ENTRETIEN AVEC UN EXPERT

NIS2 et le nouveau modèle de responsabilité dans la gouvernance des accès

Guido Kraft
Field CISO chez WALLIX

Plus de 20 ans d'expérience en cybersécurité, gouvernance , ISO 27001, TISAX et programmes de sécurité opérationnelle dans des infrastructures critiques et des environnements réglementés.

Q Comment la directive NIS2 transforme-t-elle la relation entre le CISO, la Direction et le Conseil d'Administration ?

Avec NIS2, la cybersécurité cesse d'être uniquement un sujet IT pour devenir un véritable risque métier. La Direction Générale et le Conseil d'Administration sont désormais directement responsables des mesures de cybersécurité et de la résilience de l'organisation.

Cela redéfinit le rôle du CISO, qui devient le lien entre les Opérations Techniques et les décisions stratégiques. Le Conseil d'Administration doit également jouer un rôle de supervision active, comprendre les risques cyber et poser les bonnes questions.

Q Pourquoi la gouvernance des accès prend-elle autant d'importance avec NIS2 ?

Pratiquement tout dans les environnements IT et OT repose sur les accès. Le risque apparaît lorsque les utilisateurs disposent de privilèges supérieurs à leurs besoins réels ou lorsque les autorisations ne correspondent pas à leurs responsabilités opérationnelles.

La gouvernance des accès définit qui peut accéder à quoi, dans quelles conditions et avec quel niveau de responsabilité. Les organisations doivent donc la considérer comme une couche stratégique renforçant à la fois la sécurité et la conformité réglementaire.

ENTRETIEN AVEC UN EXPERT

wallix

Quels freins limitent une gouvernance des accès plus robuste dans le secteur public ?

Les principaux freins restent les systèmes hérités, les environnements segmentés et les budgets limités.

Même si de nombreuses applications anciennes ne supportent pas les modèles modernes de gestion des accès, les organisations peuvent renforcer le contrôle grâce à la gestion des accès à privilèges, à l'authentification avancée et à des accès auditables.

Pourquoi les comptes administrateurs partagés restent-ils aussi répandus ?

Les comptes partagés restent fréquents à cause des systèmes existants et des contraintes opérationnelles.

Lorsque cela est possible, les organisations devraient privilégier les comptes individuels. Sinon, des contrôles d'accès à privilèges permettent de renforcer la traçabilité et le contrôle.

Les organisations devraient-elles aborder NIS2 sous l'angle de la conformité ou de la résilience ?

La meilleure façon d'aborder NIS2 est de la considérer comme une opportunité d'améliorer la résilience opérationnelle, et non simplement comme une obligation de conformité.

Lorsqu'une organisation améliore sa visibilité, sa gouvernance des accès et sa discipline opérationnelle, la conformité devient naturellement la conséquence de contrôles plus efficaces.

Comment les organisations devraient-elles équilibrer prévention et investigation après incident dans le cadre de NIS2 ?

La prévention et l'investigation sont tout aussi essentielles.

Les organisations doivent réduire les risques tout en conservant une visibilité complète sur les accès, les actions réalisées et les systèmes concernés en cas d'incident.

À quoi devrait ressembler une bonne gestion des accès tiers sous NIS2 ?

Les accès des tiers doivent être gérés avec le même niveau d'exigence que les accès à privilèges internes.

Une bonne pratique consiste à garantir des accès contrôlés, limités dans le temps, surveillés et totalement traçables. Les organisations doivent éviter les accès externes sans supervision, les privilèges permanents accordés aux prestataires et les comptes distants génériques.

Quel pourrait être le prochain grand chantier réglementaire européen en cybersécurité ?

Le prochain grand sujet sera probablement la gouvernance de l'intelligence artificielle.

À mesure que l'IA s'intègre davantage dans les opérations métiers, les organisations auront besoin de politiques plus claires concernant l'usage des données, la responsabilité, la gestion des risques et la conformité réglementaire.