Maîtriser les exigences de la loi DORA : de la conformité à la cyberrésilience

La loi sur la résilience opérationnelle numérique (DORA) redéfinit la cybersécurité pour le secteur financier de l'UE. La conformité est la base ; le véritable objectif est de créer une organisation résiliente capable d'empêcher une violation de données de devenir un sinistre.

Dans les environnements informatiques complexes d'aujourd'hui, les attaquants ne restent pas là où ils atterrissent. Ils évoluent latéralement et recherchent des actifs de grande valeur. **Ce n'est pas la violation initiale, mais la propagation qui provoque le plus de dommages.**

Akamai Guardicore Segmentation arrête la propagation. Notre plateforme de microsegmentation Zero Trust vous donne le pouvoir de voir, segmenter et sécuriser l'ensemble de votre environnement hybride, ce qui fait de la conformité avec DORA un avantage stratégique.

L'avantage de la plateforme Akamai Guardicore

Simplicité et rapidité. Déploiement en quelques jours, et non en plusieurs mois. Notre architecture flexible permet une mise en œuvre rapide sans modification de vos réseaux ou applications, accélérant ainsi votre mise en conformité.

Couverture complète. Bénéficiez d'une stratégie de sécurité unique et cohérente dans tous vos environnements, des systèmes hérités du centre de données aux dernières applications cloud natives.

Plateforme intégrée Zero Trust. Sécurisez l'ensemble de votre écosystème avec une plateforme unifiée. Notre solution repose sur une stratégie de microsegmentation et est renforcée par un **accès réseau Zero Trust (ZTNA)** intégré, l'**authentification multifactorielle (MFA)**, un **pare-feu DNS** et des services proactifs de **recherche des menaces**, afin d'offrir une défense multicouche.

> **Les régulateurs exigent un niveau de sécurité réseau toujours plus élevé, et grâce à la capacité de sécuriser rapidement, de manière granulaire, les applications essentielles que nous avons acquise avec Guardicore, les régulateurs estiment que nous sommes sur la bonne voie.**
>
> — Grande banque européenne

Akamai

Aligner la plateforme Akamai Guardicore sur les cinq piliers de DORA

La plateforme Akamai Guardicore offre une solution complète et pilotée par l'IA qui s'aligne directement sur les exigences fondamentales de la loi sur la résilience opérationnelle numérique.

1. Gestion des risques liés aux TIC

Défi : identification et protection des ressources critiques sur des réseaux « plats » complexes.

Solution Akamai : bénéficiez d'une visibilité complète de l'ensemble des ressources et des flux de données pour cartographier votre surface d'attaque. Utilisez notre **moteur de stratégies génératives basé sur l'IA** pour créer et appliquer des stratégies de **microsegmentation** qui isolent les systèmes critiques et empêchent les mouvements latéraux non autorisés.

2. Gestion des incidents liés aux TIC

Défi : détecter et contenir rapidement les violations afin de minimiser le « rayon de frappe » et l'impact sur l'entreprise.

Solution Akamai : détectez les menaces en temps réel et **mettez instantanément en quarantaine les systèmes compromis** pour empêcher la propagation des ransomware. Comme l'a souligné une banque mondiale après une attaque majeure de la chaîne logistique, « il nous a fallu 10 minutes pour identifier et déconnecter les serveurs concernés ».

3. Tests de résilience opérationnelle digitale

Défi : validation continue des contrôles de sécurité et preuve de la résilience aux auditeurs.

Solution Akamai : testez vos stratégies de **segmentation** et vos plans de réponse aux incidents grâce à la technologie de tromperie intégrée. Générez des rapports de conformité détaillés pour simplifier les audits et démontrer votre stratégie de sécurité.

4. Gestion des risques liés aux TIC par des tiers

Défi : sécuriser la chaîne d'approvisionnement numérique et gérer l'accès des tiers sans leur accorder une confiance excessive.

Solution Akamai : visualisez et contrôlez toutes les connexions tierces. Appliquez l'accès le moins privilégié aux partenaires et aux sous-traitants grâce à nos **solutions ZTNA** et **MFA** intégrées, en veillant à ce qu'ils n'accèdent qu'à ce dont ils ont besoin.

5. Partage d'informations et de renseignements

Défi : exploiter les informations sur les menaces pour se défendre de manière proactive contre les menaces émergentes.

Solution Akamai : intégrez les flux d'informations sur les menaces pour mettre à jour automatiquement les stratégies de sécurité. Bénéficiez de la défense collective du réseau mondial d'informations sur les menaces d'Akamai, qui alimente nos services **Hunt** et de **pare-feu DNS**.

Votre parcours vers la conformité avec DORA commence ici

DORA est l'occasion de construire un avenir financier plus solide et plus résilient. La plateforme Akamai Guardicore peut être votre partenaire de confiance pour y parvenir.

Contactez-nous dès aujourd'hui pour une démonstration personnalisée.

© 2026 Akamai Technologies | Assistance |
| Publication : 26/02