

A knight in full plate armor, including a helmet with a visor, is shown from the chest up. He is holding a sword with both hands, and a dense field of glowing blue digital lines radiates from the blade, suggesting a connection to technology or cyber security. The knight is positioned in front of a stone wall with a yellow section and a blue dragon-like emblem.

DTS

INDUSTRIAL SECURITY

INDUSTRIAL SECURITY

Die voranschreitende Digitalisierung, Industrie 4.0 sowie die zunehmende Vernetzung von Produktionsumgebungen, -prozessen und -systemen stellt zahlreiche Branchen vor völlig neue Herausforderungen. Eine wesentliche, wenn auch oft unterschätzte Aufgabe ist es, die absolut notwendige Basis für eine abgesicherte IT im Industriefeld zu legen. Die Folgen eines Cyberangriffs können hier gravierend sein. Produktionsausfälle, Industriespionage und fehlerhafte Produkte gefährden die Wettbewerbsfähigkeit der betroffenen Unternehmen, von den Image- oder Folgeschäden ganz zu schweigen. Als DTS unterstützen wir Sie in jedem Bereich der Industrial Security und machen Ihre IT zukunftssicher.

Wir verknüpfen praxiserprobte Lösungen, entwickeln spezifisch zugeschnittene, hybride Lösungen und unterstützen Sie während des gesamten Projektprozesses. Zudem geben Ihnen unsere Herstellerzertifizierungen und qualifizierten Techniker die Sicherheit, uns durch professionelle und kompetente Beratung an jedem Punkt blind vertrauen zu können. DTS, das ist Cyber Security Know-how, Sichtbarkeit, Diagnose, Analyse und Verteidigung für Ihre Produktionsumgebung.

- Sicherheit durch Sichtbarkeit
- Vollständige Absicherung für Endgeräte
- Ganzheitlicher Schutz des kompletten Netzwerkes
- Lückenlose Authentifizierung mit bis zu 3 Faktoren
- 24/7 Überwachung & DTS Security Operations Center (SOC)

1. SICHERHEIT KOMMT DURCH SICHTBARKEIT

Der Leitsatz „Sicherheit kommt durch Sichtbarkeit“ gewinnt zunehmend an Bedeutung. Es ist wichtig zu wissen, welche IT-Bestandteile und Devices sich überhaupt in einem Netzwerk befinden bzw. aktiv sind. Wir ermöglichen Ihnen diesen Überblick, ebenso wie alle Assets zu klassifizieren, zu bewerten und letztendlich richtlinienbasiert zu automatisieren.

2. VOLLSTÄNDIGE ABSICHERUNG FÜR ENDGERÄTE

Im zweiten Schritt können die erkannten Devices geschützt werden. Wir sichern Ihre Endgeräte vollständig und ganzheitlich ab. Dazu zählt neben der Abwehr von bekannten Bedrohungen insbesondere der Schutz vor unbekanntem, neuartigen Angriffen. Gleichzeitig schonen wir massiv Ihre Ressourcen und ermöglichen sogar den Schutz für z. B. veraltete Betriebssysteme.

3. GANZHEITLICHER SCHUTZ DES KOMPLETTEN NETZWERKES

Gefahren können sowohl extern als auch intern bestehen. Um sich hier zu schützen, sollten alle Zugriffe von innen und außen kontrolliert werden. Zum einen sind dafür klare Regeln notwendig, wann wer mit wem über was kommuniziert. Zum anderen ist die Aufdeckung von Anomalien in der Kommunikation unerlässlich. Wir ermöglichen Ihnen abgesicherte Industrienetzwerke mit automatischer Konfiguration, benutzerorientiertem Management und ganzheitlicher Funktionalität.

4. LÜCKENLOSE AUTHENTIFIZIERUNG MIT BIS ZU 3 FAKTOREN

Selbst wenn geregelt ist, wer in das Netzwerk hineindarf, können Sie dabei alle externen Zugriffe auf Ihre IT- und Produktionssysteme überprüfen und zweifelsfrei identifizieren? Wer sagt Ihnen, dass der Zugang nicht weitergegeben wurde oder ein Notebook inkl. Zugang gestohlen wurde? Aus diesem Grund ermöglichen wir Ihnen eine lückenlose Mehr-Faktor-Authentifizierung.

5. 24/7 ÜBERWACHUNG & SECURITY OPERATIONS CENTER (SOC)

Trotz diverser Schutzmaßnahmen und einer massiven Eingrenzung des Angriffsvektors sollte zusätzlich eine permanente Überwachung der eigenen Umgebung stattfinden, um besonders zielgerichtete und komplexe Angriffe aufzudecken. Wir überwachen vollumfängliche IT-Infrastrukturen, sammeln Log-Informationen einzelner Systeme und werten diese aus, um Anomalien schnellstmöglich aufzudecken. Sobald Auffälligkeiten auftreten, leiten wir gemeinsam mit Ihnen Gegenmaßnahmen ein. Dies machen wir nicht nur maschinengestützt, sondern mit einem hochqualifizierten Security Analysten Team.

Unsere SOC-Experten sind 24/7 an 365 Tagen verfügbar. Das DTS SOC ist unsere zentrale Sicherheitsleitstelle zum Schutz Ihrer IT-Infrastruktur und Daten vor sämtlichen Bedrohungen. Es analysiert durchgehend die zu überwachenden Daten, um bei Anomalien sofort Alarm auszulösen und Schutzmechanismen einzuleiten. Darüber hinaus sind wir mit unserem eigens entwickelten DTS Monitoring in der Lage, z. B. Zustände von Sensoren zu überwachen. Das DTS Monitoring steigert Ihre Maschinenübersicht und -verfügbarkeit erheblich. Sie können jederzeit Leistungsprobleme identifizieren und beseitigen. Damit erhöhen Sie nicht nur die Lebensdauer von Produktionsanlagen, Sie können auch schneller bei produktionskritischen Ereignissen reagieren.