

Größtmögliche Sicherheit zu jeder Sekunde des Tages

partner content

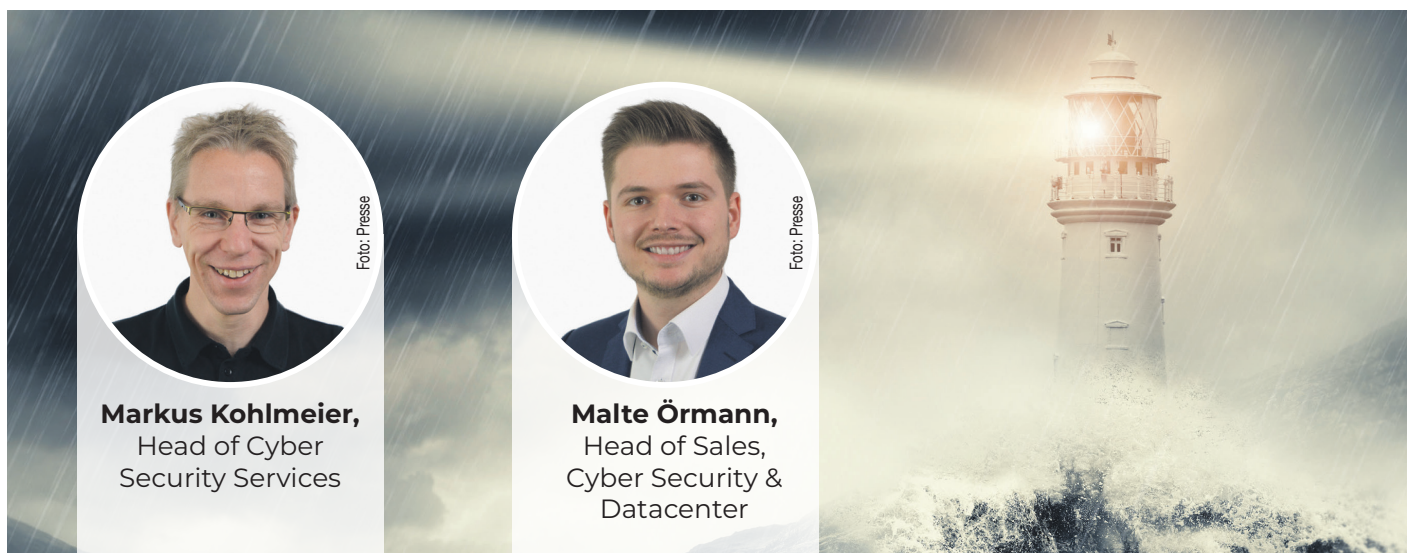
Industrie Security braucht Experten, die Ihr Unternehmen verstehen. DTS Systeme bietet ganzheitliche Sicherheitslösungen rund um die Uhr.

Welche Rolle spielen Sie für Ihre Kunden im Zuge der Digitalisierung?

Malte Örmann: Als ganzheitlicher IT-Dienstleister mit dem Fokus auf Cyber Security beraten und unterstützen wir Unternehmen in Ihrer digitalen Transformation während des gesamten Projektprozesses. Wir sind darin so erfolgreich, weil wir von Beginn an auf mögliche Cybersicherheitsrisiken hinweisen und passgenaue, individuelle Lösungen für Unternehmen konzeptionieren, implementieren, betreiben und sicherheitswirksam betreuen. Beim Aufbau neuer, digitaler Geschäftsmodelle und -prozesse ist dies leider ein Aspekt, der häufig vernachlässigt wird.

Welche Risiken verbergen sich dahinter?

Markus Kohlmeier: In der Smart Factory ist zwangsläufig der Anschluss von Maschinen und Komponenten mit lokalen sowie externen Netzen wie dem Internet erforderlich. Dadurch entsteht jedoch ein komplett neues Einfallstor in einer Umgebung, die aufgrund von ungeschützten Betriebssystemen und teils veralteten Software-Versionen eine Vielzahl



Markus Kohlmeier,
Head of Cyber Security Services

Malte Örmann,
Head of Sales, Cyber Security & Datacenter

an Sicherheitslücken aufweist. Darüber hinaus ist für viele Unternehmen die Nutzung der Cloud ein einfaches Mittel, um neu erforderliche Rechenkapazitäten sowie Datenspeicher hoch verfügbar, überall erreichbar und schnell skalierend bereitzustellen. Aber auch die Cloud ist nicht von Haus aus sicher. Mein smarterer Dienst, der fleißig Daten in der Public Cloud ablegt, muss ebenso entsprechend abgesichert werden, um nicht der Gefahr eines Datenverlustes oder gar unbemerkter Manipulation meiner Dienste ausgesetzt zu werden. Beispielsweise können nützliche IoT Devices aus zweierlei Sicht eine Bedrohung darstellen. Zum einen sind sie oft ungeschützt und öffnen dadurch ein Einfallstor in die sonst geschützte IT-Umgebung. Zum anderen haben Hacker ebenfalls erkannt, dass es sehr einfach ist, IoT Devices zu übernehmen und zu gigantischen Botnetzen zusammenzuführen. Diese sind für wenig Geld im Darknet als Service buchbar, um mit gezielten DDoS-Angriffen ein Unternehmen stunden- oder tagelang lahmzulegen.

Das klingt ja ziemlich bedrohlich. Wie kann man sich dagegen schützen?

Malte Örmann: Getreu dem Leitsatz „Sicherheit kommt durch Sichtbarkeit“ helfen wir unseren Kunden im ersten Schritt dabei, den IST-Zustand zu identifizieren. Welche Systeme gibt es, wer kommuniziert mit wem und wie ist der Zustand der eingesetzten

Komponenten? Aufgrund dieser Grundlage haben wir anschließend die Möglichkeit, eine effektive Risikobewertung vorzunehmen und im nächsten Schritt die Systeme und Kommunikationswege abzuschirmen sowie Manipulation und ungewöhnliches Verhalten aufzudecken.

Bin ich dann gegen alle Cyberbedrohungen abgesichert?

Malte Örmann: Einen einhundertprozentigen Schutz gibt es leider nicht. Für Angreifer stehen wirtschaftliche Interessen im Vordergrund und für diese sind sie bereit, enorme Aufwendungen in Kauf zu nehmen. Trotz diverser Schutzmaßnahmen und einer massiven Eingrenzung des Angriffsvektors sollte aus diesem Grund eine permanente Überwachung der eigenen Umgebung stattfinden, um besonders zielgerichtete und komplexe Angriffe in kürzester Zeit aufzudecken. Für

Unternehmen ist es allerdings eine große Herausforderung, eigene Security Experten rund um die Uhr zu beschäftigen sowie im Ernstfall ausreichend Fachkräfte kurzfristig hinzuziehen zu können.

Wie können Sie da helfen?

Markus Kohlmeier: Wir überwachen vollumfänglich IT-Infrastrukturen und sammeln Log-Informationen einzelner Systeme. Diese werten wir aus, um Anomalien schnellstmöglich aufzudecken und gemeinsam mit unseren Kunden Gegenmaßnahmen einzuleiten. Dies machen wir nicht nur maschinengestützt, sondern mit einem hochqualifizierten Team aus Security Analysten, das an 365 Tagen rund um die Uhr verfügbar ist. Unser Security Operations Center (SOC) ist dabei unsere zentrale Sicherheitsleitstelle zum Schutz sensibler Kundendaten vor sämtlichen Bedrohungen.



Für Unternehmen ist es allerdings eine große Herausforderung, eigene Security Experten rund um die Uhr zu beschäftigen sowie im Ernstfall ausreichend Fachkräfte kurzfristig hinzuziehen zu können.

DTS Systeme steht als erfolgreicher IT-Dienstleister seit über 35 Jahren deutschland- und europaweit für Innovation, Kompetenz sowie Leidenschaft. Hinter dem Namen steht eine Technik Company bestehend aus den drei Kernbereichen Datacenter, Technologies und Security. Über 300 Mitarbeitende an 13 Standorten stellen mit zwei eigenen deutschen Rechenzentren sowie einem Co-Location Partnerrechenzentrum ganzheitliche IT-Lösungen und Services, rund um die Uhr an 365 Tagen, zur Verfügung. DTS ist sowohl Urgestein als auch Vorreiter in der Cloud und IT-Sicherheit. Mit ihrem hybriden DTS Baukastenkonzept und der Managed Multicloud entwickeln sie Made in Germany Know-how in der Wolke. Zudem haben sie sich als IT-Security Hersteller, Security Operations Center und Managed Services Experten etabliert. Potenziale optimal nutzen, sämtliche Anforderungen erfüllen, innovative Lösungen, Service-Mehrwerte rund um die Uhr – das ist die DTS Systeme.

Die 10 größten Cyber Bedrohungen im Industriefeld

Einschleusen von Schadsoftware über Wechseldatenträger & externe Hardware	Infektion mit Schadsoftware über Internet & Intranet	Menschliches Fehlverhalten & Sabotage	Kompromittierung von Extranet & Cloud Komponenten	Social Engineering & Phishing
DDoS-Angriffe	Internet-verbundene Steuerungskomponenten	Einbruch über Fernwartungszugänge	Technisches Fehlverhalten & höhere Gewalt	Kompromittierung von Smartphones im Produktionsumfeld