KPMG GLD & Associés Monaco

OIV : Votre obligation de fin d'année : Règle 21

■ **ADVISORY** ■ CYBER

■ *Newsletter N°3*

OIV : Votre obligation de fin d'année : Règle 21 - Indicateurs de sécurité

Dans le cadre de la loi 1.435 et de l'arrêté ministériel 2018-1053, notamment, la Principauté de Monaco a établi des mesures rigoureuses pour la protection des systèmes d'information d'importance vitale (SIIV).

Parmi ces mesures, la **règle 21** impose aux opérateurs d'importance vitale (OIV) de mesurer et d'évaluer régulièrement le niveau de sécurité de leurs infrastructures critiques. Cette démarche renforce la transparence et la conformité en matière de cybersécurité tout en incitant les OIV à améliorer leur résilience face aux cybermenaces croissantes.

Une fois par an, **avant la fin janvier**, les OIV communiquent leurs indicateurs mis à jour à l'Agence Monégasque de Sécurité Numérique (AMSN), en utilisant des moyens adaptés pour garantir la confidentialité et la sécurité des données. Cette procédure assure une **transparence accrue** et permet aux autorités de surveiller l'évolution de la sécurité des infrastructures essentielles de la Principauté.

Les Indicateurs de Sécurité

Conformément à cette règle, les OIV doivent renseigner et mettre à jour un ensemble d'indicateurs de sécurité, disponibles via un tableau d'évaluation sur le site de l'AMSN. Ces indicateurs permettent à l'Agence de mesurer dans le temps la conformité des systèmes à l'état de l'art en matière de cybersécurité.

Chaque indicateur est évalué par une échelle à cinq niveaux, du plus faible au plus élevé :

- Non applicable (avec justification requise)
- Mesure documentée ou non mais non appliquée
- Mesure appliquée mais non documentée
- Mesure appliquée et documentée
- Appliquée, documentée et contrôlée

Les indicateurs de ce tableau sont issus de la PSSI de l'état (PSSI-E), et ne sont pas directement applicables aux OIV qui, pour rappel, peuvent disposer de leur propre PSSI. Ceci étant, utiliser la PSSI-E comme étalon de mesure unique permet à l'AMSN de comparer et harmoniser les résultats transmis par l'ensemble des OIV. L'agence peut ainsi comparer les résultats d'année en année et constater des évolutions ou des « anomalies », effectuer des statistiques, définir ses actions, etc.

5 Conseils pratiques pour effectuer votre reporting à l'AMSN

Dans le cadre de la mise en œuvre de la règle 21, KPMG Monaco conseille aux OIV d'être vigilants sur les points suivants :

- **Toujours télécharger le dernier tableau disponible sur le site de l'AMSN :** afin de s'assurer d'avoir la dernière version. Ce dernier peut être modifié d'une année sur l'autre, cela vous évitera de travailler pour rien.
- **Remplir un tableau par Système d'Information d'Importance Vitale (SIIV) :** S'il était possible auparavant de remplir un seul tableau pour l'ensemble des SIIV, l'AMSN souhaite aujourd'hui recueillir un tableau par SIIV pour éviter d'avoir des résultats trop incohérents. Attention : Cela peut considérablement augmenter la charge de travail si vous ne l'avez pas anticipé !
- **Maîtriser le périmètre de l'évaluation** : N'oubliez pas que le périmètre d'évaluation est bien le SIIV. L'appréciation doit porter sur ce périmètre. Bien entendu, il ne faut pas être trop rigide car un SIIV consomme des services communs (Active Directory est un bon exemple) le bon sens s'appliquera pour évaluer certains critères. Documentez votre choix.
- **Converser les preuves de vos évaluations :** Lorsque vous remplissez le tableau des indicateurs, gardez de côté les preuves qui justifient votre évaluation, y compris dans le cas des indicateurs non applicables. En cas de contrôle de l'AMSN, cela vous permettra de ne pas perdre de temps pour retrouver les justifications de vos notations. Cela vous permettra aussi de gagner du temps pour les prochains *reportings* et conserver la cohérence de vos notes d'années en années.

- **Faites-vous accompagner si vous n'êtes pas un expert de la sécurité :** Il est assez compliqué de bien répondre à certaines questions et rester cohérent lorsqu'on n'est pas un expert de la matière, aussi n'hésitez pas à vous faire accompagner pour éviter de mal interpréter certaines questions ou de mal évaluer les indicateurs, qui pourraient surprendre le régulateur ou leur donner des raisons de douter de votre évaluation.

En appliquant ces conseils, vous serez en mesure de maintenir au fil des années une évaluation cohérente et solide vis-à-vis du régulateur. Vous effectuerez aussi cet exercice dans l'esprit pour lequel il a été conçu : faire un point sur la sécurité informatique de vos systèmes sensibles pour la direction et participer à l'évaluation générale de la maturité cyber des OIV en Principauté.

Auteurs

Sabina DEBUSSY

Directeur Associé • Advisory • KPMG Monaco

sdebussy@kpmg.mc

Clément MAILLIOUX

Directeur • Advisory • KPMG Monaco

cmaillioux@kpmg.mc

Contactez-nous

Bettina RAGAZZONI
Associé
bragazzoni@kpmg.mc

Stéphane GARINO
Associé Principal
sgarino@kpmg.mc

Xavier CARPINELLI
Directeur Associé Expertise
xaviercarpinelli@kpmg.mc

Anne Marie FELDEN
Directeur Associé Audit
afelden@kpmg.mc

Sylvie ROTI
Directeur Associé Expertise
sroti@kpmg.mc

Sabina DEBUSSY
Directeur Associé Advisory
sdebussy@kpmg.mc

Patrice DARMON
Directeur Associé Expertise
pdarmon@kpmg.mc

Mélanie LE MOIGN
Directeur Associé Audit
mlemoign@kpmg.mc

Cécile BOZANO-BODIN
Directeur Associé Advisory
cbozanobodin@kpmg.mc

Alain CHARPENTIER
Directeur Associé Audit
acharpentier@kpmg.mc

KPMG GLD & Associés Monaco

2, rue de la Lüjerneta • "Athos Palace" • 98000, Monaco

mc-news@kpmg.mc | www.KPMG.mc | @KPMG_Monaco

+377 977 777 00 | @kpmg-monaco | @KPMGMonaco