„Pflaster-Lösungen“ reichen nicht aus

Cyber-Resilienz für vernetzte Produktionsbetriebe

Die industrielle Produktion steht an einem digitalen Wendepunkt. Vernetzte Maschinen, automatisierte Fertigungsprozesse und intelligente IoT-Ökosysteme treiben Effizienz und Innovation voran. Parallel wächst das Risiko durch Cyber-Angriffe in einer Geschwindigkeit, die Betriebe zunehmend unter Druck setzt. Ransomware bringt ganze Produktionslinien zum Stillstand, während DDoS-Attacken Remote-Zugänge und Leitstände lahmlegen. Gleichzeitig nutzen Angreifer gezielt die Schnittstellen zwischen IT und OT, um in Systeme einzudringen, die nie für heutige Bedrohungsmodelle ausgelegt waren.

Mittelständische Produktionsbetriebe, in denen ein gewachsener Maschinenpark, Retrofit-Lösungen und knappe Personalressourcen zusammentreffen, sind besonders gefordert. Vielerorts versucht man, Risiken mit isolierten, punktuellen Sicherheitsmaßnahmen wie zusätzlichen Firewalls, neuen VPN-Tunneln oder einzelnen Monitoring-Werkzeugen zu begegnen. Doch solche „Pflaster-Lösungen“ schaffen keine nachhaltige Resilienz. Sie behandeln Symptome statt Ursachen.

Autor:
Frank Rosenberger
CEO
1&1 Versatel
www.1und1.net

Der regulatorische Rahmen

Darüber hinaus verschärft sich der regulatorische Rahmen deutlich. Vorgaben wie die NIS-2-Richtlinie mit den überarbeiteten KRITIS-Anforderungen beziehen inzwischen weit größere Teile des Mittelstands ein als bisher. Viele Produktionsbetriebe, die sich früher außerhalb solcher Regulierungen wähnten, gelten nun als „wichtige Einrichtungen“ und müssen entsprechend umfassende Sicherheitsauflagen erfüllen. Für Unternehmen, die direkt oder indirekt Teil kritischer Versorgungsketten sind, wächst damit die Verantwortung erheblich. Sicherheit darf nicht länger als ergänzender Zusatz verstanden werden, sondern muss zum tragenden Bestandteil der gesamten Infrastruktur werden.

Der Weg zu echter Cyber-Resilienz erfordert ein Umdenken hin zu einer integrierten, ganzheitlichen Netzwerkinfrastruktur, die Sicherheit als Fundament verankert.

Glasfaser als Fundament industrieller Resilienz

Die physische Netzwerkinfrastruktur hat sich längst zu einem strategischen Sicherheitsfaktor entwickelt. Sie ist entscheidend dafür, wie zuverlässig, belastbar und zukunftsfähig digitale Produktionssysteme arbeiten können. Für vernetzte Fertigungsumgebungen bietet eine leistungsstarke Glasfaseranbindung Vorteile, die weit über reine Performance-Kennzahlen hinausgehen: Sie ist nahezu immun gegen elektromagnetische Störungen, äußerst schwer abzuhören und macht Manipulationsversuche deutlich schneller erkennbar als kupferbasierte Leitungen.

Niedrige Latenzzeiten

Gleichzeitig ermöglicht sie extrem niedrige Latenzzeiten – ein großer Vorteil für zeit- und sicherheitsrelevante industrielle Anwendungen. Steuerung in der Robotik, KI-gestützte Inline-Qualitätsprüfungen, Edge-Analytics oder automatisierte Produktionsentscheidungen: All diese Prozesse benötigen stetige Datenströme in Echtzeit. Dasselbe gilt für moderne Sicherheitsarchitekturen, in denen Datenverkehr kontinuierlich analysiert und kontextbasiert verifiziert wird. Da immer mehr Threat-Detection-, Verhaltensanalyse- und Policy-Entscheidungen in die Cloud verlagert werden, wird eine stabile, unterbrechungsfreie Verbindung zur Grundvoraussetzung, damit die Sicherheit selbst nicht zum Flaschenhals wird.

Schäden nehmen zu

Laut einer aktueller Bitkom-Studie hatte im vergangenen Jahr bereits jedes vierte Unternehmen Schaden durch DDoS-Attacken zu verzeichnen. Dabei überfluten die Angreifer Systeme oder Netzwerkschnittstellen mit massenhaft künstlichen Anfragen, bis legitimer Datenverkehr nicht mehr durchkommt. Während früher die meisten OT-Geräte durch Air-Gapping geschützt waren, also durch eine physische Abschottung des Geräts von externen Netzwerken, lässt sich mittlerweile eine zunehmende Konvergenz von IT- und OT-Systemen beobachten. Oft sind diese über die gleiche LAN-Infrastruktur ohne aktuelle Sicherheitspatches miteinander verbunden. Moderne Industrieumgebungen erfordern daher Sicherheitsmaßnahmen für operative Technologien, die IT wie auch OT gleichzeitig abschirmen.

DDoS-Angriffe

treffen in verstärktem Maße auch die vorgelagerten, internetabhängigen Dienste, auf die sich Produktionsbetriebe zunehmend verlassen, wie cloudbasierte MES- (Manufacturing Execution Systems) und ERP-Systeme (Enterprise Resource Planning). Eine robuste, georedundante Glasfaseranbindung in Verbindung mit adaptiertem DDoS-Schutz reduziert die Angriffsfläche, stabilisiert die standortübergreifende Kommunikation und trägt dazu bei, dass volumetrische Angriffe kritische Prozesse nicht so leicht ausbremsen können.

Von Insellösungen zu integrierter Security

Auf diesem Fundament entwickeln sich moderne Sicherheitsarchitekturen weg von isolierten Einzelmaßnahmen hin zu integrierten, dynamischen Ansätzen. SASE (Secure Access Service Edge) vereint Netzwerksteuerung und Sicherheitsfunktionen in einer zentral orchestrierten Architektur und sorgt für konsistente Richtlinien über Standorte, Werke und Lieferketten hinweg. Für Produktionsbetriebe bedeutet das

Das Testlabor von 1&1 Versatel in Essen

zum Beispiel, dass externe Techniker oder Servicepartner nur strikt kontrollierte, zeitlich begrenzte und vollständig nachvollziehbare Zugriffe erhalten.

Software-Defined Wide Area Network

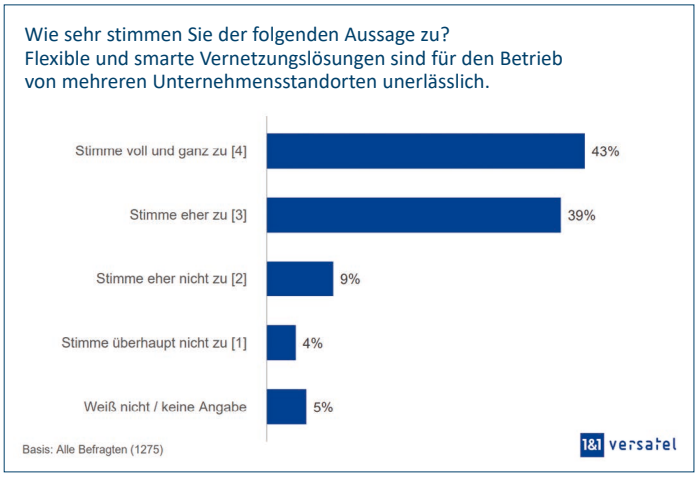
Ein entscheidender Baustein dabei ist SDWAN (Software-Defined Wide Area Network). SD-WAN steuert den Datenverkehr intelligent und passt die Routen dynamisch an die aktuelle Netzsituation über mehrere Standorte hinweg an. Dabei können Datenströme über verschiedene Leitungen – etwa Glasfaser, MPLS oder Mobilfunk – effizient verteilt werden. Produktionsunternehmen profitieren dadurch in mehrfacher Hinsicht: Daten von MES-, ERP- oder weiteren OT-Cloud-Systemen können priorisiert und mit garantierter Bandbreite übertragen werden, Remote-Wartungen bleiben zuverlässig erreichbar, und Netzwerkunterbrechungen wirken sich deutlich geringer auf kritische Fertigungsprozesse aus.

SASE kombiniert diese SD-WAN-Funktionalität mit cloudbasierten Sicherheitsdiensten wie Firewall-as-a-Service, Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) und Zero Trust Network Access (ZTNA). Sicherheitsrichtlinien werden kontextabhängig genau dort durchgesetzt, wo sich Nutzer, Geräte oder Anwendungen befinden – am Netzwerkrand. Faktoren wie Identität, Standort, Zeitpunkt oder Gerätezustand fließen in Echtzeit ein. Das Ergebnis ist eine skalierbare, flexible und standortunabhängige Sicherheitsarchitektur, die insbesondere hybride Arbeitsmodelle und Cloud-first-Strategien unterstützt.

Containerisierte, modulare Komponenten

Parallel zur konzeptionellen Weiterentwicklung verändert sich auch die technische Umsetzung. Moderne Security-Architekturen setzen zunehmend auf containerisierte, modulare Komponenten, die flexibel in Edge- oder Cloud-Umgebungen bereitgestellt werden können. Container ermöglichen es, Sicherheitsfunktionen unabhängig voneinander auszurollen, zu aktualisieren und zu skalieren, ohne bestehende Produktionsprozesse zu stören. Offene Standards und API-basierte Orchestrierung ermöglichen eine herstellerübergreifende Interoperabilität – ein entscheidender Vorteil für Industrieunternehmen, in denen gewachsene Anlagen, proprietäre Systeme und moderne Plattformen nebeneinander bestehen. Durch diese Modularität lassen sich Sicherheitsfunktionen genau dort implementieren, wo sie den größten Effekt entfalten: direkt an Maschineninseln, in der Edge-IT oder in zentralen Cloud-Gateways.

Sicherheit auf allen Ebenen mit Glasfaser als Fundament



Vernetzungslösungen als Schlüsselfaktor für den Betrieb von Unternehmensstandorten / Umfrageergebnisse

Sicherheit aus Expertenhand

In einer Zeit, in der Fachkräfte fehlen, Bedrohungslagen immer dynamischer werden und regulatorische Anforderungen spürbar steigen, fällt es vielen produzierenden Unternehmen, insbesondere im Mittelstand, zunehmend schwer, ein hohes Sicherheitsniveau eigenständig aufzubauen und dauerhaft zu halten. Managed Security Services (MSS) übernehmen in diesem Umfeld eine zentrale Rolle. In Verbindung mit einer modernen, glasfaserbasierten Netzwerkinfrastruktur bilden sie das Fundament nachhaltiger Cyber-Resilienz. Während Glasfaser stabile, latenzarme und abhörsichere Verbindungen bereitstellt, liefern MSS-Anbieter das nötige Expertenwissen, um Sicherheitsrichtlinien konsequent durchzusetzen und Sicherheitsvorfälle effizient zu bewältigen.

Der richtige Dienstleister

Die Wahl des richtigen Dienstleisters ist von zentraler Bedeutung. Neben Erfahrung, technologischer Reife, Qualifikationen und einem transparenten Preis-Leistungs-Verhältnis sollten Unternehmen besonders auf ein ganzheitliches Sicherheitsverständnis achten. Leistungsfähige MSS-Partner betreiben in der Regel ein eigenes Security Operations Center (SOC), das rund um die Uhr industrielle Angriffsflächen überwacht, OT-spezifische Threat Intelligence integriert und Anomalien in Echtzeit analysiert. So können sie ein breites Leistungsspektrum abdecken – von Firewall-Management über Intrusion Detection bis hin zu Schwachstellenmanagement und Compliance-Beratung.

OT-Expertise

Für produzierende Betriebe ist insbesondere die OT-Expertise entscheidend, da industrielle Protokolle und Normen andere Sicherheitsansätze erfordern als klassische IT-Systeme. Ebenso sollten Unternehmen darauf achten, mit ISO-zertifizierten Partnern zusammenzuarbeiten, da diese nachweislich etablierte Qualitäts- und Sicherheitsstandards einhalten und somit ein höheres Maß an Verlässlichkeit und Compliance gewährleisten.

Gleichzeitig gewinnen Aspekte wie digitale Souveränität und „Made in Germany“ beim Outsourcing von Security-Services zunehmend an Bedeutung. Entscheidend bleibt jedoch, dass Sicherheitsdienste passgenau in bestehende IT- und OT-Landschaften integriert werden. Nur wenn Security, Netzwerkarchitektur und Betriebsanforderungen eng ineinandergreifen, entsteht eine skalierbare, belastbare und regulatorisch konforme Sicherheitsarchitektur, die mit dem Unternehmen wächst.

Wer schreibt:

Frank Rosenberger ist seit Januar 2024 CEO von 1&1 Versatel, dem führenden Glasfaser-Spezialisten für Firmenkunden in Deutschland. Seine Leidenschaft für IT, Digitale Transformation und Cyber-Sicherheit treibt ihn an, Unternehmen mit sicheren und innovativen Lösungen in eine erfolgreiche digitale Zukunft zu führen. ◄