Risk'n tic

Simple Risk Management Solution

LABEL EBIOS RISK MANAGER ANSSI

La cyber sécurité est devenue un enjeu majeur pour toutes les entreprises, mais aussi pour les collectivités territoriales, la santé, la défense, la finance etc…

Des contraintes réglementaires La directive NIS et le RGDP imposent dorénavant la mise en œuvre de la sécurité du SI, avant il n'y avait que le bon sens.

La gestion des risques est au cœur de ces 2 règlements, la gestion des risques est un élément essentiel pour rappeler à tous que la Sécurité est au service des métiers et non l'inverse.

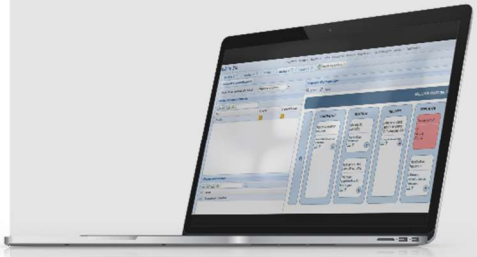
Au regard de la complexité du SI, de son ouverture vers l'extérieur avec à la fois le nomadisme (post covid) et la mise en nuage de nos SI, comment avoir une approche efficace, simple, pragmatique ?

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), rattachée au 1er Ministre a fait appel à des éditeurs pour créer des outils conformes à la méthodologie EBIOS RISK MANAGER.

Cette nouvelle méthodologie répond aux exigences de l'Etat dans sa stratégie de souveraineté et de sécurité nationale.

Fonctionnalités

- Etude Ebios Risk Manager
- Etude rapide
- Préqualification d'un projet
- RGPD
- Registre des incidents
- Rapports dynamiques



Pour une approche pragmatique et industrialisée de la Cyber Sécurité, dans un cycle vertueux d'amélioration continue.

Sur le terrain le Responsable de la sécurité des systèmes d'informations (RSSI) a d'autres besoins, c'est pourquoi nous avons intégré mais surtout enrichi la méthodologie pour répondre au besoin métier dans une approche globale du management des risques.

Une première étape simple permet d'identifier les écarts avec l'état de l'art en termes d'architecture, d'administration du SI, de nomadismes, etc… et d'identifier rapidement les mesures qui permettent d'améliorer le niveau de sécurité des acteurs publics ou privés.

Des rapports Analytiques facilitent le suivi dans le temps de l'avancée de mise en œuvre des mesures de sécurité, et de communiquer vers les clients, partenaires, autorités de tutelles, direction…

Nous avons également conservé une approche ISO 27005, tout aussi adaptée, en intégrant le parcours d'un attaquant pour atteindre ses objectifs (Cyber Kill Chain).

Une vue consolidée des risques là encore permet de communiquer vers les branches métiers, la direction de manière compréhensible. Cette vision permet d'obtenir une cotation de l'entreprise sur sa couverture des risques Cyber pour ses parties prenantes (assurance, client, partenaires…).

https://riskntic.com/

@ Christophe.delpierre@riskntic.com