Sagen Sie mal:

Thomas Soens

Betreiber kritischer Infrastruktur müssen nachweisen, dass sie Systeme zur Erkennung von Cyberattacken installiert haben. Wie sieht es hier Ihrer aus Sicht mit der Umsetzung aus?
Wir registrieren, dass sich bereits etwas in Bewegung gesetzt hat. Insbesondere größere Infrastrukturbetreiber sind schon auf einem vielversprechenden Weg. Dennoch besteht in der gesamten Branche Nachholbedarf – und es gibt sogar Betreiber, die noch keine entsprechenden Systeme installiert haben.

Es stellt sich aktuell auch die Frage, ob allein die Installation von Systemen zur Erkennung von Cyberangriffen ausreichend ist oder ob zusätzliche Maßnahmen zur Vermeidung solcher Attacken ergriffen werden müssen. Hierbei stehen wir hauptsächlich vor Herausforderungen im Bereich sicherer digitaler Identitäten und Zero-Trust-Architekturen, bei deren Implementierung wir unsere Kunden unterstützen. Diese Architekturen basieren auf dem Motto ‚Never trust, always verify'. Hier müssen sich die Anwender sowie auch die genutzten Geräte bei jedem Zugriff auf Unternehmensressourcen über einen Trust Broker verifizieren, um Missbrauch entgegenzuwirken.

Quelle: MSG Systems AG

Thomas Soens ist Leiter des Geschäftsbereichs „msg security advisors". Dort wird das Know-how der MSG-Gruppe im Informationssicherheits-, Datenschutz- und Compliance-Umfeld gebündelt

Im jüngsten Report zur Cybersicherheit des Bundesamt für Sicherheit in der Informationstechnik heißt es, dass täglich 250.000 neue Schadsoftware-Varianten auftauchen. Sind alle für die Energieversorger relevant oder gibt es ‚branchenspezifische' Viren?
Natürlich existieren auch branchenspezifische Viren, die unter anderem darauf abzielen, technische Regelsysteme zu kompromittieren, wie beispielsweise im Fall des Schadprogramms ‚Stuxnet', das zuerst unter dem Namen ‚RootkitTmphider' sein Unwesen trieb. Abgesehen davon sind die gleichen Gefahren präsent wie in anderen Branchen. Eine besondere Gefahr wird jedoch durch die Tatsache gemindert, dass in bestimmten Bereichen ‚anfällige' Kommunikationswege wie E-Mails nicht mehr verwendet werden dürfen. Stattdessen ist etwa in der Marktkommunikation Strom die Verwendung von AS4 zur sicheren Kommunikation vorgeschrieben. In diesem Kontext können Energieversorger ihre Gefahrenabwehr stärken, indem sie durch die Wahl sicherer Kommunikationswege spezifische Risiken reduzieren.

Wie können Energieversorger sicherstellen, dass die digitalen Identitäten ihrer Kunden geschützt sind und gleichzeitig eine zuverlässige und sichere Kommunikation für die Steuerung von Energieinfrastrukturen gewährleistet ist?
Dafür sollten Unternehmen eine Sicherheitsstrategie entwickeln, die sich aus ineinandergreifenden Maßnahmen zusammensetzt – etwa die Implementierung robuster Authentifizierungs- und Autorisierungssysteme und die Nutzung verschlüsselter Kommunikationskanäle. Auch regelmäßige Sicherheitsaudits sind sinnvoll. Um Identitäten abzusichern, haben sich Maßnahmen wie die Multi-Faktor-Authentifizierung und biometrische Daten bewährt. Auch die Einführung von Blockchain-Technologien kann die Integrität von Transaktionen sicherstellen.

Was die Kommunikation angeht, so sollten sich Energieversorger in Bereichen, die noch nicht durch AS4 gesichert sind, auf sichere Protokolle stützen, wie etwa TSL (Transport Layer Security) oder den Vorgänger SSL (Secure Sockets Layer). Wichtig sind Schulungen über sichere Praktiken. Auch eine engmaschige Überwachung auf ungewöhnliche Aktivitäten ist hilfreich. So können Unternehmen Sicherheitsverletzungen frühzeitig erkennen. Und auch branchenweite Sicherheitsstandards sind weitere wichtige Schritte hin zu sicheren digitalen Identitäten. **E&M**