White Paper

Einer Studie zufolge können PKI-Investitionen dazu beitragen, die Sicherheit im Unternehmen zu verbessern und Geschäftsprozesse zu modernisieren

Gesponsert von: DigiCert Inc.

Robert Westervelt
August 2019

ZUSAMMENFASSENDER ÜBERBLICKZSZ

Die rasante Entwicklung von Digitalisierungsinitiativen im Unternehmen trägt dazu bei, dass der Druck auf IT-Sicherheitsexperten und Betriebsabteilungen wächst, die für die Sicherheit und Zuverlässigkeit der geschäftskritischen Systeme verantwortlich sind. In einem Versuch, diesen Druck angesichts der kontinuierlich wachsenden hybriden und Multicloud-Umgebungen zu mindern und Ressourcen effektiver zu verteilen, richten CIOs, CISOs (Chief Information Security Officer) und Sicherheitsarchitekten jetzt den Fokus auf Public Key Infrastructure(PKI)-Implementierungen, die oft uneinheitlich sind und schlecht gemanagt werden.

PKI ist das Rückgrat vieler Unternehmen, die auf Resilienz bei der Cybersicherheit setzen, da es ihnen die Möglichkeit bietet, die Durchsetzung von Datensicherheitsrichtlinien und -verfahren mithilfe digitaler Zertifikate und öffentlicher Schlüssel zu automatisieren. Die Sicherheitsmethode wurde entwickelt, um überprüfte und zuverlässige Verbindungen zwischen Systemen herzustellen und Benutzern freien Zugriff auf sicherheitsrelevante Ressourcen bereitzustellen. Nach und nach wurde PKI auch zum Schutz von Dokumenten, E-Mails und Code mithilfe kryptografischer Signing-Zertifikate und zum Schutz von Assets und Anwendern mit digitalen Identitäten über Gerätezertifikate eingesetzt.

Da der Druck auf Sicherheitsabteilungen größer als je zuvor ist, wird PKI heute gründlichen Tests unterzogen und immer häufiger verwendet. Public Key Infrastructure wird zur Beseitigung von Risiken genutzt, wenn Unternehmen verstärkt auf Clouddienste setzen. Angreifer wiederum versuchen, sich die Komplexität und die Konfigurationsprobleme zunutze zu machen, die auf eine zerstückelte Sicherheitsinfrastruktur zurückzuführen sind. CISOs machen es sich nun zur Aufgabe, diese Herausforderung zu bewältigen. Dies ging aus der IDC-Studie *Data Services for Hybrid Cloud* (Datendienste für Hybrid-Cloud-Umgebungen) hervor, die unter mehr als 400 IT-Sicherheits- und Datenverwaltungsexperten in Europa und Nordamerika durchgeführt wurde. Dabei gaben etwa 65 % der Unternehmen an, digitale Zertifikate und PKI zu verwenden, um eine Vielzahl unterschiedlicher Funktionen zu nutzen:

- **Sicheres BYOD:** Unterstützung nicht verwalteter BYOD-Initiativen und sicherer Zugriff auf Unternehmensressourcen ohne Abstriche beim mobilen Benutzererlebnis
- **Sichere Authentifizierung:** Starke Benutzerauthentifizierung in Anwendungen, die vertrauliche Informationen enthalten
- **Sicherer Fernzugriff:** Starke Authentifizierung von Mitarbeitern und Partnern in einem WLAN oder VPN

- **Sichere E-Mails:** Verschlüsselung und digitale Signierung von E-Mails auf allen Geräten des Unternehmens
- **Signieren von Dokumenten:** Überprüfung der Integrität und Echtheit digitaler Signaturen in wichtigen Dokumenten
- **Sichere IoT-Geräte (Internet of Things):** Bereitstellung von Geräteidentität, Aufstellung eines Root of Trust und Wahrung der Integrität von Software und Firmware auf sicherheitsrelevanten IoT-Geräten

Je mehr sich Unternehmen bei der Sicherheit auf PKI verlassen – und Angreifer raffiniertere und häufigere Attacken auf sensible Daten durchführen –, desto wichtiger wird es für Sicherheitsabteilungen, umfassende und koordinierte Ansätze zu implementieren, um mit neuen Geschäftsstrategien Schritt zu halten. IDC rechnet damit, dass 60 % der Unternehmen innerhalb der nächsten 24 Monate an der Implementierung einer Digitalisierungsstrategie arbeiten werden. Dabei stellt die IT-Transformation (ITX) einen zentralen Bestandteil dar, und Datensicherheit und -verfügbarkeit bilden die Grundlage der ITX. PKI spielt eine entscheidende Rolle bei der Wahrung der Integrität, Verfügbarkeit und Resilienz der IT-Infrastruktur eines Unternehmens, doch die Verwaltung der Datensicherheit in diesen zunehmend hybriden Umgebungen gewinnt mit jeder neuen und vielfältigeren Bedrohung an Komplexität. Die jüngste Serie öffentlich bekannt gewordener Datendiebstähle macht deutlich, welche Probleme die verteilten und verschachtelten Unternehmensumgebungen von heute aufwerfen. Angreifer schlagen Kapital aus kostspieligen Fehlern, die Datenbankserver anfällig für unbefugte Zugriffe aus dem öffentlichen Netz machen. Dabei nutzen sie weiterhin unsichere und gestohlene Passwörter oder unveränderte Standardpasswörter und suchen systematisch nach Schwachstellen, die durch das Datenmanagement in verteilten Umgebungen entstehen. Mehr als 30 % der Studienteilnehmer gaben an, dass ihnen die Integration von hybriden und Multicloud-Umgebungen in die bestehende IT-Infrastruktur Probleme bereitet, und 37 % nannten die Komplexität der Sicherheitsmaßnahmen (nach den immer ausgeklügelteren Methoden der Angreifer und den Risiken bei der Cloudeinführung) als eine der drei größten Bedrohungen für ihr Unternehmen in den nächsten zwei Jahren. Die Problematik wird häufig durch fehlerhafte PKI-Vorgänge erschwert, die sich auf die Produktivität der Anwender auswirken, das Vertrauen von Kunden und Partnern untergraben und zu teuren Sicherheits- und Datenschutzverletzungen führen können.

PKI-Unterstützung für kritische Geschäftsanwendungen ist „extrem effektiv“

In den Gesprächen im Rahmen dieser Studie wurde ein durchweg positives Bild davon vermittelt, wie reibungslos sich PKI in unterschiedliche branchenspezifische Geschäftsanwendungen integrieren lässt. Demnach ermöglichen PKI-Bereitstellungen die Skalierung von Umgebungen für komplexe Zahlungsanwendungen und Point-of-Sale(POS)-Terminals für den Fernzugriff, die Integration verschiedener Backend-Systeme, einschließlich erweiterter Analyse-Repositories für die Verschlüsselung, sowie das digitale Signieren von Dokumenten, um die vertragliche Integrität bei Feldeinsätzen mit einem kundenspezifischen Content-Management-System zu gewährleisten.

Insbesondere CISOs und Sicherheitsarchitekten waren von den Vorteilen der PKI überzeugt und bezeichneten die Technologie als „extrem effektiv“ – wenn sie richtig implementiert und proaktiv gemanagt wird. Die Mehrheit der befragten Personen arbeitet mit mehreren PKI-Implementierungen, die in branchenspezifische Geschäftsanwendungen und Active Directory eingebunden sind. Ihre Erfahrung im Bereich der PKI-Verwaltung reicht so weit zurück, dass sie in ihrem Unternehmen bereits viele Entwicklungen miterlebt und an zahlreichen sicherheitsrelevanten Aktualisierungen der

bestehenden PKI-Implementierungen beteiligt waren. IDC empfiehlt folgende Maßnahmen für IT-Abteilungen, um die Effektivität der PKI zu erhöhen:

- Es sollte ermittelt werden, ob das Unternehmen Sicherheitsarchitekten gewinnen, schulen oder halten kann, um die bestehenden PKI-Implementierungen zu verwalten. Außerdem sollte bestimmt werden, ob die Abteilung über das nötige Know-how verfügt, um neue Geschäftsziele umzusetzen, die eine skalierbare Anwendung digitaler Zertifikate erfordern.
- Die Nutzung von Managed PKI-Services könnte das Management optimieren und die Komplexität reduzieren. Wenn eine PKI erst einmal entworfen und implementiert wurde, kann es sehr aufwendig sein, Spezifikationen und Prozesse wieder zu ändern. Vorabinvestitionen sind der Schlüssel zum Erfolg.

METHODIK

Für diese IDC-Studie wurden Chief Information Security Officers (CISOs) und Sicherheitsarchitekten mehrerer großer Unternehmen zu ihrer bestehenden PKI-Infrastruktur befragt. Außerdem wurde gefragt, wie die Infrastrukturen für die Cloudeinführung und die Digitalisierungsstrategien in den jeweiligen Unternehmen angepasst wurden. Die Erkenntnisse aus diesen Gesprächen wurden mit neuen Umfragedaten zu den Herausforderungen bei der Sicherung von hybriden und Multicloud-Umgebungen kombiniert. Im Rahmen der Studie wurden Effizienzsteigerungen und reduzierte Verwaltungskosten in verschiedenen Anwendungsfällen festgestellt. Zu diesen Fällen gehören verwaltete und lokale PKI-Implementierungen mit folgender Funktionalität: Code Signing zur Echtheitsprüfung von Softwareupdates auf IoT-Geräten, Dokumentsignierung zur Beseitigung von Papierdokumenten und manuellen Prozessen, sichere E-Mails, sicherer Fernzugriff sowie Anwender- und Computerauthentifizierung für den Zugriff auf vertrauliche Unternehmensressourcen.

SITUATION OVERVIEW

PKI-Grundlagen für die erfolgreiche Abwehr von Angriffen und den Schutz geschäftskritischer Ressourcen

Viele Unternehmen nehmen die Hilfe von PKI-Spezialisten in Anspruch, um das Management digitaler Zertifikate im Zuge der Digitalisierung zu optimieren, zu zentralisieren und zu automatisieren. So sollen zerstreute und überflüssige Infrastrukturkomponenten beseitigt und die Kosten gesenkt werden. Die Arbeit umfasst die Automatisierung des Managements einer oder mehrerer PKI-Implementierungen für verschiedene Geschäftseinheiten durch die Einführung eines Managed PKI-Services, um proaktive Kontrollen und Zuverlässigkeit zu gewährleisten.

Kostensenkungen und Effizienzsteigerungen wurden gemäß dieser Studie häufig als Gründe für die Investition in PKI genannt. Wesentlich vorangetrieben wurden PKI-Implementierungen jedoch durch die Schwachstellen und Sicherheitslücken, die auf die Komplexität beim Implementieren und Managen von Sicherheitsprodukten zurückzuführen sind. Laut der IDC-Studie *Data Services for Hybrid Cloud* gaben fast 40 % der Experten für IT-Sicherheit, Geschäftsbereiche und Datenmanagement an, dass die immer raffinierteren Angriffe und die zunehmende Komplexität bei Management und Betrieb von Sicherheitsprodukten wesentliche Herausforderungen darstellen. Den Untersuchungen von IDC Research zufolge müssen Sicherheitsabteilungen sich mit immer mehr Sicherheits- und Datenschutzbedenken auseinandersetzen. Sie stehen unter einem hohen Druck, die ständig

wachsende Anzahl neuer Compliance-Bestimmungen zu erfüllen. Gleichzeitig müssen sie wichtige Unternehmensressourcen kontinuierlich vor gezielten und vielseitigen Cyberangriffen schützen.

Neben den zuvor genannten Reputationsschäden, direkten Kosten und aufsichtsrechtlichen Sanktionen können Cyberangriffe ungeplante Ausfallzeiten, den Verlust wichtiger Geschäftsgeheimnisse und unwiderrufliche Datenverluste nach sich ziehen. Gemäß IDC Research belaufen sich die durchschnittlichen Kosten für Ausfallzeit branchenweit auf 250.000 USD pro Stunde. Ein Vergleich der Kosten für Angriffsprävention und Wiederherstellungssoftware mit einer einzigen Stunde Ausfallzeit ist oft schon genug, um die Investition zu legitimieren. In vielen Fällen müssen Sicherheitsverletzungen heute öffentlich bekannt gegeben werden. Dieser Umstand führt nicht selten zu einer langfristigen Rufschädigung, und verlorene Kunden und Daten lassen sich nicht immer zurückgewinnen. Laut IDC Research wird fast die Hälfte der Situationen, in denen Datenschutzverletzungen auftreten, von Reputationsschäden begleitet, was wiederum zu höheren Kosten bei Wiederherstellung und Korrekturmaßnahmen führt.

Dadurch, dass sich Sicherheitsvorfälle immer mehr unter dem Auge der Öffentlichkeit abspielen, werden Unternehmen und Verbraucher ständig daran erinnert, dass die Sicherheit auf Identitätsdaten basiert. Zahlreiche Studien haben gezeigt, dass Sicherheitsvorfälle durch Schwachstellen und Konfigurationsprobleme begünstigt werden, die oft auf eine steigende Komplexität zurückzuführen sind. Die Optimierung zerstückelter und uneinheitlicher PKI-Implementierungen kann dazu beitragen, die Anzahl der menschlichen und systembasierten Fehler zu reduzieren, die von Angreifern ausgenutzt werden, und dabei den Verlust von Daten zu verhindern. Eine ordnungsgemäß bereitgestellte und gemanagte PKI ist eins der effektivsten Werkzeuge für Unternehmen, um kostspielige und unangenehme Datenschutzverletzungen zu vermeiden. Immer mehr Unternehmen überarbeiten ihre Verschlüsselungs- und Schlüsselverwaltungsstrategien, um situationsbasierte Erkenntnisse zu gewinnen und dadurch ihre Sicherheit zu erhöhen.

Die im Rahmen dieser Studie befragten Sicherheitsexperten bezeichneten PKI als grundlegende, bewährte Komponente für die Datenverschlüsselung und die Überprüfung der Daten- und Transaktionsintegrität. Die Technologie sei von entscheidender Bedeutung, um die Identität von Benutzern und Computern in ihren Unternehmen zu bestätigen. PKI kann die Hürden erhöhen, die ein Angreifer überwinden muss, um sich Zugriff auf wichtige Ressourcen zu verschaffen. Außerdem ermöglicht PKI die skalierbare Sicherheit, die für schnelle oder vielschichtige Geschäftsprozesse erforderlich sind, und bietet Einblicke in die Aktivitäten der Endbenutzer, was bewiesenermaßen die Benutzerproduktivität und die Kundenbindung verbessert.

Ein Thema, das bei den Gesprächen aufkam, ist die anhaltende Problematik der Anwendung von Sicherheitsmaßnahmen, die den Erwartungen der Endbenutzer entsprechen. In Reaktion auf diese Herausforderung lassen immer mehr Sicherheitsverantwortliche – nachdem die Risiken eines geschäftlichen Unterfangens identifiziert wurden – Lösungen von externen PKI-Anbietern entwickeln, die einen zuverlässigen Betrieb mit der bestehenden IT- und Sicherheitsinfrastruktur ermöglichen. Für Unternehmen, die sich für die Entwicklung und proaktive Verwaltung einer PKI-Lösung entscheiden, wird die Sicherheit der Garant für Funktionalität oder Produktivität. Eine korrekt implementierte, moderne PKI kann die erforderlichen Authentifizierungsschritte verringern, die die Endbenutzer bei der Arbeit durchführen müssen. Ehemals mühselige Sicherheitsverfahren, die bei den Benutzern eines Unternehmens für Unmut sorgten, können jetzt größtenteils automatisiert werden. Sicherheitsbedenken werden häufig thematisiert, wenn die Ergebnisse einer Prüfung vorliegen, wenn eine Datenschutz- oder Sicherheitsverletzung aufgetreten ist oder, wie so oft der Fall, wenn neue aufsichtsrechtliche Bestimmungen oder Unternehmensrichtlinien erfüllt werden müssen. Heute setzen Unternehmen

verstärkt auf Funktionen, die von der PKI unterstützt werden, etwa Multifaktor-Authentifizierung, Verschlüsselung und Mobilität.

Einige der für diese Studie befragten CISOs erhielten den direkten Auftrag vom CIO, die Kosten zu verringern, Cloud-First-Initiativen umzusetzen und den Zustand der PKI-Infrastruktur zu analysieren. Die ermittelten und dokumentierten PKI-Implementierungen waren kurz davor, unter der Last der rasanten technologischen und geschäftlichen Entwicklung zusammenzubrechen. In manchen Fällen konnte die bestehende Infrastruktur nicht ausreichend gepflegt werden, weil das Unternehmen nicht in der Lage war, qualifizierte IT-Sicherheitsexperten zu gewinnen und zu halten. Bei anderen Unternehmen wurden zerstückelte PKI-Implementierungen genutzt, die aus Fusionen und Übernahmen entstanden oder auf getrennte Geschäftseinheiten zurückzuführen waren, für die aus Sicherheits- und Ablaufbeschränkungen separate Umgebungen geführt werden mussten. Meistens werden die Herausforderungen komplexer Unternehmensumgebungen durch die wachsende Anzahl verteilter Ressourcen zusätzlich verstärkt. Die Ergebnisse der IDC-Studie *Data Services for Hybrid Cloud* deuten darauf hin, dass diese Probleme auch heute noch Aktualität besitzen. PKI wurde als erhebliche Herausforderung für Unternehmen genannt, die aufwandstechnisch mit der Implementierung und Verwaltung von Verschlüsselungslösungen oder der Bereitstellung und Anpassung von Plattformen für die Datenverlustpräventation vergleichbar sei.

PKI-ANWENDUNGSFÄLLE

In den Fallstudien, die in den folgenden Abschnitten erläutert werden, erfahren Sie, wie Unternehmen die PKI an ihre individuellen Anforderungen anpassen.

Verbesserter Sicherheitsstatus dank PKI für Email Security und Authentifizierung

Cybersicherheit war für diesen globalen Hersteller von Konsumgütern nie eine Priorität. Es gab keine zuverlässige und effektive Authentifizierung für den Mitarbeiterzugriff auf vertrauliche Ressourcen oder die Integritätsprüfung für externe Mitarbeiter. Dadurch entstanden gravierende Schwachstellen, die das Unternehmen überwiegend ignorierte. Als sich eine geschäftsschädigende Ransomware in Form der Malware SamSam im Unternehmen ausbreitete, wurde die Geschäftsführung im Mutterkonzern des Herstellers auf die Angelegenheit aufmerksam. Zu den ersten Maßnahmen gehörte die Investition in PKI, um beim Hersteller Email Security und Benutzerauthentifizierung einzuführen.

Mit der SamSam-Malware hatten die Angreifer eine Sicherheitslücke im Zusammenhang mit den FTP-Servern des Unternehmens ausgemacht und gezielt ausgenutzt, um sich über einen Brute-Force-Angriff auf unsichere Passwörter Zugang ins System zu verschaffen. Durch den kostspieligen Vorfall war das Unternehmen gezwungen, fast die gesamte Produktion einzustellen, was jeden Tag einen Verlust in Millionenhöhe bedeutete. Da es praktisch keine Datensicherung gab, halfen die Mitarbeiter, auf Papier vorliegendes geistiges Eigentum zusammenzutragen. Einige Informationen konnten außerdem aus Bandsicherungssystemen wiederhergestellt werden. Zur Verbesserung der Sicherheitsinfrastruktur verpflichtete sich das Unternehmen zu erheblichen Investitionen, einschließlich des Einsatzes von PKI zur Sicherung der E-Mail-Systeme.

„Ich wurde eingestellt, um ein komplett neues Sicherheitsprogramm zu entwickeln. Es gab Richtlinien, aber keine wirklichen Maßnahmen“, erinnerte sich der CISO, der kurz nach dem Vorfall ins Unternehmen kam, um ein Sicherheitsprogramm zu erstellen und die Sicherheit des Herstellers an die Standards des Mutterkonzerns anzupassen. „Unsere Anwendungen war nicht auf dem neuesten Stand, und unsere

Sicherheitsinfrastruktur war schlecht konfiguriert oder nicht vorhanden. Als wir uns einen Überblick darüber verschafft hatten, wo sich unsere vertraulichen Daten befinden, mussten wir noch die richtigen Tools einführen. Deshalb haben wir unsere Sicherheitsinfrastruktur auf moderne PKI umgestellt, um Authentifizierung und gesicherte E-Mails für alle Benutzer bereitzustellen – unabhängig von ihrem Standort oder dem verwendeten Gerät."

Das Sicherheitsteam musste einen zukunftssicheren und mit dem Mutterkonzern kompatiblen Austausch von E-Mails und Datendateien gewährleisten, um PKI im Rahmen einer Migration von einer veralteten Implementierung von Lotus Notes auf Microsoft Office 365 einzuführen. Für den Anfang ordnete das Unternehmen den Einsatz einer Zwei-Faktor-Authentifizierung an und nutzte Clientzertifikate, um unsichere Passwörter zu beseitigen und die Identität aller 1.300 Office 365-Konten zu bestätigen. Dazu wurde die PKI in Microsoft Active Directory Federated Services integriert.

Das Unternehmen aktivierte S/MIME-Zertifikate, die standardmäßig zu Verschlüsselungs- und Integritätszwecken verwendet werden können. Dazu werden digitale Mitarbeitersignaturen bereitgestellt, einschließlich der Funktionalität, bei der Kommunikation mit Partnern, internen und externen Mitarbeitern Empfangsbestätigungen für gesendete Nachrichten anzufordern. Eine E-Mail-Appliance löscht eingehende und ausgehende Nachrichten, und Webproxys sorgen für E-Mail- und Internetschutz. Mithilfe dieses Ansatzes konnte die Sicherheit des Herstellers erheblich verbessert werden, da S/MIME Man-in-the-Middle-Angriffe verhindern und dazu genutzt werden kann, geschäftskritisches geistiges Eigentum zu verschlüsseln.

Neben Sicherheitstools investierte das Unternehmen in Schulungen und Informationskampagnen. „Unsere Mitarbeiter wissen, dass Inhalte mit eingeschränktem oder stark eingeschränktem Zugriff immer verschlüsselt werden müssen, selbst wenn sie interne E-Mails senden", so der CISO.

Um eine Unterbrechung der E-Mail-Systeme zu verhindern, beauftragte der Mutterkonzern des Herstellers einen PKI-Experten für die Entwicklung und Feinjustierung der Implementierung. Es traten ein paar Probleme mit der Anmeldung auf, und Konflikte mit bestehenden Sicherheitsrichtlinien, bei denen verschlüsselter Datenverkehr abgelehnt oder in Quarantäne verschoben wurde, unterbrachen die Zustellung von E-Mails. Außerdem hätte man die Verwaltung der Schulungsprogramme nach Ansicht des CISOs möglicherweise ausführlicher planen können. „Aufgrund des Malware-Vorfalls wurden die neuen Richtlinien und die Prozessänderungen von den Mitarbeitern anstandslos akzeptiert", berichtete der CISO. Heute befindet sich das Sicherheitsprogramm des Unternehmens weiter im Aufschwung. Kürzlich wurde eine Übung zur Ermittlung und Klassifizierung von Daten bereitgestellt, und die perimeterbasierte Sicherheit für die unternehmensinternen Assets wird kontinuierlich verbessert.

Einsatz von PKI zur Sicherung moderner Kreditvergabefunktionen und Integration erweiterter Analysen

Zur Modernisierung der Kreditvergabe und Steigerung der Kundenzufriedenheit entschied sich eine Großbank für eine Managed PKI-Lösung. Diese sollte zum Schutz digitalisierter Formulare eingesetzt werden und für eine den Compliance-Anforderungen entsprechende durchgängige Dokumentenverschlüsselung sorgen. Der Sicherheitsaspekt war ein wesentlicher Bestandteil der Investition und durfte für das Erreichen des übergeordneten Ziels, einer dynamischen und optimierten Nutzererfahrung für Neukunden, kein Hindernis darstellen.

Die Bank evaluierte verschiedene Sicherheitslösungen, mit denen die Geschäftsstrategie eines beschleunigten Kreditvergabeprozesses umgesetzt werden konnte. Das zuständige Team suchte

nach PKI-Lösungen für eine flexible Bereitstellung in den Filialen und eine Einbindung in die bestehende Backend-Infrastruktur. Da in einigen Bereichen nicht genügend Mitarbeiter zur Verfügung standen, sollte die Lösung nicht nur benutzerfreundlich und zuverlässig sein, sondern außerdem einen geringen Ressourcenbedarf aufweisen und trotz einer Integration mehrerer Zertifizierungsstellen eine gute Performance bieten.

Es musste eine Lösung entwickelt werden, um unstrukturierte Inhalte innerhalb des Big Data Lake in strukturierte Daten umzuwandeln. Diese mussten wiederum von der KI-Engine unterstützt werden, mit der der virtuelle Assistent ausgeführt wird. Die Bank verfügte über die nötigen Mittel, um Data Scientists und ein Entwicklungsteam für die Durchführung dieser Aufgabe zu beschäftigen. Für die Sicherheit dieser Daten waren PKI-Lösungen die naheliegende Wahl.

Ein PKI-Service musste in die interne Compliance-Software integriert werden, mit der das Onboarding neuer Clients überwacht wird. Weitere Sicherheitsanforderungen waren Hochverfügbarkeit, eine leistungsstarke Disaster Recovery und eine dedizierte Instanz des PKI-Services zur Ausführung in der Virtual Private Cloud der Bank. Darüber hinaus musste die PKI-Lösung die Verschlüsselung von Kreditvergabedokumenten unterstützen und sich in das Content-Repository und eine stark ausgelastete Umgebung für erweiterte Analysen einbinden lassen, die für die Kundenbindung und zur Erweiterung der Serviceangebote der Bank eingesetzt wird.

„Ausfallzeit war keine Option und wir mussten die vollständige Kontrolle über die Schlüssel auf unserer Seite des Systems haben“, sagte der CISO gegenüber IDC. „In Anbetracht unserer Sicherheitsanforderungen für äußerst kritische Assets wussten wir, dass PKI für uns die beste Lösung darstellt. In geschäftlicher Hinsicht konnten wir bereits zahlreiche Verbesserungen feststellen, und bisher hat die Lösung uns Vertrauen in unsere Fähigkeit geschenkt, diese kritischen Transaktionen zu sichern und die Compliance-Bestimmungen einzuhalten.“

Die Implementierung erfordert serverseitigen Code und nutzt Agents an den Endpunkten, um die Anforderungen für Verschlüsselung und digitale Signatur bei der Dokumentenerstellung und -übermittlung zu erfüllen. Der gesamte Workflow wird mithilfe des HTTPS-Protokolls über das Internet überwacht und aufgezeichnet. Die Erstellung der Dokumente erfolgt durch Mitarbeiter an den Endpunkten, aber das Repository befindet sich auf dem Server.

Das Content-Repository der Bank und eine Umgebung für erweiterte Analysen wird derzeit in einen neuen virtuellen Assistenten integriert, der das Abrufen von Signaturen der Kreditnehmer automatisieren und den Prozess der Kreditvergabe entlasten soll. Kreditanträge werden jetzt nicht mehr gescannt, gedruckt und gefaxt. Sobald die PKI-Lösung die Identität des Kreditnehmers bestätigt hat, sind der Besuch einer Bankfiliale und die Anwesenheit eines Privatbankiers oder Kundenberaters zur Finalisierung der Dokumente nicht mehr erforderlich. Antragssteller können jetzt jeden Schritt ganz bequem von zu Hause über eine sichere Onlineverbindung abschließen. Mittlerweile unterstützt die Lösung bis zu 20.000 Benutzer, einschließlich juristischer Mitarbeiter, Risiko- und Compliance-Experten, Kreditberater, Kunden und anderer am Kreditvergabeprozess beteiligten Personen.

„Die Implementierung der PKI-Lösung erfordert eine sorgfältige Planung“, erklärte der CISO. „Es ist zwar sinnvoll, die Sicherheitsinfrastruktur zu optimieren und zu zentralisieren, aber man muss auch politische Hürden berücksichtigen, z. B. das Risiko eines Datendiebstahls. Wenn sich alle Ressourcen an einem Ort befinden, ist die Gefahr umso größer. Das Einzige, das für den Zugriff auf alle Datensilos unbedingt zentralisiert werden sollte, ist eine Lösung zur Verhaltensanalyse.“

Regionalbank wechselt für Mobilität und erweiterte Verifizierung zu Managed PKI

Eine große Regionalbank entwickelte über mehrere Jahre ein PKI-Programm. Zur Unterstützung einer eigenen Zertifizierungsstelle wurde die Infrastruktur intern verwaltet. Mit der Zeit wurde es jedoch immer schwieriger, für diese Aufgabe qualifizierte Sicherheitsexperten zu finden, zu schulen und zu halten. Die Komplexität der Verwaltung eines zerstückelten PKI-Programms trieb einige Mitarbeiter des Sicherheitsteams „in die Flucht“, wie ein leitender Sicherheitstechniker der Bank gegenüber IDC erwähnte.

Die interne IT-Abteilung hatte mit der Verwaltung mehrerer PKI-Implementierungen zu kämpfen, die eine funktionierende Benutzerauthentifizierung verhinderten. Über einen Zeitraum von fast zehn Jahren hatte man verschiedene Lösungen zum Einsatz von Smartcards entwickelt, eine Lösung für VPN- und Mobilgerätezugriff und ein paralleles System für E-Mail-Verschlüsselung und -Signierung. Die Komplexität dieser getrennten Lösungen führte aufgrund eines veralteten Zertifikatausstellungsmechanismus oft zu Problemen für die Endbenutzer. Entweder konnte die interne Zertifizierungsstelle keine neuen Zugriffskontrolllisten mehr ausgeben oder die Benutzer konnten nicht im Netzwerk authentifiziert werden. Ausfälle konnten viele verschiedene Gründe haben – manchmal lag ein Hardwarefehler in einem Sicherheitsmodul vor, manchmal fiel ein Windows-Server aus. „Vieles kann schiefgehen“, sagte ein Sicherheitstechniker.

„Wir hatten schon die Befürchtung, wir könnten das gesamte Netzwerk zum Erliegen bringen. Wenn die PKI auf einmal ausfällt und die Benutzer nicht mehr auf bestimmte Anwendungen zugreifen oder sich anmelden können, hat unser Team ein Problem“, meinte der Sicherheitstechniker gegenüber IDC.

Heute setzt die Bank auf eine PKI-Integration in einer modernen Mobilgerätemanagement-Plattform, die Mobilgeräte- und VPN-Benutzern eine unkomplizierte Authentifizierung ermöglicht. Alle Zugangsdaten werden in einer zentralen Smartcard-Anwendung für Mobilgeräte verwaltet und durch einen Managed PKI-Service überwacht. „Die Anzahl der redundanten Systeme wird durch das IT-Team langsam reduziert. Zuerst wurden dafür die Geräteausgabeprozesse modernisiert und stärker auf Active Directory ausgerichtete Smartcards eingesetzt“, so der Sicherheitstechniker.

Die Entscheidung für einen Managed PKI-Service hat die Arbeit der IT-Abteilung zusätzlich erleichtert. „Die vollständig lokale Infrastruktur und das von uns angestrebte Sicherheitsniveau verursachten viel Komplexität und Aufwand, die wir mit dem vorhandenen Personal nicht bewältigen konnten. Die interne Verwaltung eines PKI-Programms erfordert die Ressourcen einer großen Organisation. Wenn diese Voraussetzung nicht gegeben ist, kann ich nur davon abraten.“

Das interne IT-Teamarbeitet außerdem gemeinsam mit dem PKI-Anbieter daran, die Zertifikatausstellung in die eingesetzten Smartcards zu integrieren, und hat das zerstreute E-Mail-System der Bank durch einen optimierten Managed Service für erhöhte E-Mail-Sicherheit ersetzt. Die Bank betreibt eine eigene Active Directory-Umgebung und arbeitet weiterhin daran, die Prozesse zur Verwaltung von Zertifizierungsstellen und Veröffentlichung von Zertifikaten zu konsolidieren. Da die Zertifikatverwaltung jetzt in die Smartcardmanagement-Plattform integriert ist, werden für den VPN-Zugriff digitale Zertifikate verwendet. Mit der Einführung von Managed PKI wurde die Verwaltung von Zertifikaten über den gesamten Lebenszyklus in den 40 Filialen erheblich verbessert. Dadurch wurde den IT-Teams eine weitere Aufgabe abgenommen, sodass sie sich jetzt wieder auf andere Projekte konzentrieren können.

High-Tech-Hersteller setzt auf PKI für Geräteidentitätsprüfung, VPN-Zugriff und Zero-Trust-Umgebung für kritische Assets

Ein Anbieter von Energiesparlösungen sicherte seine Umgebung mithilfe der integrierten Funktionen der Microsoft-Active Directory-Zertifikatdienste-Umgebung und durch die Vorgabe, dass verwaltete Geräte anhand von Gerätezertifikaten und über die PKI-Infrastruktur des Unternehmens validiert werden müssen. Das Ziel bestand darin, den Zugriff auf geschäftskritische Ressourcen zu beschränken. Dazu wurde eine Methode entwickelt, um Benutzer zu authentifizieren, die per VPN auf die Unternehmensumgebung zugreifen möchten, und die Integrität von verwalteten Geräten zu prüfen, bevor ihnen der Zugang zu privaten Netzwerkressourcen gewährt wird. Die Benutzer sollten jederzeit und überall sichere Verbindungen herstellen können und schnelleren Zugriff auf die Firmenressourcen erhalten. Der Einsatz von digitalen Zertifikaten ermöglicht eine strenge Mitarbeiterkontrolle, da der Zugriff auf geschützte Ressourcen nur über einen vollständig verwalteten Endpunkt erfolgen kann. Für Vertragsparteien und Geschäftspartner können Authentifizierungszertifikate ausgestellt werden, um den Zugriff zu beschränken, und nach Bedarf können Firewallregeln festgelegt werden.

„Unser Sicherheitssystem basiert in erster Linie darauf, das Auslesen von Schlüsseln von Microsoft-Geräten so schwer wie möglich zu gestalten“, sagte der CISO des Unternehmens. Außerdem fügte er hinzu, dass der Hersteller eine gestaffelte Investition in eine Zero-Trust-Umgebung vornehme. Die Durchführung dieses Unterfangens wird dabei durch ein kontinuierliches Rollout von Mac-Computern erschwert, die für Techniker, für die Marketingabteilung und für andere spezielle Anwendungsfälle im Unternehmensnetzwerk eingeführt werden. In Zusammenarbeit mit einem PKI-Experten entwickelt das Unternehmen eine Methode, um Authentifizierungszertifikate auf den Macs bereitzustellen und dafür zu sorgen, dass der private Schlüssel sicher gespeichert wird und nicht exportiert werden kann.

Im Laufe des Rollouts werden neu ausgestellten Zertifikaten Metadaten hinzugefügt, damit das Unternehmen die Funktion des Device Fingerprinting einführen kann. Auch bei der Authentifizierung und der Herstellung von VPN-Verbindungen auf der lokalen Webzugriffsmanagement-Plattform sollen künftig Zertifikate genutzt werden. Dem Unternehmen gefällt die Flexibilität der Plattform, die den Mitarbeitern ermöglicht, über ihre Mobilgeräte auf ein Portal mit Office 365 und anderen Firmenressourcen zuzugreifen.

Der leitende Sicherheitsarchitekt des Unternehmens rät beim Thema zertifikatbasierte Authentifizierung auf Mobilgeräten zur Vorsicht. „Nur weil wir in der Lage sind, ein Zertifikat auf einem Gerät zu speichern, heißt das nicht automatisch, dass jede Komponente auf diesem Gerät mit dem Zertifikat interagieren kann. Wenn der Entwickler die Anwendung nicht dazu programmiert hat, ein allgemein auf einem Gerät bereitgestelltes Zertifikat zu nutzen, wird dies auch nicht geschehen.“ Die Anwendung kann das Zertifikat von dem Gerät, auf dem es sich befindet, möglicherweise nicht abrufen. Deshalb arbeitet das Unternehmen an einer neuen Strategie mit einer Cloud-Identitätsfunktion, die selbst entwickelte Anwendungen und Anwendungen von Drittanbietern unterstützt, die von den Mitarbeitern eingesetzt werden.

Unternehmen nutzt digitale Zertifikate für Mobilitätsstrategie und Mitarbeiterfernzugriff

Eine globale Firma, die Prüfungen elektronischer Geräte durchführt, setzt eine Kombination aus Benutzer- und Gerätezertifikaten ein, um Benutzern über vom Unternehmen ausgegebene und private Laptops und Mobilgeräte Zugriff auf vertrauliche Ressourcen zu geben. Das Ergebnis ist eine hohe Mitarbeiterbindung und eine innovative Technikabteilung. So drückt es der CISO aus, der stolz auf den

starken Sicherheitsstatus des Unternehmens und den flexiblen Arbeitskomfort ist, den die Mitarbeiter genießen. Beides wird durch digitale Zertifikate ermöglicht.

„Unsere Wahl fiel auf Zertifikate, da sie für eine Vielzahl unserer Anwendungsfälle die beste Lösung darstellen und unsere Geschäftspartner und die Benutzer, per Mobilgerätemanagement für BYOD, für den VPN-Zugriff Zertifikate verwenden“, so der CISO.

Der mühsamste Teil bei der PKI-Einrichtung ist die Installation von Vertrauensketten mit Berührungspunkten zwischen allen Clients. Interoperabilität zwischen den unterschiedlichen PKI-Implementierungen gibt es nicht, da weder die Entwickler- und Technikerteams noch die Marketing- und Vertriebsabteilungen des Unternehmens daran interessiert sind, die Möglichkeiten in dieser Hinsicht zu prüfen. Die Betriebsabläufe richten sich für jede Implementierung nach einer eigenen Vertrauenskette, obwohl ein einheitlicher Ansatz möglicherweise effizienter und kostengünstiger wäre, da in dem Fall nur eine einzige Vertrauenskette benötigt wird.

Da das Unternehmen sich bemüht, einen hohen Sicherheitsstatus zu wahren, ist die PKI-Implementierung für den Mobilgeräte- und VPN-Zugriff fast vollständig für Zertifikatsprofile auf Seiten von Microsoft eingerichtet. Um das Risiko von Zertifikatsdiebstählen und Brute-Force-Angriffen zu verringern, die darauf abzielen, Zugriff auf geschäftskritische Ressourcen zu erlangen, entwickelte das Unternehmen eine eigene Zertifikatligatur. Wenn sich die Benutzer anmelden, wird statt einer Zertifikatabfrage lediglich eine Passwortabfrage angezeigt. Dadurch können Zertifikate nur von individuellen Anwendern verwendet werden. Diese 1-zu-1-Beziehung sorgt dafür, dass ein Zertifikat niemals zusammen mit einem Passwort verwendet werden kann. „Das ist meiner Meinung nach eine essenzielle Sicherheitskomponente bei der Bereitstellung von Zertifikaten“, so der CISO.

Zahlungsabwickler sichert Tausende POS-Geräte mit PKI

Herstellerunternehmen stehen immer mehr unter dem Druck, IoT-Geräte mit hardware- und softwarebasierten Sicherheitsverfahren auszustatten, um Unterstützung für Verschlüsselung, Authentifizierung und Autorisierung zu ermöglichen und die Integrität von Firmware, Betriebssystemen und Anwendungen auf Geräten zu überprüfen. Digitale Zertifikate sind die Vertrauensanker, mit denen dieses grundlegende Sicherheitsniveau in eingebetteten Systemen erreicht wird.

Ein Zahlungsabwickler in Europa sichert Zehntausende POS-Systemgeräte mithilfe eines Managed PKI-Service, der eine zuverlässige gegenseitige Drittanbieterauthentifizierung zwischen Geräten und Netzwerken ermöglicht. Der neu entwickelte Ansatz des Unternehmens erfordert die Installation digitaler Zertifikate für die Geräteidentität und einen Geräte-Agent, der mit der cloudbasierten Plattform des Zahlungsabwicklers kommunizieren kann. Diese wird zur Bereitstellung, Überwachung und Verwaltung der POS-Systeme sowie zur Schaffung eines sicheren Mechanismus für die Zertifikatrotation eingesetzt.

Laut einem Sicherheitsarchitekt, der die Implementierung beaufsichtigt, reduziert der Einsatz von digitalen Zertifikaten betrügerische Handlungen auf Herstellerebene und bietet seinem Unternehmen einen größeren Einblick in die Gerätenutzung. „Unsere Wahl fiel auf PKI, weil wir dadurch die Möglichkeit erhalten, eine große Anzahl von Zertifikaten über ihren gesamten Lebenszyklus zu verwalten. Ein wichtige Voraussetzung war eine Lösung, die nicht durch den Einsatz von gefälschten digitalen Zertifikaten von Angreifern übernommen werden kann“, erklärte der Sicherheitsarchitekt. Der entwickelte Mechanismus gewährleistet, dass inaktive Daten oder Daten bei der Übertragung geschützt sind, und prüft die Echtheit der beim Senden und Empfangen von Informationen beteiligten Entitäten.

Neben der Überwachung von Gerätebereitstellung und Zugangsdatenverwaltung über die POS-Systeme ermöglicht die Lösung dem Anbieter, richtlinienbasierte Verschlüsselungsservices zu verkaufen und sicherzustellen,dass die Händler ihren Compliance-Verpflichtungen nachkommen.

Für andere vom Anbieter eingesetzte Geräte, die ein hohes Risiko darstellen, ist ein Agent-Ansatz unmöglich. Die Produkte eines Herstellers von eingebetteten Systemen, der mit dem Zahlungsabwickler und anderen Anbietern zusammenarbeitet, bieten nicht die nötige Kapazität oder Leistung zur Unterstützung eines Agents oder einer Clientsoftware. Der Hersteller teilte IDC mit, dass seine Techniker PKI verwenden, wenn die Produktion eine sichere automatisierte Kommunikation und Code Signing erfordert. „Unsere Kunden baten uns, ein Verfahren aufzustellen, das die Integrität jeder ausgelieferten Software sicherstellt“, erzählt der Leiter des Sicherheitsteams, der mit der Technikabteilung zusammenarbeitete. Anstatt eine Lösung in die bestehende PKI-Implementierung des Herstellers einzubauen, sollte dafür Managed PKI verwendet werden.

„Wir suchten nach einer Möglichkeit, um den Prozess zu automatisieren, ohne das Team zu belasten, das für unsere internen Vorgänge zuständig ist.“

DIE VORTEILE VON DIGICERT

DigiCert ist ein Anbieter von digitalen High Assurance-Zertifikaten, der es sich zur Aufgabe gemacht hat, SSL/TLS-, PKI-, Identitäts-, Authentifizierungs- und Verschlüsselungslösungen für das Internet und das Internet of Things zu vereinfachen. DigiCert unterstützt die automatisierte Erstellung von Zertifikatprofilen mit flexiblen Konfigurationsmöglichkeiten und Anmeldungsmethoden sowie eine Wiederherstellung mit sicherer Schlüsselhinterlegung für Email Security. Zertifikate werden dazu genutzt, die Integrität von E-Mail-Inhalten zu bestätigen, die Privatsphäre zu schützen und die Autoren wichtiger Nachrichten zu verifizieren. Außerdem werden Zertifikate häufig für digitale Signaturen eingesetzt, um die Integrität von Rechtsdokumenten, Verträgen und Rechnungen zu wahren, die für die geschäftliche Entwicklung und Business Continuity unabdingbar sind.

Darüber hinaus bietet die DigiCert-Plattform IT-Administratoren ein zentrales Management-Framework für einen sicheren standortunabhängigen Systemzugriff. Die Plattform wird in der Regel zur Authentifizierung von Mitarbeitern in Anwendungen und auf Websites verwendet und bietet Unternehmen die Flexibilität, eigene Zertifikatprofile und Anmeldungsmechanismen zu entwickeln, die sichere VPN- und Netzwerkverbindungen sowie Mobilität mit hoher Geschwindigkeit und Skalierbarkeit ermöglichen. Sie kann außerdem Schutz für Mobilgeräte, mobile E-Mail-Programme und Anwendungen bieten, einschließlich der zugehörigen Daten. Dadurch können Administratoren die Anmeldung und die Zertifikatausstellung automatisieren, um den Zugriff auf Unternehmensdienste zu steuern, den Datenschutz zu überwachen und Anwendungsbeschränkungen zu verwalten. DigiCert PKI Platform bietet IoT-Unterstützung, damit Unternehmen eine große Anzahl vernetzter Geräte bereitstellen und Zertifikate mithilfe eines PKI-Clouddienstes verwalten können, der die sichere Speicherung und Verwaltung von Zertifikatsschlüsseln ermöglicht.

HERAUSFORDERUNGEN/CHANCEN

Unternehmen haben jahrelang in ihre bestehende PKI-Infrastruktur investiert. Laut den Sicherheitsexperten, mit denen IDC gesprochen hat, ist die Optimierung und Automatisierung der oft komplexen und unzusammenhängenden PKI-Umgebungen, mit deren Pflege sie beauftragt sind, ein vielschichtiges und mehrjähriges Unterfangen. Zu den Voraussetzungen gehören Vorabinvestitionen und

PKI-Spezialisten, die die bestehenden Geschäftsprozesse des Unternehmens, die IT-Infrastruktur und den Standort geschäftskritischer Ressourcen kennen und mit der Risikotoleranz und Wachstumsstrategie der Unternehmensführung vertraut sind. Rasantes Wachstum, Fusionen und Übernahmen, die Einführung neuer Technologien, Änderungen der Geschäftsstrategie und andere externe Faktoren können erhebliche Auswirkungen auf ein Optimierungsprojekt haben, wenn es nicht sorgfältig geplant und systematisch ausgeführt wird.

FAZIT

Der Trend zur Cloud hält an, und viele Unternehmen setzen für die Verwaltung des Zugriffs auf Daten und andere Firmenressourcen auf hybride und Multicloud-Umgebungen. Für die Validierung der Integrität von geschäftlichen Transaktionen und die Herstellung einer sicheren, zuverlässigen Verbindung zwischen Anwendern und Systemen spielt die PKI-Technologie deshalb eine immer zentralere Rolle. Dies wird durch die Ergebnisse der IDC-Studie *Data Services for Hybrid Cloud* bestätigt. 2010 gaben 32 % der Unternehmen mit mehr als 10.000 Mitarbeitern an, PKI im Rahmen ihrer Sicherheitsprogramme einzusetzen. 2018 gaben 65 % der Großunternehmen an, eine umfassende, robuste Implementierung für alle relevanten Datenspeicher und Ressourcen zu nutzen. Warum PKI an Bedeutung gewonnen hat, lässt sich auf folgende zentrale Faktoren zurückführen:

- **Skalierbarkeit:** Die für diese Studie befragten Personen gaben an, PKI in einem erheblichen Umfang zu nutzen, und stellten uns Daten zur Größe ihrer Anwenderbasis, zur Anzahl der Domains und zur Menge der Authentifizierungsanfragen zur Verfügung. Die entsprechenden IT-Abteilungen mussten erhebliche Skalierungsanforderungen erfüllen. Alle Studienteilnehmer, aus Unternehmen mit 1.000 bis 120.000 Mitarbeitern, äußerten ihre Zufriedenheit mit der Performance und der Funktionsfähigkeit und waren im Hinblick auf die Entwicklung des Unternehmens zuversichtlich, dass die PKI-Technologie die künftigen Anforderungen in den Bereichen Mobilität, Fernzugriff, sichere WLAN-Verbindungen, Dokumentensignierung, Verschlüsselung und sichere E-Mails erfüllen würde.
- **Managed PKI-Services:** Vorhandene Probleme und Bedenken wurden dem Einsatz mehrerer PKI-Implementierungen zugeschrieben. Zur Bewältigung der daraus entstandenen Komplexität fehlt es zudem an qualifizierten Netzwerk- und Sicherheitstechnikern. Dieser Umstand treibt die Einführung von Managed PKI-Services voran, mit denen die Arbeit der vorhandenen Mitarbeiter unterstützt und Unterbrechungen im Betriebsablauf verhindert werden sollen, indem häufige PKI-Aktivitäten wie das Onboarding neuer Mitarbeiter und das Ausstellen und Widerrufen von Zertifikaten automatisiert werden.
- **Raffinierte Angriffe:** Teilnehmer der Studie gaben an, dass IT-Abteilungen häufig abgeneigt sind, Änderungen an bestehenden PKI-Implementierungen vorzunehmen, solange keine schwerwiegenden Fehler vorliegen. Zunehmende Komplexität und ein Mangel an proaktiver Kontrolle führen jedoch unweigerlich zu Konfigurationsproblemen und Sicherheitslücken, die durch Angreifer ausgenutzt werden können. Schwachstellen in der Konfiguration können für Man-in-the-Middle-Angriffe missbraucht werden, bei denen einzelne Mitarbeiter ausspioniert oder, dies ist das wahrscheinlichere Szenario, vertrauliche Daten gestohlen werden. In beiden Fällen versuchen die Angreifer, einen finanziellen Gewinn zu erzielen.

Den Ergebnissen dieser IDC-Studie zufolge spielt PKI in verschiedenen Geschäftsszenarien und Anwendungsfällen eine entscheidende Rolle bei der Sicherung der Digitalisierungsinitiativen. Moderne Geschäftsprozesse können durch den Einsatz von PKI unterstützt werden, um die Automatisierung zu erhöhen, Unstimmigkeiten abzubauen und die Verarbeitung digitaler Informationen und elektronischer Transaktionen zu optimieren. Außerdem ist PKI ein unverzichtbares Element für Sicherheitsteams,

wenn sich relevante Datenschutz- und Datensicherheitsbestimmungen ändern. CISOs sind sich einig, dass Komplexitäten durch optimierte PKI-Implementierungen reduziert und Verwaltungsaufwand und -kosten durch die Inanspruchnahme von Managed PKI-Services gesenkt werden können, sodass sich das Sicherheitspersonal anderen dringenden Aufgaben zuwenden kann. Die Studie konnte bestätigen, dass digitale Zertifikate wichtige Komponenten darstellen, mit denen sich gezielte Angriffe vereiteln lassen und dazu beitragen, die Integrität sicherheitsrelevanter Transaktionen sicherzustellen und die Identität der an geschäftlichen Transaktionen beteiligten Parteien zu überprüfen. Darüber hinaus wurde festgestellt, dass PKI neue Geschäftsprojekte fördern kann, mit denen die Zufriedenheit der Kunden verbessert werden soll, indem ihnen ermöglicht wird, Transaktionen mit vertraulichen Daten bequem von zu Hause durchzuführen.

Über IDC

Die International Data Corporation (IDC) ist ein weltweit führender Anbieter von Marktinformationen, Beratungsdienstleistungen und Events für die Märkte Informationstechnologie, Telekommunikation und Verbrauchertechnologie. IDC hilft IT-Experten, Managern und der Investment Community, faktenbasierte Entscheidungen über Technologiekäufe und Geschäftsstrategien zu treffen. Mehr als 1.100 IDC-Analysten bieten globale, regionale und lokale Expertise über Technologie- und Branchenchancen und -trends in über 110 Ländern weltweit. Seit 50 Jahren bietet IDC strategische Einblicke, die unseren Kunden helfen, ihre wichtigsten Unternehmensziele zu erreichen. IDC ist eine Tochtergesellschaft von IDG, dem weltweit führenden Technologieunternehmen für Medien, Marktforschung und Events.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com