WHITE PAPER

Supportare gli obiettivi richiesti dal DORA con Akamai

Il concetto di resilienza operativa digitale si è evoluto notevolmente nel corso degli anni, in particolar modo all'interno dei servizi finanziari. Inizialmente, gli enti finanziari erano focalizzati sulla pianificazione del disaster recovery o della continuità operativa. Questi sforzi iniziali sono stati principalmente reattivi allo scopo di ripristinare i servizi dopo un'interruzione. Man mano che le minacce informatiche sono diventate più sofisticate e prevalenti, l'attenzione si è spostata verso misure maggiormente proattive. Gli enti finanziari hanno iniziato ad implementare solidi protocolli di cybersicurezza, regolari aggiornamenti di sistema e programmi di formazione dei dipendenti per prevenire le interruzioni prima che si verifichino. L'avvento di tecnologie avanzate, come i grandi modelli linguistici (LLM), l'intelligenza artificiale (AI) e l'apprendimento automatico (ML), ha rivoluzionato l'approccio nei confronti della resilienza operativa. Tuttavia, queste stesse tecnologie hanno rivoluzionato anche i vettori di attacco, aumentando la complessità e la frequenza delle minacce. Di conseguenza, la resilienza operativa deve continuamente adattarsi a queste sfide in continua evoluzione.

Queste tecnologie offrono l'analisi predittiva, il rilevamento automatizzato delle minacce e tempi di risposta più rapidi, migliorando notevolmente le funzionalità di resilienza. Un maggiore controllo normativo ha favorito ulteriormente l'evoluzione della resilienza operativa digitale. Alcune normative, come il regolamento generale sulla protezione dei dati (GDPR) dell'Unione europea, hanno contribuito ad innalzare gli standard per la protezione dei dati e la continuità operativa. Tuttavia, la complessità e la frequenza delle minacce informatiche sempre maggiori rappresentano i principali fattori trainanti che hanno spinto gli enti finanziari ad adottare strategie di resilienza più complete. I moderni approcci alla resilienza operativa digitale ora comprendono una gestione dei rischi olistica, che include non solo misure di protezione tecniche, ma anche sistemi di governance, gestione dei rischi di terze parti, pratiche di miglioramento e monitoraggio condotte continuamente e condivisione delle informazioni.

Introduzione al DORA

Il DORA (Digital Operational Resilience Act) è un nuovo regolamento emanato dall'Unione europea che si propone di migliorare la resilienza operativa digitale nel settore dei servizi finanziari. Il DORA stabilisce un sistema completo per la gestione dei rischi per l'ICT (Information and Communications Technology), che si applica ad un'ampia gamma di enti finanziari e provider di servizi ICT di terze parti. Il DORA, la cui entrata in vigore è fissata per il 17 gennaio 2025, prevede rigorosi requisiti in cinque aree fondamentali.

Gestione dei rischi

Segnalazione degli incidenti

Test sulla resilienza operativa digitale

Gestione dei rischi ICT di terze parti

Condivisione di informazioni e intelligence

Il DORA introdurrà un maggior numero di requisiti normativi, che richiedono agli enti finanziari di soddisfare standard più stringenti allo scopo di garantire la loro resilienza operativa nel caso di attacchi informatici, guasti del sistema e altri rischi digitali. I nuovi requisiti prevedono audit regolari, controlli della conformità e rapporti più rigorosi agli organismi di regolamentazione. Una migliore gestione dei rischi diventerà una necessità poiché il DORA richiede un approccio completo e integrato per identificare e valutare i rischi associati ai sistemi digitali e ai servizi aziendali più importanti. Gli enti finanziari dovranno implementare rigorosi controlli, monitorando continuando e mitigando tali rischi. Per molti enti finanziari, la conformità al DORA richiederà maggiori investimenti in tecnologie

avanzate, come l'intelligenza artificiale e l'apprendimento automatico, per migliorare e accelerare le loro funzionalità di risposta e resilienza operativa mediante livelli più elevati di rilevamento delle minacce, risposte automatizzate e analisi predittiva. Sarà anche fondamentale prestare attenzione alla gestione dei rischi di terze parti. Gli enti finanziari devono assicurarsi che i loro provider di servizi di terze parti abbiano adottato solide misure di resilienza operativa, tra cui condurre processi di due diligence, eseguire valutazioni regolari e stabilire chiari obblighi contrattuali per garantire la protezione dai rischi digitali. Il DORA, inoltre, richiede una maggiore trasparenza. Gli enti finanziari dovranno fornire una maggiore trasparenza sulle loro pratiche di resilienza operativa, dimostrando la propria capacità di rispondere in modo efficace alle interruzioni digitali, mantenendo record completi e comunicando apertamente con autorità di regolamentazione, utenti e clienti.

L'importanza del DORA per gli enti finanziari

Il DORA giunge in un momento critico per gli enti finanziari, che devono affrontare minacce informatiche sempre più frequenti e sofisticate. Secondo il Fondo monetario internazionale, nel corso degli ultimi due decenni, il settore dei servizi finanziari è stato uno dei bersagli più allettanti per i criminali informatici. Dal 2017, le perdite dirette si sono più che quadruplicate, fino a raggiungere i 2,5 miliardi di dollari, mentre le perdite indirette, come i danni alla reputazione o gli aggiornamenti dei sistemi di sicurezza, sono sostanzialmente più elevate. Gli attacchi non hanno solo violato informazioni finanziarie sensibili, ma hanno anche messo notevolmente a rischio la stabilità e l'integrità dei sistemi finanziari nel complesso. Poiché gli enti finanziari si affidano sempre più alle infrastrutture digitali, la complessità e l'interconnettività dei loro sistemi li rendono maggiormente vulnerabili alle minacce informatiche. I criminali sfruttano queste vulnerabilità utilizzando spesso tecniche sofisticate come il movimento laterale all'interno delle reti per ottenere l'accesso a dati preziosi o per interrompere i servizi. Questo metodo consente ai criminali di passare da un sistema all'altro, rendendo difficile rilevare e prevenire le loro attività dannose, il che aumenta la possibilità che si verifichino violazioni significative o interruzioni delle operazioni aziendali.

L'adozione del DORA è una risposta proattiva a queste minacce in continua evoluzione. Stabilendo una struttura armonizzata per la resilienza digitale all'interno degli stati membri dell'UE, il DORA mira a garantire un livello coerente di sicurezza e resilienza operativa nel settore finanziario. Questa uniformità è cruciale poiché aumenta la fiducia nell'infrastruttura digitale del settore, garantendo agli enti finanziari di riuscire a resistere e a riprendersi dalle interruzioni tecnologiche. La natura proattiva del DORA riflette una svolta strategica dalla semplice reazione agli incidenti all'anticipazione e alla mitigazione dei potenziali rischi prima che si materializzino. Questo approccio è concepito non solo per proteggere gli enti finanziari, ma anche per salvaguardare il più ampio ecosistema finanziario dai rischi sistemici. L'attenzione rivolta dalla normativa all'ottimizzazione dei meccanismi di risposta agli incidenti e al miglioramento della gestione dei rischi di terze parti sottolinea l'importanza di adottare un approccio completo e integrato alla cybersicurezza.

La trasparenza è un altro aspetto critico del DORA. Gli enti finanziari devono fornire una maggiore trasparenza sulle loro pratiche di resilienza operativa, dimostrando la propria capacità di rispondere in modo efficace alle interruzioni digitali. Questo livello di trasparenza è vitale per mantenere la fiducia di autorità di regolamentazione, utenti e clienti, oltre a sottolineare l'impegno delle istituzioni di proteggere le proprie infrastrutture digitali. L'importanza del DORA si estende oltre la conformità normativa poiché rappresenta una svolta fondamentale nel modo con cui gli enti finanziari si approcciano alla cybersicurezza e alla resilienza operativa. Allineandosi ai requisiti del DORA, gli enti finanziari non solo si proteggono dalle minacce attuali e future, ma aumentano anche la loro attendibilità in un panorama finanziario sempre più digitale.

In che modo Akamai aiuta gli enti finanziari a conformarsi al DORA

Tramite la scalabilità della nostra piattaforma globale e la sua vasta intelligence sulle minacce, possiamo aiutare gli enti finanziari a prevenire, rilevare e mitigare le minacce informatiche in ambienti on-premise e cloud per poter affrontare le complessità degli obblighi di conformità normativa in continua evoluzione. Le nostre soluzioni aiutano a gestire i pilastri fondamentali del DORA (gestione dei rischi, segnalazione degli incidenti, test di resilienza operativa digitale, gestione dei rischi ICT di terze parti e condivisione di informazioni e intelligence), garantendo una copertura completa e solidi sistemi di cybersicurezza.

API Security

Akamai API Security offre funzioni complete di individuazione delle API, gestione dei sistemi e protezione del runtime basata sull'AI/ML, essenziali per rilevare e bloccare gli avanzati attacchi alle API in tempo reale. I test di sicurezza proattivi e le analisi in tempo reale consentono agli enti finanziari di verificare tempestivamente il comportamento delle API, rispondere alle minacce e proteggere i dati sensibili, supportando la conformità ai requisiti del DORA per la gestione dei rischi ICT e la segnalazione degli incidenti.

La mitigazione dei rischi associati alle API ombra, alle API vulnerabili e all'abuso delle API rappresenta una sfida significativa dovuta ad una mancanza di visibilità e supervisione. Un'efficace sistema di sicurezza delle API offre funzioni complete di individuazione e catalogazione, rilevamento delle minacce in tempo reale e meccanismi di protezione basati sull'AI, garantendo un monitoraggio e una mitigazione costanti delle minacce correlate alle API e supportando la conformità agli standard normativi del DORA.

Akamai Guardicore Segmentation

Akamai Guardicore Segmentation consente agli enti finanziari di partizionare le proprie reti in segmenti sicuri, riducendo notevolmente il rischio di movimento laterale da parte delle minacce informatiche. Questa tecnologia si allinea con gli obiettivi del DORA ottimizzando la gestione dei rischi ICT e i test della resilienza operativa digitale. Isolando le risorse violate e limitando il movimento laterale dei criminali, la microsegmentazione aiuta a mantenere un solido livello di sicurezza e facilita un'efficace risposta agli incidenti.

Akamai Guardicore Segmentation offre una visibilità accurata sulle dipendenze delle applicazioni e un'applicazione di policy precisa, garantendo la gestione continua delle policy di microsegmentazione. La piattaforma supporta opzioni di implementazione basate su agenti e senza agenti, fornendo la flessibilità per vari ambienti, tra cui gli ambienti PaaS, IoT e OT nel cloud. Utilizzando workflow intuitivi e la creazione di policy basate sull'intelligenza artificiale, Akamai Guardicore Segmentation semplifica il processo di microsegmentazione, consentendo agli enti finanziari di implementare e adattare rapidamente le policy di sicurezza alle mutevoli condizioni della rete. Questo approccio completo non solo riduce la superficie di attacco, ma aiuta anche a supportare la conformità con i requisiti normativi per la resilienza operativa digitale.

Edge DNS

Akamai Edge DNS garantisce elevati livelli di disponibilità e performance dei servizi DNS, proteggendo le infrastrutture correlate on-premise, cloud e ibride. Questa soluzione è essenziale per mantenere la continuità dei servizi e proteggere dalle minacce informatiche su larga scala, ottemperando ai requisiti del DORA per la gestione dei rischi ICT e la segnalazione degli incidenti.

App & API Protector

Akamai App & API Protector contrasta gli attacchi sferrati al livello 7 con protezioni complete, tra cui la difesa dagli attacchi DDoS (Distributed Denial-of-Service), dai bot e dalle vulnerabilità riportate nell'elenco OWASP Top 10. Questa soluzione supporta una solida sicurezza per le applicazioni web e le API, che è fondamentale per garantire la conformità ai requisiti del DORA per la gestione dei rischi ICT e la segnalazione degli incidenti.

Client-Side Protection & Compliance

Akamai assiste nel processo di conformità al PCI e protegge i siti web dagli attacchi JavaScript, tenendo al sicuro i dati sensibili dei clienti e aiutando gli enti finanziari a soddisfare i rigorosi requisiti di conformità stabiliti dal DORA e da altre normative.

Prolexic

Akamai Prolexic protegge l'infrastruttura dagli attacchi DDoS, offrendo solidi meccanismi di difesa per garantire tempo di attività e affidabilità, anche durante attacchi su larga scala, e supportando quindi gli obiettivi del DORA relativi al miglioramento della resilienza operativa digitale e delle funzionalità di risposta agli incidenti.

Bot Manager

Akamai Bot Manager fornisce una gestione avanzata dei bot progettata per rilevare e mitigare i sofisticati bot dannosi, consentendo, al tempo stesso, l'accesso ai bot legittimi. In tal modo, la soluzione aiuta a supportare il traffico legittimo, mantenendo eccellenti user experience e aiutando le aziende ad aderire ai requisiti del DORA per la gestione dei rischi ICT.

Account Protector

Akamai Account Protector rileva e mitiga gli attacchi per il controllo degli account, l'abuso di apertura degli account e il credential stuffing. Questa funzionalità è cruciale per proteggere i conti dei clienti e mantenere la loro fiducia, allineandosi all'attenzione rivolta dal DORA ad una solida gestione dei rischi ICT e alla segnalazione degli incidenti.

Content Protector

Akamai Content Protector aiuta a impedire agli scraper di rubare i contenuti e ridurre i tassi di conversione. Questa soluzione aiuta a mantenere protetti i contenuti proprietari, supportando gli obiettivi del DORA volti alla salvaguardia delle risorse digitali e al miglioramento della resilienza operativa.

Requisiti dettagliati e soluzioni di Akamai

Governance e organizzazione

Governance della sicurezza: il SOCC (Security Operations Command Center) di Akamai offre servizi di risposta e monitoraggio 24 ore su 24, 7 giorni su 7, aiutando a monitorare continuamente la governance della sicurezza.

Integrazione SIEM (Security Information and Event Management): la soluzione di integrazione SIEM di Akamai offre un modo per distribuire gli eventi SIEM a strumenti analitici come Splunk, QRadar e ArcSight, consentendo di incorporare gli eventi di sicurezza di Akamai nell'infrastruttura di sicurezza ed eventi nel complesso.

Governance, rischio e conformità (GRC): l'Akamai Control Center fornisce un'interfaccia centralizzata per la gestione dei prodotti e dei servizi di Akamai, offrendo alle aziende l'accesso, le informazioni e il controllo che servono per aiutarle a soddisfare i requisiti normativi, di rischio e conformità con online experience ottimali.

Sistema di gestione dei rischi ICT

Software di gestione dei rischi: Akamai Secure Internet Access fornisce una protezione avanzata dalle minacce, inclusi sistemi di difesa da malware e phishing.

Piattaforme di protezione degli endpoint: Akamai Bot Manager aiuta a gestire e mitigare il traffico dannoso dei bot.

Strumenti di gestione delle vulnerabilità: le soluzioni di Akamai effettuano continuamente la scansione e la valutazione delle vulnerabilità dei sistemi ICT.

Gestione degli incidenti correlati all'ICT

Piattaforme di risposta agli incidenti: i servizi di risposta agli incidenti di Akamai automatizzano e organizzano i processi correlati.

Sistemi di tracciamento degli incidenti: le soluzioni di Akamai consentono di tenere traccia e gestire i rapporti sugli incidenti e le relative risoluzioni.

Test sulla resilienza operativa digitale

Servizi di test di penetrazione: Akamai offre ai clienti test di penetrazione e altri servizi di valutazione della sicurezza.

Esercizi Red Team/Blue Team: Akamai conduce regolarmente esercizi di sicurezza per valutare e migliorare la risposta dell'organizzazione e per raggiungere la conformità normativa.

Gestione dei rischi di terze parti

Piattaforme di gestione dei rischi di terze parti: i prodotti per la sicurezza di Akamai, incluse le soluzioni WAF (Web Application Firewall) e i gateway API, aiutano a gestire e mitigare i rischi.

Software di gestione dei contratti: le soluzioni di Akamai aiutano a gestire gli obblighi contrattuali e a garantire la conformità.

Piattaforme di intelligence sulle minacce: i servizi di intelligence sulle minacce di Akamai forniscono informazioni aggiornate sulle tendenze emergenti tramite feed interni ed esterni.

FS-ISAC (Financial Services Information Sharing and Analysis Center): Akamai è membro fondatore dell'importante programma FS-ISAC per i provider. La condivisione dell'intelligence sulle minacce e la collaborazione interna continuano a rimanere cruciali per proteggere efficacemente l'infrastruttura del settore dei servizi finanziari tramite comunicazioni rapide su vulnerabilità, interruzioni, rischi o violazioni. Il nostro esclusivo accesso ai dati sul traffico e sugli attacchi ci consente di collaborare sulla ricerca e condividere le best practice con gli altri membri.

Supervisione e applicazione

Strumenti di audit e conformità: le soluzioni per la conformità di Akamai aiutano a controllare e a garantire l'aderenza ai requisiti normativi.

Soluzioni di monitoraggio e generazione di rapporti: il Control Center fornisce funzionalità complete di monitoraggio e generazione di rapporti.

Referenze dei clienti a dimostrazione dell'efficacia delle soluzioni di Akamai

Per stabilire se Akamai può assistere nel processo di conformità normativa, può risultare utile esaminare le customer experience. Di seguito vengono riportati alcuni casi rilevanti.

Compagnia assicurativa di grandi dimensioni: la storia di questo cliente evidenzia come questa compagnia assicurativa sfrutti le soluzioni di Akamai per migliorare la sicurezza e le performance. Le soluzioni di Akamai aiutano a mitigare gli attacchi DDoS e a proteggere le API, che sono componenti cruciali per soddisfare i requisiti del DORA per la gestione dei rischi ICT e la risposta agli incidenti.

Cashflows: Cashflows utilizza le soluzioni per la sicurezza di Akamai allo scopo di proteggere la sua piattaforma di pagamento ospitata nel cloud. Questo case study mostra come Akamai aiuti a mantenere la conformità con gli standard di sicurezza e a proteggere da minacce come gli attacchi DDoS, garantendo un livello continuo di disponibilità e sicurezza nei servizi di pagamento. Tutto ciò si allinea con i requisiti del DORA per la gestione dei rischi ICT e i test della resilienza operativa digitale.

LANDBANK: LANDBANK, la più grande banca di proprietà del governo nelle Filippine, si affida ad Akamai per tenere al sicuro le sue applicazioni online, proteggersi dalle minacce informatiche e semplificare la sua trasformazione digitale. Questa storia è particolarmente importante per comprendere come le soluzioni di Akamai possono aiutare a gestire i rischi di terze parti e a garantire solidi processi di gestione degli incidenti.

Questi esempi illustrano come le funzionalità di gestione proattiva delle minacce e le soluzioni per la sicurezza di Akamai possono supportare gli enti finanziari per soddisfare i requisiti del DORA, tra cui la gestione dei rischi ICT, la segnalazione degli incidenti, i test sulla resilienza operativa digitale e la gestione dei rischi di terze parti.

Conclusione

Per gli enti finanziari, il DORA rappresenta una svolta significativa nello scenario normativo poiché richiede misure di cybersicurezza complete e proattive. La suite di soluzioni di Akamai offre agli enti finanziari un solido sistema per aiutarli a (1) soddisfare i rigorosi requisiti del DORA e a (2) garantire una migliore resilienza operativa digitale, una solida gestione dei rischi ICT ed efficaci funzionalità di risposta agli incidenti. Utilizzando le avanzate tecnologie di Akamai, gli enti finanziari possono affrontare con sicurezza le complessità del processo di conformità al DORA e salvaguardare le proprie attività dalle minacce in continua evoluzione.

Scoprite ulteriori informazioni sulle nostre soluzioni per i servizi finanziari

Akamai Security protegge le applicazioni che supportano le vostre attività aziendali in ogni momento dell'interazione senza compromettere le performance o le customer experience. Tramite la scalabilità e la visibilità della nostra piattaforma globale, possiamo collaborare con voi per prevenire, rilevare e mitigare le minacce in modo da consentirvi di rafforzare la fiducia nel brand e realizzare la vostra visione.

A sostegno e protezione della vita online c'è sempre Akamai. Le principali aziende al mondo scelgono Akamai per creare, offrire e proteggere le loro experience digitali, aiutando miliardi di persone a vivere, lavorare e giocare ogni giorno. Akamai Connected Cloud, una piattaforma edge e cloud ampiamente distribuita, avvicina le app e le experience agli utenti e allontana le minacce. Per ulteriori informazioni sulle soluzioni di cloud computing, sicurezza e delivery dei contenuti di Akamai, visitate il sito akamai.com o akamai.com/blog e seguite Akamai Technologies su X (in precedenza Twitter) e LinkedIn. Data di pubblicazione: 09/24.