ANALISI DI AKAMAI

DORA (Digital Operational Resilience Act)

Preparazione degli enti finanziari per la conformità al DORA con Akamai

Il DORA (Digital Operational Resilience Act) è un nuovo tassello importante della legislazione europea che stabilisce normative più rigorose per gli enti finanziari regolamentati, richiedendo di migliorare il sistema di resilienza operativa non solo agli enti finanziari, ma anche ai loro fornitori di servizi ICT (Information and Communication Technology) di terze parti. Il DORA entrerà in vigore il 17 gennaio 2025.

L'ambito del DORA

Il DORA si applica agli enti finanziari a livello globale che operano nei mercati europei. Nell'ambito rientrano gli enti tradizionali, come banche, società di gestione degli investimenti e istituti di credito, e quelli non tradizionali, come i provider di servizi di criptovalute e le piattaforme di crowdfunding.

Inoltre, il DORA impone alcuni obblighi per gli enti non finanziari, che, di solito, sono esenti dalle normative di questo settore. Ad esempio, i provider di servizi di terze parti che forniscono servizi e sistemi ICT alle società finanziarie, come i data center e i provider di servizi cloud, devono soddisfare alcuni requisiti del DORA. Inoltre, il DORA si rivolge alle società che forniscono servizi di informazione di terze parti, come i servizi di rating del credito e i provider di servizi di analisi dei dati. I provider di servizi ICT di terze parti designati come critici dalle ESA (European Supervisory Authorities) verranno valutati da un supervisore nominato dalle ESA.

Akamai supporterà gli obiettivi degli enti finanziari e fornirà assistenza sia come terza parte che come vendor, aiutando a soddisfare i regimi previsti dai propri clienti. La nostra azienda si impegna nell'intento di collaborare con gli enti finanziari per fornire assistenza su eventuali richieste e aiutare a comprendere i modi con cui forniamo la resilienza operativa.

I 5 pilastri del DORA

L'approccio completo del DORA si basa su cinque pilastri fondamentali, ciascuno personalizzato in modo da soddisfare diversi aspetti della resilienza operativa digitale.

Gestione dei rischi	Segnalazione degli incidenti	Test sulla resilienza operativa digitale	Gestione dei rischi ICT di terze parti	Condivisione di informazioni e intelligence

Gestione dei rischi

- Una visibilità completa sulle performance dei servizi tramite Akamai Control Center (ACC) e i suoi dashboard integrati per l'analisi della sicurezza, il monitoraggio degli SLA e le informazioni sulla documentazione, inclusi rapporti e policy.
- Le valutazioni contrattuali della gestione dei rischi di terze parti, condotte su Akamai con cadenza annuale, offrono informazioni sulla sicurezza aziendale e valutano i rischi associati ai servizi.
- La soluzione Akamai Zero Trust e i prodotti di segmentazione aiutano i clienti a minimizzare e alleggerire i rischi correlati ai ransomware e alle minacce interne per l'elevazione degli accessi.
- Le verifiche continue della sicurezza di Akamai, condotte utilizzando gli standard di sicurezza di settore e locali, come il SOC 2, l'ISO 27001 o il BSI in Germania, offrono una migliore valutazione dei rischi aziendali.

Segnalazione degli incidenti

- Una copertura 24/7 con un sistema di notifiche per tutti gli incidenti che riguardano i clienti nei tempi previsti.
- Una copertura globale con un servizio di assistenza clienti e addetti alla sicurezza disponibili in più centri operativi in tutte le principali aree geografiche.
- Comunicazione di informazioni sugli incidenti tramite akamaistatus.com, servizi della community e ACC.

Akamai

Test sulla resilienza operativa digitale

- Modello di resilienza all'avanguardia, sottoposto a test per la resistenza ai più vasti attacchi DDoS mai osservati nel settore ICT.
- Test dell'infrastruttura organizzati con cadenza trimestrale e test semestrali sulla preparazione del personale per il recupero in caso di disastri.
- Lezioni continue apprese e miglioramenti implementati di anno in anno per garantire che il regime dei test di penetrazione interni e basati sulla conformità siano allineati con i test di penetrazione di terze parti TIBER-EU per la ricerca di eventuali minacce che valutano il modello di resilienza esistente.

Gestione dei rischi ICT di terze parti

- Akamai valuta tutti i suoi vendor e le terze parti prima di avviare il processo di onboarding e di utilizzare i loro servizi e le loro piattaforme. Tutti i vendor e i prodotti vengono sottoposti a specifici controlli sul servizio di sicurezza offerto, sulla modalità di elaborazione delle informazioni, sulla conformità con le leggi sulla privacy e se lo stato finanziario dell'azienda pone eventuali rischi per Akamai.
- Il team dedicato alla gestione dei rischi di terze parti (TPRM) garantisce che i vendor siano conformi da un punto di vista contrattuale con le regole per l'engagement con i vendor di Akamai. Tutti i vendor più importanti sono soggetti ad un monitoraggio della conformità con gli obblighi contrattuali ogni anno e, in caso di mancata conformità, sono previsti dei piani di uscita dal contratto.

Condivisione di informazioni e intelligence

- L'Akamai Security Intelligence Group conduce ricerche continue sulle minacce emergenti per i provider ICT e i clienti di Akamai. Una sofisticata rete di honeypot e intelligence, raccolta all'esterno dell'edge di Akamai distribuito a livello globale, viene usata per identificare gli indicatori di compromissione (IOC), che vengono poi condivisi tramite diversi canali di comunicazione.
- Akamai fa parte dell'FS-ISAC, la comunità di condivisione di intelligence, che contribuisce con case study e campioni di intelligence di TLP Green e Amber.

"Gli enti finanziari devono disporre di una struttura di gestione dei rischi ICT solida, completa e ben documentata come parte del sistema di gestione dei rischi complessivo per poter risolvere i rischi ICT in modo rapido, efficiente ed esauriente e per garantire un elevato livello di resilienza operativa digitale" (articolo 6).

Il sistema di resilienza operativa necessita di un'attenzione costante per salvaguardare le risorse di informazione e ICT dell'organizzazione, inclusa una continua protezione dei programmi software, delle apparecchiature fisiche e dei dati. Il sistema richiede aggiornamenti regolari, almeno annualmente, che vengono attivati in caso di incidenti ICT importanti, direttive di sorveglianza o informazioni ricavate dai processi di test o verifica.

Il contributo di Akamai

Akamai si allinea con gli obiettivi delle autorità preposte per garantire un dialogo costante sui valori e un solido sistema finanziario in Europa. Lavoriamo scrupolosamente nell'intento di rispettare le normative vigenti e ci proponiamo di aiutare i clienti a comprendere il nostro approccio critico di terze parti, migliorando, al contempo, la loro resilienza operativa.

Con Akamai, le istituzioni finanziarie possono gestire in modo efficace i problemi di conformità, tra cui le incertezze e le ambiguità relative alle normative (sia che si tratti di obblighi futuri o del DORA) tramite misure di sicurezza complete che riguardano i carichi di lavoro delle applicazioni e le API fino all'infrastruttura delle app. La sicurezza diventa quindi un componente vitale degli strumenti normativi, che facilitano un cambiamento sostenibile ed efficace e, soprattutto, favoriscono la fiducia dei clienti nelle istituzioni finanziarie e in un mercato finanziario più ampio.

Scoprite ulteriori informazioni sul DORA.