Conoscere il regolamento DORA: una guida al Decreto sulla resilienza operativa digitale

Barracuda

Il Digital Operational Resilience Act (DORA) è un regolamento dell'Unione Europea (UE) che entrerà in vigore il 17 gennaio 2025 e ha lo scopo di rafforzare la resilienza delle istituzioni finanziarie alla sicurezza informatica.

La nuova legislazione segna un cambiamento essenziale nel modo in cui il pubblico e le autorità di regolamentazione vedono la sicurezza informatica e la trasparenza aziendale. Riconosce che le aziende devono prendere sul serio la difesa e che essere aperti sulle violazioni mette al riparo tutti.

DORA ammette la crescente dipendenza del settore dei servizi finanziari dall'infrastruttura digitale e l'importanza di proteggere tale infrastruttura. Rappresenta le migliori pratiche, che richiedono alle aziende di stabilire prassi resilienti e segnalare violazioni ed errori.

La legislazione riflette la consapevolezza che un attacco all'infrastruttura finanziaria digitale andato a segno può causare danni a tutta la società. Gli effetti potrebbero essere di lunga durata e per il ripristino e la riparazione servirebbero tempo e denaro. I criminali informatici e gli attori sostenuti dagli stati hanno accesso a strumenti di attacco sempre più sofisticati e automatizzati. La sicurezza digitale non è più un optional, ma un obbligo per le aziende .

Questo e-book fornisce una panoramica su DORA, fonti da consultare per maggiori informazioni e informazioni sulle migliori pratiche richieste per la conformità. Identifica inoltre le risorse Barracuda che possono essere utili per prepararsi all'implementazione.

A chi si rivolge il regolamento DORA?

DORA si applica alla maggior parte degli istituti finanziari, tra cui:

- banche, compagnie di assicurazioni, società di investimento e istituti di credito
- Fornitori di servizi di pagamento e FinTech
- Gestori patrimoniali e piattaforme di trading

DORA copre essenzialmente tutte le entità operanti nel settore finanziario che utilizzano tecnologie e servizi di comunicazione, oltre ai relativi fornitori di servizi ICT critici di terze parti. Non riguarda solo le società all'interno dell'UE, ma anche aziende di tutto il mondo con attività o clienti in territorio europeo. Sebbene le aziende del Regno Unito senza clienti nell'UE non siano tenute a uniformarsi al regolamento DORA, si prevede che il governo del Regno Unito creerà un proprio quadro normativo, che probabilmente rispecchierà molto da vicino le normative europee. Ma oltre ad assicurare la conformità, garantire che l'organizzazione sia in linea con le raccomandazioni DORA significa seguire le migliori pratiche di oggi.

Quali sono i cinque componenti principali del regolamento DORA?

L'obiettivo generale di DORA è rafforzare la resilienza operativa degli istituti finanziari agli attacchi informatici e armonizzare le regole in tutta l'UE. Il regolamento è costituito da cinque componenti principali:

Gestione del rischio: gli istituti finanziari devono disporre di solide procedure di gestione del rischio IT, incluse prassi atte a identificare, valutare e contenere i potenziali rischi legati ai propri sistemi IT, sistemi cloud e reti della supply chain.

Test della resilienza: DORA ammette che nessuna misura di sicurezza è affidabile se non viene testata. Gli istituti finanziari devono disporre di un piano di risposta agli incidenti adeguato e di personale che ne conosca il funzionamento, oltre a testare periodicamente la solidità della propria infrastruttura digitale contro le interruzioni delle attività, ad esempio attraverso test di penetrazione, stress test e valutazioni delle vulnerabilità.

Segnalazione degli incidenti: eseguire valutazioni complete dei rischi e implementare politiche solide in materia di sicurezza dei sistemi informativi. Questo garantirà un approccio proattivo per identificare e contenere potenziali minacce. Occorre poi adottare procedure di risposta agli incidenti, eseguire simulazioni e formare il personale in modo che sia preparato.

Gestione del rischio di terze parti: DORA riconosce anche il pericolo di attacchi alla supply chain e richiede pertanto agli istituti finanziari di monitorare i fornitori di servizi di terze parti, in particolare fornitori quali le società di cloud computing. Gli istituti devono stipulare con i propri fornitori contratti scritti che vertano sugli argomenti riportati nell'Articolo 30 del regolamento, ad esempio disporre di una descrizione scritta di tutti i servizi forniti e, ove applicabile, degli impegni a livello di servizio.

Condivisione delle informazioni: il regolamento mira ad armonizzare gli obblighi di reporting all'interno dell'UE e a rafforzare la posizione di sicurezza dell'intero settore, favorendo una maggiore cooperazione e condivisione delle informazioni tra aziende. Ciò implica il dovere di segnalare gli incidenti sollecitamente dopo che si sono verificati. In passato le segnalazioni sono state fatte ad hoc e in maniera non trasparente.

Conformità e applicazione

Da questi presupposti potrebbe sembrare che DORA non si allontani radicalmente dalle migliori pratiche consolidate. In effetti è una deduzione corretta. Con DORA, tuttavia, la differenza è che le istituzioni dovranno dimostrare che stanno facendo quello che devono. Non esiste un unico test per la certificazione o la conformità, ma DORA aggiungerà un onere di governance e documentazione per molte aziende. La responsabilità della sua applicazione competerà alle tre autorità di regolamentazione finanziaria dell'UE esistenti: le autorità di vigilanza europee.

Sanzioni

Le autorità di regolamentazione hanno la facoltà di multare le organizzazioni che non rispettano il regolamento e gli Stati membri hanno anche la facoltà di imporre sanzioni penali.

Quali sono i primi passi da compiere per la conformità con DORA?

La prima attività da svolgere è stabilire se DORA si applichi all'azienda direttamente. Come accennato in precedenza, anche se non si applica direttamente, gli istituti finanziari dovrebbero prendere in considerazione il ragionevole insieme delle migliori pratiche in materia di sicurezza informatica previsto da DORA. Se i piani di crescita prevedono l'espansione nell'UE o la collaborazione con istituti finanziari che operano nell'UE, è consigliabile adoperarsi subito per arrivare alla conformità. Se è necessario raggiungere la piena conformità entro gennaio, bisognerà agire rapidamente e, se necessario, chiedere aiuto all'esterno. Se si forniscono servizi a società operanti nel settore dei servizi finanziari nell'UE, si dovrà collaborare strettamente per allineare le strategie.

Il secondo passo consiste nell'eseguire un'analisi delle lacune per misurare la maturità della posizione di sicurezza informatica e quanto i sistemi aziendali rispecchiano i requisiti espressi dal regolamento. Una volta terminato, si può iniziare a colmare le lacune e a prevedere chi incaricare, i processi e le tecnologie necessari.

Scopri di più

L'Autorità europea delle assicurazioni e delle pensioni aziendali o professionali offre una buona guida su DORA per le imprese. E per approfondire, questa è la legislazione attuale (PDF di 75 pagine).

Barracuda Networks può aiutare la tua organizzazione a uniformarsi a tutti e cinque i componenti principali del regolamento DORA. La nostra suite completa di strumenti di sicurezza informatica ci consente di rafforzarne la posizione di sicurezza in ogni area, dalla posta elettronica alle applicazioni web, fino alla sicurezza di rete.

Disponiamo di una vasta gamma di risorse online che possono esserti utili per affrontare le problematiche connesse a DORA, incluso l'uso di XDR per migliorare il rilevamento e la risposta alla gestione delle minacce e come convincere il consiglio di amministrazione a sostenere le strategie di sicurezza informatica.

Possiamo anche aiutarti a perfezionare la risposta agli incidenti. Infine, Barracuda Security Insights può essere utile per dotarsi dell'intelligenza attiva necessaria per potenziare l'analisi dei rischi.

Informazioni su Barracuda

Barracuda si adopera per rendere il mondo più sicuro. Crediamo che tutte le aziende meritino l'accesso a soluzioni di sicurezza di livello enterprise cloud-first, che siano semplici da acquistare, implementare e utilizzare. Proteggiamo l'e-mail, le reti, i dati e le applicazioni con soluzioni innovative espandibili e adattabili lungo il percorso dei clienti. Oltre 200.000 organizzazioni di tutto il mondo si affidano a Barracuda per essere protette in modi per cui non sanno nemmeno di essere a rischio, per potersi concentrare sulla propria attività e salire di livello. Ulteriori informazioni sono disponibili sul sito barracuda.com.