Mareike Redder, Product Manager bei der TRIOVEGA GmbH, warum OT-Security nicht als Vorschrift, sondern als Reise betrachtet werden darf und wie man einen klaren Blick für das Wesentliche erlangt.

Zwischen Überforderung und Orientierung

Die aktuelle atp-Ausgabe zeigt eindrucksvoll, wie intensiv sich Unternehmen, Forschung und Industriepartner mit OT-Security auseinandersetzen – strategisch, technologisch und regulatorisch. Es ist ermutigend zu sehen, wie viele Akteure sich auf den Weg machen, Konzepte zu entwickeln, Standards umzusetzen und Sicherheit systematisch mitzudenken.

Gleichzeitig zeigt die Praxis stellenweise ein anderes Bild: Viele Unternehmen stehen noch an einem ganz anderen Punkt. Sie sehen den Wald vor lauter Bäumen nicht. Sie kämpfen mit fragmentierten Altanlagen, unklaren Zuständigkeiten – und der schlichten Frage, wo sie überhaupt anfangen sollen. Zwischen NIS-2, CRA, Zero Trust, IEC 62443, MITRE ATT&CK und Co. verlieren viele den Blick fürs Machbare. Es herrscht nicht Unwille, sondern teilweise Überforderung.

Ich bin regelmäßig auf Veranstaltungen unterwegs – mal als Vortragende, mal im Dialog mit Kunden, häufig in der Rolle der Zuhörenden. Was ich dort und auch in Produktionshallen erlebe, ist weniger technologische Rückständigkeit als die Suche nach Orientierung. Während in Konzeptpapieren über modulare Sicherheitsarchitekturen gesprochen wird, läuft im Werk nebenan eine kritische Steuerung auf MS-DOS. Unersetzbar – aber mit klassischen Maßnahmen kaum absicherbar. Der Wunsch, alle Anlagen auf dem Shopfloor zu vernetzen, schafft neue Schnittstellen – auch dort, wo früher keine waren. Umso wichtiger ist es, Altanlagen sicher in die digitale Infrastruktur einzubinden.

Oft entsteht der nötige Handlungsdruck aber erst dann, wenn ein Angriff das eigene Umfeld trifft oder ein Vorfall es bis in die Geschäftsführung schafft. Dabei gilt: Selbst die engagiertesten CISOs oder OT-Verantwortlichen stoßen an Grenzen, wenn das Thema nicht auf oberster Ebene ernst genommen wird. Sicherheit braucht nicht nur Technik, sondern auch ein klares, gelebtes Bewusstsein im Management – vor dem Ernstfall. Was hilft, ist nicht die perfekte Lösung, sondern ein klarer erster Schritt. Eine Architektur, die zur Realität passt. Gesprächspartner, die zuhören, bevor sie Lösungen präsentieren. Und der Mut, zwischen idealem Zielbild und pragmatischem Handeln zu vermitteln – bevor reagiert werden muss. Denn auch das gehört zur OT-Security in 2025: differenzieren zu können, priorisieren zu dürfen und trotzdem resilienter zu werden.

Es gibt sie, die Projekte, in denen Sicherheit nicht als Nachrüstlösung gedacht, sondern als Bestandteil des Betriebs verstanden wird. In denen Schutzmaßnahmen nicht nur umgesetzt, sondern mitgetragen werden – weil sie helfen, Produktionsfähigkeit zu sichern. Die Herausforderungen sind real – aber lösbar. Wer OT-Sicherheit als Reise und nicht als Vorschrift begreift, hat bessere Chancen, wirklich voranzukommen. Die stärksten Impulse entstehen nicht im Whitepaper, sondern im ehrlichen Gespräch darüber, was machbar ist – und was (noch) nicht. Manchmal reicht ein einziger klarer Blick, um den Wald wiederzusehen.

Mareike Redder

Als Produktmanager bei TRIOVEGA treibt Mareike Redder die strategische Entwicklung von OT-Sicherheitslösungen für die Industrie voran. Ihr Schwerpunkt liegt auf der Verknüpfung von IT und OT durch sichere, praktische und vorschriftsmäßige Technologien, die die Konnektivität ohne Beeinträchtigung der Betriebssicherheit gewährleisten.