ANALISI DI AKAMAI

Conformità al DORA: una panoramica dettagliata

Con l'entrata in vigore del DORA (Digital Operational Resilience Act), gli enti finanziari e i provider di servizi ICT (Information and Communications Technology) di terze parti che operano nell'UE deve seguire questa nuova normativa, i cui requisiti potrebbero già essere effettivi, ma i cui livelli di portata e complessità implicano per molte istituzioni finanziarie un continuo impegno a lavorare per i prossimi mesi e anni nell'intento di soddisfare la piena conformità al DORA.

Le principali considerazioni sulla conformità al DORA

Questo articolo sottolinea le considerazioni principali di cui tenere conto per garantire la conformità al DORA, pertanto, anche se non esaustivo, è stato redatto allo scopo di mettere in evidenza le operazioni che potrebbero aiutare gli enti finanziari a procedere nel loro percorso verso la conformità.

La conformità al DORA può aiutare le organizzazioni a mitigare meglio i rischi, a proteggere i dati critici, ad aumentare la loro resilienza alle minacce in continua evoluzione e a trarre vantaggio da una maggiore visibilità su reti, sistemi e processi.

Anche se il percorso verso la conformità al DORA può implicare complessità e costi, rappresenta, inoltre, un'opportunità per creare un sistema di sicurezza unificato e completo che può aiutare le organizzazioni a prepararsi per il successo in futuro.

Azione	Perché è importante	Soluzioni
PILASTRO 1. La gestione dei rischi ICT		
Restringere il movimento laterale in base ai carichi di lavoro.	Include gli incidenti riscontrati, protegge i flussi di dati e minimizza i problemi di downtime e il potenziale impatto aziendale.	Microsegmentazione con policy specifiche per i carichi di lavoro, ispezione del traffico est-ovest tramite firewall interni, IBAC (Identity-Based Access Control), ZTNA (Zero Trust Network Access), SDN (Software-Defined Networking), PAM (Privileged Access Management), EDR (Endpoint Detection and Response)
Limitare gli accessi degli utenti alle applicazioni necessarie in base al loro ruolo e alla loro identità.	Fornisce un approccio mirato e metodico per la protezione delle risorse critiche controllando gli accessi degli utenti. Previene gli accessi non autorizzati e fornisce un controllo granulare sugli accessi di utenti e sistemi.	RBAC (Role-Based Access Control), IAM (Identity and Access Management), ZTNA (Zero Trust Network Access), SSO (Single Sign-On), MFA (Multi-Factor Authentication) e PAM (Privileged Access Management)
Rimuovere gli accessi tramite ID e password, sostituendoli con l'MFA.	Protegge dai tentativi di violazione delle credenziali.	Autenticazione multifattore, SSO (Single Sign-On), autenticazione senza password (ad es., dati biometrici, chiavi FIDO2), policy di accesso condizionale che richiedono l'MFA, PAM (Privileged Access Management) con MFA per un accesso avanzato e soluzioni MFA basate su token per dispositivi mobili o hardware

Azione	Perché è importante	Soluzioni
Garantire visibilità su tutte le risorse ICT, dai server alle reti fino alle applicazioni.	Un'efficace gestione dei rischi inizia con la possibilità di identificare e controllare specifiche vulnerabilità presenti in tutte le risorse in qualsiasi momento. Il monitoraggio e la visibilità sono aspetti fondamentali.	CMDB (Configuration Management Database), ITAM (IT Asset Management), SIEM (Security Information and Event Management), NDR (Network Detection and Response), EDR (Endpoint Detection and Response), APM (Application Performance Monitoring), CSPM (Cloud Security Posture Management), ASPM (Application Security Posture Management) e DSPM (Data Security Posture Management)
Proteggere la trasmissione dei dati.	I dati sensibili, incluse le informazioni di identificazione personale (PII), i record finanziari e i dati delle transazioni, devono essere gestiti in modo riservato.	Protocolli di crittografia complessi, VPN, TLS, protocolli di trasferimento sicuro dei file, crittografia degli endpoint, PKI e molti altri
PILASTRO 2. Gestione e segnalazione degli incidenti correlati all'ICT		
Segmentare i confini.	Velocizza i processi di rilevamento, risposta e recupero dai problemi contenendo e isolando rapidamente gli incidenti riscontrati.	Microsegmentazione, segmentazione della rete, firewall di nuova generazione, ACL (Access Control List), SDN (Software-Defined Networking), Zero Trust Network Access
Creare la possibilità di isolare i segmenti compromessi senza interrompere le operazioni su larga scala.	Garantisce una rapida risposta agli incidenti.	Microsegmentazione, SDN (Software-Defined Networking), EDR (Endpoint Detection and Response), NAC (Network Access Control), ZTNA (Zero Trust Network Access), LAN virtuali (VLAN)
Restringere l'accesso alle informazioni sensibili e alle applicazioni critiche.	Riduce la probabilità di verificarsi di una minaccia.	RBAC (Role-Based Access Control), MFA (Multi-Factor Authentication), ZTNA (Zero Trust Network Access), IAM (Identity and Access Management), PAM (Privileged Access Management), rete e microsegmentazione
Utilizzare le funzioni di rilevamento e risposta alle minacce in tempo reale.	Una rapida risposta agli incidenti ICT è fondamentale per limitare il loro impatto. Anche un'intelligence dettagliata sulle minacce e le informazioni sugli accessi possono risultare utili per la segnalazione dei problemi riscontrati.	SIEM (Security Information and Event Management), EDR (Endpoint Detection and Response), XDR (Extended Detection and Response), IDPS (Intrusion Detection and Prevention System), integrazione e feed dell'intelligence sulle minacce, SOAR (Security Orchestration, Automation and Response), analisi comportamentale e rilevamento delle anomalie, individuazione e servizi di ricerca delle minacce

Azione	Perché è importante	Soluzioni
Mettere in atto avanzati sistemi di ricerca delle minacce con mitigazione dei problemi riscontrati.	Rileva i rischi in modo proattivo.	Servizi di ricerca delle minacce e MSSP (Managed Security Service Provider)
PILASTRO 3. Test sulla resilienza operativa digitale		
Simulare gli errori in parti segmentate della rete.	Fornisce una visibilità in tempo reale sulla resilienza operativa.	Integrazione con uno strumento di modellazione per mostrare l'intero percorso della resilienza e i punti di applicazione Strumenti di Chaos Engineering, ambienti di simulazione della rete e sandbox, SDN (Software Defined Network), esercizi per Red Team/Blue Team, test di disaster recovery e failover, ambienti di laboratorio per la sicurezza
Eseguire regolarmente test di stress e simulazioni degli attacchi.	Evidenzia la lacune presenti in reti, applicazioni e sistemi critici. Consente di apportare rapidamente le modifiche necessarie e di creare strategie di risposta adattiva, rafforzando la vostra capacità di mitigare le minacce durante la loro evoluzione.	Guida ai ransomware ed esercitazioni a tavolino per Red/Blue/Purple Team Test di penetrazione regolari, simulazioni di violazioni e attacchi, strumenti di scansione delle vulnerabilità e valutazioni dei sistemi di sicurezza, simulazioni di attacchi DDoS e simulazioni automatizzate degli attacchi
Utilizzare le tecnologie ZTNA e MFA per eseguire i test della resilienza.	Mantenendo rigorose policy per gli accessi durante le interruzioni o gli incidenti simulati, potrete capire lo stato reale del vostro sistema di sicurezza.	ZTNA (Zero Trust Network Access), MFA (Multi-Factor Authentication), IAM (Identity and Access Management), SIEM (Security Information and Event Management), microsegmentazione
Controllare gli accessi alle applicazioni e alle risorse principali in situazioni di stress.	Migliora l'affidabilità e la preparazione dei vostri sistemi di difesa.	ZTNA (Zero Trust Network Access), MFA (Multi-Factor Authentication), RBAC (Role-Based Access Control), PAM (Privileged Access Management), IAM (Identity and Access Management), rete e microsegmentazione, strumenti di bilanciamento del carico e WAAP (Web Application and API Protection)
Eseguire i test di preparazione per proteggersi dagli attacchi DDoS (Distributed Denial-of-Service).	Aiuta ad individuare le vulnerabilità e ad ottimizzare le strategie di resilienza.	Simulazione e test di preparazione per proteggersi dagli attacchi DDoS, protezione dagli attacchi DDoS basata sul cloud, WAF (Web Application Firewall), scrubbing centre del traffico, strumenti di analisi comportamentale della rete e rilevamento delle anomalie, guide di risposta agli incidenti ed esercitazioni a tavolino, esercizi per Red Team

Azione	Perché è importante	Soluzioni
PILASTRO 4. Gestione dei rischi di terze parti		
Segmentare gli ambienti in cui interagiscono vendor o applicazioni di terze parti.	Velocizza i processi di rilevamento, risposta e recupero dai problemi contenendo e isolando rapidamente gli incidenti riscontrati.	Microsegmentazione con policy basate sulle identità, LAN virtuali (VLAN), zone demilitarizzate (DMZ), firewall con controlli degli accessi granulari, ZTNA (Zero Trust Network Access), NAC (Network Access Control), gateway VPN dedicati
Proteggere l'accesso a Internet per tutte le comunicazioni esterne.	Garantisce che eventuali terze parti possano connettersi solo tramite percorsi protetti e controllati.	SWG (Secure Web Gateway), CASB (Cloud Access Security Broker), sicurezza del DNS, firewall di nuova generazione con filtraggio degli URL (NGFW), comunicazioni crittografate (ad es., HTTPS, TLS 1.2/1.3), gateway di sicurezza e-mail con crittografia, ZTNA (Zero Trust Network Access)
Monitorare continuamente gli accessi di terze parti in tempo reale.	Rileva e protegge immediatamente dai rischi provenienti dai provider di servizi ICT o dai loro vendor esterni.	Microsegmentazione, portale di analisi e regole WAAP personalizzate SIEM (Security Information and Event Management), IAM (Identity and Access Management), PAM (Privileged Access Management), UEBA (User and Entity Behaviour Analytics), ZTNA (Zero Trust Network Access), NAC (Network Access Control), EDR (Endpoint Detection and Response)
PILASTRO 5. Condivisione delle informazioni		
Segmentare i dati sensibili e restringere l'accesso solo agli utenti autorizzati.	Riduce la probabilità di verificarsi di una minaccia.	Classificazione ed etichettatura dei dati, microsegmentazione con policy incentrate sui dati, RBAC (Role-Based Access Control), IAM (Identity and Access Management), DLP (Data Loss Prevention) e PAM (Privileged Access Management)
Assicurarsi che la condivisione delle informazioni interne ed esterne avvenga tramite canali sicuri.	Riduce il rischio di violazione dei dati sensibili.	Crittografia end-to-end (ad es., TLS 1.2/1.3, S/MIME), protocolli di trasferimento sicuro dei file (ad es., SFTP, FTPS), soluzioni di crittografia e-mail, VPN (Virtual Private Network), SWG (Secure Web Gateway) e DLP (Data Loss Prevention)

Azione	Perché è importante	Soluzioni
Proteggere gli accessi delle piattaforme di comunicazione.	Riduce il rischio di violazione dei dati sensibili.	MFA (Multi-Factor Authentication), IAM (Identity and Access Management), SSO (Single Sign-On), ZTNA (Zero Trust Network Access), controlli di sicurezza degli endpoint, piattaforme di comunicazione crittografata e SWG (Secure Web Gateway)
Applicare le funzionalità di verifica delle identità.	Rafforza la fiducia nel processo di condivisione delle informazioni, proteggendo, al contempo, l'integrità dei dati.	MFA (Multi-Factor Authentication), IAM (Identity and Access Management), SSO (Single Sign-On), PAM (Privileged Access Management), autenticazione biometrica (ad es., scansione delle impronte digitali, riconoscimento facciale), certificati digitali e infrastrutture a chiave pubblica (PKI), servizi di directory (ad es., Active Directory, Microsoft Entra ID)
Condividere i dati in modo sicuro con altri paesi e utenti all'interno della comunità finanziaria relativamente alle minacce emergenti, alle vulnerabilità e ai modelli di attacco.	Distribuisce l'intelligence sulle minacce in diverse aree geografiche, creando risposte rapide e strategie di difesa collettiva.	Piattaforme per l'intelligence sulle minacce, canali di comunicazione crittografati (ad es., TLS, S/ MIME, VPN), condivisione di informazioni ed eventi (ad es., FS-ISAC), classificazione dei dati e controlli degli accessi, protocolli di trasferimento sicuro dei file (ad es., SFTP, FTPS), policy di condivisione dei dati all'estero

Nota: *le informazioni fornite in questo documento sono da intendersi unicamente come informazioni generali, non devono essere considerate una consulenza legale né rappresentano alcun impegno da parte di Akamai. Le leggi e le normative possono cambiare e le interpretazioni sono soggette a variazioni nel corso del tempo. Non viene fornita alcuna garanzia riguardo all'accuratezza, alla completezza o all'adeguatezza delle informazioni fornite. Per richiedere una consulenza legale o per questioni legali specifiche, rivolgersi ad un legale qualificato in grado di fornire consigli specifici alla propria situazione e alla giurisdizione applicabile.*