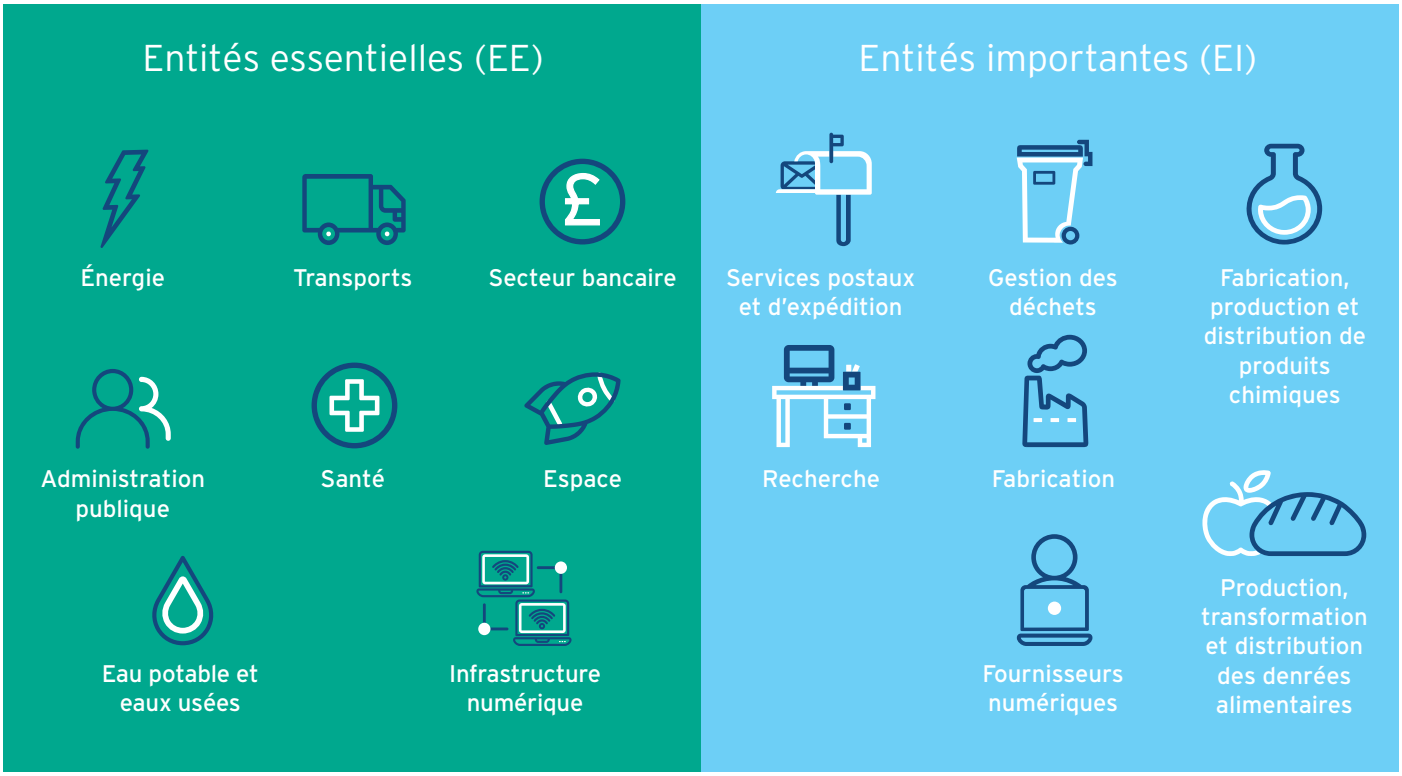
Comment une gestion globale des actifs matériels aide à se conformer aux nouvelles règles de la Directive NIS2

Les entreprises des 27 états membres de l'union européenne s'activent pour se conformer aux nouvelles règles visant à **renforcer et à affiner les bonnes pratiques en matière de cybersécurité**. La Directive 2 sur la sécurité des réseaux et des systèmes d'information (NIS2) est fondée sur des principes solides de gestion du cycle de vie des actifs informatiques.

Extension de la directive NIS de 2016, la Directive NIS2 ajoute des spécificités en tenant compte des vulnérabilités apparues lors de la pandémie de COVID-19. Elle étend la couverture à un plus grand nombre d'entreprises et opère un distinguo entre les « entités essentielles » et les « entités importantes ».

Fournisseurs de services fondamentaux pour la santé publique, la sécurité et le commerce, les entités essentielles comprennent notamment les fournisseurs d'énergie, les sociétés de transport, les établissements de services financiers et les prestataires de santé. Les entités importantes fournissent, pour leur part des services moins critiques mais néanmoins nécessaires pour la santé économique et sociale. Ces deux catégories d'entités sont assujetties aux règles de la Directive NIS2, même si les sanctions diffèrent en fonction du type d'organisation. Les entreprises en dehors de l'UE qui travaillent sur le territoire européen sont assujetties à ces nouvelles règles.



Au carrefour de la gestion des actifs de cybersécurité (CSAM) et de la gestion des actifs matériels (HAM)

La gestion des actifs de cybersécurité, ou CSAM, consiste à identifier les actifs de l'entreprise (actifs matériels, logiciels, données et services Cloud), à en établir l'inventaire, à les superviser, à les gérer et à les suivre pour savoir ce qu'ils font et détecter toute faille au niveau des protections de cybersécurité. Pour le matériel informatique tel que les équipements d'extrémité et l'infrastructure IT sur site, cela implique de connaître la valeur, l'emplacement et la vulnérabilité de chaque actif.

Cette approche de la gestion de bout en bout du cycle de vie des actifs IT matériels de l'entreprise optimise l'utilisation des équipements tout en réduisant les coûts et les risques associés.

En renforçant les processus de gestion du cycle de vie des actifs IT, les entreprises peuvent améliorer leur conformité et leur position globale en matière de cybersécurité. Avant de commencer, il est indispensable de définir un plan et une stratégie clairs. Les intersections entre les règles de la Directive et la gestion du cycle de vie des actifs sont les suivantes :

1. Sécurité de la chaîne logistique : atténuation des risques liés aux tiers

La pandémie a mis en lumière de nombreuses lacunes graves au niveau de la sécurité de la chaîne logistique. Certaines entreprises ont découvert qu'elles ne connaissaient pas tous les acteurs de leurs chaînes logistiques et qu'elles disposaient de peu d'informations sur leurs pratiques de sécurité.

Exigence NIS2 : Les entreprises doivent évaluer les risques de cybersécurité que posent leurs fournisseurs et prestataires de services en étudiant leurs pratiques en matière de sécurité, leurs protocoles de réponse aux incidents et les vulnérabilités de leurs systèmes. Les entités concernées doivent déployer de puissants protocoles de sécurité qui couvrent tous les aspects de leurs interactions avec leurs fournisseurs, procéder à une évaluation complète des risques et réaliser des audits pour s'assurer que les mesures de sécurité des fournisseurs qu'ils ont évaluées sont en phase avec leurs propres normes de sécurité.

> Les entreprises doivent évaluer les risques de cybersécurité que posent leurs fournisseurs et prestataires de services

Bonne pratique en matière de gestion du cycle de vie des actifs : Le déploiement de protocoles de gestion des risques fournisseurs pendant la phase d'approvisionnement et le contrôle régulier de leurs pratiques garantissent le respect des protocoles de sécurité de l'acheteur. Les contrats doivent préciser les mesures de sécurité que les fournisseurs doivent prendre et définir les attentes en matière de protection des données et de signalement des incidents. Les fournisseurs doivent accepter de se soumettre à des audits réguliers pour vérifier leur conformité. Tout doit être fait notamment pour comprendre les types de certifications et d'accréditations attribués au fournisseur qui apportent une validation tierce comme quoi les services fournis respectent bien les normes. Par exemple, il peut s'agir d'une certification NAID AAA décernée par i-SIGMA, ISO 9001 et ADISA.

Adéquation : Une solide stratégie de gestion du cycle de vie des actifs intègre naturellement la sécurité de la chaîne logistique. Elle commence par évaluer les risques de la chaîne logistique et par collecter des informations sur la chaîne de traçabilité des partenaires tiers. Des règles sont créées pour l'habilitation des fournisseurs, notamment en termes de sécurité tout au long du processus de passation de contrat et d'approvisionnement et de stratégies de réponse en cas de violation ou d'interruption. Une supervision et des tests continus réduisent sensiblement le risque de vulnérabilité des systèmes.

2. Sécurisation de l'acquisition, du développement et de la maintenance des actifs informatiques

Exigence NIS2 : Les entreprises doivent prendre des mesures pour garantir la sécurité tout au long du cycle de vie des réseaux et des systèmes d'information, de l'achat à la maintenance en passant par le développement et le déploiement.

Bonne pratique en matière de gestion du cycle de vie des actifs : La gestion du cycle de vie des actifs donne la priorité à la sécurité des données tout au long du cycle de vie des actifs, depuis leur stockage, leur déploiement et leur récupération sécurisés jusqu'à leur redéploiement et leur élimination sécurisée en passant par l'effacement des données qu'ils stockent. Sont concernées les procédures portant sur la régulation de l'accès aux zones de stockage, sur l'inspection des équipements pour vérifier d'éventuelles vulnérabilités avant le déploiement, sur le marquage et le traçage des actifs en service, selon un processus rigoureux d'application de correctifs et de mises à jour et de nettoyage des matériels identifiés comme devant être éliminés ou réutilisés. Le suivi et le signalement en temps réel d'un actif constituent une fonctionnalité importante pour la circulation des actifs. La sécurité des données et la prise en charge des actifs doivent être assurées par le suivi et le signalement qui sont au cœur de la prise de décision et des exigences de conformité.

Adéquation : La gestion du cycle de vie des actifs applique des pratiques de cybersécurité qui répondent à toutes les exigences de la Directive NIS2. Cette dernière oblige également à préparer un plan de réponse aux incidents qui définit les grandes lignes des procédures pour traiter rapidement les vulnérabilités et réagir aux interruptions de service.

3. Formation de base à la cyberhygiène et à la cybersécurité

Exigence NIS2 : Les entreprises doivent prendre des mesures techniques et organisationnelles appropriées pour gérer les risques de cybersécurité, notamment via des pratiques de cyberhygiène de base et des programmes de formation adaptés aux responsabilités spécifiques des employés.

Bonne pratique en matière de gestion du cycle de vie des actifs : Les utilisateurs doivent être formés aux bonnes pratiques pour une manipulation sûre et sécurisée des équipements IT de l'entreprise, en l'occurrence ne pas laisser des actifs sans surveillance et suivre des protocoles de restitution de ces équipements. L'équipe IT chargée de la gestion des actifs de l'entreprise doit être formée aux obligations de l'entreprise en matière d'effacement des données certifié entre les déploiements et lors de l'élimination d'un équipement en fin de vie. L'équipe IT doit tenir un inventaire général de l'ensemble des actifs, dont leur statut, localisation et conformité aux mesures de prévention. L'audit de l'inventaire est généralement pratiqué sous deux formes. L'approche « complète » est un effort intense visant à identifier tous les actifs en une seule fois tandis que l'approche « par roulement » permet d'auditer les actifs dans le cadre de différents projets et domaines et convient mieux aux grandes entreprises. Dans les deux cas, un audit physique des actifs IT doit être réalisé en continu pour des questions de sécurité et de gestion des actifs.

Adéquation : Une bonne stratégie de gestion du cycle de vie des actifs intègre l'élément humain à la cybersécurité, sachant que la plupart des violations sont dues à des erreurs humaines. La formation des employés aux bonnes pratiques leur permet de devenir la première ligne de défense contre les cybermenaces. Les contraintes qui exigent un effacement certifié des données stockées sur les actifs assurent la cybersécurité jusqu'à la fin de vie utile.

4. Gestion des risques et continuité de l'activité

Exigence NIS2 : La gestion des risques est au cœur de la nouvelle directive. Les équipes de gestion doivent maîtriser la pratique de l'évaluation des risques et appliquer des mesures pour minimiser les risques liés aux opérations continues. Au-delà des trois mesures évoquées ci-dessus, il s'agit de processus établis pour documenter et signaler les principaux incidents sous 24 heures. Un plan de continuité de l'activité doit être développé pour assurer la poursuite des opérations, y compris en cas d'incidents majeurs.

Bonne pratique en matière de gestion du cycle de vie des actifs : La gestion du cycle de vie des actifs prend racine dans la gestion des risques. Après la phase de création de procédures et de politiques, les priorités sont fixées en fonction de l'évaluation des risques pour l'entreprise. Les risques liés à l'achat et au déploiement des actifs sont intégrés au processus d' approvisionnement. Les évaluations des risques permettent de déterminer la fréquence et l'étendue des activités de maintenance. Les mises à niveau, les modifications et la mise au rebut des équipements obsolètes sont principalement décidées en fonctions des risques identifiés. Dans une perspective de gestion des risques, il est indispensable que les données soient effacées et qu'un certificat d'effacement des données (COD) soit remis lorsque les actifs sont revendus pour récupérer une partie de leur valeur. La récupération de valeur obtenue de la revente joue un rôle important pour optimiser la valeur d'un actif. Cependant, il faut avoir l'assurance que l'effacement irrémédiable des données appartenant au premier propriétaire a été vérifié, ce que certifie l'attestation.

Adéquation : Les principes de gestion des risques intégrés aux bonnes pratiques de gestion du cycle de vie des actifs s'alignent directement sur les exigences définies dans la Directive NIS2.

Réflexion finale

La Directive NIS2 et la gestion du cycle de vie des actifs partagent le même objectif, à savoir renforcer la cybersécurité organisationnelle en lien avec le suivi, le traitement et la destruction des actifs IT matériels. Les entreprises qui appliquent de bonnes pratiques de gestion des actifs matériels (HAM) sont mieux placées pour se conformer aux réglementations et pour protéger leur infrastructure IT, leurs données et leurs opérations. À l'ère de la Directive NIS2, une stratégie bien définie de gestion du cycle de vie des actifs qui donne la priorité à la visibilité de la chaîne logistique, à des pratiques d'acquisition et de configuration sécurisées ainsi qu'a l'élimination responsable des actifs IT est incontournable pour une cybersécurité efficace.

0800 215 218 | ironmountain.com/fr-fr

À propos d'Iron Mountain

Fondée en 1951, l'entreprise Iron Mountain Incorporated (NYSE : IRM), est le spécialiste mondial des services de conservation et de gestion de l'information. Avec plus de 225 000 entreprises qui lui font confiance à travers le monde et des installations dont la surface cumulée atteint plus de 9,1 millions de m2 sur plus de 1 400 sites répartis dans plus de 60 pays, Iron Mountain conserve et protège des milliards d'actifs de valeur, y compris des documents vitaux pour l'activité de l'entreprise, des données hautement sensibles ainsi que des artefacts culturels et historiques. Proposant des solutions de conservation sécurisée, de gestion de l'information, de transformation numérique, de destruction sécurisée ainsi que des services de data center, cloud et de stockage d'œuvres d'art et de logistique, Iron Mountain aide ses clients à réduire les coûts et les risques, à se conformer à la réglementation, à faciliter la reprise après un sinistre et à adopter un mode de travail plus numérique. Pour en savoir plus, rendez-vous sur www.ironmountain.com/fr-fr.