PRÉSENTATION AKAMAI

Conformité avec le règlement DORA : recommandations par pilier

La loi sur la résilience opérationnelle digitale (DORA) étant désormais applicable, les entités financières et les fournisseurs de services tiers TIC (technologies de l'information et de la communication) qu opèrent dans l'UE jouent un nouveau rôle. Même si les nouvelles exigences sont déjà en vigueur, leur ampleur et leur complexité vont pousser de nombreuses institutions financières à travailler vers une pleine conformité DORA au cours des prochains mois et années.

Principales considérations de conformité avec le règlement DORA

Cet article présente les principaux éléments à prendre en compte pour assurer la conformité avec le règlement DORA. Bien qu'il ne soit pas exhaustif, il est conçu pour mettre en évidence les actions susceptibles d'aider les entités financières à se rapprocher de la conformité.

Travailler à la mise en conformité avec le règlement DORA peut aider les organisations à mieux atténuer les risques, à sécuriser les données critiques, à devenir plus résilientes face aux menaces en constante évolution et à bénéficier d'une meilleure visibilité sur les réseaux, les systèmes et les processus.

Bien que le chemin vers la conformité avec le règlement DORA puisse être complexe et coûteux, il offre également la possibilité de créer un cadre de sécurité unifié et complet qui peut aider une organisation à se préparer pour la réussite future.

Action	Pourquoi est-ce important	Solutions
PILIER 1 : Gestion des risques liés aux TIC		
Limiter les mouvements latéraux en fonction de la charge de travail.	Enraye les incidents, protège les flux de données critiques et limite les interruptions de service ainsi que l'impact potentiel sur l'entreprise.	Microsegmentation avec des stratégies spécifiques à la charge de travail, inspection du trafic est-ouest via des pare-feu internes, contrôle d'accès basé sur l'identité (IBAC), Zero Trust Network Access (ZTNA), mise en réseau logicielle (SDN), gestion des accès privilégiés (PAM), détection et réponse aux points de terminaison (EDR)
Limiter l'accès des utilisateurs aux applications nécessaires en fonction de leur rôle et de leur identité.	Fournit une approche ciblée et méthodique pour protéger les ressources critiques en contrôlant qui peut accéder à quoi. Empêche les accès non autorisés et vous donne un contrôle granulaire sur les utilisateurs et l'accès au système.	Contrôle d'accès basé sur les rôles (RBAC), gestion des identités et des accès (IAM), accès réseau Zero Trust (ZTNA), authentification unique (SSO), authentification multifactorielle (MFA) et gestion des accès privilégiés (PAM)
Supprimer l'accès par ID et mot de passe et le remplacer par l'authentification multifactorielle.	Protège contre les informations d'identification compromises.	Authentification multifactorielle, authentification unique (SSO), authentification sans mot de passe (par exemple, biométrie, clés FIDO2), stratégies d'accès conditionnelles nécessitant une authentification multifactorielle, gestion des accès privilégiés (PAM) avec authentification multifactorielle pour un accès élevé, et des solutions MFA basées sur des jetons matériels ou des notifications Push mobiles

Action	Pourquoi est-ce important	Solutions
Assurer la visibilité dans toutes les ressources TIC, des serveurs aux réseaux en passant par les applications.	Une gestion efficace des risques commence par la capacité d'identifier et de contrôler des vulnérabilités spécifiques sur l'ensemble des ressources à tout moment. La surveillance et la visibilité sont essentielles.	Base de données de gestion de configuration (CMDB), gestion des actifs informatiques (ITAM), gestion des événements et des informations de sécurité (SIEM), détection et réponse réseau (NDR), détection et réponse aux points de terminaison (EDR), suivi des performances des applications (APM), gestion de la posture de sécurité dans le cloud (CSPM), gestion de la posture de sécurité des applications (ASPM) et gestion de la posture de sécurité des données (DSPM)
Sécuriser la transmission des données.	Les données sensibles, y compris les informations d'identification personnelle (PII), les registres financiers et les données transactionnelles, doivent être traitées de manière confidentielle.	Protocoles de chiffrement forts, VPN, TLS, protocoles de transfert de fichiers sécurisés, chiffrement de point final, PKI, etc.
PILIER 2 : Gestion et reporting des incidents liés aux TIC		
Segmenter les limites.	Accélère les processus de détection, de réponse et de restauration en regroupant et en isolant rapidement les incidents.	Microsegmentation, segmentation du réseau, pare-feux nouvelle génération, listes de contrôle d'accès (ACL), SDN (Software-Defined Networking), accès réseau Zero Trust
Créer la possibilité d'isoler les segments compromis sans perturber les opérations plus vastes.	Garantit une réponse rapide aux incidents.	Microsegmentation, SDN (Software-Defined Networking), détection et réponse des points d'extrémité (EDR), contrôle d'accès au réseau (NAC), ZTNA (Zero Trust Network Access), réseaux locaux virtuels (VLAN)
Limiter l'accès aux informations sensibles et aux applications critiques.	Réduit la probabilité d'une menace.	Contrôle d'accès basé sur les rôles (RBAC), authentification multifactorielle (MFA), accès réseau Zero Trust (ZTNA), gestion des identités et des accès (IAM), gestion des accès privilégiés (PAM), réseau et microsegmentation
Utiliser la détection et la protection automatisées en temps réel contre les menaces.	Une réponse rapide aux incidents TIC est essentielle pour limiter leur impact. Les informations détaillées sur les menaces et les informations de journalisation peuvent également être utiles pour la création de rapports.	Gestion des événements et des informations de sécurité (SIEM), détection et réponse aux points de terminaison (EDR), détection et réponse étendues (XDR), systèmes de détection et de prévention des intrusions (IDP), intégration et flux de renseignements sur les menaces, orchestration de la sécurité, automatisation et réponse (SOAR), analyse comportementale et détection des anomalies, tromperie et services de recherche des menaces

Action	Pourquoi est-ce important	Solutions
Envisager de mettre en place une recherche avancée des menaces avec des mesures correctives.	Détecte les risques de manière proactive.	Services de recherche des menaces et fournisseurs de services de sécurité gérés (MSSP)
PILIER 3 : Tests de résilience opérationnelle digitale		
Simuler une panne dans des parties segmentées du réseau.	Fournit une vue en temps réel de la résilience opérationnelle.	Intégration à un outil de modélisation pour montrer la résilience complète des chemins et les points d'application Outils d'ingénierie de chaos, environnements de simulation réseau et sandbox, mise en réseau logicielle (SDN), exercices d'équipe rouge/bleue, reprise après sinistre et tests de basculement, environnements de laboratoire de sécurité
Exécuter régulièrement des tests de résistance et des simulations d'attaque.	Met en évidence les défaillances dans les réseaux, les applications et les systèmes critiques. Vous permet d'effectuer rapidement les ajustements nécessaires et de mettre en place des stratégies de réponse adaptatives, ce qui renforce votre capacité à atténuer les menaces à mesure qu'elles évoluent.	Guide sur les ransomwares et exercices de simulation pour les équipes rouges, bleues et violettes Tests d'intrusion réguliers, simulation des violations et des attaques, outils d'analyse des vulnérabilités et évaluations de posture, simulation DDoS, simulation automatisée des attaques
Utiliser ZTNA et MFA pour les tests de résilience.	En maintenant des stratégies d'accès strictes lors de simulations d'incidents ou de perturbations, vous obtenez une image fidèle de votre état de sécurité.	ZTNA (Zero Trust Network Access), authentification multifactorielle (MFA), gestion des identités et des accès (IAM), gestion des événements et des informations de sécurité (SIEM), microsegmentation
Contrôler l'accès aux applications et ressources clés sous contrainte.	Améliore la fiabilité et la préparation de vos défenses.	Accès réseau Zero Trust (ZTNA), authentification multifactorielle (MFA), contrôle d'accès basé sur les rôles (RBAC), gestion des accès privilégiés (PAM), gestion des identités et des accès (IAM), réseau et microsegmentation, équilibreurs de charge, protection des applications Web et des API (WAAP)
Tester le niveau de préparation face à une attaque par déni de service distribué (DDoS).	Permet d'identifier les vulnérabilités et d'optimiser les stratégies de résilience.	Simulation et tests DDoS, protection DDoS basée sur le cloud, pare-feu d'applications Web (WAF), centres de nettoyage du trafic, outils d'analyse du comportement du réseau et de détection des anomalies, guides et exercices de réponse aux incidents, et exercices d'équipe rouge

Action	Pourquoi est-ce important	Solutions
PILIER 4 : Gestion des risques liés aux tiers		
Segmenter les environnements dans lesquels des fournisseurs ou des applications tiers interagissent.	Accélère les processus de détection, de réponse et de restauration en regroupant et en isolant rapidement les incidents.	Microsegmentation avec stratégies basées sur l'identité, réseaux locaux virtuels (VLAN), zones démilitarisées (DMZ), pare-feu avec contrôles d'accès granulaires, accès réseau Zero Trust (ZTNA), contrôle d'accès réseau (NAC), passerelles VPN dédiées
Sécuriser l'accès Internet pour toutes les communications externes.	Garantit que les tiers ne se connectent que par le biais de voies sécurisées et contrôlées.	Passerelles Web sécurisées (SWG), courtiers de sécurité d'accès au cloud (CASB), sécurité DNS, pare-feux nouvelle génération avec filtrage d'URL (NGFW), communications chiffrées (par exemple, HTTPS, TLS 1,2/1,3), passerelles de sécurité de messagerie électronique avec chiffrement, accès réseau Zero Trust (ZTNA)
Activer la surveillance continue en temps réel des accès tiers.	Détecte et protège immédiatement contre les risques provenant de fournisseurs TIC ou de leurs fournisseurs externes.	Microsegmentation, portail d'analyse et règles WAP personnalisées Gestion des événements et des informations de sécurité (SIEM), gestion des identités et des accès (IAM), gestion des accès privilégiés (PAM), analyse du comportement des utilisateurs et des entités (UEBA), Zero Trust Network Access (ZTNA), contrôle des accès au réseau (NAC) et détection et réponse aux points de terminaison (EDR)
PILIER 5 : Partage d'informations		
Segmenter les données sensibles et limiter l'accès aux utilisateurs autorisés uniquement.	Réduit la probabilité d'une menace.	Classification et étiquetage des données, microsegmentation avec règles centrées sur les données, contrôle d'accès basé sur les rôles (RBAC), gestion des identités et des accès (IAM), prévention des pertes de données (DLP) et gestion des accès privilégiés (PAM)
S'assurer que le partage d'informations internes et externes s'effectue par des canaux sécurisés.	Réduit le risque de compromission des données sensibles.	Chiffrement de bout en bout (par exemple, TLS 1,2/1,3, S/MIME), protocoles de transfert de fichiers sécurisés (par exemple, SFTP, FTPS), solutions de messagerie chiffrée, réseaux privés virtuels (VPN), passerelles Web sécurisées (SWG) et prévention des pertes de données (DLP)

Action	Pourquoi est-ce important	Solutions
Permettre un accès sécurisé aux plateformes de communication.	Réduit le risque de compromission des données sensibles.	Authentification multifactorielle (MFA), gestion des identités et des accès (IAM), authentification unique (SSO), accès réseau Zero Trust (ZTNA), contrôles de sécurité des points de terminaison, plateformes de communication chiffrées et passerelles Web sécurisées (SWG)
Appliquer la vérification d'identité.	Renforce la confiance dans le processus de partage des informations tout en protégeant l'intégrité des données.	Authentification multifactorielle (MFA), gestion des identités et des accès (IAM), authentification unique (SSO), gestion des accès privilégiés (PAM), authentification biométrique (par ex. empreinte digitale, reconnaissance faciale), certificats digitaux et infrastructure à clé publique (PKI), et services d'annuaire (par exemple, Active Directory, Microsoft entra ID)
Partager en toute sécurité des données transfrontalières avec d'autres membres de la communauté financière sur les menaces émergentes, les vulnérabilités et les modèles d'attaque.	Répartit les renseignements sur les menaces dans différentes zones géographiques, créant ainsi des réponses rapides et des stratégies de défense collective.	Plateformes de renseignements sur les menaces, canaux de communication chiffrés (par exemple, TLS, S/MIME, VPN), partage d'informations et événements (par exemple, FS-ISAC), classification des données et contrôles d'accès, protocoles de transfert de fichiers sécurisés (par exemple, SFTP, FTPS), politiques de partage de données transfrontalières