DORA
Digital Operational Resilience Act

Une production : Demey Consulting

Version 1.00 - Octobre 2024

Objectif de la présentation

- Explorer les impacts de la nouvelle réglementation DORA sur les infrastructures de type Messaging, en particulier celles utilisant IBM MQ.

Qu'est-ce que DORA ?

- DORA (Digital Operational Resilience Act) est un règlement européen qui définit un certain nombre d'exigences concernant la cybersécurité et la résilience opérationnelle numérique du secteur financier (mais pas que ...).

Qu'est-ce que DORA ?

- En novembre 2022, le règlement DORA a été adopté par le Conseil de l'Union européenne
  - *règlement 2022/2554 du Parlement européen*
- Ce règlement est entré en vigueur le 16 Janvier 2023
- DORA sera applicable à partir du 17 janvier 2025, ce qui a laissé un délai de 24 mois aux entités concernées de l'U.E. pour se préparer.

Obligations apportées par DORA

- Les entités concernées par ce règlement devront s'assurer de leur capacité à résister, à répondre et à se rétablir face aux perturbations liées aux technologies de l'information et de la communication (TIC).
- Ceci est mis en œuvre via cinq principales obligations :
  - Gestion des risques liés aux TIC
  - Gestion, classification et déclaration des incidents liés aux TIC
  - Test de résilience opérationnelle numérique
  - Gestion des risques liés aux prestataires tiers de services TIC
  - Dispositions relatives à l'échange d'informations

Qui est concerné ?

- Les entités concernées par le règlement DORA sont celles des secteurs Banque, Assurance et Finance, mais également les prestataires de service liés à ces secteurs.
- Notes :
  - Cette notion de "prestataires de service" est à priori relativement explicite, il s'agit des sociétés qui fournissent des services de TIC aux entités concernées.
  - Exemple : Une grande banque française sous-traite à une petite société l'analyse et la validation des documents transmis par les clients (scans de cartes d'identité, de déclaration de revenus, ...)
  - Cette petite société est de facto dans le périmètre DORA.

Conséquences sur les environnements MQ

- Tests de résilience
  - Il faut disposer d'une solution de secours testée
- Risques liés aux prestataires tiers
  - Inventaire
  - Interrogation
  - Contrôle
  - Tests E2E

DORA & IBM MQ

- 3 volets
  - Durcir la configuration sécurité (prévention)
  - « Observer" le fonctionnement (détection)
  - Valider un PRA (remédiation)

Prévention

- Activer les fonctions de sécurité, par exemple :
  - CHLAUTH, MCAUSER
  - TLS avec les liens partenaires : indispensable
  - TLS sur les liens internes : hautement recommandé
- Activer les events MQ
- Backup configurations (MQSC, qm.ini, magasins, ...)
- Architecture HA
- Préparer le PRA

Détection

- Collecter les logs
- Analyse préventive des events MQ & des logs AMQERRxx
- Outils d'observabilité
- Alerting
- Apport de l'IA ?

Remédiation

- Vérification régulière des éléments
  - sauvegardes, binaires, documentation
- Bascule systématique entre les nœuds HA
- Formation des équipes à la reprise
- Tester le PRA global au moins 2 x par an

Merci de votre attention

La formation avec Demey Consulting

- Un organisme de formation déclaré et Datadocké"
- Un catalogue de modules sur WebSphere Application Server et IBM MQ
- Plus de 50 modules MQ disponibles (1500 slides)
- Des supports de cours totalement francisés et au dernier niveau technique (MQ version 9.4.1)
- Des travaux pratiques sur Windows, Linux et iSeries avec les corrigés
- Des filières prédéfinies de 2 à 5 jours, ou à la carte.

https://demey-consulting.fr/formationMQ