FireEye

FireEye SmartVision

Erkennt verdächtiges Lateral Movement in Unternehmensnetzwerken

HIGHLIGHTS

- Identifizierung bislang nicht erkennbarer verdächtiger Lateral Movements
- Aufdeckung verdächtiger Datenübertragungen im Netzwerk
- Einsatz einer bahnbrechenden Korrelations- und Analyseeinheit in Verbindung mit einem Modul für maschinelles Lernen und über 120 Intrusion-Detection-Regeln
- Unterstützung diverser Bereitstellungsoptionen als Teil von FireEye Network Security

Eine äußerst dynamische Bedrohungslage

Die Bedrohungslage ändert sich derzeit so schnell, dass der Erfolg von Präventivmaßnahmen zur Abwehr raffinierter Angriffe immer ungewisser wird. Früher verschafften Angreifer sich mit Brute-Force-Angriffen Zugang; stahlen, was sie greifen konnten und verschwanden dann wieder. Das ist vorbei. Heute setzen sie sich in den einmal infiltrierten Umgebungen fest und spionieren diese oft über einen langen Zeitraum aus, um die wertvollsten Daten zu finden, bevor sie sich bedienen.

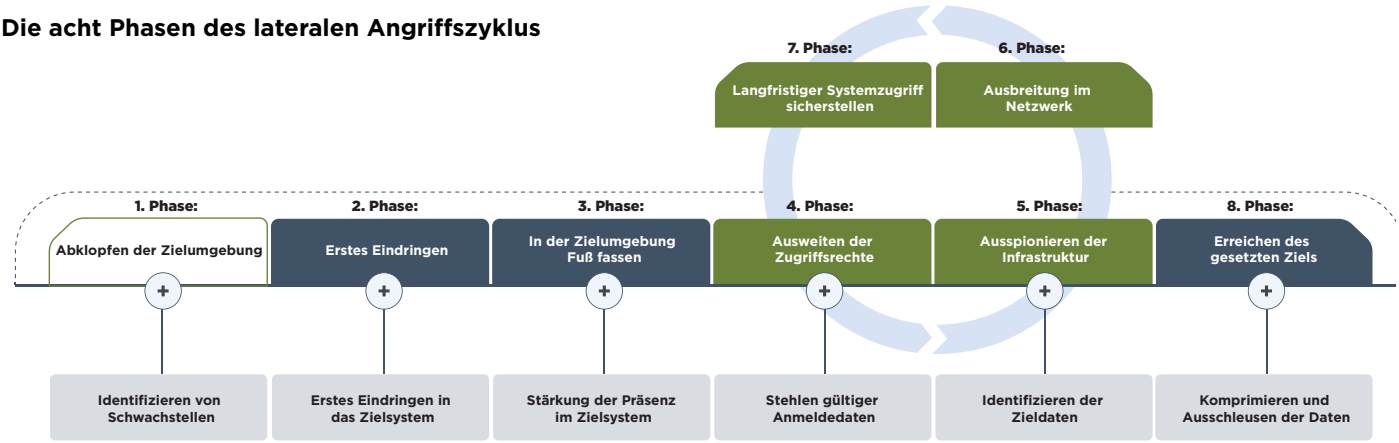
Sie umgehen IDS und andere Bedrohungserkennungsmaßnahmen mit raffinierten Methoden, tarnen sich beim Ausspionieren des Netzwerks und verwischen zudem ihre elektronischen Spuren, um Computerforensikern die Arbeit zu erschweren. Diese Cyberkriminellen installieren oft in jedem infiltrierten System eine eigene Backdoor, die dann speziell für dieses System konfiguriert wird, um ihnen dauerhaft System- und Netzwerkzugang zu bieten.

Eindringlinge im Netzwerk erkennen – eine schwierige Aufgabe

Mit den derzeit verfügbaren Tools ist es leider schwierig oder sogar unmöglich, die Aktivitäten von Hackern zu erkennen, die bereits in Ihr Netzwerk eingedrungen sind und sich nun darin ausbreiten. SIEM-Systeme (Security Information und Event Management) sind beispielsweise für ihren hohen Konfigurations- und Managementaufwand bekannt. Dabei treten oft Fehler auf, die dann dazu führen, dass verdächtige laterale Bewegungen übersehen werden oder (vielleicht noch schlimmer), dass das System Unmengen von Fehlalarmen generiert und das Sicherheitsteam damit hoffnungslos überlastet.

In vielen Unternehmen und Institutionen wird das Netzwerk segmentiert. Zwischen den Segmenten werden Firewalls installiert, um die Aktivitäten von Angreifern – und den damit verbundenen Schaden – wenigstens auf ein Netzwerksegment zu beschränken. Dieser Ansatz treibt jedoch die Kosten und die Netzwerkkomplexität in die Höhe. Oft ist er zudem nicht einmal erfolgreich, weil die Angreifer bereits gültige Anmeldedaten privilegierter Nutzer gestohlen haben, mit denen sie die Firewalls passieren können, ohne Verdacht zu erregen.

Die acht Phasen des lateralen Angriffszyklus



FireEye SmartVision

FireEye hat verschiedene Indikatoren und Aktivitäten identifiziert, die darauf hindeuten, dass Datendiebe in einem Netzwerk aktiv sind. Darauf aufbauend haben wir FireEye SmartVision™ entwickelt, eine neue Fähigkeit zur Erkennung verdächtiger Lateral Movements in Netzwerken, die bislang nicht erkennbar waren.

Wenn Sicherheitsadministratoren SmartVision gemeinsam mit FireEye Network Security nutzen, können sie verdächtige Lateral Movements erkennen und sich damit Einblicke in den Netzwerkverkehr innerhalb des Perimeters sowie zwischen Clients und Servern verschaffen. Früher war das nur an der Netzwerkgrenze möglich.

Zu den wichtigsten Komponenten von SmartVision gehören:

Eine leistungsstarke Korrelations- und Analyse-Engine

Ein Modul für maschinelles Lernen, das Versuche erkennt, Daten auszuschleusen

Über 120 Intrusion-Detection-Regeln, die schwer zu identifizierende IOCs (indicators of compromise) erkennen

Wie SmartVision das Verborgene sichtbar macht

SmartVision erkennt eine Vielzahl verdächtiger Aktivitäten in Unternehmensnetzwerken. Das ist möglich, weil Hackeraktivitäten in den verschiedenen Phasen des lateralen Angriffszyklus charakteristische Merkmale aufweisen, nach denen SmartVision gezielt sucht.

Ausweiten der Zugriffsrechte

In dieser Phase findet SmartVision:

- **Anmeldeversuche mit der Pass-the-Hash-Methode:** Dabei nutzen Angreifer den NTLM- oder LanMan-Hash eines Nutzerpasworts, um sich per Fernzugriff bei einem Server oder Service anzumelden.
- **Dateilose Malware:** SmartVision erkennt Angriffe, bei denen statt Malware legitime Tools wie Mimikatz missbraucht werden, um unverschlüsselte Passwörter, Hashes, PIN-Codes und Kerberos-Tickets zu stehlen.

Ausspionieren der Infrastruktur

In dieser Phase identifiziert FireEye Network SmartVision:

- **Netzwerk-Mapping:** Angreifer nutzen möglicherweise SNMP-basierte Ansätze oder die aktive Erkundung und Analyse von Netzwerkpfaden, um Endpunkte, Server und andere Geräte in einem Netzwerk zu finden und sich Informationen über deren Betriebssystem und Verbindungszustand zu verschaffen.
- **Auflisten von Hosts und Services:** Manche Angreifer missbrauchen Ermittlungstools, um sich Nutzernamen, Arbeitsgruppen, freigegebene Ressourcen, offene Ports, per Fernzugriff erreichbare Hosts und andere Netzwerkdienste anzeigen zu lassen.
- **Nutzersuche:** Auch mithilfe von Tools, die WinAPI-Aufrufe nutzen, können Angreifer herausfinden, welche Nutzerkonten es auf einem Server, Active Directory-Server, Domain Controller oder Endpunkt gibt und welche von ihnen Administratorrechte haben.

Ausbreiten im Netzwerk

In dieser Phase deckt SmartVision Versuche auf, Malware, Dateien und insbesondere Passwort-Dumper mit den Protokollen SMB und SMB2 zu übertragen.

Ausschleusen von Daten

In dieser Phase nutzt SmartVision das Modul für maschinelles Lernen, um anomale Datenübertragungen zu identifizieren, bei denen es sich möglicherweise um Versuche handelt, gestohlene Daten auszuschleusen.

Bereitstellung von SmartVision

SmartVision kann als Bestandteil einer FireEye Network Security-Implementierung auf verschiedene Weise eingesetzt werden, um in unterschiedliche Netzwerkdesigns eingepasst zu werden und deren spezifische Anforderungen zu erfüllen. Die Sensoren für FireEye Network Security werden normalerweise hinter einer Firewall installiert, um den an einen Server gerichteten Netzwerkverkehr zu überwachen. Dort können die Sensoren sowohl den Netzwerkverkehr zwischen Clients und Servern als auch zwischen gleichgestellten Systemen erfassen.

SmartVision unterstützt die Bereitstellung im Inline- und im Out-of-Band-Modus und kann sowohl unternehmensintern als auch in NPB- und TAP-Umgebungen eingesetzt werden.

Fazit

Die Bedrohungslage ändert sich derzeit so schnell, dass der Erfolg von Präventivmaßnahmen zur Abwehr hoch entwickelter Angriffe immer ungewisser wird. Deshalb gewinnt die Suche nach Angreifern, die sich bereits Zugang zu Ihrem Netzwerk verschafft haben, an Bedeutung. Noch brisanter wird die Situation dadurch, dass diese Hacker auch kontinuierlich daran arbeiten, beim Ausspionieren Ihrer Umgebung möglichst lange unbemerkt zu bleiben.

Der typische Verlauf eines solchen Angriffs bringt zahlreiche Herausforderungen mit sich, die mit den derzeit verfügbaren Sicherheitslösungen nicht zufriedenstellend gelöst werden können. FireEye hat jedoch Indikatoren und Aktivitäten identifiziert, die auf Datendiebe in Ihrem Netzwerk hindeuten.

Darauf aufbauend haben wir FireEye SmartVision™ entwickelt, eine innovative Lösung zur Erkennung verdächtiger Lateral Movements in Netzwerken, die bislang nicht erkennbar waren. SmartVision kann nun in verschiedenen Netzwerkarchitekturen als Teil der Plattform FireEye Network Security eingesetzt werden, um verdächtigen lateralen Netzwerkverkehr zu erkennen und Unternehmen vor diesen sich in ihrem Netzwerk ausbreitenden Bedrohungen zu schützen.

Mehr Informationen zu FireEye erhalten Sie unter: **www.FireEye.de.**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035, USA
+1 408 321 6300/+1 877 FIREEYE (347 3393)
info-dach@FireEye.com

SB.FSV.DE-DE-032018