SERVICEWARE

CASE STUDY

VARTA MICROBATTERY GMBH stärkt Cyber-Resilienz mit Wingman for CrowdStrike



Wie die VARTA MICROBATTERY ihre IT, OT und Security zusammenführt

Die VARTA MICROBATTERY GMBH steht seit mehr als einem Jahrhundert für Batterietechnologie und Energiespeicherlösungen. Das Unternehmen mit Hauptsitz in Ellwangen betreibt weltweit zahlreiche Standorte darunter mehrere Produktionsstandorte, und verbindet klassische Industrie-IT mit sensiblen OT-Umgebungen. Nach einem schweren Cyberangriff im Februar 2024 wurde Cybersicherheit zu einem zentralen strategischen Thema. Mit CrowdStrike, dem Serviceware-Service „Wingman for CrowdStrike“ und einem konsequenten Plattformansatz gewann VARTA MICROBATTERY GMBH mehr Transparenz, schnellere Reaktionsfähigkeit und eine belastbarere Sicherheitsarchitektur für IT, OT, Identitäten und SIEM.



Auf einen Blick

Die Herausforderungen

- Heterogene IT-/OT-Landschaft mit tausenden von Endpunkten
- Bedarf an 24/7-Schutz
- Transparenz, Auto-Response und Datenschutz vereinen

Die Ergebnisse

- Kein tiefgreifender Vorfall mit eigener Reaktion seit der Attacke
- Zentrale Security-Plattform für IT, OT, Identitäten und SIEM
- Moderne Dashboards dank des Serviceware Wingman Services

Der Kunde
VARTA MICROBATTERY GMBH

Die Branche
Elektrotechnik- und Batterie-industrie

Das Projekt
Einführung der CrowdStrike Falcon-Plattform

VARTA MICROBATTERY GMBH: Batterieherstellung zwischen Tradition und Transformation

Die VARTA MICROBATTERY GMBH gehört zu den bekanntesten deutschen Namen in der Batterietechnologie. Das Unternehmen mit Hauptsitz in Ellwangen entwickelt und produziert Energiespeicherlösungen für anspruchsvolle Anwendungen in den Bereichen Hörgeräte, Wearables, Medizin, IoT, Smart Home/Metering und Konsumelektronik. Die Produkte der VARTA MICROBATTERY GmbH stehen für präzise und langlebige Energielösungen Made in Germany.

In der öffentlichen Wahrnehmung steht die Marke oft für die Batterie im Alltag. In der industriellen Realität ist die VARTA MICROBATTERY zugleich ein global vernetzter Hersteller mit komplexen Produktionsprozessen, internationaler Lieferkette und hohen Anforderungen an Verfügbarkeit, Qualität und Sicherheit.

Rund 2.200 Mitarbeitende und weltweit mehrere Administrations- und Produktionsstandorte prägen die Größenordnung, in der VARTA MICROBATTERY GMBH IT-Sicherheit organisieren muss. Die IT-Organisation deckt mit seinen Mitarbeitenden drei wesentliche Kernbereiche ab: ERP, MES/OT und IT Operations. Die Besonderheit liegt nicht nur in der Unternehmensgröße, sondern auch in der besonderen Struktur. Das Unternehmen ist historisch gewachsenen, hat unterschiedliche Unternehmensbereiche integriert und betreibt eine globale IT- und OT-Landschaft mit mehreren Active

Directories, produktionsnahen Systemen, Office-IT, Cloud-Anbindungen und spezialisierten Anlagen.

Ein Thema, das auch viele andere Industrieunternehmen kennen, ist auch bei der VARTA MICROBATTERY eine Herausforderung: „In einem Umfeld mit Produktionsanlagen, gewachsenen Domänen und internationalen Standorten lässt sich eine Sicherheitsarchitektur nicht über Nacht neu aufsetzen. Dieser Vorgang braucht einfach Zeit“, beschreibt Matthias Kruger, Information Security Officer und IT Security Manager bei der VARTA MICROBATTERY GMBH, die Ausgangslage.

Wo Produktion, Office IT, Identitäten, ERP- und MES-Systeme ineinandergreifen, können Störungen schnell weit über die IT hinauswirken. Die Relevanz der IT-Sicherheit ist in diesem Umfeld daher besonders hoch. Verfügbarkeit ist für einen produzierenden Mittelständler nicht nur eine technische Kenngröße, sondern eine betriebliche Voraussetzung. Gleichzeitig steigen die Anforderungen an Transparenz und Nachvollziehbarkeit: Welche Systeme kommunizieren miteinander? Welche Identitäten greifen auf welche Umgebungen zu? Wo entstehen Schatten-IT, unbekannte Assets oder ungewollte Verbindungen zwischen Office- und Produktionszonen? Die VARTA MICROBATTERY GMBH musste diese Fragen nicht theoretisch beantworten, sondern unter sehr realen Bedingungen: Ein Cyberangriff 2024 machte sichtbar, wie entscheidend ein integrierter Blick auf IT und OT ist. Das Unternehmen reagierte mit einer Security-Strategie, die Technologie zunächst in den Mittelpunkt stellt: schnelle Sichtbarkeit, zentrale Steuerung, konsequente Absicherung der Endpunkte, Einbindung von Identitäten und ein Next-Gen SIEM als operativer Daten- und Reaktionskern. Und das Ganze mit Serviceware als externer Partner und Value Added Reseller an der Seite.



Warum die VARTA MICROBATTERY GMBH ein neues Auge für IT und OT brauchte

Die Ausgangslage vor dem Ausbau der Sicherheitsplattform war geprägt von typischen, aber kritischen Herausforderungen produzierender Unternehmen. Die VARTA MICROBATTERY verfügte über eine heterogene IT-Umgebung und eine breite OT-Landschaft. Unterschiedliche Domänen, verschiedene Paketier- und Verwaltungssysteme sowie produktionsnahe Anlagen machten es schwierig, Sicherheitsmaßnahmen schnell und flächendeckend umzusetzen.

Im Zentrum stand zunächst die Endpoint Security. Eine bestehende Sicherheitslösung musste abgelöst werden. Zugleich war klar, dass ein reiner Austausch eines Endpoint-Produkts nicht reichen würde. VARTA brauchte eine Architektur, die zu einer internationalen, produktionsnahen Umgebung passt: mit 24/7-Überwachung, zentraler Transparenz, schneller Reaktionsmöglichkeit und möglichst wenig zusätzlichem Betriebsaufwand für das kleine interne Security-Team.

„Wir haben keine großen personellen Ressourcen, die sich selbst um alles kümmern können. Also brauchen wir 24/7-Service. Wir wollen ein Auge, das alles sehen kann, und wir wollen immer die Möglichkeit haben, reinzugrätschen“, sagt Matthias Kruger. Damit formuliert er die vier zentralen Anforderungen: Kosten im Blick behalten, Aufwand reduzieren, vollständige Transparenz herstellen und Auto-Response ermöglichen. Als fünfter Punkt kam der Wunsch hinzu, nicht permanent zwischen unterschiedlichen Tools wechseln zu müssen. Eine Plattform sollte möglichst viele Informationen bündeln.

Der Cyberangriff vom 12. Februar 2024 veränderte die Prioritäten zusätzlich. Während der Angriff aufgearbeitet wurde, rückte eine Erkenntnis in den Vordergrund: Dort, wo CrowdStrike als umfassende Security-Plattform bereits installiert war, entstand ein anderer Schutz- und Reaktionskontext als in Bereichen, die noch nicht entsprechend abgesichert waren. In den folgenden Wochen und Monaten ging es deshalb darum, möglichst viele erreichbare Systeme mit dem Sensor auszustatten, neue Sicherheitssegmente aufzubauen und die Gesamtarchitektur grundlegend weiterzuentwickeln.

Dabei stieß die VARTA MICROBATTERY auf eine Herausforderung, die viele Unternehmen unterschätzen: Security ist nicht nur Technik, sondern auch Organisation. Rollouts von Sicherheitssoftware berühren Datenschutz, Mitbestimmung, Arbeitsprozesse und Vertrauen im Unternehmen. Kruger beschreibt das offen: „Sicherheit muss intern gut erklärt werden, weil sie aus Sicht mancher Mitarbeitender schnell wie Überwachung wirken kann. In einem traditionellen Unternehmen wie der VARTA MICROBATTERY brauche dieser Dialog Zeit“.

Die eigentliche Herausforderung lag deshalb in der Verbindung dreier Ebenen: Technologie, Prozesse und Mensch. Prozesse und kulturelle Veränderungen lassen sich nicht beliebig beschleunigen. Die Technologie hingegen konnte schneller helfen, Schutz aufzubauen und Handlungsfähigkeit zurückzugewinnen. Der Batteriehersteller entschied sich daher für einen „Technology first“-Ansatz: zuerst Sichtbarkeit und Reaktionsfähigkeit erhöhen, danach Prozesse und Awareness weiterentwickeln.



Besonders deutlich wurde der Bedarf im OT-Umfeld. In produktionsnahen Netzen ist eine vollständige Abschottung selten realistisch. ERP- und MES-Systeme müssen Daten austauschen, Wartungszugänge müssen kontrolliert möglich sein, Produktionsanlagen brauchen definierte Verbindungen. Segmentierung bedeutet daher nicht, alles zu trennen, sondern erlaubte Brücken sichtbar, überprüfbar und absicherbar zu machen. Genau dafür fehlte zuvor in Teilen die Transparenz.

Der Anspruch lautete: erst sehen, dann bewerten, dann handeln. Ohne verlässlichen Überblick über Assets, Identitäten, Datenflüsse und Verbindungen bleibt Risikomanagement abstrakt. Die VARTA MICROBATTERY GMBH wollte deshalb nicht nur Endgeräte schützen, sondern ein Lagebild schaffen, das IT, OT, Identitäten, Cloud-Quellen und Netzwerkdaten zusammenführt.

Wie Serviceware CrowdStrike operativ wirksam macht

Die technische Grundlage der neuen Sicherheitsarchitektur bildet die CrowdStrike Falcon-Plattform. Dabei kommen unter anderem die Funktionen für Endpoint Protection, Managed Detection and Response, Identity Protection, Next-Gen SIEM, Exposure Management, Falcon for IT und XIoT Security zum Einsatz. Der Plattformansatz war für die VARTA MICROBATTERY GMBH besonders wichtig, weil er eine zentrale Sicht auf unterschiedliche Sicherheitsbereiche ermöglicht. Statt Daten, Alarme und Maßnahmen in vielen Einzelsystemen zu verteilen, sollen relevante Informationen in einer Umgebung zusammenlaufen.

CrowdStrike Falcon Complete übernimmt dabei den 24/7-Schutz und die operative Reaktion auf erkannte Bedrohungen. Für ein kleines internes Security-Team ist dieser Managed-Service-Ansatz entscheidend. Die VARTA MICROBATTERY GMBH kann auf externe Security-Expertise zugreifen, ohne intern ein vollumfängliches Security Operations Center (SOC) aufbauen zu müssen. Gleichzeitig bleibt die Möglichkeit erhalten, selbst in relevante Fälle einzusteigen, Regeln zu verstehen und die Plattform aktiv weiterzuentwickeln.

Die Serviceware-Dienstleistung „Wingman for CrowdStrike“ ergänzt diese Struktur. Sie ersetzt nicht den Managed Service von CrowdStrike, sondern setzt dort an, wo die Plattform für den konkreten Kunden nutzbar, integriert und optimiert werden muss. Dazu gehören das Onboarding zusätzlicher Datenquellen, die Arbeit am Next-Gen SIEM, Parser, Korrelationsregeln, Dashboards, Policies, Security Validation und operative Unterstützung im Alltag.

„Der Hauptpunkt vom Wingman ist, die Verbindung vom Next-Gen SIEM zu unseren Produkten hinzubekommen: Parser, Daten korrelieren und dann zum Beispiel automatisch auf diese Sachen zu reagieren“, erklärt Kruger. Genau in dieser Übersetzung von Plattformfähigkeiten in konkrete VARTA MICROBATTERY -Use-Cases liegt der Wert der Zusammenarbeit.

Ein Beispiel sind die angebundenen Datenquellen. Die VARTA MICROBATTERY integriert unter anderem seine Firewalls, Microsoft- und AWS-Umgebungen sowie weitere Systeme und Quellen in das Next-Gen SIEM. Nicht jede Quelle ist gleich relevant, nicht jedes Log-Level sinnvoll. Deshalb braucht es

Beratung und technische Umsetzung: Welche Daten werden gebraucht? Welche Parser müssen angepasst werden? Welche Korrelationsregeln erzeugen brauchbare Hinweise statt Rauschen? Welche Reaktionen sollen künftig automatisiert werden?

Serviceware unterstützt den Batteriehersteller außerdem beim Aufbau spezifischer Dashboards direkt im CrowdStrike Next-Gen SIEM. Ein Schwerpunkt liegt auf Identity Protection und Mikrosegmentierung. Die VARTA MICROBATTERY GMBH wollte nicht nur lange Listen sehen, sondern Zusammenhänge erkennen: Welche Regeln werden von welchen Usern ausgelöst? Zu welchen Zeiten entstehen Detections? Welche Prioritäten häufen sich? Welche Verbindungen führen aus Office-Netzen in OT-Bereiche oder aus der OT ins Internet?

„Serviceware baut uns die Dashboards, die CrowdStrike vor allem im Mittelstand so schnell noch nicht liefern kann“, sagt Kruger. Die Serviceware-Boards machen aus vorhandenen Daten operative Arbeitsmittel. Sie helfen, Regeln zu überprüfen, Segmentierung zu kontrollieren, ungewöhnliche Verbindungen sichtbar zu machen und Entscheidungen für nächste Schritte vorzubereiten.

Besonders relevant ist dies in der OT Security. Die VARTA MICROBATTERY kann nicht jede Verbindung zwischen IT und OT pauschal blockieren. Manche Brücken sind betrieblich notwendig, etwa zwischen Produktionssystemen. Die Dashboards helfen, gewollte und ungewollte Brücken zu unterscheiden. Perspektivisch sollen bestimmte unbekannte oder unerwünschte Verbindungen automatisch blockiert werden können, etwa über Auto-Response-Skripte und Firewall-Integrationen.

Auch die Zusammenarbeit selbst spielt eine zentrale Rolle. Die VARTA MICROBATTERY nutzt ein monatliches Wingman-Kontingent, in dem technische Themen, Security Validation, SIEM-Weiterentwicklung und Projektmanagement bearbeitet werden. Für Kruger ist dabei nicht allein die fachliche Kompetenz entscheidend, sondern auch die Reaktionsgeschwindigkeit. In der IT-Sicherheit zählt Zeit. Wenn ein Vorfall, eine Frage oder ein Sonderfall entsteht, hilft es nicht, nur eine Ticketnummer zu erhalten. Entscheidend ist, ob jemand reagiert, versteht und direkt an einer Lösung arbeitet.

Mehr Transparenz, schnellere Reaktion

Die Ergebnisse der neuen Architektur zeigen sich vor allem in drei Bereichen: Sichtbarkeit, Reaktionsfähigkeit und Vertrauen in die eigene Sicherheitslage. Die VARTA MICROBATTERY hat seit dem Cyberangriff keinen weiteren tiefgreifenden Sicherheitsvorfall erlebt, bei dem das interne Team selbst umfassend reagieren musste. Detections und Reaktionen werden über CrowdStrike und die angebundenen Services abgefangen oder bearbeitet. Für ein Unternehmen, das zuvor einen massiven Angriff bewältigen musste, ist das ein wichtiges Ergebnis.

„Seit der Cyberattacke hatten wir keinen Vorfall mehr in der Tiefe, dass wir irgendwo selbst noch reagieren mussten. Das hat alles CrowdStrike weggefischt“, sagt Matthias Kruger. Gleichzeitig bleibt er realistisch: Absolute Sicherheit gibt es nicht. Angriffe verändern sich, künstliche Intelligenz wird Angreifern helfen, Schwachstellen schneller zu finden und automatisiert auszunutzen. Gerade deshalb braucht die VARTA MICROBATTERY GMBH eine Architektur, die nicht statisch ist, sondern weiterentwickelt werden kann.

Ein besonders greifbarer Effekt ist die Asset-Transparenz. Beim Ausbau der OT-Sichtbarkeit stellte der Batteriehersteller fest, dass die Zahl der OT-Assets deutlich höher lag als ursprünglich angenommen. Dieses Aha-Erlebnis ist zentral: Erst wenn Systeme bekannt sind, lassen sie sich bewerten, priorisieren, segmentieren und ins Risikomanagement aufnehmen. Vorher bleibt Security in Teilen Schätzung.

„Du musst erst alles sehen können, damit du auf die Sachen reagieren oder überhaupt agieren kannst“, sagt Kruger. Genau dieses Prinzip bildet den Kern der neuen Sicherheitsstrategie. Sichtbarkeit wird zur Voraussetzung für Steuerung. Die Kombination aus CrowdStrike, Serviceware Wingman, Next-Gen SIEM, Identity Protection und XIoT macht IT- und OT-Assets, Identitäten, Zugriffe und Datenflüsse greifbarer.

Auch Penetrationstests zeigten laut Kruger eine veränderte Sicherheitslage. Bei Tests sei es notwendig gewesen, Schutzmechanismen zu deaktivieren und Firewalls zu öffnen, weil die Prüfer sonst nicht wie gewünscht in die Umgebung gekommen seien. Für die VARTA MICROBATTERY GMBH bestätigt das die Wirkung aus Segmentierung, Endpoint-

Schutz und Plattformüberwachung. Aus redaktioneller Sicht ist dabei wichtig: Solche Tests ersetzen keine Garantie, zeigen aber, dass die Angriffspfade deutlich enger kontrolliert werden.

Ein weiterer Effekt liegt im operativen Arbeiten. Das Next-Gen SIEM und die Dashboards reduzieren die Notwendigkeit, Informationen mühsam aus verschiedenen Systemen zusammenzutragen. Statt einzelne Teams mit Tickets zu bedienen, können IT, Security und Fachbereiche anhand zentraler Daten zusammenarbeiten. Das beschleunigt Triage, Abstimmung und Reaktion. Für Management und IT-Führung werden Sicherheitsinformationen zudem verständlicher aufbereitet.

Serviceware wird dabei nicht als anonymer Dienstleister empfunden, sondern als Partner mit hoher Nähe. Kruger nennt zwei Faktoren: Vertrauen und Geschwindigkeit. Vertrauen entsteht über Zeit, über persönliche Zusammenarbeit und über die Erfahrung, dass auch schwierige Themen weiterbearbeitet werden. Geschwindigkeit zeigt sich in der Praxis, wenn Anrufe, E-Mails oder Nachrichten nicht nur formal bestätigt werden, sondern direkt zu Handlung führen. So konnte etwa bei einem Mobile-Device-Vorfall kurzfristig ein Modul temporär von Serviceware aktiviert werden, um das betroffene Gerät zu prüfen. Für Kruger unterscheidet genau das eine belastbare Security-Partnerschaft von einem Standard-Support. In einem Umfeld, in dem ein Vorfall schnell eskalieren kann, ist Reaktionszeit kein Komfortfaktor, sondern Teil der Sicherheitsarchitektur.





Agentic SOC soll zukünftig für mehr Automatisierung sorgen

Der Blick nach vorn geht in Richtung Agentic SOC. Die VARTA MICROBATTERY GMBH denkt darüber nach, künftig für einzelne Datenquellen spezifische AI Agents einzusetzen. Ein möglicher Use Case: Ein kompromittierter User versucht aus einem ungewöhnlichen Kontext heraus auf OT-Systeme zuzugreifen. Ein Identity Agent könnte Token zurücksetzen und den User deaktivieren, ein Endpoint Agent könnte das Gerät isolieren, ein Firewall Agent könnte Verbindungen schließen. Noch ist das Zukunftsbild, aber es zeigt die Richtung: Automatisierung soll schneller werden, ohne die Kontrolle vollständig aus der Hand zu geben.

Für die VARTA MICROBATTERY ist die Plattform damit kein abgeschlossenes Projekt, sondern ein Ausbaupfad. Die aktuelle Architektur schafft Transparenz, der Serviceware Wingman hilft bei Integration und Optimierung, CrowdStrike übernimmt Detection und Response. Zusammen entsteht ein Sicherheitsmodell, das zu einem produzierenden Mittelständler passt: pragmatisch, zentralisiert, skalierbar und auf konkrete Risiken ausgerichtet.

Fazit

- Die VARTA MICROBATTERY schützt IT, OT und Identitäten zentral mit CrowdStrike
- Serviceware optimiert SIEM, Parser und Policies
- Individuelle Dashboards werden vom Serviceware Team erstellt und zur Verfügung gestellt
- Seit der Attacke kein tiefgreifender Vorfall mit eigener Reaktion
- Wesentlich höhere Sicherheitsstandards im gesamten Unternehmen



Matthias Kruger
Security Officer & IT Security Manager,
VARTA MICROBATTERY GMBH

Kurzportrait: Matthias Kruger ist Information bei der VARTA MICROBATTERY GMBH. Er verantwortet dort strategische und operative Informationssicherheit und war bereits zuvor als IT-Security Architect beim Batteriehersteller tätig, unter anderem mit Fokus auf Produktionssegmentierung, Hybrid Alert and Response Center und industrielle Compliance. Vor seiner Zeit bei der VARTA MICROBATTERY GMBH arbeitete er unter anderem bei FNT Software und der Porsche Lifestyle Group. Neben der IT-Sicherheit ist Kruger in der Breaking-Kultur aktiv – als Tänzer, Coach und Lehrer.

Über Serviceware

Serviceware bietet seit mehr als 25 Jahren Software, Beratung und Managed Services zur Digitalisierung moderner Unternehmensprozesse. Von Enterprise Service Management über IT Financial Management bis Security, Data und Endpoint Management – hochautomatisiert und sicher.

Serviceware SE
Serviceware-Kreisel 1
65510 Idstein • Germany
+49 6434 9450 0
contact@serviceware-se.com
serviceware-se.com

10/2026

SERVICEWARE