Leistungselektronik für E-Mobilität | BRUSA HyPower

BRUSA HyPower stärkt mit NTT DATA die Cyber-Abwehr und minimiert Compliance-Risiken

Client | Kurzprofil

Die BRUSA HyPower AG mit Sitz in Buchs (Kanton St. Gallen) wurde 2021 als Spin-off der BRUSA Elektronik AG gegründet, einem Anbieter für Leistungselektronik im Bereich E-Mobility. Das international agierende Unternehmen ist auf elektrische Energiewandler- und Onboard-Ladesysteme spezialisiert und entwickelt Lösungen für On-Highway-, Off-Highway- sowie stationäre Anwendungen. Die BRUSA HyPower beschäftigt rund 220 Mitarbeitende.

Gründe für NTT DATA

- Führender Anbieter im Bereich Security Operations Center
- Langjährige Expertise bei der Abwehr moderner Cyber-Gefahren und der Reduzierung von Compliance-Risiken
- Globale Präsenz und Rund-um-die-Uhr-Betreuung

> NTT DATA lag bei der Bewertung der verschiedenen SOC-Angebote unangefochten an der Spitze. Die globale Präsenz und die langjährige Erfahrung helfen dabei, unser stetig wachsendes Geschäft abzusichern.

Richard Knuchel, Corporate Security Officer bei der BRUSA HyPower AG

Die Gefährdung von Assets und Compliance-Verletzungen durch die Zunahme von Cyber-Angriffen wurde für die BRUSA HyPower AG zunehmend zu einer Herausforderung. Um die Abwehr zu stärken und die Risiken zu reduzieren, setzt das Unternehmen auf eine umfassende Lösung von NTT DATA.

Die Herausforderung

Als weltweit tätiges Unternehmen mit einer Vielzahl von digitalen Anwendungen und Prozessen muss die BRUSA HyPower in der Lage sein, Compliance-Verstöße und Gefährdungen von Vermögenswerten frühzeitig zu erkennen und Maßnahmen zu deren Schutz zu ergreifen.

Die Lösung

Ein Managed Security Service (MSS) SIEM/SOC in Kombination mit Digital Forensic and Incident Response (DFIR) und Consulting-Leistungen rund um Cyber-Security sorgen dafür, dass die BRUSA HyPower optimal auf verschiedenste Angriffe und Risiken vorbereitet ist.

Die Vorteile

- Schnelle Erkennung von Bedrohungen und Vorfällen
- Tiefgehende Analyse und Beweissicherung
- Modernste Überwachung rund um die Uhr

> In der Evaluierungsphase und jetzt im Betrieb gibt es immer eine kompetente und schnelle Kommunikation, bei Bedarf bis hin zum Experten.
>
> **Richard Knuchel,** Corporate Security Officer bei der BRUSA HyPower AG

Die Herausforderung

Fortschrittliche Angriffe erfordern ein Umdenken

Cyber-Sicherheit ist nicht mehr nur ein technologisches Risiko. Angesichts der Kosten, des möglichen Reputationsschadens, des Vertrauensverlusts bei den Stakeholdern und der rechtlichen Haftung, die auf dem Spiel stehen, ist sie auch ein Compliance-Risiko und damit eine strategische Notwendigkeit. Angriffe können viele Formen annehmen, von Ransomware und Phishing bis hin zu Insider-Bedrohungen und gezielten Angriffen durch staatlich unterstützte Akteure. Die Frage ist längst nicht mehr, ob ein Unternehmen ins Visier von Cyberkriminellen gerät, sondern wann und in welchem Ausmaß.

Ziel muss es daher sein, die Auswirkungen von Cyber-Vorfällen auf den Geschäftsbetrieb zu minimieren und im Falle eines Falles die Geschäftskontinuität sicherzustellen. Um dies zu erreichen, haben moderne Erkennungs-, Reaktions- und Wiederherstellungsfunktionen oberste Priorität. Dazu gehört einerseits die Fähigkeit, Bedrohungen rund um die Uhr zu erkennen, zu untersuchen und darauf zu reagieren. Andererseits ist ein gut durchdachter Incident-Response-Plan der Schlüssel, um schnell auf Sicherheitsvorfälle zu reagieren und so den Schaden zu minimieren. Die meisten Unternehmen verfügen jedoch nicht über die Ressourcen, um diese Aufgaben mit ihrem eigenen IT-Team zu bewältigen.

Vor dieser Herausforderung stand die BRUSA HyPower AG. Die Schweizer Leistungselektronik-Herstellerin, die auf die Entwicklung und Produktion von Technologien für die Elektromobilität spezialisiert ist, benötigte eine moderne IT-Sicherheitsumgebung zum Schutz ihrer sensiblen Daten.

Die Lösung

Managed Services schützen die sensiblen Daten

Die BRUSA HyPower hat sich für ein umfassendes Paket von NTT DATA entschieden, das aus einem Managed Security Service (MSS) SIEM/SOC (Security Information and Event Management/Security Operations Center), einem DFIR (Digital Forensics and Incident Response) Retainer und Consulting-Leistungen besteht. Ausschlaggebend war, dass NTT DATA bei der internen Bewertung der verschiedenen Security-Operations-Center-Angebote unangefochten an der Spitze lag. Neben der ausgewiesenen Expertise kann NTT DATA durch seine globale Präsenz zudem die besonderen Anforderungen eines international agierenden Herstellers abdecken.

Der MSS SIEM/SOC von NTT DATA ist ein gemanagter Service, der Bereitstellung, Plattformmanagement, Erkennung von Cyber-Bedrohungen, Compliance-Reporting, benutzerdefinierte Anwendungsfälle, Dashboards und Playbooks für die Eskalation von Vorfällen umfasst. Der Service kombiniert kommerzielle SIEM-Funktionen mit fortschrittlicher Analytik und Threat Intelligence zur Erkennung von Angriffen. Im Vorfeld wurde das System an die spezifischen Geschäftsanforderungen von BRUSA HyPower angepasst, einschließlich der Bewertung von Schlüsselelementen wie Topologie, Protokollquellen, Rechenzentrumsstandorten und wichtigen logischen Netzwerkanforderungen.

Im Rahmen des SLA-basierten DFIR Retainer stehen der Schweizer Leistungselektronik-Herstellerin im Notfall erfahrene Sicherheitsanalysten und Forensiker von NTT DATA rund um die Uhr zur Seite.

Die Vorteile

Hoher Schutzwall gegen Cyber-Bedrohungen und Compliance-Risiken

Mit dem Managed Security Service SIEM/SOC und DFIR hat die BRUSA HyPower eine hochmoderne Sicherheitsumgebung implementiert. Für das Unternehmen ergeben sich daraus mehrere Vorteile.

Schutz rund um die Uhr

Die SOC-Experten von NTT DATA überwachen das SIEM-System von BRUSA HyPower rund um die Uhr, so dass eine Analyse und Reaktion auf Sicherheitsvorfälle in Echtzeit erfolgen kann. Regelmäßige Reports geben einen Überblick über die verschiedenen Risiken und Bedrohungen. Zusätzlich werden Tools wie Google SecOps und ServiceNow eingesetzt, mit denen die BRUSA-Mitarbeitenden Risikoanalysen einsehen und Informationen über Tickets abrufen können. Verdächtige Aktivitäten werden mit den Cyber-Security-Analysten aus dem Security Operations Center von NTT DATA besprochen. So ist eine schnelle Reaktion auf Vorfälle inklusive Beweissicherung und Compliance-Reporting gewährleistet.

Starker Partner an der Seite

Mit NTT DATA hat die BRUSA HyPower zudem einen erfahrenen Partner an der Seite, der die eigene IT-Umgebung im Ernstfall optimal schützt. Die Sicherheitsexperten und -analysten von NTT DATA nehmen eine Risikobeurteilung vor, geben Technologieempfehlungen gegen Bedrohungen und unterstützen bei der Compliance-Evaluation. Gleichzeitig profitiert das Unternehmen von strategischen Partnerschaften sowie der jahrzehntelangen Erfahrung und globalen Präsenz von NTT DATA, die dem expandierenden Geschäft der Schweizer Leistungselektronik-Herstellerin zugutekommen.

Dadurch kann sich die BRUSA HyPower auf ihre Kerngeschäftsziele konzentrieren und sich bei Wartung, Überwachung und Betrieb ihrer Sicherheitsumgebung auf die Experten von NTT DATA verlassen.

Über NTT DATA

NTT DATA – ein Teil der NTT Group – ist Trusted Global Innovator von Business- und IT-Lösungen mit Hauptsitz in Tokio. Wir unterstützen unsere Kunden bei ihrer Transformation durch Consulting, Branchenlösungen, Business Process Services, IT-Modernisierung und Managed Services.

Mit NTT DATA können Kunden und die Gesellschaft im Allgemeinen selbstbewusst in die digitale Zukunft gehen. Wir setzen uns für den langfristigen Erfolg unserer Kunden ein und kombinieren globale Präsenz mit lokaler Kundenbetreuung in über 50 Ländern.

Weitere Informationen finden Sie auf **de.nttdata.com**

Kontaktieren Sie unsere Expertin

Ann-Cathrin Gauweiler
Service Delivery Manager | Cyber Security Consulting
Ann-Cathrin.Gauweiler@nttdata.com