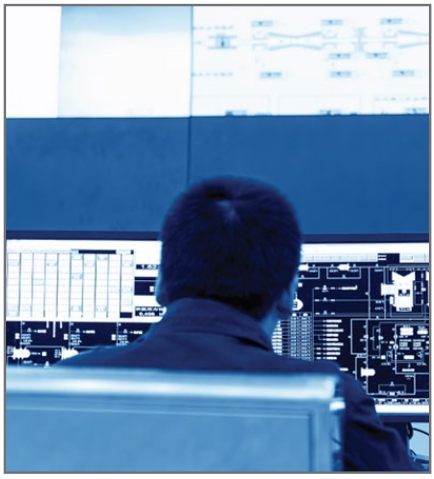
Produkt-Datenblatt

iSEC

Cybersicherheit-Assessment-Leistungen



- Von Radiflow-Spezialisten für ICS/SCADA-Sicherheit bereitgestellt
- Aufzeichnen des Netzwerkverkehrs, ohne Eingriff oder Stopp des laufenden Betriebs
- Vollständige Visualisierung Ihrer OT-Netzwerk-topologie und aller verbundenen Anlagen
- Erkennen aller bekannten SCADA-spezifischen Schwachstellen und Expositionen, Logik-manipulationen in SPS und offenen Remote-SSH-Sitzungen
- Strukturierter, standardisierter Prozess, z.B. ISA/IEC-62443 (Früher ISA-99)
- Detaillierter Bedrohungs- und Schwach-stellenbericht und Maßnahmenplan

WIE SICHER IST IHR ICS-NETZWERK (PROZESSLEITSYSTEM) ?

Nach vielen Cyberattacken auf kritische Infrastrukturanlagen in den letzten Jahren erhielt der Schutz kritischer Infrastrukturen (Critical Infrastructure Protection, CIP) weltweit höchste Priorität bei Finanzierung, Regulierung und im allgemeinen Bewusstsein.

Unternehmen in vielen Branchen sehen heute, dass es nötig ist, wirtschaftliche und einfach zu bedienende Cyberschutzpläne einzuführen, um sich an die ständig weiterentwickelnden Angreifer und deren Methoden anpassen.

Das Erstellen eines ICS-Schutzplans kann schon erschrecken. Es gibt keine einheitliche Lösung, und oft haben die Betreiber nur geringen Einblick in ihre Netzwerke.

Ein wirksamer ICS/SCADA-Schutzplan erfordert das vollständige Identifizieren und Abbilden aller Geräte, Verbindungen, Ports und anderen Netzwerkgeräte. Nur dann können Schwach-stellen und Gefährdungen erkannt und ihnen je nach Schweregrad und möglichen Auswir-kungen begegnet werden.

Anschließend wird ein praktisch anwendbarer Maßnahmen- und Notfallplan erstellt, der aus-schließlich auf Fakten und Expertenanalysen basiert und die Leistungsfähigkeit und Effizienz des Projekts gewährleistet.

ÜBER RADIFLOW

Radiflow entwickelt zuverlässige Lösungen für industrielle Cyber-Sicherheit für kritische Geschäftsabläufe. Unser Portfolio an bahnbrechenden Lösungen für ISC / SCADA-Netzwerke ermöglicht es Benutzern, die Transparenz und Kontrolle über ihre OT-Netzwerke aufrechtzuerhalten. Unsere intelligente Plattform zur Erkennung und Analyse von Bedrohungen für die industrielle Cybersicherheit minimiert potenzielle Geschäftsunterbrechungen und -verluste in Ihrer OT-Umgebung.

Das Radiflow-Team besteht aus Fachleuten mit unterschiedlichem Hintergrund, aus Cyber-Experten von Elite-Militäreinheiten und aus Automatisierungsexperten von globalen Anbietern von Cybersicherheit. Radiflows Lösungen wurden 2009 gegründet und werden von großen Industrieunternehmen und Versorgungsunternehmen erfolgreich eingesetzt, um mehr als 3.000 kritische Einrichtungen weltweit zu schützen. Mehr unter www.radiflow.com.

radiflow

Der iSEC-Cybersicherheits-Assessment-Prozess

Die von erfahrenen Fachleuten erstellte Sicherheits-bewertung von Radiflow ist ein strukturierter, stan-dardisierter Prozess (z. B. nach ISA/IEC-62443).

1. Vorabbewertung:

a. **Vorbereiten und Koordinieren**: Vorheriges Prüfen der Netzwerktopologie, der Anbieter von SCADA-Geräten und anderer relevanter Informationen.

b. **Vor-Ort-Treffen mit den Hauptbeteiligten**: Überprüfen der Netzwerkstruktur und -kompo-nenten, Beschreiben bekannter Probleme und Definieren des Prüfplans und Arbeitsablaufs Gleichzeitig zeichnet unser Team Teile des Netzwerkverkehrs für Topologiezuordnung und -analyse auf.

2. Analyse

Auf Grundlage dieser Netzwerkanalyse werden die Betriebsaktivitäten definiert, um Schwachstellen und mögliche Angriffsvektoren zu erkennen. Diese Phase dauert normalerweise zwei bis vier Wochen, in der das Radiflow-Team folgendes macht:

a. Alle Netzwerkgeräte, Betriebssysteme, Anwen-dungen und Verbindungen bis zu den umfassenden IT- und OT-Protokollen und -Komponenten identifi-zieren und zuzuordnen,

b. die aktuellen Sicherheitsmaßnahmen analysieren, um festzustellen, ob Angreifer vertrauliche Infor-mationen aus dem Netzwerkverkehr extrahieren, und die Netzwerksegmentierung zwischen Controllern, Servern und Workstations prüfen,

c. die Ausfallsicherheit der Datenverbindungsschicht bewerten, um Schwachstellen zum LAN-Öffnen zu finden,

d. alle Managementschnittstellen zu SPS, Switches und Routern analysieren,

e. Trennungen zwischen Engineering-Workstations und Servern überprüfen

f. die Sicherheit von Kommunikationsanschlüssen prüfen

g. den Zugriff auf ICS über drahtlose und drahtgebundene Fernsteuerungen überprüfen,

h. die Interaktion des ICS mit externen Systemen prüfen,

i. die Internetverbindung aller ICS-Komponenten unter¬suchen,

j. die Nutzung nichtdeklarierter Protokolle überprüfen,

k. Sicherheitsschränke und Telekommunikationsgeräte prüfen

l. Prüfen, ob industrielle Geräte verwendet werden: Router, Switches, Firewalls, Konverter, Medien usw...

m. Netzwerk- und Geräteschwachstellen sowie

mögliche Gefahren aufdecken,

n. Schwachstellen der Zugriffskontrolle, z. B. auf schlecht geschützten Dateiservern gespeicherte vertrauliche Infor¬mationen und unzureichende oder fehlende Firewalls suchen,

o. Informationen suchen, die von Passwörtern ableitbar sind (NTLM, MD5-Hash usw.), um eine Liste passiver Pass¬wörter und ein Wörterbuch mit allgemeinem Passwort zu generieren,

p. Möglichkeiten für Angreifer eliminieren, sich in das Netz¬werk einzugraben und auf kritische ICS-Komponenten unberechtigt zuzugreifen,

q. prüfen, ob die Geräte den Sicherheitsnormen, z.B. ISO/IEC 2700, bzw. ISA-99 entsprechen

3. Berichten und Sichern

Der Betreiber erhält einen vollständigen Bericht mit Maßnahmen zum Eliminieren gefundener Bedrohungen und Schwachstellen.

Der Bericht enthält eine zusammenfassende Kurzdarstellung der Schlussfolgerungen und Empfehlungen für die oberste Leitung im Dashboard-Stil sowie einen umfassenden technischen Bericht mit folgenden Angaben:

a. eine übersichtliche Beschreibung aller gesammelten Daten,

b. eine vollständige Liste der gefundenen Sicherheitslücken, sortiert nach Schweregrad und Missbrauchswahrscheinlichkeit durch Hacker sowie eine Beschreibung deren Folgen

c. ein Angriffsszenario, in dem die praktischen Auswirkungen auf Ihr Unternehmen detailliert beschrieben werden, falls Hacker die kritischen Schwachstellen ausnutzen sollten

d. Ein programmatischer Maßnahmenplan mit Empfehlungen zum Beheben von Schwachstellen und zum Überbrücken von Sicher-heitslücken. Dazu gehören vorgeschlagene Änderungen an Gerätekonfigurationen und Einstellungen, die Nutzung von Erkennungs-/Schutzmechanismen, die Installation notwendiger Softwareupdates auf Geräten (SPS, RTUs, MMS usw.) und Änderungen an Richtlinien, Verfahren und Prozessen.

Warum sind industrielle Umgebungen besonders anfällig?

Moderne industrielle Steuerungssysteme (ICS) sind aus mehreren Gründen für Cyber-attacken anfällig.

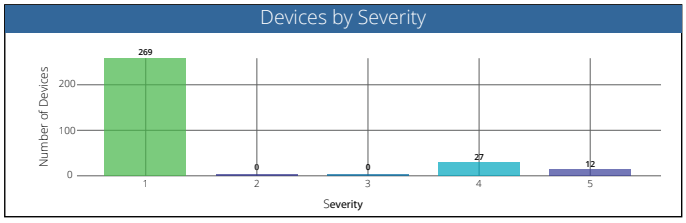
Erstens setzen sie häufig Netzwerktechnologien auf Altsysteme auf, ohne kritische Schwachstellen zu patchen, um den Prozess nicht zu unterbrechen – etwas, das Cyber-kriminelle wissen.

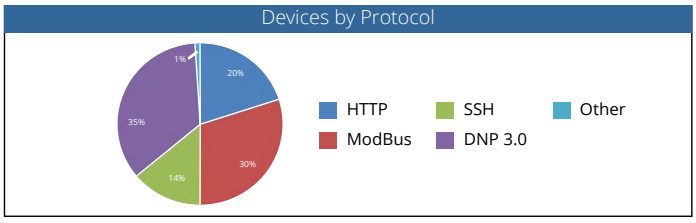
Zweitens erhöhen mangelhafte Kontrollen der Zugriffsrechte sowie Standardeinstellungen, Nutzerregeln und -richtlinien – alles im Namen der Betriebskontinuität – das Gesamtrisiko.

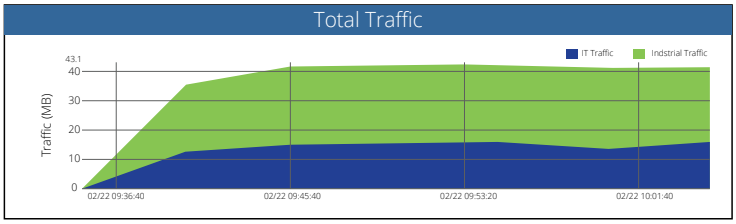
Einige Schwachstellen für branchenspezifische Software, wie beispielsweise hartkodierte Kennwörter und unsichere Protokolle, sind Überbleibsel aus der Vergangenheit, in der ICS nicht mit dem Netzwerk eingebunden war und “Software-Schwachstellen” kaum existierten.

Top KnownThreats Detected

Event	Event Time	Port	Severity	Src Device Name	Src IP	Dst Device Name	Dst IP	Number of Events
Restart Communications Option	2/22/2017 10:13	Modbus	5	[NAME]	123.456.0.1	[NAME]	123.456.0.1	1
Report Server Information	2/22/2017 10:13	Modbus	5	[NAME]	234.567.0.2	[NAME]	234.567.0.2	2
Read Device Information	2/22/2017 10:13	Modbus	5	[NAME]	345.678.0.3	[NAME]	345.678.0.3	3







Einige der an die ICS-Betreibern übermittelten Tabellen und Diagramme aus dem iSEC-Bewertungsbericht

Von Top-Profis aufgeführt

Wir bieten Ihnen unsere Sicherheitsbewertungen auf der Grundlage unserer langjährigen Erfahrung, bekannten Fachkenntnissen und Produktpalette an.

Das Bewertungsverfahren wird von den besten Radiflow-Sicherheitsexperten durchgeführt. Sie nutzen die neuesten Methoden aus unserer Palette dedizierter ICS/SCADA-Produkte.

Nach Prüfungsabschluss wird dem Kunden ein ausführlicher Bericht vorgelegt, der alle gesammelten und protokollierten Informationen, Analysenergebnisse und einen vollständigen Cybersicherheits-Plan für Ihre Organisation enthält. Sie können frei wählen, wie und mit wem Sie den Plan ausführen wollen.

Fordern Sie Sofortmaßnahmen an

Um die Sicherheitsbewertung von Radiflow besser zu verstehen und das Bewertungs-verfahren zu beginnen, kontaktieren Sie uns bitte unter:

US and Canada:
Tel: +1 (302) 547-6839
sales_NA@radiflow.com

EMEA:
Tel: +972 (77) 501-2702
sales@radiflow.com

UK:
Tel: +44 (0) 800 246-1963
sales_UK@radiflow.com

France:
Tel : +33 1 77 47 87 25
sales_FR@radiflow.com

DACH:
Tel: +49 (160) 109 75 65
sales_DACH@radiflow.com

Oder besuchen Sie und auf www.radiflow.com

Radiflow ist ein führender Anbieter von Cybersicherheits-Lösungen für kritische Infrastruktur-netzwerke (d.h. SCADA) von Energieversorgern, bei Öl & Gas, Wasser und anderen Unternehmen.

Radiflows Sicherheits-Werkzeugkasten validiert das Verhalten von M2M-Anwendungen und H2M-Sitzungen (Human-to-Machine) in verteilten betrieblichen Netzwerken. Radiflows Sicherheitslösungen sind als Inline-Gateways für Remote-Anlagen und nicht-intrusive IDS (Intrusion Detection Systeme) verfügbar, die örtlich oder zentral angewendet werden können.

Radiflows Sicherheitslösungen werden als Komponenten innerhalb eines integrierten Anwender-pakets globaler Automatisierungsanbieter und von örtlichen Vertriebs-partnern als eigenständige Sicherheitslösungen vertrieben.