EUROPEAN
RENTAL
ASSOCIATION

SYNTHESE

Guide ERA sur les principales initiatives en matière de cybersécurité dans le secteur de la location d'équipements

Cybersécurité : êtes-vous armé pour le défi ?

L'une des plus grandes menaces du secteur de la location d'équipements réside en la vulnérabilité de nos entreprises en matière de cybersécurité. En 2021, il n'existe pas de feuille de route établie dans notre secteur, qui permette à une entreprise de location d'équipements d'évaluer sa situation en matière de cybersécurité et d'identifier les mesures qu'elle peut adopter. L'objectif de ce guide est de définir la portée des interventions de cybersécurité à l'échelle de l'entreprise, d'identifier les éléments essentiels d'une stratégie réussie, y compris les facteurs spéciaux pouvant avoir un impact sur les sociétés de location, et de présenter les principales mesures adoptées aujourd'hui par les leaders de notre secteur. Ce guide a été réalisé avec l'aide inestimable et les contributions des sociétés membres de l'ERA.

Les menaces actuelles en matière de cybersécurité et « l'appel à l'action »

Ce guide explique comment le secteur de la location d'équipements en Europe est confronté à un défi sans précédent du fait des menaces que représentent les vulnérabilités et les expositions des technologies de l'information dans nos activités, et en particulier comment les clients sont de plus en plus exigeants envers nous en matière de protection de la cybersécurité. Le secteur est dans une phase de consolidation, les petites entreprises fusionnant avec d'autres pour atteindre une certaine échelle, les grandes entreprises rachetant les plus petites pour accéder à de nouveaux marchés, se consolider ou gagner des parts de marché. Le secteur de la location d'équipements est en pleine « numérisation ». Plus de présence en ligne implique davantage de menaces de la cybersécurité. L'équipement de location devient de plus en plus intelligent et connecté aux réseaux, ce qui peut constituer un canal pour une attaque. Les sociétés de location d'équipements qui ont subi un accident important ont l'impression d'avoir exposé leur activité, leur réputation et, plus important encore, leurs clients et leurs parties prenantes à des risques. La législation européenne devient de plus en plus exigeante et le guide traite des développements les plus récents de la directive Network and Information System Security (NIS). Le secteur a maintenant besoin d'une communauté d'entreprises européennes collaborant en permanence sur les meilleures pratiques en matière de cybersécurité, les menaces communes et les problèmes rencontrés par toutes les organisations.

Exigences de la cybersécurité en matière de budget et d'investissements

Ce guide indique les investissements et les coûts d'une cybersécurité digne de ce nom. Il présente une échelle d'investissement et de « maturité » indiquant l'investissement initial nécessaire pour mettre en place les mesures de base. Une bonne cybersécurité requiert un investissement conséquent et doit être réévaluée tous les ans. L'investissement direct dans la cybersécurité dans l'ensemble des secteurs est estimé à 5 % environ des dépenses informatiques, voire plus au départ. Les leaders montrent également que le principal investissement est constitué par les coûts indirects et intangibles de la « conception », de la gestion et de l'intégration de la sécurité dans l'ensemble des activités, lesquels peuvent finalement être plus élevés que les coûts directs.

Feuille de route des principales mesures et « liste de contrôle »

L'intervention en matière de cybersécurité est souvent axée sur la technologie et les systèmes, mais de nombreux risques trouvent leur origine dans le comportement humain, la robustesse des processus et du suivi, ainsi que dans le signalement et la réaction au sein de l'entreprise. Selon les leaders de la location d'équipements, une organisation doit adopter une stratégie à l'échelle de l'entreprise pour garantir la prise en compte de tous les points faibles. Chaque organisation fait face à différents risques, a des activités et des lacunes différentes, mais les

leaders considèrent qu'une liste de contrôle permettant une vue d'ensemble complète peut être réalisée à partir de quatre éléments couvrant le processus, le personnel, la technologie et l'infrastructure. Ce guide les analyse et présente les exigences principales à chacun des trois niveaux suivants : « niveau de base », « maturation » et « leader ». Une liste de contrôle incluse indique l'évaluation des risques et des vulnérabilités avec les niveaux actuels de maturité dans l'entreprise afin d'aider à planifier et à réduire les risques.

« Vous obtenez ce que vous mesurez... » Les leaders indiquent qu'il est essentiel de s'assurer que les principaux domaines de performance ayant un impact sur la cybersécurité sont mesurés à l'aide d'indicateurs clés de performance (ICP). Le plan d'action dans ce guide indique également les mesures et les systèmes de mesure des performances généralement utilisés aujourd'hui par les entreprises leaders pour chacun des éléments.

Illustration des principales initiatives

Ce guide illustre ensuite certaines des principales initiatives utilisées aujourd'hui pour chacun des quatre éléments. Les leaders soulignent que, même si un plan de sécurité exhaustif constitue une part essentielle d'une stratégie globale, un plan global n'est pas nécessairement la toute première étape. Un plan complet passe généralement par différentes étapes de maturité. Les principales caractéristiques incluent :

- **Processus** : Les leaders soulignent que, dans un premier temps, il est plus important de prendre des mesures pour identifier toutes les zones à risque élevé dans l'entreprise et de donner la priorité aux actions visant à combler ou à corriger les vulnérabilités. Une analyse exhaustive des risques dans chacun des domaines principaux de ce guide peut être un bon point de départ. Lorsque les zones à risque élevé sont traitées, il est possible de passer aux zones à risque moyen. Il convient de souligner que les recherches indiquent que, à partir d'un niveau de base, passer à la couverture de toutes les zones à risque élevé peut représenter un processus de trois à cinq ans, exigeant du matériel et un investissement conséquent. Les leaders préconisent un parcours de type basique, meilleur, optimal pour parvenir à une sécurité adaptée, qui peut utiliser des accréditations officielles comme jalons ou être réalisé sur mesure en interne et suivre les mêmes principes. Plusieurs cadres internationaux utilisés sont mis en évidence.

- **Personnel :** *La cybersécurité ne concerne pas que le service informatique...* Le service de gestion des ressources humaines (RH) joue un rôle important dans la garantie de la cybersécurité. L'intervention et le soutien des RH dans les entreprises leaders s'étend à l'ensemble de l'entreprise, à travers la conception et le développement de politiques ainsi que de procédures (y compris le RGPD et les protocoles de protection des données) et leur communication à l'ensemble du personnel, l'adaptation des conditions d'emploi et des descriptions des rôles pour inclure les responsabilités en matière de données et de sécurité, la sensibilisation et la formation aux impératifs de cybersécurité ainsi que l'analyse des besoins en formation pour les rôles de première ligne et le personnel de sécurité spécifique. Il est essentiel d'utiliser des moyens de communication comme les newsletters ou les publications sur les réseaux sociaux pour informer l'ensemble de l'entreprise sur les dernières tendances ou menaces.

- **Technologie :** Les outils des technologies d'information continuent à se développer rapidement et représentent un puissant moyen d'action contre la cybercriminalité, pour un « avertissement précoce » et l'interception de menaces. La surveillance des menaces et de l'état du système est facilitée par la technologie, avec des systèmes avancés comme « Splunk » et « MS Azure Sentinel », illustrés en action. Il est crucial d'établir un « COS » (centre des opérations de sécurité) afin d'obtenir le maximum des systèmes automatisés. Les leaders peuvent s'appuyer sur un COS interne, souvent assisté par des centres tiers pouvant offrir une assistance 24 h/24 et des services avancés de surveillance et de gestion.

- **Infrastructure :** *« Si le pire se produit, malgré les meilleures mesures de prévention, vous devez avoir un plan de gestion des incidents à disposition. »* Les attaques peuvent avoir de nombreuses formes, mais l'un des types les plus dangereux est ce qu'on appelle un « rançongiciel ». Dans une situation de déni de service, une réponse d'urgence immédiate est nécessaire, mais un processus doit avoir été mis en place pour évaluer et « catégoriser » la situation. Ce guide illustre la manière dont les leaders analysent et réagissent. En outre, il fournit un modèle des « 48 heures après incident » pouvant aider à planifier la période de gestion de crise qui

suit immédiatement un événement de déni de service ou une autre menace majeure.

Préparation d'un futur sûr

La lutte pour obtenir une sécurité informatique adéquate reste constante mais, afin d'avoir une longueur d'avance, les leaders soulignent que les sociétés de location d'équipements doivent :

1. *Connaître leurs ressources, leurs points forts et leurs points faibles*
2. *Effectuer une évaluation des risques*
3. *Planifier et investir de manière adéquate*
4. *Se préparer au pire*
5. *Se tenir au courant et progresser*

Le guide ERA sur les meilleures pratiques en matière de cybersécurité vise à aider les entreprises de location d'équipements de tous types et de toutes tailles à planifier, développer ou améliorer en permanence leur cybersécurité.