SOLUTION NOTE

DIGITAL OPERATIONAL RESILIENCY ACT (DORA) UND DNS

Wie wendet man DNS Best Practices an, um DORA-Konformität zu erreichen

EINLEITUNG

Der Digital Operational Resiliency Act (DORA) ist eine EU-Verordnung, die darauf abzielt, die digitale Resilienz von Finanzinstituten zu stärken. Sie trat am 17. Januar 2025 in Kraft und stellt sicher, dass Banken, Versicherungsunternehmen, Investmentfirmen und andere Finanzinstitute Störungen im Bereich der Informations- und Kommunikationstechnologie (IKT), wie Cyberangriffen oder Systemausfällen, standhalten, darauf reagieren und sich davon erholen können.

DORA ist in neun Kapitel mit entsprechenden regulatorischen technischen Standards (RTS) gegliedert. Neben Banken und anderen traditionellen Finanzdienstleistern gelten die Verordnung und ihre Standards auch für weitere Unternehmen des Finanzsektors, wie z. B. Anbieter von Krypto-Asset-Diensten und Drittanbieter von IKT-Diensten. Laut PWC erstreckt sich die verpflichtende Einhaltung von DORA auf mehr als 22.000 Unternehmen,[1] da die Verordnung nicht nur für Unternehmen mit Sitz in der EU gilt, sondern auch für alle Finanzinstitute, die in der EU tätig sind oder Geschäfte abwickeln.

Artikel 1 von DORA legt die verschiedenen regulatorischen Standards fest, die sich auf die Sicherheit von Netzwerk- und Informationssystemen beziehen. Zu den behandelten Themen gehören Risikomanagement, Vorfallberichterstattung, Resilienztests, das Management von IKT-Drittrisiken und der Austausch von Informationen und Erkenntnissen über Cyberbedrohungen.[2]

Mit der Weiterentwicklung dieser Standards werden die spezifischen Anforderungen für Finanzunternehmen klarer. So bietet beispielsweise der *Abschlussbericht über den Entwurf von RTS, in dem Elemente im Zusammenhang mit bedrohungsgesteuerten Penetrationstests*[3] festgelegt sind, zusätzliche Klarheit über die Anforderungen an Penetrationstests. In dem Bericht wird erläutert, dass die DORA-Anforderungen mit anderen sicherheitsrelevanten Regulierungsinitiativen zusammenarbeiten werden, etwa das Threat Intelligence-Based Ethical Red-Teaming (TIBER-EU)-Framework, das mit der Europäischen Zentralbank verbunden ist. In dem Bericht heißt es: Der TIBER-EU-Rahmen kann den zuständigen Behörden und Finanzunternehmen auch dabei helfen, die Anforderungen für bedrohungsorientierte Penetrationstests im Rahmen des Digital Operational Resilience Act (DORA) zu erfüllen.[4] Der Bericht verweist auch auf das Dokument der Europäischen Zentralbank mit dem Titel *„Adopting TIBER-EU will help fulfil DORA requirements“*.[5]

WIE DNS BEI DER EINHALTUNG VON DORA HILFT

Das Domain Name System (DNS) spielt eine zentrale Rolle bei allen Netzwerkinteraktionen zwischen Geräten, Anwendungen, Internetdomänen, Datenbanken und Cloud-Ressourcen. Wenn das DNS-Protokoll strategisch verwaltet und bereitgestellt wird, dient es auch als proaktiver Durchsetzungspunkt für Netzwerksicherheit, als wertvolle Quelle für digitale Forensik und als effektiver Vermittler für eine schnelle Reaktion auf Vorfälle. DNS ist daher einzigartig positioniert, um Finanzinstitute bei der Durchführung einer Reihe von DORA-Compliance-Aktivitäten zu unterstützen, einschließlich:

- IKT-Risikomanagement (Kapitel II)
- Management, Klassifizierung und Meldung von IKT-bezogenen Vorfällen (Kapitel III)
- Test der digitalen betrieblichen Resilienz (Kapitel IV)
- Verwaltung von IKT-Drittrisiken (Kapitel V)
- Vereinbarungen zum Informationsaustausch (Kapitel VI)

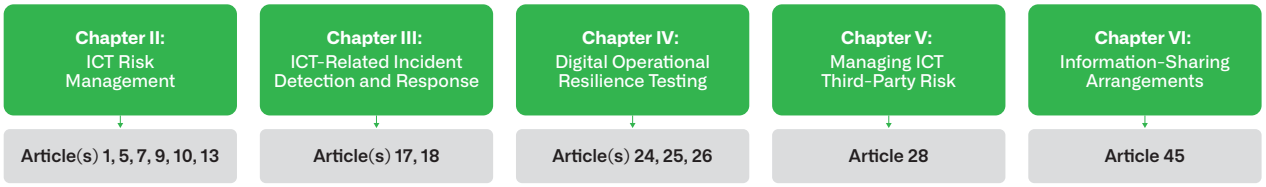

Abbildung 1. Wo DNS zu DORA-Compliance-Aktivitäten beiträgt

Es sollte beachtet werden, dass DNS neben der Übereinstimmung mit bestimmten DORA-Prinzipien so effizient ist, dass viele Unternehmen davon profitieren würden, seine Fähigkeiten zur Erfüllung der meisten Vorschriften einzusetzen. Da DNS bereits in Unternehmensnetzwerke integriert ist, bietet es eine praktischere und effizientere Möglichkeit, die Ausfallsicherheit und Sicherheit zu verbessern, als die Einführung völlig neuer Technologien und Kontrollen. Bei der Überlegung, wo DNS zu DORA-Aktivitäten beitragen kann, sollten die Entitäten das Verhältnismäßigkeitsprinzip gemäß Artikel 4 der Verordnung anwenden.

Die nachstehenden Empfehlungen sind nach den relevanten Kapiteln der DORA-Leitlinien gegliedert, zusammen mit Anmerkungen zu den spezifischen Artikeln der Verordnung, mit denen sie übereinstimmen.

IKT-RISIKOMANAGEMENT

Viele Finanzunternehmen betrachten DNS als „nur einen Teil der Netzwerk-Infrastruktur“, doch es ist entscheidend für die operative Resilienz, die DORA verbessern möchte. Ein DNS-Ausfall ist katastrophal, da er nahezu alle Anwendungen und Dienste eines Finanzinstituts beeinträchtigt. Daher sollten Unternehmen, die DORA einhalten, die Verfügbarkeit von DNS-Diensten ebenso in die Risikomanagementplanung einbeziehen wie andere Kernsysteme.[6] Ein Teil dieser Bemühungen umfasst die Anwendung branchenweit bewährter Verfahren bei der Implementierung und Verwaltung der internen DNS-Infrastruktur.

Da Finanzinstitute regelmäßig mit externen Unternehmen und Nutzern interagieren, muss der Sicherheitshygiene für externe DNS die gleiche Aufmerksamkeit gewidmet werden. Zu Compliance-Zwecken sollten Unternehmen sicherstellen, dass öffentliche (autoritative) DNS-Domains widerstandsfähig und sicher bleiben. Bedrohungsakteure zielen aktiv auf falsch konfigurierte autoritative Domains ab, die aufgrund lockerer Sicherheitsrichtlinien und -prozesse anfällig sind. Die externe DNS-Verwaltung kann auch Drittparteien einbeziehen, für die die Vorschriften weiterhin gelten. Daher sollten die für die Einhaltung von DORA Verantwortlichen das Risikomanagement und die Risikominderung der mit diesen Parteien verbundenen DNS-Dienste in Betracht ziehen.

Empfehlungen:

- Implementieren Sie belastbare DNS-Architekturen, die zur Unterstützung der Servicekontinuität konzipiert und für Spitzenkapazitäten ausgelegt sind, zusammen mit konsistenten Richtlinien und Verfahren zur Aufrechterhaltung der Verfügbarkeit und Sicherheit der DNS-Infrastruktur und des Dienstes. (Artikel 7, 9)
- Stellen Sie sicher, dass ein Teil der Organisation für die Verwaltung externer Domänennamen verantwortlich ist und als interne Registrierungsstelle fungiert, um zu vermeiden, dass unterschiedliche Teile der Organisation Domains über mehrere Anbieter registrieren und verwalten. (Artikel 5)
- Implementieren Sie Protective DNS-Dienste, um bösartigen DNS-Verkehr zu blockieren und zu protokollieren, zu verhindern, dass DNS für Datenexfiltration verwendet wird, anomalen Datenverkehr zu identifizieren und Daten für die Forensik und die Reaktion auf Vorfälle bereitzustellen. (Artikel 9, 10 und 13)

IKT-BEZOGENES VORFALLMANAGEMENT, KLASSIFIZIERUNG UND BERICHTERSTATTUNG

Sicherheitsexperten nutzen DNS während der Reaktion auf Sicherheitsvorfälle, um weitere bösartige Kommunikation zu identifizieren und zu blockieren sowie die Klassifizierung und den Umfang einer Kompromittierung zu unterstützen. Alle Netzwerkkommunikationen beginnen mit einer DNS-Abfrage, wodurch die Protokolle, die Abfrage- und Antwortdaten sowie DHCP-Protokolle und Asset-Informationen enthalten, für das Vorfallmanagement von entscheidender Bedeutung sind. Zum Beispiel ermöglicht der schnelle Zugriff auf Aufzeichnungen darüber, welche Geräte in einem Netzwerk möglicherweise mit einem bösartigen Host kommuniziert haben, Sicherheitsteams, das Ausmaß und die Klassifizierung eines Vorfalls zu bestimmen. Ähnlich identifizieren DHCP-Protokolle, welche IP-Adressen mit einem bestimmten Asset verknüpft wurden. Da die meisten Sicherheitsprotokolle Geräte anhand vorübergehender und nicht fester IP-Adressen identifizieren, sollten Unternehmen, die eine genaue und konsistente Ereignis- und Bedrohungskorrelation sicherstellen möchten, darauf achten, dass relevante gerätebezogene Daten und Kontexte mit Sicherheitsoperationstools geteilt werden können.

Empfehlungen:

- Protokollieren Sie kontinuierlich DNS-Anfrage- und Antwortdaten, DHCP-Lease-Aktivitäten und Bestandsdaten, um eine genaue Ereigniskorrelation zu ermöglichen und den Kontext für die Forensik als Teil des Vorfallmanagements bereitzustellen. (Artikel 17 Absatz 3, Artikel 18 Absatz 1)
- Implementieren Sie Protective DNS-Dienste als Kontrollpunkt zum Blockieren von bösartigem DNS-Verkehr. Dieser Kontrollpunkt sollte Bedrohungsinformationen zu den im Protective DNS-Dienst verwendeten Indikatoren enthalten, damit der Kontext des blockierten Datenverkehrs mit den Tools des Sicherheitsökosystems geteilt werden kann, um die Bewertung zu unterstützen. (Artikel 17)

DIGITAL OPERATIONAL RESILIENCE TESTING

Um den digitalen Resilienzstandard gemäß DORA zu erfüllen, sind zusätzliche Tests zur Geschäftskontinuität und Disaster Recovery (Artikel 24) sowie die Bewertung von Schwachstellen und Penetrationstests im Rahmen eines Rahmens der zuständigen Behörde (Artikel 25 und 26) erforderlich. Wie bei den Risikoüberlegungen sollten diejenigen, die die Einhaltung von DORA überwachen, die grundlegende Rolle, die DNS für die Netzwerkverfügbarkeit spielt, berücksichtigen. Beispielsweise können Unternehmen DNS nutzen, um die Geschäftskontinuität durch Global Server Load Balancing sicherzustellen. Im Bereich des Disaster Recovery kann ein DNS-Ausfall aufgrund eines Cyberangriffs, einer Fehlkonfiguration oder einer Naturkatastrophe den Geschäftsbetrieb zum Erliegen bringen. Daher ist es für Finanzinstitute unerlässlich, DNS und damit verbundene kritische Netzwerkdienste wie DHCP zu stärken, um die Anforderungen an die betriebliche Resilienz zu erfüllen.

Empfehlungen:

- Überprüfen Sie die interne und externe DNS-Architektur und -Dienste, um „Schwachstellen, Mängel und Lücken in der digitalen operativen Widerstandsfähigkeit zu identifizieren und umgehend Korrekturmaßnahmen zu ergreifen.“ Technische Standards wie NIST 800-81 können in dieser Hinsicht nützlich sein. (Artikel 24 Absatz 1)
- Achten Sie bei der Entwicklung eines umfassenden Testprogramms für die digitale operationale Resilienz darauf, dass es speziell DNS-Dienste, Infrastruktur und Protokolle abdeckt. Die Wiederherstellung von DNS-Diensten ist eine wesentliche Voraussetzung für die Wiederherstellung der Anwendungen und Dienste eines Unternehmens, und DNS selbst kann die Kontinuität der Dienste und das Disaster Recovery erleichtern. (Artikel 24 Absatz 1)
- Angesichts der Abhängigkeit eines Netzwerks von DNS sollten Sie sicherstellen, dass spezifische Testverfahren für DNS-Dienste und die Infrastruktur Teil des Gesamtplans für Resilienztests sind. (Artikel 24 Absatz 2)
- Wenn Sie die betriebliche Resilienz testen und mit externen Anbietern von bedrohungsgesteuerten Penetrationstests (TLPT) zusammenarbeiten, stellen Sie sicher, dass spezifische DNS-bezogene Tests zur Verfügbarkeit und Sicherheit durchgeführt werden. (Artikel 25, 26)
- Zu den wichtigsten Bereichen gehören:
    - » Die Überprüfung, ob die DNS-Resilienz wie vorgesehen funktioniert, insbesondere, ob es mehrere redundante Pfade für die Namensauflösung gibt.
    - » Die Sicherstellung, dass ausgehender DNS-Datenverkehr aus den Netzwerken eines Unternehmens über kontrollierte DNS-Resolver geleitet wird, die Abfrage- und Antwortdaten protokollieren.
    - » Die Abfrage nach Domainnamen, die mit der aktuellen bösartigen Aktivität in Verbindung stehen.
    - » Tests, ob es möglich ist, Daten über DNS-Anfragen zu exfiltrieren und Malware über DNS-Antworten einzuschleusen.
    - » Einführung von Verfahren und automatisierten Tools, die die DNS-Sicherheitshygiene berücksichtigen und etwa sicherstellen, dass verwaiste Domänennamen und falsche Delegationen von Subdomänen korrigiert werden.

VERWALTUNG VON IKT-DRITTANBIETERRISIKEN

DNS-Dienste, wie externe DNS, fallen in den Geltungsbereich von DORA, da sie möglicherweise von Dritten verwaltet werden. Darüber hinaus können sie auch DNS-Subdomains verwalten, die ihnen für bestimmte Dienste delegiert wurden.

Empfehlungen:

- Überprüfen Sie die Vereinbarungen mit Drittanbietern, die DNS-Dienste oder -Infrastrukturen (z. B. externe Domains) verwalten, um sicherzustellen, dass sie den Vorschriften und Richtlinien Ihres Unternehmens entsprechen und das gleiche Maß an betrieblicher Ausfallsicherheit und Sicherheit bieten. (Artikel 28)

VEREINBARUNGEN ZUM INFORMATIONSAUSTAUSCH

Finanzinstitute teilen regelmäßig Indikatoren für Kompromittierungen (IoCs) sowie Taktiken, Techniken und Verfahren (TTPs) mit vertrauenswürdigen Finanzdienstleistungsgemeinschaften, einschließlich geeigneter Schutzmaßnahmen zum Schutz sensibler Informationen. Innerhalb dieser vertrauenswürdigen Gruppen können Finanzinstitute DNS-Abfrage- und Antwortprotokolle sowie Informationen von gesperrten bösartigen Domains als Teil der Informationen nutzen, die sie austauschen.

Empfehlungen:

- Bereiten Sie sich auf den Informationsaustausch vor, indem Sie eine Richtlinie zur Bereitstellung von DNS-bezogenen IoCs implementieren. Die Vereinbarung von Datenformaten mit einer gemeinsamen Nutzungsgruppe im Voraus wäre betrieblich hilfreich, insbesondere wenn Indikatoren in operative Werkzeuge wie ein SIEM-System (Security Information and Event Management) eingespeist werden sollen. Insbesondere helfen Informationen über böswillige Aktivitäten, die durch Protective DNS-Dienste erfasst und weitergegeben werden, anderen Finanzunternehmen häufig dabei, den Netzwerkschutz zu verbessern. (Artikel 45)

VEREINFACHEN SIE DIE DORA-COMPLIANCE MIT INFOBLOX

Um die DORA-Konformität zu erreichen, sollten Finanzunternehmen ihre DNS-Dienste an den DORA-Prinzipien ausrichten, indem sie sich auf Resilienz und Sicherheit konzentrieren, um IKT-Risiken effektiv zu managen. Diese Ausrichtung umfasst die Verbesserung des Schutzes vor Bedrohungen wie Phishing und Datenexfiltration sowie die Einhaltung von Frameworks wie TIBER-EU und MITRE ATT&CK für Bedrohungsinformationen. Infoblox bietet maßgeschneiderte Lösungen zur Minderung dieser Risiken und zur Unterstützung der Einhaltung der Vorschriften zum IKT-Risikomanagement.

Darüber hinaus sind die robuste DNS-Infrastruktur und Sicherheitslösungen von Infoblox einzigartig positioniert, um Finanzunternehmen bei der Einhaltung der DORA-Grundsätze zu unterstützen. Infoblox konzentriert sich auf sichere und widerstandsfähige DNS-Dienste und hilft den DORA-Kunden, die Risiken zu minimieren, die mit einer nicht verwalteten DNS-Kommunikation verbunden sind, wie z.B. Phishing, Malware Command and Control und Datenexfiltration. Durch die Nutzung branchenführender Frameworks wie MITRE ATT&CK bietet Infoblox verwertbare Informationen und maßgeschneiderte Schadensbegrenzungsmaßnahmen, die den Anforderungen des IKT-Risikomanagements entsprechen. Darüber hinaus stellt die Expertise von Infoblox bei der Integration von Richtlinien von ENISA und NIST sicher, dass Finanzunternehmen Verfügbarkeits- und Sicherheitsverpflichtungen erfüllen und gleichzeitig komplexe regulatorische Rahmenbedingungen effektiv bewältigen.

---

1. Wie das Digital Operational Resilience Act Ihre Kontinuität unterstützt, PwC.
2. DORA Kapitel 1 Allgemeine Bestimmungen, Artikel 1(1) Gegenstand
3. endgültiger Bericht über den Entwurf einer RTS zur Festlegung von Elementen im Zusammenhang mit bedrohungsgesteuerten Penetrationstests (Referenz JC 2024 29), Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA), 07. Juli 2024.
4. Was ist TIBER-EU?, Europäische Zentralbank.
5. Die Einführung von TIBER-EU wird dazu beitragen, die DORA-Anforderungen zu erfüllen, Europäische Zentralbank, September 2024.
6. DORA-Verordnung „(22) ‚kritische oder wichtige Funktion' bezeichnet eine Funktion, deren Unterbrechung die finanzielle Leistungsfähigkeit eines Finanzunternehmens oder die Solidität oder Kontinuität seiner Dienstleistungen und Tätigkeiten wesentlich beeinträchtigen würde, oder deren Einstellung, mangelhafte oder fehlgeschlagene Ausführung die kontinuierliche Einhaltung der Bedingungen und Pflichten eines Finanzunternehmens, die mit seiner Zulassung verbunden sind, oder seiner sonstigen Pflichten nach geltendem Finanzdienstleistungsrecht wesentlich beeinträchtigen würde."

Firmenhauptsitz
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054, USA

+1.408.986.4000
www.infoblox.com/de

Version: 20250625v1