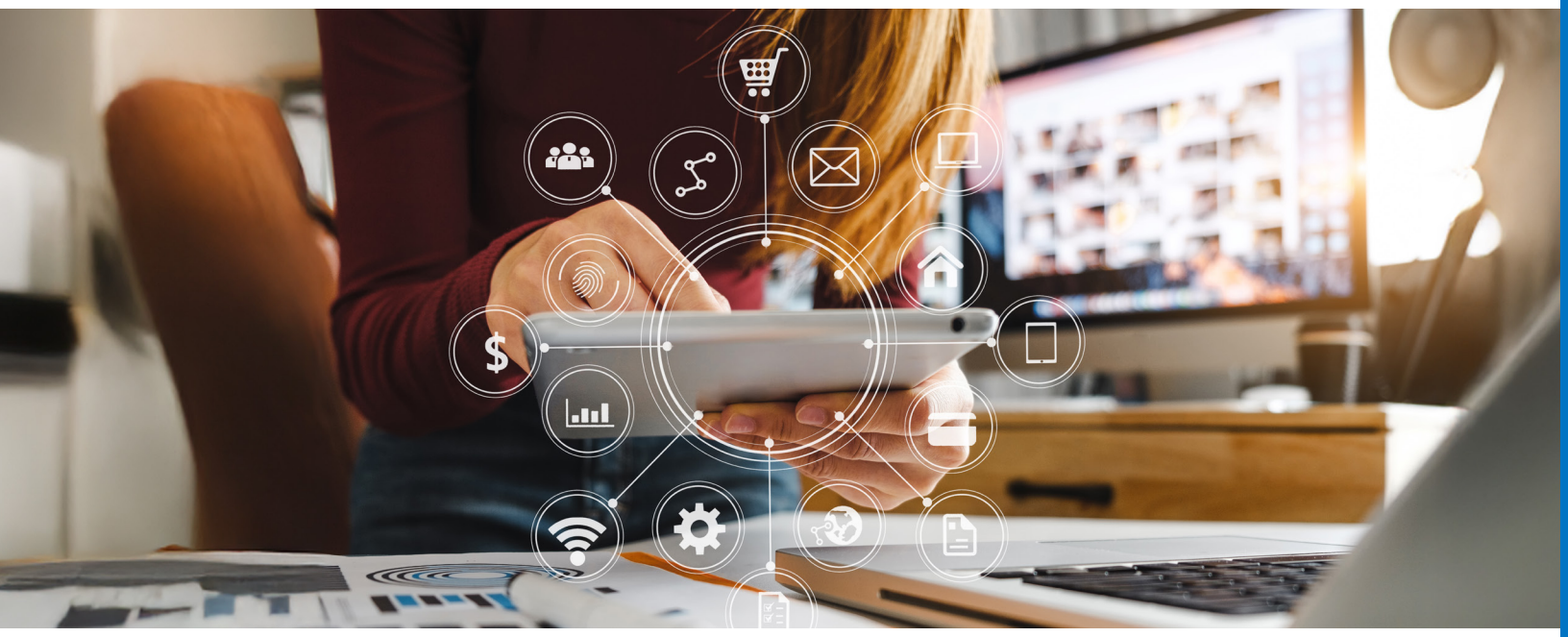
DigiCert Group

Einhaltung der EU-Verordnung DORA

DigiCert ONE Lösungen für Zuverlässigkeit und Sicherheit



digicert®

Januar 2025

WHITEPAPER

Einhaltung der EU-Verordnung DORA

DigiCert ONE Lösungen für Zuverlässigkeit und Sicherheit

Zusammenfassung

Finanzdienstleistungen sind die wahrscheinlich am stärksten regulierte Branche überhaupt. Von Sicherheitsstandards für Zahlungssysteme bis hin zu Vorgaben zur Bekämpfung von Geldwäsche gibt es unzählige Gründe, warum Finanzdienstleistungen ausgereifte Risikomanagementprogramme benötigen. Das Ziel der Verordnung über die digitale operationale Resilienz (Digital Operational Resilience Act, DORA) der Europäischen Union ist es, das Risikomanagement für Informations- und Kommunikationstechnologie im Finanzsektor zu vereinheitlichen. DORA gibt einen Rahmen für das Risikomanagement vor, darunter für die Überwachung, Meldepflichten für Vorfälle und die Weitergabe von Informationen. Die EU hat die Verordnung im Dezember 2022 eingeführt und sie tritt vollumfänglich am 17. Januar 2025 in Kraft.

Geltungsbereich

DORA betrifft einen Großteil der Finanzindustrie. Eine vollständige Liste aller betroffenen Unternehmenstypen ist in Artikel 2 Absatz 1 der Verordnung zu finden. Sie gilt auch für nicht klassische Finanzunternehmen wie jene, die mit Kryptowährungen handeln, sowie Drittanbieter von Informations- und Kommunikationstechnologie (IKT) und zugehörigen Dienstleistungen. Viele der enthaltenen Vorgaben werden bereits jetzt vielerorts von den Unternehmen umgesetzt, sei es aufgrund ihrer eigenen Compliance-Pflichten oder ihres Governance-Systems.

Ein allgemeiner Überblick über die DORA-Verordnung Regularien ist in Kapitel 1 Artikel 1 zu finden:

- Schaffung eines internen Governance- und Kontrollrahmens für das Management von IKT-Risiken
- Meldung schwerwiegender IKT-bezogener Vorfälle und freiwillige Meldung erheblicher Cyberbedrohungen an Behörden
- Meldung schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfälle (sowohl im IKT-Bereich als auch anderer Natur) an die zuständigen Behörden
- Umfassendes Testen von Sicherheitspraktiken und -kontrollen
- Austausch von Informationen im Zusammenhang mit Cyberbedrohungen und Schwachstellen
- Maßnahmen für das solide Management des IKT-Drittparteienrisikos

Auswirkungen

Angesichts dieses zusätzlichen Maßes an Aufsicht und potenziellen Geldbußen für Verstöße darf DORA beim Risikomanagement nicht außer Acht gelassen werden. So gibt beispielsweise Artikel 1 Absatz 1 vor, dass Unternehmen schwerwiegende zahlungsbezogene Betriebs- oder Sicherheitsvorfälle an die zuständigen Behörden melden müssen. Auch weniger schwerwiegende Zwischenfälle, von denen sich Unternehmen bisher im Stillen erholen konnten, müssen nun gemeldet werden, da sonst Geldbußen drohen. Das bedeutet, dass Risiken, die ein Unternehmen bisher vielleicht als akzeptabel erachtet hat, nun eine Lücke darstellen könnten, die umgehend geschlossen werden muss.

Nächste Schritte

Falls Ihr Unternehmen noch kein Risikomanagement-Framework wie ISO 27001 oder NIST 800-53 eingeführt haben sollte, wird es höchste Zeit. Für Unternehmen, die bereits über ein Framework verfügen, gilt: Prüfen Sie es auf Lücken, um Defizite zwischen Ihrem aktuellen Vorgehen und den von DORA geforderten Prozessen zu ermitteln. Erarbeiten Sie einen Plan, wie Sie diese Lücken schließen können, und beginnen Sie mit dessen Umsetzung. Dokumentieren Sie Ihren Prozess, damit Sie Ihren Plan und dessen Fortschritt schwarz auf weiß haben.

Risiken, die ein Geschäftsbereich bisher vielleicht akzeptiert hat, könnten nun aufgrund der Meldepflicht inakzeptabel sein. Prüfen Sie zuerst ältere Systeme und andere Ressourcen, die regelmäßig hohen Administrationsaufwand erfordern und instabil sind, auf Schwachstellen und nötige Upgrades.

DigiCert Lösungen

DigiCert arbeitet mit führenden Finanzinstitutionen weltweit zusammen, um die Sicherheit und Verfügbarkeit ihrer kritischen Systeme zu verbessern. Die DigiCert ONE Plattform, in die das umfassende Know-how von DigiCert hinsichtlich Public Key Infrastructure (PKI) und des Zertifikatslebenszyklus-Management einfließt, bietet folgende Vorteile:

- Prävention von Ausfällen aufgrund abgelaufener Zertifikate
- bessere Möglichkeiten der Behebung von Sicherheitsproblemen im Zusammenhang mit digitalen Zertifikaten
- automatisiertes Identitätsmanagement für Nutzer, Geräte und Maschinen für eine robustere Authentifizierung und sichere Kommunikation
- Schwachstellenmanagement für die von Ihrer Organisation entwickelten Software
- Schutz der Authentizität und Integrität von Software und Dokumenten

Artikel 1–3, Ausfälle und andere Vorfälle

Artikel 1 bis 3 der DORA-Verordnung enthalten Vorgaben zur Meldung von Sicherheitsvorfällen und Ausfällen mit Auswirkungen auf IKT- und Zahlungssysteme an die zuständigen Behörden. Achtung: Versäumnisse oder Fehler, die Zahlungssysteme betreffen, müssen nicht unbedingt mit IKT-bezogenen Vorfällen zusammenhängen. In Artikel 3 sind diese Vorfälle definiert:

- (8) „IKT-bezogener Vorfall" [ist] ein von dem Finanzunternehmen nicht geplantes Ereignis bzw. eine entsprechende Reihe verbundener Ereignisse, das bzw. die die Sicherheit der Netzwerk- und Informationssysteme beeinträchtigt und nachteilige Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder auf die vom Finanzunternehmen erbrachten Dienstleistungen hat
- (9) „zahlungsbezogener Betriebs- oder Sicherheitsvorfall" [ist] ein von den in Artikel 2 Absatz 1 Buchstaben a bis d aufgeführten Finanzunternehmen nicht geplantes Ereignis bzw. eine entsprechende Reihe verbundener Ereignisse, unabhängig davon, ob es sich um IKT-bezogene Vorfälle handelt oder nicht, das bzw. die nachteilige Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit zahlungsbezogener Daten oder auf die vom Finanzunternehmen bereitgestellten zahlungsbezogenen Dienste hat

Mit dem DigiCert Trust Lifecycle Manager können Unternehmen ein vollständiges Inventar ihrer digitalen Zertifikate erstellen und durch Automatisierung, Warnungen und Berichte Ausfälle und Sicherheitsvorfälle, die durch abgelaufene Zertifikate, Zertifikatswiderrufe und andere Notfalländerungen verursacht werden, frühzeitig erkennen.

Artikel 9, Schutz und Prävention

Artikel 9, Schutz und Prävention, gibt eine grobe Richtschnur für die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit von Daten bei der Verarbeitung, Übertragung und Speicherung vor. Finanzunternehmen jeder Größe nutzen Public Key Infrastructures (PKI), um eine starke Authentifizierung von Nutzern und Geräten und die Verschlüsselung dazwischen zu gewährleisten.

DigiCert Trust Lifecycle Manager kombiniert PKI as-a-Service, agnostisches Zertifikats-Lebenszyklus-Management und robuste Integrationen, um sichere Identitäten und Workloads über Nutzer, Clouds und On-Premises-Infrastrukturen hinweg zu untersützen.

Artikel 11, Reaktion und Wiederherstellung

Im Zusammenhang mit PKI gilt es auch, schnell auf problematische Zertifikate, Zertifikatsrevozierung und den seltenen, aber umso schwerwiegenderen Fall, dass einer öffentlichen Zertifizierungsstelle das Vertrauen entzogen wurde, zu reagieren.

Dank den zentralisierten Inventar- und Automatisierungsfunktionen des DigiCert Trust Lifecycle Manager können Unternehmen diese Probleme rasch isolieren, eindämmen und beheben – ohne den üblicherweise damit verbunden Arbeitsaufwand.

Artikel 25, Schwachstellenmanagement und Sicherheitstests

Einer der umfangreichsten Abschnitte von DORA ist Artikel 25 Absatz 1. Darin werden die unterschiedlichen Kategorien von Tests von IKT-Tools und -Systemen aufgeführt.

> …Durchführung angemessener Tests, wie etwa Schwachstellenbewertung und -scans, Open-Source-Analysen, Netzwerksicherheitsbewertungen, Lückenanalysen, Überprüfungen der physischen Sicherheit, Fragebögen und Scans von Softwarelösungen, Quellcodeprüfungen soweit durchführbar, szenariobasierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests und Penetrationstests.

Um all diese Testkategorien zu erfüllen, ist ein ganzes Sicherheitsprogramm vonnöten, das die physische und die digitale Infrastruktur umspannt. Ein interessanter Punkt sind die Verweise auf Softwarescans und Quellcodeprüfungen. Softwareentwicklungszyklen und -lieferketten unterliegen immer häufiger Branchen- und Behördenvorschriften und die dafür nötigen Maßnahmen gehen weit über herkömmliche Tools zum Testen der Anwendungssicherheit hinaus.

Der DigiCert Software Trust Manager vereint unternehmensweites Code Signing mit verschiedenen Softwarescantechniken, um die Code-Signing-Prozesse zu steuern und Softwarepakete auf kompromittierte oder anfällige Komponenten zu prüfen. Darüber hinaus umfasst die Lösung auch das Management von Code-Signing-Keys und Zertifikaten, die Analyse des Softwareaufbaus (Software Composition Analysis, SCA), eine Software-Stückliste (Software Bill of Materials, SBOM) sowie die Prüfung auf Bedrohungen – alles in einem regelbasierten Ansatz. Der Software Trust Manager lässt sich unkompliziert in Softwareentwicklungsprozesse und automatisierte CI/CD-Umgebungen integrieren, um das Risiko von Sicherheitsvorfällen in der Softwarelieferkette proaktiv zu senken.

Tools, Methoden, Prozesse und Richtlinien

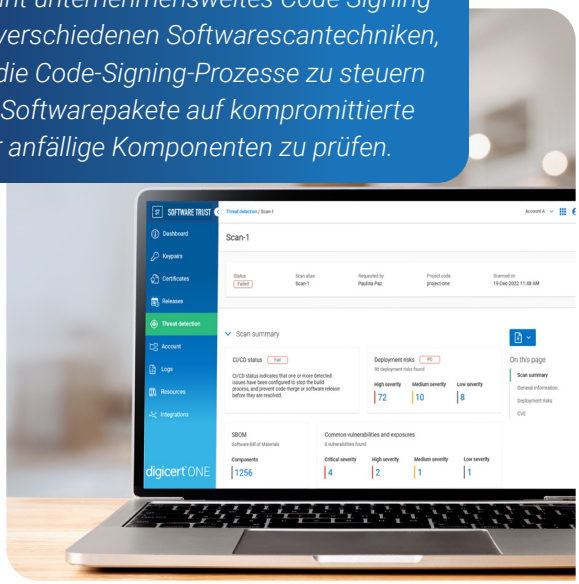
Die EU hat ergänzende Informationen zu den technischen und anderen Kontrollen herausgegeben, die zur Einhaltung der DORA-Verordnung erforderlich sind.

Verschlüsselung und Kryptografie

Daten bei der Speicherung, Übertragung und Verarbeitung zu verschlüsseln, ist in der Finanzindustrie nicht nur üblich sondern wird sogar erwartet. Ein Verschlüsselungssystem ist nur so stark wie das Management der zugehörigen kryptografischen Schlüssel. Deshalb fordern Artikel 6 und 7 der technischen Regulierungsstandards die Anwendung von Verschlüsselung, das Lebenszyklumanagment der Schlüssel sowie die Umsetzung aller relevanten Richtlinien.

Mit dem Trust Lifecycle Manager können Unternehmen Richtlinien zur unternehmensweiten Steuerung digitaler Zertifikate (z. B. Zertifikatsausstellung, -erneuerung und -revozierung) zentral durchsetzen. Dabei werden unterschiedliche Unternehmensbereiche nicht daran gehindert, Zertifikate dezentral zu besitzen und zu nutzen. Der Software Trust Manager, eine weitere Lösung der DigiCert ONE Plattform, kann Trust Lifecycle Manager um das Management von Code-Signing-Schlüsseln und Zugriffskontrollfunktionen ergänzen, die speziell für Softwareentwicklungsumgebungen konzipiert wurden.

Der DigiCert Software Trust Manager vereint unternehmensweites Code Signing mit verschiedenen Softwarescantechniken, um die Code-Signing-Prozesse zu steuern und Softwarepakete auf kompromittierte oder anfällige Komponenten zu prüfen.



Schwachstellen- und Patch-Management

Der Geltungsbereich von Schwachstellenmanagement-Programmen wird durch behördliche Vorgaben um den Softwareentwicklungszyklus erweitert. DORA ist eines der jüngeren Beispiele dafür. Artikel 10, Absatz 2d schreibt Unternehmen vor, dass:

- nachverfolgt wird, wie Folgendes verwendet wird:
  - Bibliotheken Dritter, einschließlich Open-Source-Bibliotheken, die für IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen genutzt werden;
  - IKT-Dienstleistungen, die das Finanzunternehmen selbst entwickelt hat oder von einem IKT-Drittdienstleister speziell für das Finanzunternehmen angepasst oder entwickelt wurden;

Die Anforderung, Softwarekomponenten von Drittanbietern zu dokumentieren, sowie die anderen Vorgaben dieses Abschnitts, wie das Patch-Management und die Offenlegung von Schwachstellen, lassen sich mit Software-Stücklisten (SBOMs), einer Software Composition Analysis (SCA) und dem Scannen der finalen Software-Builds auf Malware und bekannte Schwachstellen, die sich versehentlich oder absichtlich eingeschlichen haben, erfüllen.

Software Trust Manager vereint unternehmensweites Code Signing und Softwaresicherheitsprüfungen mit Zertifikatssignierung und Schlüsselverwaltung. Das Ergebnis ist ein regelbasierter Ansatz für die sichere Softwareentwicklung und Veröffentlichung. Die Integration des Software Trust Manager in Ihren Softwareentwicklungslebenszyklus (SDLC) und Ihre Pipelines für die Continuous Integration/Continuous Delivery (CI/CD) ermöglicht eine automatisierte Steuerung des Code Signings und die routinemäßige Schwachstellenevaluierung bei Software-Releases.

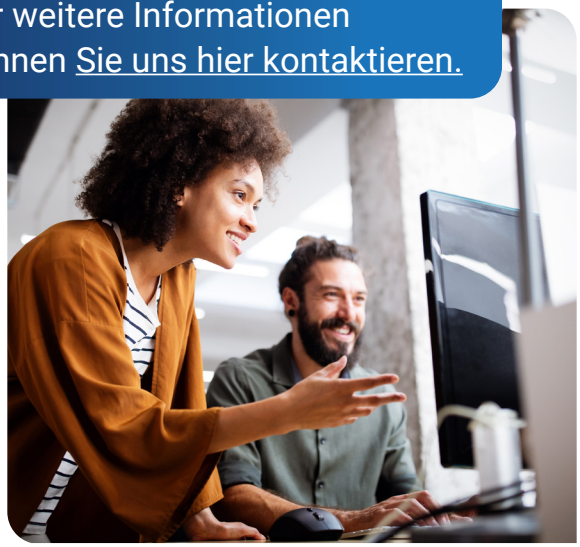
Fazit

Die DORA-Verordnung schreibt einen umfassenden Ansatz für Cybersicherheit und operationale Resilienz im Finanzsektor vor. Dazu gehören Anforderungen wie die Schaffung eines Risikomanagement-Frameworks und die Implementierung von Kontrollmechanismen für Prävention und Erkennung, die Meldung von Vorfällen sowie regelmäßige Tests der Sicherheitsmaßnahmen.

Wenn Finanzinstitute ihre PKI mithilfe der Lösungen von DigiCert modernisieren, profitieren sie mehrfach:

- Mehr Sicherheit: Implementierung einer starken Authentifizierung und Verschlüsselung zum Schutz sensibler Daten
- Bessere Resilienz: Schnelle Reaktion auf Risiken im Zusammenhang mit Cyberangriffen und betrieblichen Unterbrechungen
- Gestraffte Betriebsabläufe: Automatisierte Zertifikatsverwaltung und Softwaresicherheitsprozesse
- Gewährleistung der Compliance: Nachverfolgung der Einhaltung der DORA-Vorgaben durch Prüfprotokolle

Für weitere Informationen können Sie uns hier kontaktieren.



Technische Standards und Funktionsüberblick von DigiCert

Technischer Standard gemäß Verordnung	DigiCert Funktionen
Artikel 6 Verschlüsselung und kryptografische Kontrollen	
1. Als Teil ihrer IKT-Sicherheitsstrategien, -verfahren, -protokolle und -instrumente, gemäß Artikel 9 Absatz 2 der Verordnung (EU) 2022/2554, müssen die Finanzinstitute eine Strategie für die Verschlüsselung und kryptografische Kontrollen entwickeln, dokumentieren und entsprechend umsetzen.	Der Trust Lifecycle Manager ermöglicht die zentrale Überwachung und Durchsetzung von Verschlüsselungsrichtlinien bezogen auf digitale Zertifikate, welche zur Identifizierung von Nutzern und Geräten, zur Verschlüsselung von Daten bei der Übertragung sowie zur Erzeugung digitaler Signaturen verwendet werden.
Artikel 7 Management kryptografischer Schlüssel	
2. Um kryptografische Schlüssel während ihres gesamten Lebenszyklus vor Verlust, unbefugtem Zugriff, Offenlegung und Veränderung zu schützen müssen Finanzunternehmen entsprechende Kontrollmechanismen ermitteln und implementieren	Die Plattform DigiCert ONE nutzt Hardware-Sicherheitsmodule (HSM) für die Speicherung privater und geheimer Schlüssel. Der Software Trust Manager enthält beispielsweise ein cloudbasiertes HSM für die sichere Speicherung privater Code-Signing-Schlüssel.
3. Die Finanzunternehmen müssen Methoden entwickeln und implementieren, um die kryptografischen Schlüssel im Fall von Verlust, Kompromittierung oder Beschädigung auszutauschen.	Der Trust Lifecycle Manager und der Software Trust Manager bieten einen automatisierten Austausch von Zertifikaten sowie den zugehörigen Schlüsselpaaren, entweder mehrere gleichzeitig oder einzeln, auf Basis von Zeitintervallen, Kompromittierung oder einer anderen Logik.
4. Finanzunternehmen müssen ein Register aller Zertifikate und zertifikatspeichernden Vorrichtungen, zumindest für IKT-Anlagen die kritische oder wichtige Funktionen unterstützen, erstellen und führen. Dieses Register muss auf dem neuesten Stand sein.	Der Trust Lifecycle Manager bietet ein kontinuierliches Bestandsverzeichnis aller digitalen Zertifikate in Ihrem Unternehmen, unabhängig von der ausstellenden Zertifizierungsstelle. Das Tool nutzt verschiedene Methoden wie die direkte Integration in Schwachstellenmanagement-Plattformen und Drittanbieter-Zertifizierungsstellen (CA).
5. Finanzunternehmen müssen sicherstellen, dass die Zertifikate vor Ablauf unverzüglich erneuert werden.	Die Plattform DigiCert ONE automatisiert das Management Ihres Zertifikatslebenszyklus für zahlreiche Anwendungsbereiche, wie Infrastrukturen der Enterprise-Klasse, Software-Code-Signing, vernetzte Geräte, Nutzerauthentifizierung und das Signieren von Dokumenten.
Artikel 10 Schwachstellen- und Patch-Management	
1. Als Teil der in Artikel 9 Absatz 2 der Verordnung (EU) 2022/2554 genannten IKT-Sicherheitsstrategien, -verfahren, -protokolle und -instrumente, sind Finanzunternehmen dazu aufgefordert Verfahren für das Schwachstellenmanagement zu entwickeln, zu dokumentieren und zu implementieren.	Der Software Trust Manager bietet zwei Arten von Analysen, um potenzielle Probleme in der von Ihrem Unternehmen entwickelten Software, zu erkennen: Die Software Composition Analysis (kurz SCA), um Open-Source-Komponenten und Drittanbietersoftware zu erkennen und auf bekannte Bedrohungen zu prüfen. Statische Analysen von Binärdateien, um Schwachstellen, potenzielle Malware und offengelegte Secrets zu identifizieren. Beide Prozesse generieren eine Software-Stückliste (SBOM), die abgeglichen werden kann, um sicherzustellen, dass keine zusätzlichen Komponenten in den Softwareentwicklungszyklus eingeschleust wurden.

2 (a) Identifizierung und Aktualisierung relevanter und vertrauenswürdiger Informationsquellen, um ein Bewusstsein für Schwachstellen zu schaffen und aufrechtzuerhalten	DigiCert arbeitet mit Partnern zusammen, die Schwachstellen- und Malware-Datenbanken aktiv pflegen. Diese nutzen wir zur Prüfung auf Softwarebedrohungen und für die Benachrichtigung über neue Schwachstellen.
2(d) Nachverfolgung der Nutzung von: (i) Bibliotheken Dritter, einschließlich Open-Source-Bibliotheken, die von IKT-Diensten zur Unterstützung kritischer oder wichtiger Funktionen verwendet werden; (ii) IKT-Dienste, die vom Finanzinstitut selbst entwickelt oder von einem IKT-Drittdienstleister speziell für das Finanzinstitut angepasst oder entwickelt wurden; 2(e) Verfahren festlegen, um Schwachstellen gegenüber Kunden, Geschäftspartnern und der Öffentlichkeit verantwortungsbewusst offenzulegen;	Der Software Trust Manager erstellt eine Software-Stückliste (SBOM), um die Komponenten zu identifizieren, die Ihre Software enthält oder auf die sie verweist. Im Rahmen des Schwachstellenmanagement-Programms für die Software, die Ihr Unternehmen entwickelt, erkennt der gleiche Scanprozess auch bekannte Schwachstellen und potenziell gefährlichen Code. Der Software Trust Manager erstellt SBOMs, die Sie signieren und mit jedem Release veröffentlichen können, um das Schwachstellenmanagement zu unterstützen und Offenlegungspflichten zu erfüllen.
Artikel 12 Datenaufzeichnung	
2 (c) (iii) die Anforderung, Ereignisse im Zusammenhang mit allen folgenden Punkten zu protokollieren: Änderungsmanagement;	Die DigiCert ONE Plattform, den Trust Lifecycle Manager und Software Trust Manager beinhaltet, ermöglicht eine detaillierte Protokollierung und Benachrichtigung bei Ereignissen wie Zertifikatserneuerung, Schlüsselrotation, Signieren von Software und anderen sicherheitsrelevanten und administrativen Aktivitäten.
Artikel 13 Management der Netzwerksicherheit	
(d) Festlegung und Durchführung von Netzzugangskontrollen, um Verbindungen mit dem Netz des Finanzinstituts von nicht autorisierten Geräten oder Systemen oder von Endpunkten aus, die nicht den Sicherheitsanforderungen des Finanzinstituts entsprechen, zu verhindern und aufzudecken;	Der Trust Lifecycle Manager ist eng mit Endpoint-Management-Technologien wie Microsoft InTune und Infrastruktur-Management-Lösungen wie Terraform integriert, um das Management von Zertifikaten, welche zur Authentifizierung von Benutzern und Geräten in Unternehmensnetzwerken verwendet werden, zu automatisieren
((e) Verschlüsselung von Netzverbindungen über Unternehmensnetze, öffentliche Netze, nationale Netze, Netze Dritter und drahtlose Netze für die verwendeten Kommunikationsprotokolle unter Berücksichtigung der Ergebnisse der genehmigten Datenklassifizierung, der Ergebnisse der IKT-Risikobewertung und der Verschlüsselung von Netzverbindungen gemäß Artikel 6 Absatz 2;	Die Erkennungsfunktionen des Trust Lifecycle Manager sorgen dafür, dass Ihre Netzwerkendgeräte über gültige Zertifikate verfügen, um eine verschlüsselte Datenübertragung (TLS) zu gewährleisten.