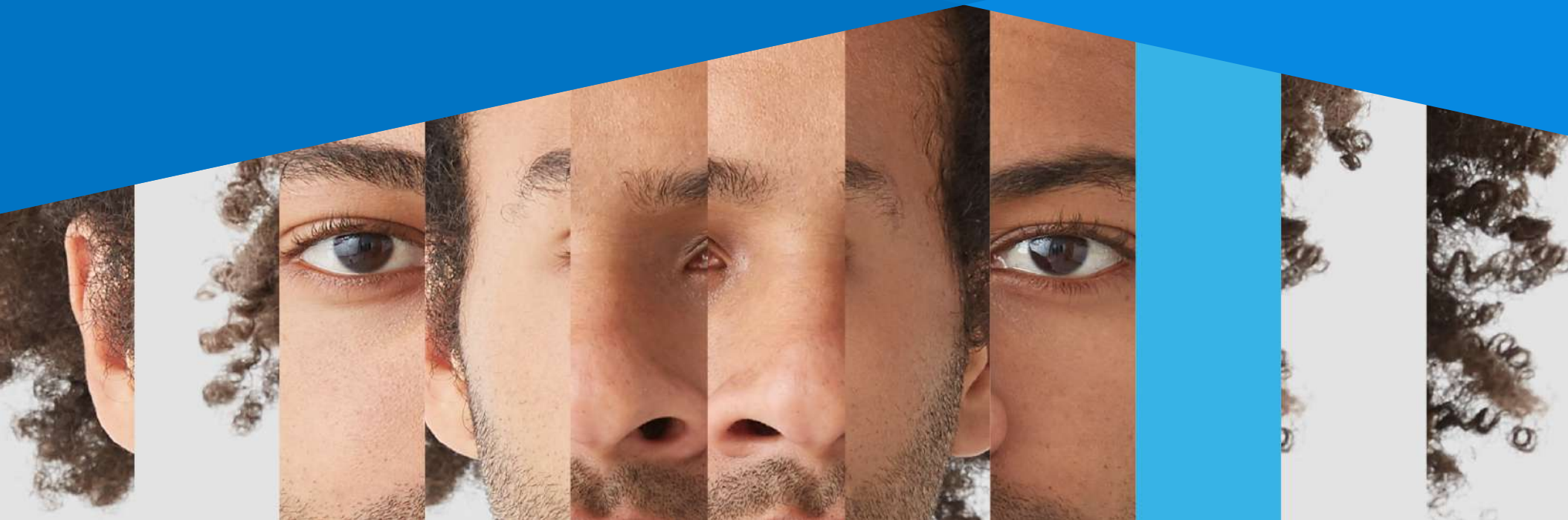
E-Book

digicert®

10 TIPPS ZUM SCHUTZ IHRER MARKE, IHRER KUNDEN UND IHRES RUFES



digicert®

Wenn Verschlüsselung die Grundlage Ihrer Sicherheit ist, ist Identität ihr Herzstück – oder eher das menschliche Gesicht Ihrer digitalen Marke. Seit Beginn des E-Commerce in den 1990ern bilden Vertrauen und zuverlässige Identität die Basis eines ehrlichen geschäftlichen Austauschs.

Heute aber verstecken sich oftmals auch Websites mit schädlichem Inhalt hinter Verschlüsselung. Diese weit verbreitete Anonymität gefährdet die Identität von Unternehmen, leitet Verbraucher in die Irre und lässt sie dann alleine mit ihrer Unsicherheit. Außerdem kann eine fehlende Identitätsprüfung von Benutzern, Anwendungen und Geräten in Ihrem Netzwerk Hackern den Zugriff erleichtern und für eine Publicity sorgen, die keine Organisation gebrauchen kann.

Mit den Tools in diesem E-Book können Sie die Identität Ihres Unternehmens gegenüber Ihren Kunden nachweisen, die Legitimität Ihrer Website unter Beweis stellen und in Kundenvertrauen investieren.

Indem Sie nämlich die Identität Ihres Unternehmens authentisch beweisen und die Daten Ihrer Kunden sowie Ihre eigenen Daten schützen, stärken Sie Ihre vertrauensvolle Geschäftsbeziehung.

Sie sind Sie – Ihre Kunden sollen darauf vertrauen können.

INHALT

Phishing war 2019 an 78 % der Cyberspionage-Fälle beteiligt.*

Verizon Data Breach Investigations Report, 2019

*https://www.nextgov.com/cybersecurity/2019/05/cyber-espionage-targeting-public-sector-rose-168-2018/156849/

digicert®

SIE SIND SIE — IHRE KUNDEN SOLLEN DARAUF VERTRAUEN KÖNNEN

1. NUTZEN SIE TLS/SSL-ZERTIFIKATE, DIE IHRE IDENTITÄT BEWEISEN

1.1 DV vs. OV vs. EV

DV-Zertifikate (Domain Validation) bieten Verschlüsselung, aber keinerlei Validierung der Identität der Organisation. Viele Cyberkriminelle nutzen DV-Zertifikate, um rechtmäßige Websites zu fälschen. Auf diese Weise schädigen sie den guten Ruf der kopierten Identitäten. Daher sollten Organisationen ein stärkeres Authentifizierungsniveau wählen, um ihre Marke zu schützen.

Legitimieren Sie sich gegenüber Ihren Kunden mit TLS-Zertifikaten der Niveaus OV (Organization Validation) und EV (Extended Validation). Um diese starken TLS-Zertifikate zu erhalten, muss Ihr Unternehmen sich strikten Kontrollen unterwerfen und zusätzliche Nachweise beibringen, beispielsweise Ihren Namen und Standort. So haben Kunden die Garantie, dass Ihre Website authentisch ist.

EV-Zertifikate bieten das stärkste Niveau an Authentifizierung, Markenschutz und Anwenderschutz. Ihre bewährten Authentifizierungsmethoden gehen über die der Niveaus OV und DV hinaus. Um die EV-Anforderungen zu erfüllen, werden Zertifikate für Ihre Marke nur von dazu autorisierten Personen ausgegeben und alle Anträge sowie die Antragsteller müssen vollständig identifiziert werden – keine Chance also für Betrüger.

Bei führenden Unternehmen und Behörden gilt EV als empfohlener Standard für viele Branchen wie Finanzwesen und E-Commerce. Studien haben ergeben, dass Phishing-Versuche bei Einsatz von EV-Zertifikaten im Vergleich zu DV- und OV-Zertifikaten fast keine Rolle spielen[1].

Hoch sichere Zertifikate bieten nicht nur einen umfassenden Schutz der Website gegen gezielte Angriffe mit falscher Identität, sondern zeigen Ihren Kunden, dass nur Sie genau diejenigen sind, für die Sie sich ausgeben.

[1]Certified Phishing: Taking a Look at Public Key Certificates of Phishing Websites. (Vincent Drury und Ulrike Meyer, Fachgruppe Informatik an der RWTH Aachen)
*https://info.phishlabs.com/blog/more-than-half-of-phishing-sites-use-https

1. NUTZEN SIE TLS/SSL-ZERTIFIKATE, DIE IHRE IDENTITÄT BEWEISEN

1.2 ZUSÄTZLICHER IDENTITÄTSSCHUTZ UND VERTRAUEN IM FINANZSEKTOR

Aufgrund unterschiedlich vertrauenswürdiger Standards auf den Online-Finanzmärkten der EU wurde eIDAS (electronic IDentification, Authentication and trust Services) für Zahlungsdienstanbieter (Payment Service Providers, PSPs) eingeführt.

eIDAS senkt dank Standardisierung und höherer Sicherheit die bürokratischen Hürden in der Branche. Zwei der qualifizierten Zertifikate sind Qualified Web Authentication Certificates (QWAC) und Qualified eSeal Certificates (QsealC).

Mit einem QWAC wird die Identität des Anbieters gegenüber dem Kunden über die Website validiert und gleichzeitig werden sensible Zahlungsdaten verschlüsselt und geschützt. Die Authentifizierungs-Methoden für QWACs sind noch strikter als die für EV und erfordern die persönliche Identifikation eines autorisierten Vertreters der im Zertifikat genannten Organisation.

QsealCs bilden ein „Siegel“ auf Daten, sensiblen Dokumenten und anderen Mitteilungen und sorgen so für Manipulationssicherheit und den Nachweis der Herkunft aus vertrauenswürdiger Quelle.

Während die gesetzlichen Regelungen für PSPs von der jeweiligen geografischen Region abhängen, wurden diese Zertifikate im September 2019 mit dem Inkrafttreten der Zahlungsdiensterichtlinie für PSPs in der EU verpflichtend.

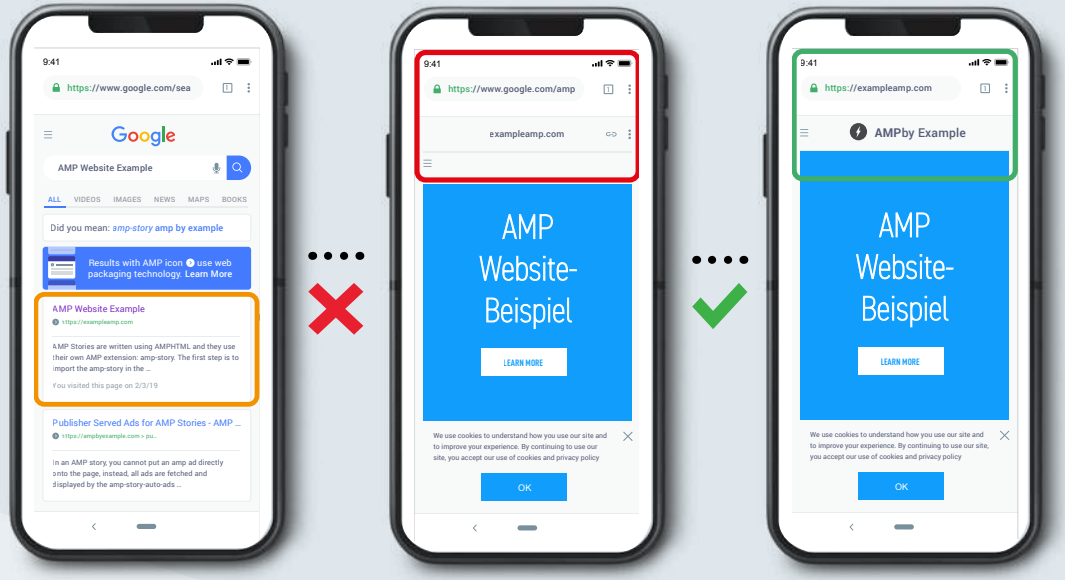
Die Absicherung von Transaktionen mit starken Zertifikaten und Siegeln signalisiert Ihren Kunden klar und offen, dass ihre Daten sicher bei Ihnen ankommen.

1. NUTZEN SIE TLS/SSL-ZERTIFIKATE, DIE IHRE IDENTITÄT BEWEISEN

1.3 SIGNED HTTP EXCHANGE (SXG)-ZERTIFIKATE

Wenn Ihr Geschäft darauf beruht, dass große Mengen Ihrer Web-Inhalte auf Mobilgeräten angezeigt werden, nutzen Sie möglicherweise Google AMP (Accelerated Mobile Pages) zur Beschleunigung der Ladezeiten. Dadurch sehen Ihre AMP-gehosteten Webseiten aber leider aus, als wären sie Eigentum von Google. Das führt nicht selten zu Verwirrung beim Kunden und trägt nichts zur Pflege Ihrer Marke bei.

DigiCert® SXG-Zertifikate korrigieren diesen Eindruck, sodass Ihr Firmenname ordnungsgemäß in der URL angezeigt wird, bei gleichzeitig kurzen Ladezeiten für gecachte Inhalte und unter Wahrung des gewünschten Sicherheitsniveaus.



Ohne DigiCert SXG-Zertifikat sieht es aus, als gehörten Ihre Marke und Inhalte zu Google.

Mit einem DigiCert SXG-Zertifikat präsentieren Sie Ihre Domain und Inhalte mit Ihrer URL und Ihrer Marke.

2. DEMONSTRIEREN SIE ÜBERALL IDENTITÄT: SIGNIEREN SIE IHREN CODE, SIGNIEREN SIE IHRE DOKUMENTE, VERSENDEN SIE GESICHERTE E-MAILS

Ihr Unternehmen wird auch anhand der E-Mails, Dokumente und Anwendungen identifiziert, die Sie versenden. Cyberkriminelle fangen solches Material gerne ab und spicken es mit ihrer Malware, sodass die Empfänger diese nun ihrerseits unbeabsichtigt verbreiten. Ihr Unternehmen erscheint dann aber nicht als Opfer, sondern als Quelle der Malware – das ist schlecht für Ihren Ruf und kann finanzielle Verluste bedeuten.

Mithilfe digitaler Zertifikate zum Signieren von Code und Anwendungen, Dokumenten und E-Mails garantieren Sie Ihren Kunden und Partnern, dass sie unverändertes Material erhalten. Wenn das Material manipuliert wurde, werden die Empfänger gewarnt und das Material wird nicht mehr mit Ihrem Unternehmen in Verbindung gebracht. So kann Ihre Identität nicht mehr zur Verbreitung von Malware missbraucht werden.

DigiCert Enterprise PKI (Public Key Infrastructure) Manager™ vereinfacht die Sicherheit sowohl der E-Mail-Kommunikation als auch der Dokumentsignierung. Mit flexiblen Konfigurationen für Zertifikatprofile und flexiblen Registrierungsmethoden gewährleisten Sie schnell den von Ihrem Unternehmen erwarteten Sicherheitsstatus. Dank der zugrunde liegenden DigiCert ONE™-Plattform verwalten Sie alles nach Ihren Wünschen – in der Cloud, On-Premises, im Hybrid-Modell oder auch lokal.

In 2017, wurden 76 % aller Unternehmen Opfer von Phishing-Angriffen.*

Wombat Security, 2017

01100011
01101111
01100100
01100101

*https://www.wombatsecurity.com/news/76-organizations-report-being-victims-phishing-attacks

3. GEBEN SIE ALLEN IHREN IoT-GERÄTEN EINE IDENTITÄT

Bis 2025 wird mit 75,44 Milliarden installierten IoT-Geräten gerechnet[3]. Bei der Nutzung des IoT durch Unternehmen gilt die Sicherheit als eines der Top-Themen. Es liegen bereits Berichte über Angriffe von Cyberkriminellen auf IoT-Geräte wie z. B. Sicherheitskameras vor.[4]

Durch die Implementierung von PKI und digitalen Zertifikaten können Hersteller auch ihren IoT-Geräten eine Identität verleihen. Dadurch können sie ihre Geräte nachverfolgen und die notwendigen System-Updates zur Gewährleistung der Sicherheit bereitstellen. Auch Interaktionen zwischen Geräten werden dadurch möglich, beispielsweise in Branchen wie der Autoindustrie. Außerdem kann die Interaktion mit unbekannten oder unberechtigten Geräten unterbunden oder eingeschränkt werden, wodurch das Risiko eines Cyberangriffs sinkt.

DigiCert IoT Device Manager™ ermöglicht die zentrale Einbindung zertifikatsbasierter Identität in Ihre IoT-Geräte und die Zuweisung, Definition und Kontrolle der verschlüsselungsbasierten Identität für jedes einzelne Gerät in Ihrem Netzwerk. Indem die Identität der Geräte als zusätzliche Sicherheitsebene bereits im Werk eingebaut wird, lässt sich das Risiko für Endanwender senken.

Die durchschnittlichen Kosten eines Datendiebstahls im Jahr 2020 liegen bei über 150 Mio. USD.*

Juniper Research, 2019

[3]https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
[4]https://www.propertycasualty360.com/2019/12/19/protecting-iot-devices-from-cyberattacks/?slreturn=20191119173130
*https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion-by-2019

4. STELLEN SIE EIN ECHTES SIEGEL AUF IHRE WEBSITE

Die Sicherheit bei Online-Bezahlungen liegt Kunden am Herzen. Dabei denken sie vor allem auch an die immer größer werdende Cyberkriminalität. 2017 gingen fast 20 % aller Abbrüche von Kaufvorgängen auf das Konto von Bedenken bei der Zahlungssicherheit[5]. Es ist also ausschlaggebend für Sie, Ihre Identität am Point of Sale sichtbar zu verteidigen.

Vertrauenssiegel gehören weiterhin zu den wichtigsten vertrauensbildenden Maßnahmen und sind ein wertvolles Zeichen starker TLS-Zertifikate. Tests haben eine Senkung der Absprungraten um 18 % und eine Zunahme der Konversionen um 19 % nach der Einführung von Vertrauenssiegeln auf Websites ergeben[6].

Zu allen DigiCert Secure Site™ TLS-Zertifikaten gehört das DigiCert Secured™-Siegel oder das Siegel „Norton Powered by DigiCert“. Damit sehen Ihre Kunden am kritischsten Punkt des Verkaufs einen gut wiedererkennbaren Sicherheitsfaktor – und können bei Zweifeln mit einem einzigen Klick die Vertrauenswürdigkeit Ihrer Website überprüfen.

DigiCert Vertrauenssiegel werden online zu den vertrauenswürdigsten gezählt.

Website Security Seal Study, 2018

[5]https://www.barilliance.com/10-reasons-shopping-cart-abandonment/
[6]https://www.digicert.com/site-seal-conversion-rate-benefits.htm

digicert®

SCHÜTZEN SIE SICH GEGEN UNBEABSICHTIGTE AUSSTELLUNG UND UNAUTORISIERTEN ZUGRIFF

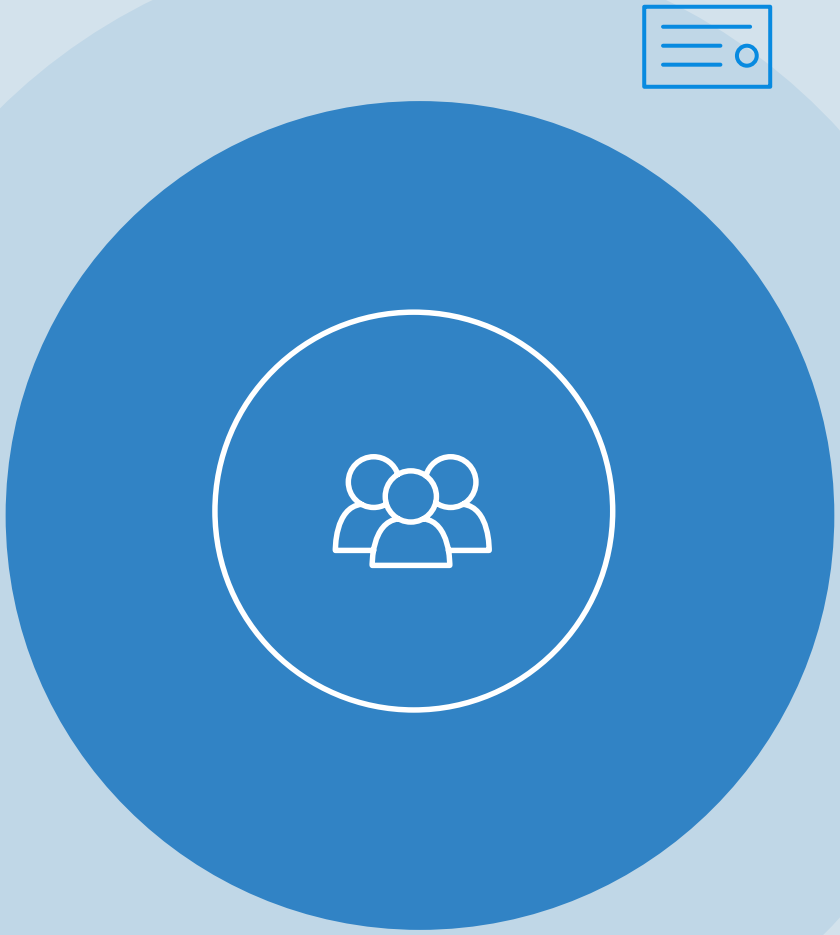
5. TREFFEN SIE MAßNAHMEN GEGEN DIE UNBEABSICHTIGTE AUSSTELLUNG VON ZERTIFIKATEN

5.1 EINTRAG IN EINE CERTIFICATE AUTHORITY AUTHORIZATION (CAA)-LISTE

Hacker – sowohl intern als auch extern – versuchen manchmal, sich ein vertrauenswürdiges Zertifikat mit dem Namen einer rechtmäßigen Domain von einer Zertifizierungsstelle (CA) zu erschleichen. Da solche Zertifikate von einer bekannten Stelle im Namen eines echten Unternehmens ausgegeben werden, haben Endanwender keinen Anlass, ihm zu misstrauen, sodass der Angreifer seine schädlichen Inhalte praktisch ganz offen platzieren kann. Dies ist besonders für größere Organisationen gefährlich, in denen ein einzelnes nichtkonformes Zertifikat möglicherweise nicht auffällt.

Um Domain-Eigentümer vor solchen Angriffen zu schützen, ist es seit 2017 für jede CA verpflichtend, vor der Ausstellung eines Zertifikats die Domain-CAA zu überprüfen.

CAA-Einträge sind eine „Whitelist“ vertrauenswürdiger CAs, die vom Eigentümer der Domain definiert wurde. Indem Sie Ihren CAA-Eintrag strikt kontrollieren und Zertifikate nur von CAs mit strengen Authentifizierungsstandards akzeptieren, können Sie verhindern, dass Angreifer sich nichtkonforme Zertifikate beschaffen und die Identität Ihres Unternehmens missbrauchen.



5. TREFFEN SIE MAßNAHMEN GEGEN DIE UNBEABSICHTIGTE AUSSTELLUNG VON ZERTIFIKATEN

5.2 ÜBERWACHUNG DER CT-LOGS (ZERTIFIKATSTRANSPARENZ-LOGS)

Ein CT-Log ist eine vorsortierte Liste von Zertifikaten, die es Unternehmen erlaubt, unrechtmäßig oder betrügerisch ausgestellte Zertifikate schnell zu erkennen.

Die Zertifikatstransparenz ermöglicht es dem Domain-Eigentümer, mit entsprechenden Überwachungs-Tools alle ausgestellten Zertifikate einzusehen und solche zu identifizieren, die unbeabsichtigt oder in betrügerischer Absicht ausgestellt wurden, und die Endanwender vor ihnen zu schützen.

Durch eine proaktive Überwachung der CT-Logs gelingt Ihnen das Auffinden solcher Zertifikate, die ohne Ihre ausdrückliche Genehmigung oder unter Umgehung Ihrer Domain-Richtlinien ausgestellt wurden, in wenigen Minuten, wo Sie sonst Tage oder gar Monate gebraucht hätten.

Ohne die Überwachung von CT-Logs entgehen Ihnen möglicherweise Zertifikate, die nicht den Sicherheitsrichtlinien Ihrer Organisation entsprechen, von nicht vertrauenswürdigen oder gar betrügerischen CAs ausgestellt wurden oder fehlerhaft installiert wurden, sodass sie die Sicherheit Ihrer wichtigsten Domains bedrohen.

6. PRÜFEN SIE AUF SPERRUNGEN

Bei einem Sicherheitsproblem auf einer Ihrer Websites verlieren Sie womöglich das Vertrauen Ihrer Kunden und riskieren, dass Ihre Domain von Suchmaschinen gesperrt wird. Vereinfachen Sie die Verwaltung Ihrer Zertifikate mit einem Blacklist-Checker und sorgen Sie dafür, dass Ihnen nicht entgeht, wenn Browser Ihrer Domain misstrauen.

*https://www-cdn.webroot.com/8415/0585/3084/Webroot_Quarterly_Threat_Trends_September_2017.pdf

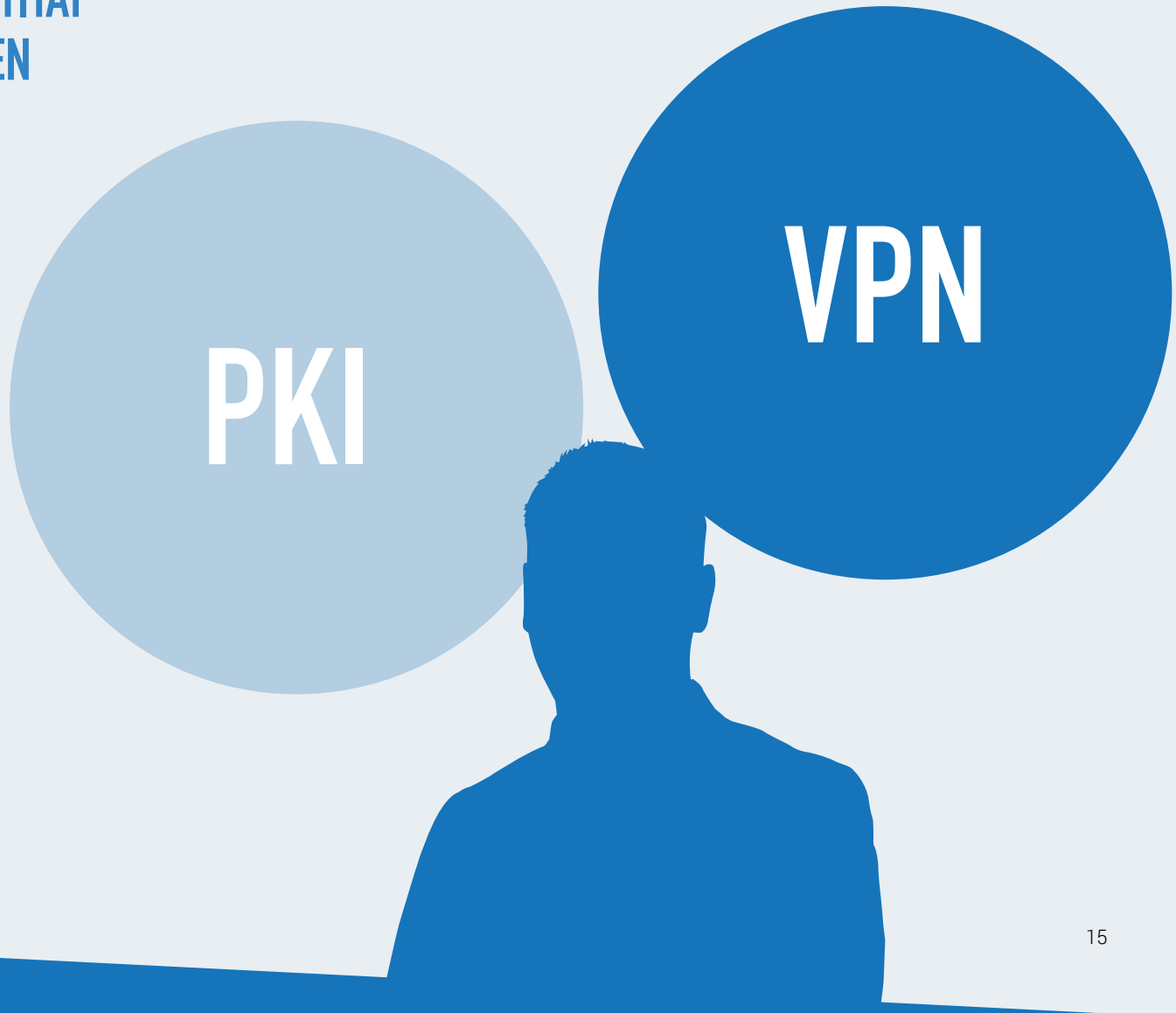
Jeden Monat erscheinen über 1 Millionen neue Phishing-Websites.*

Webroot Quarterly Threat Trends, 2017

7. VERIFIZIEREN SIE DIE IDENTITÄT VON BENUTZERN UND GERÄTEN

In einem Unternehmen greifen Mitarbeiter, Zulieferer und Partner mit den verschiedensten Geräten über Unternehmensnetzwerke und -anwendungen auf sensible Daten zu. Werden Benutzer und Geräte nicht ordentlich authentifiziert, kommt es schnell zu einer Sicherheitsverletzung, die zu Datenverlust und Rufschädigung führen kann.

Mithilfe einer Public Key Infrastructure (PKI) für Mobilgeräte, Zugang über VPN und Anmeldung per Smartcard sorgen Sie dafür, dass nur autorisierte Benutzer und Geräte auf die Informationen zugreifen, die Sie ihnen erlauben.



digicert®

EINFACHE VERWALTUNG

8. ERKENNEN UND AUTOMATISIEREN

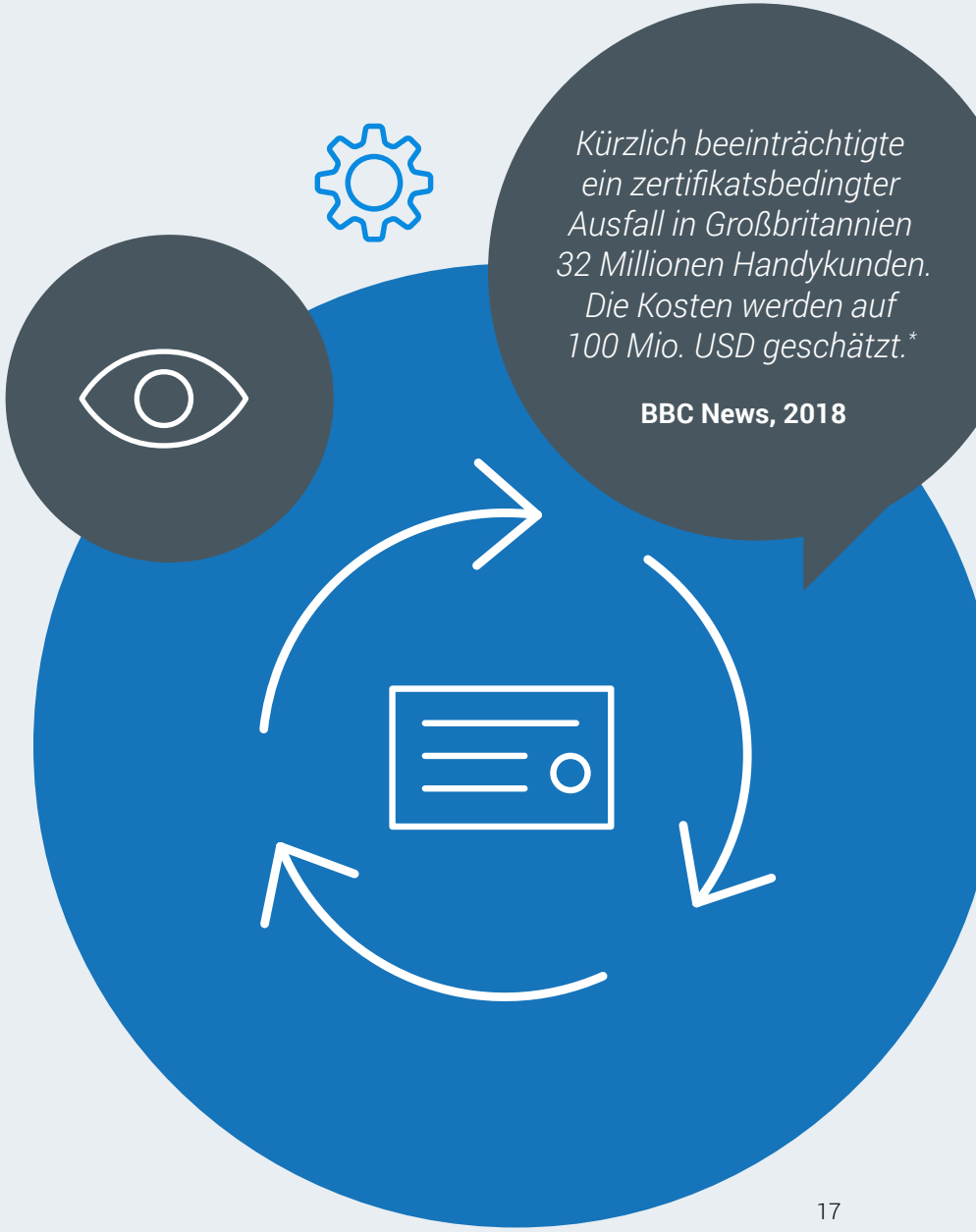
Fehlende Transparenz ist für viele Organisationen bei der Verwaltung ihrer Zertifikate eine der größten Herausforderungen. Und so wissen viele Unternehmen beim täglichen Betrieb nicht, ob alle ihre Zertifikate noch gültig sind. Dies ist einer der häufigsten Gründe für zertifikatsbedingte Ausfälle, die der Marke schaden können. Eine übersichtlichere Verwaltung der gesamten Abläufe ist daher notwendig.

DigiCert CertCentral® verfügt über Funktionen zur Zertifikatsuche und automatisierten Verwaltung. So können Sie Probleme und Schwachstellen im Zertifikat-Portfolio schnell erkennen und beheben Probleme anhand der Empfehlungen des Analyse-Tools. So haben Sie wieder den Überblick über Ihren gesamten Zertifikatsbestand und sofortige Kontrolle über problembehaftete Zertifikate.

Das ACME-Protokoll in CertCentral ermöglicht die automatische Implementierung von OV- und EV-Zertifikaten und sogar die Definition von Gültigkeitsdauern, und Sie haben dabei auf nur einem Bildschirm die Übersicht über den gesamten Lebenszyklus.

CertCentral ist Ihre Zentrale für die Ausstellung, Installation, Inspektion und Erneuerung von Zertifikaten sowie für die Problembehebung. Sie sparen viel zeitraubende manuelle Arbeit und hektische Schadensbegrenzungen und haben mehr Zeit für die Pflege Ihrer Marke unter dem Schutz gut organisierter Zertifikate.

*https://www.bbc.co.uk/news/business-46499366



9. VEREINFACHEN SIE DIE VERWALTUNG DIGITALER ZERTIFIKATE FÜR UNTERNEHMENS-IT

Viele Unternehmen verwalten ihre Zertifikate in einer hoch komplexen Umgebung. Aufgrund dieser Unsicherheit bevorzugen immer mehr Unternehmen die bewährte Sicherheit von PKI für den Schutz ihrer sensiblen Ressourcen.

Public Key Infrastructure (PKI) besteht aus Hardware, Software, Prozessen und Richtlinien, mit denen ein Unternehmen alle digitalen Zertifikate und öffentlichen Schlüssel erstellen und verwalten kann. Aber die Einrichtung oder bereits die Umsetzung einer PKI kann eine komplexe und schwierige Aufgabe sein.

Viele Unternehmen machen sich jedoch angesichts der heutigen modernen Infrastrukturen neue, agnostische Integrationstechniken zunutze. PKI-Plattformen vereinfachen die Lebenszyklus-Verwaltung und den Umgang der Endnutzer mit sicherer Kommunikation. Außerdem lassen sie sich nahtlos in Ihr Netzwerk und Ihre Geschäftsanwendungen integrieren und erweitern den Datenzugang erheblich.

DigiCert Enterprise PKI Manager, Teil von DigiCert ONE, ermöglicht mittleren und großen Unternehmen eine starke Authentifizierung und Verschlüsselung sowie sichere E-Mail-Kommunikation und digitale Signaturen mit hoher Leistungsstärke, Verfügbarkeit und Skalierbarkeit.

Die Plattform DigiCert ONE stellt PKI-Lösungen mit geringstmöglicher Komplexität und branchenweit führender Flexibilität im cloudbasierten, On-Premises, oder Hybrid-Modell zur Verfügung, je nach den Anforderungen Ihres Standorts oder Unternehmens.

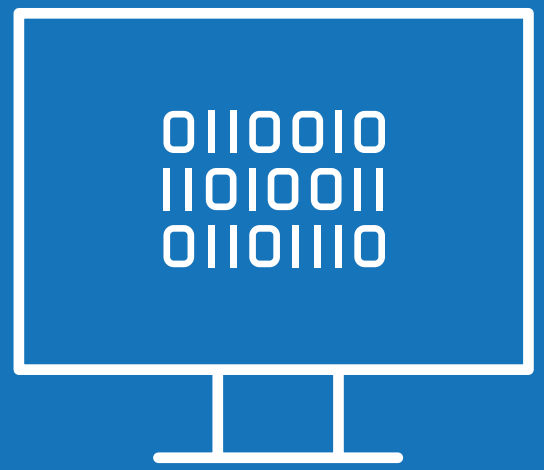
10. INTEGRIEREN SIE SICHERHEIT NAHTLOS IN DEVOPS UND BUSINESS-KOMMUNIKATION

Die bisher genannten Schritte bieten ausreichenden Schutz gegen die häufigsten Schwachstellen, die die Identität eines Unternehmens schädigen können. Viele Unternehmen, die sich den Compliance-Standards ihrer Branche unterwerfen und Best Practices für ein starkes Sicherheitsprofil befolgen, müssen jedoch erleben, dass sich dadurch die Produktentwicklung verlangsamt und die allgemeine Produktivität leidet.

Durch die Automatisierung von Sicherheitsfunktionen und deren Integration in den DevOps-Prozess bleibt Ihr Code oder Ihre App während der gesamten Entwicklung durch einen einfachen Mausklick kontinuierlich geschützt.

DigiCert Secure App Service™ (SAS) erleichtert Unternehmen die Integration von automatisierten, sicheren und leistungsstarken Code-Signing-Funktionen in den DevOps-Prozess. Die einfache Integration mit Continuous Integration/Continuous Delivery (CI/CD)-Plattformen und dem Cryptographic Service Provider™ (CSP) von DigiCert unterstützt die Automatisierung und erhöht die Kosteneffizienz.

Optionen für die Schlüsselverwaltung, rollenbasierte Zugriffsrechte und Audit-Logs erhöhen die Sicherheit und erleichtern die Kontrolle und Rückverfolgung. Zudem lassen sich mit Hash-basiertem Signing rasch große Volumina und Dateien signieren. All dies beruht auf dem Secure App Service von DigiCert, der es Unternehmen aller Größen erlaubt, beim Code-Signing zeitgemäße Sicherheit und Sorgfalt walten zu lassen.



KONTAKT

Weitere Informationen über die besten Lösungen für Ihre TLS-Investitionen erhalten Sie von unseren Experten per E-Mail:

contactus@digicert.com

Näheres zu IoT- und PKI-Management-Lösungen für Ihr gesamtes Unternehmensnetzwerk erfragen Sie hier:

pki_info@digicert.com