

WHITEPAPER

Schutz der Fertigung durch Sicherheit auf höchstem Niveau

Wechseln Sie zu passwortlosen Lösungen, gewährleisten Sie die Produktintegrität, sichern Sie Ihre Lieferkette und vermeiden Sie Ausfallzeiten



Inhalt

- 2 Inhaltsverzeichnis
- 3 Sicherstellung der Widerstandsfähigkeit in der Fertigung: Umgang mit der doppelten Realität der KI
- 6 Modernisierung der MFA und passwortlose Nutzung für sicheren Benutzerzugriff auf kritische Systeme und Daten
 - 6 Wichtige Überlegungen zur Authentifizierung in IT- und OT-Umgebungen
 - 9 Nachteile der veralteten Authentifizierung
 - 10 Was ist Phishing-resistente Authentifizierung?
 - 10 Was sind Passkeys?
 - 11 Die Zukunft wird passwortlos sein
 - 12 Sichere Kommunikation zwischen Mensch und Maschine mit dem YubiKey
- 14 Sicherung der Fertigungslieferkette
 - 14 Schutz des Zugriffs durch Dritte
 - 14 Gewährleistung der höchsten Integrität Ihrer Produktteile
 - 15 Sichern von externem Code und Daten
 - 15 Sichere Maschine-zu-Maschine-Kommunikation mit dem YubiHSM 2
 - 16 Unterstützung für PKI-Umgebungen (Public Key Infrastructure)
- 17 Fallstudie: Sicherung der Systeme und Lieferkette bei Schneider Electric
- 18 Fallstudie: Mitsubishi Electric stärkt die globale Cybersicherheit mit dem YubiKey
- 18 Fallstudie: Eine portable Vertrauensbasis für EasyMile zur Sicherung autonomer Fahrzeuge
- 19 Schnelle und reibungslose Implementierung passwortloser Authentifizierung in großem Maßstab
- 20 Zusammenfassung

180.000+



Industrielle Steuerungs- und OT-Systeme sind jeden Monat dem Internet ausgesetzt.⁸

72 %



der Angriffe auf OT-Systeme nutzen den IT-Bereich als Einstiegspunkt.⁹

3.300



Industrieunternehmen hatten im Oktober 2025 Daten auf Ransomware-Leak-Seiten veröffentlicht.¹⁰

42 %



der Angriffe (z. B. Phishing, Malware, Ransomware) führten zu Betriebsausfällen, die sich auf den Umsatz auswirkten.¹¹

78 %



der CISOs geben an, dass KI-gestützte Cyberbedrohungen bereits erhebliche Auswirkungen auf ihre Unternehmen haben.¹²

Sicherstellung der Widerstandsfähigkeit in der Fertigung: Umgang mit der doppelten Realität der KI

Seit fünf Jahren in Folge ist die Fertigungsindustrie die am häufigsten angegriffene Branche weltweit und macht 27,7 % aller globalen Cybervorfälle aus.¹ Der Fertigungssektor ist nach wie vor ein Hauptziel für ausgeklügelte Malware, Ransomware, Phishing und Man-in-the-Middle-Angriffe (MitM). Grund für diese Fokussierung ist die zentrale Rolle der Branche in der globalen Lieferkette und ihr umfangreicher Bestand an informationsreichem geistigem Eigentum (IP – intellectual property). Zu diesem Druck kommt noch das Aufkommen der künstlichen Intelligenz (KI) hinzu, die als leistungsstarker geschäftlicher Wegbereiter für die Produktion dient, gleichzeitig aber auch von böswilligen Akteuren genutzt wird, um Angriffsvektoren noch wirkungsvoller zu machen. In ihren fortschrittlichsten Formen wird KI mittlerweile dazu genutzt, die Echtzeitkommunikation bei Phishing-Kampagnen zu automatisieren, was es selbst für die aufmerksamsten Mitarbeitenden immer schwieriger macht, zwischen echten und böswilligen Anfragen zu unterscheiden.

Da die Informationstechnologie (IT) und die Betriebstechnologie (OT – operational technology) immer weiter zusammenwachsen, nimmt die Komplexität zu, da ehemals isolierte Systeme mit dem Internet vernetzt werden. Tatsächlich ist das Ausmaß dieser Gefährdung beträchtlich: Monatlich sind über 180.000 industrielle Steuerungssysteme (ICS – industrial control systems) und OT-Umgebungen dem Internet ausgesetzt.² In diesem Umfeld ist ein „Secure-by-Design“-Ansatz nicht mehr nur optional – er ist von entscheidender Bedeutung. Der Aufstieg von softwaredefinierter Energieversorgung und agentenbasierter KI – also spezialisierten Agents, die die Produktion optimieren und Lieferketten autonom verwalten – bringt neue Risiken mit sich, die es erfordern, dass jeder potenzielle Zugangspunkt gegen unbefugten Zugriff abgesichert wird. Insbesondere können KI-Agenten mit privilegiertem Zugriff manipuliert werden, um erhebliche physische oder betriebliche Störungen auszulösen, was potenziell zu Schäden an Geräten oder einer Gefährdung von Menschenleben führen kann.

Die finanziellen Folgen aller durch Cyberangriffe verursachten Störungen sind enorm; Unternehmen aus der Fertigungsbranche müssen mit Kosten für Datenlecks in Höhe von durchschnittlich 5 Millionen \$³ rechnen, dazu kommt der potenzielle Verlust von geistigem Eigentum und der Produktintegrität. Die Folgen des Angriffs auf die Colonial Pipeline im Jahr 2021 sind nach wie vor eine eindringliche Mahnung, wie wichtig operative Widerstandsfähigkeit und Transparenz in der Lieferkette sind. Da ungeplante Ausfallzeiten der Branche schätzungsweise jährlich 50 Milliarden \$ kosten⁴ und 42 % aller Sicherheitsverletzungen zu Betriebsausfällen führen, die sich direkt auf den Umsatz auswirken⁵, ist die Absicherung sowohl der Mensch-zu-Maschine- als auch der Maschine-zu-Maschine-Kommunikation für die Geschäftskontinuität unerlässlich.

Zwar halten sich Unternehmen, die im Rahmen von Regierungsaufträgen tätig sind, schon seit Langem an strenge Standards wie FIPS, DFARS und ISO 9001, doch haben die jüngsten, viel beachteten Angriffe zu umfassenderen regulatorischen Anforderungen geführt. Im Januar 2026 haben die „Five Eyes“-Allianz, Deutschland und die Niederlande neue Leitlinien herausgegeben: die „Secure Connectivity Principles for OT“.⁶ Diese gemeinsamen Leitlinien betonen, dass die Vernetzung von IT und OT zwar unverzichtbar ist, aber nach einem „Secure-by-Design“-Modell erfolgen muss, bei dem die Absicherung der OT-Grenze durch den Einsatz einer Phishing-resistenten Authentifizierung im Vordergrund steht.

Warum verlagert sich der Fokus so stark auf die Phishing-resistente Multi-Faktor-Authentifizierung (MFA)? Die Realität ist, dass veraltete Lösungen – insbesondere Benutzernamen, Passwörter und Authentifizierung per Mobilgerät – gegen KI-gestützte Bedrohungen nicht mehr wirksam sind. Eine Untersuchung von 350.000 tatsächlichen Hijacking-Versuchen ergab, dass SMS-basierte Einmalpasswörter (OTP – one-time passwords) nur 76 % der gezielten Angriffe abwehrten, während Push-Benachrichtigungen 90 % abwehrten.⁷ Damit bleibt eine Durchbruchrate von mindestens 10 % – was bedeutet, dass bei veralteten MFA-Verfahren ein erfolgreicher Angriff nicht mehr die Frage ist, ob, sondern wann er stattfindet.

Fertigungsunternehmen erkennen die dringende Notwendigkeit, die Authentifizierung und Sicherheit in konvergenten IT- und OT-Umgebungen zu modernisieren. Diese Entwicklung ist nicht nur für einen nahtlosen Zugriff auf kritische Daten und Systeme unerlässlich, sondern auch für den Schutz der Integrität und des geistigen Eigentums jedes Bestandteils im Produktionslebenszyklus. Die beispiellose Geschwindigkeit von KI und die zunehmende Komplexität von Cyberbedrohungen haben jedoch zu einer Reihe einzigartiger Herausforderungen geführt, die sich auf diesen Sektor auswirken:

Herausforderungen in der Fertigungsbranche



**Veraltete
Infrastruktur**



**Agentenbasierte
KI und Autonomie**



**Gemeinsam genutzte
Arbeitsplätze**



**Raue Umgebungen,
in denen Handschuhe
getragen werden**



**Bereiche mit
Einschränkungen
für Mobilgeräte**



**Lieferketten-
Management**



**Probleme wegen
Unterbrechungen
im Arbeitsablauf**



**Integrität der
Produktkomponenten**



**Schutz des geistigen
Eigentums in der Fertigung
und Konstruktion**

Fertigungsabläufe sind oft auf veraltete Produktionsanlagen und Anwendungen angewiesen, was die Skalierbarkeit und Interoperabilität von modernen Sicherheitslösungen häufig beeinträchtigt. Außerdem entspricht die herkömmliche Trennung von Fertigungssystemen von Unternehmens-IT-Netzwerken durch eine physische Netztrennung nicht mehr der Realität der heutigen integrierten Fertigungsökosysteme.

Diese verbesserte Vernetzung hat den Weg für einen tiefgreifenden Wandel geebnet: den Übergang von menschlich ausgeführten Aufgaben hin zu autonomen Maschinen-zu-Maschinen-Abläufen. In einer Zeit, in der KI-Agents die Produktion und Lieferketten ohne ständige menschliche Eingriffe steuern, werden die Zugangspunkte dieser Agents zu bevorzugten Zielen für Cyberangriffe, die auf Seitwärtsbewegungen und die Eskalation von Privilegien abzielen. Die Absicherung dieser autonomen Grenzen durch hardwaregestützte Zugangsdaten ist mittlerweile entscheidend, um unbefugte Steuerungsmaßnahmen zu verhindern, die zu physischen Schäden oder umsatzbeeinträchtigenden Ausfällen führen könnten.

Umgebungen mit gemeinsam genutzten Arbeitsplätzen sind auch in der Fertigung üblich. Häufig werden dabei nicht unterstützte Betriebssysteme mit minimalen Kontrollen durch das Unternehmen und einem Mangel an definierten Zugriffsrechten verwendet. Die durchschnittliche angestellte Person in der Fertigung kann bereits an ihrem ersten Arbeitstag auf über 27.000 sensible Dateien zugreifen (z. B. Finanzdaten, Informationen zur Lieferkette, geistiges Eigentum).¹³ Die Authentifizierung kann eine erste Verteidigungslinie zum Schutz vor modernen Cyberbedrohungen darstellen, doch die Abhängigkeit von „veralteten Authentifizierungsmethoden wie Benutzername und Passwort sowie Authentifizierung per Mobilgerät kann Fertigungsunternehmen einem höheren Risiko von Sicherheitsverletzungen aussetzen.

70 %



der Cloud-Sicherheitsverletzungen entstehen aus kompromittierten Identitäten und nicht aus Softwarefehlern.¹⁴

60 %



der IT-Service-Desk-Interaktionen beziehen sich auf das Zurücksetzen von Passwörtern.¹⁶

Kompromittierte Zugangsdaten sind nach wie vor der häufigste Angriffseinstiegspunkt – 70 % der Cloud-Sicherheitsverletzungen gehen auf kompromittierte Identitäten zurück, nicht auf Softwarefehler.¹⁴ Passwörter können zudem die Kosten des IT-Helpdesks durch Passwortzurücksetzungen in die Höhe treiben. Der ideale Zustand ist der Übergang in eine passwortlose Zukunft, bei der Passwörter vollständig abgeschafft werden. Die durchschnittliche angestellte Person muss 191 Passwörter verwenden und sich diese merken, was zu Komplexität und Frustration der Benutzenden beiträgt.¹⁵ Für ein durchschnittliches Unternehmen sind derzeit etwa 60 % der Interaktionen mit dem IT-Service-Desk auf das Zurücksetzen von Passwörtern zurückzuführen.¹⁶ Abgesehen von den IT-Kosten verliert ein durchschnittliches Unternehmen jährlich 5,2 Millionen \$ an Produktivität aufgrund von Kontosperrungen.¹⁷

In der Fertigungsindustrie ist es entscheidend, die Echtheit aller Komponenten sicherzustellen, um unbefugte Nachahmung und Diebstahl zu vermeiden, aber auch zur Qualitätssicherung, da eine Fertigungslinie nur aus Produkten aus authentischen Quellen bestehen sollte, da das Ganze immer die Summe seiner Teile ist. Produktionslinien für verschiedene Produktkomponenten können sowohl aus verschiedenen Produktionsstätten als auch aus Drittanbieter-Produktionsanlagen auf der ganzen Welt stammen. Probleme bei der Produktintegrität können auftreten, wenn die Firmware der Komponenten nicht digital signiert und zertifiziert wird, um die Authentizität und Integrität der Komponenten am Ende der jeweiligen Produktionslinien sicherzustellen. Dies ist auch wichtig, um sicherzustellen, dass bei der Wartung oder dem Austausch durch einen Drittanbieter nur Originalkomponenten verwendet werden, um die Funktionsfähigkeit und Zuverlässigkeit des Geräts zu gewährleisten.

Fertigungsleiter benötigen zuverlässige Lösungen, die moderne Sicherheitsfunktionen bieten und gleichzeitig den nahtlosen Übergang zu einem passwortlosen Workflow ermöglichen. Diese Entwicklung ist von entscheidender Bedeutung, nicht nur für die Optimierung der User Experience und der Gesamteffizienz, sondern auch für die Stärkung des Unternehmens gegenüber der sich schnell entwickelnden Bedrohungslandschaft. Außerdem müssen diese Lösungen eine schnelle Bereitstellung in großem Maßstab ermöglichen, um die Qualität, Integrität und das geistige Eigentum jeder Komponente über den gesamten Lebenszyklus hinweg zu gewährleisten – von der ersten Produktion und Montage bis hin zu späteren Reparaturen und Austauschmaßnahmen. Um sicherzustellen, dass eine Fertigungslinie ein geschlossenes Ökosystem aus authentisch beschafften Produkten bleibt, müssen Unternehmen eine kryptografische Vertrauensbasis schaffen, die die gesamte Wertschöpfungskette schützt.





Sicherheit



Produktivität



Zuverlässigkeit



Langlebigkeit



Kosten

Modernisierung der MFA und passwortlose Nutzung für sicheren Benutzerzugriff auf kritische Systeme und Daten

Bei der Auswahl von Authentifizierungslösungen zur Verbesserung der Sicherheit von IT- und OT-Systemen in der Fertigung ist es wichtig zu prüfen, wie wirksam die Lösung beim Schutz vor externen Cyberangriffen, inklusive KI-gestützter, und Insider-Bedrohungen ist, wie sich die Lösung auf die Benutzerproduktivität auswirkt und wie zuverlässig die Lösung in unterschiedlichen Umgebungen ist.

Wichtige Überlegungen für die Authentifizierung in IT- und OT-Umgebungen

Links sehen Sie die fünf wichtigen Authentifizierungsanforderungen, die Fertigungsunternehmen berücksichtigen sollten:



SICHERHEIT

Wie stellen Sie sicher, dass nur autorisierte Benutzer auf gemeinsam genutzte Geräte zugreifen?

Wie sichern Sie gemeinsam genutzte Terminals und Geräte, die in der Fertigung häufig anzutreffen sind und von mehreren wechselnden Benutzern genutzt werden, um sicherzustellen, dass die Benutzerkonten sicher sind und die Benutzer nur Zugriff auf die Anwendungen, Services und Daten erhalten, auf die sie tatsächlich Zugriff haben sollten?

Derzeit verfügen 44 % der Fertigungsunternehmen über mehr als 1000 „Geisterbenutzer“-Konten, die mit inaktiven Benutzer- und Dienstkonten in Verbindung stehen.¹⁸

Admin-Konten oder gemeinsam genutzte Arbeitsplatzgeräte mit Zugriff auf vertrauliche Informationen sollten mit einem Authentifizierungsmechanismus geschützt werden, der gegen Identitätswechsel geschützt ist.

Gemeinsam genutzte Arbeitsplatzgeräte sollten sich in hohem Maße auf Benutzerberechtigungen und Zugriffskontrollen verlassen (keine gemeinsamen, Gast- oder anonymen Anmeldungen) und über Einschränkungen verfügen, die das Speichern von Passwörtern verhindern. Administrator-Konten sollten auch individuell und nicht gemeinsam genutzt werden, um die persönliche oder Remote-Fehlerbehebung zu unterstützen.

Darüber hinaus ist es in einem Fertigungskontext wichtig, sicherzustellen, dass die Authentifizierungslösung keine neuen Sicherheitsherausforderungen mit sich bringt. Beispielsweise mussten viele Fertigungsunternehmen Richtlinien für mobile Geräte einführen, um Mobiltelefone aus dem Fertigungsbereich fernzuhalten, da diese die Produktivität beeinträchtigen und potenzielle Gefahren durch unsachgemäßen Gebrauch bergen – was zu Unaufmerksamkeit gegenüber der aktuellen Aufgabe oder der Umgebung führen kann. Dies ist in einer Fertigungsumgebung sowohl gefährlich als auch kostspielig.



SICHERHEIT

Wie stellen Sie sicher, dass die Person, die sich bei einem Computer anmeldet, der legitime Benutzer ist?

Bei der Bewertung von Authentifizierungslösungen ist es wichtig zu bedenken, dass sich die Prioritäten in Sachen Cybersicherheit zwischen IT- und OT-Umgebungen erheblich unterscheiden. Im IT-Bereich liegt der Schwerpunkt auf der CIA-Triade, die sich auf die Vertraulichkeit, Integrität und Verfügbarkeit von Daten konzentriert. Innerhalb der OT verlagert sich der Schwerpunkt jedoch auf das AIC-Modell, bei dem Verfügbarkeit, Integrität und Vertraulichkeit die wesentlichen Säulen sind. Auch für die OT sind Zuverlässigkeit und Sicherheit von größter Bedeutung, denn während eine Sicherheitslücke in der IT zu Datenverlusten führen kann, können unsichere Vorgehensweisen in der OT verheerende physische Folgen haben.

Die OT-Sicherheit erfordert einen äußerst zuverlässigen Schutz, um die Betriebsverfügbarkeit zu gewährleisten und Sicherheitsprotokolle zu verbessern, die direkt Menschenleben schützen. Da IT und OT immer weiter zusammenwachsen, vergrößert sich die Angriffsfläche. Die OT-Grenze ist ein Hauptziel für Seitwärtsbewegungen. Die Authentifizierung muss gegen Identitätsmissbrauch geschützt sein, um unbefugte Steuerungsaktionen zu verhindern, die kritische Funktionen stören.



PRODUKTIVITÄT

Wie stellen Sie sicher, dass sich Benutzer nahtlos über mehrere Geräte und Anwendungen hinweg authentifizieren können?

44 %



der Fertigungsunternehmen verfügen derzeit über mehr als 1.000 „Geisterbenutzer“-Konten, die mit inaktiven Benutzer- und Dienstkonten in Verbindung stehen.¹⁸

54 %



der Mitarbeiter glauben, dass Zwei-Faktor-Authentifizierungslösungen wie OTP und Push-Codes ihren täglichen Arbeitsablauf stören.¹⁹

Jeder Authentifizierungsmechanismus sollte eine schnelle und einfache Authentifizierung für die Mitarbeitenden gewährleisten, um Unterbrechungen des Arbeitsablaufs und nicht genehmigte Problemumgehungen wie das Teilen von Passwörtern zu verhindern. Derzeit glauben 54 % der Mitarbeitenden, dass Zwei-Faktor-Authentifizierungslösungen (2FA) wie OTP und Push-Codes ihren täglichen Arbeitsablauf stören.¹⁹ Wenn zudem auf Systeme nur selten zugegriffen wird, wie beispielsweise auf HR- oder Gehaltsabrechnungssysteme, ist die Wahrscheinlichkeit von vergessenen Passwörtern und Kontosperrungen hoch.

Nicht alle Formen der Multi-Faktor-Authentifizierung (MFA) bieten ein optimales Gleichgewicht zwischen starker Sicherheit und einer schnellen und einfachen User Experience, die eine hohe Produktivität ermöglicht. Authentifizierung per Mobilgerät erhöht die Anzahl der Schritte im Authentifizierungsprozess, sodass Benutzer auf OTPs oder Push-App-Codes warten oder Handschuhe ausziehen müssen, um die Interaktion durchzuführen. Darüber hinaus unterliegen diese Prozesse den Besonderheiten von Umgebungen mit Einschränkungen für Mobilgeräte und Gewerkschaftsregeln.

Überlegen Sie unabhängig vom Szenario, wie viel Zeit für die Authentifizierung angemessen ist und wie oft ein Benutzer sich im Verlauf einer Schicht oder eines Tages authentifizieren muss. Berücksichtigen Sie auch die Größe der IT-Abteilung und die durchschnittliche Zeit für die Bearbeitung von Kontosperrungen – all dies trägt zu Ausfallzeiten und direkten Arbeitskosten bei. Wo hohe Effizienzanforderungen bestehen, sollten Sie eine passwortlose Authentifizierung oder die Vorteile einer „Tap-and-Go“-NFC-Lösung in Verbindung mit Mobilgeräten in Betracht ziehen, wo dies möglich ist, insbesondere bei gemeinsam genutzten Arbeitsplatzgeräten.



ZUVERLÄSSIGKEIT

Wie stellen Sie eine konsistente Authentifizierung sicher, die immer funktioniert, selbst in schwierigen Umgebungen mit unterschiedlichen Fehlerquellen?

Authentifizierung ist ein unternehmenskritischer Service. Wenn Mitarbeiter nicht in der Lage sind, sich bei den von ihnen verwendeten Apps oder Portalen anzumelden, können sie ihre Arbeit nicht erledigen. Jede Authentifizierungslösung muss für jeden Benutzer zuverlässig funktionieren und darf nicht von üblichen Fehlerpunkten wie Konnektivität, Geräte-Akku, Mobilfunkempfang oder Hardtoken-Akku abhängen. Authentifizierungslösungen sollten auch Funktionen wie NFC aufweisen, die für Umgebungen wie die industrielle Fertigung, Reinräume oder funkenfreie Bereiche geeignet sind.

Denken Sie daran, dass jede Authentifizierungslösung, die auf „etwas, das man kennt“ (z. B. auf einem Passwort) basiert, menschlichem Versagen unterliegt – verloren gegangene, vergessene oder falsch eingegebene Angaben, die die Authentifizierungserfahrung beeinträchtigen. Dadurch werden Benutzer möglicherweise aus ihren Konten ausgeschlossen. Außerdem funktionieren Lösungen zur Authentifizierung per Mobilgerät in Umgebungen mit gemeinsam genutzten Arbeitsgeräten, in denen die Mobilfunkabdeckung an Orten wie Umgebungen für Betriebstechnologie (OT) nicht immer zuverlässig ist, ganz zu schweigen von der Abhängigkeit vom Geräteakku bei der Authentifizierung per Mobilgerät.



LANGLEBIGKEIT

Wie stellen Sie sicher, dass das Produkt den Anforderungen der Fertigungsumgebung standhält?

Jede Lösung, die in einer Produktionsstätte verwendet wird, muss so konzipiert sein, dass sie den täglichen Belastungen der industriellen Umgebung standhält. Das Vorhandensein von beweglichen schweren Maschinen, harten Oberflächen und die Notwendigkeit, dicke Schutzhandschuhe zu tragen, erhöht das Risiko von Schäden an Authentifizierungslösungen, die am Arbeitsplatz zum Einsatz kommen, erheblich. Ihr Gerät muss nicht nur bruchstark sein und regelmäßigen Desinfektionsvorgängen standhalten, sondern auch über eine IP68-Zertifizierung verfügen, um sicherzustellen, dass es vollständig staubdicht und wasserdicht ist.

Wichtig ist, dass die Haltbarkeit die menschliche Sicherheit umfasst. Eine hochsichere Authentifizierungslösung ist von Natur aus sicher – sie verfügt über eine batteriefreie, funkenfreie Bauweise, die physische Risiken mindert, anstatt neue Gefahren im Produktionsbereich zu verursachen. Indem Sie die Ablenkungen und Sicherheitslücken beseitigen, die mit der MFA per Mobilgerät einhergehen, stellen Sie sicher, dass der Schutz des Systems niemals auf Kosten der Sicherheit von Menschenleben geht.





KOSTEN

Wie können Sie die Anzahl der authentifizierungsbezogenen Support-Tickets reduzieren?

Jede Form der veralteten Authentifizierung, beispielsweise Benutzernamen und Passwörter sowie die Authentifizierung per Mobilgerät, die massengerecht angewendet und durchgesetzt wird, erfordert eine kontinuierliche Durchsetzung von Richtlinien, Benutzerschulungen und IT-Support. Selbst die einfachsten Formen der 2FA- und MFA-Authentifizierung per Mobilgerät, wie z. B. OTP, verursachen einen enormen Supportaufwand, wenn Codes verzögert werden, Benutzer aus ihren Konten ausgesperrt sind oder Benutzer neue Geräte registrieren müssen. Darüber hinaus können Gewerkschaften verlangen, dass Unternehmen die vollen Kosten für das Gerät tragen, einschließlich Hardwarekosten, wiederkehrender Servicekosten, Geräteverwaltung und Sicherheitssoftware für Unternehmen sowie Kosten für den Austausch von Telefonen aufgrund unvermeidlicher Schäden, die in Produktionsumgebungen auftreten können.

Immer wenn ein Benutzer Probleme mit der Authentifizierung per Mobilgerät hat, ist er nicht produktiv. Je schneller ein Mitarbeiter sich authentifizieren und seine Aufgaben sicher ausführen oder bei Bedarf sogar sein Passwort selbst zurücksetzen kann, desto höher ist die Rentabilität.



Nachteile der veralteten Authentifizierung

Geringe Zuverlässigkeit und Sicherheit, hohe Reibungsverluste und Kosten

Es ist wichtig, zu beachten, dass jede Form von 2FA oder MFA mehr Sicherheit bietet als Passwörter allein, die veralteten Authentifizierung jedoch weiterhin auf Passwörter als ersten Faktor setzt – nach wie vor unsicher, ineffizient und immer noch eine Quelle der Frustration für Mitarbeiter. Und diese Frustration führt nur zu unsicheren Problemumgehungen wie der Weitergabe von Passwörtern, der Wiederverwendung von Passwörtern für mehrere Konten oder dem Speichern von Passwörtern im Browser oder in Anwendungen, wo sie angreifbar sein können.

Darüber hinaus ist bei der MFA per Mobilgerät (SMS, OTP und Push-App) der zweite Faktor an das mobile Gerät gebunden. Dabei stellen vier Aspekte ein Problem dar:

1. Es kann zu Verfügbarkeitsproblemen kommen, wenn Mobilgeräte aufgrund schlechter Konnektivität oder unzuverlässiger Dienste Codes nicht zeitnah senden.
2. Es gibt keine wirkliche Garantie dafür, dass der private Schlüssel auf einem sicheren Element auf dem Mobilgerät landet.
3. Das OTP oder der private Schlüssel könnte auf irgendeine Weise abgefangen werden (beispielsweise durch SIM-Swapping).
4. Es ist unmöglich, den Besitznachweis zu gewährleisten – oder, in den Begriffen des NIST ausgedrückt, es ist unmöglich nachzuweisen, dass das System gegen Identitätsbetrug geschützt ist.

Die herkömmliche Authentifizierung per Mobilgerät ist anfällig für moderne Cyberangriffe wie Phishing, Brute-Force-Angriffe, MitM-Angriffe, Malware und das zuvor erwähnte SIM-Swapping. Neben diesen Sicherheitsaspekten bringt die veraltete Authentifizierung per Mobilgerät viele versteckte Kosten mit sich, die mit Produktivitätseinbußen, Gerätekosten, erhöhtem IT-Support und Reibung bei der User Experience zusammenhängen. Tatsächlich geben 43 % der Unternehmen an, dass die User Experience das größte Hindernis bei der Nutzung der MFA darstellt.²⁰ Weitere Details finden Sie in unserem Whitepaper:

[The Top 5 Mobile Authentication Misconceptions: Demystifying the myth versus reality of legacy MFA \(Die fünf größten Missverständnisse in Bezug auf Authentifizierung per Mobilgerät: Aufklärung der Mythen hinsichtlich veralteter MFA\).](#)

Der erste Schritt bei der Verbesserung der Sicherheitspraktiken ist das Ersetzen der herkömmlichen Single-Factor-Authentifizierung (Benutzername und Passwort) durch eine Phishing-resistente Multi-Faktor-Authentifizierung (MFA).

Wahrscheinlichkeit für riskierte Kontoübernahmen



0 %

FIDO-Sicherheitsschlüssel (YubiKey)

10 %

Eingabeaufforderung auf dem Gerät

21 %

Sekundär

24 %

SMS-Code

50 %

Telefonnummer

Google, „How effective is basic account hygiene at preventing hijacking“ (zu Deutsch: Wie effektiv ist die grundlegende Kontohygiene beim Schutz vor Kontoübernahmen?)

Was ist Phishing-resistente Authentifizierung?

Phishing-resistente Authentifizierungsprozesse basieren auf einer kryptografischen Überprüfung zwischen Geräten oder zwischen dem Gerät und einer Domäne, wodurch sie ideal gegen Versuche geschützt sind, den Authentifizierungsprozess zu gefährden oder zu untergraben. Der Fachpublikation (SP) 800-63 des National Institute of Standards and Technology (NIST) zufolge erfüllen nur zwei Authentifizierungsmethoden die Kriterien für Phishing-resistente MFA: PIV/Smart Card und der moderne FIDO2/WebAuthn-Authentifizierungsstandard.



Was sind Passkeys?

Passkeys sind ein neuer Name für FIDO2-Zugangsdaten ohne Passwort. Dieser Standard ersetzt Passwörter und Phishing-anfällige MFA-Anmeldungen durch sicherere passwortlose Verfahren. Es gibt verschiedene Passkey-Implementierungen:

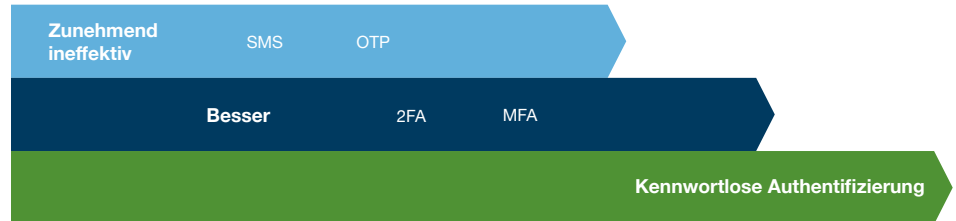
Synchronisierte Passkeys befinden sich in der Cloud, sodass Zugangsdaten auf einem Smartphone, Tablet oder Laptop zwischen Geräten geteilt werden können. Während synchronisierte Passkeys die Wiederherstellung von Zugangsdaten im Falle eines verlorenen oder gestohlenen Telefons oder Laptops erleichtern, sind FIDO-Zugangsdaten schwieriger nachzuverfolgen und eignen sich daher für Szenarien mit geringerer Sicherheitsgewährleistung.

Gerätegebundene Passkeys bieten Unternehmen im Vergleich zu synchronisierten Passkeys eine bessere Kontrolle über ihre FIDO-Zugangsdaten. Es gibt jedoch verschiedene Arten von gerätegebundenen Passkeys – solche, die sich in Allzweckgeräten wie Smartphones, Laptops und Tablets befinden, und solche, die sich in Hardware-Sicherheitsschlüsseln befinden, die speziell für hohe Sicherheit entwickelt wurden. Gerätegebundene Passkeys in modernen FIDO-Sicherheitsschlüsseln bieten die höchste Sicherheitsgarantie und stellen Unternehmen bewährte Fähigkeiten zum Lebenszyklusmanagement von Zugangsdaten und zur Nachweisbarkeit bereit. Mit diesem Passkey-Ansatz können Unternehmen die einfachste Benutzererfahrung beim Onboarding und bei der Wiederherstellung von Zugangsdaten auf allen Geräten und Plattformen bieten und dabei die strengsten Compliance-Vorschriften erfüllen.



Die Zukunft ist passwortlos

Der Übergang von der veralteten MFA zur Phishing-resistenten MFA ist ein wichtiger Schritt in Richtung einer Sicherung gemeinsam genutzter OT- und IT-Umgebungen in der Fertigungsindustrie. Der nächste Schritt für die moderne MFA ist jedoch die Einführung der passwortlosen Authentifizierung. Da letztendlich die Aktionen des Benutzers die größte Schwachstelle bei der herkömmlichen Authentifizierung darstellen und die mehrstufige Authentifizierung einen großen Beitrag zur Unzufriedenheit des Benutzers darstellt, entwickelt sich die globale beste Praxis hin zu einer passwortlosen Authentifizierung – d. h. einer Authentifizierung, bei der der Benutzer bei der Anmeldung kein Passwort eingeben muss.



Herkömmliche Smartcards sind eine weitere Form der passwortlosen Authentifizierung, die hohe Sicherheit bietet, jedoch in der Regel hohe Investitionskosten (CapEx) für Smartcard-Lesegeräte, Karten und Backend-Verwaltungsplattformen erfordert. Die Smartcard-Technologie wird vor allem in lokalen Umgebungen eingesetzt. Je nach Ihren Anforderungen können Smartcards eine geeignete Lösung für Sie sein. Die Branche als Ganzes bewegt sich in Richtung eines passwortlosen Anmeldevorgangs, der moderne Authentifizierungsstandards wie FIDO2/WebAuthn nutzt, die sich gut mit der Cloud kombinieren lassen.

Der moderne Authentifizierungsstandard FIDO (Fast IDentity Online) ermöglicht eine starke Zwei-Faktor-, Multi-Faktor- und passwortlose Authentifizierung. Der FIDO-Standard wurde von der FIDO Alliance entwickelt, einem offenen Industrieverband mit dem Ziel, die Abhängigkeit von Passwörtern zu verringern. FIDO2/WebAuthn ist der neueste FIDO-Standard und verwendet Public-Key-Kryptografie für hohe Sicherheit, wobei die privaten Schlüssel niemals den Authentifikator verlassen. Für Fertigungsunternehmen mit älteren OT-Systemen und geringer Toleranz für nicht produktive Aufgaben bieten FIDO2-Hardware-Sicherheitsschlüssel eine Multi-Faktor- und passwortlose Authentifizierung mit hoher Sicherheit und einer User Experience, die bislang kaum zu erreichen war. FIDO2-basierte Hardware-Sicherheitsschlüssel können eine portable Vertrauensbasis schaffen, die sich sowohl für gemeinsam genutzte Arbeitsplätze als auch für Umgebungen mit Einschränkungen für Mobilgeräte hervorragend eignet.



Der YubiKey

ist die **einzige** Lösung, die äußerst Phishing-resistent ist und in unabhängigen Untersuchungen nachweislich **100 %** der Kontoübernahmen verhindert.²¹



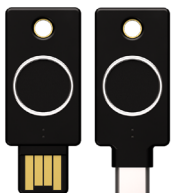
Die YubiKey 5 Serie

Von links nach rechts: YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano und YubiKey 5C Nano



Die YubiKey 5 FIPS Serie

Von links nach rechts: YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS und YubiKey 5C Nano FIPS



YubiKey Bio Series – FIDO Edition

Von links nach rechts: YubiKey Bio – FIDO Edition, YubiKey C Bio – FIDO Edition

yubico

Securing Operational Technology with Yubico

Hardening OT access to protect safety, uptime, and continuity

How expanded connectivity is reshaping cyber risk in operational technology. Operational Technology (OT) supports critical infrastructure including manufacturing, energy, healthcare, and government. These OT environments consist of large-scale machines and Industrial Control Systems (ICS), including Distributed Control Systems and SCADA, to manage physical processes including machine-to-machine and human-to-machine communication. Historically, these environments were designed to prioritize safety and uptime, rather than secure connectivity. By their nature, these systems are often considered shared workstations.



The guidance stresses that OT-IT connectivity is essential but must follow a secure-by-design model. It outlines eight principles to help organizations modernize connectivity while minimizing exploitable risk across industrial environments. Among these, hardening the OT boundary is identified as a strategic priority.

Principle 5: Why hardening the OT boundary is now a strategic imperative

The OT boundary is the critical contact point between these trusted operational systems and external networks.



Erfahren Sie, wie Sie die OT-Grenze mit Yubico absichern können

Sichere Mensch-Maschine-Kommunikation mit dem YubiKey

Phishing-resistente Authentifizierung und der Weg hin zur Passwortlosigkeit

Yubico bietet den YubiKey an – einen Hardware-Sicherheitsschlüssel, der speziell für höchste Sicherheitsstandards, Benutzerfreundlichkeit und industrielle Langlebigkeit entwickelt wurde. Gerätegebundene Hardware-Passkeys wie der **YubiKey** bieten den höchsten Schutz. Mit dem YubiKey können Fertigungsunternehmen eine Phishing-resistente Multi-Faktor- und passwortlose Authentifizierung in großem Maßstab bereitstellen und dabei eine schnelle und nahtlose User Experience bieten, die zu hoher Produktivität führt. Der YubiKey gewährleistet maximale Ausfallsicherheit, indem er private Schlüssel auf einem Sicherheitselement schützt, aus dem diese nicht abgezogen werden können.

Mit dem YubiKey können Sie die Mensch-zu-Maschine Kommunikation in einer Zeit KI-gestützter Bedrohungen absichern und so sowohl IT- als auch OT-Systeme vor unbefugtem Zugriff schützen. Der YubiKey verwendet moderne Authentifizierungsprotokolle wie FIDO U2F und offene FIDO2-Authentifizierungsstandards, um Phishing-Angriffe auf Zugangsdaten zu verhindern. Darüber hinaus unterstützen YubiKeys auch SmartCard-, OTP- und OpenPGP-Protokolle, was die Verwendung eines einzigen Sicherheitsschlüssels in einer Vielzahl moderner und älterer IT- und OT-Umgebungen sowie mit einer Vielzahl von **IAM-Lösungen von Drittanbietern** wie Microsoft, Okta, Duo und Ping ermöglicht und die Authentifizierung für **Tausende von Anwendungen und Diensten erlaubt**. Dank der Unterstützung mehrerer Protokolle können Hersteller den YubiKey als Brücke zur passwortlosen Authentifizierung nutzen und damit die Lücke zwischen der Absicherung veralteter industrieller Infrastrukturen und moderner Cloud-Umgebungen schließen.

YubiKeys sind bestens tragbar, einfach zu verwenden und unterstützen so die Produktivität. Der YubiKey bietet eine schnelle, passwortlose Anmeldung per „Tap-and-Go“, die viermal schneller ist als die Anmeldung per SMS. Ein einziger YubiKey funktioniert bequem auf mehreren Geräten, darunter Desktops, Laptops, Mobiltelefone, Tablets, Notebooks und gemeinsam genutzte Arbeitsplatzgeräte. Er ist in verschiedenen Formfaktoren erhältlich, von denen einige an einen Schlüsselbund passen, und verfügt über USB-A-, USB-C-, NFC- und Lightning-Anschlüsse.

YubiKeys bieten robuste Sicherheit in allen Fertigungsbereichen



benötigen weder eine Batterie noch eine Internetverbindung.



äußerst strapazierfähig, staubdicht, bruchfest und wasserfest (IP68-zertifiziert).



geeignet für funkenfreie bzw. funkenarme Umgebungen.



keine Softwareinstallation und keine Mobilfunkverbindung erforderlich.

Um die User Experience und Authentifizierungsgeschwindigkeit weiter zu verbessern, bietet Yubico auch die YubiKey Bio Series – FIDO Edition an. Sie unterstützt FIDO U2F und FIDO2 und bietet die gleiche gewohnte Sicherheit aller YubiKeys, jedoch mit einer neuen biometrischen, passwortlosen Erfahrung.

Für stark regulierte Umgebungen sind YubiKeys auch in FIPS 140-3-validierten Formfaktoren erhältlich, die die höchsten Anforderungen der Authentifizierungssicherheitsstufe 3 (AAL3) gemäß NIST SP 800-63B erfüllen.

”

Wir haben den YubiKey in unseren SCADA-Systemen für den Energiebetrieb eingeführt, um die Sicherheit durch MFA zu erhöhen. Dieser Prozess ermöglicht einem Bediener, bei Schichtbeginn schnell eine Authentifizierung durchzuführen und bei Bedarf Maßnahmen zu ergreifen, ohne dass es zu Systemunterbrechungen kommt. MFA stellt sicher, dass nur authentifizierte Benutzer Zugriff auf das System erhalten können.“

Chad Lloyd

Director of Cybersecurity Architecture for Energy Management | Schneider Electric



[Mehr Infos](#)

”

Unser Ziel war es, Kontoübernahmen durch die Einführung einer strengeren mehrstufigen Authentifizierung (MFA) zu verhindern. Die Einführung von YubiKeys hat es uns leicht gemacht, unsere Authentifizierungsstrategie kontinuierlich voranzubringen. Unser Ziel ist es, in Zukunft eine passwortlose Authentifizierung für alle Benutzer zu ermöglichen.“

Herr Daisuke Okamoto

IT Platform Division | Mitsubishi Electric Digital Innovation



[Mehr Infos](#)

”

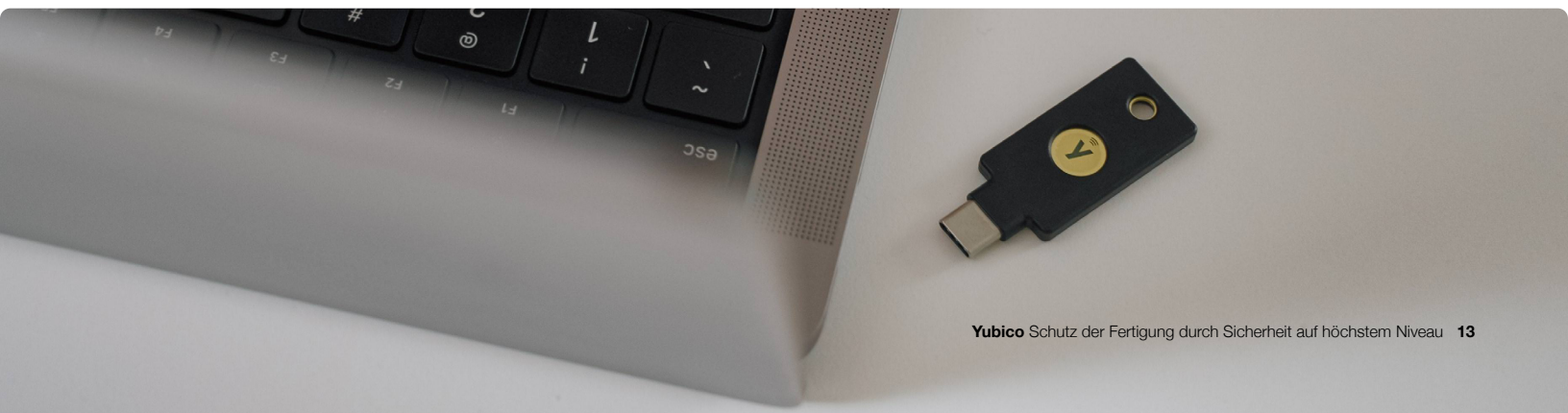
YubiKeys sind schnell, robust und branchenführend: ein branchenführendes Gerät und branchenführende Sicherheit. Das funktioniert reibungslos und spart Zeit im Vergleich zu denjenigen, die den TOTP eingeben müssen, da man für jedes Konto sechs Ziffern eingeben muss. Es ist viel schneller, nur eine Taste zu drücken.“

Ángel Uruñuela

Chief Information Security Officer (CISO) bei der Fluidra Group

FLUIDRA

[Mehr Infos](#)





Zugriff durch Dritte



Eigentums- und
Produktintegrität



Sichere
Codesignatur

” Zum proaktiven Schutz unserer Lieferkette arbeiten wir eng mit wichtigen Lieferanten zusammen, um eine doppelte Verschlüsselung zu schaffen, da sowohl der Lieferant als auch Schneider Electric YubiHSM 2-Module in den Fertigungsprozess integriert haben.“

Chad Lloyd

Director of Cybersecurity Architecture
for Energy Management |
Schneider Electric

Schneider Electric [Mehr Infos](#)

Sicherung der Fertigungslieferkette

Fertigungslieferketten umfassen den Transport physischer Güter und Komponenten von Ort zu Ort, aber auch die anderen Partnerschaften und Geschäftsbeziehungen, die das Unternehmen unterstützen, einschließlich oft übersehener Integrationen wie der Nutzung von Ressourcen oder Code von Drittanbietern. So definiert umfasst eine externe Lieferkette *alle* Produkte oder Dienstleistungen, die „unverändert“ zur Entwicklung der eigenen Produkte oder Dienstleistungen eines Unternehmens verwendet werden.

Die Sicherung der Lieferkette erfordert sowohl die Absicherung des *Zugriffs* als auch der *Eingaben* (physische Komponenten, Software oder Daten) im Fertigungsprozess, um die Qualität und Integrität des Produkts zu gewährleisten und vor dem Verlust von geistigem Eigentum oder Produktionszeit zu schützen.

Schutz vor unbefugtem Zugriff durch Dritte

Der Angriff auf Colonial Pipeline war nur einer von vielen hochkarätigen Vorfällen in der Lieferkette, die Hersteller in Alarmbereitschaft versetzt haben. Produktionsausfälle können in vielen Fertigungsszenarien kostspielig sein, ganz zu schweigen von den Bedenken hinsichtlich des Verlusts von geistigem Eigentum. Eine kürzlich durchgeführte Umfrage ergab, dass bis zu 97 % der Unternehmen Opfer eines Cybersicherheitsverstoßes wurden, der auf eine Schwachstelle in der Lieferkette zurückzuführen war.²² So waren beispielsweise gestohlene Zugangsdaten eines Drittanbieters letztlich die Ursache für den Target-Hack 2013, der allein zu Geldstrafen in Höhe von über 18,5 Millionen \$ führte.²³

Die größte Herausforderung für Hersteller besteht darin, dass der Schutz nachgeschalteter Lieferketten angesichts der Hunderte (wenn nicht Tausende) von Zugangspunkten, die entlang der Kette überwacht werden müssen, nicht einfach ist. Fertigungsunternehmen müssen jeden Benutzer identifizieren und authentifizieren, der Zugriff auf Vorleistungen, geistiges Eigentum oder auf die an der Lieferkette beteiligten Systeme hat. Beispielsweise wurde das interne Netzwerk von KP-Snacks gehackt, was es den Hackern ermöglichte, auf vertrauliche Dateien zuzugreifen und diese zu speichern, was zu Unterbrechungen der Lieferkette führte.²⁴

Der YubiKey von Yubico bietet moderne, Phishing-resistente Authentifizierung in großem Maßstab über die gesamte Lieferkette hinweg und hilft Fertigungsunternehmen und ihren Lieferanten dabei, eine robuste, benutzerfreundliche Authentifizierung für jeden Benutzer zu implementieren, der vorgelagerten Zugriff auf das Netzwerk oder an kritischen IP-Übergängen hat.

In Kombination mit YubiKey as a Service (siehe unten) können Sie eine kostengünstige und einfache Lösung zur Verbesserung der Lieferkettensicherheit anbieten.

Gewährleistung der höchsten Integrität Ihrer Produktteile

Hersteller wissen, dass es entscheidend ist, die Echtheit aller an einem End-to-End-Prozess beteiligten Komponenten sicherzustellen, um unbefugte Nachahmung und Diebstahl zu vermeiden, aber auch zur Qualitätssicherung, da eine Fertigungslinie nur aus Produkten aus authentischen Quellen bestehen sollte. Daher muss jederzeit eine Lösung vorhanden sein, um die Integrität und das geistige Eigentum hinsichtlich aller Komponenten von der Produktion und Montage bis hin zu Reparatur und Austausch zu schützen. Da sich zudem agentenbasierte KI und autonome Funktionen immer weiter verbreiten, ist die Absicherung der Maschine-zu-Maschine-Kommunikation sowie der Zugangspunkte, die der menschlichen Kontrolle entgehen, von entscheidender Bedeutung für die Gewährleistung der Gesamtsystemintegrität.

Das YubiHSM 2



ermöglicht eine sichere Maschine-zu-Maschine Kommunikation, manipulationsresistente Speicherung und Verwaltung von Schlüsseln, indem es das versehentliche Kopieren und Verbreiten von kryptografischen Schlüsseln sowie den Diebstahl von in Software gespeicherten Schlüsseln aus der Ferne verhindert.

Der traditionelle Ansatz zum Schutz der IP und zur Verhinderung von Fälschungen in der Fertigung umfasst die Verwendung digitaler kryptografischer Schlüssel und Verschlüsselung. Kryptografische Schlüssel werden entweder in einer hoch anfälligen Software oder in einem Hardware-Sicherheitsmodell (HSM) gespeichert. Leider sind herkömmliche rackmontierte und kartenbasierte HSMs groß und teuer, was sie in der Fertigung, in gesicherten Rechenzentren oder für IoT-Geräte unpraktisch macht.

Sichern von externem Code und Daten

Fertigungsunternehmen, die Software in ihren Produkten verwenden, müssen eine Methode zur sicheren Codesignierung für die Aufnahme von Code oder Daten aus externen Quellen haben. Der Bedarf an Lösungen für eine sichere Codesignierung hat in jüngster Zeit zugenommen, wie die Folgen des SolarWinds-Angriffs von 2020 gezeigt haben. Bei diesem Angriff nutzten Hacker eine Schwachstelle im Codesignatursystem von SolarWinds aus, wodurch sie bösartigen Code als legitime Updates an mehr als 18.000 Installationen des SolarWinds Orion-Produkts weltweit betrügerisch verteilen konnten.²⁵

Darüber hinaus ist die Stärke der Kryptografielösung, die Sie verwenden, nur so stark wie die Attestierungsmethode Ihres Lieferkettenteilnehmers. Daher ist es von entscheidender Bedeutung, dass diese Partner eine Nachverfolgbarkeitskette für den Code vorweisen können, die bis zum Computer des ursprünglichen Entwicklers zurückreicht.

Sichere Maschine-zu-Maschine-Kommunikation mit dem YubiHSM 2

Kryptografischer Schutz von IP und Produktintegrität

Als Ergebnis der Zusammenarbeit mit mehreren Partnern im Fertigungssektor, die für die Großserienproduktion elektronischer Komponenten verantwortlich sind, hat Yubico das ultraportable und kostengünstige YubiHSM 2 entwickelt, das weltweit kleinste HSM im Nano-Formfaktor. Das YubiHSM 2 ermöglicht eine sichere, manipulationssichere Speicherung und Verwaltung von Schlüsseln, indem es das versehentliche Kopieren und Verbreiten von kryptografischen Schlüsseln sowie den Diebstahl von in Software gespeicherten Schlüsseln aus der Ferne verhindert. Das YubiHSM 2 kann in jedem Prozess eingesetzt werden, in dem Sicherheitsschlüssel und die Authentizität von Komponenten verwaltet werden müssen und Manipulationen verhindert werden sollen.

Es kann leicht an einem USB-Anschluss auf Servern, Datenbanken, Roboter-Produktionslinien, Anwendungen und IoT-Geräten eingesetzt werden.

Das YubiHSM 2 dient dem Schutz des Herstellungsprozesses, indem sichergestellt wird, dass nur zertifizierte Programmierstationen eine Schnittstelle zu den Komponenten herstellen können, oder um digitale Signaturen auf jede Komponente zu schreiben und so deren Authentizität zu gewährleisten. In beiden Szenarien trägt die zusätzliche Sicherheit des YubiHSM 2 dazu bei, den Ruf eines Unternehmens zu wahren, und gibt ihm die Gewissheit, dass seine Produkte auch nach Verlassen der Fertigungshalle wie erwartet funktionieren.

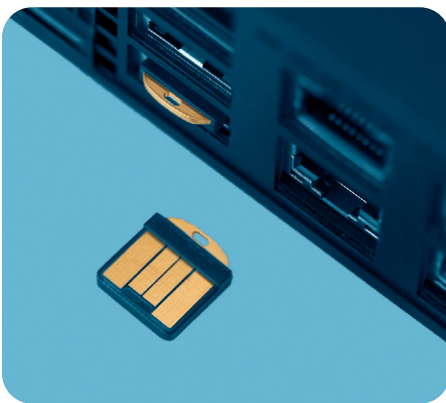
Das YubiHSM 2 eignet sich ideal zum Schutz der Signaturschlüssel und Zertifikate für die Codesignatur und unterstützt so den Austausch vertraulicher Daten innerhalb der Lieferkette. Unternehmen, die die Anforderungen von FIPS 140-3 erfüllen müssen, haben die Möglichkeit, das nach FIPS 140-3, Level 3 validierte YubiHSM 2 FIPS einzusetzen, um ein Höchstmaß an Datenschutz zu gewährleisten.

Es ist wichtig, darauf hinzuweisen, dass der kryptografische Schlüssel, der zum Signieren und/oder zur Zertifizierung von Komponenten verwendet wird, niemals außerhalb der YubiHSM 2-Hardware offengelegt wird, wodurch ein hohes Maß an Sicherheit gewährleistet ist. Ein Beispiel zur Veranschaulichung: Selbst wenn ein Angreifer aus der Ferne in der Lage ist, ein Netzwerk oder den damit verbundenen Computer zu kompromittieren, gibt es dennoch keine offensichtlichen Angriffsvektoren. Ist derselbe Angreifer hingegen in der Lage, vollständigen Zugriff auf eine entsprechende Software zu erlangen, könnte er zumindest den Speicher oder lokale Dateien auf potenzielle Schwachstellen oder Muster analysieren.

Das YubiHSM 2



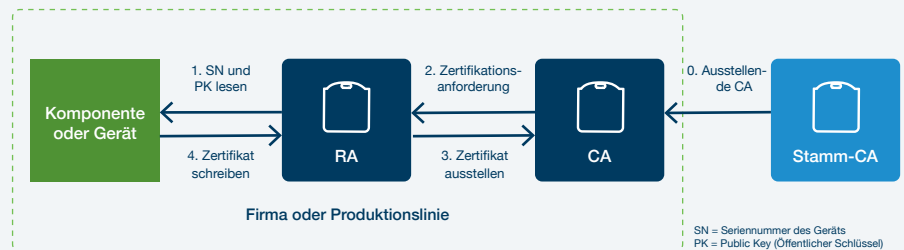
dient dem Schutz des Herstellungsprozesses, indem sichergestellt wird, dass nur zertifizierte Programmierstationen eine Schnittstelle zu den Komponenten herstellen können, oder um digitale Signaturen auf jede Komponente zu schreiben und so deren Authentizität zu gewährleisten.



Unterstützung für PKI-Umgebungen (Public Key Infrastructure)

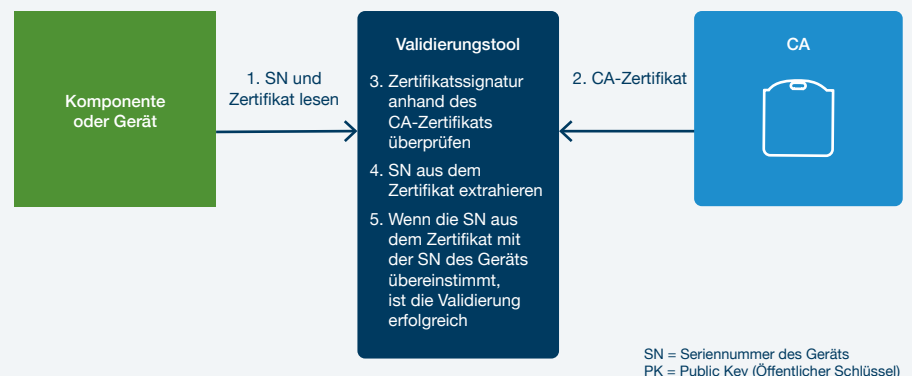
Da das YubiHSM 2 für die Speicherung kryptografischer Schlüssel konzipiert ist, eignet es sich ideal zum Schutz der PKI-Infrastruktur und des Netzwerks von kryptografischen Schlüsseln. Der Ausstellungsprozess von Zertifikaten unter Verwendung einer auf dem YubiHSM 2 basierenden PKI für die Fertigung wird wie folgt dargestellt:

Übersicht über die PKI und den Ausstellungsprozess eines Zertifikats



In diesem Diagramm verwendet die Root-Zertifizierungsstelle (Root CA) ein YubiHSM 2, um das Schlüsselpaar (d. h. sowohl den privaten als auch den öffentlichen Schlüssel) zusätzlich zum Zertifikat entweder vor Ort oder in einem externen Rechenzentrum zu speichern. In der Produktionslinie kann eine Zertifizierungsstelle (CA) bereitgestellt und mit einem Zertifikat konfiguriert werden, das von der Root-Zertifizierungsstelle als Delegierter signiert wurde. Mit diesem Schlüsselpaar und Zertifikat können alle nachfolgenden Zugangsdaten signiert und ebenfalls durch einen YubiHSM 2 geschützt werden. Diese zusätzlichen Zugangsdaten werden von einer Registrierungsstelle (RA) ausgestellt, deren Zertifikat wiederum von der CA signiert wurde. Letztendlich können die Komponentenzertifikate dann verwendet werden, um die Authentizität jeder Komponente, jedes Produkts oder jedes Geräts, das hergestellt wird, zu überprüfen, wie in der Abbildung unten dargestellt.

Der Zertifikat-Validierungsprozess



In der Praxis ermöglicht dies den Herstellern, die Authentizität jedes Bauteils zu überprüfen, das gerade hergestellt wird. Die Erfassung verschlüsselter Seriennummern im elektronischen Steuergerät (ECU) kann ebenfalls die Prüfung unterstützen und zur Nachverfolgung bei Audits genutzt werden.

FALLSTUDIEN



Sicherung der Systeme und Lieferkette bei Schneider Electric



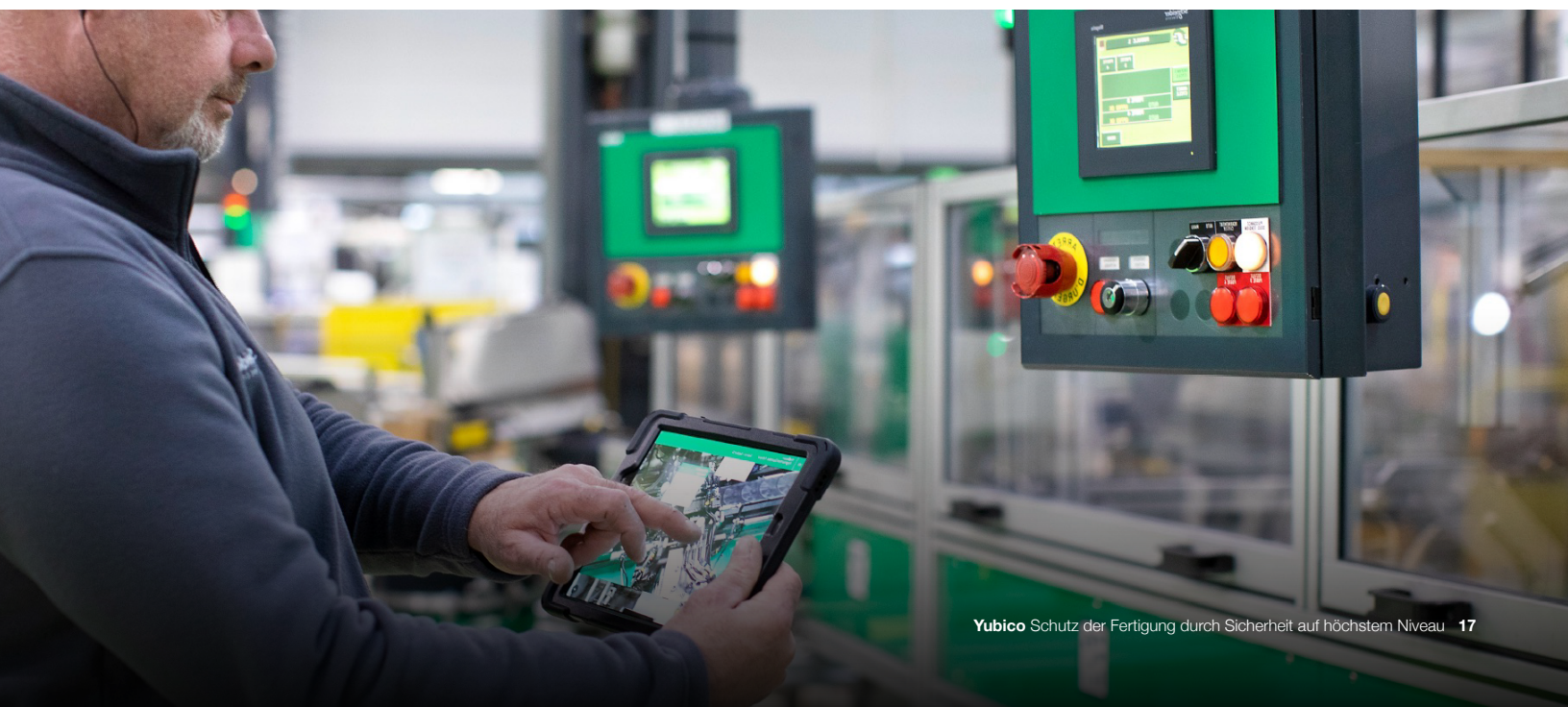
Schneider Electric ist führend bei der digitalen Transformation von Energiemanagement und Automatisierung und stellt elektrische Bauteile sowie Energiemanagementsysteme her, darunter ein SCADA-System (Supervisory Control and Data Acquisition) für die Fernverwaltung kritischer Infrastrukturen (z. B. Rechenzentren, Krankenhäuser, Öl- und Gasindustrie).

Mit dem YubiKey konnte Schneider Electric MFA in ein isoliertes System integrieren, ohne auf das Internet oder eine weniger sichere SMS-basierte Authentifizierung angewiesen zu sein, wodurch die Authentifizierung bei Schichtwechseln optimiert wurde. Der YubiKey wird auch in Kontrollsituationen eingesetzt, in denen Überbrückungsmaßnahmen durch das Personal erforderlich sind. Moderne MFA mittels YubiKeys war Teil des Prozesses zur erfolgreichen Erlangung der IEC-62443-SL2-Zertifizierung.

„Sicherheit steht bei Schneider Electric an erster Stelle und spiegelt sich in allem wider, was wir tun“, erklärt Chad Lloyd, Director of Cybersecurity Architecture for Energy Management bei Schneider Electric. „Im Rahmen unserer IEC-SL2-Zertifizierung haben wir MFA in unser Energieversorgungssystem integriert und sind damit gut aufgestellt, um künftig die SL3-Anforderungen zu erfüllen. Das ist jetzt ein Unterscheidungsmerkmal von Schneider Electric“, so Lloyd.

Neben der Integration von YubiKeys in seine SCADA-Systeme, die von Kunden in kritischen Infrastrukturen genutzt werden, hat Schneider Electric Maßnahmen ergriffen, um die Qualität und Integrität seiner Lieferkette sicherzustellen, indem das YubiHSM 2-Hardware-Sicherheitsmodul zur Integration mit wichtigen Lieferanten im Fertigungsprozess eingesetzt wird. Die hochsichere kryptografische Hardware-Sicherheit von YubiHSM 2 unterstützt die strengen Test- und Fertigungsprozesse aller Originalprodukte von Schneider Electric.

Der Nano-Formfaktor von YubiHSM 2 war entscheidend für die flexible Bereitstellung und Verwendung in Fertigungsbereichen, da zur Verbindung nur ein einfacher USB-Anschluss erforderlich ist.



FALLSTUDIEN



Mitsubishi Electric stärkt die globale Cybersicherheit mit dem YubiKey

Mitsubishi Electric ist ein weltweit führendes Unternehmen im Bereich der Produktinnovation und Hersteller von elektrischen und elektronischen Produkten und Systemen für Verbrauchende, Unternehmen sowie eine Vielzahl kritischer Infrastrukturen, darunter Energie-, Verkehrs- sowie Informations- und Kommunikationssysteme. Mitsubishi Electric wurde 1921 gegründet und hat seinen Hauptsitz in Tokio, Japan, und ist weltweit in über 120 Ländern aktiv.

Als ein wichtiger Anbieter von Elektro- und Elektronikprodukten und -Lösungen für kritische Infrastruktursektoren weltweit und großer Anbieter von japanischen Verteidigungssystemen ist für Mitsubishi Electric der Schutz vor anhaltenden Cyberangriffen von entscheidender Bedeutung.

Um sicherzustellen, dass sich die Investition in MFA gelohnt hat, wollte Mitsubishi Electric gewährleisten, dass die Lösung den Standards der „Digital Identity Guidelines“ des National Institute of Standards and Technology (NIST) sowie dem „Authenticator Assurance Level“ (AAL) entspricht, die weltweit als maßgebliche Standards für das Identitätsmanagement anerkannt sind. Bei der Einführung der MFA in verschiedenen Geschäftsbereichen und Tochtergesellschaften sah sich Mitsubishi Electric mit einer Vielzahl von Herausforderungen konfrontiert, darunter häufig Szenarien mit Einschränkungen hinsichtlich der Nutzung mobiler Geräte, da in den meisten Produktionsstätten die Nutzung mobiler Geräte eingeschränkt ist.

Der YubiKey erwies sich als optimale Lösung sowohl für die IT als auch für die Betriebstechnik (OT), einschließlich des Zugriffs auf industrielle Steuerungssysteme (ICS), da er keine zusätzliche Hardware, Software, externe Stromversorgung, Batterien oder Netzwerkverbindungen erfordert. Mit der Einführung von Yubico-Lösungen wie dem YubiKey erhöht Mitsubishi Electric die Sicherheitsstandards deutlich und schafft eine robuste Grundlage für seine digitale Transformation. Durch die Einführung eines sicheren Authentifizierungsprozesses, der auf Passwörtern nicht angewiesen ist, erleichtert und schützt Mitsubishi Electric seine digitale Transformation.



Eine portable Vertrauensbasis für EasyMile zur Sicherung autonomer Fahrzeuge

EasyMile entwickelt Softwarelösungen für seine Flotte autonomer Fahrzeuge (hauptsächlich für den Transport von Personen und Gütern) nach den höchsten Sicherheitsstandards. EasyMile nutzte bereits YubiKeys von Yubico zur Sicherung von Administratorkonten und wandte sich an Yubico, um seine PKI-Infrastruktur zielgerichtet zu stärken. EasyMile führte YubiHSM 2 schnell und einfach ein, um die PKI X.509 CA-Infrastruktur zu sichern, die zur Absicherung seines Ökosystems autonomer Fahrzeuge dient. Das Ergebnis? Ein Vertrauenszeichen für sein Sicherheitszertifikat-Ökosystem.

YubiHSM 2 bietet zudem eine portable Vertrauensbasis (root of trust) in der globalen Fertigungsindustrie. Nach der Entwicklung einer eigenen internen PKI konsultierte beispielsweise ein Fortune-500-Unternehmen Yubico, um eine kostengünstigere Lösung zur Erhaltung der Produktintegrität zu finden. Dieses Unternehmen nutzte YubiHSM 2, um jede in verschiedenen Werken hergestellte Komponente digital zu signieren und zu zertifizieren, um die Produktauthentizität und -integrität am Ende der jeweiligen Produktionslinien sicherzustellen.



Schnelle und reibungslose Bereitstellung von passwortloser Authentifizierung in großem Maßstab

Hardware-Passkeys, wie sie in modernen Sicherheitsschlüsseln, beispielsweise YubiKeys, zum Einsatz kommen, haben sich als wirksames Mittel erwiesen, um KI-gestützte Cyberbedrohungen in großem Umfang abzuwehren, und entwickeln sich zunehmend zur bevorzugten Methode, mit der kluge Unternehmen Cyberbedrohungen einen Schritt voraus sind. Auch wenn der Weg hin zu einer Phishing-resistenten MFA und einer passwortlosen Zukunft abschreckend erscheinen mag, muss er dies nicht sein.

Um die skalierbare Sicherung digitaler Identitäten mit Phishing-resistenter Authentifizierung zu erleichtern, bietet [YubiKey as a Service](#) Unternehmen eine flexible und kostengünstige Möglichkeit zur Bereitstellung von YubiKeys für alle Mitarbeitenden, Lieferketten und die Endkundschaft.

Mit [YubiKey as a Service](#) profitieren Unternehmen von einer einfachen, skalierbaren weltweiten Bereitstellung des YubiKey für ihre Beschäftigten, ihre Lieferkette und ihre Endkundschaft. YubiKey as a Service bietet den Kunden verschiedene Formfaktoren, Ersatzbestände und einen bevorzugten Kundensupport – und das alles für weniger als den Preis einer Tasse Kaffee pro Monat. Unternehmen erhalten automatisch Zugriff auf das [Kundenportal](#), ein zentralisiertes, webbasiertes Dashboard, mit dem IT-Teams die Bereitstellung von YubiKeys effizient durchführen, nachverfolgen und verwalten können, mit Echtzeit-Einblick in den Bestand, den Fortschritt der Einführung und die Aktivierung durch die Benutzer.

Die Kundschaft hat zudem Zugang zu schlüsselfertigen [Registrierungs-](#) und [Delivery-](#)Diensten, mit deren Hilfe die IT-Abteilung den YubiKey schnell unter den Benutzern bekannt machen kann, um die Phishing-Resistenz zu beschleunigen, und anschließend an Endbenutzer mit Firmen- und Privatadressen weltweit weiterleiten kann. Benutzer können den YubiKey sogar im [Self-Service-Verfahren](#) bestellen und haben so die Freiheit, die Schlüssel jederzeit an ihre bevorzugte Adresse liefern zu lassen. Kunden von YubiKey as a Service profitieren von kontinuierlichen Verbesserungen an verfügbaren und neuen Diensten, sodass eine intelligente, zukunftsichere Sicherheitsinvestition gewährleistet ist.

Yubico bietet zudem [Professional Services](#) an, um Unternehmen dabei zu unterstützen, YubiKeys zügig und in großem Umfang erfolgreich einzuführen. Wir bieten eine Reihe von Beratungsdiensten an, darunter technische Integrationsunterstützung, Entwickler- und API-Support sowie Bereitstellungsplanung und Implementierung.

Bei der Beschaffung des YubiHSM 2 erweist sich [YubiHSM 2](#) als eines der kleinsten und kostengünstigsten HSMs auf dem Markt. Es eignet sich ideal für eine Vielzahl von Anwendungsfällen sowie für alle Arten von Organisationen und Branchen, wodurch sich der Kauf, die Beschaffung und die Bereitstellung einfach und schnell gestalten lassen. Dank seiner geringen Größe bietet das YubiHSM 2 eine zugängliche Lösung für starke, Phishing-resistente Sicherheit für eine Vielzahl von Fertigungs- und Lieferkettenkunden auf der ganzen Welt.





Sichern Sie die Lieferkette und schützen Sie den Zugriff durch Dritte, geistiges Eigentum sowie die Produktintegrität, indem Sie den YubiKey und das YubiHSM 2 nutzen, um höchste Sicherheit zu gewährleisten.

Hoher ROI bei niedrigeren Risiken und Kosten

In einer im Auftrag von Yubico durchgeführten Studie befragte Forrester Consulting vor Kurzem Sicherheitsexperten von fünf Unternehmen, die YubiKeys verwenden, und stellte fest, dass die Ergebnisse für Composite Organizations enorm sind:



Reduzierung der Gefahr von Phishing und Diebstahl von Zugangsdaten



Weniger Helpdesk-Tickets



ROI über 3 Jahre

² Basierend auf Forrester-Interviews mit sechs Entscheidungstragenden in großen Unternehmen, die Erfahrung mit YubiKeys gesammelt haben. Dabei wurden die Erfahrungen in einer einzigen Composite Organization zusammengefasst, einer globalen Organisation mit 5.000 Mitarbeitenden und einem Jahresumsatz von 2,5 Mrd. \$, die zuvor herkömmliche MFA verwendet hatte.

[Mehr erfahren →](#)

Zusammenfassung

Aufbau einer cyberresilienten Zukunft für die Fertigungsindustrie

Moderne Fertigungsunternehmen benötigen moderne Sicherheitslösungen, um ihre Effizienz und betriebliche Widerstandsfähigkeit in einer Zeit zu steigern, in der künstliche Intelligenz sowohl als entscheidender Faktor für den Geschäftserfolg als auch als starker Beschleuniger von Bedrohungen fungiert. Um wirksam zu sein, müssen diese Lösungen langlebig und einfach in der Produktion einsetzbar sein und gleichzeitig die Benutzer in Umgebungen unterstützen, die von industriellen Produktionsstätten bis zum Vorstandszimmer reichen. Im Idealfall sollten diese Lösungen so konzipiert sein, dass sie einen Teil des kostspieligen, unproduktiven Aufwands im Zusammenhang mit der veralteten Authentifizierung verringern. Da agentenbasierte KI und softwaredefinierte Energieversorgung die Branche weiterhin grundlegend verändern, ist es zudem von entscheidender Bedeutung, die Authentifizierung und Autorisierung dieser autonomen Endpunkte zu verstärken, um unbefugte Störungen zu verhindern.

Die ausgeklügelten Cyberangriffe der jüngsten Vergangenheit haben deutlich gemacht, wie dringend es ist, die Produktionslinie und die gesamte Lieferkette zu sichern, um die Geschäftskontinuität aufrechtzuerhalten. Aus diesem Grund setzen führende Unternehmen der Fertigungsbranche Phishing-resistente MFA-Verfahren, passwortlose Authentifizierung sowie kryptografische Schutzmaßnahmen ein, um sich gegen moderne Bedrohungen zu schützen, die sowohl auf IT- als auch auf OT-Ökosysteme abzielen. Die Sicherung der Mensch-Maschine-Kommunikation und der Maschine-zu-Maschine-Kommunikation sind wichtige Säulen, um eine umfassende Strategie zur Cyber-Resilienz zu entwickeln und zu gewährleisten.

Ein proaktiver Ansatz, bei dem Sie Ihre Daten und Produkte mit der richtigen Sicherheitslösung schützen, verschafft Herstellern die besten Voraussetzungen für den Erfolg – indem das Risiko von Ausfällen gemindert, die Erfolgsquote von Angriffen minimiert und wertvolles geistiges Eigentum geschützt wird. Darüber hinaus gewährleistet diese Strategie wesentliche Transparenz und kryptografische Kontrolle über jeden einzelnen Schritt im End-to-End-Fertigungsprozess.

Der YubiKey und das YubiHSM 2 von Yubico sind sichere, tragbare und benutzerfreundliche Lösungen, die speziell auf die Anforderungen von Fertigungsunternehmen zugeschnitten sind und sowohl ältere Infrastrukturen als auch moderne, cloudbasierte Systeme nahtlos unterstützen.

Durch die exklusive Registrierung und die weltweite schlüsselfertige Bereitstellung über „YubiKey as a Service“ unterstützt Yubico Sie dabei, hochsichere, hardwaregestützte Sicherheitslösungen auf globaler Ebene einzuführen.

Sicherheit ist nicht einfach eine defensive Maßnahme, sondern die Grundlage der industriellen Innovation. Die Stärkung Ihrer Grenzen durch hardwarebasierte Sicherheit schützt nicht nur Ihre Systeme, sondern gibt Ihnen auch die Macht, Ihre Zukunft zu gestalten. Mit Yubico steht Ihnen die Grundlage für Ihren sicheren Fertigungsbetrieb zur Verfügung.

Diese Marken vertrauen darauf:



Kontaktieren Sie uns
yubi.co/kontakt



Erfahren Sie mehr
So legen Sie mit Phishing-resistenter MFA los

Quellen

- ¹ IBM, X-Force Threat Intelligence Index 2026
- ² Industrial Cyber, BitSight warns of surge in ICS/OT Internet exposure, raising critical infrastructure cybersecurity concerns
- ³ IBM, Cost of a Data Breach Report 2025
- ⁴ Emerson, How Manufacturers Can Achieve Top Quartile Performance
- ⁵ Fortinet, 2025 State of Operational Technology and Cybersecurity Report
- ⁶ The Five Eyes Alliance et al., Secure connectivity principles for Operational Technology (OT)
- ⁷ Kurt Thomas, Angelika Moscicki, New research: Wie effektiv ist die grundlegende Konto-hygiene beim Schutz vor Hijacking
- ⁸ Industrial Cyber, BitSight warns of surge in ICS/OT Internet exposure, raising critical infrastructure cybersecurity concerns
- ⁹ ABI Research and Palo Alto Networks, The State of OT Security
- ¹⁰ Dragos, 2026 OT Cybersecurity Year in Review
- ¹¹ Fortinet, 2025 State of Operational Technology and Cybersecurity Report
- ¹² LandBase, Agentic AI Statistics Every GTM Leader Should Know in 2026
- ¹³ Varonis, 2021 Data Risk Report, Manufacturing
- ¹⁴ SentinelOne, Key Cyber Security Statistics for 2026
- ¹⁵ Amber Steel, LastPass Reveals 8 Truths about Passwords in the New Password Exposé
- ¹⁶ Gartner, 3 Simple Ways IT Service Desks Should Handle Incidents and Requests
- ¹⁷ Ponemon Institute, 2019 State of Password and Authentication Security Behaviors Report
- ¹⁸ Varonis, 2021 Data Risk Report, Manufacturing
- ¹⁹ Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report
- ²⁰ 451 Research, 2021 Yubico and 451 Research Study
- ²¹ Kurt Thomas, Angelika Moscicki, New research: Wie effektiv ist die grundlegende Konto-hygiene beim Schutz vor Hijacking
- ²² BlueVoyant, Managing Cyber Risk Across the Extended Vendor Ecosystem 2021
- ²³ Reuters, Target Settles 2013 Hacked Customer Data Breach for \$18.5 Million
- ²⁴ Reuters, Hackers Hold Hula Hoops Hostage in cyber-raid on Britain's KP Snacks
- ²⁵ SEC, Form 8-K SolarWinds Corporation



Über Yubico

Yubico (Nasdaq Stockholm: YUBICO) ist ein modernes Cybersicherheitsunternehmen mit dem Ziel, das Internet für alle sicherer zu machen. Als Erfinder des YubiKey setzen wir den Goldstandard für moderne, Phishing-resistente, hardwaregestützte Authentifizierung, verhindern Kontoübernahmen und machen sicheres Einloggen einfach.

Bereits seit 2007 gestalten wir aktiv globale Authentifizierungsstandards mit, haben an der Entwicklung von FIDO2, WebAuthn und FIDO U2F mitgewirkt und sind Wegbereiter des originalen Passkeys. Heute schützt unsere Passkey-Technologie Menschen und Unternehmen in über 160 Ländern und verändert grundlegend, wie die digitale Identität geschützt wird – vom Onboarding bis hin zur Kontowiederherstellung.

Weltweit vertrauen führende Marken, Regierungsbehörden und Institutionen mit höchsten Sicherheitsanforderungen auf unsere Lösungen. YubiKeys sind sofort einsatzbereit, funktionieren standardmäßig mit Hunderten von Apps und Diensten und bieten einen schnellen, passwortlosen Zugang ganz ohne Reibungsverluste oder Kompromisse bei der Sicherheit.

Wir glauben, dass jeder von starker Sicherheit profitieren können sollte. Im Rahmen unserer philanthropischen Initiative „Secure it Forward“ spenden wir YubiKeys an gemeinnützige Organisationen, die gefährdete Gemeinschaften unterstützen.

Unser Unternehmen mit Hauptsitzen in Stockholm, Schweden, und Santa Clara, Kalifornien, ist stolz darauf, von TIME als eines der 100 einflussreichsten Unternehmen und von Fast Company als eines der innovativsten Unternehmen ausgezeichnet worden zu sein. Weitere Informationen finden Sie unter www.yubico.com.