FIREEYE™

DATENBLATT

Malware-Analyse

Angriffsanalyse mit 360° Transparenz

HIGHLIGHTS

- Umfassende forensische Analyse des gesamten Angriffszyklus mithilfe der FireEye MVX-Engine
- Effiziente, stapelweise Analyse von verdächtigem Webcode sowie ausführbaren und anderen Dateien
- Umfassende Informationen zu Eingriffen auf Systemebene in Betriebssystem und Anwendungen, darunter Änderungen an Dateisystem, Speicher und Systemregistrierung
- Live- oder Sandbox-Analyse zur Bestätigung von Zero-Day-Exploits
- Dynamische Erstellung von Bedrohungsdaten für sofortigen lokalen Schutz durch Anbindung an FireEye Central Management
- Erfassung von Datenpaketen für die Analyse von Verbindungen zu schädlichen URLs und dabei ausgeführtem Schadcode
- Anbindung an die AV-Suite von FireEye zur effizienten Priorisierung von Sicherheitsvorfällen
- Support für Windows- und MacOS X-Umgebungen

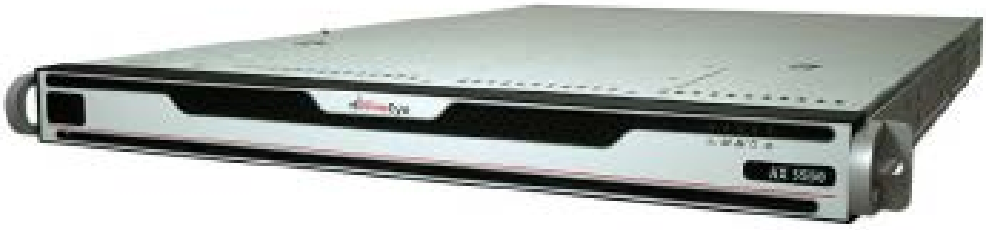

Abbildung 1: Die FireEye Malware-Analyse-Appliance AX 5550

Überblick

Mit einer FireEye Malware-Analyse-Appliance steht Sicherheitsanalysten eine leistungsstarke, vorkonfigurierte Testumgebung für die Untersuchung von komplexer Malware, Zero-Day-Exploits und gezielten APT-Angriffen (Advanced Persistent Threats) zur Verfügung, die Webseiten, E-Mail-Anhänge und infizierte Dateien als Angriffsvektoren nutzen.

Da Cyberkriminelle ihre Angriffsmethoden heute auf einzelne Unternehmen und mitunter sogar auf einzelne Benutzerkonten oder Systeme abstimmen, benötigen Sicherheitsanalysten eine benutzerfreundliche forensische Analyseplattform, mit der sie zügig auf derart gezielte Angriffe reagieren können.

Einschätzung von Angriffen auf Betriebssysteme, Browser und Anwendungen

Mithilfe der FireEye MVX-Engine (Multi-Vector Virtual Execution™) stellen die AX-Appliances internen Sicherheitsanalysten umfassende Informationen über einen Angriff bereit – vom ersten Exploit über die Callback-Ziele bis hin zu Versuchen, weiteren Schadcode herunterzuladen.

Die FireEye MVX-Engine führt verdächtigen Code in einer vorkonfigurierten virtuellen Microsoft Windows- und Apple MacOS X-Analyseumgebung aus, damit gemeinsam genutzte Webobjekte, E-Mail-Anhänge und Dateitypen eingehend untersucht werden können. Darüber hinaus nutzt die Appliance die MVX-Engine, um einzelne Dateien oder ganze Dateigruppen auf Malware zu untersuchen und ausgehende Verbindungen protokollübergreifend zu verfolgen.

Analysieren statt administrieren

Die AX-Appliances entlasten Administratoren von zeitaufwendigen Aufgaben wie der Einrichtung, Konfiguration und Wiederherstellung der virtuellen Maschinen für die manuelle Malware-Analyse. Mit integrierter Anpassung und Steuerungsmöglichkeiten für die testweise Ausführung von Schadcode schaffen sie die forensischen Voraussetzungen für die umfassende, den Anforderungen des Unternehmens entsprechende Aufklärung von Angriffen.

Live-Analyse oder Sandbox-Modus

Die Malware-Analyse-Appliances unterstützen zwei Analysemodi: einen Live-Modus und einen Sandbox-Modus. Malware-Analysten können den Live-Modus mit Netzwerkanbindung nutzen, um den gesamten Angriffszyklus einschließlich der Verbindungen nach außen zu verfolgen. Auf diese Weise können sie komplexe Angriffe über mehrere Phasen und Angriffsvektoren hinweg verfolgen. Im Sandbox-Modus ist die Ausführung der zu untersuchenden Malware-Proben vollständig in die virtuelle Umgebung eingeschlossen und dort transparent.

In beiden Modi ist es möglich, ein dynamisches und anonymisiertes Profil des Angriffs zu erstellen, das anschließend über FireEye Central Management an andere FireEye-Lösungen übermittelt werden kann. Die von AX-Appliances erstellten Malware-Angriffsprofile enthalten die Merkmale des Malware-Codes, URLs von Exploits und andere Quellen eingehender Infektionen und Angriffe. Auch die Merkmale des Kommunikationsprotokolls der Malware können erfasst und mithilfe der FireEye DTI-Lösung (Dynamic Threat Intelligence™) verbreitet werden, um versuchten Datendiebstahl im Bereich der gesamten FireEye-Infrastruktur eines Unternehmens zu verhindern.

Individuelle Anpassung durch YARA-Regeln

Die Malware-Analyse-Appliances unterstützen den Import eigener YARA-Regeln, sodass Regeln auf Byte-Ebene definiert und verdächtige Objekte schnell und gezielt auf bestimmte Bedrohungen untersucht werden können.

Globales Netzwerk zum Schutz vor Malware

Über FireEye Central Management können die Malware-Analyse-Appliances forensische Malwaredaten automatisch mit anderen FireEye-Plattformen austauschen, versuchten Datendiebstahl unterbinden und erkannte eingehende Angriffe stoppen. Zudem können die Bedrohungsdaten der AX-Appliances über die FireEye DTI-Cloud weitergeleitet werden, um andere Installationen vor neuen Angriffen zu schützen.

Da die FireEye MVX-Engine vorkonfiguriert ist, müssen die Administratoren sich weder um ihre Einrichtung und Konfiguration noch um die Feineinstellung der Heuristik kümmern. Des Weiteren erleichtern die AX-Appliances Sicherheitsexperten die Analyse komplexer gezielter Angriffe, ohne zusätzlichen Aufwand beim Netzwerk- und Sicherheitsmanagement zu verursachen.

Tabelle 1: Technische Daten

	AX 5550
Leistung*	Bis zu 8.200 Analysen pro Tag
Unterstützte Betriebssysteme	Microsoft Windows / Apple MacOS X
Netzwerk-Ports	2 Ports für 10/100/1000 Base-T
IPMI-Port (Rückseite)	Vorhanden
Tastenfeld	Vorhanden
DB15-VGA-Ports (Rückseite)	Vorhanden
USB-Ports (Rückseite)	4 USB-Ports Typ A
Serieller Port (Rückseite)	115.200 bit/s; keine Parität; 8 Bit; 1 Stoppbit
Laufwerkskapazität	2 HDD mit je 4 TB; RAID 1; 3,5 Zoll; FRU
Gehäuse	1 HE, passend für 19-Zoll-Rack
Abmessungen (B × T × H)	437 × 650 × 43,2 mm
Gleichstromanschluss	Nicht verfügbar
Wechselstromanschluss	Redundant (1+1) 750 Watt bei 100–240 V AC; 8–4,5 A; 50–60 Hz; Eingang nach IEC 60320-C14; FRU
Maximaler Stromverbrauch	225 W

Tabelle 1: Technische Daten

	AX 5550
Maximale thermische Verlustleistung	225 W
MTBF (mittlere Betriebsdauer zwischen Ausfällen)	54.200 Std.
Nettogewicht der Appliance / Versandgewicht (kg)	12,2 kg / 17,2 kg
Sicherheitszertifizierungen	IEC 60950, EN 60950, CSA 60950-00, CE-Kennzeichnung
EMC-/EMI-Zertifizierungen	FCC (Teil 15 Klasse A), CE (Klasse A), CNS, AS/NZS, VCCI (Klasse A)
Richtlinien und Normen	RoHS, REACH, WEEE
Betriebstemperatur	0–40 °C
Relative Luftfeuchtigkeit bei Betrieb	10 bis 95% bei 40 °C, nicht kondensierend
Maximale Betriebshöhe	3000 m

* Hinweis: Die Leistungswerte beziehen sich auf die standardmäßige Analysedauer beim Einsatz der Malware-Analyse-Appliance. Die tatsächlichen Werte sind abhängig von der Systemkonfiguration und der Art des verarbeiteten Datenverkehrs.

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

Über FireEye, Inc.
FireEye spezialisiert sich auf datengestützte Sicherheit. FireEye erweitert die Sicherheitskapazitäten seiner Kunden nahtlos und skalierbar und bietet über eine einheitliche Plattform die weltweit anerkannten Beratungsdienste von Mandiant®, innovative Sicherheitstechnologien und Bedrohungsdaten an, die denen staatlicher Sicherheitsbehörden in nichts nachstehen. Mit diesem Ansatz übernimmt FireEye die Verantwortung für die Vorbereitung von Kundenunternehmen auf die Erkennung und Abwehr von Cyberangriffen.