FIREEYE™

DATENBLATT

Cyber Physical Threat Intelligence

So schützen Sie komplexe, cyber-physische Systeme vor Angriffen

HIGHLIGHTS

- Analyse von Sicherheitslücken bei cyber-physischen Systemen mit anschließendem Bericht
- Technische Analyse der Taktiken, Techniken und Prozesse von Angreifern, die sich auf physische Systeme spezialisieren
- Auswertung von quellenübergreifenden Daten über Bedrohungen für cyber-physische Systeme
- Analyse von aktuellen, aus betriebstechnologischer Perspektive relevanten Nachrichten und Forschungsergebnissen
- Bildungsangebote zur Steigerung des Sicherheitsbewusstseins

Die wachsende Nutzung von Kommunikationstechnologien in nahezu jeder Branche hat dazu geführt, dass immer mehr digitale Funktionen zur Kontrolle und Wartung physischer Prozesse eingesetzt werden. Diese Schnittstelle zwischen virtuellen und physischen Umgebungen hat zu bahnbrechenden Innovationen in den Bereichen Konnektivität und Instrumentierung geführt, stellt aber gleichzeitig auch eine Schwachstelle in puncto Sicherheit dar.

Daher wird es immer wichtiger, dass Unternehmen technische Anfälligkeiten und realistische Bedrohungen proaktiv erkennen, damit Angriffe auf cyber-physische Systeme (CPS) vorhergesehen und abgewehrt werden können.

Cyber Physical Threat Intelligence ist ein abonnementbasierter Service von FireEye, bei dem Unternehmen wichtige Kontextinformationen, relevante Daten und praxistaugliche Analyseergebnisse erhalten, die es ihnen ermöglichen, ihre cyber-physischen Systeme vor Bedrohungen zu schützen. Gängige Anwendungsbereiche umfassen Betriebstechnik, industrielle Steuersysteme (ICS), das Internet der Dinge und andere Technologien zur Unterstützung physischer Prozesse (beispielsweise in der Medizin oder in der Telekommunikation).

Vorteile eines Abonnements

Cyber Physical Threat Intelligence bietet Verantwortlichen, die mit der Sicherheit und kontinuierlichen Verfügbarkeit physischer Systeme beauftragt sind, ein Frühwarnsystem, das über betriebstechnische Schwachstellen, Angriffskampagnen und die dahinter stehenden Akteure informiert. Unser Service ermöglicht Sicherheitsteams, Angreifern stets einen Schritt voraus zu sein und fundierte Entscheidungen in Bezug auf den Sicherheitsstatus cyber-physischer Systeme zu treffen.

Im Rahmen des Abonnements erhalten Sie detaillierte Berichte mit strategischen Einblicken und konkreten Informationen über Malware und andere schädliche Taktiken, Techniken und Prozesse, Hackergruppen, schädliche Aktivitäten und Schwachstellen. In Tabelle 1 sind die Schwerpunkte aufgeführt, auf die sich die FireEye-Experten bei der Aufbereitung von Daten konzentrieren.

Tabelle 1: Umfang von FireEye Cyber Physical Threat Intelligence

Schwerpunktbereich	Beschreibung
Aktuelle Bedrohungsdaten	Taktische und strategische Analyse von Angreiferaktivitäten unter Einbeziehung von Erkenntnissen aus aktuellen Einsätzen der Mandiant-Experten und von Daten, die weltweit von den FireEye-Sensoren und -Technologien zusammengetragen werden
Überblick über die cyber-physische Infrastruktur	Analyse der Terminologie, Netzwerkarchitektur, Sicherheitsmaßnahmen für ICS-Ports und Protokolle sowie der bekannten Hacker, die cyber-physische Systeme anvisieren
Schwachstellen der cyber-physischen Infrastruktur	Taktische Berichte zu Schwachstellen bei industriellen Steuersystemen
Aktivitäten im ICS-Netzwerk	Auswertung von Firewall-Logs und Analyse des Netzwerkverkehrs an ICS-Ports
Trends bei der ICS-Sicherheit	Erfassung, Analyse und Auswertung (einschließlich zu erwartender Folgen) von Veröffentlichungen zum Thema ICS in den Medien
Daten von FireEye Mandiant	Trenddaten und Sicherheitsstandards basierend auf aktuellen Einsätzen der Mandiant-Experten
Tools und Recherche	Recherche und Auswertung ICS-spezifischer Spionage- und Angriffstools

Auf neueste Bedrohungen vorbereitet

Cyber-physische Systeme bieten eine ganze Reihe von Vorteilen, sind aber auch mit ganz speziellen Anforderungen und Risiken verbunden. Um Bedrohungen vorherzusehen und wirksam abzuwehren, müssen Sie daher …

- das Bewusstsein für gängige Sicherheitsprobleme steigern und ein wirksames Schwachstellenmanagement sicherstellen. Mithilfe der FireEye-Technologien können Sie Ranglisten für CPS-spezifische Sicherheitslücken und geeignete Abwehrmaßnahmen erstellen.
- einen Überblick über Bedrohungen, Angriffskampagnen und aktive Angreifergruppen gewinnen, die es auf Ihre cyber-physischen Systeme abgesehen haben.
- detailliertes Referenzmaterial und Informationen über CPS-spezifische Ereignisse für Ihre Teams und externe Stakeholder bereitstellen.
- fundierte Entscheidungen über Ihre CPS-Strategie treffen können.
- anwendbare Bedrohungsdaten zur Hand haben, die Ihnen einen proaktiven statt eines reaktiven Ansatzes beim Risikomanagement ermöglichen.

Wenn Sie mehr darüber wissen möchten, wie FireEye Cyber Physical Intelligence Ihr Sicherheitsteam bei einer fundierten Entscheidungsfindung unterstützen kann, empfehlen wir einen Besuch unserer Website: **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.

FIREEYE™