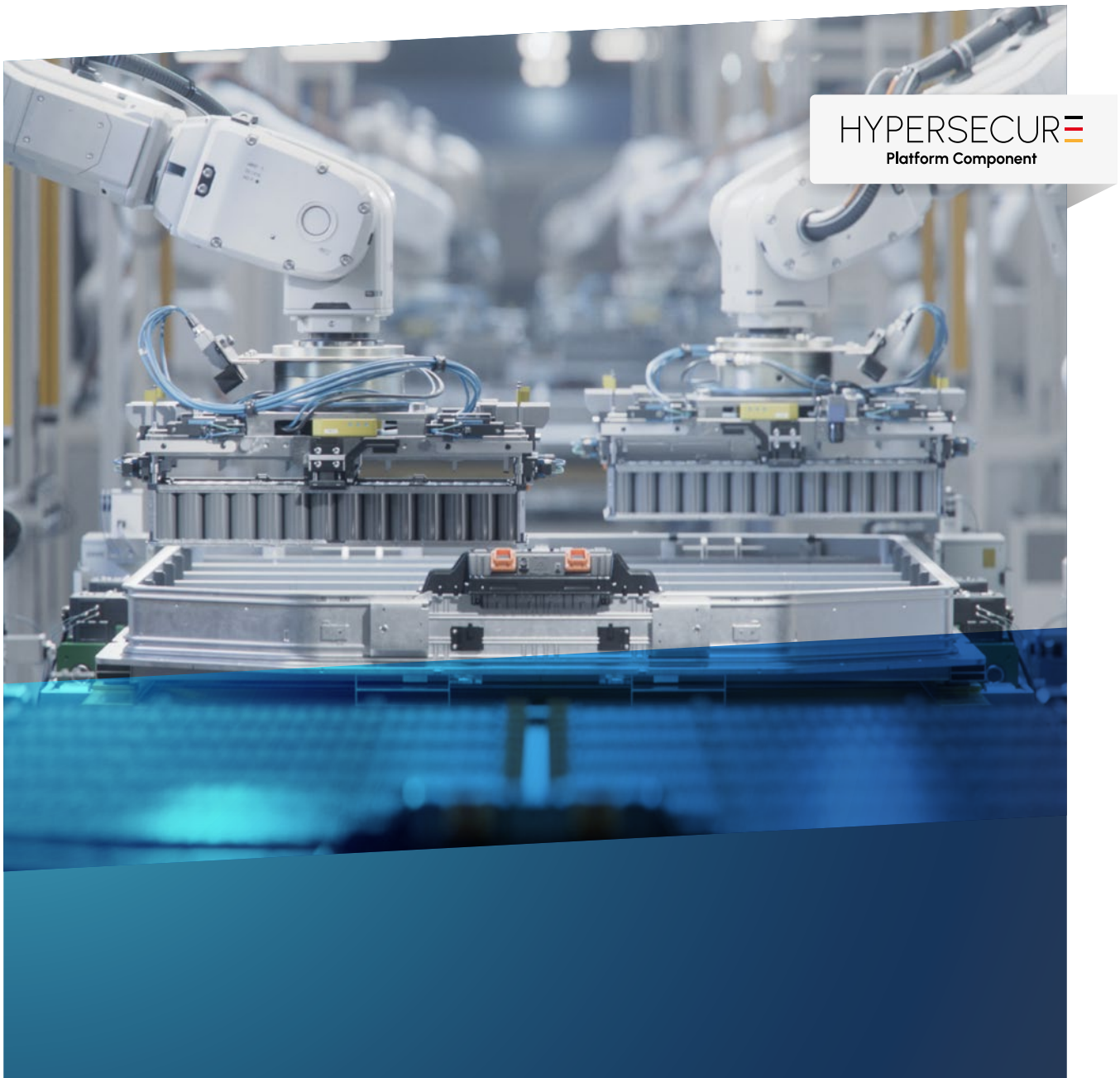
DriveLock

WHITEPAPER

OPERATIONAL TECHNOLOGY/IIOT



EINLEITUNG

1 Management Summary 3

2 Cyberangriffe auf ICS sind auf dem Vormarsch 5

3 TOP 3 Gefahren – Typische Angriffsszenarien für ICS Systeme 11

4 Schutzmaßnahmen für ICS Systeme 14

5 Industrial Security mit DriveLock 16

6 Fazit 26

1

MANAGEMENT SUMMARY

MANAGEMENT SUMMARY

Die Fertigungsindustrie durchlebt einen Wandel. Industrie 4.0 steht für die stetig wachsende intelligente Vernetzung von Maschinen und Abläufen in der Industrie durch Digitalisierung. Zu den Chancen gehören neue Wertschöpfungsmodelle. Unter anderem wird die Herstellung kundenspezifischer und selbst-designter Produkte ermöglicht, Lieferzeitpunkte können genau vorhergesagt werden. Zum anderen wird Qualität und Effizienz in der Produktion gesteigert.

Im Gegenzug aber hinken die Sicherheitslösungen oft noch hinterher. Immer mehr Unternehmen erkennen jetzt, dass ohne die richtigen Security-Maßnahmen besonders hochautomatisierte Produktionsanlagen ein leichtes Ziel für Cyberangriffe sind. Die Digitalisierung wird nicht mit der smarten Fabrik enden, sondern die Fabrikgrenzen erweitern, indem sie die Anlagen auch mit den externen Lieferanten vernetzt. Ein zweischneidiges Schwert, das sowohl die Produktivität als auch die Risiken steigert. Unternehmen benötigen eine umfassende und kostengünstige IT Security ohne Beeinträchtigung der Produktionsleistung, um die Vorteile integrierter Fertigungssysteme voll auszuschöpfen und gleichzeitig die Gefahren zu minimieren.

Smarte Fabrik braucht smarte Security. Wir helfen Ihnen bei der Umsetzung. DriveLock bietet Beratungsunterstützung und Lösungen an: Applikationskontrolle und Gerätekontrolle zum Schutz vor Schadsoftware und Kontrolle mobiler Datenträger, Endpoint Detection-Werkzeuge sowie Datenverschlüsselung für Festplatten, Verzeichnisse, Dateien und externe Datenträger. Zudem können Anlagentechniker, IT- und Produktionspersonal durch unser Security Education-Modul kontinuierlich mit Informationskampagnen direkt am Arbeitsplatz geschult und sensibilisiert werden.

Weitere Fragen beantworten wir Ihnen gerne.
Kontaktieren Sie uns auf www.drivelock.com,

telefonisch unter +49 (89) 546 36 49-0
oder per E-Mail an info@drivelock.com.

2

CYBERANGRIFFE AUF ICS SIND AUF DEM VORMARSCH

CYBERANGRIFFE AUF ICS SIND AUF DEM VORMARSCH

Systeme zur Fertigungs- und Prozessautomatisierung – zusammengefasst unter dem Begriff Industrial Control Systems (ICS) – werden in nahezu allen Infrastrukturen eingesetzt, die physische Prozesse abwickeln. Dies reicht von der Energieerzeugung und -verteilung über Gas- und Wasserversorgung bis hin zur Fabrikautomation, zu Verkehrsleittechnik und zum modernen Gebäudemanagement.

Angriffe auf Produktionsanlagen, kritische Infrastrukturen oder Geräte, die nicht zur klassischen Büro-IT, sondern zu operativen Technologien gehören, sind keine Zukunftsmusik mehr, sondern Realität im Unternehmensalltag. Industrielle Kontrollsysteme (ICS) oder SCADA (Supervisory control and data acquisition) Systeme sind zunehmend denselben Cyber-Angriffen ausgesetzt, wie dies in der konventionellen IT der Fall ist.

Die Betreiber müssen sich angesichts einer zunehmenden Häufigkeit von Vorfällen und neu entdeckten Schwachstellen dringend dieser Thematik annehmen.[1] Industrielle Cybersicherheit ist eine Notwendigkeit geworden.

IT vs. OT – die Verschmelzung IT und OT

OT wird von Marktforschungsunternehmen und Analysten wie Gartner als Betriebstechnik, englisch „Operational Technology"(OT) definiert. Sie besteht aus Hard- und Software zur Überwachung und Steuerung von physikalischen Geräten und deren Prozessen und Ereignissen im Unternehmen. Verallgemeinert werden industrielle Produktions- & Kontrollsysteme (ICS) und zugehörige Netzwerke und Endpunkte oft als Operational Technology (OT) bezeichnet.

In der Vergangenheit war die Mehrheit der OT-Systeme herstellerspezifisch, von der restlichen Informationstechnologie abgekapselt und die meisten Geräte waren nicht internetfähig (IP). Heutzutage sind durch die Digitalisierung viele ICS-Systeme und -Subsysteme eine Kombination aus OT und IT. Die Verantwortung für die industrielle Cybersicherheit ist somit auch etwas verschwommen: Wir können dies IT-OT-Konvergenz oder das Industrial Internet of Things (IIoT) nennen.

> Das Industrial Internet of Things (IIoT) stellt die industrielle Ausprägung des Internet of Things (IoT) dar. Es repräsentiert im Gegensatz zum IoT nicht die verbraucherorientierten Konzepte, sondern konzentriert sich auf die Anwendung des Internets der Dinge im produzierenden und industriellen Umfeld.[2]

Einige Analysten bevorzugen den Begriff „durchgängig verbundene Geräte". Tatsache ist, dass die Grenze zwischen IT- und OT-Domäne früher sehr klar war, heute nicht mehr.

IT-Komponenten und IT-Technologien aus der Office IT werden zunehmend in der OT eingesetzt und sind inzwischen vergleichbaren Risiken ausgesetzt.

Diese Entwicklung wird durch den Trend zur Optimierung von Fertigungsprozessen zur Steigerung der Wettbewerbsfähigkeit im Rahmen von Industrie 4.0 beschleunigt.

[1] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_005.pdf?__blob=publicationFile&v=12

[2] https://www.bigdata-insider.de/was-ist-das-industrial-internet-of-things-iiot-a-654986/

IT-Organisationen haben in der Regel industrielle Unternehmensbereiche (siehe Abbildung: Ebenen 4 und 5) verwaltet. Die IT hat sich im Allgemeinen mit der Sicherung von Systemen befasst, in denen Daten wie Finanz- und Kundeninformationen, geistiges Eigentum und zukunftsorientierte Unternehmensinformationen gespeichert sind. Diese Systeme können aus Servern, Workstations, E-Mail-Systemen, Anwendungen und Datenbanken bestehen.

Die Domäne der OT-Organisation ist die Werkshalle, die Prozessautomatisierung und die Produktionssysteme. Diese Systeme können Geräte umfassen, die über weite geografische Gebiete verteilt sind, wie z.B. Wasserpumpstationen oder elektrische Übertragungsstationen. Die gesamte OT-Domäne ist auf den Ebenen 0 bis 3 dargestellt. Die OTTeams sind in erster Linie um die Sicherheit und Verfügbarkeit ihrer physischen und Cyber-Anlagen besorgt, da eine Unterbrechung menschliche Schäden oder Produktionsausfälle verursachen könnte.[3]

Purdue Model for Control Hierarchy logical framework. Source SANS Institute

Eine Unterscheidung zwischen OT und IT ist anhand folgender Kriterien möglich:[4]

Operation Technology vs. Information Technology (IT)

Raue Umgebung	Einsatzort	Klimatisierte Büros
Anlagen-ISB-Personal	Installation	Netzwerk Fachpersonal
15-16 Jahre	Lebensdauer	3-5 Jahre
Anlagenspezifisch	Topologie	Sternförmig
Netzausfallzeiten max. einige ms	Verfügbarkeit	Sekunden- bis Minutenbereich akzeptiert
Niedrig, Switches mit wenigen Ports	Gerätedichte	Hoch, Switches mit hoher Portanzahl
Relativ kleine Netzwerke	Ausdehnung	Große Netzwerke
Oft Teil der Anlagenüberwachung	Netzüberwachung	Durch ausgebildete Fachkraft
Selten	Outsourcing	Weit verbreitet
Selten	Patchmanagement	Oft, täglich

[3] Quelle: Th e Sans Institute (2020): Purdue logical framework or Control Hierarchy

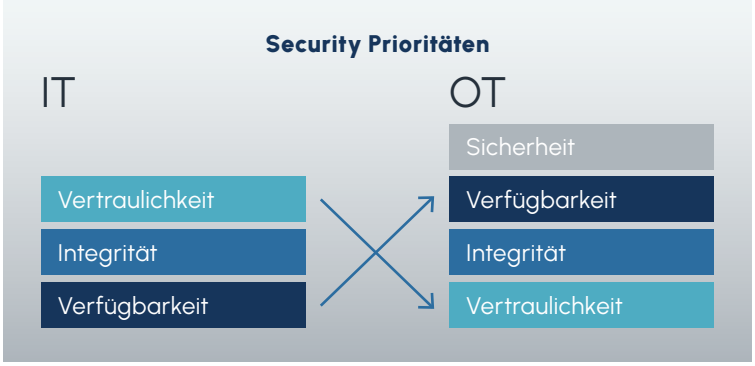
[4] DriveLock: Cyber Summit 2020

Wichtige Erkenntnisse:

- **Personal für die Inbetriebnahme und Instandhaltung der Anlagen ist unzureichend in Cybersecurity geschult.**
- **Die Lebensdauer der Anlagen ist sehr lang.**
- **Die Verfügbarkeit im OT-Bereich ist extrem wichtig. Patchen ist problematisch (siehe Abschnitt „Schwachstellen von ICS-Systemen").**

Unterschiedliche Schutzprioritäten IT vs. OT

IT und OT haben unterschiedliche Definitionen von Sicherheit und Prioritäten. Während klassische IT-Sicherheit mit Vertraulichkeit als höchste Priorität, danach Integrität und Verfügbarkeit definiert ist, gibt es in der OT einen zusätzlichen Sicherheitsbegriff: Den der Betriebssicherheit (engl. „Safety"). Betriebssicherheit bzw. Arbeitsschutz hat den Schutz von Mensch und Umwelt vor physischem Schaden zum Ziel - während die Informationssicherheit in erster Linie den Schutz der Daten vor Mensch (Insider-Attacke) und Umwelt (z. B. Cyberangriff) meint.



In der OT stehen Betriebssicherheit und Verfügbarkeit an oberster Stelle, danach folgen Integrität und Vertraulichkeit. Eine alternative Darstellung der Sicherheitsdimensionen findet sich bei Gartner [5]. Weshalb eine Gesamtbetrachtung beider Welten unvermeidbar geworden ist, zeigt sich in dem vielzitierten Vorfall in einer Chemieanlage in Saudi-Arabien. Dort wurde eine Schadsoftware entdeckt, die gezielt die Safety-Systeme befallen hatte.[6] Diese war darauf ausgelegt, deren Funktion außer Kraft zu setzen. Die als Trisis bezeichnete Schadsoftware zeichnete sich durch eine sehr hohe Spezialisierung auf das verwendete Safety-System aus. Nur durch einen Zufall wurde der Angriff entdeckt und es kam zu keinen weiteren Auswirkungen.[7]

Architecting Security for New OT SecurityRequirements

[5] Quelle: Gartner (2020): OT Security Best Practices

[6] https://www.sichere-industrie.de/trisis-wenn-it-sicherheitsmaengel-die-safety-beeintraechtigen/

[7] https://www.sichere-industrie.de/safety-security-unterschied-erklaert-kombination-ziele-industrial-security/

WESHALB DIE OT VERWUNDBAR GEWORDEN IST

Der Wandel zu einer offenen OT

Wie bereits erwähnt, ist die Produktions-IT nicht mehr isoliert von der internen bzw. Office-IT und somit verwundbarer geworden. Dafür gibt es Gründe, die sowohl mit der Historie bestehender Produktionssysteme als auch der Digitalisierung zusammenhängen:

- **Steuerung von außen: Produktionsanlagen werden heutzutage zunehmend auch von außen gesteuert und überwacht, z. B. wenn Techniker über Remote-Wartungszugang auf Produktionsanlagen zugreifen.**
- **Produktionsreports: Die Firmenleitung wünscht Reports aus der Produktion in Echtzeit. Dazu ist eine Verbindung von IT-Netzen zur OT notwendig.**
- **IoT wird zu IIot: Die vielfältigen Möglichkeiten des Internets der Dinge ermöglichen Steuerungsmöglichkeiten für Produktionsanlagen. Basierend auf dem Internet der Dinge (IoT) entsteht unter dem Stichwort IIoT (Industrial Internet of things) die intelligente „Smart Factory", die über Endgeräte gesteuert werden kann.**

Dies alles ist nur möglich, durch eine Kopplung der Produktions-IT an Netze und somit Zusammenschluss von IT und OT, um eine permanente Erreichbarkeit von OT-Anlagen (Fertigungs-/Produktionsanlagen) von außen zu gewährleisten. Diese Netze können angegriffen werden.

Schwachstellen von ICS-Systemen
Traditionelle ICS-Systeme und deren IT-Betreuung begünstigen Cyberattacken.

Langlebige Produktionsanlagen und veraltete Systeme
Klassische Produktionsanlagen haben oft Laufzeiten von 7 bis 10 Jahren und werden nicht – wie beispielsweise ein Notebook - nach ein wenigen Jahren ausgetauscht. Vielfach sind deren Betriebssysteme veraltet und Sicherheitsupdates (Patches) stehen nicht mehr bereit.

Problematisches Patchen
Patchen ist perse im Industrieumfeld problematisch, da Systeme heruntergefahren werden müssen und die Verfügbarkeit der Produktionsanlage als oberste Priorität leidet. Veraltete Systeme sind guter und leichter Nährboden für Zero Day-Attacken, Angriffe durch nicht geschlossene Sicherheitslücken in der Software. Angreifer über die Netze haben somit leichtes Spiel.

Mangelhafte IT-Sicherheitslösungen
Alte Produktionsanlagen sind nicht standardmäßig mit IT-Sicherheitslösungen ausgestattet, da es zum Zeitpunkt ihrer Herstellung noch keine Cybergefahren wie heute gab. Antiviren-Scanner können nicht ohne weiteres auf Fertigungskontrollsystemen installiert werden, da der Verlust von (Hersteller-)Zertifikaten und -Garantien droht. Oft ist hier auch der Echtzeitscanner deaktiviert. Ein zeitnahes Einspielen von Updates in den Scanner ist nicht immer möglich.

WESHALB DIE OT VERWUNDBAR GEWORDEN IST

Zu wenig IT-Security Know-how

Produktionsmitarbeiter, die für den Betrieb der Anlagen verantwortlich sind, wissen zu wenig über mögliche Angriffsmöglichkeiten und IT-Risiken. Insgesamt gibt es zu wenige IT-Fachkräfte mit Security Know-how.

Warum ist der Industriesektor besonders interessant für Angriffe?

Die Attraktivität des Industriesektors für Cyberattacken basiert auf dem hohen Anspruch an Verfügbarkeit und dem Safety-Begriff, der der Arbeitssicherheit Rechnung trägt. Eine manipulierte Anlage oder Industrieroboter können zu einer Gefahr für den Menschen werden. Zudem werden in einem industriellen Produktionsprozess nur Ausfallzeiten im Millisekunden-Bereich toleriert. Der Stillstand von Produktionsprozessen aufgrund einer Attacke verursacht hohe Kosten.

Cyber-Kriminelle nutzen diese Voraussetzungen als Druckmittel für ihre Angriffe z. B. mit Erpressungssoftware. Einige bekannt gewordene Beispiele aus der Industrie:

HACKERANGRIFF

- **Der Cyberangriff auf den norwegischen Aluminiumhersteller Norsk Hydro legte wichtige IT-Systeme lahm. Die Erpressungssoftware/Ransomware befiel über das Office-Netz auch Produktionssysteme und behinderte die Fertigung. In der Folge sank die Aktie des Konzerns, der Preis für Metall stieg hingegen.[8] Die IT-Katastrophe wurde von Norsk Hydro sehr offen kommuniziert.**
- **der Computerwurm Stuxnet - ursprünglich gegen das iranische Atomprogramm eingesetzt - befiel Kontrollsysteme für Industrieanlagen und schädigte im Zuge seiner Verbreitung auch andere Industrieunternehmen.**
- **der Trojaner Industroyer legte das ukrainische Stromnetz lahm. Der Schadcode beherrscht mehrere Kommunikationsprotokolle, die von SCADA (Supervisory Control And Data Acquisition) - Anlagen verwendet werden.**

[8] https://www.handelsblatt.com/unternehmen/industrie/aluminiumkonzern-cyberangriff-auf-norsk-hydro-treibt-den-aluminiumpreis-/24119924.html?ticket=ST-7802151-O1OR01dBj6GvsdbK4grn-ap5

3

TOP 3 GEFAHREN – TYPISCHE ANGRIFFSSZENARIEN FÜR ICS SYSTEME

TOP 3 GEFAHREN – TYPISCHE ANGRIFFSSZENARIEN FÜR ICS SYSTEME

Risiken für industrielle Produktions- und Kontrollsysteme resultieren aus Bedrohungen, die aufgrund existierender Schwachstellen dem ICS und damit einem Unternehmen Schaden zufügen können. Die kritischen und am häufigsten auftretenden TOP 10-Bedrohungen für ICS werden jährlich vom Bundesamt für Sicherheit in der Informationstechnik (BSI) publiziert. Die folgende Tabelle zeigt die wichtigsten drei.[9]

RANGFOLGE	TOP 3 BEDROHUNGEN	TREND SEIT 2016
1	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	↗
2	Infektion mit Schadsoftware über Internet und Intranet	↗
3	Menschliches Fehlverhalten und Sabotage	↑

Abbildung: Quelle BSI10

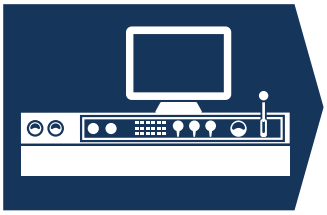
Auf den weiteren Plätzen folgen u. a. Kompromittierung von Extranet und Cloud-Komponenten, Social Engineering und Phishing, (D)DoS-Angriffe.

TOP 1: Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware (z. B. Bad USB)
Beispiel: Stuxnet-Angriff über einen Wechseldatenträger (USB-Drop Attack).

Dafür kommen auch kommerzielle Wechseldatenträger und Hardware zum Einsatz, die Plug & Play ausnutzen, z. B.:

- **USB Rubberducky**
- **Bash Bunny**
- **USB Ninja Cable**

Angriffs-Szenario:
Ein führendes Industrieunternehmen betreibt über 15 Jahre alte Anlagen, deren Steuerungssystem auf Windows XP basiert. Um Updates einzuspielen, verfügen die Industrieanlagen über einen USB-Port, der eine ungeschützte Schnittstelle zum SCADA-System darstellt.



[9] Quelle: BSI (2019): Empfehlung: IT in der Produktion. Industrial Control System Security Top 10 Bedrohungen und Gegenmassnahmen 2019 https://www.allianzfuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_005.pdf?__blob=publicationFile&v=12

[10] ebenda

Diese USB-Schnitstelle wird von den Mitarbeitern nicht nur für das Einspielen von Updates genutzt, sondern auch um beispielsweise Musik zu hören oder Handy zu laden.

Ein von Malware befallenes Mitarbeiterhandy war somit in der Lage, den Viurs auf das SCADA-System zu übertragen und den normalen Betrieb der Fabrik still zu legen.

FOLGEN:

- **Das Werkstück wird zerstört.**
- **Die Maschine wird beschädigt.**
- **Konstruktionsdaten werden sublim modifiziert.**
- **Malware fährt den Arbeitsarm des Produktionsroboters auf Endpositionen und gefährdet damit Leib und Leben der Arbeiter.**

Quelle: DriveLock

TOP 2: Infektion mit Schadsoftware über das Internet und Intranet

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) registrierte in seinem Lagebericht zur IT-Sicherheitslage 2020 im Zeitraum Juni 2019 bis Mai 2020 täglich durchschnittlich 322.000 neue Schadprogramm-Varianten (Malware) und potentiell unerwünschte Anwendungen (PUA). Zu Spitzenzeiten gab es bis zu 420.000 neue Varianten pro Tag. Insgesamt haben in dem Zeitraum die Schadprogrammvarianten um 117,4 Millionen zugenommen - Tendenz zum Vorjahresbetrachtungszeitraum steigend.[11]

TOP 3: Menschliches Fehlverhalten und Sabotage

Hierunter finden sich Angriffe mit Phishing-Mails, die die Unerfahrenheit oder Unachtsamkeit von Mitarbeitern ausnutzen. Wie erwähnt werden Produktionsanlagen nicht von ausgebildetem IT-Personal überwacht und gewartet. Zudem sind Insiderangriffe nicht zu unterschätzen. Hierzu zählt auch der bereits erwähnte Übergriff von Schadsoftware von Office- auf Produktionssysteme.

[11] https://www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html

4

SCHUTZMASSNAHMEN FÜR ICS SYSTEME

SCHUTZMASSNAHMEN FÜR ICS SYSTEME

Das BSI empfiehlt für ICS-Systeme neben anderen Maßnahmen vier wirksame Vorkehrungen, um sich gegen Cyberattacken zu schützen.[12]

1. Restriktive Nutzung von Wechselmedien und mobilen Geräten
Für die Nutzung von Wechseldatenträgern und mobilen Endgeräten sollten Regelungen aufgestellt und bekannt gemacht werden. Der Einsatz von Wechseldatenträgern und mobilen Endgeräten in ICS-Umgebungen sollte grundsätzlich beschränkt werden.

2. Schutz vor Schadprogrammen
Es bedarf eines Konzepts zum Schutz vor Schadprogrammen und dessen Umsetzung. Darin müssen die bedrohten IT-Systeme sowie die möglichen Infektionswege wie Außenschnittstellen, Wechselmedien betrachtet werden, heißt es beim BSI.

3. Sensibilisierung und Mitarbeiterschulung
Das Betriebspersonal muss regelmäßig zu relevanten Sicherheitsbedrohungen im OT-Bereich informiert und sensibilisiert werden.

4. Überwachung, Protokollierung und Erkennung von Ereignissen auf den Endpunkten und Systemen
Betriebs- und sicherheitsrelevante Ereignisse müssen zeitnah identifiziert werden.

[12] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/IND/IND_1_Betriebs-_und_Steuerungstechnik.html?nn=10137148#doc10095914bodyText19

[13] Bundesamt für Sicherheit in der Informationstechnik (2019): Empfehlung: IT in der Produktion, Industrial Control System Security, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_005.pdf?__blob=publicationFile&v=12

5

INDUSTRIAL SECURITY MIT DRIVELOCK

INDUSTRIAL SECURITY MIT DRIVELOCK

In diesem Kapitel beschreiben wir, wie die DriveLock Zero Trust Plattform hilft, die genannten Maßnahmen im Industriesektor effektiv und sicher zu verwirklichen. Die cloud-basierten DriveLock Endpoint Security-Lösungen tragen zur „Härtung" Ihrer Produktionssysteme bei.

Der Sicherheitsansatz Zero Trust als Benchmark

Zero Trust ist ein Sicherheitskonzept, dessen Ziel es ist, Unternehmen vor Bedrohungen und den Auswirkungen von Datendiebstahl zu schützen. Das Modell hat zum Grundsatz „never trust, always verify". Im Vergleich zu herkömmlichen Konzepten stellt das Zero Trust Modell einen Paradigmenwechsel dar, indem es alle Geräte, Dienste und Benutzer gleichbehandelt und ihnen grundsätzlich misstraut, während traditionelle Sicherheitskonzepte den Angreifer von außerhalb des Netzwerks bekämpfen, ihn aber innerhalb des Netzwerks nicht mehr als Eindringling betrachten.

Zero Trust im Grundsatz bedeutet:

- **Der Zugriff auf alle Ressourcen und Assets erfolgt sicher und standortunabhängig: Dazu zählen z. B. Applikationen, Netzwerk-Laufwerke oder USB-Geräte.**
- **Die Zugangskontrolle erfolgt nach dem Prinzip: benötigt ein User diese Anwendung wirklich für seinen Arbeitsalltag und welche Rechte (z. B. Lesen, Schreiben, Vollzugriff) bekommt er? Dieses Prinzip wird strikt eingehalten.**
- **Der gesamte Datenverkehr wird überprüft und protokolliert.**
- **Die Infrastruktur ist darauf ausgelegt, alles zu überprüfen und nichts und niemandem zu vertrauen.**

Das Zero Trust Konzept hat keinen Einfluss auf die Schnelligkeit bzw. Performance der Endpunkte bzw. Devices, da der sog. „Agent" nicht ständig läuft.

DriveLock bietet mit seiner Zero Trust-Plattform eine Palette von effektiven IT-Security-Lösungen an, die diesem Prinzip gerecht werden.

- **Device Control**
- **Application Control**
- **Security Awareness**
- **Endpoint Detection & Response**

DRIVELOCK ZERO TRUST PLATFORM

Application Control

Flexible Applikationskontrolle mit einem granularen Regelwerk. Verschiedene Lernmodi und Integration von Softwareverteilsytemen.

Device Control

Kontrollierter und protokollierter Zugriff auf externe Laufwerke und Geräte mit entsprechender Benutzerakzeptanz.

Endpoint Detection & Response

Kontinuierliche Echzeit-Überwachung von Endpunkten. Über 600 verschiedene Ereignisse werden erkannt, korreliert und ausgewertet.

Security Awareness

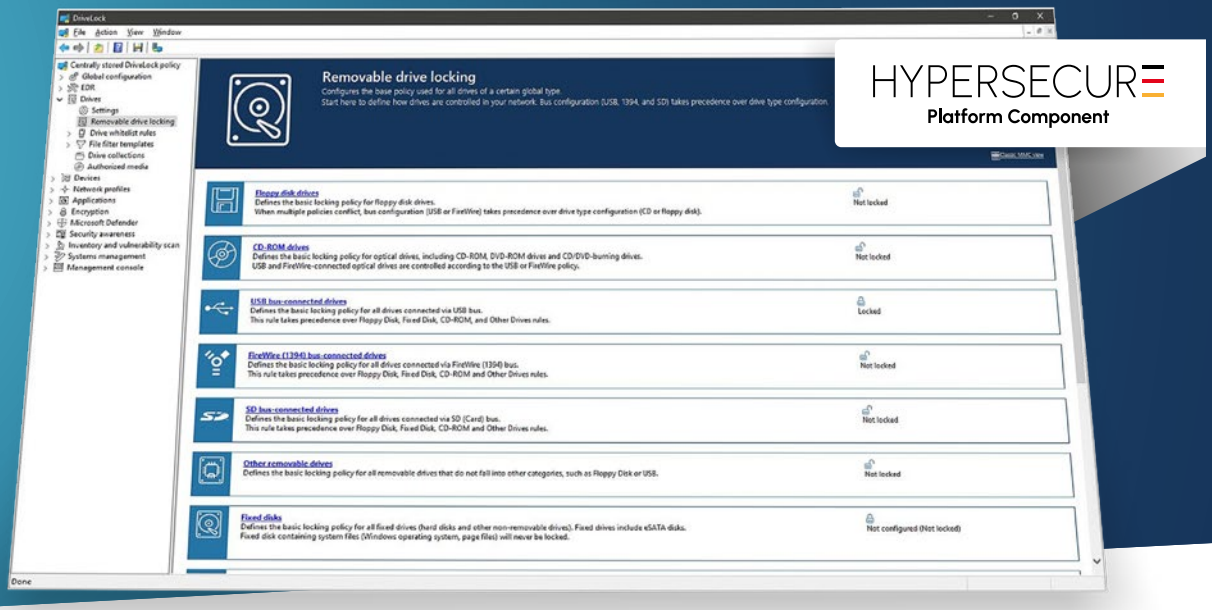
Multimediale Security Awareness Bibliothek mit regelmäßigen Updates oder eigene Inhalte. Anzeige basierend auf Triggern (Events, Recurring etc.).

Quelle: DriveLock

Restriktive Nutzung von Wechseldatenträgern und externen Geräten durch Device Control

Als Schutzmaßnahme empfiehlt das BSI einen sorgsamen Umgang mit (mobilen) Datenträgern und Austausch von Datenträgern. Bei der smarten Gerätekontrolle ist eine Vielzahl granularer Einstellmöglichkeiten für die Flexibilität und den reibungslosen Ablauf in der Produktion relevant. Ein generelles Verbot von z. B. Memory-Sticks ist in vielen Produktions-Umfeldern nicht vorstellbar. Mobile Datenträger können aber auch verloren gehen. Daher sollten Sie Daten auf diesen Geräten immer verschlüsseln, damit Unbefugte diese Daten nicht lesen können. Zudem kann durch den sorglosen Umgang mit Datenträgern aus unbekannter Quelle, Schadsoftware in die ICS-Systeme gelangen. Auch das gilt es zu verhindern.

DEVICE CONTROL VON DRIVELOCK



Mit **DriveLock Device Control** verhindern Sie, dass sensible Daten auf externe Speichermedien gelangen oder externe Datenträger einfach angeschlossen und ausgelesen werden können.

Sie haben somit Kontrolle über externe Datenträger und den Datenfluss. DriveLock prüft jedes angeschlossene Gerät und sperrt es gegebenenfalls. Somit stellen Sie sicher, dass nur genehmigte Geräte oder externe Laufwerke verwendet werden können. Schließt ein Mitarbeiter ein Gerät an den USB-Port an, so erkennt der Rechner, ob es sich um eine externe Festplatte, einen USB-Stick o. ä. handelt. Via DriveLock lässt sich folglich regulieren, welche USB-Medien überhaupt zulässig sind. Eine andere Regel könnte vorsehen, dass das Anschließen von USB-Geräten zwar erlaubt ist – der Nutzer darf jedoch keinerlei Dateien auf das Gerät schreiben, sondern die Daten darauf nur lesen.

DriveLock ermöglicht die Erstellung von Schattenkopien, um Produktionsanlagen im Sinne der DSGVO abzusichern. Darüber hinaus bietet DriveLock Funktionen zur erzwungenen Verschlüsselung von Daten, welche auf externe Laufwerke geschrieben werden.

Bei der Verwendung von externen Geräten kommt dem Thema Security Awareness eine große Bedeutung zu. Anwender nutzen die heute allgegenwertigen USB-Anschlüsse in vielfacher Weise. Dabei kann das „einfache" Aufladen eines Smartphones über einen USB-Anschluss eines ICS zu weitreichenden Sicherheitsproblemen führen. Neben dem Management von Black- und Whitelists für Geräte, ist der Einsatz von sogenannten Verwendungsrichtlinien sehr effizient. Hierbei wird das Gerät erst nach der Bestätigung durch Anwender oder sogar nach Eingabe von Benutzername und Passwort freigegeben.

Applikationskontrolle schützt vor Schadsoftware

Applikationskontrolle, die auf einer Positivliste basiert, gehört zu den wirksamsten Präventionsmaßnahmen.

DriveLock Application Control verhindert die Ausführung von Schadsoftware, die Ausnutzung von Tools (wie Powershell) durch schädliche Skripte und schützt vor Zero-Day-Exploits. Dahinter liegt ein Verfahren, das jedes auszuführende Programm gegen eine Whitelist (Positivliste) genehmigter Programme prüft. Diese Liste wird dynamisch erweitert. Unbekannte Software, die ggfs. durch einen nicht aktuellen Virenscanner geschlüpft wäre, wird nicht ausgeführt.

Dieses intelligente und lernende Management von Whitelists erlaubt es, mit minimalem Personaleinsatz eine Vielzahl an sehr heterogenen ICS sicher zu verwalten.

Damit entlastet die Lösung Security-Teams und gewährleistet unternehmensweit, dass nur bekannte und sichere Anwendungen laufen.

Zum Vergleich: Bei einer Antivirus (AV) Software besteht das Problem, dass nur bekannte Schadsoftware erkannt wird. Aber Malware tarnt sich oder ist zum Zeitpunkt eines Angriffs dem AV-Scanner noch nicht bekannt. Generell stehen diese Scanner vor einer Aufgabe, die nicht zu bewältigen ist. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) identifiziert wie bereits erwähnt jeden Tag 322.000 neue Schadsoftware-Programme oder Varianten davon. Das sind rund 224 pro Minute – fast 4 pro Sekunde.

Vielleicht fragen Sie sich jetzt, ob die eigene Anwendungssteuerung aus Windows nicht einen ähnlichen Schutz bietet wie DriveLock. Windows 10 enthält AppLocker, einen stark verbesserten Nachfolger der Richtlinien für Softwareeinschränkung (Software Restriction Policies). Vergleicht man aber die DriveLock Applikationskontrolle mit AppLocker, stellt man fest, dass AppLocker nur einen begrenzten Schutz enthält: Dieser Dienst ist keine ausreichende und voll funktionale Applikationskontrolle: Die Möglichkeiten von DriveLock gehen darüber hinaus. DriveLock unterstützt beispielsweise ältere Betriebssystem-Versionen (vor Windows 7). Richtlinien sind granularer umsetzbar, da z. B. Technikern höhere Rechte als Betriebsanwendern zugestanden werden. Auch benötigt DriveLock einen wesentlich geringeren Administrationsaufwand, um das gleiche Sicherheitsniveau wie AppLocker zu ermöglichen.

Abschließend nennen wir noch einige Beispiele von Szenarien, die DriveLock ermöglicht, welche jedoch mit Windows 10 allein unmöglich oder nur sehr schwierig konfiguriert werden können:

- **Automatisches Whitelisting aller Anwendungen, die von bestimmten Administrator- oder Service Accounts installiert werden**
- **Blacklist- oder Whitelist-Regeln auf der Basis einer unternehmensweiten Anwendungsdatenbank**

Anwendungsfall: Wartung/Notfallzugriff an einem Produktionssystem

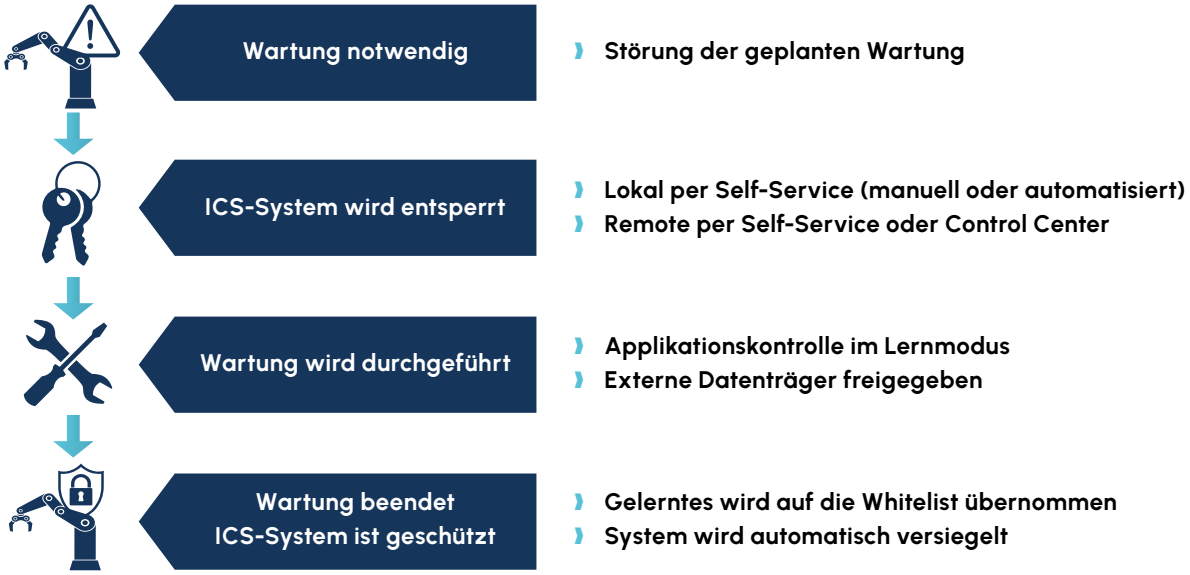
Das effektive Zusammenspiel von Applikationskontrolle und Wechseldatenträgerkontrolle soll am Beispiel der Wartung erläutert werden.

Besondere Anforderung:
Im industriellen Umfeld erfolgen Wartungsarbeiten an IT-Systemen häufig adhoc bzw. sind an sehr enge Zeitfenster gebunden. Wichtig ist dabei, dass keine Abhängigkeiten zu einem zentralen Service-Desk entstehen und der sichere Betrieb jederzeit gewährleistet ist. Dies macht ein zentrales Management entsprechender Sicherungslösungen von Produktionsanlagen ebenfalls sehr arbeitsintensiv. Um hier wirkungsvoll entgegenzuwirken, ist die Kombination unterschiedlicher Ansätze notwendig. Zum einen ist es entscheidend, dass Wartungsarbeiten dezentral ohne entsprechende Vorlaufzeiten bei der Konzern-IT möglich sind – auch im Offline-Betrieb der ICS. Zum anderen müssen die Lösungen in der Lage sein, sicherheitsrelevante Veränderungen an den Maschinensteuerungen zu protokollieren bzw. zu dokumentieren. Schließlich muss beim Einsatz von Applikationskontrolle die Möglichkeit bestehen, bei Updates und Patches Änderungen an den Black- und Whitelists automatisch durchzuführen. Selbstlernende Whitelists sind in der Lage, Software-Updates individuell pro ICS zu erkennen und basierend auf einem entsprechenden Regelwerk zu erlauben.

Nun zum eigentlichen Ablauf:

Im Falle einer planmäßigen oder adhoc-Wartung (oder Störung) entsperren Techniker zunächst das System. Dies kann manuell geschehen oder bei Produktionsstraßen remote z. B. vom Leitstand aus. Kurzzeitig wird also die „Security geöffnet". Ein wesentlicher Aspekt dabei ist, dass in dem Zeitfenster mit „gelockerter" Sicherheit eine vollständige Protokollierung stattfindet.

Anschließend können die Techniker die Software-Wartung durchführen, während die DriveLock Applikationskontrolle im Lernmodus das Softwareupdate „registriert". DriveLock stellt sicher, dass Software-Updates und Neuinstallationen nach Beendigung des Wartungsmodus Bestandteil der Whitelist sind. Es garantiert, dass die neuen Applikationen ohne permanente Umgehung des definierten Sicherheitsprofiles ausgeführt werden können.AppLocker zu ermöglichen.

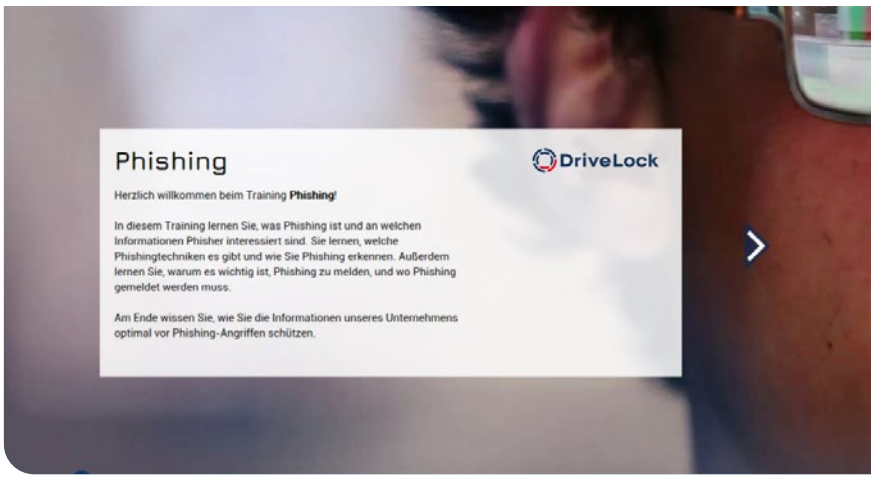


Vermeidung menschlichen Fehlverhalten und Aufklärung der Mitarbeiter durch Security Awareness

Der Mensch ist und bleibt das schwächste Glied in einer ganzheitlichen Sicherheitsstrategie. Untersuchungen unter Sicherheitsverantwortlichen belegen immer wieder, dass menschliche Fehler zu den größten Risiken gehören. Entsprechende fahrlässige Handlungen müssen nicht böswillig sein. Wir machen alle Fehler und Hacker agieren immer trickreicher. Deshalb ist es wichtig, die Belegschaft zu sensibilisieren und ihnen zu erklären, wie wichtig sie innerhalb der Kette von Schutzmaßnahmen sind. Security Awareness Trainings helfen und schärfen ein nachhaltiges Sicherheitsbewusstsein.

Security Awareness von DriveLock:

DriveLock Security Education-Programme wie z. B. Anti-Phishing-Training helfen, auf Phishing und Social Engineering-Angriffe zu reagieren und ein nachhaltiges Sicherheitsbewusstsein bei den Anwendern zu schaffen. Anlassbezogene Security Awareness kann im Zeitpunkt des Arbeitens eingesetzt werden – on the job: Beim Start einer neuen Applikation überprüft DriveLock, ob es sich um eine sichere Anwendung handelt und spielt im Zweifelsfall eine kurze Security-Kampagne zum Thema „Umgang mit neuen Anwendungen" aus. Anwender erhalten kontextbezogen entsprechende Sicherheitshinweise.



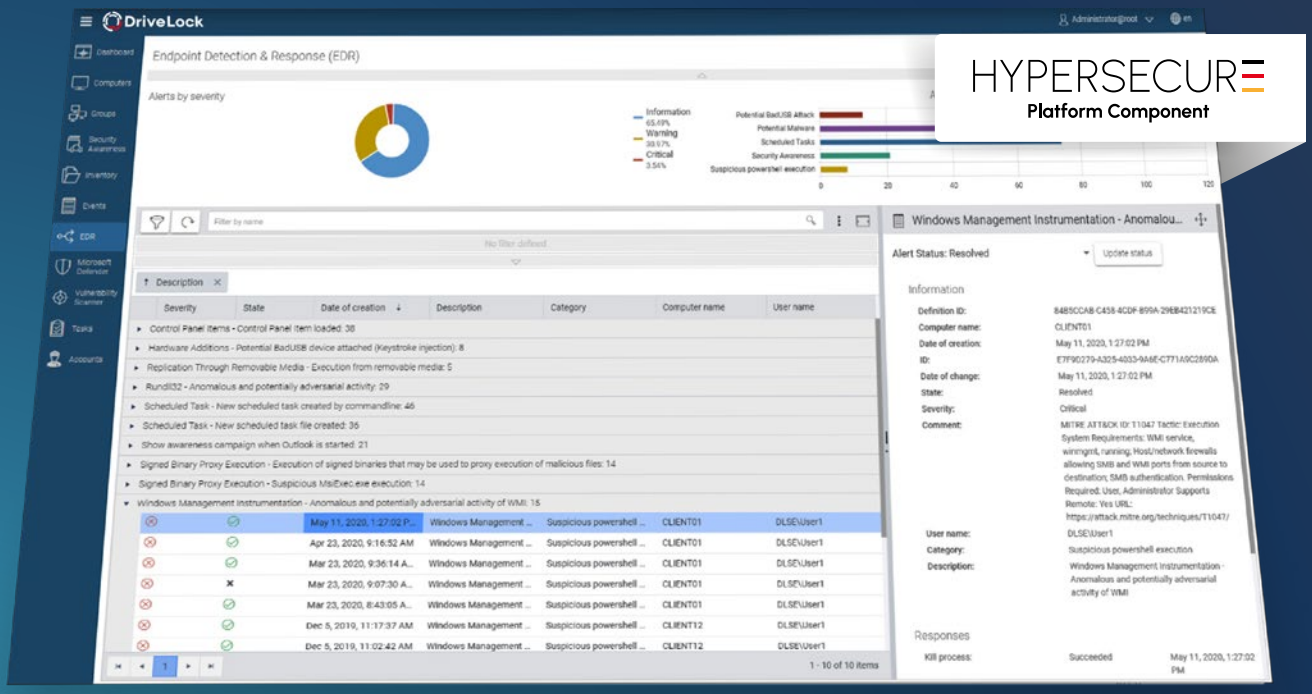
Endpoint Detection and Response

Die beschriebenen Präventionsmaßnahmen machen Angreifern das Leben signifikant schwerer. Aber: Sie geben keine 100%ige Garantie auf vollständige Sicherheit. Es gibt Fälle, bei denen diese Präventivmaßnahmen nicht weit genug gehen. Wenn Schadsoftware bereits in die Systeme eingedrungen ist, dann sind Hilfsmittel wichtig, den Eindringling aufzuspüren und die Angriffstaktiken und Muster zu erkennen.

Endpoint Detection & Response (EDR) von DriveLock

Endpoint Detection & Response Lösungen, kurz EDR, bieten Transparenz und Kontrolle über die Endgeräte in Echtzeit. Sie ermöglichen Verhaltens- und forensische Analysen durch die Erfassung und Überwachung sicherheitsrelevanter Ereignisse, sogenannte Events. Auf kritische Vorfälle und den Eingang von Alarmmeldungen („Alerts"), z. B. eine Warnung, kann sowohl automatisch wie auch manuell reagiert werden.

ENDPOINT DETECTION AND RESPONSE



Vollverschlüsselung von Datenträgern und Wartungsnotebooks
Das BSI empfiehlt zum Schutz sensibler Daten auch externe Datenträger zu verschlüsseln. In dem Zusammenhang wird auch die Verschlüsselung von Wartungsnotebooks als Maßnahme gegen das Einschleusen von Schadsoftware genannt.[14]

Verschlüsselungsmodule von DriveLock:

DriveLock Verschlüsselungslösungen ermöglichen die Verschlüsselung von Festplatten, Verzeichnissen, Ordnern, Dateien und von USB-Sticks:

- **Transparente und schnelle Festplattenverschlüsselung**
- **Zuverlässige Datei- und Verzeichnisverschlüsselung**
- **Verschlüsselung von Wechselmedien wie USB-Sticks, CD/DVD oder mobilen Festplatten**
- **Erweiterung des Handlings der Microsoft BitLocker-Verschlüsselung um für Unternehmen essenzielleZusatzfunktionen (DriveLock BitLocker Management)**

[14] Bundesamt für Sicherheit in der Informationstechnik (2019): Empfehlung: IT in der Produktion, Industrial Control System Security, gefunden unter https://www.allianzfuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_005.pdf?__blob=publicationFile&v=12

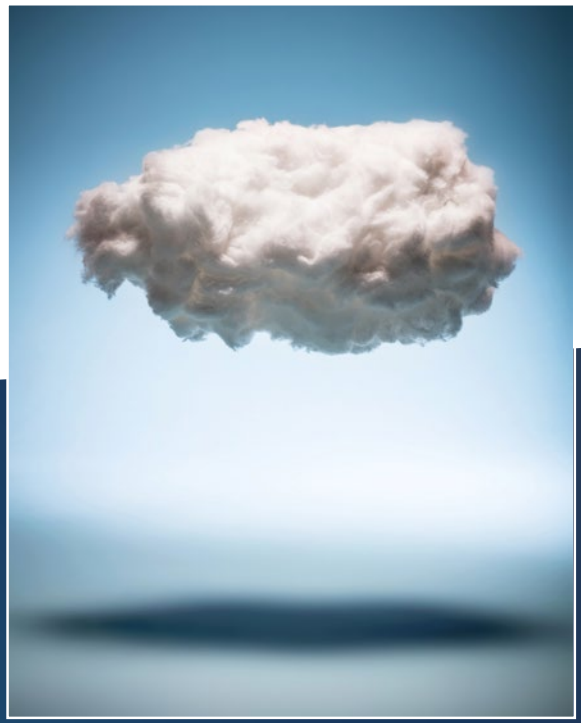
Vorteile des DriveLock BitLocker Management gegenüber der reinen Microsoft-Funktionalität
BitLocker ist die in Windows 10 enthaltene Full Disk Encryption. Doch mit steigenden regulatorischen Anforderungen ist diese allein oft nicht ausreichend. DriveLock BitLocker Management verwaltet die bestehende BitLocker-Installation und erweitert diese um essenzielle Funktionen. Mehr dazu finden Sie hier.

Effektiver Schutz für Industrieanlagen mit Security aus der Cloud

Wie wir in den ersten Kapiteln dargestellt haben, steigen nicht nur die möglichen Einfallstore für Schadprogramme, sondern die Zahl der Schadprogramme wird exponentiell größer, die Angriffe immer komplexer. Um die empfohlenen Maßnahmen mit eigenem Personal stemmen zu können, d. h. die Lösungen einzuführen und zu betreuen, braucht es Investitionen in Mitarbeiter, Ausbildung und Systeme. Der Fachkräftemangel ist hier nur eines von mehreren Hindernissen. Diese Rahmenbedingungen können dazu führen, dass Security-Lösungen zwar initial eingerichtet und konfiguriert werden, es aber im laufenden Betrieb keine weiteren Anpassungen mehr gibt. Dadurch sinkt das Sicherheitsniveau mit der Zeit.

Eine Alternative ist, die vorgeschlagenen IT-Lösungen von einem Servicedienstleister managen zu lassen.

DriveLock bietet seine Endpoint Protection-Lösungen als **Managed Security aus der Cloud**. Wir stellen ein umfängliches fertig konfiguriertes Sicherheitsprofil zur Verfügung, das auf den jeweiligen Lösungsmodulen basiert. Somit kann das Produktionsunternehmen sofort mit dem Schutz seiner Endgeräte starten. Darüber hinaus werden diese Sicherheitsprofile von uns permanent weiterentwickelt bzw. an aktuelle Bedürfnisse angepasst und optimiert.

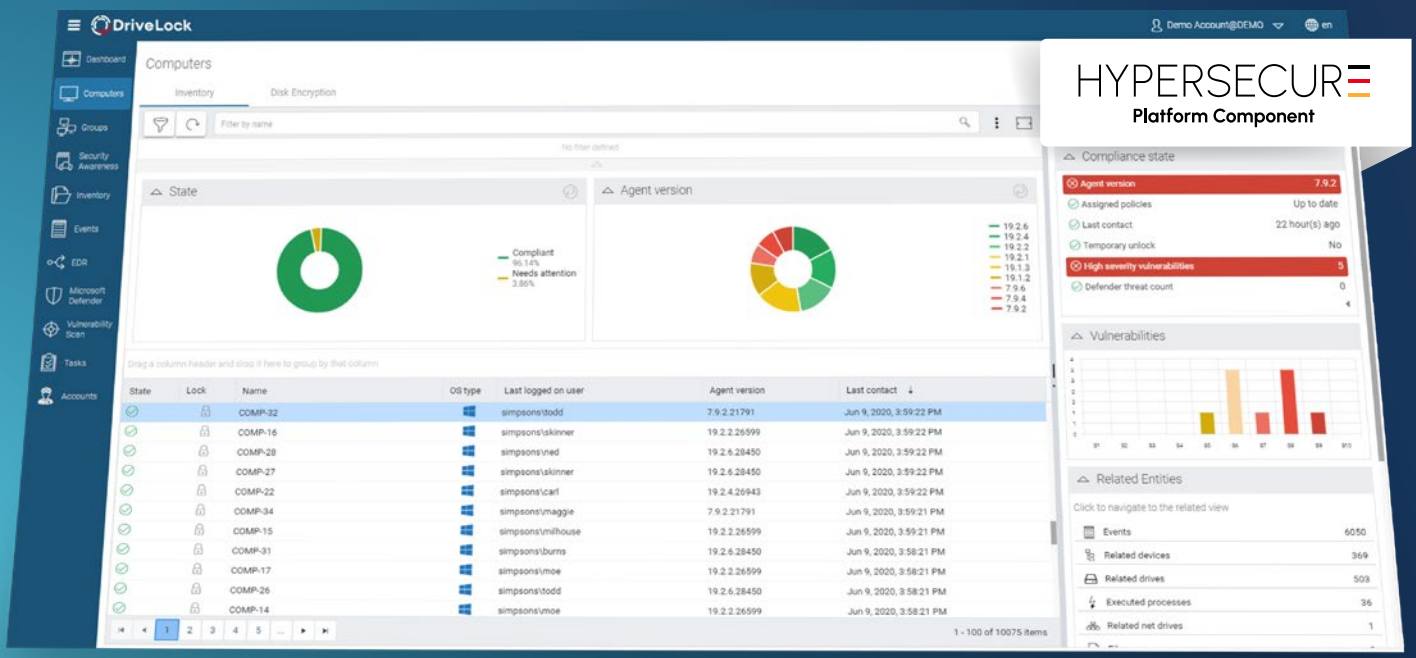


Sie profitieren von:

- Kostenvorteilen
- schneller Bereitstellung & automatischen Updates
- vordefinierten Sicherheitsrichtlinien
- keinen eigenen Investitionen in Hardware
- höchstem Schutz für Ihre Daten und Hochverfügbarkeit

AUSSERDEM BIETET DRIVELOCK

- Eine einheitliche Oberfläche zur Konfiguration sämtlicher Schutzfunktionen/Module/Schutzmaßnahmen - die DriveLock Management Console (DMC)
- Eine moderne und anpassbare web-basierte Oberfläche mit umfangreichen Auswertungs- und Analysemöglichkeiten - das DriveLock Operations Center (DOC) höchstem Schutz für Ihre Daten und Hochverfügbarkeit
- Ein flexibles, richtlinienbasiertes Management für On- und Offline-Systeme
- Integrationsmöglichkeiten mit zum Beispiel Softwareverteilungs- oder Security Information und Event Management (SIEM)-Systeme
- Umfangreiche Protokollierungsmöglichkeiten mit einer integrierten Anonymisierung personenbezogener Daten



6

FAZIT

FAZIT

Die Fertigungsindustrie und die OT durchleben mit wachender Digitalisierung einen Wandel, aber die Sicherheitslösungen hinken noch hinterher. Dabei profitieren Angreifer vom unzureichenden Security-Wissen der Mitarbeiter, von langlaufenden Anlagen mit beschränkten Sicherheitslösungen und einer mit der Büro-IT vernetzten OT, die auf Cybergefahren nicht vorbereitet war.

Unternehmen benötigen eine umfassende und kostengünstige Security ohne Beeinträchtigung der Produktionsleistung, um die Vorteile integrierter Fertigungssysteme voll auszuschöpfen und gleichzeitig die Gefahren zu minimieren. DriveLock bietet als Endpoint Security Spezialist eine Zero Trust-Lösungsplattform zur Realisierung einer gesamtheitlichen Sicherheitsstrategie an.

DriveLock

DriveLock SE
Landsberger Straße 396
81241 München
Telefon +49 (0) 89 5463649-0
E-Mail info@drivelock.com