Kurzvorstellung

Absicherung von IoT-Geräten zum Schutz vor Angriffen

Der erfolgreiche Distributed-Denial-of-Service-Angriff (DDoS) auf die verwaltete DNS-Infrastruktur von Dyn im Oktober 2016 wurde im *McAfee Labs Threats-Report vom April 2017* umfassend analysiert.

Der Angriff wurde mithilfe des DNS-Protokolls durchgeführt, sodass Sicherheitstechnologien äußerste Schwierigkeiten hatten, legitimen und böswilligen Datenverkehr zu unterscheiden. Das Problem wurde dadurch verschärft, dass der legitime und böswillige Datenverkehr von Millionen IP-Adressen aus der ganzen Welt stammte.

Da die IoT-Infrastruktur (Internet der Dinge) häufig unzureichend gesichert ist, nimmt die Zahl solcher DDoS-Angriffe zu. Die beim Dyn-Angriff verwendete Mirai-Malware missbrauchte unterschiedlichste unzureichend gesicherte IoT-Geräte wie Videorecorder, Drucker, Überwachungskameras, Kühlschränke oder Thermostate. Sobald ein IoT-Gerät infiziert war, weitete die Malware die Infektion auf weitere IoT-Geräte aus, um ein Botnet zu bilden und anschließend die gesamte Verarbeitungsleistung für einen DDoS-Angriff zu nutzen.

Laut dem Dyn-Sicherheitsteam waren auf dem Höhepunkt des Angriffs dutzende Millionen böswilliger IoT-Geräte Teil des Mirai-basierten Botnets.

Es gibt keine einfache Möglichkeit, Netzwerkgeräte auf entsprechende Infektionen zu überprüfen oder die aktuelle Infektionsphase festzustellen (d. h. erste Schritte der Code-Ausführung, Ausweitung im Netzwerk oder Kommunikation mit dem Kontroll-Server für die Einbindung ins Botnet zur Durchführung von DDoS-Angriffen). Es gibt jedoch Sicherheitsempfehlungen für die Absicherung Ihrer IoT-Geräte sowie für den Schutz Ihres vertrauenswürdigen Netzwerks.

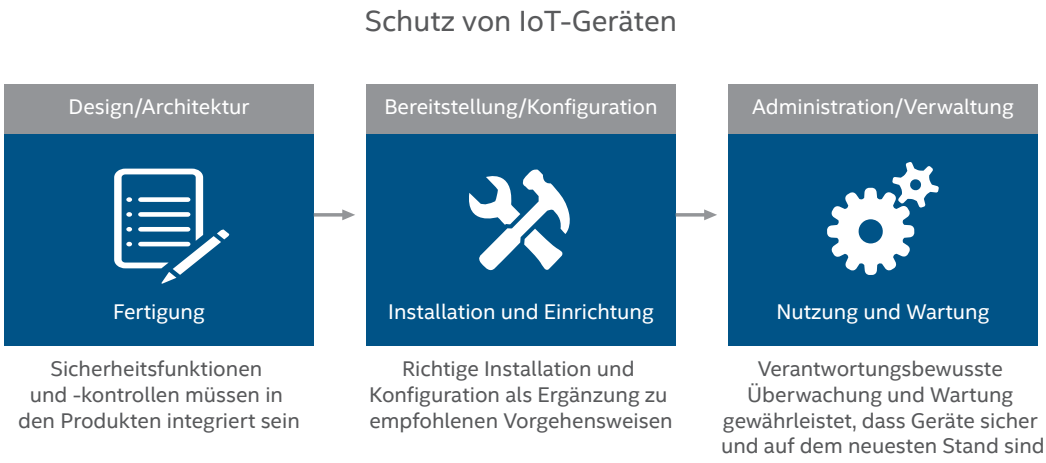
Absicherung von IoT-Geräten

Angreifer wählen stets den Weg des geringsten Widerstands, um die Kontrolle über IoT-Geräte zu erlangen. Am häufigsten kommen dafür schwache Anmeldeinformationen in Frage, doch auch stärkere Anmeldedaten und andere Sicherheitskontrollen stellen keine unüberwindbare Hürde dar. Dieses Muster haben wir bei vielen Angriffsvektoren erlebt.

Intel Security empfiehlt die Blockierung bekannter Exploits und wahrscheinlicher zukünftiger Angriffsmethoden. Mit den folgenden Maßnahmen können Sie IoT-Geräte von der Herstellung bis hin zur Außerdienststellung absichern:

intel Security

Kurzvorstellung



1. **Sicherheit als Teil des Entwicklungsprozesses:** IoT-Hersteller müssen Sicherheit in die Architektur, Schnittstellen und Konzepte ihrer Produkte integrieren. Implementieren und testen Sie grundlegende Sicherheitskonzepte sowie -funktionen wie die Trennung von Daten und Code, Kommunikation zwischen vertrauenswürdigen Parteien, Datenschutz bei verwendeten und gespeicherten Daten sowie Benutzerauthentifizierung. Produkte werden in Zukunft noch leistungsfähiger sein, mehr Daten speichern und vielfältigere Funktionen besitzen. Daher sollten die Produkte Sicherheitsaktualisierungen, Funktionssperrungen, Versionsüberprüfung, Software-Analysen sowie Standardkonfigurationen zulassen, die Branchenempfehlungen folgen. Den Anfang macht der Hersteller, und die Zukunftssicherheit beginnt auf dem Reißbrett. Hardware, Firmware, Betriebssysteme und Software müssen so konzipiert sein, dass sie in einer feindlichen Umgebung sicher funktionieren können. Vor dem Kauf sollten potenzielle IoT-Gerätekäufer die Frage stellen, ob der Hersteller bei der Konzeption und Entwicklung des Geräts die Sicherheit berücksichtigt hat.
2. **Sichere Bereitstellung und Konfiguration:** Die meisten IoT-Geräte müssen bei der Installation in irgendeiner Form konfiguriert und bereitgestellt werden. Die Geräteidentität und Authentifizierung ist ein grundlegender Teil dieses zweistufigen Prozesses. Daher sind angemessene Standardkonfigurationen unverzichtbar, die den empfohlenen Vorgehensweisen entsprechen und für Benutzer einfach verständlich sind. Regeln sollten keine Standard-kennwörter zulassen, Signaturen für Patches sowie Updates erzwingen, die Verschlüsselung von Daten vorschreiben und lediglich sichere Web-Verbindungen erlauben. Unternehmen können einen großen Beitrag zur Absicherung ihrer IoT-Geräte leisten, indem sie den Netzwerkzugang einschränken, Patches zeitnah ausbringen und ausschließlich zulässige Software gestatten. Geräte mit entsprechendem Funktionsumfang sollten zusätzlich mit Sicherheits-Software für Malware- und Eindringungsschutz sowie lokalen Firewalls abgesichert werden. Erkennung und Telemetrie sollten so konfiguriert werden, dass sie Angriffe auf Systeme oder Abweichungen vom beabsichtigten Verhalten erkennen. Außerdem sind Richtlinien für Datenschutz, Daten-aufbewahrung, Fernzugriff, Schlüsselsicherheit und Gerätesperrung erforderlich.
3. **Ordnungsgemäße Kontrolle und Verwaltung:** Bei Geräten für Verbraucher müssen diese das letzte Wort darüber haben, wie das Gerät verwaltet wird. Hersteller und Online-Dienst-anbieter spielen eine Rolle bei der Bereitstellung, doch die Besitzer müssen die Kontrolle über die Aktivitäten der Geräte behalten. Bereitstellung ist nicht das gleiche wie Verwaltung. Beispielsweise ist es während der Installation von Heimkameras sinnvoll, beim Hersteller die neuesten Patches anzufordern und vielleicht sogar einen Cloud-Speicher einzurichten. Doch die Kunden möchten keine Heimkameras, die vom Hersteller kontrolliert werden. Er sollte daher keine Möglichkeit besitzen, die Geräte ohne Wissen des Käufers zu betreiben. Die Besitzer müssen ihre Produkte ein- und ausschalten sowie festlegen können, mit welchen Online-Diensten eine Verbindung hergestellt werden darf. Diese Funktionen erfordern ordnungsgemäße Benutzeridentifizierung und -authentifizierung. Die Möglichkeit zur Festlegung

eines häufig verwendeten Kennworts ist nicht wünschenswert, da sich sonst jedermann als Administrator anmelden könnte. Stellen Sie sich vor, wenn Windows auf jedem System ein standardmäßiges Anmeldekennwort bieten würde. Das würde einen sicherheitstechnischen Alptraum bedeuten, da viele Benutzer es niemals ändern würden und die Angreifer sich an ihrer Stelle anmelden könnten. IoT-Systeme müssen zuerst in der Lage sein, ihre Besitzer zu authentifizieren. Verwaltungsfunktionen müssen den Besitzern auch die Möglichkeit bieten, Beschränkungen, Datenrichtlinien und Datenschutzparameter festzulegen, die restriktiver sind als die aller potenziellen Drittanbieter. Signierte Sicherheits-Updates sollten sofort nach ihrer Veröffentlichung automatisch installiert werden. Erfahrene Benutzer sollten Beschränkungen für ein- und ausgehende Verbindungen, Datentypen, Ports und Sicherheitseinstellungen festlegen können. Protokolle, die auf ein vertrauenswürdiges System übertragen oder lokal angezeigt werden können, sollten Fehler sowie unerwartete und ungewöhnliche Aktivitäten erfassen. Ein System für Remote-Warnungen per E-Mail oder SMS ist bei einigen Geräten eine sinnvolle Funktion. Und zu guter Letzt ist eine Reset-Funktion notwendig, falls es zu einer nicht behebbaren Kompromittierung oder einem Besitzerwechsel kommt.

Umsetzbare Richtlinien und Vorgehensweisen zur Absicherung von IoT-Geräten

- **Untersuchen Sie die Sicherheitshistorie des IoT-Geräts.** Vor dem Kauf eines IoT-Geräts sollten Sie überprüfen, ob bei dem Gerät oder dem Anbieter bzw. Hersteller Probleme aufgetreten sind. Eine schnelle Internetsuche genügt häufig bereits. Die Webseite der US-Bundeshandelskommission (Federal Trade Commission, FTC) listet frühere Maßnahmen auf. Mit einiger Recherche stellen Sie vielleicht fest, dass einige Unternehmen die Sicherheitsbelange ihrer Produkte vernachlässigen, während andere deutlich aktiver sind.
- **Halten Sie die Software aller IoT-Geräte auf dem neuesten Stand.** Dieser grundlegende Schritt beseitigt häufig Schwachstellen, insbesondere solche, die erst kürzlich bekannt wurden und breite Aufmerksamkeit erfuhren. Sie sollten ein Verfahren zur Patch-Installation ausarbeiten und überprüfen, ob die Patches ordnungsgemäß installiert wurden.
- **Minimieren Sie das Risiko für nicht patchbare IoT-Geräte** mit Anwendungs-Whitelists, die Systeme abriegeln und die Ausführung nicht genehmigter Programme verhindern.
- **Trennen Sie IoT-Geräte vom restlichen Netzwerk,** z. B. mit einer Firewall und einem Eindringungsschutzsystem. Deaktivieren Sie nicht benötigte Dienste und Ports auf diesen Systemen, um die Zahl der möglichen Infektionseintrittspunkte zu reduzieren. Mirai nutzt nicht verwendete Ports aus.
- **Ändern Sie Standardwerte, und legen Sie starke Kennwörter fest.** Die größte Gefahr für IoT-Geräte sind schwache oder standardmäßig festgelegte Kennwörter. Verwenden Sie für Ihre Kennwörter daher lange Phrasen, Sonderzeichen, Groß-/Kleinschreibung sowie Ziffern. Kennwörter müssen stark sein, damit sie nicht leicht erraten werden können.
- **Nutzen Sie IoT-Sicherheitseinstellungen.** Einige IoT-Geräte bieten erweiterte Konfigurationsmöglichkeiten, die Sie so weit wie möglich nutzen sollten. Zudem erlauben manche IoT-Produkte separate Netzwerkeinstellungen, ähnlich wie bei einem Gast-WLAN-Netzwerk, das parallel zu Ihrer Hauptverbindung betrieben werden kann. Das ist nur ein Beispiel – andere Produkte können noch weitere Funktionen bieten.
- **Vernetzen Sie IoT-Geräte über sichere WLAN-Verbindungen.** Nutzen Sie starke Kennwörter sowie die neuesten Sicherheitsprotokolle (z. B. WPA2).
- **Schränken Sie den physischen Zugriff auf IoT-Geräte ein.** Auch die unmittelbare Manipulation an den Geräten kann Hacks ermöglichen.
- **Deaktivieren Sie Universal Plug and Play (UPnP).** Viele IoT-Geräte unterstützen UPnP, sodass sie über das Internet leicht zu finden und somit für Malware-Infektionen anfällig sind. Daher sollte UPnP möglichst deaktiviert werden.
- **Schalten Sie IoT-Geräte regelmäßig aus.** Malware befindet sich meist im flüchtigen Speicher und kann durch einen Neustart entfernt werden.

So können Intel Security-Produkte Systeme und Netzwerke vor Angriffen durch IoT-Geräte schützen

Neben der oben genannten Liste empfohlener Vorgehensweisen für IoT-Geräte können Intel Security-Produkte dabei helfen, die Risiken von Malware-Infektionen bei IoT-Geräten zu minimieren und böswillige Botnet-Aktivitäten zu blockieren. Folgende Intel Security-Produktkonfigurationen können IoT-Geräte absichern und Systeme sowie Netzwerke vor Angriffen durch IoT-Geräte schützen:

McAfee VirusScan® Enterprise 8.8 oder McAfee Endpoint Security 10

- Halten Sie DAT-Dateien auf dem neuesten Stand.
- Stellen Sie sicher, dass McAfee Global Threat Intelligence (McAfee GTI) verwendet wird. McAfee GTI erkennt mehr als 600 Millionen verschiedene Malware-Signaturen.
- Erstellen Sie Zugriffsschutzregeln, um die Installation und Inhalte von Malware zu stoppen:
  - Sehen Sie sich hierzu die KnowledgeBase-Artikel zu Zugriffsschutzregeln an: KB81095 und KB54812.
  - Lesen Sie die empfohlenen Vorgehensweisen zur Konfiguration von McAfee VirusScan Enterprise 8.8: PD22940.
  - Lesen Sie die empfohlenen Vorgehensweisen zur Konfiguration von McAfee Endpoint Security: KB86704.

McAfee Host Intrusion Prevention

- McAfee Host Intrusion Prevention unterstützt Sie dabei, die Ausbreitung der Malware zu verhindern. Dank benutzerdefinierter IPS-Signaturen können Sie Regeln erstellen, mit denen von der Malware generierte Dateiaktionen (z. B. Erstellen, Schreiben, Ausführen, Lesen) blockiert werden.
- Aktivieren Sie die Signatur 3894 von McAfee Host Intrusion Prevention, „Access Protection—Prevent svchost.exe executing non-Windows executables“ (Zugriffsschutz, um zu verhindern, dass „svchost.exe“ ausführbare Dateien ausführt, die nicht von Windows stammen).
- Aktivieren Sie die Signaturen 6010 und 6011 von McAfee Host Intrusion Prevention, um die Injektion sofort zu blockieren.
- Dies erreichen Sie mit zwei Unterregeltypen:
  1. Erstellen Sie im Files-Modul eine benutzerdefinierte IPS-Signatur sowie eine Unterregel mit den folgenden Kriterien:
     - Name: <Namen einfügen>
     - Rule type: Files
     - Operations: Create, Execute, Read, Write
     - Parameters: Include - Files - <Pfad/Dateiname der Malware>
       - Der Dateiname muss einen Pfad enthalten. Wenn Sie im Pfad Platzhalter verwenden möchten, beginnen Sie den Dateinamen mit „**\“ bzw. „?:\“, wenn sich der Platzhalter auf den Laufwerkbuchstaben beziehen soll (z. B. „**\Dateiname.exe“ oder „?:\Dateiname.exe“).
       - Sie können für den Parameter „Files“ keine MD5-Hash-Werte, sondern nur Pfad/Dateiname verwenden.
       - Sie können den Laufwerktyp angeben, um den Pfad auf ein bestimmtes Laufwerk zu beschränken (z. B. Festplatte, CD-ROM, USB, Netzwerk, Diskette).
     - Executables: Kann leer bleiben, sofern Sie nicht die Signatur auf bestimmte Prozesse beschränken möchten, die die Dateiaktion ausführen (z. B. explorer.exe oder cmd.exe).

2. Erstellen Sie im Program-Modul eine benutzerdefinierte IPS-Signatur sowie eine Unterregel mit den folgenden Kriterien:
   - Name: <Namen einfügen>
   - Rule type: Program
   - Operations: Run target executable
   - Parameters: <leer lassen>
   - Executables: Kann leer bleiben, sofern Sie nicht die Signatur auf einen bestimmten Prozess als ausführbare Quelle beschränken möchten (z. B. wenn Sie verhindern möchten, dass „explorer.exe“ ein Target Executable (z. B. notepad.exe) ausführen kann).
   - Target Executables: Definieren Sie die ausführbaren Eigenschaften, für die Sie die Ausführung verhindern möchten (z. B. wenn Sie die Ausführung von „notepad.exe“ blockieren möchten, geben Sie Pfad/Dateiname der ausführbaren Datei an). Die ausführbare Datei kann mit mehreren Kriterien definiert werden (Dateibeschreibung, Dateiname, Fingerabdruck, Signaturgeber).

McAfee SiteAdvisor® Enterprise oder McAfee Web Protection

- Nutzen Sie die Reputation von Webseiten, um Benutzer vor Webseiten zu schützen oder zu warnen, über die Malware verbreitet wird.

McAfee Threat Intelligence Exchange und McAfee Advanced Threat Defense

- Richtlinienkonfiguration bei McAfee Threat Intelligence Exchange:
  - Starten Sie im Beobachtungsmodus: Wenn Endgeräte mit verdächtigen Prozessen erkannt werden, nutzen Sie System-Tags, um die Durchsetzungsrichtlinien von McAfee Threat Intelligence Exchange anzuwenden.
  - Säubern bei Reputation „Known malicious“ (Bekannt böswillig).
  - Blockieren bei Reputation „Most-likely malicious“ (Höchstwahrscheinlich böswillig). (Die Blockierung bei Status „Unknown“ (Unbekannt) würde besseren Schutz bieten, aber möglicherweise auch den Anfangsaufwand für Administratoren erhöhen.)
  - Legen Sie für die Option „Submit files to McAfee Advanced Threat Defense“ (Dateien an McAfee Advanced Threat Defense senden) die Statuswerte „Unknown“ (Unbekannt) und darunter fest.
  - McAfee Threat Intelligence Exchange Server-Richtlinie: Akzeptieren Sie die von McAfee Advanced Threat Defense festgelegten Reputationen für Dateien, die von McAfee Threat Intelligence Exchange noch nicht erkannt wurden.
- Manueller Eingriff bei McAfee Threat Intelligence Exchange:
  - Erzwingung der Datei-Reputation (bei Betriebsmodus): Bereinigen/Löschen bei Reputation „Most likely malicious“ (Höchstwahrscheinlich böswillig).
  - Blockieren bei Reputation „Might be malicious“ (Möglicherweise böswillig).
- Die Reputation innerhalb des Unternehmens kann McAfee GTI außer Kraft setzen.
  - Sie können optional festlegen, dass unerwünschte Prozesse blockiert werden (z. B. nicht unterstützte oder anfällige Anwendungen).
  - Kennzeichnen Sie die entsprechende Datei als „Might be malicious“ (Möglicherweise böswillig).
- Oder Sie erlauben einen unerwünschten Prozess zu Testzwecken:
  - Kennzeichnen Sie die entsprechende Datei als „Might be trusted“ (Möglicherweise vertrauenswürdig).

McAfee Advanced Threat Defense

- Erkennungsfunktionen:
  - Erkennung auf Signaturbasis: McAfee GTI umfasst mehr als 600 Millionen Malware-Signaturen.
  - Reputationsbasierte Erkennung durch McAfee GTI.
  - Statische Analyse und Emulation in Echtzeit für signaturlose Erkennung.
  - Benutzerdefinierte YARA-Regeln.
  - Vollständige statische Code-Analyse: Führt ein Reverse Engineering des Datei-Codes durch, um Attribute sowie Befehle zu untersuchen und den Code vollständig zu analysieren, ohne ihn dabei auszuführen.
  - Dynamische Sandbox-Analyse.
- Erstellen Sie Analyseprofile für die Bereiche, unter denen Malware vermutlich ausgeführt wird:
  - Verbreitete Betriebssysteme, Windows 7, 8, 10.
  - Installieren Sie Windows-Anwendungen (Word, Excel), und aktivieren Sie Makros.
- Internetzugriff für das Analyseprogramm-Profil:
  - Viele Malware-Varianten führen ein Skript aus einem Microsoft-Dokument aus, das eine ausgehende Verbindung herstellt und den Schadcode aktiviert. Dem Analyseprogramm-Profil wird eine Internetverbindung bereitgestellt, was die Erkennungsraten weiter erhöht.

McAfee Network Security Platform

- McAfee Network Security Platform verfügt in den Standardrichtlinien über Signaturen zur Erkennung des Netzwerks Tor, das zur Übertragung von Dateien genutzt werden kann, die in Verbindung mit Malware stehen.
- Integrieren Sie McAfee Advanced Threat Defense zur Abwehr neuer Angriffsvarianten:
  - Konfigurieren Sie die Integration von McAfee Advanced Threat Defense in der erweiterten Malware-Richtlinie.
  - Konfigurieren Sie McAfee Network Security Platform so, dass EXE-Dateien, Microsoft Office-Dateien, Java-Archivdateien und PDF-Dateien zur Überprüfung an McAfee Advanced Threat Protection gesendet werden.
  - Überprüfen Sie, ob die Konfiguration von McAfee Advanced Threat Protection auf Sensorebene angewendet wird.
- Aktualisieren Sie die Callback-Erkennungsregeln (zum Schutz vor Botnets).

McAfee Web Gateway

- Aktivieren Sie die Analyse durch McAfee Gateway Anti-Malware.
- Aktivieren Sie McAfee GTI für URL- und Datei-Reputation.
- Integrieren Sie McAfee Advanced Threat Defense für Sandbox-Analysen und Zero-Day-Erkennung.

VirusTotal Convicter: Automatischer Eingriff

- Convicter ist ein Python-Skript, das vom automatischen Reaktionssystem von McAfee ePolicy Orchestrator® (McAfee ePO) ausgelöst wird, um eine Datei, die ein McAfee Threat Intelligence Exchange-Bedrohungsereignis erzeugt, mit VirusTotal abzugleichen.
- Sie können das Skript so ändern, dass andere Daten zu Bedrohungsanalysen ausgetauscht werden, z. B. GetSusp.
- Wenn der Schwellenwert zum Vertrauen der Community erreicht wird, setzt das Skript automatisch die Unternehmensreputation fest. Vorgeschlagener Schwellenwert: 30 % der Anbieter und zwei wichtige Anbieter müssen zustimmen.
- Filter: "Target File Name Does Not Contain (Name der Zieldatei enthält nicht): McAfeeTestSample.exe".
- Dies ist ein kostenloses, von der Community unterstütztes Tool (wird von Intel Security nicht unterstützt).

McAfee Endpoint Threat Defense and Response

- McAfee Endpoint Threat Defense and Response findet und beseitigt hochentwickelte Bedrohungen. Wenn die Anwendung zusammen mit Bedrohungsdaten-Feeds von McAfee GTI, Dell SecureWorks oder ThreatConnect eingesetzt wird, können Sie nach neuen Bedrohungen suchen und diese entfernen, bevor sie die Gelegenheit haben, sich auszubreiten.
- Benutzerdefinierte Kollektoren ermöglichen die Entwicklung spezieller Tools, um mit Malware in Verbindung stehende Kompromittierungsindikatoren zu finden und zu identifizieren.
- Der Benutzer legt mit Auslösern und Reaktionen fest, welche Aktionen bei bestimmten Bedingungen ausgeführt werden sollen. Wenn zum Beispiel Hash-Werte oder Dateinamen gefunden werden, kann automatisch eine Löschen-Aktion ausgeführt werden.

Weitere Informationen

Whitepaper: *More Confidence, Safety, and Security in the Digital World (Mehr Vertrauen und Sicherheit in der digitalen Welt)*

Best Practices for how to use Host IPS rules for a malware outbreak (Empfohlene Vorgehensweisen für die Verwendung von McAfee Host Intrusion Prevention-Regeln bei einem Malware-Ausbruch): KB84507

SIEM orchestration. How McAfee Enterprise Security Manager can drive action, automate remediation, and increase situational awareness (Koordinierung von SIEM: So kann McAfee Enterprise Security Manager die Durchführung von Maßnahmen unterstützen, die Fehlerbehebung automatisieren und den Einblick in die Sicherheitslage verbessern): PD24830

Whitepaper: *Sicherheit auch ohne Signatur*

FAQs for Network Security Platform: Advanced Malware Detection (Häufige Fragen und Antworten zu McAfee Network Security Platform: Erkennung hochentwickelter Malware): KB75269

Produkthandbuch zu McAfee Web Gateway. Web-Filterung: PD26339

McAfee. Part of Intel Security.
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com