglich und wird kaum bemerkt. Als Folge davon bleiben Angreifern Tür und Tor in die Unternehmensnetze offen.
- Den einfachsten Angriffsvektor stellen heute MS Office-Dokumente mit Makros dar. Diese werden von Schutzmassnahme selten als bösartig erkannt. An zweiter Stelle stehen Schwachstellen in clientseitigen Applikationen.
- Obwohl dem Patch-Management eine grössere Bedeutung gegenüber früher beigemessen wird, ist die Client-Flotte selten gesamthaft konsistent. Bereits ein einzelnes, nicht vollständig gepatchtes System genügt jedoch für einen erfolgreichen Angriff.
- Konfigurationsfehler auf den Clients ermöglichen es häufig, lokal an erhöhte Rechte zu gelangen. Grund dafür sind meist Third-Party- oder auch In-House-Applikationen. Damit wird die Ausbreitung der Angreifer im internen Netzwerk vereinfacht.
- Unverschlüsselte Harddisks auf Desktop-Systemen führen innert Minuten zu lokalen Administratoren-Rechten.
- Die Effektivität der Schutzmassnahmen auf Netzwerkebene (IDS/IPS, Web-Proxy, E-Mail-GW etc.) ist oft bedenklich gering. Festgestellte Detektionsraten lagen zwischen 10% und maximal 85%.

- Lokale Security-Lösungen stossen an Grenzen. Selbst bekannte Angriffs-Scripts und Tools werden nicht durchgehend als bösartig erkannt.
- Mit wenigen Zeilen Powershell lässt sich ein Remote Administrationstool (inkl. Proxy-Awareness) erstellen. Bekannte Angriffstools lassen sich zudem via Powershell ausführen, ohne verräterische Dateien auf der Festplatte zu hinterlassen. Abwehrmassnahmen gegen solche Szenarien sind kaum vorhanden.
- Im Bereich der Detektion verlässt man sich allzu oft auf „Blackbox"-Lösungen. Deren Schutzfunktionen werden selten hinterfragt oder ausreichend getestet.
- Netzwerk-Segmentierungen, um administrative Zonen von normalen Arbeitsplatz-Zonen abzugrenzen, sind nicht durchgängig eingeführt und erlauben ein einfaches "Lateral Movement" des Angreifers.
- Ein effektives Security-Monitoring über die gesamte Infrastruktur fehlt oftmals. Dies ist jedoch zwingend notwendig, um auch gezielte Angriffe zu detektieren und damit zeitnah reagieren zu können.

Fazit

Fortgeschrittene Angriffe sind keine Utopie. Berichte darüber sind fast tagtäglich in den Medien. Hinzu kommt, dass ein Grossteil dieser Angriffe gar nie an die Öffentlichkeit gelangt. Das Sicherheitsniveau der Unternehmen in der Schweiz ist für diese Art von Szenarien noch nicht genügend.

Empfehlungen

Die Sicherheitsmassnahmen müssen laufend den sich verändernden Angriffsszenarien angepasst und periodisch in der notwendigen Tiefe überprüft werden. Dies umfasst nicht nur die präventiven Elemente, welche weiterhin ergänzt und gepflegt werden müssen sondern auch Detektionsverfahren, die eine zeitnahe Reaktion ermöglichen. Investitionen in ein gezieltes Security-Monitoring sind ein Muss, um die aktuell vorhandenen Lücken zu schliessen.