WHITEPAPER

Schutz des IoT-Ökosystems mit Fortinet

Die möglichen Folgen eines erfolgreichen Cyberangriffs auf ein IoT-Ökosystem (Internet der Dinge) können zum Ausfall kritischer Systeme und Produktionsanlagen bis hin zu physischen Gefahren für Mensch und Umwelt führen. Anbieter von IoT-Lösungen müssen sich dieser Problematik bewusst sein und sollten nur Dienste bereitstellen, die von Grund auf sicher ist.

Managed Service Provider (MSP), Managed Security Service Provider (MSSP) und Mobilfunkbetreiber (MNO) müssen die Security in IoT-Lösungen und -Diensten integrieren, um drei Hauptziele zu erreichen:

1. Schutz des gesamten IoT-Ökosystems, um die Dienstkontinuität zu gewährleisten
2. Servicevereinbarungen (SLA) speziell für die IoT-Security, um die Einführung und Akzeptanz von IoT-Diensten zu fördern
3. Erschließen neuer Einnahmequellen durch IoT-Sicherheitsdienste

IoT-Security-Lösungen von Fortinet

Die Fortinet IoT-Lösung besteht aus mehreren bewährten Sicherheitskomponenten, die gemeinsam einen umfassenden Schutz für ein IoT-Ökosystem bieten. Da der Begriff IoT eher weitreichend ist, muss jede Lösung eine breite, integrierte und automatisierte Funktionalität bieten, die bei Bedarf jeden einzelnen Anwendungsfall abdeckt.

Fortinet IoT-Sicherheitsfunktionen werden über die branchenweit umfassendste Palette von Netzwerk-Security-Produkten bereitgestellt. Diese Produkte sind nicht nur untereinander vernetzt, sondern auch in die Fortinet Security Fabric integriert. Unternehmen erhalten damit eine leistungsstarke Plattform, um eine durchgängige Security für das IoT-Ökosystem sowie End-to-End-Sicherheitsdienste zu realisieren.

Die Fortinet IoT-Sicherheitsfunktionen werden über die FortiGate Next Generation Firewall (NGFW) und die FortiWeb Application Firewall bereitgestellt. Beide Lösungen umfassen mehrere physische und virtuelle Angebote.

FortiGate-Segmentierung und Stateful Firewalling

Die Traffic-Muster eines IoT-Geräts sind meistens sehr vorhersehbar und eine FortiGate Stateful Firewall kann jeglichen Verkehr an unautorisierte Ziele blockieren sowie Warnungen bei ungewöhnlichem Geräteverhalten auslösen. In einer typischen IT-Umgebung kann es viele Gründe für Datenverkehr zu unautorisierten Zielen geben und in der Regel wird eine solche Kommunikation einfach unterbrochen. In IoT- und anderen Machine-to-Machine-Netzwerken ist eine solche Kommunikation normalerweise ein Zeichen für eine Fehlkonfiguration oder eine Kompromittierung. Daher sollten bestimmte negative Regeln mit einer geeigneten Aktion konfiguriert werden, damit auf jeden Fall eine Warnung bzw. eine automatische Korrektur erfolgt.

FortiGate Intrusion Prevention

Der FortiGate Intrusion Prevention Service wurde entwickelt, um unterschiedlichste IoT-Angriffe zu erkennen und zu blockieren wie z. B.:

- **Exploits:** allgemeine Bezeichnung von Angriffen auf Schwachstellen. Darunter fallen DoS-Attacken (Denial-of-Service), bei denen die Software zum Abstürzen gebracht oder mit massiven Anfragen überlastet wird. Exploits können aber auch zur Ausführung von lokalem Code führen, um eine zweite Angriffsstufe vorzubereiten, z. B. die Einschleusung einer bösartigen EXE-Datei.
- **Scan-Angriffe:** Suche nach offenen TCP-Ports (Transmission Control Protocol) oder UDP-Ports (User Datagram Protocol) oder nach als anfällig bekannten Software- oder Protokollversionen. Normalerweise besteht das Ziel solcher Sondierungsangriffe darin, anfällige oder wertvolle Ziele zu identifizieren.
- **Fuzzing-Angriffe:** weitere Methode zum Auffinden von Schwachstellen. Ein Angriff erfolgt normalerweise lokal in einer kontrollierten Umgebung, kann sich jedoch auch mit „stumpfen Waffen“ gegen ein Live-Netzwerk richten. Beispiele hierfür sind absichtliche Protokollanomalien, die Verwendung extrem langer Felder sowie ungültige oder ungewöhnliche Daten. All diese Techniken sollen Programmierfehler auslösen, um so Schwachstellen zu finden oder Störungen zu verursachen.

Diese und weitere Angriffsformen werden vom FortiGate Intrusion Prevention System (IPS) abgedeckt. Die Fortinet IPS-Funktion umfasst über 30 000 Regeln, darunter ein optionales Regelpaket speziell für die Industrie. Die Regelpakete werden täglich automatisch aktualisiert, damit der Schutz stets auf dem neuesten Stand ist.

Mit dem Fortinet IPS können auch durchsatzbasierte Regeln definiert werden. Da viele IoT-Geräte eine vorhersagbare Paketrate haben, lassen sich so ungewöhnliche Aktivitäten erkennen, die oft ein Hinweis auf Fehlfunktionen oder Kompromittierungen sind. Verdächtige IoT-Geräte werden dann gleich aus dem Netzwerk genommen.

In allen Netzwerk-Bereichen gibt es einen allgemeinen Trend zur Datenverschlüsselung. Dies gilt auch für das Internet der Dinge (IoT), wo viele vertrauliche Daten übertragen werden. Am häufigsten wird hier die Transport Layer Security (TLS) verwendet. Das IPS kann auch TLS-Inspektionen durchführen, um versteckte Angriffe über solche sicheren Verbindungen zu erkennen.

FortiGate Application und Protocol Control

Mit der Application-Control-Funktion lassen sich die Protokolle überwachen oder einschränken, die ein IoT-Gerät verwenden kann. Nicht autorisierte Protokolle können eine Warnung generieren und optional blockiert werden. Die Anwendungsdefinitionen umfassen über 4000 Anwendungsregeln in 24 Kategorien. Alle gängigen IoT-Protokolle wie MQTT, AMQP, HTTP und CoAP sind abgedeckt. Auch kann die TLS-Inspektion im IPS speziell konfiguriert werden. Zudem werden zahlreiche Industrie-Protokolle für IIoT-Lösungen (Industrielles Internet der Dinge) unterstützt.

Antivirus

Fortinet verfügt über eine bewährte Virenschutz-Lösung für die Industrie, gestützt durch die Bedrohungsforschung der FortiGuard Labs und künstliche Intelligenz (KI). Gemeinsam mit der Intrusion Prevention sorgt Fortinet Antivirus dafür, dass der Großteil bösartiger Dateien erst gar nicht das Ziel erreicht.

Ein Virenschutz ist heute vor allem für die IoT-Infrastruktur (z. B. für Plattformen und Webserver) wichtig. Bedrohungsforscher rechnen aber in den kommenden Jahren verstärkt mit Malware, die Geräte direkt angreift – wie die Mirai IoT-Malware, das wahrscheinlich bekannteste aktuelle Beispiel.

Die FortiGuard Labs verfügen über fast 20 Jahre Erfahrung beim Schutz vor Malware aller Art. Obwohl gerätebezogene Malware bislang nur selten vorkommt, wird bereits auf diesem Gebiet geforscht, um proaktiv einen leistungsstarken, verlässlichen Schutz sicherzustellen.

Anti-Botnetz

Jede Botnetz-Aktivität kann eine Warnung auslösen und blockiert werden – unabhängig davon, ob sie anhand der Zieladresse, der Domain oder des Protokolls erkannt wird. Bemerkt der FortiGuard Indicators of Compromise Service eine Verbindung zu anderen bekannten Hacker-Zielen, wird zudem ein Kompromittierungsalarm generiert. Die FortiGuard Labs führen eine ständig aktualisierte Liste mit bekannten Botnet-Zieladressen und Port-Kombinationen, die mit allen ausgehenden Sitzungen verglichen werden. Botnetze, die Fast-Flux-Domänen verwenden (in denen eine Domain ihre IP-Adresszuordnung ständig ändert), werden durch Abfangen und Überprüfen des DNS-Requests (Domain Name System) mit der Domain verglichen. Selbst bei unbekannter Zieladresse und Domain können viele Botnetze anhand ihres CC-Protokolls (Command and Control) identifiziert werden. Fortinet setzt diese drei Methoden parallel ein und gewährleistet so die höchste Chance, mit Botnetzen infizierte Geräte zu finden.

API-Schutz mit FortiWeb

Anwendungsprogrammierschnittstellen (APIs) kommen in IoT-Netzwerken in mehreren Bereichen zum Einsatz. Geräte und IoT-Plattformen interagieren über APIs üblicherweise mit Protokollen wie MQTT, HTTP und CoAP. Das Datenformat ist meistens JSON oder XML, wobei bei langsamen Durchsätzen auch hochkomprimierbare Binär-Codierungen wie CBOR verwendet werden. APIs dienen auch zur Kommunikation zwischen Anwendungen und der IoT-Plattform (normalerweise über HTTP).

Fortinet FortiWeb bietet eine extrem starke API-Schutzfunktion, mit der sich zahlreiche Einschränkungen definieren lassen – von einfachen Regeln wie maximalen Header- und Feldlängen bis hin zur Schema-Validierung und -Durchsetzung mit Schwerpunkt auf HTTP und die Formate JSON oder XML.

Gemeinsam mit FortiWeb können sowohl generische Attacken als auch Angriffe auf REST-APIs (Representational State Transfer) und Web-Frontends abgewehrt werden.

Automatisierung

Fortinet verfügt über ein umfassendes Automatisierungs-Framework, mit dem sich zahlreiche Auslöser mit Aktionen wie Warnungen, Entfernung unerwünschter Geräte aus dem Netzwerk oder API-Aufrufen anderer Geräte verknüpfen lassen.

Beispielsweise kann jede der oben genannten Erkennungen dazu führen, dass ein Gerät unter Quarantäne gestellt und für die weitere Kommunikation gesperrt wird, bis die Ursache ermittelt und das Problem gelöst wurde.

Die Fortinet Security Fabric

Angesichts der Fülle unterschiedlicher Anforderungen an die IoT-Security installieren viele Unternehmen isolierte Einzelprodukte. Das führt jedoch oft zu noch mehr Problemen, da Einzellösungen die betriebliche Komplexität erhöhen.

Die Fortinet Security Fabric verfolgt dagegen einen ganzheitlichen Ansatz bei der IoT-Security: Sie bietet ein zentrales Management und integriert Security-Komponenten zu einem „Sicherheitsnetz", das die einheitliche Funktionsweise von Geräten gewährleistet – einschließlich Austausch von Bedrohungsinformationen, umfassender Transparenz, einheitlichen Berichten sowie aggregierter Log-Verarbeitung und -Analyse. Die Fortinet IoT-Lösungen sind dabei Teil der Gesamtfunktionalität, die Unternehmen, MSPs, MSSPs und Mobilfunkbetreiber mit der Fortinet Security Fabric erhalten.

Für zusätzliche Anforderungen: Integration mit Technologie-Partnern

Aptilo und Fortinet IoT Connectivity Control Service

Die Fortinet Security Fabric lässt sich auf ausgewählte Drittprodukte aus dem Fortinet Fabric-Ready-Programm erweitern. Diese Partnerschaften gewährleisten eine genau abgestimmte Integration von Drittprodukten in die Security Fabric und bringen einen hohen Mehrwert für die Gesamtlösung.

Bei der Integration von externen IoT-Lösungen arbeitet Fortinet eng mit Technologiepartnern zusammen. Kommunikationsdienstleister (CSP) sollen so dabei unterstützt werden, umfassende innovative IoT-Dienste für Unternehmenskunden anzubieten. Dieses Ökosystem für vorintegrierte Lösungen ermöglicht eine schnelle, effektive Einbindung der ständig wachsenden Anzahl integrierter IoT-Dienste.

Der Aptilo IoT Connectivity Control Service (IoT CCS) ist ein Beispiel für eine IoT Security Fabric-Integration und den Mehrwert, den diese für Mobilfunkbetreiber bietet.

Mit IoT CCS können Mobilfunkbetreiber einige Einschränkungen von mobilen Packet Cores (und sogar Enhanced Cores) angehen, die mit der umfassenden Einführung von flexiblen IoT-Diensten zusammenhängen. Einige der häufigsten Probleme lassen sich so lösen, wie z. B.:

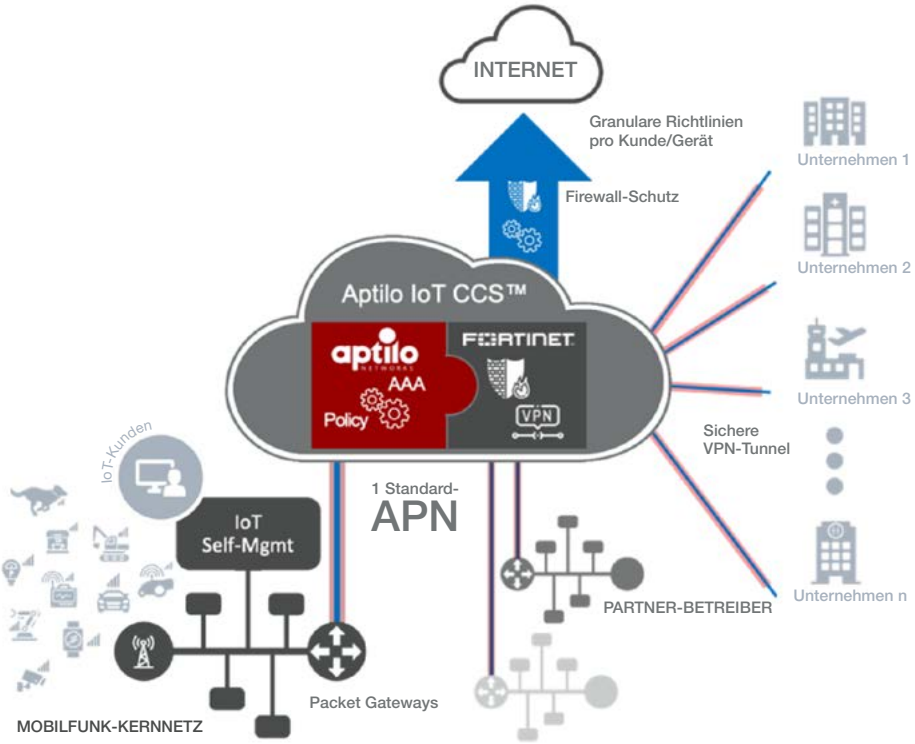
- Komplexität eines skalierbaren Angebots von privaten APN (Private Access Point Names) und VPN-Verbindungen (Virtual Private Network) für Unternehmenskunden
- fehlendes Angebot an IoT-Security-Diensten, die über APNs hinausgehen
- kein automatisches Onboarding von Neukunden
- Kundenprobleme beim Management der eigenen Security- und Konnektivitätsrichtlinien
- keine Festlegung eindeutiger Richtlinien pro Kunde – geschweige denn pro Gerät
- komplizierte APN-Einrichtung für mehrere Stakeholder vom selben Gerät aus
- schwierige Bereitstellung einer globalen IoT-Konnektivität ohne Roaming und mit richtlinienbasiertem Traffic-Breakout

Mit der gemeinsamen Lösung von Fortinet und Aptilo müssen Mobilfunkbetreiber ihr Kernnetz nicht anpassen und können dennoch bislang nicht mögliche IoT-Konnektivitätsdienste schaffen. IoT CCS – als Dienst auf Amazon AWS erhältlich und so den Betriebskosten zurechenbar – bietet eine flexible Steuerungs- und Sicherheitsschicht für die IoT-Konnektivität und läuft auf jedem heutigen und künftigen Mobilfunk-Kernnetz. Mobilfunkbetreiber können damit innovative IoT-Konnektivitätsdienste in Tagen statt in Monaten zu einem Bruchteil der Kosten bereitstellen.

FortiGate, die Netzwerk-Firewall-Serie von Fortinet, stellt beim IoT CCS die Security-Ebene sowie die Traffic-/Datenebene bereit. IoT CCS profitiert dabei u. a. von folgenden FortiGate-Funktionen: Durchsetzung von Richtlinien am Netzwerk-Rand, Routing, VPN-Management, Traffic Filtering, Schutz vor DDoS-Angriffen (Distributed Denial-of-Service), Begrenzung der TCP-Verbindungsanzahl, um nur einige zu nennen. Die Erkennung von Anomalien wird ebenfalls über die IoT-CCS-Sicherheitsschicht abgedeckt.

IoT CCS bietet einen virtuellen Multitenancy-APN, mit dem das komplexe Einrichten einzelner privater APNs für jeden Geschäftskunden entfällt. Stattdessen wird bei IoT CCS **ein einziger** Standard-APN für **alle** Unternehmen verwendet, die mit dem Dienst verbunden sind. Die VPNs werden automatisch über eine API bereitgestellt, wodurch sich das Onboarding von Neukunden einfach und reibungslos gestaltet.

Mit demselben APN-Namen können Mobilfunkbetreiber auch internationale Mobilfunkpartner zu ihrem IoT-CCS-Dienst hinzufügen. Gemeinsam mit der sofortigen eSIM-Lokalisierung (eUICC) über das Mobilfunknetz können Betreiber so eine wirklich globale, sichere Konnektivität ohne Roaming-Gebühren anbieten.



Über den virtuellen IoT CCS Multitenancy APN können Betreiber eine sichere internationale Konnektivität mit optionalem Breakout für ausgewählten Traffic am nächstgelegenen AWS-POP bereitstellen und mit den SD-WAN-Funktionen (Software Defined Wired Area Network) der FortiGate die Leistung optimieren. Dies ist eine einzigartige Funktion, die im Standard-3GPP-Kern mit dem Standard-Home-Routing kaum realisierbar ist.

Fazit

Das Internet der Dinge (IoT) verändert unsere Welt und bringt sowohl gewaltige Chancen als auch bedeutende Herausforderungen mit sich – und Kommunikationsanbieter (CSP) spielen bei der Bereitstellung und Security des IoT-Ökosystems für ihre Kunden eine zentrale Rolle.

Fortinet ist ideal positioniert, um IoT-Dienste und -Ökosysteme mit ihren unterschiedlichen Anforderungen zu schützen – vom Unternehmen bis hin zum Service Provider. Fortinet bietet CSPs eine IoT-Security-Plattform mit Carrier-Grade-Performance, Multitenancy und flexiblen Abrechnungsmodellen, die IoT-Dienste schützt, den Umsatz sichert und die Kundenerwartungen an das Internet der Dinge erfüllen kann.

18. Februar 2021, 19:56 Uhr

785701-0-1-DE