Sind Sie sicher?

Mit der zunehmenden Vernetzung in der Industrie stellt sich auch immer häufiger die Frage: Wie lassen sich die Daten in Konstruktion und Produktentwicklung überhaupt noch wirksam schützen? Sieben Fachleute aus Unternehmen und Forschung berichten aus der Praxis. **Von Andreas Müller**

DIE FRAGEN

1. **Wo sehen Sie heute das größte Gefährdungspotenzial für den Schutz der Produktdaten in Fertigungsunternehmen?**
2. **Welche Möglichkeiten bestehen, diesen Gefahren zu begegnen? Welchen Beitrag können PDM und Dokumentenmanagement leisten, um firmeninternes Know-how in der verteilten Produktentwicklung zu sichern?**
3. **Können Sie uns hierfür ein Beispiel nennen?**
4. **Wie verändern sich die Anforderungen an das sichere Datenmanagement durch Trends wie Internet der Dinge, Big Data und Cloud?**

Ulrich Isermeyer, Sr. Business Development Manager Acrobat/TCS/CCE, Adobe Systems GmbH:

1 Die größte Gefahr findet wahrscheinlich innerhalb des Unternehmens selber statt, wenn eigene Mitarbeiter mit krimineller Energie Daten über die sogenannte Shadow IT nach außen befördern. Durch Smartphones mit 3G/4G-Internet-Verbindung können Daten sehr leicht versendet werden. Wenn Fertigungsdaten an externe Zulieferer verschickt werden, dann werden diese in der Regel auch geschützt über VPN und andere Mechanismen. Wenn vom Zulieferer die Daten allerdings dann geöffnet wurden, hat das Fertigungsunternehmen keine Kontrolle mehr, was damit gemacht wird.

2 DMS-Systeme können den Zugriff, den Transport und die Speicherung der Daten kontrollieren. Auch cloudbasierte Systeme sind mittlerweile – entgegen anderer Meinungen – sehr sicher. Die Private Cloud Services können als eigene Instanzen über VPN mit Datenverschlüsselung beim Transport und bei der Speicherung der Daten Sicherheit gewährleisten. Wer die Daten als solches zusätzlich noch schützen möchte, kann dies im einfachsten Fall über ein sicheres Passwort tun, über Unterschriften, Zertifikate oder bei hochsensiblen Daten über das Digital Rights Management.

Ulrich Isermeyer, Sr. Business Development Manager Acrobat/TCS/ CCE, Adobe Systems GmbH.

3 Ein Beispiel für sicheres Datenmanagement in der Cloud sind die Managed Services (Private Cloud) bei der Adobe Creative Cloud, bei der die Daten auf einem Frankfurter Server gehostet werden. Die Dokumentenverschlüsselung für PDF kann mit Adobe Acrobat DC oder über den Adobe Experience Manager Forms mit Passwort oder Zertifikaten verschlüsselt werden. Beim Digital Rights Management bietet der Adobe Experience Manager – Dokumentunsicherheit ein Digital Rights Management an, bei dem PDF-Dokumente, 3D-PDF-Dokumente oder auch PDFs mit Dateianlagen, aber auch native CAD-Daten wie zum Beispiel PTC Creo hochverschlüsselt werden. Der kostenlose Acrobat Reader kann sogar auf mobilen Endgeräten diese Daten nach Eingabe von Login und Passwort entschlüsseln. Dabei kann der Hersteller kontrollieren, von wann bis wann die Daten sich öffnen lassen, oder er kann nachträglich die Rechte entziehen, so dass der Nutzer nichts mehr damit anzufangen in der Lage ist. Das Dokument funkt dabei regelmäßig „nach Hause" zum Server des Herstellers. Auch kann hier mit einem Protokoll festgestellt werden, was mit dem Dokument gemacht wurde. Beim Öffnen des Dokuments läßt sich forcieren, dass der Benutzername und die Uhrzeit quer über das Dokument eingeblendet ist und das Kopieren sowie Screenshots verhindert werden. Auch geänderte neue Versionen eines Dokuments können über Push Notifications eingeblendet werden.

4 Deutsche Industriekunden sind besonders sensibel beim Thema Datensicherheit und Cloud. Wir sehen aber, dass alle Cloud-Provider mittlerweile immer heftigere Sicherheitsmechanismen, zum Beispiel Hochverschlüsselung beim Transport und bei „at rest" einbauen, die in Kombination mit einer Private-Cloud-Umgebung den Datenklau minimieren oder fast unmöglich machen. Durch solche technologischen Fortschritte wird sich auch in Deutschland die Verhaltensweise und das Vertrauen in die Cloud in absehbarer Zeit sicherlich ändern. Adobe setzt auf diese neuesten Sicherheitsmöglichkeiten in allen Cloud-Lösungen wie Document Cloud, Creative Cloud und Marketing Cloud.

Thomas Deutschmann, CEO, Brainloop:

1 Die eigenen Mitarbeiter stellen ein großes Gefährdungspotenzial dar, stehen allerdings oft nicht im Fokus. Vielmehr konzentrieren sich die meisten Firmen auf die Abwehr von Hackerangriffen, die oft tief in das firmeninterne System eindringen. Das ist eine zweckmäßige Maßnahme. Häufig wird dabei allerdings übersehen, dass die eigenen Mitarbeiter das geistige Eigentum der Firma mitunter auf dem Silbertablett präsentieren. So werden beispielsweise Produkt- und Konstruktionsdaten sowie Verträge nicht selten als E-Mail-Anhang versendet. Laut einer Studie von KPMG nannten 87 Prozent der befragten Unternehmen „Unachtsamkeit" der Mitarbeiter als Hauptfaktor für digitale Delikte. So haben Hacker leichtes Spiel.

Viele Datenverluste lassen sich schon vermeiden, indem folgende Punkte beachtet werden:

■ **Verschlüsselter Informationsaustausch**
E-Mail-Anhänge sind meist nicht verschlüsselt oder so aufwändig zu chiffrieren, dass entsprechende Lösungen oft von Mitarbeitern umgangen werden. Ein verschlüsselter Datenaustausch in einem sicheren Datenraum ist eine denkbar einfache und sichere Alternative für den Datenschutz. Die Nutzung

ist selbsterklärend und intuitiv. So wird eine reibungslose und sichere Zusammenarbeit mit Dienstleistern, Lieferanten und Kunden gewährleistet.

■ Mangelnde Kenntnis der Möglichkeiten einer geschützten Zusammenarbeit

Im Zeitalter des Internet of Things fallen riesige Mengen an Produktdaten an. Hier wird in Zukunft ein großes Risikopotenzial liegen. Unternehmen sollten sich eingehend über Lösungen für eine sichere Arbeitsumgebung erkundigen und sie einsetzen.

■ Individuelle Kategorisierung

Der Zugriff auf Dokumente sollte individuell gestaltet werden. So können sie beispielsweise nur zum Lesen bereitstehen, jedoch nicht gespeichert, ausgedruckt oder weitergeleitet werden. Auch lässt sich in einem sicheren Datenraum genau nachvollziehen, welches Dokument wann und von wem hoch- oder heruntergeladen wurde.

2 Die genannten Lösungen unterstützen dabei, sensible Daten umfassend zu schützen. Dokumente können im „Read-only"-Format eingesehen, jedoch nicht verändert werden. Hinzu kommt die Möglichkeit, ein Wasserzeichen sowie eine Dokumenten-ID einzufügen. Durch diese Maßnahmen wird der Schutz zusätzlich erhöht und die Integrität der Dokumente gewährleistet – eine Manipulation ist so nicht möglich. Zudem erlaubt eine revisionssichere Protokollierung die lückenlose Nachvollziehbarkeit aller Aktivitäten. Mit einer Rollen- und Berechtigungsvergabe lässt sich individuell bestimmen, wer in welchem Umfang Einblick in die genannten Dokumente erhält. Vertrauliche Inhalte werden sogar in den eigenen Reihen vor dem Zugriff des technischen Personals geschützt. Sowohl Systemadministratoren als auch Mitarbeiter des Rechenzentrums haben keinen Zugriff auf Inhalte.

3 Ein Szenario lässt sich jedem Fertigungsprozess entnehmen. Hat die Entwicklungsabteilung ein neues Produkt entworfen, das in Serie gehen soll, müssen viele Faktoren bedacht und externe Dienstleister eingebunden werden. Spätestens wenn externe Partner als Zulieferer bei der Herstellung mitwirken, treten gewöhnlich erste Sicherheitslücken auf. Lieferanten müssen schließlich Zugriff auf die relevanten Informationen erhalten. Damit diese Daten nicht per E-Mail versendet werden, ist ein virtueller Datenraum zu empfehlen. So kann Lieferanten individuell eine Berechtigung über Umfang und Inhalte der Dokumentennutzung eingeräumt werden.

Thomas Deutschmann, CEO, Brainloop.

4 Das Internet of Things ist noch gar nicht zu Ende gedacht und birgt ein immenses Risikopotenzial. Häufig sind Produktentwickler mehr auf Prozesse als auf die Sicherheit bedacht und überlassen das Thema Sicherheit gerne anderen. Die Sicherheit muss aber Teil jeder Lösung und von vornherein Teil des Konzepts sein. Sonst ist sie zum Scheitern verurteilt. Ein Sonderthema ist dabei der Datenschutz. Damit sind gegebenenfalls wieder andere Experten in der Organisation befasst. Auch die Übertragung von personenbezogenen Daten muss gut durchdacht und transparent sein. Die Cloud bietet für das sichere Datenmanagement ebenso viele Chancen wie Risiken. Gerade die Safe-Harbor-Entscheidung des Europäischen Gerichtshofs zum Thema des Zugriffs durch ausländische Behörden hat die Schwächen deutlich gemacht. Durch solche Begebenheiten wird es immer wichtiger, Daten in lokalen, ausfallsicheren Rechenzentren im eigenen Land zu speichern.

Frank Patz-Brockmann, Mitglied der Geschäftsleitung und Entwicklungsleiter bei CONTACT Software:

1 Unseres Erachtens geht die weitaus größte Gefahr von denjenigen aus, die mit den Daten umgehen. Neben Lecks, die durch den sorglosen Umgang mit Daten entstehen, ist das wichtigste Problem der Missbrauch durch eigene Mitarbeiter, die beispielsweise das Unternehmen verlassen, oder Personen bei Geschäftspartnern, die Zugriff auf vertrauliche Daten erhalten.

Die Gefährdung durch technische Angriffe „von außen" ist ebenfalls nicht zu vernachlässigen. Auch hier adressieren die meisten dieser Angriffe zunächst die Schwachstelle Mensch, indem zum Beispiel Passwörter ausgespäht oder geraten werden oder Schadsoftware mit Hilfe nichtsahnender Anwender eingeschleust wird.

2 Der wichtigste Beitrag jeder Datenmanagementlösung ist die geordnete Ablage von Daten und die überprüfbare Anwendung

Frank Patz-Brockmann, Mitglied der Geschäftsleitung und Entwicklungsleiter bei CONTACT Software.

von Richtlinien für den Umgang damit. Darüber hinaus sollte die grundlegende Systemarchitektur Schutzkonzepte unterstützen. So dürfen PDM-Vaults grundsätzlich nicht als Laufwerke erreichbar sein, und die Systeme müssen transparente Verschlüsselungsverfahren unterstützen oder selbst anbieten.

3 Es ist nahezu unmöglich, differenzierte Zugriffsrechte für auf Fileshares „herumfliegende" Daten zu vergeben. Unser Produkt CIM DATABASE bietet dafür ein regelbasiertes Rechtesystem, das die Vergabe von differenzierten Zugriffsrechten komplett automatisiert. Das erhöht nicht nur die Sicherheit, sondern senkt auch die Betriebskosten gewaltig.

4 Alle Welt schaut ja zunächst auf die Risiken einer „Cloud". Dahinter steckt die Frage, ob man Anbietern von internetbasierten Diensten und Lösungen vertrauen kann. Einerseits haben qualifizierte Anbieter größtes Interesse daran, die Daten ihrer Kunden zu schützen. Andererseits wirft der Einfluss von Organisationen wie der NSA natürlich die Frage auf, ob sich selbst große Anbieter staatlichen Übergriffen entziehen können. Wer also Geheimnisse hat, die nur den Wettbewerb im eigenen Land interessieren, ist bei Cloud-Anbietern wahrscheinlich gut aufgehoben.

IoT und Big Data gehören insofern zusammen, als dass das Internet der Dinge viele Daten produziert, die durch „Big Data" auszuwerten sind. Hier gilt: Datensparsamkeit und vernünftige Richtlinien zur Vernichtung nicht mehr benötigter Daten sind unbedingt notwendig. Daten, die es nicht mehr gibt, können einem Angreifer keine ungewünschten Informationen liefern. Wer keine Geheimnisse hat, kann keine verlieren!

Dipl.-Inform. Siniša Đukanović, Fraunhofer Institut, Fraunhofer-Institut für Sichere Informationstechnologie SIT:

1 Für sensible Produktdaten sollten die Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität erfüllt werden. Die Verfügbar-

DIE FRAGEN

1. **Wo sehen Sie heute das größte Gefährdungspotenzial für den Schutz der Produktdaten in Fertigungsunternehmen?**
2. **Welche Möglichkeiten bestehen, diesen Gefahren zu begegnen? Welchen Beitrag können PDM und Dokumentenmanagement leisten, um firmeninternes Know-how in der verteilten Produktentwicklung zu sichern?**
3. **Können Sie uns hierfür ein Beispiel nennen?**
4. **Wie verändern sich die Anforderungen an das sichere Datenmanagement durch Trends wie Internet der Dinge, Big Data und Cloud?**

keit kann bereits heute durch den Einsatz von PDMs und Backup-Lösungen gewährleistet werden, während Integrität und Vertraulichkeit von derartigen Lösungen oft vernachlässigt werden, oder der Schutz der Daten endet, sobald diese das PDM- beziehungsweise Office-Netzwerk verlassen. Szenarien, in denen Daten aber auch über Unternehmensgrenzen hinweg übertragen werden, dürften im Zuge von I4.0, verteilter Produktion und „Cloudifizierung" zur Regel werden. Ohne explizite Mechanismen zum Schutz der Daten in verteilten Umgebungen droht die ungewollte Abwanderung von Know-how.

Dipl.-Inform. Siniša Đukanović, Fraunhofer Institut, Fraunhofer-Institut für Sichere Informationstechnologie SIT.

2 PDM und Dokumentenmanagement können im verteilten Produktionsumfeld nur dann zur Daten-Integrität und -Vertraulichkeit beitragen, wenn sie die Daten über ihren gesamten Lifecycle, also Erzeugung, Übertragung und Verarbeitung, hinweg schützen. Es reicht nicht, wenn Daten im PLM verschlüsselt vorliegen, dann aber in Form von Fabrikationsdaten unverschlüsselt auf eine Werkzeugmaschine übertragen werden. PDM und Datenmanagement müssen nahtlos mit nachgelagerten Schutzmechanismen zusammenarbeiten, um einen wirksamen Schutz von Know-how zu gewährleisten.

3 Der Schutz der Fabrikationsdaten erfordert weitere Standards und eine Weiterentwicklung der Maschinenhersteller dahingehend, dass zum Beispiel PDM-Systeme Daten sicher zu Maschinen übertragen können und diese dort vor Zugriff, etwa auch durch Wartungspersonal, geschützt sind.

4 Das Internet der Dinge, die dezentrale Produktion und die zugehörigen autonom agierenden Maschinen sind mit einer zunehmenden Erzeugung und Übertragung von Daten verbunden. Datenmanagementlösungen müssen diese Veränderungen berücksichtigen, um die Schutzziele weiterhin zu erreichen. Sie müssen leistungsfähig genug sein, um die anfallenden Datenmengen bewältigen und über Unternehmensgrenzen hinweg absichern zu können.

Während die Datenhaltung in der Vergangenheit lokal erfolgte, ergeben sich durch Cloud-Lösungen vor allem im Kontext Big Data Möglichkeiten zur Auslagerung und entfernten Verarbeitung. Hierdurch hält eine weitere Partei mit eigenen Interessen und eigenen Schwachstellen Einzug in die Unternehmensprozesse. Bevor ein Unternehmen Daten in die Cloud ausgelagert, sollte es sich genau überlegen, welche Daten vor was und vor wem zu schützen sind. Je nachdem sollten dann technische Schutzmaßnahmen wie Kryptografie soweit wie möglich ausgeschöpft werden. Das verbleibende Restrisiko muss zudem vertraglich zwischen allen beteiligten Parteien abgesichert werden.

Peter Schmitt, Geschäftsführer, GAIN Software GmbH:

1 Ich sehe erstens eine große Gefahr im Austausch von Daten (2D und 3D) mit Zulieferern. Hier lässt sich nicht zu 100 Prozent sicherstellen, dass das Know-how nicht doch weitergegeben wird. Zweitens: Ein Datenverwaltungssystem ist unabdingbar. Nur ein solches System kann den Umgang mit Daten protokollieren. Wer hat wann was mit einem Dokument gemacht? Und schließlich: Ohne PDM-System stehen dem nicht autorisierten Zugriff von außen alle Türen offen.

Peter Schmitt, Geschäftsführer, GAIN Software GmbH.

2 Dokumente (Dateien) sollten sicher in einem Archiv verwahrt werden, dass von außen nicht zugänglich ist. Das Abrufen von Dokumenten ist nur über das PDM-System möglich. Es gilt, Dokumente (Dateien) mit einem Zertifikat zu schützen (SSL-Verschlüsselung). Außerdem ist es ratsam, vereinfachte Daten (2D- und 3D-CAD-Dokumente) zur Verfügung zu stellen, aber das ist eher eine Richtlinie als Aufgabe eines PDM-Systems.

3 Nur bestimmte Personen oder Gruppen haben über ein PDM-System Zugriff auf sensible Dokumente. Den Gruppen sollten jeweils unterschiedliche Rechte beim Lesen, Schreiben usw. eingeräumt werden. Alle Ereignisse, die im Zusammenhang mit der Datenverarbeitung stehen, müssen sich lückenlos protokollieren lassen. Das betrifft beispielsweise Aktionen wie Dokumente öffnen, drucken oder per E-Mail versenden.

4 Hier liegt der größte Sicherheitsaspekt und vor allem das Risiko bei den Anbietern der Plattformen. Es gibt viele und wer sorgt wirklich für die notwendige Sicherheit? Heute kann niemand mit Bestimmtheit sagen, welche Plattform für den Austausch von sensiblen Daten tatsächlich sicher ist. Unternehmen, die Daten austauschen möchten, müssen gemeinsam einen zuverlässigen Anbieter für die Austauschplattform suchen. Dropbox etwa ist schlecht, ein Anbieter wie Centron dagegen stellt Unternehmen eigene Server bereit, die von den Unternehmen selbst kontrolliert werden können (eigenes Cloud-System). Das Datenmanagement muss die Daten von vornherein verschlüsseln, da der Zugriff von außen auf Austauschplattformen nicht gänzlich ausgeschlossen werden kann.

Und schließlich sollte die Verweildauer von Daten auf Austauschplattformen kurz und begrenzt sein. Hierfür könnte unter Umständen ein PDM-System sorgen.

Raimund Schlotmann, Geschäftsführer der PROCAD GmbH & Co. KG:

1 Größter Risikofaktor ist und bleibt der Mensch, der Daten entweder fahrlässig oder mutwillig weitergibt beziehungsweise sie ungewollt anderen zugänglich macht. Dies

Raimund Schlotmann, Geschäftsführer der PROCAD GmbH & Co. KG.

ist umso gefährlicher, je unstrukturierter und unabhängiger voneinander die Stellen sind, an denen Informationen im Unternehmen abgelegt werden: im Windows Explorer, auf lokalen Verzeichnissen, in diversen Applikationen oder auf mobilen Geräten.

2 Ein PDM/DMS-System wie PRO.FILE kann ein zentrales Datenrückgrat (Product Data Backbone) bereitstellen, das alle Dokumente zusammenführt und an einer zentralen Stelle sichert. So entsteht ein zentraler geschützter Bereich, in dem alle Mitarbeiter Produktdaten strukturiert und sicher ablegen. Sämtliche Entnahmen beziehungsweise Änderungen werden dokumentiert und können so nachvollzogen werden. Über die Benutzerverwaltung werden die Zugriffsrechte rollenabhängig gesteuert. Der wichtigste Beitrag zur Sicherung des Firmen-Know-hows ist also die Zusammenführung des Wissens im Product Data Backbone.

Wird Produktentwicklung mit Partnern betrieben, müssen PDM- und DMS-Lösungen sicherstellen, dass beim Austausch der Produktdaten (CAD-Modelle, Prüf- und Testunterlagen) kein Wissen abfließt. Der traditionelle Datenaustausch – per FTP oder gar E-Mail – ist aus Sicherheitsgründen bedenklich.

Die Lösung, vor allem in komplexen Projekten mit vielen Beteiligten, sind Datenaustausch-Plattformen mit virtuellen Projekträumen wie zum Beispiel PROOM, die direkt in das PLM-System integriert sind und für die der Administrator Berechtigungen vergeben kann. Damit lässt sich auch der externe Produktdatenaustausch bis hin zu kompletten Baugruppeninformationen automatisiert durchgängig dokumentieren und protokollieren. Durch den kontrollierten Zugriff werden außerdem Änderungskonflikte vermieden und damit der Abstimmungsaufwand reduziert.

3 Der Automobil-Zulieferer Muhr & Bender tauscht technische Dokumente mit externen Partnern über unsere Plattform PROOM aus. Die Lösung deckt die branchentypischen Anforderungen im Maschinen- und Anlagenbau ab und ist direkt an das PLM-System PRO.FILE angebunden. Die Konstruktions- und Entwicklungsabteilung übermittelt darüber große CAD-Dateien an externe Konstruktionsbüros. Für den gezielten Datentausch mit unterschiedlichen Partnern und Benutzergruppen wurden jeweils geschützte und getrennte virtuelle Projekträume eingerichtet.

4 Cloud-basierende Lösungen im Produktdatenmanagement eröffnen die Chance, von überall her auf die Daten zugreifen zu können. Je umfassender die Datenmengen, die durch öffentliche oder private Netze fließen, desto höher natürlich auch die Gefahr eines unkontrollierten Zugriffs. Zusätzliche Sicherheitsmaßnahmen sind unerlässlich. Dabei stellt die Cloud in dieser Hinsicht per se gar keine größere Gefährdung dar, wenn entsprechende Maßnahmen ergriffen werden. In der neuen vernetzten Welt gibt es keine Alternative zum elektronischen Austausch – die Sicherheit muss über im Netz gesicherte Daten erfolgen. Abschottung ganzer Systeme hinter einer Firewall gehört der Vergangenheit an.

Das heißt, bei mehr Kommunikation, mehr Daten und mehr Wegen, die über das Firmentor hinausgehen, muss stärker als bisher auf Rechtevergabe und Verschlüsselung geachtet werden. Dann ist auch bei größeren Datenmengen und in der Cloud ein sicheres Datenmanagement möglich.

Wolfgang Völker, Leiter Produktmanagement der WIBU-SYSTEMS AG:

1 Einerseits bietet die wachsende Vernetzung heutzutage Vorteile bei Service, Steuerung und Überwachung von Geräten und ganzen Industrieanlagen aus der Ferne. Anderseits können Hacker, Wirtschaftsspione oder Saboteure über diese Schnittstelle, die nach außen geht, eindringen und wertvolles Know-how stehlen oder die Produktion manipulieren. Aus meiner Sicht ist der größte Fehler, dass Unternehmen eine Firewall um ihr Gesamtnetzwerk bauen und sich sicher fühlen. Sie vergessen, ein Schutzkonzept für das Produktionsnetzwerk und das darin enthaltene geistige Eigentum aufzubauen.

Wolfgang Völker, Leiter Produktmanagement der WIBU-SYSTEMS AG.

2 Eine technisch-präventive Lösung wie CodeMeter erlaubt, ein Schutzkonzept für die Produktion aufzubauen, denn es wirkt, bevor ein Schaden entstehen kann. Das Konzept basiert auf der Ver- und Entschlüsselung der Software der Maschinen und Geräte einschließlich der sicheren Speicherung von Schlüsseln. Zusätzlich wird der Programmcode vor Manipulation durch Einsatz von elektronisch signiertem Code und Prüfung gegen eine Zertifikatskette geschützt. Das heißt, jede einzelne Maschine oder jedes Gerät soll durch technische Maßnahmen gesichert werden. Grundsätzlich muss das Unternehmen darüber hinaus dafür sorgen, dass durch Schulungen und Trainings das Sicherheitsbewusstsein der Mitarbeiter geschärft wird, damit sie mögliche Einfallstore potenzieller Eindringlinge identifizieren und sofort verschließen.

3 Am Beispiel einer Stickmaschine wird deutlich, wo überall das zu schützende geistige Eigentum steckt. Ist die Steuerungssoftware verschlüsselt, können Produktpiraten das darin befindliche Know-how weder analysieren noch unberechtigt benutzen. Viel Wissen steckt auch in Service-Unterlagen oder in technischen Zeichnungen. Werden diese PDF-Dokumente verschlüsselt und mit Berechtigungen versehen, können nur die gewünschten Personen mit diesen Informationen arbeiten. Darüber hinaus muss unbedingt die Integrität der einzelnen Stickmaschine gesichert werden, damit Saboteure am Manipulieren behindert werden. Das geeignete Schutzsystem signiert die Embedded-Software der Stickmaschine digital. Nur die korrekt signierten Programmteile werden vom Schutzsystem entschlüsselt und ausgeführt. Passt die Signatur nicht, wird die manipulierte Software nicht ausgeführt und ein möglicher Schaden verhindert.

4 Durch die immer weitergehende Vernetzung verschwinden zunehmend die harten Grenzen der Infrastruktur. Damit gibt es neue Einfallstore, zum Beispiel durch den Datentransfer in und aus der Cloud. Die Daten müssen daher vor unberechtigter Veränderung innerhalb und außerhalb des Unternehmens geschützt werden. Eine Verschlüsselung ist oft nicht möglich, da die Daten auch in den intelligenten Speichersystemen weiterverarbeitet werden. Signiert aber der Erzeuger die Daten bei der Erstellung, kann die Integrität auch nach Abruf aus Cloud-Systemen überprüft werden. *(anm)* ■