SOLUTION BRIEF

Zero-Day-Schutz für Betriebstechnologie mit Fortinet

Zusammenfassung

IT-Netzwerke verfügen über eine breite Palette von Security-Technologien, um Unternehmen vor komplexen Bedrohungen zu schützen. Bei Betriebstechnologie (OT) sieht die Lage anders aus: Hier gibt es deutlich weniger Optionen für die Cyber-Sicherheit und Bedrohungsabwehr. Besonders besorgniserregend ist, dass Sicherheitsverletzungen bei OT-Systemen oft kritische Infrastrukturen wie Staudämme, Kernkraftwerke oder Öl- und Gas-Pipelines betreffen. Angriffe können schwerwiegende Folgen für die Umwelt haben und sogar Menschenleben gefährden. Network-Operations-Analysten benötigen daher spezielle Security-Tools für OT-Systeme, mit denen sich auch unbekannte Malware und Angriffsformen erkennen lassen, ohne präzise abgestimmte Betriebsabläufe zu stören. FortiSandbox und FortiDeceptor sind dafür ideal geeignet: Diese Fortinet-Lösungen unterstützen eine umfassende OT-Security und nutzen gemeinsame Bedrohungsdaten, die vor Zero-Day-Bedrohungen schützen.

Fast 74 % der OT-Unternehmen haben in den letzten 12 Monaten einen Malware-Angriff erlebt, der Schäden für Produktivität, Ertrag, Markenvertrauen, geistiges Eigentum und die physische Sicherheit nach sich zog.[1]

Immer mehr Angriffe richten sich gegen OT-Umgebungen

OT-Umgebungen können Mensch-Maschine-Schnittstellen (HMI), industrielle Steuerungssysteme (ICS) für den Betrieb von Anlagen und Maschinen für kritische Infrastrukturen sowie Subsysteme zur Überwachung und Datenerfassung (SCADA) umfassen, die eine grafische Benutzeroberfläche für die Steuerungstechnik bereitstellen. Wer für den Betrieb von OT-Netzwerken zuständig ist, muss vor allem die Ausfallsicherheit dieser Systeme ohne Störung der Betriebsabläufe gewährleisten können.

Einige Bedrohungen für IT-Netzwerke können auch für Betriebstechnologie gefährlich werden. Beispielsweise konnte sich eine Cryptomining-Infektion aufgrund der zunehmenden Konvergenz mit IT-Systemen kürzlich auf die Hälfte aller OT-Workstations an einem großen internationalen Flughafen in Europa ausbreiten.[2] Kritische Probleme, die im IT-Bereich längst gelöst sind, machen Network-Operations-Analysten in OT-Umgebungen weiterhin zu schaffen, wie z. B. seitliche Bewegungen von Angreifern im Netzwerk mit dem Ost-West-Datenverkehr. Erschwerend kommt hinzu, dass Cyber-Angriffe zunehmend zum Waffenarsenal feindlicher Staaten gehören, die vermehrt OT-Systeme mit immer ausgefeilteren Techniken (wie agile Entwicklung, Polymorphismus) angreifen und damit die Bedrohungserkennung und -abwehr noch schwieriger gestalten.

Speziell entwickelte OT-Security-Tools – wie Segmentierung oder der Schutz der Netzwerk-Grenze mit SCADA/ICS-Signaturen – bieten zwar einen grundlegenden Schutz, versagen aber bei der Erkennung und Abwehr von bislang unbekannten Gefahren (sogenannten „Zero-Day-Bedrohungen“).

Zero-Day-Bedrohungen erfordern besondere Security-Maßnahmen: Indicators of Compromise (IOCs) müssen erkannt und im geschützten Rahmen überprüft werden können. Die hieraus gewonnenen Bedrohungsinformationen müssen dann in der gesamten Security-Architektur übernommen werden. Für Betriebstechnologie benötigen Network-Operations-Analysten dafür eine Lösung, die aus zwei Teilen besteht:

- Sandboxing-Funktionen, die Objekte auf bösartige Absichten überprüfen (einschließlich ungewöhnlicher Kommunikation an Steuerungstechnik)
- Deception Decoys – Köder, die im Netzwerk implementiert werden und sich als bestimmte IP-Geräte (z. B. eine SPS von Siemens) ausgeben, um Angreifer zu enttarnen

Sandboxing- und Deception-Lösungen ergänzen einander bei der Erkennung von Zero-Day-Bedrohungen. Um ihre Aufgabe in der „Kill-Chain“ zu erfüllen, müssen beide über eine integrierte Next Generation Firewall (NGFW) auf die gleichen Bedrohungsdaten zugreifen können. Die NGFW erzwingt interne Netzwerk-Steuerungen (über die Segmentierung) und aktualisiert die breitere OT-Security, damit bislang unbekannte Angriffsformen blockiert werden.

	FortiSandbox	FortiDeceptor
Ziel	Aktivieren von **verdächtigen Objekten** in einer simulierten Umgebung	Enttarnen von **Angreifern** mit Decoys (virtuelle Maschinen, die als Köder dienen und Angriffsziele vorspiegeln)
Angriffs-Lebenszyklus/ Cyber-Kill-Chain (frühestmögliche Abwehr)	**Mittlere Phase:** Blockieren von Exploits und der Installation unbekannter Malware	**Frühphase:** Umlenken von Ausspähversuchen und Blockieren von „Angriffs-Tests“ vor der eigentlichen Attacke
Erkennung	Erfassen des **Malware-Verhaltens**, um vor bösartigen Absichten zu warnen	Erfassen des **Angreifer-Verhaltens**, um vor böswilligen Absichten zu warnen
Abwehrreaktion	Teilen der IOCs für einen Echtzeit-Schutz **während eines Angriffsversuchs**	Teilen der IOCs für einen Echtzeit-Schutz **vor einem Angriffsversuch**

Abbildung 1: Gemeinsam stärker: Fortinet Sandboxing- und Deception-Lösungen bieten einen ganzheitlichen Schutz vor Bedrohungen und Sicherheitsverletzungen.

Ein Mangel an Cyber-Sicherheit erhöht das Risiko in OT-Umgebungen: 78 % der Unternehmen haben nur teilweise eine zentrale Transparenz, 65 % haben keine rollenbasierte Zugriffskontrolle und über die Hälfte verwendet keine interne Netzwerk-Segmentierung.[3]

Für 2020 rechneten Experten mit mehr Angriffen gegen kritische Infrastrukturen: Botnets, die DDoS-Angriffe (Distributed Denial-of-Service) gegen OT-Netzwerke ausführen, Angriffe auf Fertigungssysteme, die Cloud-Dienste verwenden, und Supply-Chain-Angriffe, bei denen Drittanbieter von Bedrohungsakteuren kompromittiert werden, um über sie kritische Bereiche anzugreifen.[4]

Fortinet-Lösungen für Sandboxing und Deception

Fortinet bietet Network-Operations-Analysten einen effektiven Schutz vor Zero-Day-Bedrohungen, um Angriffe auf OT-Umgebungen zu verhindern – von der Erkennung bis hin zur Verbreitung von Bedrohungsinformationen in Echtzeit. Diese passiven Technologien wurden speziell für Betriebstechnologie entwickelt, damit empfindliche Systeme nicht gestört werden.

Malware-Schutz mit der FortiSandbox

Fortinet ist der einzige Anbieter, der einen Sandboxing-Prozess mit einem SCADA/ICS-Simulator integriert. Unternehmen erhalten damit einen Malware-Schutz, der in der Branche einzigartig ist. Die FortiSandbox erkennt Verhaltensweisen, die auf Malware zurückgehen, wenn der bösartige Code versucht, mit einem SCADA/ICS-Gerät zu kommunizieren. Die FortiSandbox erstellt anschließend Bedrohungsinformationen, um die bösartige Kommunikation und die Malware in der restlichen OT-Umgebung über FortiGate NGFWs zu blockieren.

Als integraler Bestandteil der Fortinet Security Fabric-Architektur verwendet die FortiSandbox drei Arten von Bedrohungsinformationen zur automatisierten Erkennung und Verhinderung von Sicherheitsverletzungen: 1) Weltweite Bedrohungsdaten über neue Threats, bereitgestellt von den FortiGuard Labs. 2) Lokale Bedrohungsdaten, die mit anderen Sicherheitslösungen von Fortinet und Drittanbietern über die Security-Infrastruktur geteilt werden und unternehmensweit eine Einschätzung der Lage ermöglichen. 3) KI-Funktionen – einschließlich statischer und Verhaltensanalysen –, um Zero-Day-Bedrohungen noch effizienter zu entdecken.

Dass die FortiSandbox KI-Funktionen für den gesamten Sandboxing-Prozess verwendet, unterscheidet sie von allen anderen Sandboxing-Lösungen: Die meisten Sandbox-Anbieter haben noch keine KI implementiert, andere werben zwar mit KI-Funktionen, tatsächlich werden aber nur statische Analysen angewendet. Eine effektive Sandbox-KI erfordert jedoch sowohl statische als auch dynamische Abläufe, um gewisse hochkomplexe Bedrohungen richtig zu erkennen.

Performance und Schutz in unabhängigen Tests nachgewiesen

Die NSS Labs testen Security-Lösungen mit sogenannten BPS-Tests (Breach Prevention System), die den Schwerpunkt auf die Erkennung und Blockierung komplexer Malware, Exploits und anderer Umgehungsversuche legen. Diese Tests zeigen, wie wichtig ein automatisierter Abwehrzyklus ist, der mehrere Angriffsvektoren wie Web, E-Mail und anfällige Endgeräte berücksichtigt. Die integrierte BPS-Lösung von Fortinet – bestehend aus FortiSandbox, FortiGate und FortiClient – erreichte bei den NSS-Tests eine allgemeine Wirksamkeit von 97,8 % bei den geringsten Gesamtbetriebskosten (TCO) und erhielt die Bewertung „Empfehlenswert“.[5]

Auch bei anderen anerkannten Tests wie der ATD-Zertifizierung der ICSA Labs[6] und den Breach-Detection-System-Tests der NSS Labs[7] schnitt die FortiSandbox als empfehlenswert ab.

Frühzeitige Enttarnung von OT-Angriffen mit FortiDeceptor

Während FortiSandbox verdächtige Objekte (wie Malware) in einer simulierten Umgebung ausführt, legt der FortiDeceptor Köder (Decoys) aus. Diese präsentieren Angreifern eine täuschend echte Simulation eines OT-Geräts. Sobald sich ein Angreifer an diesem SCADA/ICS-Decoy zu schaffen macht, wird das bösartige Verhalten vom FortiDeceptor erkannt und enttarnt. Fortinet ist der einzige Anbieter mit einer Deception-Technologie, die Decoys für OT (SCADA/ICS-Geräte) und IT (Server, Endpunkte, IoT-Geräte) umfasst. Der FortiDeceptor sendet dann die Bedrohungsdaten an die FortiGate NGFWs, um die Ursprünge der Sicherheitsverletzung zu blockieren. Dabei werden Indicators of Compromise (IOCs) in Echtzeit geteilt, um den Angriffs-Lebenszyklus frühzeitig zu unterbrechen.

Die Zeit von der ersten Aktion eines Angreifers in einer Ereigniskette bis zur ersten Infektion einer Ressource wird normalerweise in Minuten gemessen, während die Zeit bis zur Erkennung eher Monate beträgt.[9] Derzeit dauert es durchschnittlich 279 Tage, bis eine einzige Sicherheitslücke erkannt und geschlossen wird.[10] Während dieser Zeit kann eine Infektion enormen Schaden anrichten – von umfassenden, irreparablen Finanzverlusten und Reputationsschäden bis hin zur Gefährdung der physischen Sicherheit in Anlagen wie Wasserkraftwerken, Kernkraftwerken oder Öl- und Gas-Pipelines. Um dies zu vermeiden, können Network-Operations-Analysten mit FortiDeceptor ein Netzwerk von OT-spezifischen Decoys anlegen, die Angreifer von wertvollen Ressourcen weglocken. Dies reduziert das Risiko von Sicherheitsverletzungen durch unbekannte Bedrohungen erheblich. Der FortiDeceptor analysiert dann sämtliche Bedrohungsaktivitäten und teilt die Bedrohungsdaten über die Fortinet Security Fabric mit allen anderen Sicherheitskomponenten, um die weitere OT-Umgebung zu schützen.

Es wird weiterhin Malware-Angriffe geben, die speziell für Steuerungstechnik und SCADA-Systeme entwickelt wurden – und Schutzsysteme sind jetzt ebenfalls ein Ziel.[8]

Gegenüber Nachzüglern der Branche ist es in erfolgreichen Unternehmen um 68 % wahrscheinlicher, dass Sicherheitsereignisse angegangen und überwacht sowie Ereignisanalysen durchgeführt werden. Das verringert Risiken durch Sicherheitsverletzungen, da die Zeit bis zur Erkennung minimiert wird.[11]

Spezielle Tools für OT-Bedrohungsinformationen

Bislang gab es nur wenige Tools für Network-Operations-Analysten, um OT-Umgebungen (und damit kritische Infrastrukturen) vor der neuesten Malware und neuartigen Angriffsstrategien zu schützen. Fortinet bietet einzigartige Security-Lösungen für das komplexe Zusammenspiel von IT- und OT-Umgebungen, mit denen sich Zero-Day-Bedrohungen erkennen und abwehren lassen und die Ausfallsicherheit kritischer Systeme sichergestellt wird. Fortinet vereinheitlicht und automatisiert den OT-Schutz vor bekannten und unbekannten Bedrohungen, indem Sandbox-Funktionen (FortiSandbox) und Deception-Lösungen (FortiDeceptor) mit anderen Sicherheitsprodukten von Fortinet und Drittanbietern integriert werden.

[1] „Bericht zum Stand der operativen Technologie und der Cyber-Sicherheit“. Fortinet, 10. September 2019.

[2] Tara Seals: „Major Airport Malware Attack Shines a Light on OT Security“. Threatpost, 18. Oktober 2019.

[3] „Bericht zum Stand der operativen Technologie und der Cyber-Sicherheit“. Fortinet, 10. September 2019.

[4] Bruce Sussman: „15 Cyber Threat Predictions for 2020“. SecureWorld, 12. Dezember 2019.

[5] Jessica Williams, et al.: „Breach Prevention Systems Report: Fortinet FortiGate 500E + FortiClient + FortiSandbox“. NSS Labs, 7. August 2019.

[6] „Q4 2019 Advanced Threat Defense (ATD) Testing Report“. ICSA Labs, 8. Januar 2020.

[7] „Breach Detection Systems Report: Fortinet FortiSandbox-2000E“. NSS Labs, 19. Oktober 2017.

[8] „Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems“. Fortinet, 16. Mai 2019.

[9] „2019 Data Breach Investigations Report“. Verizon, 2019.

[10] „2019 Cost of a Data Breach Report“. Ponemon Institute und IBM Security, Juli 2019.

[11] „Bericht zum Stand der operativen Technologie und der Cyber-Sicherheit“. Fortinet, 10. September 2019.

FORTINET

www.fortinet.com/de

14. Dezember 2020, 16:26 Uhr

560486-0-0-DE