FIREEYE™

SCHEDA TECNICA

Verifica dell'integrità dei sistemi di controllo industriale

Scoprire le vulnerabilità del sistema di controllo industriale e creare un piano realistico per la riduzione dei rischi informatici del sistema

VANTAGGI PRINCIPALI

- L'approccio minimamente invasivo evita i rischi operativi associati agli agenti software e alla scansione della rete in un ambiente ICS.
- Identificazione di vulnerabilità della sicurezza ICS, configurazioni errate e altri difetti.
- Analisi umana delle attività anomale e sospette, eseguita dagli esperti ICS usando strumenti appositi.
- Raccomandazioni pratiche ordinate per priorità, personalizzate e contestualizzate in base ai rischi e alle preoccupazioni specifiche per il vostro processo industriale.

Mandiant è il consulente fidato delle aziende di tutto il mondo, con oltre 10 anni di esperienza nel contrastare gli autori di minacce avanzate internazionali. Stiamo al fianco delle aziende nei momenti più delicati successivi all'individuazione di una violazione della sicurezza, aiutandole a migliorare le proprie capacità proattive di rilevamento, risposta e contenimento. La verifica dell'integrità dei sistemi di controllo industriali (*Industrial Control Systems*, ICS) combina le conoscenze di Mandiant in merito agli attori delle minacce e l'esperienza nel rispondere agli eventi di sicurezza con le specializzazioni dei nostri consulenti ICS per valutare approfonditamente l'effettivo grado di segmentazione, protezione e monitoraggio della tua rete ICS.

Panoramica

La verifica dell'integrità ICS valuta in maniera minimamente invasiva la condizione complessiva della sicurezza informatica di uno stabilimento industriale. La valutazione è specificamente concepita per soddisfare le esigenze di quelle organizzazioni che sono preoccupate dei rischi operativi associati agli agenti software, alle scansioni della rete o ad altre tecniche più aggressive per la valutazione della rete. La verifica dell'integrità ICS combina un workshop di revisione dell'architettura ICS con la dettagliata analisi tecnica delle configurazioni firewall e del traffico della rete ICS in tempo reale.

Gli specialisti ICS di Mandiant conoscono il linguaggio della tecnologia operativa (*Operational Technology*, OT) e lavorano direttamente con i tecnici responsabili della stessa, per adattare le migliori pratiche di sicurezza informatica nel modo più idoneo per l'ambiente ICS. Lavorano inoltre con i responsabili della sicurezza IT per dotarli delle conoscenze di settore e della credibilità necessarie per coinvolgere il personale della OT in produttive discussioni sulla sicurezza informatica.

Il nostro approccio

Analisi dei rischi dell'architettura e modellazione delle minacce

Documentazione della situazione corrente della rete

- Revisione di schemi, flussi di dati e progetti dell'architettura esistente.
- Inventario e valutazione dei protocolli di comunicazione industriale in uso.
- Revisione delle norme di sicurezza eventualmente esistenti per la distribuzione dei prodotti software.

CHE COSA SI RICEVE

- **Schema del modello di minaccia:**
  schema rappresentativo del vostro sistema di controllo industriale (ICS) che mappa i vari vettori delle minacce utilizzabili dagli aggressori per interrompere o danneggiare le vostre attività, seguito da una discussione su come ordinare per priorità gli appropriati controlli di sicurezza.
- **Relazione sull'integrità dell'ICS:**
  dettagliata relazione tecnica contenente le osservazioni di Mandiant, incluse eventuali vulnerabilità della protezione, configurazioni errate, punti deboli dell'architettura, traffico di rete sospetto o attività anomale con raccomandazioni tecniche e pratiche per ogni osservazione, ordinate per priorità, insieme al riepilogo delle tematiche principali emergenti dalla valutazione.
- **Presentazione delle raccomandazioni strategiche e tecniche:**
  riepilogo delle nostre osservazioni e raccomandazioni per tecnici e dirigenti.

Sviluppo del modello di minaccia

- Durante un workshop interattivo con il personale informatico e tecnico/operativo del cliente, partiamo dagli schemi di architettura risultanti per gettare le basi del modello di minaccia.
- In base alle nostre ampie conoscenze delle reali tattiche usate dagli aggressori, generiamo delle rappresentazioni visuali dei possibili attacchi al sistema di controllo.
- Assistiamo nell'ordinare per priorità l'implementazione del controllo di sicurezza dell'ICS, identificando i vettori di attacco che rappresentano i rischi e l'esposizione maggiori.

Ordinamento dei controlli per priorità

- Coordiniamo la discussione con il vostro personale tecnico per identificare i controlli di sicurezza che possono meglio affrontare le minacce identificate.
- Ordiniamo per priorità i potenziali controlli in base alla loro convenienza, considerando fattori quali la riduzione del rischio, il costo/laboriosità e la velocità di implementazione.

Analisi dei dati tecnici

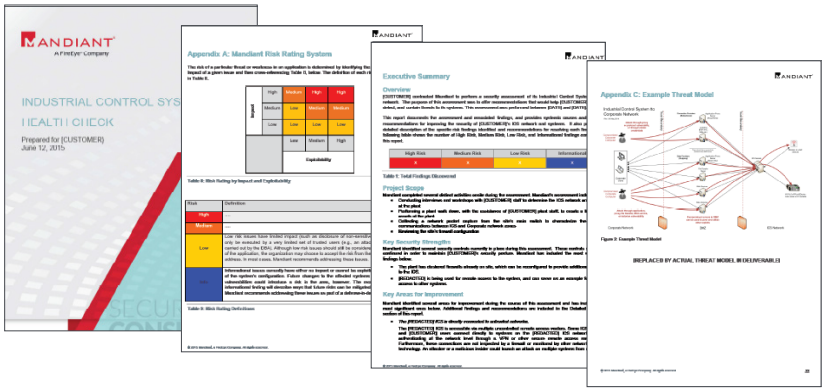
Revisione della segmentazione della rete: analizziamo il file dei pacchetti della rete acquisiti dal dispositivo FireEye PX che è stato installato nella rete ICS del cliente. I pacchetti vengono esaminati per cercare i rischi per la sicurezza quali:

- Connessione involontaria dall'ICS a Internet o alla rete aziendale;
- Dispositivi dual-homed;
- Protocolli ICS che attraversano il firewall ICS;
- Connessioni anomale fra due computer.

Revisione della configurazione del dispositivo di sicurezza: prendiamo in esame l'efficacia della configurazione e gli insiemi di regole dei dispositivi di sicurezza della rete, come i firewall. Ad esempio:

- Il traffico in ingresso alla rete ICS deve essere sempre instradato tramite una DMZ;
- Le reti ICS non devono poter avere l'accesso diretto a Internet e non devono mai connettervisi direttamente.

Esempio del report



Per ulteriori informazioni su FireEye, visita il sito Web **www.FireEye.com**

FireEye Italia Srl
Piazza IV Novembre, 7. 20124 Milano
Italia
+39 0294750535
italy@FireEye.com

Informazioni su FireEye, Inc.

FireEye è un'azienda che offre servizi di sicurezza informatica basati sull'intelligence. Operando come estensione intuitiva e scalabile dei processi operativi di sicurezza dei clienti, FireEye offre un'unica piattaforma in grado di coniugare tecnologie di sicurezza innovative, intelligence sulle minacce a livello nazionale e servizi di consulenza Mandiant® di fama mondiale. Grazie a questo approccio, FireEye elimina la complessità e l'onere della sicurezza informatica per le aziende che hanno difficoltà a prepararsi per futuri attacchi, prevenirli e rispondere ad essi.