



Asset Management in der vernetzen Produktion

*Transparenz, Sicherheit und Effizienz
für IT- und OT-Assets*

Inhalt

1 Aktuelle Herausforderungen in der Produktion	03
2 Asset Management im Produktionsumfeld	04
2.1 Vernetzung mit Unified Endpoint Management	04
2.2 Die Vorteile eines einheitlichen Managementsystems	05
2.3 Mehr Überblick: Discovery – automatisierbar & manuell	07
2.4 Daten anreichern – Inventarisierung	07
2.5 UEM in die Produktion implementieren	08
2.6 Einfache Automatisierungslösungen	08
2.7 Mobile Endgeräte einfach verwalten	09
3 IT-Sicherheit in Produktionsprozessen	11
3.1 Risikomanagement	11
3.2 Cybersicherheit	12
3.3 Wichtige Infos zur NIS2-Regulierung und ihren Anforderungen	14
4 Wie die effiziente Produktion im digitalen Wandel gelingt	15

© 2026 baramundi software GmbH | Aussagen über Ausstattung und technische Funktionalitäten sind unverbindlich und dienen nur der Information. Änderungen vorbehalten.



1 Aktuelle Herausforderungen in der Produktion

Wir befinden uns inmitten der vierten industriellen Revolution. Mit dem Einzug von Industrie 4.0 ist die Digitalisierung im Produktionsumfeld von Unternehmen immer relevanter geworden – insbesondere mit Blick auf das Asset Management. Assets sind in diesem Zusammenhang alle Ressourcen eines Unternehmens, die für den wirtschaftlichen Erfolg relevant sind. Im Produktionsumfeld zählen dazu neben Maschinen auch vernetzte Endgeräte und Systeme – von Windows- und Linux-Geräten über mobile Endgeräte bis hin zu Netzwerkkomponenten. Sie kommen auf unterschiedlichen Ebenen der Produktion zum Einsatz – von der Kontroll- über die Steuerungs- bis hin zur Feldebene.

Industrie 4.0 trifft auf OT

Eine der größten Herausforderungen beim Umsetzen des **Industrie 4.0** Konzepts sind die gewachsenen Strukturen, die vielerorts ohne Standardisierung in der **OT (Operational Technology)** entstanden sind. Damit einher geht die Notwendigkeit, vorhandene Assets in der Produktion manuell zu verwalten. Unterschiedliche Fachbereiche, wie Anlagenbau, Instandhaltung oder IT-Spezialisten, kümmern sich nur um einzelne Aspekte. Diese oft komplizierten Einzellösungen anstelle einfacher und übergreifender Systeme machen die Verwaltung sehr komplex und unübersichtlich. Verantwortlichkeiten sind verteilt und nicht immer klar definiert. Das führt im Falle einer Störung zu unnötigem Zeitverlust im Wiederanlauf einer Anlage.

Ebenso ist die Gefährdung der Verfügbarkeit ein Thema: Viele Firmen stellen kritische Sicherheitslücken fest, die Angriffspunkte für Cyberattacken darstellen können. Um auf der Höhe der Zeit zu bleiben, empfiehlt sich ein stärkerer Fokus auf die Digitalisierung von Prozessen. Das Ziel sollte sein, vorhandene und vernetzte Strukturen weiter auszubauen. Dazu bedarf es einer abgestimmten Zusammenarbeit der IT mit den Fachabteilungen der Produktion bzw. der OT-Organisation. So wird es Unternehmen möglich, eine Effizienzsteigerung entlang der Wertschöpfungskette zu erreichen und flexibel auf Marktveränderungen zu reagieren.

Industrie 4.0

Industrie 4.0 ist die Bezeichnung für ein Konzept zur umfassenden Digitalisierung der industriellen Produktion. Im Kern geht es darum, die industrielle Produktion mit moderner Informations- und Kommunikationstechnik zu verzahnen mithilfe intelligenter und digital vernetzter Systeme. Durch die Vernetzung soll es möglich werden, nicht mehr nur einen Produktionsschritt, sondern eine ganze Wertschöpfungskette zu optimieren und weitere Effizienzgewinne zu realisieren.

Operational Technology

Operational Technology (OT) beschreibt die Verwendung von Hard- und Software zur Steuerung von industriellem Equipment. OT stellt dabei eine Abgrenzung zur klassischen IT dar. OT-Systeme kommen zumeist in Produktionsumgebungen zum Einsatz. Viele Aspekte von OT und IT überschneiden sich, da OT-Systeme in der Regel mit Netzwerken verbunden sind und immer größere Datenmengen generieren und verwenden.

2 Asset Management im Produktionsumfeld

Das Asset Management hat einen starken Einfluss auf Instandhaltungsprozesse, die Verfügbarkeit von Maschinen und letztendlich auch auf die Fertigungskosten. Ein transparenter Überblick über installierte Systeme und aktuelle Informationen zu den Assets ist eine Grundvoraussetzung, um die Leistungsfähigkeit und Stabilität der Systeme sicherzustellen und steigern zu können. Dazu zählen unter anderem Industrie PCs, Maschinensteuerungen oder Netzwerkinfrastrukturgeräte wie Switches, weitere Steuerungen, Raspberry Pies oder Router. Auch mobile Assets wie Hand und IIoT-Geräte spielen eine immer größere Rolle, wenn es darum geht, die Produktion am Laufen zu halten.

2.1 Vernetzung mit Unified Endpoint Management

Unified Endpoint Management (UEM) beschreibt die einheitliche Verwaltung von Assets mithilfe einer einzigen maßgeschneiderten Software. Damit ist es möglich, einen transparenten Gesamtüberblick über alle Elemente in einem Netzwerk zu erhalten und IT-Routineaufgaben, wo möglich, zu automatisieren. UEM ermöglicht es innerhalb einer Datenbank, alle Assets auf einer gemeinsamen Oberfläche zu erfassen. Neue Geräte und Software können automatisch erkannt und verwaltet werden. Mithilfe dieser zentralen Managementlösung ist es außerdem möglich, die IT-Sicherheit in der Produktion zu erhöhen.



Chancen und Herausforderungen der vernetzten Produktion

Ein Überblick über die grundlegenden Aufgaben einer zentralen UEM-Lösung:

- Erkennung von Geräten im Netzwerk
- Inventarisierung von Hardware und Software
- Verwaltung von Windows-, Linux-, macOS-, Android- und iOS-Geräten
- Aufdecken von Schwachstellen und Risiken
- Automatisierung alltäglicher IT-Aufgaben
- Datensicherheit und Compliance-Unterstützung
- Verwaltung mobiler Endgeräte
- Software-, Patch- und Update-Management
- Reporting und Nachvollziehbarkeit von Veränderungen

Sei es die zentrale Aktualisierung bei erstmaliger Inbetriebnahme, die Verteilung von Software oder die Überprüfung auf Schwachstellen hinsichtlich Sicherheits- und Compliance-Richtlinien. Der Einsatz spart den einzelnen Fachbereichen wertvolle Zeit und setzt Ressourcen für andere Aufgaben frei.

2.2 Die Vorteile eines einheitlichen Managementsystems

Durch die zentrale Bündelung des Asset Managements vereinfacht sich die Organisation aller involvierten Geräte.

Einheitliche Datenbasis für die Assets in der Produktion

Trotz steigender Komplexität in der Produktion, einer höheren Anzahl an Geräten und vielfältiger Software ist es mit einer UEM-Lösung möglich, mit nur wenigen Klicks alle Assets transparent zu überblicken und ihre Eigenschaften festzustellen. Selbst die besten IT-Mitarbeiter können sich in größeren, produzierenden Unternehmen nicht alle einzelnen Systemversionen, Wartungstermine, erforderlichen Updates und Gerätetypen merken. Updates müssen oftmals für alle Asset-Typen manuell zugewiesen werden – die manuelle Dokumentation inklusive. Das kostet Zeit, bindet Personal und verkompliziert Abläufe. Mit UEM finden die Kontrollen automatisiert statt. Damit kann die komplette Unternehmenssoftware durchgehend auf dem neuesten Stand gehalten werden.

Der schnelle, vollständige Überblick über die Assets in der Produktion per UEM erleichtert regelmäßige Wartungen und präventives Eingreifen. Plötzliche und teure Ausfälle essenzieller Produktionselemente können somit verhindert werden, bevor sie eintreten.

„Der schnelle, vollständige Überblick über die Assets in der Produktion per UEM erleichtert regelmäßige Wartungen und präventives Eingreifen.“

Digitale Sicherheit erhöhen

Wenn Software veraltet, fällt dies oft erst auf, wenn Inkompatibilität mit neueren Systemen auftritt. Dabei stellt veraltete Software jedoch schon vorher eine konkrete Gefahr für die Verfügbarkeit der Produktion dar. Es gilt der Grundsatz: Je weniger aktuell, desto angreifbarer für Cyberattacken und Datendiebstahl ist ein System. Der bedeutende Vorteil einer UEM-Lösung liegt in der zentralen Erfassung der Assets. Da nicht mehr jedes Asset einzeln registriert und verwaltet werden muss, ist die gesamte IT-Sicherheit einfacher handhabbar. Mögliche Sicherheitslücken können schneller aufgespürt werden. Zudem lassen sich dank des verbesserten Überblicks geplante Wartungsfenster leichter nutzen, um Betriebssysteme und Software auf einem sicheren Stand zu halten. Die jeweiligen Anwendungen sind somit resistenter gegen Angriffe. Mit dem entsprechenden Element lassen sich auch wenig oder gar nicht genutzte Anwendungen aufspüren. Deren Deinstallation stört den Arbeitsfluss nicht, reduziert aber den Wartungsaufwand und verbessert die allgemeine Systemsicherheit.

Einsparpotenziale entdecken

In Zeiten politischer Krisen, steigender Energiepreise und höherer Produktionskosten müssen Unternehmen die ein oder andere Einsparung vornehmen. Mithilfe eines einheitlichen Managementsystems lassen sich zeitraubende Routineaufgaben automatisieren. Ressourcen, die vorher für die händische Konfigurationen, das Führen von Excel-Tabellen oder manuelle Dokumentationen eingesetzt wurden, können an anderer und relevanterer Stelle eingesetzt werden. Mithilfe des Überblicks und der regelmäßigen Kontrolle aller Assets wird die Lebensdauer maximal ausgeschöpft. Unnötige Anschaffungen, die auf Basis einer mangelnden Übersicht getätigt wurden, werden vermieden. Dazu zählen unnötige Lizenzen oder redundante Endgeräte. Zudem gelingt mit einer aktuellen Datenbasis die Beseitigung von Störungen im Regelfall schneller und reduziert Ausfallzeiten. Langfristig sparen Unternehmen dadurch bares Geld.

„Die Erfahrung zeigt, dass händische Eingaben eine der größten Fehlerquellen sind.“

Potenzielle Fehlerquellen ausschalten

Wer die Analyse seiner Assets manuell durchführt, nimmt in Kauf, dass beim Eintragen wichtiger Daten und der Konfiguration von Einstellungen Fehler entstehen. Fehler, die aus falschen oder veralteten Daten und Einstellungen entstehen, verursachen oft erheblichen Zeit- und Personalaufwand. Diese Probleme kann ein einheitlich verwendetes Managementsystem unterbinden. Auch ein professionelles Risikomanagement ist nur auf Basis von aktuellen Daten sinnvoll. Eine automatisierte und aktuelle Übersicht über alle Assets liefert die geforderten Informationen und kann mögliche Schwachstellen aufdecken und dadurch Risiken grundlegend minimieren.

2.3 Mehr Überblick: Discovery – automatisierbar & manuell

Für einen Überblick zu den gesamten Assets sind verschiedene Discovery-Ansätze essenziell. Sie dienen als Grundlage für die Inventarisierung aller Komponenten. Vielerorts erfolgt die Erfassung von Assets im Produktionsumfeld noch immer manuell. Teilweise werden sie in einer Excel-Tabelle oder einer vergleichbaren Software aufgelistet.

Integrierte Discovery-Funktionen unterstützen dabei, aktive Geräte im Netzwerk automatisiert zu erkennen und zu erfassen. Über definierte Netzwerkbereiche, Zeitpläne und geeignete Protokolle lassen sich Discovery-Prozesse flexibel an die jeweilige Produktionsumgebung anpassen. Dadurch entsteht ein aktueller Überblick über inventarisierbare Systeme und deren Einbindung in die Infrastruktur. Offline-Assets können manuell angelegt und in die Verwaltung mit aufgenommen werden. Ebenso lassen sich Informationen zu den Assets aus anderen Datenbanken über die vorhandene Standardschnittstelle importieren.

2.4 Daten anreichern – Inventarisierung

Für das Unternehmen ist es wichtig zu wissen, welche Hard- und Software in Verwendung und welche Lizenzen dafür erforderlich sind. Die automatisierte Inventur zeigt an, welche Hard- und Software vorliegt. Über Discovery-Funktionen lassen sich aktive Geräte im Netzwerk erkennen und die Ergebnisse zentral auswerten. So entsteht ein aktueller Überblick über inventarisierbare Systeme und deren Einbindung in die Infrastruktur.

Auch Linux-basierte Systeme lassen sich in die Inventarisierung einbeziehen. Dadurch erhalten Unternehmen zusätzliche Transparenz über produktionsnahe Geräte, Industrie-PCs oder andere Linux-basierte Systeme. Je nach eingesetzter Distribution können außerdem Paket-Updates geprüft und kompatible Pakete gesammelt aktualisiert werden; eigene Skripte lassen sich zentral ausführen und die Ergebnisse in der Konsole nachvollziehen.

Individuell definierbare Variablen und Schwellwerte ermöglichen es, gezielt nach relevanten Informationen zu filtern und die Verwaltbarkeit zu verbessern. So lassen sich z. B. leicht Verantwortlichkeiten oder Kostenstellen abbilden. Auf Basis dieser Auswertungen ist es dann der jeweiligen Fachabteilung möglich, strategische Entscheidungen zu treffen.

Damit bildet die Inventarisierung die Basis für fundiertes Reporting und erlaubt die Priorisierung von kritischen Aufgaben, wie Wartung und Instandhaltung. Innerhalb der Asset-Datenbank können außerdem alle Komponenten über ihre gesamte Lebensdauer im Blick behalten werden. Im Hinblick auf Compliance-Regelungen ist damit auch ein einfacher Abgleich des Soll- und Ist-Zustands möglich.

2.5 UEM in die Produktion implementieren

Wenn sich ein Unternehmen eine UEM Software anschafft, ist es entscheidend, dass diese tatsächlich die Arbeit erleichtert. Darüber hinaus sollte eine Managementsoftware über moderne Schnittstellen verfügen, um die Implementierung in das Gesamtkonzept so gründlich wie möglich zu gestalten. Ob Lagerwesen, Materialversorgung, Fertigung, Abtransport oder Kundenservice – eine ausgeklügelte UEM Software sollte in der Lage sein, alle am Prozess beteiligten Endgeräte von Beginn an mit einzubeziehen.

Mit der baramundi Management Suite können die notwendigen Geräte und Tools entlang der gesamten Supply Chain nahtlos inventarisiert und verwaltet werden. Damit bildet UEM keine separate Insel der Infrastruktur, sondern wird automatisch zu einem zentralen Knotenpunkt in der Produktion. Viele Bestandteile – etwa Industrie-PCs, mobile Endgeräte, Linux-basierte Systeme und Netzwerkkomponenten – können zentral inventarisiert und verwaltet werden. Produktionsnahe Komponenten und Maschinensteuerungen lassen sich je nach Erreichbarkeit, Gerätetyp und Protokoll über Discovery- und Inventarisierungsfunktionen sichtbar machen.

2.6 Einfache Automatisierungslösungen

Speziell bei Routineaufgaben bietet sich die Automatisierung wiederkehrender Prozesse an. Das betrifft zum Beispiel Wartungsarbeiten, Updates, Softwareinstallationen, Betriebssysteminstallationen in unterstützten Szenarien sowie das regelmäßige Scannen auf Schwachstellen. Für produzierende Unternehmen ist es enorm wichtig, Störungen zu vermeiden, Stillstände auf ein Minimum zu reduzieren und Maschinen optimal auszulasten. Hierfür eignet sich besonders die Automatisierung wiederkehrender Wartungsaufgaben. Das unterstützt den reibungslosen Ablauf in der Produktion. Mit der Management Suite lassen sich Wartungsfenster gezielt nutzen und wiederkehrende Aufgaben automatisiert ausführen. Zusätzlich entlastet die Automatisierung die IT- bzw. OT-Administration. Durch diese Automatisierungslösung ist es möglich, deutlich schneller auf anfallende Probleme zu reagieren, neue Einstellungen vorzunehmen und Freiraum für andere relevante Aufgabenbereiche zu schaffen.

Eine weitere Entlastung kann ein Self-Service-Kiosk bieten. Dort können grundlegende Installationen bereitgestellt und Standardanfragen ohne großen Aufwand beantwortet werden. Die IT-Administration kann lizenzierte Programme und Updates so aufbereiten, dass sie für jeden Anwender intuitiv nutzbar sind. Bei bestimmten Programmen oder Komponenten vergeben die Administratoren die Rechte nur an relevante Produktionsmitarbeiter, damit diese einen schnellen Zugriff erhalten.

2.7 Mobile Endgeräte einfach verwalten

Insbesondere im Produktionsumfeld stehen Unternehmen vor der großen Herausforderung, den Überblick über alle mobilen Endgeräte zu behalten, die Mitarbeiter teilweise auch in ihrem privaten Umfeld einsetzen. Doch wie kann eine technisch einwandfreie Integration und ein sicherer Zugriff außerhalb des Unternehmensnetzwerks gelingen? Mithilfe einer professionellen UEM Software lassen sich Smartphones, industrielle Handhelds und Tablets sicher in das Asset-Inventar integrieren.

Ob iOS oder Android – besonders unter dem Einsatz verschiedener mobiler Betriebssysteme können Unternehmen mit der baramundi Management Suite viel Zeit sparen. Denn sie ist in der Lage, alle Geräte zu erfassen und zu integrieren. Die Einrichtung muss nicht mehr umständlich über verschiedene Eingabemasken vorgenommen werden. So kann ein neues mobiles Endgerät beispielsweise per QR-Code in das plattformübergreifende System aufgenommen werden. Die Steuerung erfolgt zentral über das Dashboard der UEM-Lösung und kann ortsunabhängig vorgenommen werden. Übrigens: Unternehmen, die auf eine solche zentrale Software zurückgreifen, sparen nicht nur Zeit und Ressourcen, sondern reduzieren auch das Fehlerrisiko – Stichwort: Compliance. Denn in einer ausgefeilten UEM-Lösung können Compliance-Regeln direkt definiert und kontrolliert werden. Verstöße gegen die festgelegten Compliance-Richtlinien sendet die Software direkt an die Administration.



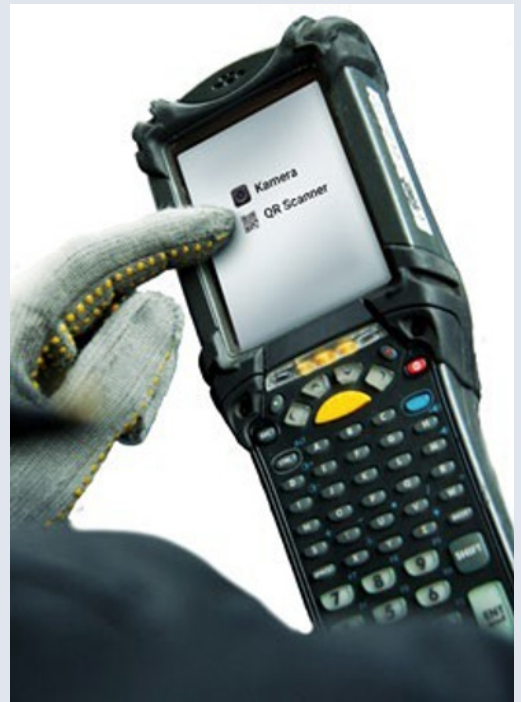
Aufnahme ins Management per QR-Code

Die zentrale Verwaltung wird zusätzlich durch moderne Support-Möglichkeiten ergänzt. So können mobile Endgeräte bei Bedarf per Remote-Support unterstützt werden, ohne dass Administratoren physisch vor Ort sein müssen. Die UEM-Software schützt die mobilen Endgeräte ebenfalls bei Diebstahl oder sonstigem Verlust. Maßnahmen sind etwa automatisierte Sperren, das Löschen von Zugängen „Over-The-Air“ und die Generierung starker Passwörter. Umfassende Schutzmaßnahmen erschweren bei einem Verlust einen möglichen Datendiebstahl. Außerdem können Administratoren Mobilgeräte aus der Entfernung vom System abkoppeln und Zugriffsrechte zurücknehmen.

Um alle verwendeten Endgeräte vor unseriösen Apps und Programmen zu schützen, kann der Administrator Block- oder Allow-Listen anlegen. Damit werden unseriöse Anbieter von Beginn an ausgeschlossen und Malware der Zugang stark erschwert.

Erwähnenswert ist hier insbesondere der Einsatz von Corporate Owned Single Use Geräten (COSU). Diese Geräte sind in ihrer Funktionalität auf einen Einsatzzweck abgestimmt und können nach Maßgabe des Administrators nur eine App oder eine definierte Liste von Apps ausführen. Beispiele dafür sind mobile Barcode Scanner – sowohl bei der Auslieferung als auch in der Lagerlogistik, oder Maschinenbediener Tablets für BDE/MDE-Zwecke (Betriebsdatenerfassung und Maschinendatenerfassung).

Da diese Geräte im täglichen Einsatz frei unter verschiedenen Benutzern im Unternehmen weitergegeben werden müssen, haben diese Konfigurationen keinerlei Nutzerbezug und verlangen auch keine User-Authentifizierung. Das heißt auch, dass man das Gerät bei missbräuchlichem Verhalten keinem Anwender zuordnen kann. Dementsprechend durchdacht und restriktiv muss die Konfiguration des Geräts sein, um Risiken für das Unternehmensnetzwerk zu minimieren.



Zweckbestimmte Geräte im Management

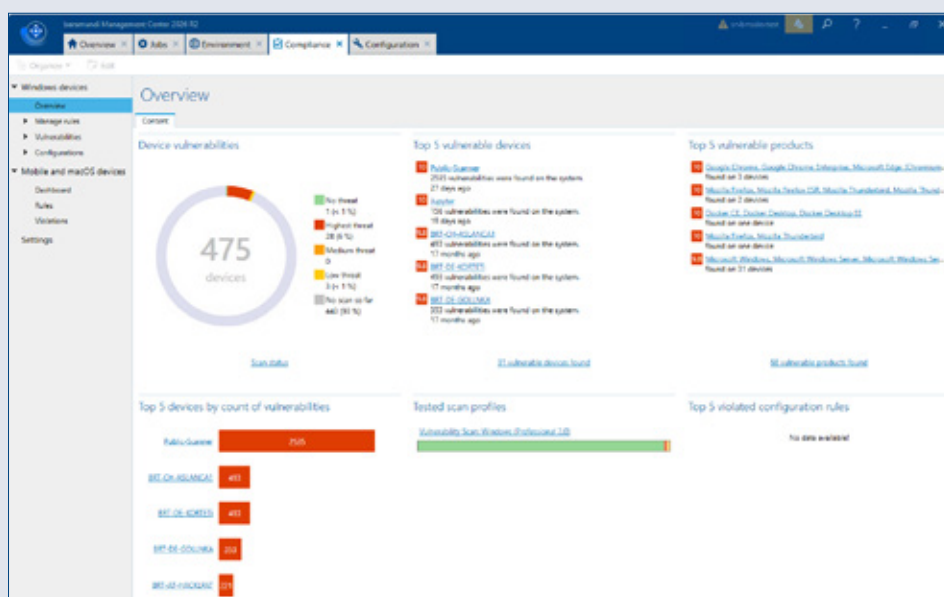
Mit der **baramundi Management Suite** ist es zusätzlich möglich, die aktuellen Zustände von Hardware und Software der einzelnen mobilen Endgeräte zu erfassen. Sollten Updates, Sicherheits-Patches oder neue Installationen erforderlich sein, kann der Administrator die jeweiligen Anwendungen einheitlich auf allen Geräten verteilen. Damit wird der aktuelle Betrieb problemlos aufrechterhalten. Die Fehleranfälligkeit im gesamten Produktionsumfeld sinkt. Gleichzeitig kann das Unternehmen ein EU-DSGVO konformes Arbeiten sicherstellen und aufkommende Sicherheitslücken jederzeit schließen.

3 IT-Sicherheit in Produktionsprozessen

Die Fertigungsindustrie ist weltweit seit mehreren Jahren in Folge die am häufigsten von Cyberangriffen betroffene Branche. Besonders Ransomware-Angriffe treten hier gehäuft auf und führen immer wieder zur Unterbrechung von Lieferketten¹. Industrie 4.0 erfordert daher zunehmende Sicherheitsvorkehrungen entlang der gesamten Wertschöpfungskette. Eine ausgeklügelte IT-Sicherheit schützt hier zeitgleich vor Produktionsausfällen und Datendiebstahl. Doch wie kann es bei dem Einsatz zahlreicher Geräte und Software gelingen, produzierende Unternehmen umfassend vor Angriffen abzusichern und die Risiken auf ein Minimum zu reduzieren?

3.1 Risikomanagement

Zum Risikomanagement gehören die Identifikation, Analyse und Bewertung vorhandener Schwachstellen sowie die Reaktion auf Veränderungen. Dazu ist es notwendig, dass jederzeit korrekte Daten und Informationen vorhanden sind. Verantwortliche des Risikomanagements sollten aus diesen Analysen Rückschlüsse ziehen und Notfallpläne für verschiedene Szenarien bereithalten. Maßnahmen gegen eventuelle Ausfälle, wie zum Beispiel die Erstellung umfassender Backup-Systeme, sollten frühzeitig vorbereitet und vorgehalten werden. Mit der baramundi Management Suite behalten produzierende Unternehmen alle Assets im Überblick und können schnell mit passenden Maßnahmen auf eventuelle Störfälle reagieren.



Compliance Dashboard zur Unterstützung des Risikomanagements

Zu möglichen Risiken zählen: Ausfälle der Hardware, Software-Fehler, Datendiebstahl bzw. Ransomware Angriffe oder anders gelagerter Datenverlust. Eine professionelle UEM-Lösung bietet eine Reihe von notwendigen Schutzmaßnahmen. Sie ist in der Lage, Sicherheitslücken frühzeitig zu melden und sichtbar zu machen. Sie erhöht den Datenschutz, hilft Zugriffe von unberechtigten Dritten zu verhindern und minimiert die Risiken, die mit dem zusätzlichen Einsatz mobiler Endgeräte einhergehen.

1 IBM Security, X-Force Threat Intelligence Index, 2026

3.2 Cybersicherheit

Im Produktionsumfeld kommt es immer wieder vor, dass Unternehmen zwar einzelne Schutzmaßnahmen im Rahmen der Cybersecurity durchführen, sich aber nicht konsequent an ein ganzheitliches Sicherheitskonzept halten. Dabei bietet eine zunehmend vernetzte Produktionsinfrastruktur viel Angriffsfläche für Cyberattacken, zum Beispiel in Form von Ransomware. Vor allem Maschinen mit Fernzugriff und veraltete Betriebssysteme können ein leichtes Ziel für Angreifer sein.

Defense in Depth

Die „Defense in Depth“ Strategie sieht vor, mit verschiedenen voneinander unabhängigen, organisatorischen Schutzmaßnahmen die Infrastruktur der vernetzten Produktion zu schützen.

Die Grundlage dafür sind Informationssicherheitsrichtlinien. Diese beziehen die jeweilige Geschäftsstrategie ein und stellen sicher, dass sich alle Beteiligten sowohl an die Sicherheitsstandards als auch an die gesetzlichen Vorgaben halten.

Kontinuierliche Mitarbeiterschulung

Die besten Technologien bringen wenig, wenn sie nicht richtig zur Anwendung kommen. Es müssen Rollen und Aufgabenbereiche genau definiert bzw. verteilt werden. Hier sind die Führungskräfte gefragt, um zusammen mit OT-Verantwortlichen und der IT-Abteilung die bestmögliche Absicherung für den Produktionsbereich zu finden. So müssen etwa Mitarbeiter der Produktion in puncto Cybersicherheit sensibilisiert und mit aktuellen Informationen versorgt werden. Dazu gehört, alle Angestellten regelmäßig zu schulen – zum Beispiel in Form eines Security Awareness Trainings, ausgerichtet an den Bedürfnissen der Produktion. In diesem lernen sie, wie sie richtig auf Phishing reagieren, USB-Stick-Köder vermeiden und weitere Tricks des Social Engineerings erkennen.

Segmentierung des OT-Netzwerks

Neben der Trennung des Office- vom Produktionsbereich durch eine designierte DMZ ist es zur Erhöhung des Sicherheitsniveaus wichtig, das Produktionsnetzwerk in einzelne Subnetze zu trennen. Diese Segmentierung und die damit einhergehende Beschränkung der Kommunikation kann genutzt werden, um Legacy-Systeme zu schützen, die sonst nicht oder nur schwer mit Updates versorgt werden können. Sollte es zu einem Cyberangriff kommen, ist damit nicht direkt das ganze Netzwerk betroffen, sondern lediglich einzelne, kleinere Bereiche.

Schutz der Endgeräte

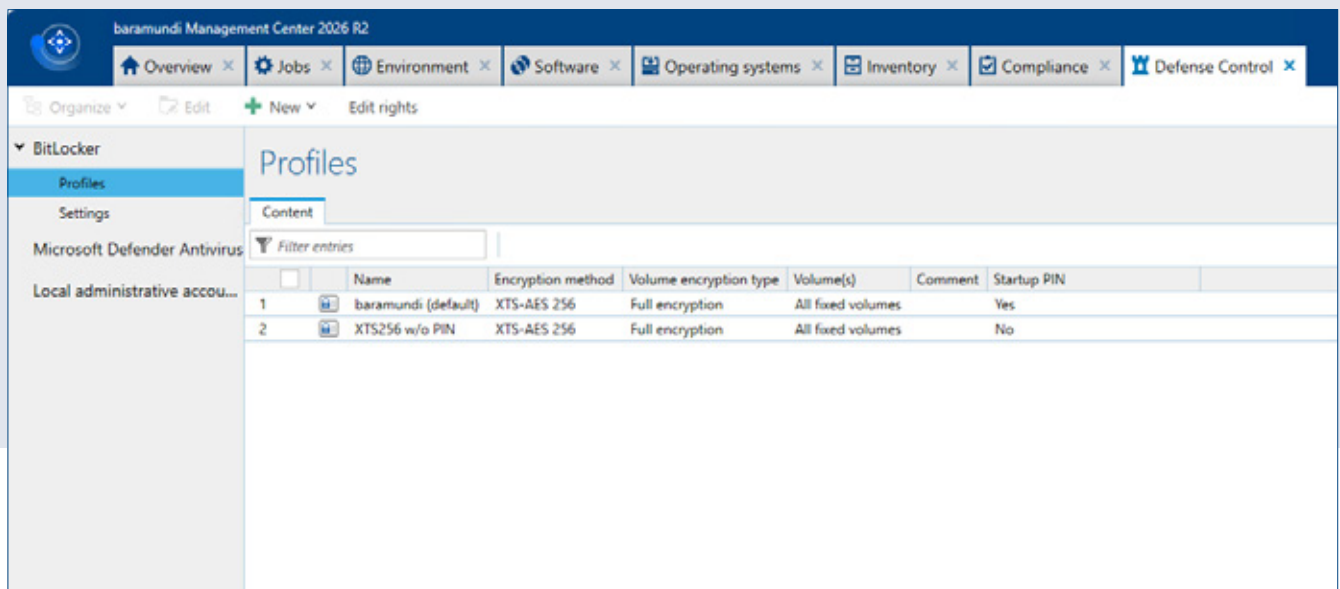
Ob Anlagen, Steuerungs- und Netzwerksysteme, IPCs oder mobile Endgeräte – Unternehmen sollten alle Bestandteile der Produktion absichern. Es ist notwendig, Betriebssysteme, Firmware und die gesamte, benötigte Software, wo es möglich ist, auf dem aktuellen Stand zu halten.

Dazu zählen professionelle Prozesse für Patch- und Update-Management, um Betriebssysteme und Anwendungen aktuell zu halten und bekannte Sicherheitslücken zeitnah zu schließen. Ergänzend helfen Schwachstellenanalysen auf unterstützten Endpunkten dabei, potenzielle Risiken frühzeitig zu erkennen und zu bewerten. Für die gesamte Cybersicherheit bieten sich außerdem „Allow Lists“ an, die für Mitarbeiter nur die Anwendung zulassen, die zuvor als vertrauenswürdig definiert wurde.

An Endgeräten finden sich zudem viele Schnittstellen, die vor unautorisiertem Zugriff geschützt werden müssen. Nicht zugelassene USB-Sticks oder andere Datenträger können schädliche Software in das firmeneigene Asset-System einschleusen und so für massive Ausfälle sorgen. Mit der baramundi Management Suite lässt sich die Hardware eines Unternehmens zuverlässig absichern. Die Komponente baramundi Device Control sorgt beispielsweise für die Kontrolle von extern angeschlossenen Datenträgern.

UEM – ein Beitrag für die IT-Sicherheit

UEM ist dadurch ein wichtiger Beitrag für die Cybersecurity im Produktionsumfeld. Eine Software wie die baramundi Management Suite sorgt dafür, dass die vernetzten Assets in der Produktion und die damit verbundene Risiken sichtbar werden: Sie hilft, diese auf dem bestmöglichen Stand zu halten und Sicherheitsmaßnahmen zuverlässig und nachvollziehbar umzusetzen.



Festplattenverschlüsselung zur Endpunktabsicherung

3.3 Wichtige Infos zur NIS2-Regulierung und ihren Anforderungen

Die NIS2-Richtlinie (Richtlinie (EU) 2022/2555) verschärft die Anforderungen an die Cybersicherheit von Unternehmen und Organisationen EU-weit. Sie wird von den einzelnen Mitgliedstaaten in nationales Recht umgesetzt und betrifft je nach Land mehrere zehntausend Unternehmen in bis zu 18 Sektoren. Die Schwellenwerte orientieren sich EU-weit an Mitarbeiterzahl und Umsatz – üblicherweise ab 50 Mitarbeitenden oder 10 Millionen Euro Jahresumsatz in einem der erfassten Sektoren. Erfasst sind neben klassischen kritischen Infrastrukturen wie Energie, Wasser oder Gesundheit ausdrücklich auch industrielle Produktion, Maschinenbau, Lebensmittelproduktion, Chemie und Logistik. Für viele produzierende Unternehmen in ganz Europa bedeutet das: Sie unterliegen möglicherweise erstmals einer gesetzlichen Cybersicherheitsregulierung.

Betroffene Unternehmen müssen sich bei der jeweiligen nationalen Aufsichtsbehörde registrieren und erhebliche Sicherheitsvorfälle gestuft melden: üblicherweise eine Frühwarnung innerhalb von 24 Stunden, ein ausführlicher Bericht innerhalb von 72 Stunden und ein Abschlussbericht innerhalb eines Monats. Zusätzlich schreibt die Richtlinie Risikomanagementmaßnahmen in zehn Kernbereichen vor, darunter Risikoanalyse, Backup-Management, Lieferkettensicherheit und Multi-Faktor-Authentifizierung. Besonders wichtige Einrichtungen müssen zudem regelmäßig nachweisen, dass die Umsetzung tatsächlich erfolgt ist.

Bei Verstößen drohen empfindliche Bußgelder – die NIS2-Richtlinie sieht als EU-weiten Rahmen bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Jahresumsatzes für besonders wichtige Einrichtungen vor; die konkrete Höhe hängt von der jeweiligen nationalen Umsetzung ab. In mehreren Mitgliedstaaten können Geschäftsführungen und Vorstände zudem persönlich haftbar gemacht werden, wenn sie notwendige Maßnahmen nicht angeordnet oder überwacht haben.

Besonders relevant für die Produktion: NIS2 erfasst ausdrücklich auch OT-Umgebungen (Operational Technology) – also Maschinensteuerungen, Industrie-PCs und Netzwerkinfrastruktur, nicht nur klassische Office-IT. Gerade hier zeigt sich häufig eine Wissenslücke, da viele OT-Komponenten auf Linux- oder anderen Embedded-Systemen statt auf Windows laufen und dadurch in klassischen IT-Sicherheitskonzepten leicht übersehen werden. Eine vollständige Inventarisierung muss deshalb beide Welten abdecken – Windows-basierte IT ebenso wie Linux- und Embedded-Systeme in der OT –, da Sicherheitslücken in beiden Bereichen gleichermaßen Angriffsflächen bieten.

Auch internationale Standards und etablierte Frameworks wie ISO 27001 oder das NIST Cybersecurity Framework können Unternehmen dabei unterstützen, die Anforderungen von NIS2 strukturiert umzusetzen. Ergänzend bieten viele nationale Behörden eigene Practice-Leitfäden und Grundsatzwerke an, die sich an den jeweiligen NIS2-Vorgaben orientieren. Unabhängig von der jeweiligen nationalen Ausgestaltung wird von Organisationen europaweit zunehmend erwartet, dass sie ihre Prozesse transparent dokumentieren, Veränderungen nachvollziehbar protokollieren und aussagekräftige Reports bereitstellen.

Je übersichtlicher und besser dokumentiert die IT- und OT-Infrastruktur entlang der Fertigungsprozesse ist, desto besser können Firmen ihre Sicherheitsmaßnahmen nachweisen und aufzeigen, dass alle Elemente bestmöglich geschützt sind. Basis für die Handhabung kritischer Komponenten in der Produktion ist eine präzise Inventarisierung. Gerade im Kontext der NIS2-Risikomanagementpflichten – etwa bei Lieferkettensicherheit oder Vorfallmeldung – schafft eine UEM-Lösung die richtige Grundlage: Sie bietet aktuelle Berichte und sorgt für die Nachvollziehbarkeit sicher eingesetzter Software sowie den Einsatz sensibler Daten in wachsenden, industriellen Netzwerken – über Windows-, Linux- und Embedded-Systeme in IT und OT hinweg.

4 Wie die effiziente Produktion im digitalen Wandel gelingt

Die großen Veränderungen und zunehmenden Regularien rund um die Digitalisierung bedeuten viele Herausforderungen für Unternehmen der Fertigungsindustrie. Sie bringen jedoch auch zahlreiche Chancen mit sich. Dazu zählen die Vereinfachung von Prozessen, eine schnellere Reaktionsfähigkeit, die individuelle Erfüllung von Kundenwünschen und der dadurch entstehende Gewinn von Wettbewerbsvorteilen. Insgesamt sorgt die Industrie 4.0 für eine höhere Effizienz in der Produktion.

Mithilfe automatisierter IT-Prozesse können industrielle Unternehmen schneller agieren und ressourceneffizienter produzieren. Das gelingt allerdings nur, wenn sich diese intern mit neuen Technologien, Organisationsformen und -prozessen auseinandersetzen. Grundlage dafür ist eine aufgeschlossene Unternehmenskultur, die sich mit diesen Veränderungen auseinandersetzt. Im Prozess der Digitalisierung sollten alle Mitarbeiter eingebunden werden. Mit fortschreitender Vernetzung ist es notwendig, kontinuierlich Schulungen anzubieten, um Awareness für IT-Security in der Produktion zu schaffen.

Eine vernetzte Produktion erfordert außerdem eine engere Zusammenarbeit zwischen den Fachabteilungen der IT- und OT-Organisation. Denn nur wenn das Know-how aus beiden Welten genutzt wird, kann eine praxisorientierte, effiziente und zugleich sichere Produktion gelingen. Unternehmen erreichen einen klaren Wettbewerbsvorteil, wenn sie zur Verwaltung ihrer Assets zentrale Lösungen wie ein Unified Endpoint Management einsetzen, um langfristig die steigende Komplexität im Griff zu behalten und die Verfügbarkeit der Produktion sicherzustellen.

Ihre Vorteile mit UEM in der vernetzten Produktion

- ✓ **Höhere Transparenz**
durch das Aufzeigen von Abhängigkeiten und der Visualisierung von Systeminformationen
- ✓ **Mehr Sicherheit**
mit Schnittstellenabsicherung, Risikoerkennung und Schwachstellenbehebung
- ✓ **Größere Effizienz**
durch die Reduzierung von manuellem Arbeitsaufwand, schnellerer Reaktion auf Probleme und der automatisierten Nutzung von Wartungsfenstern

Über die baramundi software GmbH

Die baramundi software GmbH sorgt als Spezialist für Unified Endpoint Management (baramundi Management Suite) und Proactive Endpoint Operations (baramundi Proactive Hub) dafür, dass Unternehmen und Organisationen effizient, sicher und plattformübergreifend Arbeitsumgebungen und digitale Arbeitsplätze managen – On-Prem und in der Cloud. Der Hauptsitz der baramundi software GmbH befindet sich in Augsburg. Die Produkte und Services des im Jahr 2000 gegründeten Unternehmens sind komplett Made in EU. Beim Vertrieb, der Beratung und Betreuung von Kunden arbeitet baramundi weltweit erfolgreich mit Partnerunternehmen zusammen.

www.baramundi.com



Sie möchten mehr über die baramundi Management Suite erfahren?

Melden Sie sich zum Live-Webinar an! Erleben Sie im kostenfreien Webinar, wie Sie die baramundi Management Suite Ihre Endpoints, Server und Mobilgeräte automatisiert verwaltet und absichert.

<https://www.baramundi.com/de-de/it-training/webinare/>

Kontaktieren Sie uns.

Wir freuen uns auf Sie!



baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany
+49 821 56708-380
request@baramundi.com



+48 735 91 44 54
request@baramundi.com



+44 2071 93 28 77
request@baramundi.com



+43 1 928 0136 0010
request@baramundi.com



baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA
+1 508 861 7561
requestUSA@baramundi.com



+41 77 280 49 79
request@baramundi.com



+39 340 8861886
request-italia@baramundi.com



+49 821 56708-390
request@baramundi.com



Making IT Admins Smile