Was Sie über DORA wissen müssen: Ein Leitfaden zum Digital Operational Resilience Act

Barracuda

Der Digital Operational Resilience Act (DORA) ist eine Verordnung der Europäischen Union (EU), die am 17. Januar 2025 in Kraft tritt und die Stärkung der Cybersecurity im Finanzsektor zum Ziel hat.

Das Gesetz stellt einen entscheidenden Wandel dar beim Umgang der Öffentlichkeit und der Regulierungsbehörden mit Cybersecurity und Unternehmenstransparenz . Darin wird betont, dass es für Unternehmen notwendig ist, Cybersecurity ernst zu nehmen und dass ein offener Umgang mit Sicherheitsverletzungen das Leben für alle sicherer macht.

DORA beweist, dass der Finanzsektor zunehmend auf digitale Infrastrukturen angewiesen ist und unterstreicht, wie wichtig der Schutz dieser ist. Die Verordnung veranschaulicht Best Practices, die Unternehmen dazu verpflichten, effektive Schutzmaßnahmen einzuführen und Sicherheitsverletzungen sowie Ausfälle zu melden.

Das Gesetz trägt der Erkenntnis Rechnung, dass ein erfolgreicher Angriff auf die digitale Finanzinfrastruktur der gesamten Gesellschaft schaden könnte. Die Auswirkungen wären möglicherweise langanhaltend, und sich davon zu erholen bzw. den Schaden zu beheben würde Zeit und Geld kosten. Cyberkriminelle und staatlich finanzierte Akteure haben Zugang zu immer ausgefeilteren und stärker automatisierten Angriffs-Tools. Digitale Sicherheit ist keine Option mehr, sondern eine Notwendigkeit.

Dieses E-Book liefert einen Überblick über DORA, Best Practises zur Einhaltung der Compliance sowie eine Übersicht über weitere nützliche Informationsquellen.Sie erfahren außerdem, welche Barracuda-Ressourcen Ihnen bei der Umsetzung helfen können.

Für wen gilt DORA?

DORA gilt für die meisten Finanzinstitute, darunter:

- Banken, Versicherungen, Investmentfirmen und Kreditinstitute
- Zahlungsdienstleister und FinTech-Unternehmen
- Vermögensverwalter und Handelsplattformen

DORA umfasst im Wesentlichen alle im Finanzsektor tätigen Unternehmen, die Informations- und Kommunikationstechnologien nutzen, sowie deren kritische IKT-Drittdienstleister. Sie gilt nicht nur für Unternehmen innerhalb der EU, sondern auch für alle Unternehmen weltweit, die in diesem Gebiet tätig sind oder ebendort Kunden haben. Auch wenn britische Unternehmen, die keine EU-Kunden haben, die DORA-Richtlinien nicht einhalten müssen, wird von der britischen Regierung erwartet, ein eigenes Regelwerk zu schaffen, das wahrscheinlich weitgehend mit den europäischen Vorschriften übereinstimmen wird. Doch es geht hier nicht nur um die Einhaltung einer Verordnung. Folgt Ihr Unternehmen den DORA-Empfehlungen, bedeutet das, dass Sie moderne Best Practices anwenden.

Was sind die 5 Säulen der DORA-Verordnung?

Ziel von DORA ist die Stärkung der operationalen Resilienz von Finanzinstituten gegenüber Cyberangriffen und die Harmonisierung der Vorschriften innerhalb der EU. Die Verordnung stützt sich auf fünf Säulen:

Risikomanagement: Finanzinstitute müssen über ein effektives IT-Risikomanagement verfügen. Dazu gehören Maßnahmen zur Identifizierung, Bewertung und Minderung potenzieller Risiken im Zusammenhang mit ihren IT-Systemen, Cloudsystemen und Lieferantennetzwerken.

Testen der Resilienz: DORA legt fest, dass Sicherheitsmaßnahmen erst dann zuverlässig sind, wenn sie angemessen getestet worden sind. Finanzinstitute müssen über einen angemessenen Incident Response-Plan verfügen, sowie über Mitarbeiter, die wissen, wie er funktioniert. Die Institute müssen die Widerstandsfähigkeit ihrer digitalen Infrastruktur gegenüber Betriebsstörungen regelmäßig testen, z.B. mit Penetrationstests, Stresstests und Schwachstellenanalysen.

Meldung von Vorfällen: DORA schreibt die Durchführung umfassender Risikobewertungen und die Implementierung strenger Richtlinien zur Sicherheit von Informationssystemen vor. Dadurch wird ein proaktiver Ansatz zur Identifizierung und Minderung potenzieller Bedrohungen gewährleistet. Um gut vorbereitet zu sein, müssen Prozesse für die Incident Response etabliert, Simulationen durchgeführt und Ihre Mitarbeiter geschult werden.

Management von Drittparteienrisiken: DORA erfasst auch das Risiko von Angriffen auf die Lieferkette. Es verpflichtet Finanzinstitute dazu, Drittanbieter zu überwachen, insbesondere Anbieter wie Cloud-Computing-Unternehmen. Institute müssen einen schriftlichen Vertrag mit Dienstleistern abschließen. Diese Verträge müssen die in Artikel 30 von DORA angeführten Bestandteile enthalten. Dazu zählen eine schriftliche Beschreibung aller Dienstleistungen sowie gegebenenfalls Service Level Agreements.

Informationsaustausch: Die Verordnung zielt darauf ab, Meldepflichten innerhalb der EU zu harmonisieren und den Sicherheitsstatus im gesamten Sektor zu verbessern. Sie regt eine verstärkte Zusammenarbeit und einen intensiveren Informationsaustausch zwischen den Firmen an. Daraus ergibt sich die Pflicht, Vorfälle unverzüglich nach deren Auftreten zu melden. In der Vergangenheit wurde dies ad hoc und auf intransparente Art und Weise.

Einhaltung und Durchsetzung

Es mag vielleicht so klingen, als ob DORA keine radikale Abkehr von etablierten Best Practises darstellt. Das ist eine berechtigte Annahme. Doch der wesentliche Unterschied besteht darin, dass die DORA-Verordnung Institute tatsächlich dazu verpflichtet, auch nachzuweisen, dass sie auch tun, was getan werden sollte. Es gibt kein Zertifizierungsprogramm und keine Compliance-Tests, aber DORA wird für viele Unternehmen eine zusätzliche Last in puncto Governance und Dokumentation bedeuten. Für die Durchsetzung sind die drei bestehenden EU-Finanzaufsichtsbehörden zuständig — die European Supervisory Authorities.

Strafen

Es liegt im Ermessen der Regulierungsbehörden, Strafen gegen Unternehmen zu verhängen, die sich nicht an die Verordnung halten. Auch Mitgliedsstaaten können selbständig entscheiden, strafrechtliche Sanktionen zu verhängen.

DORA-Compliance: Was sind die ersten Schritte?

Zunächst müssen Sie feststellen, ob Ihr Unternehmen der DORA-Verordnung unterliegt. Wie bereits erwähnt, sollten Finanzinstitute, die nicht unter die Verordnung fallen, nichtsdestotrotz die in DORA angeführten angemessenen Best Practices zur Cybersecurity berücksichtigen. Wenn Ihre Wachstumspläne die Expansion in die EU oder Geschäfte mit Finanzinstituten, die in der EU tätig sind, beinhalten, ist es ratsam, jetzt auf die Einhaltung der Verordnung hinzuarbeiten. Müssen Sie die Richtlinien bis Januar vollständig erfüllen, gilt es schnell zu handeln und gegebenenfalls externe Hilfe in Anspruch zu nehmen. Falls Sie Dienstleistungen für EU-Unternehmen erbringen, die im Finanzdienstleistungssektor tätig sind, sollten Sie eng mit diesen zusammenarbeiten, um Ihre Strategien aufeinander abzustimmen.

In einem zweiten Schritt führen Sie eine Gap-Analyse durch, um zu ermitteln, wie ausgereift ihre Cybersecurity-Maßnahmen sind und wie nahe Ihre Systeme an die in der Verordnung geforderten Vorgaben herankommen. Sobald dieser Schritt abgeschlossen ist, können Sie sich daran machen, gegebenenfalls Lücken zu schließen und die erforderlichen Mitarbeiter, Prozesse und Technologien in Gang zu setzen.

Barracuda

Mehr erfahren

Die Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung bietet einen guten, auf Unternehmen ausgelegten Leitfaden für DORA. Und wenn Sie tiefer in die Materie eintauchen möchten, finden Sie hier den Verordnungstext (75-seitiges PDF).

Barracuda Networks kann Ihr Unternehmen dabei unterstützen, die Vorgaben aller fünf Säulen von DORA zu erfüllen. Unsere umfassende Palette an Cybersecurity-Tools trägt zur Verbesserung Ihres Sicherheitsstatus in allen Bereichen bei, von E-Mail über Web-Applikationen bis hin zur Netzwerksicherheit.

Wir verfügen über eine Fülle an Online -Ressourcen, die Ihnen bei der Umsetzung von DORA helfen, wie zum Beispiel die Nutzung von XDR, um Ihre Erkennung und Reaktion auf Bedrohungen zu verbessern sowie Argumente, wie Sie den Vorstand dazu bringen Cybersecurity-Strategien zu unterstützen.

Außerdem können wir Ihnen dabei helfen, Ihre Incident Response zu beschleunigen. Und Barracuda Security Insights unterstützt Sie bei der Bereitstellung der Active Intelligence, die Sie für Ihre Risikoanalyse brauchen.

Barracuda

Über Barracuda

Barracuda strebt danach, die Welt zu einem sichereren Ort zu machen. Wir glauben, dass jedes Unternehmen Zugang zu Cloud-First-Sicherheitslösungen auf Unternehmensniveau verdient hat, die einfach zu kaufen, zu implementieren und zu verwenden sind. Wir schützen E-Mails, Netzwerke, Daten und Anwendungen mit innovativen Lösungen, die mit unseren Kunden wachsen und sich anpassen. Mehr als 200.000 Organisationen weltweit vertrauen auf den Schutz durch Barracuda – auf eine Art und Weise, von der sie vielleicht nicht einmal wissen, dass sie gefährdet sind. Daher können sie sich darauf konzentrieren, ihr Unternehmen auf die nächste Stufe zu heben. Weitere Informationen dazu unter de.barracuda.com.

Barracuda