Eine Themenbeilage der
Heise Medien GmbH & Co. KG

SICHERHEIT & DATENSCHUTZ

I 2019

IoT, Verschlüsselung und Industrie 4.0

IoT-Security:
Wie sich vernetzte Geräte absichern lassen

Log- und Protokollmanagement:
Wann SIEM-Lösungen Alarm schlagen

IIoT-Sicherheitsarchitektur:
Was Servicetechnikern die Arbeit erleichtert

E-Mail-Verschlüsselung:
Warum Johnny jetzt seine Mails verschlüsselt

Digitale Signatur:
Wie die Hausbank zum ID-Provider wird

Zertifikatsmanagement:
Womit sich das MIM-Tool effektiver nutzen lässt

Quantum Computing:
Was die Quantentechnologie mit sich bringt

www.it-security-und-management.de

powered by: TeleTrusT Pioneers in IT security. iX

// heise devSec()

24.–26. September 2019

Print Media Academy, Heidelberg

DIE KONFERENZ FÜR SICHERE SOFTWARE- UND WEBENTWICKLUNG

PROGRAMM ONLINE!

Sichere Software beginnt vor der ersten Zeile Code…

AUSZUG AUS DEM PROGRAMM:

- Der lange Weg zum sicheren Code
- Moderne Sicherheitsstandards für Web-Applikationen
- Safety & Security by Design
- Automatische Security-Tests in Continuous Integration
- Datenschutz jenseits von EU-DSGVO
- Security-Fallstricke von Python-Applikationen in produktiven Umgebungen
- Eine DevSecOps-Geistergeschichte
- Node.js/NPM Security
- Bedrohungsanalyse in der Praxis
- LFI/RFI – Remote Code Execution einfach gemacht

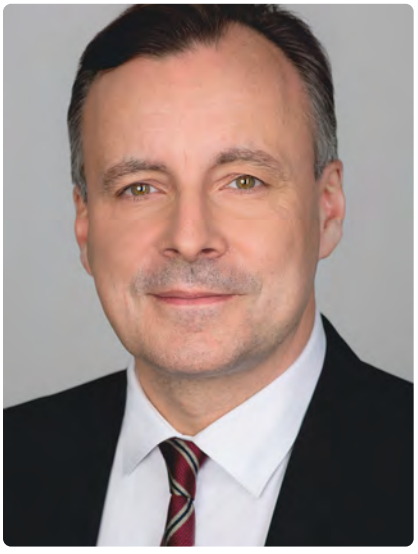
www.heise-devsec.de

Goldsponsoren RIGS IT, WIBU SYSTEMS

Silbersponsor RIPSTECH

Veranstalter heise Security, heise Developer, dpunkt.verlag

Industrie 4.0 braucht IT-Sicherheit



Liebe Leserinnen und Leser,

gleich zu Anfang des Jahres 2019 wurden Politiker und Journalisten Opfer eines digitalen Angriffs. Dabei ist deutlich geworden, dass die Bedrohung durch Hackerangriffe, Cyberkriminelle und Datenlecks nicht nur nach wie vor unverändert hoch ist, sondern zugleich präsenter denn je, auch in den Medien. Unsichere IT stellt einen Sachmangel dar. Es bedarf deshalb einer konsequenten Anwendung von Sanktionen und Haftungsregeln. Notwendig sind Mechanismen, die Angriffe grundsätzlich verhindern. Zu erreichen ist das beispielsweise durch die favorisierte verstärkte Virtualisierung, Separierung und Datenflusskontrolle in IT-Systemen.

Kommen nun neue Impulse aus der Politik, um die technologische Hoheit über kritische IT-Anwendungen nicht zu verlieren? So viel ist sicher: Insbesondere vertrauenswürdige, robuste IT-Systeme, die die Probleme „Softwaresicherheit“ und „Malwarebefall“ adressieren, sollten seitens der Politik gefördert werden. Dabei würde es helfen, wenn die rechtliche Verantwortung für IT-Lösungen erhöht würde, um Hersteller und Dienstleister zu mehr IT-Sicherheit zu motivieren. Ein pragmatischer und ausgewogener Rechtsrahmen sollte dem Schutzbedürfnis der Anwender ebenso gerecht werden wie der unternehmerischen Risikokalkulation.

IT-Sicherheitslösungen für Industrie 4.0 müssen direkt umgesetzt werden, damit Deutschland eine Vorreiterrolle bei der IT-Sicherheit der Leitindustrien übernehmen kann. Bei der Erarbeitung von Lösungen, Maßnahmen und Produkten rund um Cyber Security sollten verstärkt Synergien zwischen Anwendern und IT-Sicherheitsindustrie genutzt werden. Usability- und Betriebsanforderungen großer IT-Architekturen müssen zudem an den Bedürfnissen des Mittelstandes ausgerichtet werden.

Als Bundesverband IT-Sicherheit e.V. (TeleTrusT) möchten wir die Industrie bestmöglich unterstützen. TeleTrusT hat mit seiner AG „Smart Grids/Industrial Security“ ein Prüfschema für Produkte nach IEC 62443-4-2 „Industrielle Kommunikationsnetze – IT-Sicherheit für industrielle Automatisierungssysteme“ erarbeitet und mit anderen Verbänden erörtert. Ziel des TeleTrusT-Prüfschemas ist, unter einschlägigen Produkten ein hohes und gleichartiges IT-Sicherheitsniveau sicherzustellen und dieses von unabhängigen Prüfstellen nach einheitlichen Kriterien prüfen zu lassen.

Die IT-Sicherheitsbranche in Deutschland steht auch im Jahr 2019 mit ihren Experten vor großen Herausforderungen. Die vorliegende Themenbeilage fokussiert auf innovative Lösungen rund um IoT und Industrie 4.0, bietet iX-Lesern aber noch weitere interessante Beiträge. Gemeinsam mit den TeleTrusT-Mitgliedern wünsche ich Ihnen eine Lektüre, die zum Nachdenken und Handeln einlädt.

Dr. Holger Mühlbauer
Geschäftsführer TeleTrusT – Bundesverband IT-Sicherheit e.V.

Inhalt

Sichere Verwaltung gewachsener IT-Landschaften

Mit digitalen Zertifikaten erreichen wir mehr Sicherheit in der vernetzten Welt

Internet of Things, Industrie 4.0 und Digitalisierung sind die Schlüsselbegriffe für die nächste große industrielle Revolution. Doch in einer global vernetzten Welt müssen wir zur Sicherheit aller Teilnehmer höchste Ansprüche an den Schutz sensibler Daten und ihre Infrastruktur im Allgemeinen stellen.

Wenn es um die Implementierung einer mehrschichtigen, identitätsbasierten Sicherheitsumgebung geht, ist ein zuverlässiges Identitätsmanagement auf der Metaebene der Anwender ein erster Schritt in Richtung einer sicheren Infrastruktur. Das Verschlüsseln von Geräten, als den eigentlich neuralgischen Punkten, ist allerdings weitaus elementarer. Genau hier liegt die Herausforderung, da aufgrund der Komplexität bisher gar keine oder nur wenige Anstrengungen für ein adäquates Zertifikatsmanagement unternommen wurden. Auch wenn neue Technologien theoretisch zur Verfügung stehen – Stichwort: Blockchain – werden am Ende weiterhin Schlüssel und Zertifikate in der über Jahre hinweg heterogen gewachsenen IT-Infrastruktur der einzelnen Marktteilnehmer eine zentrale Rolle spielen.

Komplexe Umgebungen

Für die Administration von Public-Key-Infrastrukturen mit einer Vielzahl an Geräten und Usern sind die üblichen Bordmittel jedoch nicht ausreichend. Wenn es um die Synchronisierung von Benutzern, Gruppen und Kontakten zwischen Verzeichnisdiensten geht, greifen viele Unternehmen auf den Microsoft Identity Manager (MIM) – früher Forefront Identity Manager (FIM) – zurück. Eine Kernkomponente dieses leistungsfähigen Identity- und Access-Management-Tools ist die Verwaltung digitaler Zertifikate. Die umfangreiche Lösung von Microsoft erfordert allerdings einen erheblichen manuellen administrativen Aufwand.

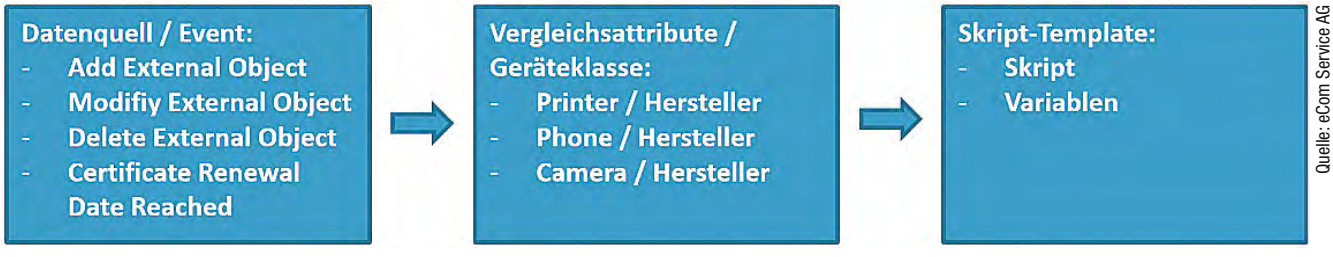
Ein Add-on bringt neue Möglichkeiten

An dieser Stelle setzen Lösungen wie die Add-on-Software m2trust an. Ihr Einsatz gestaltet auf der einen Seite über eine klar strukturierte, benutzerfreundliche und plattformunabhängige Benutzeroberfläche Workflows bei der Arbeit mit MIM/FIM deutlich schlanker. Administrationsprozesse lassen sich intuitiv über assistentengestützte Dialoge durchführen. Zusätzlich sorgt die Möglichkeit, Menüpunkte abhängig von der Verwaltungsrolle auszublenden, für mehr Übersicht und damit auch für weniger Bedienungsfehler. Prozesse werden auf diese Weise auf das Notwendige reduziert.

Auf der anderen Seite ermöglicht der Core Service die Erweiterung von MIM/FIM um zusätzliche Funktionen, wie die Automatisierung der Zertifikatsverwaltung, die Integration von Nicht-Windows-Systemen und Certificate Authorities (CA) von Drittanbietern sowie die Aufbringung und Verwaltung von Zertifikaten auf mobilen Endgeräten. Dabei läuft der m2trust Core Service, ohne dass es der Anwender merkt, im Hintergrund. Über eine browserbasierte Benutzeroberfläche lassen sich automatische Aktionen als Folge von definierbaren Ereignissen konfigurieren. Dies und eine Vielzahl von Schnittstellen ermöglichen die Harmonisierung verschiedenster heterogener Systeme.

Mobile Endgeräte im Griff

Heutige heterogen gewachsene IT-Landschaften stellen ein effektives Zertifikatsmanagement vor große Herausforderungen. Neben Softwarelösungen von Drittherstellern, müssen auch eine Vielzahl unterschiedlicher Geräte und deren Betriebssysteme nahtlos in die unternehmenseigene Public-Key-Infrastruktur eingebunden werden. Ein Beispiel ist hier das Widerrufen von Zertifikaten für mobile Endgeräte bei Verlust durch einen Mitarbeiter oder auch deren rechtzeitige Erneuerung. Automatisierte Lösungen für solche Anwendungsfälle existieren im Grunde nicht, weshalb eine konsequente Durchsetzung der



Quelle: eCom Service AG

Cert Deployment ermöglicht die Anbindung und Zertifikatsverteilung an zahlreiche Fremdsysteme und Geräteklassen.

Corporate Compliance sowie ein reibungsloser Betrieb oftmals kaum realisierbar ist.

Der unter MIM/FIM hohe Aufwand für das Aufbringen und Verwalten von Zertifikaten auf mobilen Endgeräten wird durch den Einsatz des Mobile Device Management (MDM) Connector signifikant reduziert. Durch die Integration des MDM ins Zertifikatsmanagement laufen die Zertifikatslebenszyklusprozesse für mobile Endgeräte selbstständig ab. Die erforderlichen Verzeichniskonten für jedes Endgerät mit provisionierten Zertifikaten werden automatisch erzeugt oder können alternativ auf ein gemeinsames Dienstekonto eingebunden werden. Der Connector arbeitet sowohl mit Generic SCEP als auch mit herstellerspezifischen Systemen wie MobileIron Core, Citrix XenMobile und in Kürze auch SAP Afaria.

Vielfältige Anwendungsbereiche

Das Add-on ermöglicht es über unterschiedlichste Schnittstellen, den kompletten Zertifikatslebenszyklus, gerade in solchen IT-Landschaften, automatisch abzubilden. So lässt sich über diverse Connectoren auch Software von Drittherstellern anbinden und für das FIM/MIM-Zertifikatsmanagement über ein Webservice-Interface nutzbar machen. Über die Microsoft-Zertifikatsverwaltung lassen sich dadurch vollumfänglich Beantragungen, Erneuerungen und Sperrungen von Zertifikaten durchführen, Schlüssel und Zertifikate sicher wiederherstellen und Zertifikatsinformationen abrufen. Zertifikatsprofile werden, wenn vom Webservice unterstützt, automatisch abgeglichen und synchronisiert. Für eine lückenlose Dokumentation sorgen weitreichende Protokollierungs- und Auditfunktionen.

Verzeichnisse, Betriebssysteme und Endgeräte verwalten

Der Directory Connector – ein weiteres Feature – automatisiert Prozesse vollständig auf Basis von Verzeichnisänderungen. Ohne weiteren manuellen Eingriff werden solche Ereignisse erkannt und entsprechende flexibel konfigurierbare Aktionen und Prozesse im FIM/MIM-Zertifikatsmanagement ausgelöst. Zertifikatsobjekte und Profile, die sich im Verzeichnisdienst und in der Zertifikatsdatenbank befinden, werden effektiv gesäubert und konsistent gehalten. Das bedeutet auf Anwenderseite weniger Aufwand und geringere Supportkosten. Darüber hinaus stehen umfangreiche Protokollierungs- und Auditfunktionen bereit. Der Directory Connector ist sowohl für Active Directory als auch für weitere Verzeichnisdienste wie OpenLDAP verfügbar.

In der Praxis wird häufig mit heterogenen Systemen gearbeitet. Das hat teilweise historische, teilweise praktische Gründe. Für die Integration nicht Windows-basierter Systemlandschaften mit ihren unterschiedlichen Endgeräten und Betriebssystemen, kommt der Deployment Connector zum Einsatz, um diese optimal in die Zertifikatsverwaltung einzubinden. Darüber hinaus automatisiert der Deployment Connector wichtige Betriebsaufgaben. So lassen sich Zertifikate automatisch für Linux- und Macintosh-Systeme, aber auch für diverse Peripheriegeräte wie Drucker und IP-Telefone ausstellen, erneuern und sperren.

Fazit

Digitale Zertifikate sind ein elementarer Bestandteil für die Sicherheit von Unternehmen und deren IT-Infrastruktur in einer vernetzten Welt. Die Zertifikatsverwaltung erfordert ab einer bestimmten Komplexität den Einsatz spezieller Software wie MIM/FIM.

Mit der Add-on-Software m2trust können Administratoren das Potenzial von MIM/FIM effektiver nutzen, Prozesse automatisieren und Kosten senken. Zudem werden sie in die Lage versetzt, Produkte in die Public-Key-Infrastruktur einzubinden, die nicht aus der Microsoft-Welt stammen, und deren Standards zu harmonisieren. Im Ergebnis bedeutet dies weniger Aufwand sowie mehr Sicherheit, Compliance und zufriedenere Nutzer.

Daniel Dyroff
eCom Service AG

Dank Vertrauensnetzwerken qualifiziert signieren

Rechtskonformes Signieren digitaler Dokumente wird deutlich kundenfreundlicher

Die letzte große Hürde für die qualifizierte Signatur fällt: Mittlerweile können bereits vorhandene Evidenzen von Banken genutzt werden, um eine Person eindeutig zu identifizieren. Das Protokoll, das auf OAuth-2.0-Technologie basiert, ermöglicht hierbei Vertraulichkeit der ausgetauschten Daten.

Ein Dokument elektronisch zu signieren, ist nicht nur für den Kunden praktisch und zeitsparend, es ist auch für Unternehmen ein großer Vorteil: Ohne die Digitalisierungskette zu unterbrechen, können Firmen Dokumente in einem End-to-End-Prozess digital bearbeiten. Gemäß der europäischen eIDAS-Verordnung verlangt die qualifizierte digitale Signatur die Identifikation einer Person durch seine physische Anwesenheit oder ein Verfahren, das dem entspricht, wie etwa eine Videoidentifizierung. Dabei werden in Zukunft sogenannte Identity Provider (IDP) eine tragende Rolle spielen.

Insbesondere etablierte Banken sehen hier ein neues Geschäftsfeld: Sie können ihren bereits persönlich identifizierten Kunden die Vertragsunterzeichnung oder den digitalen Behördengang ganz einfach ermöglichen. Fernsignaturanbieter haben als Vertrauensdienstanbieter die Aufgabe, die drei Parteien Bank, den Endnutzer auf der Signaturapplikation und sich selbst in einem vertrauenswürdigen Netzwerk zusammenzubringen.

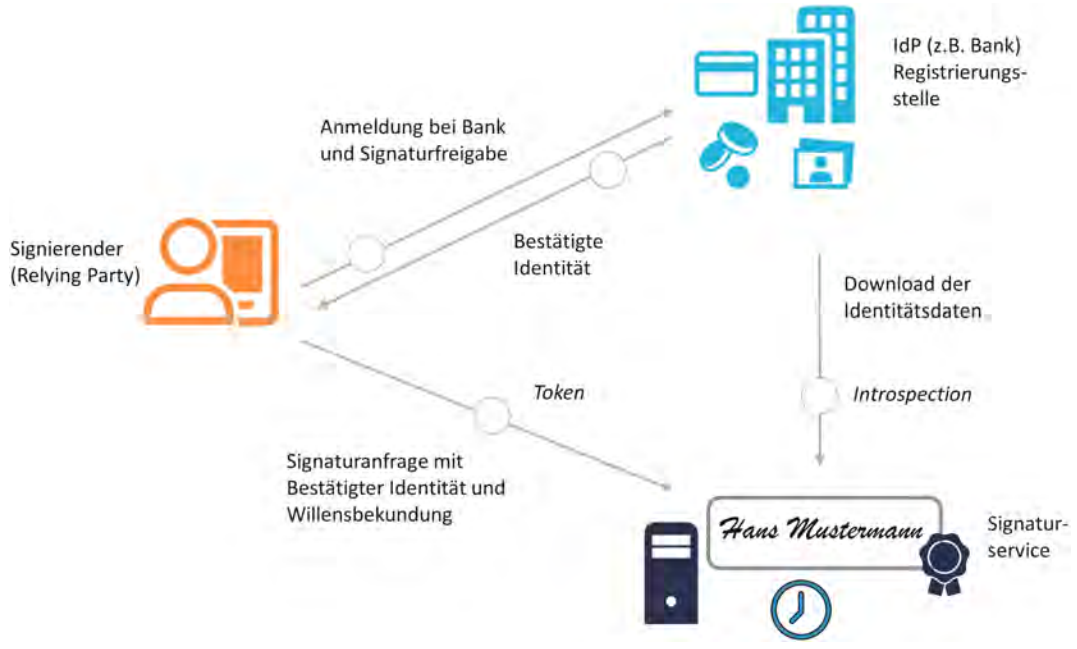
Vorhandene Daten nutzen

Für diese Netzwerke wird ein rasantes Wachstum erwartet: Tausende Applikationen, die eine Signatur benötigen, werden dieses einfache Verfahren nutzen wollen. Sie werden Relying Parties genannt. Außerdem können alle Hausbanken an Vertrauensnetzwerken teilnehmen. Aufgrund der bestehenden Gesetze und Auflagen müssen sie ihre Kunden ja bereits identifiziert haben. Diese Daten können sie als IDP für weitere Anwendungsfälle nutzen, wie beispielsweise die digitale Signatur. Natürlich sind nebst Banken auch weitere IDP denkbar, zum Beispiel Dienste, die eine Identifizierung auf Basis des neuen Personalausweises anbieten.

Und so funktioniert es

Wenn ein Kunde ein Dokument digital signieren will, wird er über die Applikation zum Login seiner Bank weitergeleitet. Dort wird seine bereits geprüfte und hinterlegte Identität bestätigt. Anschließend wendet sich die Signaturapplikation an den Fernsignaturanbieter und bittet ihn um die Ausstellung einer qualifizierten Fernsignatur. Der Fernsignaturanbieter wendet sich wiederum an die Bank und fragt nach einer sicheren Übertragung der Identitätsnachweise. Das können beispielsweise die Ausweisdaten in Kombination mit weiteren regulatorisch erforderlichen Informationen sein.

Die besondere Herausforderung liegt darin, dass alle drei Parteien Daten austauschen, die untrennbar zusammengehören – und doch nicht für alle Augen bestimmt sind. Die sensitiven Identitätsdaten wer-



Identifikationsverfahren per Token und Introspection.

Quelle: Swisscom IT Services Finance S.E.

den sicher zwischen IDP und Fernsignaturanbieter ausgetauscht, ohne dass die Signaturapplikation der Relying Party diese erhält. Gleichzeitig dürfen die IDP und Fernsignaturanbieter natürlich die Dokumenteninhalte nicht sehen.

Open Authorization macht's möglich

Als Fernsignaturanbieter und anerkannter Vertrauensdienst nach eIDAS setzt Swisscom IT Services Finance S.E., Wien dieses Verfahren gemeinsam mit dem Vertrauensnetzwerk YESÆ und den angeschlossenen Banken in Deutschland um. Technisch basiert die Lösung auf dem OAuth-2.0-Protokoll. Der Fernsignaturservice ist dabei der OAuth-2.0-Resource-Server. Der Betreiber eines Vertrauensnetzwerkes stellt den Relying Parties eine Auswahl von IDPs (zum Beispiel Banken) zur Verfügung, die eine Identifizierung auf Niveau „qualifiziert" ermöglichen.

Der IDP generiert nach der erfolgreichen Identifikation auf Basis des Dokumentenhashs Signaturaktivierungsdaten in Form eines OAuth-Access-Tokens. Die Relying Party nutzt das Access-Token nach der Identifikation beim IDP für die Anfrage beim Fernsignaturservice und übermittelt den Hash des zu signierenden Dokuments. Der Fernsignaturservice entnimmt dem Token den bestätigenden IDP und verifiziert das Token.

Der Fernsignaturservice nimmt nun über einen sogenannten „Introspection Call" des OAuth-2.0-Protokolls Kontakt auf zum IDP und holt sich hier alle erforderlichen Nachweise der Identität, sowie den Dokumentenhash, für den der IDP den Signierenden identifiziert hat. Sind alle Daten korrekt und vorhanden, wird ein kurzlebiges Signaturzertifikat erstellt, mit dem der übertragene Dokumentenhash signiert wird. Die Relying Party erzeugt aus dem signierten Dokumentenhash ein signiertes Dokument.

Das Identifikationsverfahren wurde bereits bei der Konformitätsbewertungsstelle eingereicht. Für das Protokollverfahren, das auf dem ETSI-Standard für die Fernsignatur ETSI TS 119 432 basiert, laufen schon Pilotprojekte. Anhand von Testzertifikaten werden so live Audits abgeschlossen, damit das Verfahren komplett bei der Konformitätsbewertungsstelle angemeldet werden kann. Damit werden auch in Mitteleuropa relevante Signaturverfahren mit qualifizierter Signatur basierend auf einer Bankidentität möglich. In Nordeuropa (BankID) und den Niederlanden (iDIN) sind Verfahren für fortgeschrittene Signaturen, die sich auf eine Bankidentität stützen, bereits weit verbreitet.

Fazit

Die Vorteile liegen auf der Hand: Der Kunde muss keine Identitätsdaten neu einpflegen, sondern greift auf Vertrauensstellen zurück, denen er bereits heute seine Daten anvertraut. Die Kundenfreundlichkeit, Verbreitung und Akzeptanz der qualifizierten Signatur wird damit stark erhöht.

Ingolf Rauh
Swisscom

Den Qubits Paroli bieten

Mit erweiterten Verschlüsselungsverfahren können sich Unternehmen schützen

Quantencomputer eröffnen viele und noch nie da gewesene Möglichkeiten für das, was Technologie zu leisten vermag. Ihre enorme Rechenleistung hat allerdings auch erhebliche Auswirkungen auf die Ver- und Entschlüsselung von Daten. Nicht alle Verschlüsselungsverfahren sind jedoch gleichermaßen betroffen.

Seit Jahrzehnten werden Computer immer schneller und kompakter. Mehr und mehr Transistoren werden auf Chips gepresst und die Größe von Schaltkreisen wurde bis in den mikroskopischen Bereich verkleinert. Trotz aller Bemühungen lässt sich dieser Ansatz jedoch nicht ewig weiterverfolgen. Es gibt physikalisch bedingte Beschränkungen, die letztlich irgendwann eine Obergrenze für die Hardware der digitalen Entwicklung markieren. Diese physikalischen Beschränkungen gelten aber nicht für Quantencomputer in derselben Art und Weise. Über ihre tatsächliche Leistungsfähigkeit kursieren derzeit verschiedenste Spekulationen.

Transit in die Quantenwelt

Große Hoffnungen – und große Mengen an finanziellen Mitteln – fließen in die Entwicklung von Quantencomputern. Mit Quantencomputern könnten hochkomplexe Modelle genau und verlässlich in kurzer Zeit berechnet werden, wodurch viele zeitaufwendige und teure Testmethoden und Versuche obsolet würden. Für Branchen wie die Pharmaindustrie etwa würde dies eine wirklich revolutionäre Wende bedeuten, da sie dann Medikamente kosten- und zeitsparend am Computer entwickeln und testen könnte. Des Weiteren können Quantencomputer als ein wirksamer Beschleuniger für künstliche Intelligenz dienen. Auch wenn die Präsenz dieser neuen Technologie am Markt noch weit davon entfernt ist, allgegenwärtig zu sein, sieht die Zukunft für Quantencomputer und ihre Anwendungsgebiete sehr vielversprechend aus.

Momentan steckt diese Technologie aber noch in den Kinderschuhen. Und angesichts der enormen Investitionskosten ist sie bisher nur für sehr wenige zugänglich. In einer Übergangsphase, in der sowohl digitale Computer wie auch Quantencomputer benutzt werden, hieße dies höchstwahrscheinlich, dass diejenigen, die über Quantencomputer verfügen (wenige reiche Organisationen), auch allein von diesem technologischen Vorteil profitieren könnten. Während dieser Übergangszeit müssen Daten also mit herkömmlichen Mitteln gegen die Power der Quantencomputer geschützt werden.

Verschlüsselung auf dem Prüfstand

Die enorme Rechenleistung der Quantencomputer hat das Potenzial, die Verschlüsselung und Entschlüsselung von Daten fundamental zu transformieren. Besonders jenseits der relativen Sicherheit der eigenen Firewall, also dort wo Informationen am gefährdetsten sind, werden Quantencomputer große Veränderungen für die Verschlüsselung und

Foto: refresh(PIX), Fotolia

Der Transit in die Quantentechnologie eröffnet ungeahnte Möglichkeiten. Kryptografische Risiken scheinen jedoch beherrschbar und es ergeben sich Chancen für neue Verschlüsselungsverfahren.

Entschlüsselung von Daten im Transit verursachen. Quantencomputer können mathematische Berechnungen bedeutend schneller als digitale Computer ausführen. Dadurch stellen sie eine ernsthafte Bedrohung für diejenigen Verschlüsselungsmethoden dar, die sich bislang auf die Tatsache verlassen haben, dass es nicht möglich ist, aus dem Produkt von zwei Primfaktoren mit mathematischen Methoden auf diese Primfaktoren zurückzuschließen, wie es für die Verschlüsselung mit Public/Private Keys der Fall ist.

Symmetrische Verschlüsselung ist hier besser gerüstet und wird von der Rechenleistung von Quantencomputern weniger stark beeinträchtigt. Kryptografie-Experten erwarten, dass die Schlüssellänge verdoppelt werden müsste, um Verschlüsselungsmethoden wie AES zu sichern und den Vorteil von Quantencomputern zu eliminieren. Es scheint durchaus möglich zu sein, dies zu implementieren, ohne größere Eingriffe in bestehende Systeme vornehmen zu müssen. Für die Transportverschlüsselung TLS (Transport Layer Security) ist die Sache komplizierter. TLS benutzt Public/Private-Key-Methoden, um eine Verbindung zwischen Client und Server herzustellen. Für die weitere Verbindung verwendet sie typischerweise einen symmetrischen Session Key. Wenn der erste Teil nicht gesichert ist (und er scheint dies sicherlich nicht zu sein), kann der Session Key herausgefunden und der Inhalt der gesamten Verbindung gelesen werden.

Die Herausforderung, die Quantencomputer für die Verschlüsselung darstellen, wurde erkannt und es wird daran geforscht, wie auf diese neue Technologie reagiert werden kann. Das Gebiet der Post-Quanten-Kryptografie beschäftigt sich damit, wie vertrauliche Informationen vor der Rechenleistung der Quantencomputer geschützt werden können, indem gewöhnliche elektronische Systeme passende kryptografische Methoden verwenden. Zudem wird an alternativen Methoden für den Aufbau von TLS-Verbindungen gearbeitet. Diese werden höchstwahrscheinlich bedeutend mehr Ressourcen für die Verschlüsselung und Entschlüsselung benötigen, aber immer noch in der Lage sein, Daten wirksam zu schützen.

Fazit

Es ist immer noch unklar, ob und wann Quantencomputer für den allgemeinen Gebrauch bereitstehen werden. Die kryptografischen Risiken dieser Technologie jedoch scheinen beherrschbar, wenn die angemessenen Maßnahmen getroffen werden. Die intensivierte Forschung zu quantencomputerresistenten Algorithmen wird sicherlich noch weitere Fortschritte machen und gängige wie auch innovative Verschlüsselungsverfahren unter die Lupe nehmen. Doch die Quantentechnologie stellt nicht nur eine Bedrohung dar, sie bietet vielmehr auch vielversprechende Möglichkeiten, zum Beispiel für den sicheren Transfer von Schlüsseln zwischen zwei Kommunikationspartnern. Diese Chancen sollten wir nicht aus den Augen verlieren, wenn es darum geht, neue Technologien auf bestehende Herausforderungen anzuwenden.

Matthias Kess
befine Solutions AG – The Cryptshare Company

Verschlüsselt Johnny jetzt endlich seine Mails?

Neue Impulse fördern Akzeptanz und Umsetzung der E-Mail-Verschlüsselung

Trotz aller Sicherheitsvorfälle verschlüsseln nach wie vor nur wenige Nutzer ihre E-Mails. Dank neuer gesetzlicher Vorschriften soll sich dies nun ändern. Damit es funktioniert, muss der Anwender der Verschlüsselungslösung mehr als bisher im Vordergrund stehen, insbesondere bei der Benutzerfreundlichkeit.

Der Forschungsaufsatz „Why Johnny Can't Encrypt" ist zwar schon 20 Jahre alt, doch viele Experten halten ihn immer noch für aktuell. In dieser Arbeit von Alma Whitten und J. D. Tygar geht es um die Frage, wie ein Durchschnittsanwender („Johnny") im praxisnahen Test das Verschlüsseln von E-Mails bewältigt. Das Ergebnis ist ernüchternd. Bezeichnenderweise hat „Why Johnny Can't Encrypt" 2015 den USENIX Test of Time Award erhalten. Dieser wird für Forschungsarbeiten vergeben, die auch nach mindestens einem Jahrzehnt noch aktuell sind.

Mehr Bewusstsein und neue Gesetze

Dabei wäre mehr E-Mail-Verschlüsselung (momentan sind nur etwa 0,1 Prozent aller Mails auf diese Weise gesichert) wichtiger denn je. Man denke nur an die zahlreichen E-Mail-Sicherheitsvorfälle, die regelmäßig durch die Presse gehen. Und spätestens seit den Enthüllungen von Edward Snowden hat sich herumgesprochen, dass die NSA und andere Geheimdienste im großen Stil mitlesen.

Weniger beachtet wird bisher, dass die Snowden-Affäre die Notwendigkeit von E-Mail-Verschlüsselung auch auf eine andere Weise deutlich gemacht hat. Erstaunlich ist nämlich, dass Snowden an 1,7 Millionen NSA-Dateien herankam, obwohl die NSA zweifellos eines der am besten geschützten Computer-Netze der Welt betreibt. Die Erklärung dafür ist äußerst banal: Snowden hatte als Administrator legalen Zugriff auf die von ihm geleakten Dokumente und musste daher keine größeren Sicherheitsvorkehrungen aushebeln. Die Affäre bestätigt daher die – keineswegs neue – Erkenntnis, dass Insider-Angriffe eine große Gefahr sind.

Um das Verschlüsseln von E-Mails endlich populärer zu machen, hat sich inzwischen der Gesetzgeber eingeschaltet. Am bekanntesten ist in diesem Zusammenhang die Datenschutz-Grundverordnung (DSGVO) der EU, die in einigen Bereichen nur durch das Verschlüsseln von E-Mails zu erfüllen ist. Eine Verschlüsselungspflicht gibt es außerdem für Berufsgeheimnisträger wie Rechtsanwälte, Patentanwälte, Notare, Wirtschaftsprüfer und Steuerberater – gemäß dem 2017 neu gefassten § 203 des Strafgesetzbuchs. Die Details werden derzeit erarbeitet, wobei vor allem die DATEV (der IT-Dienstleister der Steuerberater, Wirtschaftsprüfer und Rechtsanwälte) eine wichtige Rolle spielt. Von Bedeutung sind außerdem das IT-Sicherheitsgesetz mit der zugehörigen Kritisverordnung des Bundesamts für Sicherheit in der Informationstechnik (BSI), das E-Government-Gesetz und das für das Gesundheitswesen bedeutsame E-Health-Gesetz. Sie alle fordern – direkt oder indirekt – das Verschlüsseln von E-Mails.

Ein gestiegenes Bewusstsein und gesetzliche Vorschriften sind die eine Seite, wenn E-Mail-Verschlüsselung populärer werden soll. Die andere ist der Anwender. Wenn Johnny seine E-Mails endlich verschlüsseln soll, dann muss er dies erst einmal können und wollen. „Anwender-zentrierte IT-Sicherheit" heißt das Stichwort. Zu den weltweit führenden Expertinnen in diesem Segment gehört die deutsche Professorin Angela Sasse von der Ruhruniversität Bochum.

Zusammen mit vier Kollegen hat Sasse beispielsweise den Umgang mit E-Mail-Clients untersucht. Viele Anwender hatten schon bei der Installation und Konfiguration ihre Probleme. Bis zur Verschlüsselung der ersten Mail vergingen im Schnitt über 40 Minuten. Im Rahmen eines neuen Forschungsprojekts namens Casa (Cyber-Sicherheit im Zeitalter großskaliger Angreifer) untersucht Sasse derzeit Aspekte wie Nutzer-Akzeptanz und Benutzerfreundlichkeit in der IT-Sicherheit unter anderem gemeinsam mit Psychologen, wobei auch die E-Mail-Verschlüsselung eine wichtige Rolle spielt.

Johnny muss in den Mittelpunkt

Damit Johnny endlich seine Mails verschlüsselt, hält Sasse es zunächst für notwendig, die Anwender zu sensibilisieren. „So mancher E-Mail-Nutzer denkt immer noch, Verschlüsselung bringe nichts, denn man kann das sowieso knacken", berichtet sie. „Diese Einschätzung ist jedoch komplett falsch, denn heutige Krypto-Algorithmen gelten als äußerst sicher."

Bekannt ist allerdings, dass auch heute noch so manche Lösung zur E-Mail-Verschlüsselung diverse Kinderkrankheiten aufweist. Sasses Arbeit berichtet beispielsweise von Bugs in den untersuchten Clients, die zur Nichtverfügbarkeit von Funktionen, Abstürzen und unerwünschten Nebenwirkungen führen. Darüber hinaus sieht Sasse noch Verbesserungsmöglichkeiten in der Benutzerfreundlichkeit. Ein Mail-Client sollte beispielsweise die Kommunikation mit der Zertifizierungsstelle übernehmen und dabei für eine reibungslose Registrierung und Zertifikatserneuerung sorgen, die ohne größere Interaktion des Anwenders abläuft.

Geheimschutz als Vorbild

Eine Vorreiterrolle in Sachen E-Mail-Verschlüsselung könnten demnächst Behörden und Unternehmen übernehmen, die Geheimschutzanforderungen erfüllen müssen. Diese dürfen Daten bis zur Geheimhaltungsstufe „Verschlusssache – Nur für den Dienstgebrauch" (VS-NfD)

verschlüsselt per Mail verschicken, sofern die dazu genutzte Lösung entsprechend zugelassen ist. Die von Outlook oder Notes bereitgestellten Verschlüsselungsfunktionen verfügen nicht über eine solche Zulassung (es ist auch kaum zu erwarten, dass der Geheimschutz in Deutschland in die Hände von US-Herstellern gelegt wird), doch es gibt inzwischen VS-NfD-zugelassene Add-ins.

Viele Organisationen nutzen für den VS-NfD-Datenaustausch jedoch keine Mail-Verschlüsselung, sondern die Software Chiasmus. Chiasmus ist kein Tool für das Verschlüsseln von E-Mails, sondern dient der Datei-Verschlüsselung und ist vor allem für das stationäre Sichern von Daten gedacht. Ein Anwender kann damit jedoch Daten sicher übertragen, indem er eine verschlüsselte Datei über ein geteiltes Verzeichnis zugänglich macht oder als Mail-Anhang verschickt. Allerdings muss der Schlüssel hierbei manuell übergeben werden, da Chiasmus keine asymmetrische Kryptografie unterstützt. Da es sich um symmetrische Schlüssel handelt ist das Verfahren stark reglementiert und weder flexibel noch benutzerfreundlich.

Neuere Entwicklungen steigern die Benutzerfreundlichkeit, indem sie E-Mail-Verschlüsselung und Datei-Verschlüsselung als eine Einheit betrachten. Der Anwender kann hierbei beispielweise eine verschlüsselte Datei als Mail verschicken, wobei der Client des Empfängers diese als verschlüsselte Mail erkennt. Umgekehrt kann der Anwender eine verschlüsselte Mail abspeichern und später mit der Datei-Verschlüsselungslösung entschlüsseln. Der zugrunde liegende Standard der dies ermöglicht ist S/MIME. Das Schlüssel-Management erfolgt über digitale Zertifikate. Eine Lösung, die so arbeitet und VS-NfD-zugelassen ist, ist z. B. GreenShield von cryptovision.

Oft lässt sich E-Mail-Verschlüsselung im Geheimschutzbereich benutzerfreundlicher umsetzen als in anderen Umgebungen. So ist in VS-NfD-Kommunikation das hierarchisch ausgelegte S/MIME-Format deutlich weiter verbreitet als das oft nur provisorisch genutzte PGP – Johnny muss sich also nicht mit zwei inkompatiblen Formaten herumschlagen. Die digitalen Zertifikate kommen von einer VS-NfD-konformen Zertifizierungsstelle, die der Betreiber festlegt und die im Normallfall von allen Beteiligten anerkannt wird – die Flut an Zertifizierungsstellen, mit denen sich ein Anwender herumschlagen muss, wird dadurch eingedämmt.

Fazit

Es könnte also durchaus sein, dass sich E-Mail-Verschlüsselung zumindest im Geheimschutzsegment durchsetzen wird. Es bleibt zu hoffen, dass diese Entwicklung auch auf andere Bereiche überspringt. Wer weiß, vielleicht erscheint demnächst eine Forschungsarbeit, in der die erfolgreiche Umsetzung von E-Mail-Verschlüsselung bei einer Organisation mit Geheimschutzanforderung beschrieben wird („Why Johnny Finally Can Encrypt“)? Und vielleicht wird diese Arbeit dann zehn Jahre später den USENIX Test of Time Award gewinnen.

Klaus Schmeh
cv cryptovision GmbH

Nach Lage der Dinge entscheiden

Die Sicherheit im IoT hängt maßgeblich vom Anwendungsfall ab

Das Internet der Dinge hat das Potenzial, durch kontinuierliche Erhebung großer Messdatenmengen und intelligente Auswertung dieser Daten, Produktionsprozesse zu optimieren. Zugleich aber machen sich aufgrund von Berichten über mangelnde Sicherheit bisheriger IoT-Lösungen Zweifel in den Unternehmen breit.

Für eine grundsätzliche Betrachtung des Themas Sicherheit im IoT wäre es zunächst wichtig zu definieren, was das Internet of Things eigentlich ist. Eine Recherche zeigt schnell, dass eine einheitliche Definition nicht existiert, sondern IoT vielmehr als eine Sammlung von Konzepten und Ideen in bestimmten Anwendungsfällen, wie etwa Industrie 4.0, zu verstehen ist. Dadurch wird die Frage nach den Möglichkeiten der Absicherung von IoT-Lösungen nicht allgemein, sondern immer nur bezogen auf bestimmte Anwendungsfälle zu beantworten sein.

Um sich hier einen Überblick zu verschaffen, betrachten wir im Folgenden vier Quadranten, die sich in Bezug auf die Platzierung von IoT-Geräten (eigenes vs. fremdes Netzwerk) und die Geräte selbst (eigene vs. fremde Geräte) unterscheiden. Ziel ist eine vereinfachte Einordnung nach Anwendungsfällen, um dann innerhalb der Quadranten Risiken beim Einsatz von IoT-Geräten und Möglichkeiten der Absicherung untersuchen zu können. Der Begriff „IoT-Gerät“ soll dabei bewusst nicht auf die abstrakte Idee eines Geräts begrenzt sein, das über Sensoren Daten erfasst und über ein Netzwerk sendet, sondern schließt auch Vorrichtungen mit ein, die nur im weiteren Sinne als IoT-Geräte gelten: Netzwerkkameras, Heizungs- und Klimatechnik, Frankiermaschinen, POS, Telefonie- und Videokonferenzsysteme, Smart-TVs, Kaffeemaschinen und Anzeigetafeln, aber natürlich auch alle Arten von industriellen Produktionssystemen.

Gruppierung in Quadranten

Im ersten Quadranten befinden sich alle Ressourcen in unserem eigenen Netzwerk. Es ist dabei nicht relevant, ob es sich um ein einzelnes lokales oder um einen über VPN oder MPLS hergestellten Verbund von Netzwerken handelt. Die eingesetzten IoT-Geräte werden aus unserem Netzwerk heraus gesteuert und die Daten nicht nach außen gesendet. Damit wäre dies streng genommen kein IoT-Anwendungsfall, weil hier schließlich das „I“ für „Internet“ fehlt. Wir betrachten diesen Quadranten dennoch, weil er die Basis für weiterführende Anwendungsfälle darstellt und die Umsetzung in der Praxis bereits zu Sicherheitsproblemen geführt hat.

Die IoT-Geräte im zweiten Quadranten werden von externen Anbietern in unserem Netzwerk betrieben oder sind auf externe Dienste angewiesen (Stichwort: Cloud). Eingesetzte Geräte können die Steuerung von Heizung- und Klimatechnik ebenso wie eine Alarmanlage oder eine Frankiermaschine, aber natürlich auch eine industrielle Anlage sein. Für die Auswertung anfallender Informationen fließen Daten zu externen Anbietern, von dort werden wiederum Steuerkommandos von den IoT-Geräten in unserem Netzwerk empfangen und verarbeitet. In diesen Quadranten fallen auch die im Heimbereich eingesetzten Sicherheits- und Automatisierungslösungen, die den Anwendern über Cloud-Dienste der jeweiligen Anbieter Zugriffe mittels Smartphone-Apps erlauben.

Im dritten Quadranten steuern wir als Anbieter IoT-Geräte, die in fremden Netzwerken stehen. Wir wechseln also von der Rolle eines Konsumenten (II. Quadrant) in die Rolle des Anbieters von Diensten.

Eine Besonderheit stellen Lösungen im vierten Quadranten dar, weil hier weder das Netzwerk noch die eingesetzten Geräte unter unserer Kontrolle stehen. Trotzdem erfolgen Interaktionen, bei denen Daten von Sensoren erfasst und versendet werden. Typische Anwendungsfälle dafür sind vernetzte Fahrzeuge, die Daten über Mobilfunk an den Hersteller senden oder die in Zukunft, etwa über die kommenden 5G-Netze, Daten mit anderen Fahrzeugen in der Nähe austauschen. Aus technischer Sicht ist es dabei nicht relevant, ob die erfassten Daten Vorgänge im Motor oder Daten über den Fahrer enthalten.

Geeignete Maßnahmen

Da sich Anwendungsfälle aus dem I. Quadranten nur im eigenen Netzwerk abspielen, können die Maßnahmen, die zur Absicherung von Büro- und Rechenzentrumsnetzwerken bekannt und erprobt sind, eingesetzt werden: Zugangskontrolle für alle Netzwerkendpunkte (NAC); Segmentierung des Netzwerks (physikalisch oder über VLAN); Sicherung der Netzwerkübergänge durch Firewalls und IDS-/IPS-Systeme (Intrusion Detection/Intrusion Prevention). Zusätzliche Maßnahmen wie Protokolle aller Verbindungen und die Anreicherung dieser Protokolle mit GeoIP-Informationen helfen, Auffälligkeiten im Netzwerk zu entdecken und ermöglichen eine zielgerichtete Reaktion.

Durch die Umsetzung dieser Maßnahmen können IoT-Geräte sicher betrieben, unberechtigte Zugriffe und der Abfluss von Daten auf Netzwerkebene verhindert werden. Leider muss man aber feststellen, dass sie in der Praxis nicht überall konsequent umgesetzt werden. Dies zeigt etwa der erfolgreiche Angriff mit der Ransomware WannaCry auf die Deutsche Bahn oder das Beispiel KraussMaffei, wo nach unbestätigten Berichten vom Büronetzwerk ausgehend, die industrielle Fertigung betroffen war. Die Umstände legen in beiden Fällen die Vermutung nahe, dass Netzwerkübergänge nicht ausreichend geschützt waren oder eine hinreichende Segmentierung des Netzwerks sogar ganz fehlte.

Die für den ersten Quadranten beschriebenen Maßnahmen können und wollen wir für die Anwendungsfälle aus dem zweiten nicht anwenden, denn die Funktionalität der eingesetzten IoT-Geräte beruht maßgeblich auf ihrer Fähigkeit, Daten mit externen Diensten austauschen zu können. Statt Datenverkehr zu externen Diensten pauschal zu verhindern, bleibt nur die Möglichkeit, bekannte (sprich: von den Anbietern dokumentierte) Verbindungen zuzulassen oder die Geräte so weit wie möglich zu isolieren.

Während große Unternehmen aufgrund ihres Einkaufsvolumens bei den jeweiligen Anbietern gute Chancen haben sollten, detaillierte Dokumentation über Verbindungen zu externen Diensten zu verlangen und zu bekommen, erhalten kleine bis mittlere Betriebe solche Information leider oft nicht. Meistens liegt z. B. einem Kreditkartenterminal (POS) nur der Hinweis bei, dass eine Verbindung ins Internet benötigt wird. Selten ist dann über eine weiterführende Dokumentation oder die technische Hotline des Anbieters mehr zu erfahren. Wenn die Situation bei mehreren Anbietern ähnlich ist und ein Anbieterwechsel somit keinen Unterschied machen würde, bleibt nur, das betroffene Gerät so weit wie möglich vom Rest des Netzwerks zu isolieren und den Zugriff auf das Internet komplett freizugeben. Weitere Maßnahmen sind die Protokollierung aller ein- und ausgehenden Verbindungen und der Versuch, Anomalien in diesen Daten zu erkennen.

Durch die zu erwartende größere Verbreitung von netzwerkfähigen IoT-Geräten besteht aber die Hoffnung, dass Anbieter mehr Know-how bei der Integration ihrer Lösungen sammeln, ihre eigenen Prozesse und Dokumentationen verbessern und lernen, transparenter zu werden. Aktuell verstehen viele Hersteller die Funktion ihrer Geräte als einziges großes Betriebsgeheimnis, was in einer vernetzten und offenen Welt nur begrenzt sinnvoll erscheint.

Hersteller in der Pflicht

Die Anwendungsfälle im dritten Quadranten führen zu gänzlich neuen Aufgaben: Dienstanbieter müssen IoT-Geräten aus Kundennetzwerken heraus sicheren Zugriff auf ihre (Cloud-)Dienste ermöglichen. Auf Ebene der Netzwerkstruktur erfolgt die Absicherung über Maßnahmen wie Router, Firewalls und IDS-/IPS-Systeme. Analog zu NAC (Network Access Control) in einem lokalen Netzwerk sollte ein Anbieter außerdem sicherstellen, dass nur autorisierte Geräte Daten senden können. Hierfür gibt es keine herstellerübergreifenden Standards, der Einsatz von Zertifikaten wäre hier ebenso denkbar wie einmalig auf den Geräten generierte und beim zentralen Dienst registrierte Token o. ä.

Die meisten Hersteller dokumentieren die verwendeten Verfahren nicht. Hier ist den Anwendern solcher Dienste dringend zu empfehlen, die Anbieter zur Offenlegung der Mechanismen zu verpflichten. Dies geschieht im Regelfall auf Basis einer Geheimhaltungsvereinbarung zwischen Anbieter und Kunden und ggfs. beteiligten Dienstleistern. Diese Option steht allerdings realistisch ebenfalls nur Großunternehmen zur Verfügung, kleinere und mittlere Unternehmen können genauso wie Heimanwender die Dienste nur so nutzen, wie sie von den Anbietern bereitgestellt werden, und erhalten nur die Informationen, die der Anbieter freiwillig zur Verfügung stellt.

Die Anwendungsfälle aus dem vierten Quadranten schließlich lassen keine Kontrolle über die Geräte oder das verwendete Netzwerk zu. Es wäre außerdem möglich, dass IoT-Geräte oder Netzwerke nicht als solche erkennbar sind, wie es z. B. bei der Bordelektronik im Automobilbereich der Fall ist. Schwachstellen in den IoT-Geräten oder in der Kommunikation, die die Funktion nicht beinträchtigen, könnten von den Anwendern nicht festgestellt werden. Bei der Verwendung personenbezogener Daten, wie z. B. Informationen über das Verhalten des Fahrers eines Kfz, gilt in der EU die DSGVO (Datenschutz-Grundverordnung). Sollten Daten unbeabsichtigt abfließen, könnte das, wenn es bekannt wird, geahndet werden.

Ob der Aufwand auf Kundenseite für regelmäßige Schwachstellenscans oder gezielte Penetrationstests der eingesetzten IoT-Geräte sinnvoll ist, muss im konkreten Einzelfall entschieden werden. Es sollte good practice sein, alle Geräte vor einem Rollout im eigenen Netzwerk solchen Tests zu unterziehen, schließlich wäre erst dann eine Bewertung des Risikos für den Einsatz möglich. In der Praxis wird dies aber nicht selten notorisch zu knapp bemessenen Budgets und einer gewissen Sorglosigkeit untergeordnet.

Unsichere Heimnetzwerke

Für alle hier betrachteten Anwendungsfälle gilt: Die aufgeführten Maßnahmen werden nur in Unternehmensnetzwerken zur Anwendung kommen. Selbst ambitionierte Anwender können mit der von den Internet-Providern gelieferten Hardware ein Heimnetzwerk nicht so absichern, wie es nötig wäre. Die meisten Router in diesem Segment erlauben nicht einmal die Kontrolle über ausgehende Datenströme, weitergehende Funktionen fehlen völlig.

Erst eigene Firewalls sowie VLAN-fähige Switche und WLAN-Access-Points zur Segmentierung des eigenen Netzwerks würden diese Funktionen bieten. Die Anschaffungskosten dafür sprengen aber normalerweise das Budget der Anwender, deren Hauptinteresse darin liegt, dass das Netzwerk läuft und alle Komponenten und Geräte miteinander funktionieren. Schon eine Segmentierung des eigenen Netzwerks würde diesem Wunsch nach Einfachheit im Weg stehen. Sollte ein IoT-Gerät in einem Heimnetzwerk kompromittiert und Teil eines Botnetzes werden, ist die Chance sehr hoch, dass dies von den Anwendern nicht einmal wahrgenommen wird. Somit bleibt die Sicherheit von IoT-Geräten in Heimnetzwerken bislang eine absolute Illusion. Die Anwender müssen sich mehr oder weniger blind darauf verlassen, dass die eingesetzten IoT-Geräte sicher vor Angreifern sind.

Fazit

Wie gezeigt sind technische Maßnahmen zur Absicherung je nach Anwendungsfall ganz oder in Teilen möglich. Unternehmen tun gut daran, die Verarbeitung der Daten aus vernetzten Geräten und Sensoren analog zu einem Vertrag über die Auftragsdatenverarbeitung bei personenbezogenen Daten mit den jeweiligen Anbietern zu vereinbaren. Kleinere und mittlere Unternehmen werden von dieser Möglichkeit nur eingeschränkt Gebrauch machen können, Endanwender können dies de facto gar nicht. Aktuell könnte es darauf hinauslaufen, dass große Unternehmen über Verträge abgesichert sind und auch aus technischer Sicht sicher mit ihren Anbietern kommunizieren, während der größte Teil der an das Internet angeschlossenen Netzwerke von Heimanwendern sowie kleineren und mittleren Unternehmen betrieben werden, die nur eingeschränkte Möglichkeiten haben, gegenüber den Anbieter ihre Interessen und Erwartungen an Datenschutz und Datensicherheit durchzusetzen.

Mögliche gesetzliche Regelungen mit konkreten Anforderungen an Anbieter wie garantierte Patches und Sicherheitsupdates und die sichere Speicherung aller Daten in der Cloud sind umstritten, die Durchsetzbarkeit fraglich. Sie könnten aber dafür sorgen, dass das Sicherheitsniveau in Summe steigt und nicht wie bisher auf einem sehr niedrigen Wert stagniert.

Stefan Beyer
THREATINT GmbH & Co. KG

Geräte-Service per Tablet

Sicher und benutzerfreundlich: SSH-Authentifizierung und NFC-Smartcards

Eine ausgereifte IIoT-Sicherheitsarchitektur basiert auf erprobten und bewährten Sicherheitsprotokollen, integriert diese aber in ein modernes Anwendungsszenario mit Smartcards und Tablets. Sie ist sicher und robust und bietet dennoch eine hohe Benutzerfreundlichkeit für Servicetechniker.

Die Vision einer Industrie 4.0 kann nur durch eine übergreifende Vernetzung von Industrieanlagen umgesetzt werden. Die Einführung eines solchen „Industrial Internet of Things“ (IIoT) geht mit erhöhten Sicherheitsanforderungen an die initiale Inbetriebnahme, Administration und Konfiguration dieser Geräte einher. Da diese Tätigkeiten normalerweise von Servicetechnikern der Maschinenbauunternehmen durchgeführt werden, sollte dieser Prozess möglichst komfortabel und einfach sein.

Kritische Infrastrukturen

Mit der zunehmenden Digitalisierung von industriellen Anlagen innerhalb kritischer Infrastrukturen sind eine Reihe von Bedrohungen verbunden. So arbeiten diese Anwendungen nicht nur mit hochsensiblen, geschäftskritischen Daten der Hersteller, physische Aktoren und Effektoren können im schlimmsten Fall auch die Anlage selbst zerstören oder Menschenleben bedrohen. Einschlägige Normen wie die IEC 62443 sehen hier eine Reihe von Gegenmaßnahmen vor, um unbefugten Zugriff zu verhindern, darunter physisch getrennte Schlüsselspeicher und die Nutzung von Public-Key-Kryptografie. Im Folgenden wird eine Auswahl der Anforderungen an die Login-Mechanismen dargestellt, die für Level 2 und höher auf einer Skala von 0 (keine Sicherheit) bis 4 (gesichert gegen staatliche Akteure) notwendig sind.

Menschliche Nutzer müssen identifiziert und authentifiziert sein. So muss auf jedem Interface eine vorherige Authentifizierung stattfinden. Für Security Level 2 und höher muss jede Person individuell, eindeutig authentifiziert werden. Für Maschinenkommunikation gilt entsprechend, dass jede Maschine und jeder Softwareprozess eindeutige Login-Credentials nutzt. Identifikatoren müssen in ein Managementsystem integrierbar sein. Sie müssen zurückziehbar und erneuerbar sein. Für Level 3 gilt ein zusätzlicher Hardwareschutz wie TPMs oder SEs. Für Public-Key-Kryptografie gilt hier selbstverständlich die Nutzung von generell als sicher anerkannten kryptografischen Verfahren und Primitiven. So gilt etwa RSA mit Schlüssellängen unter 2048 Bit sowie ECC mit Schlüssellängen unter 256 Bit als nicht mehr zeitgemäß. Revozierungsmechanismen müssen vorhanden und verwendbar sein.

Industrial Internet of Things

Industrielle IoT-Geräte werden in unterschiedliche Kategorien aufgeteilt, je nachdem, ob sie an der Maschine selbst platziert sind, oder in einer speziell gesicherten Zone in einem Rechenzentrum. Generell gilt, je mehr potenziell nicht vertrauenswürdige Personen ein Gerät im physischen Zugriff haben und je höher der Schaden bei eingetretenem Sicherheitsvorfall ist, desto höher ist der Schutzbedarf. Häufig finden sich in diesem Umfeld eingebettete Linux-Varianten, die auf Industriecomputern auf Basis von x86- oder ARM-Prozessoren laufen. Als solche stehen im Allgemeinen die typischen Linux-Administrationswerkzeuge wie SSH zur Verfügung. Oft wird ein VPN-Tunnel zu einem gesicherten Backend aufgebaut, sodass bei ordentlicher Konfiguration keine Netzwerk-Ports aus dem öffentlichen IP-Netz offen sind.

Dies birgt jedoch Herausforderungen, wenn ein Gerät initial deployed werden soll. Da solche Geräte häufig kein vollwertiges User-Interface besitzen, können initiale Netzwerkparameter oft nur umständlich vordeployed werden. Hier bieten moderne Mobilgeräte die Möglichkeit, z. B. mittels NFC, Bluetooth oder USB eine Verbindung zu dem Gerät aufzubauen und – über entsprechende Protokolle, Certificates und Schlüssel geschützt – ein temporäres lokales UI bereitzustellen. So können etwa Android Open Accessory und WebUSB genutzt werden, um ein Smartphone oder Tablet mit einem Industrie-Gateway zu verbinden. Das Industrie-Gerät wird als Accessory erkannt und gibt direkt einen Hinweis, welche App notwendig zur Konfiguration ist. Über einen Bulk-Transfer-Endpunkt können beliebige Daten ausgetauscht werden. Wir haben uns hier dazu entschlossen, diese Daten an den lokalen SSH-Unix-Dämon weiterzuleiten, um auf bewährte Sicherheitsmechanismen und Konzepte aufsetzen zu können.

OpenSSH User Certificates

Die Nutzerauthentifizierung erfolgt mit Public-Key-Kryptografie. Hierbei wird jedem Nutzer ein unabhängig generiertes Public-/Private-Key-Paar zugewiesen. Um Security Level 3 des IEC 62443 zu erreichen, werden diese auf Smartcards generiert und gespeichert. Diese bieten ein wesentlich höheres Sicherheitsniveau als Passwörter, da Nutzer oft schwache Passwörter wählen und komplexe Passwörter nur schwer auf Tablets eingegeben werden können.

Zur Autorisierung der Nutzer und Verwaltung der Zugangskontrolle werden OpenSSH User Certificates genutzt. Ähnlich wie X.509 Client Certificates für eine anwenderseitige TLS-Authentifizierung genutzt werden können, ist dies auch bei SSH möglich. Jedoch sind OpenSSH User Certificates einfacher umgesetzt. Es werden keine komplexen Kodierungsregeln und mehrstufigen Zertifizierungsebenen genutzt. Das vereinfacht die Implementierung und vermindert die Angriffsoberfläche. Diese einstufige CA-Infrastruktur erlaubt also zusammen mit einer Public-Key-Infrastruktur die Zugriffs-Autorisierung von Nutzern.

Viele Server- und Client-Implementierungen von SSH unterstützen User Certificates bereits. In Client-Implementierungen können sie außerdem leicht nachgerüstet werden, da die eigentliche Challenge-Response-Authentifizierung von SSH nicht geändert werden muss. Eine Anpassung des publickey-Formats reicht aus. Als konkreten Algorith-

mus empfehlen wir „ecdsa-sha2-nistp384-cert-v01@openssh.com“ für die NIST-Kurve P-384.

NFC-Smartcards

Bei den eingesetzten Smartcards wird auf bewährte JavaCard-Technologie gesetzt. Typischerweise werden Smartcards an Desktop-Systemen mit externen Smartcard-Readern genutzt, an Laptops mit dem integrierten Reader. Oft sind dies kontaktbehaftete Smartcards. Für eine Nutzung über die NFC-Schnittstelle von Tablets bieten sich kontaktlose oder hybride Smartcards an. Die JavaCard-Plattform stellt eine API bereit, um eigene Smartcard-Standards zu implementieren. Als eigentlicher Standard kann also die OpenPGP Card Specification, NIST Personal Identity Verification (PIV) oder auch ISO 7816-4 implementiert werden. Wichtig ist, dass Schlüssel immer auf den Smartcards selbst generiert werden und eine Extraktion von Schlüsselmaterial nicht möglich ist. Das zugehörige SSH User Certificate wird ebenfalls auf der Smartcard gespeichert und ist somit geräteunabhängig verfügbar.

Basierend auf den Sicherheitsanforderungen kann die Authentifizierung zwischen Smartcard und Tablet durch eine PIN gesichert werden. Durch den Hardwareschutz der Smartcard muss diese nur aus vier Zahlen bestehen. Smartcards werden mit den Namen der Techniker personalisiert und bedruckt, in einem sicheren Zustand ausgeliefert und eine PUK sicher an den Hersteller übertragen. So kann der Techniker vor Ort eine eigene PIN wählen und setzen.

Public-Key-Infrastruktur

Die Nutzung von OpenSSH User Certificates erlaubt wie bereits beschrieben den Aufbau einer einstufigen CA-Infrastruktur. Um die Sicherheit der ausgestellten Certificates zu gewährleisten, untersteht diese jedoch einem besonderen Schutzbedarf. So sollte der private Schlüssel der CA in einem HSM gesichert und der Ausstellungsprozess durch adäquate Mechanismen geschützt sein. Typische CA-Software nutzt hier eine vorgeschaltete Registration Authority. Die Kartenpersonalisierung wird in einer speziell gesicherten Umgebung nur von vertrauenswürdigem, speziell unterwiesenem Personal durchgeführt.

Kryptografische Algorithmen

Die Wahl der asymmetrischen Kryptografie ist in dieser Architektur mehreren Einschränkungen unterlegen. Die meisten Smartcards – insbesondere die kontaktlosen und hybriden – unterstützen RSA nur bis 2048 bit. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt diese Schlüssellänge nur noch bis 2022. Danach sollte RSA mit mehr als 3000 bit genutzt werden. Das National Institute of Standards and Technology (NIST) empfiehlt für den aktuellen Zeitraum 2016–2030 auch 3072 bit. Zudem benötigt die Generierung eines 2048-bit-RSA-Schlüssels auf der Smartcard im Durchschnitt drei Sekunden bei einer Stromversorgung über NFC.

Elliptische Kurven sind somit eine sinnvolle Alternative. Selbst kosteneffektive Smartcards unterstützen oft Schlüsselgenerierung und Signaturerstellung mit ECDSA. Da hier nur eine Challenge signiert werden muss und keine Entschlüsselung stattfindet, benötigt es kein ECDH, was von vielen Smartcards nicht unterstützt wird. Eine aktuell von BSI und NIST empfohlene Schlüssellänge ist 256 bit. Für höhere Sicherheitsniveaus, wie z. B. in der Commercial National Security Algorithm (CNSA) Suite, wird 384 bit empfohlen.

Nicht gewählt wurden die vom BSI empfohlenen Brainpool-Kurven oder modernere Kurven und Signaturalgorithmen wie Ed25519. Brainpool-Kurven sind aktuell nicht für OpenSSH User Certificates spezifiziert. Ed25519 wird aktuell von den meisten Karten noch nicht unterstützt. Dies ist aber eine sinnvolle Wahl, sobald JavaCard 3.1 eine höhere Verbreitung gefunden hat und kosteneffektive Smartcards zur Verfügung stehen. Zusammenfassend fällt die Wahl somit auf die Kurve NIST P-384 unter Nutzung von ECDSA. Als Hash-Algorithmus wird SHA-256 verwendet.

Smartcards und Tablets

Ist das Tablet mit dem IIoT-Gerät verbunden, wird der Nutzer über eine passende Konfigurations-App informiert. Nach deren Installation kann der Nutzer sich gegenüber dem Gerät authentifizieren, indem er die PIN eingibt und die Smartcard für NFC-Kommunikation gegen die Rückseite des Gerätes hält. Die Smartcard ermöglicht somit ein portables System, d. h. es müssen keine Konfigurationen oder Schlüssel auf ein neues Tablet kopiert werden.

Die Smartcard-Kommunikation findet mit einem eigenen SDK statt. Es implementiert und abstrahiert die Smartcard-Protokolle und detektiert Smartcards automatisch über NFC. Ein User Interface bietet PIN-Abfrage und Hilfestellung zur Positionierung der Smartcard. Im Hintergrund wird das User Certificate von der Smartcard abgerufen und beim SSH-Challenge-Response-Verfahren als „pubkey“ genutzt. Die SSH-Server-Challenge wird über USB empfangen und per NFC an die Smartcard weitergegeben. Auf der Smartcard findet die ECDSA-Signaturerstellung statt. Die signierte Challenge bietet somit den Beweis, dass sich zu dem gesendeten User Certificate der Private Key im Besitz des Nutzers befindet.

Nutzlose Angriffe

Die Sicherheit gegenüber Angreifern im Netzwerk, die sich nicht physisch Zutritt verschafft haben, ist sehr hoch. Durch die Nutzung einer Public-Key-Infrastruktur zusammen mit SSH User Certificates gibt es praktisch keine bekannte Möglichkeit, Gerätezugriff durch Brute-Force-Angriffe zu erlangen. Durch die Nutzung von externen Smartcards wird außerdem ausgeschlossen, dass Private Keys durch Malware auf dem Tablet gestohlen werden können.

Ein Angreifer, der sich in physikalischer Nähe befindet, könnte versuchen die NFC-Kommunikation abzuhören. Das einzige sinnvolle Datum, das abgegriffen werden könnte, wäre die signierte Challenge. Zum einen ist das Abhören von NFC durch die Beschaffenheit der NFC-Antenne nur bis auf wenige Meter möglich. Zum anderen passt diese signierte Challenge nur zu der aktuellen Verbindung zwischen Gerät und Tablet. Einen erweiterten Schutz bietet eine NFC-Verschlüsselung, die mit einem Key Agreement initiiert wird.

Fazit

Eine benutzerfreundliche und dennoch sichere Konfiguration von IIoT-Geräten ist möglich: Servicetechniker benötigen vor Ort nur ein handelsübliches Smartphone oder Tablet und ihre persönliche Smartcard. Da die Smartcard SSH User Certificate und Private Key speichert, ist das Verfahren portabel und unabhängig vom Mobilgerät. Dennoch erreicht das Verfahren ein hohes Sicherheitsniveau, das sich auf Empfehlungen des BSI, NIST und verschiedenen Standards wie z. B. IEC 62443 stützt.

Dr. Jó Bitsch
exceet Secure Solutions GmbH
Dr. Dominik Schürmann
Cotech – Confidential Technologies GmbH

Jedes Ereignis im Blick

Um weiter zu wachsen, braucht Industrie 4.0 tragfähige SIEM-Lösungen

Produktion, Prozess, Mensch und Maschine – wo im Fahrwasser zunehmender Vernetzung bei Industrie 4.0 Sicherheitsrisiken aufploppen, ergeben sich neue Herausforderungen. Auch deshalb ist das Log- und Protokollmanagement einer der dringlichsten Aufgabenbereiche bei der Absicherung von IT-Strukturen.

Sichere Identitäten sind der Startpunkt für Vertrauensketten, die Erhebung, Transport und Verarbeitung von Daten auf Hardware-, Software- und Prozessebene absichern. Sie bilden die Voraussetzung für weitere Schutzmaßnahmen, die Unternehmen in puncto Datensicherheit ergreifen sollten, um sich regelkonform und wettbewerbsfähig aufzustellen. Denn eines ist klar: Sobald es einem Angreifer gelingt, sich unberechtigt einer Identität zu bemächtigen, laufen alle darauf aufbauenden Maßnahmen, insbesondere der kontrollierte Zugriffsschutz, ins Leere. Mit der Einführung eines Sicherheitsprozesses leiten IT-Verantwortliche notwendige organisatorische Veränderungen ein, definieren eine Strategie und nutzen Hilfsmittel zur Erreichung ihrer Schutzziele.

Logmanagement in der Industrie 4.0

Das Logmanagement ist ein wesentlicher Bestandteil jedes Managementsystems zur Informationssicherheit. Es stellt deshalb eine vorrangige Aufgabe bei der sicheren Ausgestaltung von ITK-Systemen dar. Hier genießt die Sicherstellung der Authentizität des jeweiligen Nutzers oberste Priorität. Pharmazie, Lebensmittelbranche und chemische Industrie achten schon seit Langem darauf. Organisationen wie die Food and Drug Administration (FDA) in den USA und die europäische Verordnung REACH (Registration, Evaluation, Authorisation and Restriction of Chemicals) aus dem Jahr 2007 haben in diesen Branchen zu einer erheblichen Regulierung geführt, die wiederum eine Nachvollziehbarkeit der Frage „Wer hat wann wie mit welcher Charge der Substanz an welchem Produktionsschritt mitgearbeitet?“ impliziert. Folglich ist die persönliche Anmeldung eines Mitarbeiters an einer Anlage der chemischen Industrie durchaus üblich.

Andere Industrien verfolgten diese Ansätze bisher kaum, mitunter überhaupt nicht. Mögliche Gründe dafür sind oftmals Vorbehalte gegenüber einer vermuteten Arbeitnehmerüberwachung, Bedenken bei der Einhaltung von Datenschutzvorschriften oder vielfältige technische Probleme.

SICHERHEIT IN 10 ETAPPEN

1. Strategie festlegen

Protokollierung muss, wie jede wichtige IT-Komponente, eine Strategie verfolgen. Schon bei der Strukturierung des DevOps-Aufbaus und der Veröffentlichung jeder neuen Funktion achten IT-Administratoren im Idealfall darauf, dass sie einen organisierten Protokollierungsplan beifügen. Dieser Plan sollte auch Hinweise beinhalten, ob personenbezogene Daten und Archivierungsanforderungen vorliegen.

2. Strukturierung der Logdaten

Parallel zur Strategieentwicklung ist es wichtig, das Protokollformat zu berücksichtigen. Wer effektive Protokollierungsformate nicht versteht, kann aus den hinterlegten Informationen keine Erkenntnisse gewinnen. Lesbare Protokolle erleichtern Fehlerbehebungen.

3. Protokolldaten separieren und zentralisieren

Protokolle sollten immer automatisch gesammelt und an einen zentralen Ort geschickt werden. Dies erleichtert die organisierte Verwaltung und erweitert die Analysefunktionen, sodass Verantwortliche Cross-Analysen effizient durchführen und Korrelationen zwischen verschiedenen Datenquellen identifizieren können. Die Zentralisierung von Protokolldaten reduziert auch das Risiko des Datenverlusts in einer Umgebung mit automatischer Skalierung. Eine Weiterleitung von Protokolldaten an einen zentralen Ort ermöglicht es Systemadministratoren, Zugriff auf die Daten zu gewähren, um Probleme zu beheben, ohne Projekte zu gefährden. Die Replikation und Isolierung von Protokolldaten minimiert auch das Risiko, dass Angreifer Protokolldaten löschen, um Sicherheitsverletzungen zu verbergen.

4. End-to-End-Protokollierung anwenden

End-to-End-Protokollierung an einem zentralen Ort ermöglicht es Verantwortlichen, Datenströme aus diversen Quellen dynamisch zu aggregieren, um die wichtigsten Trends und Kennzahlen in Beziehung zueinander zu setzen. Die Korrelation von Daten unterstützt sie dabei, Ereignisse, die Systemstörungen verursachen, schnell und sicher zu identifizieren.

5. Datenquellen verknüpfen

Um häufig auftretende Komplexitäten bei der Fehlerbehebung zu überwinden und eine ganzheitliche Sicht auf Anwendungen und Systeme zu erhalten, sollten Systemadministratoren alle Systemkomponenten überwachen und protokollieren. Dazu gehören auch Windows-Sicherheitsprotokolle, relevante Metriken und Ereignisse aus der zugrunde liegenden Infrastruktur, den Anwendungsschichten und den Endbenutzerarbeitsplätzen.

Fakt ist allerdings, dass die Nachvollziehbarkeit von Handlungen und eine individualisierte, eindeutige Zuordenbarkeit nur durch die Nutzung persönlicher Nutzerkonten an den Anlagen und Maschinen sowie den Bedienungsrechnern erreicht werden können. Dies erfordert wiederum die Verwaltung einer weitaus größeren Zahl an Konten, die bisher eher nur zwischen Einrichter, Instandhalter und Nutzer unterschieden haben.

Diese Personalisierung der Benutzerkonten führt wiederum dazu, dass diese auch auf einer Vielzahl von Anlagen und Maschinen parallel und effizient verwaltet werden müssen. Zumindest sollte eine persönliche Zuordenbarkeit auf Ebene der Fachanwendung möglich sein, wenn der Zugang zu den Betriebssystemen aus technischen Gründen nicht personalisiert werden kann oder soll.

SIEM-Lösungen schlagen Alarm

Letztlich ist nicht auszuschließen, dass es zu Unregelmäßigkeiten oder offensichtlich missbräuchlicher Nutzung von Anlagen und Applikationen kommen kann. Hier müssen verantwortliche Administratoren detailliert nachverfolgen können, wer wann und wo zugegriffen und wer wann und wo welche Änderungen vorgenommen hat. Dies setzt jedoch voraus, dass die Anwendung entsprechend detaillierte Logmeldungen erzeugt, diese speichert und sie auch über längere Zeitfenster möglichst unveränderbar zentral vorhält. Im Sinne einer in der IT üblichen Log-Zentralisierung erweisen sich Funktionen zur direkten, zugriffgeschützten Speicherung der Logs auf einem zumindest logisch abgesetzten Logmanagement-Server als sinnvoll.

Idealerweise beachten Entscheider hier Standardformate, wie sie etwa durch Syslog, Log Event Extended Format (LEEF), Common Event Format (CEF), DMTF's Common Information Model (CIM) oder die Cloud Auditing Data Federation (CADF) vorgegeben werden. Dies erleichtert die zentrale Auswertung und Korrelation von Meldungen und ermöglicht die Definition zentraler Schwellenwerte (Thresholds). Dazu gehört auch die Alarmierung der IT-Sicherheit, falls mit einem Benutzerkonto mehrfach innerhalb kurzer Zeit an diversen Geräten erfolglose Zugriffsversuche unternommen werden.

Diese Benachrichtigung erfolgt am besten vornehmlich über die Nutzung von sogenannten SIEM-Lösungen. Technisch und auf Prozessebene kann ein solches „Security Information and Event Management" unschätzbare Dienste leisten. In diesem Zusammenhang sollten Entscheider unbedingt eine skalierbare Lösung wählen, da zum einen wirklich umfangreiche Datensammlungen entstehen können und zum anderen Angreifer mit DDoS-Attacken bewusst die Grenzen solcher Systeme ausloten, um unprotokollierten Schabernack zu treiben.

Logmanagement in vier Schritten

Die Notwendigkeit eines transparenten Logmanagements ergibt sich aus dem Dreiklang aus gesetzlichen Auflagen, notwendiger Analyse von Sicherheitsvorfällen und kontinuierlichen Analyseprozessen wie bei der Hardware-/Softwareentwicklung. Dabei folgt ein effizientes Logmanagement stets diesen Prozessphasen: *Annahme – Verarbeitung – Auswertung – Visualisierung.*

Jeder am Logmanagement Beteiligte sollte verstehen, dass sich hinter dem Begriff ein Prozess und kein Produkt verbirgt. Dementsprechend liegt im Wissensmanagement, im internen Aufbau von Logging-Know-how, der wahre Benefit. Dazu gehören zwangsläufig der Aufbau und die Organisation entsprechender Strukturen, die eindeutige Definition aller personenbezogener Daten, die im Betrieb anfallen, eine sinnhafte Archivierung aller Protokolle sowie eine übergreifende Konzernbetriebsvereinbarung (KBV).

6. Eindeutige Identifikatoren verwenden

Eindeutige Identifikatoren nützen beim Debugging, Support und bei Analysen. Sie erlauben es, komplette Benutzersitzungen und Aktionen einzelner Benutzer genau zu verfolgen. Wenn IT-Mitarbeiter die eindeutige ID eines Benutzers kennen, können sie die Suche nach allen Aktionen filtern, die dieser Benutzer in einem bestimmten Zeitraum durchgeführt hat. Hier ist jedoch dem Datenschutz gemäß EU-DSGVO und der Betriebsvereinbarung Vorrang einzuräumen.

7. Kontext hinzufügen

Sobald Protokolle als Daten verwendet werden, ist es wichtig, den Kontext jedes Datenpunkts zu berücksichtigen. Zu wissen, dass ein Mitarbeiter auf eine Schaltfläche geklickt hat, ist möglicherweise nicht so nützlich, wie zu wissen, dass er beispielsweise gezielt auf die Schaltfläche „Verbrauchsmaterial bestellen" geklickt hat.

8. Echtzeit-Überwachung durchführen

Bei Serviceunterbrechungen oder Problemen auf Produktionsniveau kann eine Echtzeit-Überwachungslösung entscheidend sein, da oftmals jede Sekunde zählt. Eine „Live-Tail"-Sicht auf ihre Protokolldaten kann Entwickler und Administratoren befähigen, Protokollereignisse nahezu in Echtzeit zu analysieren, wenn Anwender mit ihren Anwendungen oder Systemen interagieren. Die Live-Tail-Suche und -Berichterstattung ermöglicht es zudem den Support-Teams, Kundenprobleme zu untersuchen und zu lösen, sobald sie auftreten.

9. Trends identifizieren

Während Protokolle früher als schmerzhafte letzte Möglichkeit galten, Informationen zu finden, befähigen heutige Protokollierungsdienste jeden, vom Entwickler bis zum Datenwissenschaftler, Trends und wichtige Erkenntnisse aus ihren Anwendungen und Systemen zu identifizieren. Die Behandlung von Protokollereignissen als Daten schafft die Möglichkeit, statistische Analysen zukünftig auch mit künstlicher Intelligenz auf Benutzerereignisse und Systemaktivitäten anzuwenden. Diese Einblicke öffnen die Tür zu fundierten Geschäftsentscheidungen auf der Grundlage von Daten, die außerhalb der Protokolle oft nicht verfügbar sind.

10. Teamprofit generieren

Ein Protokollverwaltungs- und Analysedienst, der nur einem hochtechnisierten Team zugänglich ist, schränkt die Möglichkeiten des Unternehmens, von Protokolldaten zu profitieren, erheblich ein. Deshalb sollten die Werkzeuge Entwicklern Live-Tail-Debugging, Administratoren Echtzeitalarmierung, Datenwissenschaftlern aggregierte Datenvisualisierungen und Support-Teams Live-Such- und Filterfunktionen bieten.

Vom Log- zum Protokollmanagement

In den letzten zehn Jahren hat die Weiterentwicklung verteilter Systeme neue Komplexitäten in der Verwaltung von Protokolldaten geschaffen. Heutige Systeme können Tausende von Serverinstanzen oder Micro-Service-Container enthalten, die jeweils ihre eigenen Protokolldaten erzeugen. Mit der raschen Entstehung und Dominanz von cloudbasierten Systemen erleben wir ein explosionsartiges Wachstum maschinell generierter Protokolldaten. Infolgedessen ist auch das Protokollmanagement zu einem festen Grundpfeiler eines modernen IT-Betriebes geworden und unterstützt eine Reihe von Anwendungsfällen wie Debugging, Produktionsüberwachung oder Support.

Während verteilte Systeme eine hohe Effizienz in Bezug auf die Skalierbarkeit bieten, stellen sie Teams, die sich auf Protokolldaten beziehen, vor enorme Herausforderungen: Wo sollen sie anfangen, welcher Aufwand ist angemessen und welche Hilfsmittel stehen zur Verfügung, um die benötigten Protokolldateien zu finden? IT-Administratoren, DevOps-Profis und alle anderen Mitarbeiter, die den protokollerstellenden Systemen am nächsten stehen, haben die Aufgabe, dezentrale Protokolldateien unter Einhaltung von Sicherheits- und Compliance-Protokollen zu verwalten. Allerdings könnten sich Entwickler und Ingenieure, die Probleme auf Anwendungsebene beheben müssen, durch den Zugriff auf Protokolldateien auf Produktionsniveau eingeschränkt fühlen. Betriebs-, Entwicklungs-, Datenwissenschaftler- und Support-Teams, die Einblicke in das Benutzerverhalten für Trendanalysen und Fehlerbehebungen benötigen, fehlt hingegen oft das technische Fachwissen, das erforderlich ist, um Protokolldaten effizient zu nutzen.

Angesichts dieser Herausforderungen ist es wichtig, bei der Implementierung einer Protokollierungslösung – abhängig vom jeweiligen Unternehmen und dem vorliegenden Komplexitätsgrad – Best Practices im weiten Industrie-4.0-Feld zu berücksichtigen. Von der Strategieentwicklung über die Erfassung und Archivierung der Daten bis hin zu deren Auswertung empfiehlt es sich, ein Sicherheitskonzept zu entwerfen, das über 10 Etappen ein zuverlässiges und praktikables Log- und Protokollmanagement gewährleistet (siehe Kasten oben).

Fazit

Die Weiterentwicklung verteilter Systeme hat in den letzten zehn Jahren neue Komplexitäten in der Verwaltung von Log- und Protokolldaten geschaffen. Gesetzliche Auflagen und geforderte Analysekompetenz bei Softwareentwicklung und Sicherheitsvorfällen triggern Security-Konzepte in Industrieunternehmen, die sich in der Industrie-4.0-Ära angekommen wägen. Wo Maschinen personenbezogene Daten produzieren und Produktionsdaten digital verfügbar sind, ist ein transparentes Logmanagement das A und O. Es gewährt Kontrolle und Nachweisbarkeit durch eine direkte Zuordnung des Bedieners an einer Maschine, Produktionsanlage oder einem datengetriebenen System. Technisch und auf Prozessebene leistet dies ein tragfähiges Security Information and Event Management. Ein verlässliches Log- und Protokollmanagement ist eine Grundbedingung für die sichere Fortentwicklung der Industrie 4.0.

Pierre Gronau
Gronau IT Cloud Computing

Impressum
Themenbeilage Sicherheit & Datenschutz

Redaktion just 4 business GmbH
Telefon: 08061 34811100, Fax: 08061 34811109,
E-Mail: tj@just4business.de

Verantwortliche Redakteure:
Thomas Jannot (v.i.S.d.P.), Ralph Novak, Franziska J. Bock (Redaktion), Rudolph Schuster (Lektorat)

Autoren dieser Ausgabe:
Stefan Beyer, Dr. Jó Bitsch, Daniel Dyroff, Pierre Gronau, Matthias Kess, Dr. Holger Mühlbauer, Ingolf Rauh, Klaus Schmeh, Dr. Dominik Schürmann

DTP-Produktion:
Lisa Hemmerling, Matthias Timm, Hinstorff Media, Rostock

Korrektorat:
Marei Stade, Hinstorff Media, Rostock

Titelbild:
© shutterstock, piick

Verlag
Heise Medien GmbH & Co. KG,
Postfach 61 04 07, 30604 Hannover; Karl-Wiechert-Allee 10, 30625 Hannover;
Telefon: 0511 5352-0, Telefax: 0511 5352-129

Geschäftsführer:
Ansgar Heise, Dr. Alfons Schräder

Mitglieder der Geschäftsleitung:
Beate Gerold, Jörg Mühle

Verlagsleiter:
Dr. Alfons Schräder

Anzeigenleitung (verantwortlich für den Anzeigenteil):
Michael Hanke (-167), E-Mail: michael.hanke@heise.de, www.heise.de/mediadaten/ix

Leiter Vetrieb und Marketing:
André Lux

Druck:
Dierichs Druck + Media GmbH & Co. KG, Frankfurter Straße 168, 34121 Kassel

storage2day

17.–19. September 2019

Print Media Academy, Heidelberg

Die Konferenz
zu Speichernetzen
und Datenmanagement

PROGRAMM ONLINE
Frühbucher bis 26.07.2019

AUSZUG AUS DEM PROGRAMM:

- **Software Defined Storage**
  - SDS-Grundlagen
  - Erasure Coding
  - Praxisbericht: SDS im Petabyte-Bereich
  - Einführung, Betrieb und Ausbau einer produktiven Ceph-Umgebung
- **Cloud-Storage**
  - Grundlagen des Cloud-Storage
  - Cloud-Sicherheit
  - Cloud-Storage und DSGVO
- **Archivierung und Backup**
  - Revisionssichere Speicherung sensibler Daten
  - Disaster Recovery
  - Die Zukunft von Tape Storage
- **Storage-Infrastruktur und Vernetzung**
  - NVMe-oF – Grundlagen und Möglichkeiten
  - Sichere Dateidienste
  - Speicherinfrastrukturen für Künstliche Intelligenz

www.storage2day.de

Platinsponsor

THOMAS KRENN®

Goldsponsoren

aikux.com · cisco · CLOUDIAN · DATACORE · FASTLTA · FUJIFILM · FUJITSU · PURESTORAGE · Tintri BY DDN

Silbersponsoren

EUROstor · Lenovo · TechData Advanced Solutions · TOSHIBA

Bronzesponsor

SCALITY

Veranstalter

iX · dpunkt.verlag