Zugriffssicherheit
für die Industrie 4.0

Zugriffssicherheit
für die Industrie 4.0

IT-Infrastrukturen beeinflussen in zunehmendem Maße die industriellen Prozesse und sind in fast allen Bereichen unverzichtbar. Zukünftig werden komplexe Systeme die gesamte industrielle Wertschöpfungskette durchdringen und heute kaum vorstellebare Flexibilitäts- und Effizienzsteigerungen ermöglichen. Und neben künstlicher Intelligenz werden schon heute immer mehr Automatisierungslösungen eingesetzt. Dabei werden die einzelnen Komponenten immer autonomer und dadurch auch deutlich komplexer. IT-Sicherheit ist in diesem Zusammenhang unternehmenskritisch und unabdingbar.

Der Schutz vor Datenmissbrauch oder der Sabotage IT-basierter industrieller Prozesse betrifft ganze Wertschöpfungsketten bzw. -netzwerke, die vielfach global organisiert sind. Das Thema IT-Sicherheit gilt noch immer als das weitaus größte Hindernis für den Einzug von Industrie 4.0 in die produzierenden Betriebe Deutschlands. Obwohl IT-Sicherheit sich in der Öffentlichkeit und in der Wirtschaft längst als wichtiges Thema etabliert hat und das Bewusstsein bezüglich der potenziellen Risiken weit verbreitet erscheint, muss man konstatieren, dass insbesondere kleine und mittlere Industrieunternehmen (KMU) bei der Umsetzung entsprechender Vorkehrungen einen deutlichen Nachholbedarf aufweisen.

Neue Risiken und Herausforderungen ergeben sich aus den folgen vier Kerneigenschaften von Industrie 4.0:

1. Die **Vernetzung von Industrieanlagen** und deren Komponenten wird künftig nicht nur organisations- und länderübergreifender, sondern vor allem auch dynamischer stattfinden als bisher. Um die IT-Sicherheit zu gewährleisten, muss eine belastbare Grundlage von Vertrauen und Verlässlichkeit geschaffen werden, die sich über alle Teilnehmer der Wertschöpfungsnetzwerke erstreckt.

2. Die **Menge an Daten**, die innerhalb der Kommunikation absichtlich mitgeteilt oder zugänglich gemacht werden, nimmt zu. Darunter befinden sich auch solche Daten, die nicht nur aus Sicht eines einzelnen Unternehmens als Geschäftsgeheimnis gelten, sondern an die aufgrund staatlicher Vorgaben eine besonders hohe Anforderung an die Vertraulichkeit besteht.

3. Entscheidungen werden bei Industrie 4.0 zunehmend von **autonomen Systemen** getroffen. Diese IT-sicherheitsrelevanten Entscheidungen und die daraus resultierenden Änderungen von Abläufen und Teilnehmer-Konfigurationen können sich aufgrund von Ereignissen aus unterschiedlichsten Domänen und Partnersystemen ergeben sowie aus der Analyse von Daten aus unterschiedlichsten Quellen. [1]

4. Die Integration von immer neuen, **externen Elementen** wie Zulieferer, Logistiker, Entwickler, Wartungspersonal für Maschinen, Steuerungssysteme (wie ICS / SCADA) in die digitale Wertschöpfungskette schafft auch immer neue Angriffspunkte. Zusätzlich werden laut Gartner 90% der industriellen Systeme bis 2025 mit dem Internet verbunden sein.

[1] Studie „IT-Sicherheit für die Industrie 4.0“, Bundesministerium für Wirtschaft und Energie

Der Begriff Industrie 4.0 steht für die vierte industrielle Revolution, einer neuen Stufe der Organisation und Steuerung der gesamten Wertschöpfungskette über den Lebenszyklus von Produkten. Dieser Zyklus orientiert sich an den zunehmend individualisierten Kundenwünschen und erstreckt sich von der Idee, dem Auftrag über die Entwicklung und Fertigung, die Auslieferung eines Produkts an den Endkunden bis hin zum Recycling, einschließlich der damit verbundenen Dienstleistungen. Basis ist die Verfügbarkeit aller relevanten Informationen in Echtzeit durch Vernetzung aller an der Wertschöpfung beteiligten Instanzen sowie die Fähigkeit aus den Daten den zu jedem Zeitpunkt optimalen Wertschöpfungsfluss abzuleiten.[2]

Industrie 4.0 steckt in vielen Unternehmen noch in den Kinderschuhen. Eine zentrale Herausforderung ist die Fähigkeit der Industrie 4.0-Systemarchitektur, sich an Änderungen anzupassen. Neue Anlagen oder Produktionsprozesse werden in das System und deren Netzwerk eingebracht oder bestehende Produktionssysteme und zugehörige Netzwerke verändert und nach außen geöffnet. Eine wesentliche Veränderung durch Industrie 4.0 ist die Entstehung von dynamischen, echtzeitoptimierten und sich selbst organisierenden, unternehmensübergreifenden Ad-hoc-Wertschöpfungsnetzwerken.

Hauptcharakteristika der Industrie 4.0-Systeme sind hierbei die:

- Ab- bzw. Auflösung der klassischen Automatisierungspyramide
- Verteilung der Prozesse auf verschiedene Akteure
- hohe Dynamik der Kooperationsdauer der im Prozess beteiligten Partner
- unterschiedliche technologische, betrieblich-organisatorische wie auch rechtliche Ausgangslagen bei den Partnern: sehr kleine Unternehmen (wie z. B. ein zwei bis-fünf-Mitarbeiter-Ingenieurbüro) und international agierende Großkonzerne

Die Ablösung der klassischen Automatisierungspyramide und die Verteilung des Prozesses auf verschiedene Akteure führen zu neuen Herausforderungen hinsichtlich der IT-Sicherheit und bedingen neue Abläufe beim IT-Sicherheitsmanagement, die nun über die Unternehmensgrenzen hinweg etabliert werden müssen. Unternehmensübergreifende Bedrohungsanalysen und Vertrauensbeziehungen werden notwendig. Es sind Fragen zu beantworten wie bspw.:

- Wie soll IT-Sicherheitsmanagement in einem Ad-hoc-Wertschöpfungsnetz gestaltet werden?
- Bei wem liegt die Verantwortung/Haftung für die Gewährleistung der IT-Sicherheit in einem Wertschöpfungsnetzwerk?

[2] Umsetzungsstrategie Industrie 4.0 – Ergebnisbericht der Plattform Industrie 4.0, April 2015

• Müssen die beteiligten Akteure bestimmte IT-Sicherheitsmaßnahmen umsetzen, um ein Teil eines Wertschöpfungsnetzes zu werden?

• Oder können die IT-Sicherheitsmaßnahmen an externe Dienstleister übertragen werden? Unter welchen Voraussetzungen?

• Welche Auswirkungen haben die dynamischen Kooperationsbeziehungen in einem Wertschöpfungsnetzwerk auf die klassischen IT-Sicherheits-Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität?

  o Wie ist die Ausfallsicherheit der Produktionsanlagen zu bewerten? (Verfügbarkeit)

  o Wie ist die Echtzeitverarbeitung der produktionsrelevanten Daten zu bewerten? (Verfügbarkeit)

  o Wie ist die funktionale Sicherheit hinsichtlich der Integrität eines Systems sowie die Verfügbarkeit von Sicherheitsfunktionen zu bewerten?

• Kommen neue Schutzziele durch Industrie 4.0 hinzu?

• Welche organisatorischen, rechtlichen und technologischen Rahmenbedingungen müssen für die dynamischen, unternehmensübergreifenden und vor allen Dingen sicheren Wertschöpfungsnetzwerke geschaffen werden, um die genannten Schutzziele zu erreichen?

• Welche neuen Anforderungen, z. B. hinsichtlich Benutzerfreundlichkeit, entstehen durch Industrie 4.0?[1]

Mit dem Begriff „Industrie 4.0" verbindet sich eine Entwicklung in der industriellen Produktion und der dafür erforderlichen Gestaltung der Wertschöpfungsketten, die wesentlich durch den zunehmenden Vernetzungsgrad und durch zunehmend autonomes Agieren von Maschinen gekennzeichnet ist. Was die IT-Sicherheit angeht, entsteht dadurch in der Automatisierungsindustrie und Logistik nicht etwa ein neues Problem: Die Bedrohungen werden jedoch vielfältiger und die Risiken erhöhen oder verändern sich. Bereits heute existieren Kommunikationsbeziehungen zwischen den Ebenen der so genannten Automatisierungspyramide (siehe Abbildung 1) und zwischen den Komponenten untereinander. Und die Komponenten und deren Kommunikationskanäle sind angreifbar.

Insgesamt setzt der Trend zur Industrie 4.0 Unternehmen deswegen Bedrohungen aus, da er industrielle Systeme nach außen öffnet. Bisher funktionierten diese traditionell als Insellösung. Jede Sicherheitsverletzung oder IT-Störung kann jedoch durch die zunehmende Vernetzung den Produktionsprozess zum Stillstand bringen. Das Personal, das diese Systeme verwaltet, ist möglicherweise nicht genug mit den Risiken durch Vernetzung vertraut, um eine entsprechende Absicherung zu gewährleisten.

[1] Studie „IT-Sicherheit für die Industrie 4.0", Bundesministerium für Wirtschaft und Energie

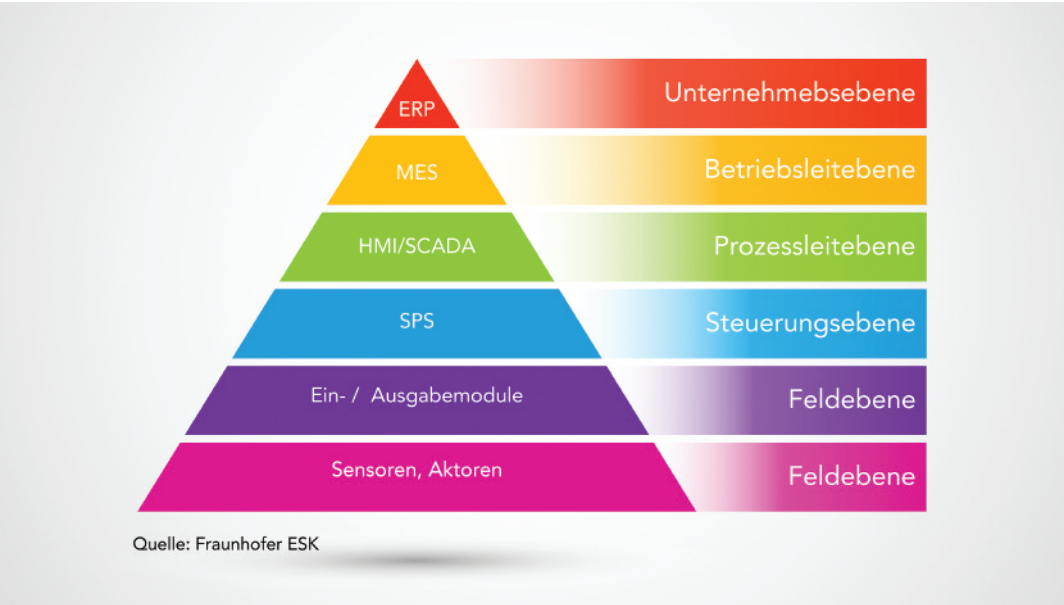


Abbildung 1

Die Herausforderungen in der vernetzten Industrie – was treibt OT und IT Sorgenfalten ins Gesicht?

Die Informationstechnologie (IT) und Operationale Technologie (OT) waren in der Vergangenheit getrennte Bereiche. In friedlicher Koexistenz erledigten sie ihre jeweiligen Aufgaben. Anknüpfungspunkte zwischen beiden Fachbereichen gab es kaum. Das ändert sich in der Ära des Internets der Dinge radikal. IT und OT sollen und müssen jetzt nahtlos ineinandergreifen. Die OT war bislang auf Produktions- und Industrieanlagen konzentriert – allerdings in der Regel in geschlossenen Systemen, ohne Anbindung an das Internet. Sie war darauf ausgerichtet, in erster Linie die Verfügbarkeit der Anlagen zu gewährleisten. Die IT hingegen hat weit mehr Erfahrung und Berührungspunkte mit dem Internet vorzuweisen. Die IT befasst sich klassischerweise mit dem gesamten Spektrum an Technologien zur Datenverarbeitung, wie Software, Hardware, Kommunikationstechnologien und damit verbundene Services. Darüber hinaus ist sie so konzeptioniert, um Datensicherheit zu maximieren. IT-Teams haben dafür wenig Erfahrung mit industriellen Systemen, kennen sich zum Beispiel mit Anlagen unter Starkstrom nicht aus. Eine enge Zusammenarbeit wäre also die Ideallösung. Allerdings arbeiten beide Bereiche noch immer eher nebeneinander als miteinander. Ein Beispiel: Nach wie vor speisen viele Unternehmen ihre Produktionsdaten nicht in die Unternehmenssysteme ein. Genau diese Integration aber ist notwendig, um die Chancen von IoT nutzen zu können. Ein weiteres Beispiel: Unternehmen, deren Produktionsdaten mit


“Ein gekaperter privilegierter Account ermöglicht legale Zugriffe & Aktionen durch eine fremde Person.”

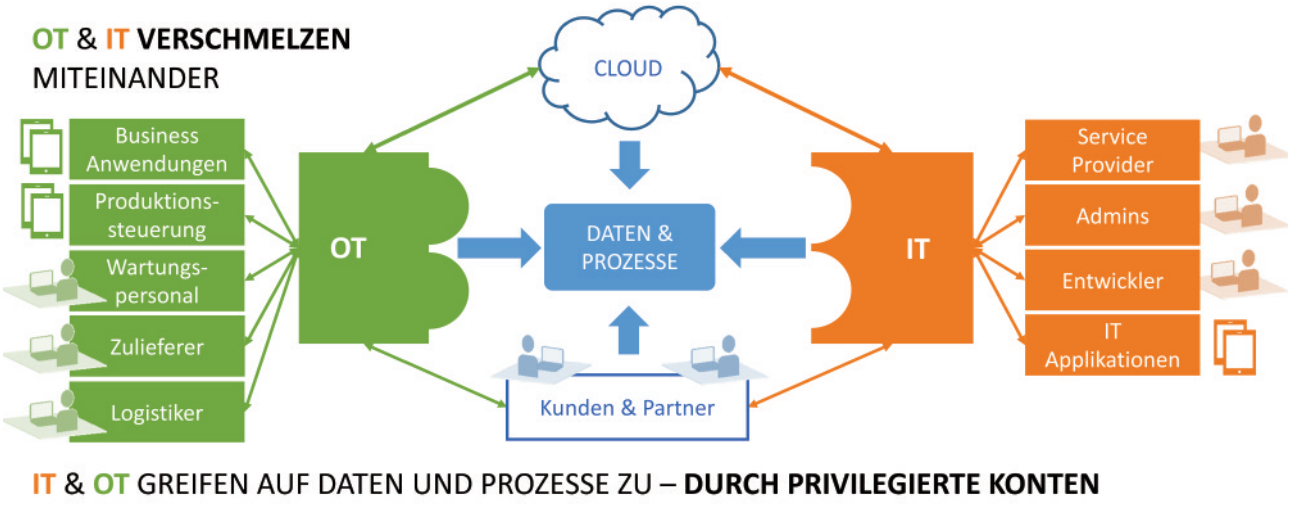


Abbildung 2

modernen Big Data Systemen arbeiten und analysiert werden, können auf Basis dieser Ergebnisse gezielt Produktivitätsverbesserungen durchführen.

Und noch ein anderes Beispiel: Im Bereich der IT werden Patches schnell zur Verfügung gestellt und oft automatisch eingespielt. Hier geht es auch darum, sich gegen neue Angriffsszenarien schnell zu schützen. Wenn ein Betriebssystem oder eine Anwendung aus der Wartung des Herstellers genommen wird, ist es für die Kunden meist auch der späteste Zeitpunkt, an dem auf neue Releases migriert wird. Ganz anders in der OT: Hier sind Steuerungssysteme oft mehr als 20 Jahre im Einsatz und alte Hardware als Ersatz wird zu hohen Preisen gehandelt. Also steht der zuverlässige Betrieb im Vordergrund und ein Patch wird zunächst einmal als mögliches Risiko betrachtet. Deshalb ist bisher, auch durch die historische Trennung solcher Umgebungen in der Netzwerk-Infrastruktur, der Umgang mit Patches ein völlig anderer als in der IT.

Eine simple Antwort auf die Frage, wie OT und IT in Sicherheitsfragen zueinander finden, gibt es nicht, aber das Thema muss eine hohe Priorität bei der Diskussion über vernetzte Produktion haben – es geht um jede Form von Sicherheit. Der erste Schritt ist, dass sich die Sicherheitsexperten aus den OT- und IT-Umgebungen verständigen und beginnen, an gemeinsamen Sicherheitskonzepten zu arbeiten. Vernetzte Produktion ist nur dann ein Erfolgsmodell, wenn sie auch sicher ist. Um produktiv, effizient und erfolgreich im Zeitalter des IoT zu arbeiten, ist die Zusammenarbeit von IT und OT unerlässlich.

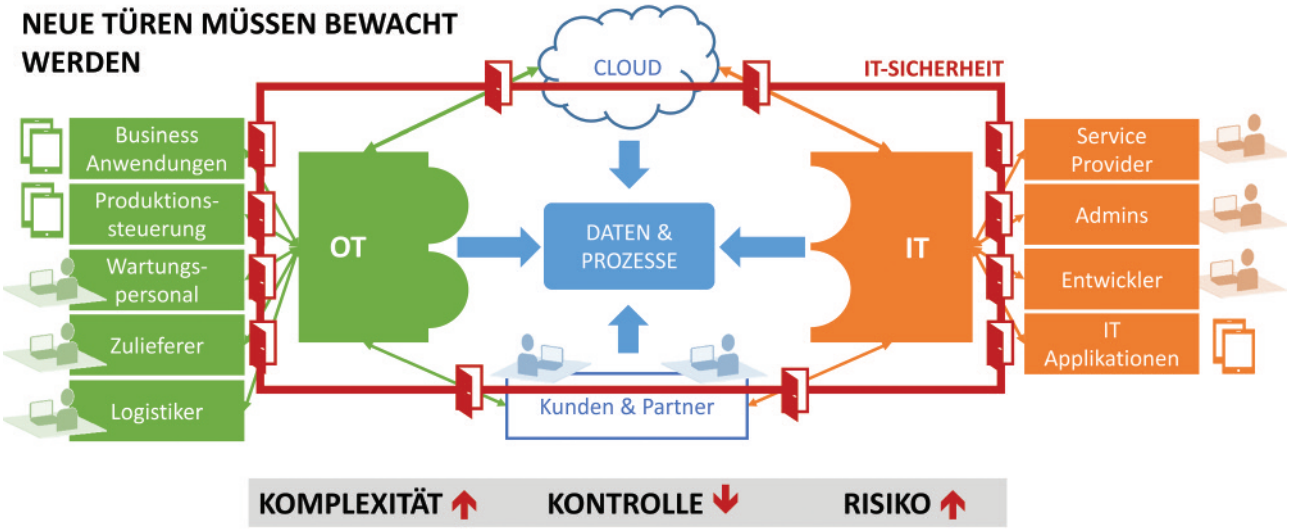


Abbildung 3

Privileged Access Management minimiert Schwachstellen

Die meisten Cyber-Angriffe basieren in irgendeiner Weise auf dem Diebstahl privilegierter Anmeldeinformationen. Tatsächlich sind es sogar sagenhafte 80% der gesamten IT-Verstöße, bei denen der Missbrauch von bevorrechtigten Anmeldeinformationen eine entscheidende Rolle spielt – wie ein kürzlich veröffentlichter Forrester-Report aufzeigt. 74% aller Datenschutzverletzungen erfolgten dem Ponemon Institut zufolge aufgrund von Identitätsdiebstahl. Es gibt einen simplen Grund dafür, dass privilegierte Zugänge mittlerweile zum Hauptangriffsziel von Cyber Attacken geworden sind: Sie stellen den einfachsten und schnellsten Weg in ein IT-System dar, um dort dann sensible Daten zu stehlen. Traditionelle Sicherheitslösungen bieten hier keinen Schutz. Die Krux an der Sache ist, dass Unternehmen mit privilegierten Zugängen ihre Zugriffsrechte effizient und sicher managen wollen – dabei wird diese Zielscheibe oft sträflich unterschätzt!

	Privat	Business
Situation	Haustürschlüssel gelangt in die Hände einer fremden Person mit Kenntnis des Wohnsitzes.	Privilegierter Account gelangt in die Hände eines internen/externen Angreifers
Ergebnis	**Legaler Zugriff** durch passenden Schlüssel auf ein fremdes Haus durch eine **illegale Person**.	**Legaler Zugriff** auf die entsprechenden Systeme, Daten, Produktionsumgebungen etc. durch eine **illegale Person**.
Fazit	Türschlösser verhindern keinen legalen Zutritt sondern ermöglichen den lautlosen Zugang ohne Aufmerksamkeit zu erregen und somit den Diebstahl von Persönlichen Dingen und Wertsachen.	Vorhandene Security Lösungen stoppen keine legalen Zugriffe & ermöglichen die unbemerkte Manipulation von Produktionsumgebungen sowie den Abfluss von personenbezogenen Daten und unternehmenskritischen Daten.

Abbildung 4

Die Kontrolle und Dokumentation der Aktionen, die von privilegierten Konten aus durchgeführt werden, ist von ganz zentraler Bedeutung für die Gewährleistung der Sicherheit sowie die Einhaltung von Vorschriften und den Schutz der öffentlichen Sicherheit.

Bei dem berühmt-berüchtigten Datendiebstahl von 2014 bei Target verschafften sich die Hacker ganz offensichtlich mit gestohlenen Anmeldedaten Zugang zum Unternehmen. Diese Anmeldedaten stammten von einer Firma, die HVAC-Dienste für Target zulieferte. Die Hacker eskalierten diese ursprünglichen Privilegien bis auf die Randbereiche des Netzwerks und erhielten so Zugang zu den Zahlungssystemen.

An diesem Beispiel lässt sich sehr schön aufzeigen, bei welchem Kernproblem PAM-Systeme ansetzen: Passwörter nämlich, die entweder an sich schon unsicher sind oder die an Auftragnehmer von dritter Seite vergeben werden. Wäre im beschriebenen Fall eine PAM-Lösung im Einsatz gewesen, hätte der Auftragnehmer nicht einmal das Geräte-Passwort gekannt… und niemand hätte demzufolge überhaupt die Gelegenheit gehabt, dieses Passwort zu stehlen. Der Zugang wäre routinemäßig gewechselt und überwacht worden. Und selbstverständlich wären die fraglichen Passwörter Gegenstand der gleichen Überwachung, Verwaltung und Gegenstand der gleichen Audit-Anforderung gewesen, wie alle privilegierten Anwender auch. All das wäre mehr als ausreichend gewesen, um diesen Angriff zu stoppen, noch bevor er überhaupt gestartet worden wäre.

Bedrohungen durch Bevorrechtigte, Insider und von dritter Seite

Es gibt drei grundlegende Typen von Bedrohungen durch Insider:

- Vorsätzlich Handelnde – Diese Personen führen ihre Insider-Attacken vorsätzlich und aus niederen Beweggründen aus.
- Unabsichtlich Handelnde – Damit sind Nachlässigkeiten (ohne Vorsatz) wie die Weitergabe von Passwörtern gemeint.
- Kompromittierte Insider – Hier handelt es sich um Systemnutzer, deren Zugangsrechte von Dritten gestohlen wurden, oftmals ohne jedwedes Insider-Wissen. Erreicht wird dieser Zugangsdatenklau üblicherweise durch Phishing oder ähnlich gelagerte Attacken.

Diese drei Angriffsarten können sich auch überschneiden. Ein planvoller Angreifer von Innen wird sehr wahrscheinlich in erster Instanz nach unabsichtlich Handelnden Ausschau halten, dessen Anmeldedaten er nutzen kann. Und der unabsichtliche Akteur von gestern wird zum kompromittierten Insider von heute, sobald die Hacker erst einmal die erbeutete Info vollumfänglich ausgeschlachtet haben.

Wir können die neuen Sicherheitsrisiken kontrolliert werden

- Zugriffsregeln festlegen (WER darf WAS, WANN, WIE machen?)
- kein direkter Remote-Zugang mehr auf das Zielsystem
- ein zentraler Zugang für privilegierte Konten statt viele Zugänge
- privilegierte User kennen keine Passwörter auf Zielsystemen mehr
- starke Authentifizierung privilegierter User
- Überführung von Account-basierten Privilegien zu Rollen-basierten Privilegien
- Umsetzen von Berechtigungsworkflows
- Zugang ausschließlich zu berechtigten Systemen möglich
(siehe DSGVO Artikel 29; ISO27001 A.5;A.9;A.18)
- nur noch autorisierte Tätigkeiten sind erlaubt
- vollständige personalisierte Nachvollziehbarkeit und Auditierbarkeit sämtlicher Aktivitäten während einer privilegierten Sitzung gewährleisten (siehe DSGVO Artikel 15; ISO27001 A.6;A.9;A.12)

Privilegierte Accounts

Wenn Insider-Bedrohungen die primäre Quelle von Angriffen sind, dann verläuft die primäre Angriffslinie durch bevorrechtigte (privilegierte) Accounts, könnte man sagen. Denn Accounts mit besonderen Rechten stellen im wahrsten Sinne des Wortes den Generalschlüssel zum gesamtenIT-Königreich dar.

Privilegierte Nutzer verfügen üblicherweise über Administrator- und Root-Berechtigungen wie beispielsweise

- das Recht, die System-Konfigurationen zu ändern
- den Zugriff auf Installations-Software
- die Berechtigung, Nutzer neu anzulegen oder die Berechtigungen zu ändern
- die Berechtigung auf gesicherte Daten zuzugreifen oder sie zu ändern
- die Möglichkeit, Privilegien-Stufen für andere oder sich selbst zu verwalten.

Diese Berechtigungen sind unabdingbar für System-Updates und Wartungsaufgaben. Allerdings bringen es diese Privilegien auch mit sich, dass der Inhaber typischerweise in der Lage ist, sich über bestehende Sicherheitsprotokolle hinweg zu setzen. Das ist dann genau die Schwachstelle, die böswillige Anwender ausnutzen, um unerlaubte Systemänderungen vorzunehmen, auf gesperrte Daten zuzugreifen und/oder ihre Aktionen zu verschleiern.

Je umfangreicher und komplexer ein System wird, desto mehr privilegierte Nutzer sind erforderlich. Diese Anwender können beispielsweise Angestellte sein, Auftragsnehmer, Personen, die remote zugreifen oder sogar maschinelle Nutzer. Für die meisten Unternehmen ist es schier unmöglich, all diese Nutzer effektiv – oder etwa händisch zu verwalten und zu überwachen.

Man stelle sich vor: Nicht wenige Unternehmen haben mehr privilegierte Nutzer als Mitarbeiter!

Privileged Account Management (PAM)

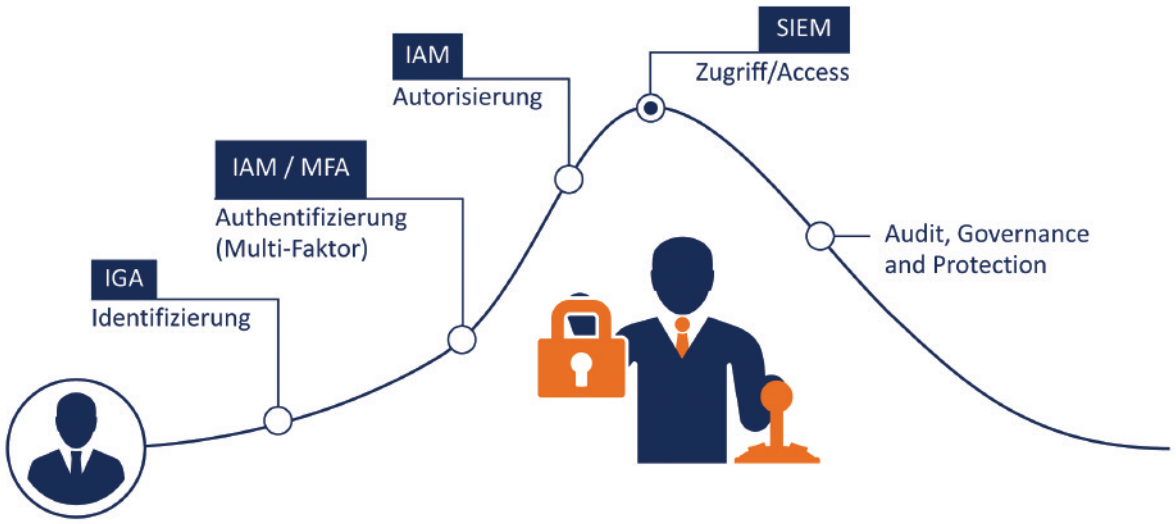
All das hat zu einem exponentiellen Wachstum im Bereich der „Privileged Account Management" Software geführt. Folgt man Gartner, dann wächst diese Branche um rund 33 Prozent jedes Jahr.

PAM bietet schnelle und sichere Autorisation, Neu-Bevollmächtigung sowie die Überwachung aller privilegierten Nutzer. PAM unterstützt darüber hinaus Policies, die verhindern, dass privilegierte Nutzer Sicherheitssystem außer Kraft setzen. Das Ziel besteht nicht nur darin, Schutz vor Bedrohungen von innen zu bieten, sondern darüber hinaus auch Außenseiter abzuwehren, die erweiterten privilegierten Zugang suchen.

Wie funktioniert PAM?

PAM ermöglicht

- die Vergabe von Privilegien an Nutzer ausschließlich für diejenigen Systeme, für die sie berechtigt sind
- die Vergabe von Zugangsrechten immer nur dann, wenn sie benötigt werden und den prompten Entzug, sobald die Notwendigkeit nicht mehr gegeben ist
- die Löschung direkter/lokaler System-Passwörter für privilegierte Nutzer
- die zentrale Zugangsverwaltung über ein disparates Set heterogener Systeme
- die Schaffung eines unveränderlichen Protokolls für alle privilegierten Vorgänge



Die blauen Kästchen (IGA, MFA, IAM, SIEM) stehen für die Integration mit anderen Security-Komponenten, um maximale Sicherheit zu ermöglichen.

Zusammenfassend begleitet PAM den kompletten Aktionsradius einer privilegierten Identität über die gesamte Digital Journey in jedem beliebigen Einsatzgebiet. Dazu gehören:

1. Identifizierung
2. Authentifizierung
3. Autorisierung
4. den Zugriff selbst
5. Auditierung, Governance und Nachvollziehbarkeit

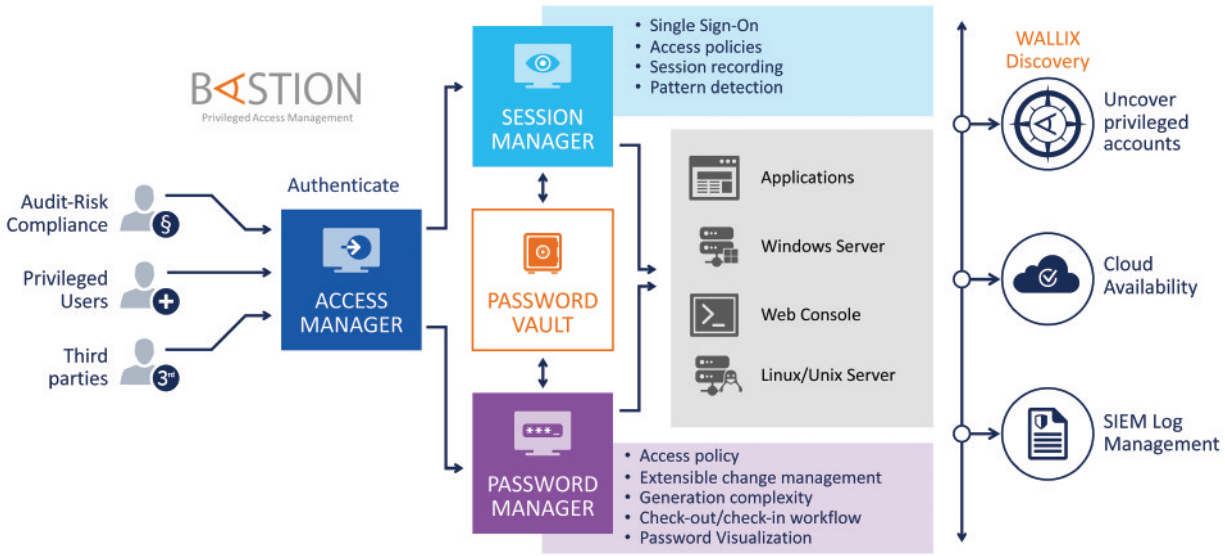
Die Komponenten einer PAM-Lösung

• Zugangs-Manager

Dieses Feature regelt den Zugriff auf privilegierte Konten über einen einzelnen Punkt und über die klare Definition und Durchsetzung von Policies für das privilegierte Account-Management. Ein übergeordneter Administrator (ein sogenannter Super-Admin) kann als Acces Manager in einem zentralisierten System privilegierte Nutzer-Accounts entweder neu aufsetzen, modifizieren oder löschen – dadurch wird die Effizienz bei diesen Abläufen deutlich verbessert und die unterschiedlichen Compliance-Levels werden effektiver umgesetzt.

• Session-Manager

Die Funktion verfolgt und überwacht alle Maßnahmen, die während einer Sitzung mit privilegierten Konten ergriffen werden, damit sie für spätere Prüfungen oder Audits nachvollzogen werden können. Darüber hinaus können einige Systeme sogar böswilligen oder nicht autorisierten Maßnahmen vorbeugen und Super-



Admins alarmieren, falls verdächtige Aktivitäten entdeckt werden.

• Tresore für Passwörter/Passwort-Manager

Passwörter sollten in einem sicheren und zertifizierten, virtuellen „Tresor" aufbewahrt werden. Jedweder System-Zugang sollte über den Passwort-Tresor laufen. So ist sichergestellt, dass Endanwender niemals direkten Zugriff auf Root-Passwörter erhalten.

Wallix sichert Ihre Industrieanlagen!

Die Wallix PAM-Lösung bietet eine Reihe von Funktionen, die sich auf die Risiken des privilegierten Zugriffs in Industrie-4.0-Umgebungen beziehen. Der Betrieb vor Ort oder auf Cloud-Ebene automatisiert den Schutz der Netzwerke vor Hackern und anderen externen Bedrohungen. IT-Administratoren brauchen ein zentrales Werkzeug zur Durchsetzung und Verwaltung von Richtlinien, egal wie viele verbundene Geräte und Endpunkte ihr Netzwerk umfasst. Wallix bietet seinen Kunden genau diesen Ansatz. Die Lösung enthält einen Password Manager und Session Manager. Beide bieten eine kontinuierliche Verteidigung gegen Bedrohungen auf dem Gebiet der Zugangskontrolle in Verbindung mit Cloud-Diensten, externer Anwendungsnutzung und Nutzern dritter Parteien, die sich überall befinden können.

Durch ihre vereinfachte Installation, Nutzung und Kontrolle profitieren Industriebetriebe sehr schnell von der Wallix PAM-Lösung. An ständige Veränderung passt sie sich dank ihrer

agentenlosen Architektur an. Diese schließt zudem Schwierigkeiten bei der Installation von dedizierten Software-Agenten auf einzelnen Systemen aus. Industrie-4.0-Umgebungen sind dynamisch und gegenseitig abhängig. Daher stellt dies einen entscheidenden Vorteil für die Sicherheit dar.

Wallix gehört zu den führenden Anbietern von PAM-Lösungen, die für den industriellen Einsatz maßgeschneidert sind. Industrieunternehmen verfügen über derart hochkomplexe IT-Umgebungen, dass sie eine gradlinige Lösung brauchen, die mit all ihren on premise aufgesetzten, cloudbasierten und hybriden System, die oft auch noch über mehrere Standorte weltweit verteilt sind und darüber hinaus von zahlreichen Angestellten ebenso wie von Auftragsnehmern von dritter Seite genutzt werden, nahtlos zusammen arbeitet.

Warum auf Wallix setzen?

WALLIX ist ein europäischer Anbieter,

Schnörkellose Architektur

Der Betriebsablauf bei Industrieunternehmen ist schlicht zu komplex und schnelllebig, um von PAM-Lösungen profitieren zu können, die sich nur unter großem Aufwand implementieren und betreiben lassen. Die Architektur von Wallix ist ausgesprochen geradlinig aufgebaut, wodurch es vergleichsweise einfach ist, die Lösung zu implementieren und anzupassen. Wallix lässt sich unkompliziert in bestehende Verzeichnisdienste und Zielanwendungen integrieren, da es agentenlos arbeitet und REST-Webdienste nutzt. Selbst wenn kundenseitig Konfigurationen und Integrationen mit einer Vielzahl von Altsystemen vorliegen, besteht dennoch wenig Bedarf an kostenaufwändigen professionellem Service um das Roll-Out auf den Weg zu bringen.

Schnelle Implementierung

Die agentenlose Architektur der „Wallix-Bastion“ ermöglicht eine vereinfachte Einrichtung, die mit sehr viel weniger Systemkonflikten und Ausfallzeiten bei der Implementierung und Anpassung der PAM-Lösung einhergeht. Viele PAM-Lösungen erfordern einen dezidierten Software-Agenten auf jedem administrierten Endgerät oder Workstation. Das allerdings verlangsamt unvermeidbar den Implementierungsprozess und dann später auch das Management und die finale Anpassung. Im Gegensatz dazu ist Wallix normalerweise binnen ein oder zwei Tagen vollständig implementiert und im Betriebsmodus.

Dank der schnellen und effizienten Einrichtungsroutinen bei Wallix brauchen Unternehmen nicht zu befürchten, in die weit verbreitete Falle zu tappen, in zeitaufwändige, teure und komplexe Roll-Out-Prozesse investiert zu haben, nur um dann festzustellen, dass die tatsächliche Nutzung nur schwer und unter hohem Aufwand möglich oder sogar ganz unmöglich ist. Genau dieses Szenario hat bereits unzählige hochkarätige Unternehmen während ihrer Implementierungs-Odyssee ernsthaften Bedrohungen ausgesetzt. Darüber hinaus gibt Wallix seinen Kunden

verschiedene Implementierungs-Optionen zur Auswahl an die Hand. Die PAM-Lösung funktioniert gleichermaßen in der Cloud, on premise oder als gehostetes Einsatzszenario.

Benutzerfreundlichkeit für allgegenwärtige Nutzung

Wallix erleichtert die flächendeckende Nutzung von PAM durch den Bedienkomfort. Wallix bietet ein einziges HTML 5-basiertes Portal, in dem die Administratoren sehr einfach den Zugang für privilegierte Nutzer festlegen können, ebenso wie die Definition der jeweils verfügbaren Systeme und Protokolle. Diese Herangehensweise vereinfacht die Verwaltung ebenso wie es für die Anwender auf diese Weise sehr viel leichter nachzuvollziehen ist, wer mit einem einfachen Klick eine Session starten kann.

Flexible Authentifizierung

Wallix kommt mit einem integrierten „Passwort-Tresor für die Authentifizierung", der auch mit LDAP, LDAPs Active Directory, Radius und TACACS+ zusammen arbeitet und darüber hinaus die Fähigkeit besitzt, sich mit jeder bereits bestehenden Authentifizierungslösung Dritter zu verbinden.

Verfügbarkeit

Wallix bietet eine vollständige mandantenfähige Umgebung mit dem Einsatz von WAB Access Manager und WAB-Clustern. Wallix kann auch mit Load Balancern wie F5, BIG IP und A10 Thundera Application Delivery Controllern integriert werden.

Die Bastion ist auch auf dem Azure Marketplace wie auch via AWS erhältlich.

Audits und Compliance-Vorgaben

Wie Hacker auch, richten Auditoren und Regulierungsbehörden ihre Aufmerksamkeit vermehrt auf Versorgungsunternehmen und Netzsicherheit. Regulatorische Rahmenbedingungen wie NERC CIP, NIST, SOX, und PCI DSS, gar nicht erst zu reden von Qualitätsstandards wie ISO 20071, erfordern alle eine grundlegende und umfassende Auseinandersetzung seitens dieser Organisationen mit dem Thema Cyber Security. Und, nicht zu vergessen: Die Unternehmen müssen in der Lage sein, die Einhaltung der Compliance-Vorgaben im Falle eines Audits auch zu beweisen!

Wallix zeichnet fortlaufend die Sessions bevorzugter Accounts auf zuvor definierten Zielgeräten auf und legt so einen über jeden Zweifel erhabenen Audit-Trail an. Diese Session-Protokolle enthalten auch die Kommandozeilen der Sitzungen (SSH, Telnet, rsh) und die graphischen Sessions der Windows Terminal Server (RDP). Administratoren können die Sessions entweder in Echtzeit überwachen oder bei Bedarf alle aufgezeichneten Sitzungen anschauen bzw. gezielt durchsuchen. Die RDP-Sessions werden via OCR analysiert, damit sich der Content hinterher auf zweckdienliche Weise durchsuchen lässt.

Weitere Informationen über die Möglichkeiten von Wallix bei besonderen regulatorischen Anforderungen gibt es auf Anfrage. Wir haben detaillierte Leitfäden zum Thema Compliance, die alle wichtigen regulatorischen Rahmenbedingungen behandeln.

Wallix lässt sich auch zur Verbesserung der Sicherheitsanalysen von SIEM-Lösungen einsetzen: Relevante Logs werden einfach integriert und an Lösungen wie LogRhythm, Splunk, Tibco LogLogic, ArcSight und andere weitergeleitet und ausgewertet.

Ebenfalls können Lösungen zu Identity & Access Management (IAM), Mutifaktor-Authentifizierung (MFA) oder Vulnerability Management integriert werden, um den Zugriff auf kritische Assets noch sicherer und messbarer zu machen.

Fazit

Das Thema vernetzte Industrie ist hochkomplex, weil zwei Welten und damit Formen des Security-Verständnisses aufeinander treffen. OT und IT müssen aber gerade in Fragen der Sicherheit zusammenspielen, wenn sie das volle Potentzial neuer Technologien nutzen wollen. Hier gilt es Technologien einzusetzen, die beide Welten miteinander verschmelzen lassen. Die PAM-Lösung von Wallix ist ein Beispiel für eine „State of the art"-Technologielösung, welche die komplexen Sicherheitsanforderungen von OT und IT gleichermaßen lösen kann und dabei allen rechtlichen Anforderungen an Industriestandards, -normen und Regularien entspricht!

über WALLIX

Die WALLIX Group ist ein europäischer Anbieter von Softwarelösungen für Cybersicherheit und Spezialist für die Verwaltung privilegierter Konten. Die Produkte und Lösungen von WALLIX unterstützen die Anwender beim Schutz ihrer kritischen IT-Ressourcen. Damit liefern sie eine Antwort auf die jüngsten regulatorischen Veränderungen (NIS/DSGVO in Europa und OVIs in Frankreich) und die Cybersicherheitsbedrohungen, von denen heute alle Unternehmen betroffen sind.

WWW.WALLIX.COM

WALLIX
CYBERSECURITY SIMPLIFIED