FAQ – Anwendungsbeispiele
IT-Sicherheitsgesetz 2.0 mit VIDEC und AUVESY

Herr Woehl, sie haben ja sehr eindrucksvoll gezeigt wie lange Angreifer sich unter Umständen schon im Netzwerk aufhalten können. Wie verhält sich IRMA denn, wenn sie erst nach einer Infektion im Netzwerk eingebracht wird?

Markus Woehl: Heutige Angriffssysteme bzw. Schadsoftwaren sind nicht immer isoliert auf den Systemen, sondern kommunizieren häufig auch mit dem Verursacher. Da IRMA ein ideales Abbild des Kommunikationsprofils der Anlage darstellt erhalten sie eine maximale Transparenz und sollten sich auch immer Fragen welche Kommunikationsteilnehmer in zu erwartendem Umfang miteinander sprechen. Wenn eine IP-Adresse mit anderer Länderkennung auftaucht, muss es nicht unbedingt falsch sein. Sie erhalten damit die einfache Möglichkeit selber zu entscheiden und damit auch Angriffe zu erkennen, auch wenn er bereits läuft.

Bei uns im Werk ist ein Ringnetzwerk mit über 50 Switchen. Brauche ich jetzt an jeder Stelle eine IRMA?

Markus Woehl: Schön wäre es. Idealerweise schauen wir gemeinsam auch ihre Netzwerkinfrastruktur und entscheiden anhand der wichtigen Übergabepunkte wo eine IRMA Sinn macht und wo nicht.

Gibt es Kunden die Integration von Versiondog und IRMA im Einsatz haben, und damit schon Angriffe erkannt bzw. verhindert haben?

Markus Woehl: Ja, die gibt es. Aktuell führt auch ein Kunde einen Pen-Test durch. Erfahrungen aus diesem Vorgang werden wir anonymisiert präsentieren. Voraussichtlich noch vor der Sommerpause.

Arbeitet IRMA bis hinunter auf die Feldbusebene?

Das hängt vom Feldbus ab. Ethernet basierende Feldbusse wie Profinet und ähnlich sind natürlich mit IRMA einfach monitorbar. Andere Netzwerkphysiken wie Profibus oder Serielle Protokolle werden von IRMA nicht erfasst.

Wie viele Risikolevel gibt es?

Es wird für jedes Asset ein Bedrohungswert gebildet. Dieser ist ein programmierter Algorithmus aus dem Bereich „machine learning“ und setzt sich aus mehreren Faktoren zusammen. z.B. Ist das Asset validiert, Anzahl der Verbindungen des Assets, Anzahl der validierten/unvalidierten Verbindungen, Anzahl Alarme bzw. neu aufgetretene Alarme.

Wie bildet sich der Risikowert?

Es wird für jedes Asset ein Bedrohungswert gebildet. Dieser ist ein programmierter Algorithmus aus dem Bereich „machine learning“ und setzt sich aus mehreren Faktoren zusammen. z.B. Ist das Asset validiert, Anzahl der Verbindungen des Assets, Anzahl der validierten/unvalidierten Verbindungen, Anzahl Alarme bzw. neu aufgetretene Alarme.

Kann versiondog auch PCS7/WinCC-Archive versionieren?

versiondog kann auch sowohl PCS7 als auch WinCC Archive versionieren, weitere Informationen hierzu finden Sie auf versiondog.info unter Geräteunterstützung für PCS7 & WinCC. Generell können alle Arten von Daten in versiondog versioniert werden, es gibt hinsichtlich der Usability unterschiedliche Ausbaustufen. Bei Fragen helfen wir Ihnen gerne unter <KONTAKT SALES> weiter.