

Guides de maturité pour éditeurs de services numériques

05 septembre 2023, 17:02

Tatiana Galibus

Comment être prêt pour la directive NIS 2 ?

Ce n'est un secret pour personne que la nouvelle directive NIS 2 aura d'importantes conséquences pour les éditeurs de services numériques. Selon cette nouvelle règlementation, beaucoup de fournisseurs numériques et data centers seront considérés comme des entités dites essentielles ou importantes. Les exigences seront plus strictes pour quasi tout le monde : dès lors qu'un fournisseur de service aura un client important relevant de la règlementation NIS, il devra systématiquement démontrer sa fiabilité, répondre aux questions sur la sécurité et mener un audit. Les éditeurs de logiciels, y compris les start-ups et scale-ups, doivent se renseigner au sujet de la règlementation, et d'ailleurs leurs clients les pressent souvent de le faire.

Quelles normes sont applicables en Belgique ?

La directive NIS 2 ne donne pas de consignes détaillées aux entreprises. Les États-membres transposent les règles générales selon leur propre situation de façon à garantir la conformité. En Belgique, ce travail est mené par le Centre pour la Cybersécurité Belgique (CCB) dans le cadre du

Cyberfundamentals framework. Celui-ci est assez général : bien qu'adapté aux PME, il ne s'adresse pas spécifiquement aux éditeurs de logiciels, développeurs, testeurs, data centers, éditeurs de services numériques, etc.

Quelles normes de cybersécurité s'appliquent aux éditeurs de logiciels ?

La bonne nouvelle est qu'il existe un ensemble d'outils et de directives à la fois reconnu et bien défini en matière de cybersécurité. Il est soutenu par l'Open Web Application Security Project (OWASP), une fondation à but non lucratif qui œuvre à l'amélioration de la sécurité des logiciels. Le projet OWASP fournit et développe une série de normes clés destinées aux entreprises numériques.

Pourquoi les éditeurs de logiciels devraient-ils tenir compte de ces normes ? Parce qu'elles sont exploitables, compréhensibles, pratiques et largement adoptées par les experts en sécurité des éditeurs de logiciels.

- OWASP ASVS
- OWASP DSOMM
- OWASP SAMM

La norme ASVS d'OWASP

L'Application Security Verification Standard (ASVS) d'OWASP fournit une liste d'exigences de base pour garantir la sécurité des développements. Nous recommandons cette norme pour les développeurs et testeurs. L'ASVS propose trois niveaux de maturité :

NIVEAU	POUR QUI ?
ASVS Niveau 1	Niveau d'assurance basique nécessitant peu d'interaction entre l'assesseur et les co mise en œuvre.
ASVS Niveau 2	Niveau d'assurance pour la majorité des applications qui impliquent des données sen
ASVS Niveau 3	Niveau réservé aux applications les plus critiques, nécessitant une étroite collaboratio concepteurs de l'application.

Modèle DSOMM d'OWASP

Le modèle de maturité DevSecOps (DSOMM) d'OWASP fournit des outils pour renforcer et prioriser les stratégies DevOps. Il définit des niveaux d'exigences et de mise en œuvre pour les pipelines d'automatisation, l'édition de logiciels et le renforcement des infrastructures. Nous recommandons cette norme pour les opérateurs d'automatisation, les testeurs, les conseillers en infrastructure et les chefs de projet. Le DSOMM propose cinq niveaux de maturité (nous présentons les trois premiers) :

NIVEAU	POUR QUI ?	CONTRÔLES
DSOMM Niveau 1	Compréhension basique des pratiques de sécurité	23 contrôles
DSOMM Niveau 2	Adoption des pratiques de sécurité	47 contrôles
DSOMM Niveau 3	Adoption poussée des pratiques de sécurité	45 contrôles

Modèle SAMM d'OWASP

Le modèle de sécurité Software Assurance (SAMM) donne un cadre ouvert destiné à aider les organisations à formuler et mettre en œuvre une stratégie de sécurisation des logiciels personnalisée, basée sur les risques spécifiques auxquels fait face l'organisation. Il aide les organisations à évaluer leurs pratiques de sécurisation des logiciels existantes et à élaborer un programme équilibré d'assurance de la sécurité des logiciels.

Nous recommandons cette norme pour les directeurs généraux, chefs de projet et propriétaires de projet. La fondation du modèle s'appuie sur les fonctions opérationnelles basiques du développement de logiciels, avec des pratiques de sécurité associées à chacune d'entre elles (voir diagramme ci-dessous). Le modèle compte trois niveaux de maturité pour chacune des douze



Sirris vous soutient

Le **18 octobre 2023**, Sirris organise **une session d'échange d'avis d'experts, axée sur la directive NIS 2** et d'autres futurs besoins en cybersécurité pour les services numériques. La session est entièrement gratuite. Durant cette réunion en ligne, vous écouterez l'avis de plusieurs experts sur les nouvelles réglementations et les défis en matière de cybersécurité, et vous échangerez avec les anciens participants à notre master class au sujet de leurs parcours vers la maturité en cybersécurité.

Inscrivez-vous ici.

Cette session marquera aussi le démarrage de notre **Formation intensive en cybersécurité destinée aux services numériques et SaaS** (logiciels en tant que services). Financée par le VLAIO pour les entreprises flamandes, cette formation est conçue comme un parcours de formation incluant un enseignement théorique poussé et des sessions pratiques sur mesure. Nous

réalisons cette formation en partenariat avec des fournisseurs de cybersécurité de toute la Flandre de façon à pouvoir vous proposer le meilleur des leçons apprises, des moments de networking et des sessions individuelles de micro-coaching pour aborder vos questions personnelles.

Pour en savoir plus sur notre formation intensive et vous inscrire, consultez notre agenda !

Auteurs



Tatiana Galibus