

Une cybersécurité parée pour l'avenir, même pour les PME !

14 septembre 2021, 02:00

Annanda Rath
Tatiana Galibus

À l'heure de la transformation numérique et d'Industrie 4.0, la cybercriminalité n'a jamais été aussi réelle pour les PME belges. Toute entreprise qui n'est pas assez résiliente sur le plan de la sécurité est une victime potentielle. Les PME ont besoin d'une stratégie sur mesure et d'une feuille de route claire pour se protéger aujourd'hui et à l'avenir. Sirris et Agoria répondent à ces attentes avec une nouvelle approche adaptée aux PME !

Maintenant que les grandes entreprises ne sont plus ses seules cibles, la cybercriminalité n'a jamais été aussi réelle pour les PME belges. On recense actuellement plus de 30 000 cyberattaques, avec une augmentation annuelle de 20% du nombre d'incidents. La transformation numérique et Industrie 4.0 représentent un grand risque pour les entreprises. Les machines obsolètes sont en effet associées à un risque de sécurité élevé et les données sont collectées et échangées entre les sites web sans le moindre contrôle. Toute entreprise qui n'est pas suffisamment résiliente sur le plan de la sécurité peut donc être victime de la cybercriminalité. Les conséquences des violations de la sécurité (interruption des activités, perte de données et atteinte à la réputation) peuvent miner une entreprise et ont souvent des conséquences majeures à court et à long terme.

Pour se protéger contre ces attaques, les PME de différents secteurs doivent avoir leur propre approche. C'est ce que Sirris et Agoria ont mis sur pied dans une large offre d'ateliers très ciblés et pratiques, adaptés au groupe cible, au secteur et au type d'entreprise.

De l'accueil à l'analyse de la cybersécurité

Sirris a mis au point une nouvelle approche flexible de la cybersécurité afin d'aider les PME à réaliser leur stratégie de cybersécurité sans investir trop d'efforts et de ressources financières. Nous commençons par une **séance d'accueil en ligne gratuite d'une heure**. Au terme de cette session, nous fournissons un rapport structuré mentionnant les problèmes déjà détectés et nous prodiguons des conseils sur la façon d'aborder ces problèmes. L'entreprise peut immédiatement commencer à améliorer sa cybersécurité globale en se basant sur la ou les recommandations de ce document.

Si l'entreprise veut aller un peu plus loin et souhaite un **examen plus approfondi de la cybersécurité**, nous nous rendons sur place et nous examinons tous les points individuels de manière beaucoup plus détaillée, sur la base des résultats des examens de sécurité et d'entretiens. Le résultat de cette analyse fournit un tableau structuré des actifs, des vulnérabilités

et des risques. Il est ainsi plus facile pour l'entreprise de décider des prochaines étapes et des priorités pour une cybersécurité plus résiliente.

Vous trouverez plus d'informations sur cette approche [ici](#).

Des ateliers pour chaque type d'entreprise, quel que soit son secteur

Vous cherchez des conseils et astuces concrets en matière de cybersécurité ?

Nous vous aidons à éviter un blocage numérique de votre entreprise (ou pire encore) au cours de la [masterclass très pratique et pragmatique « La cybersécurité en 30 mesures »](#). Nous discutons d'une approche basée sur les risques, qui devrait constituer une base fondamentale pour chaque entreprise, en nous concentrant sur la cybersécurité de ses ressources internes. Nous vous expliquerons 30 mesures réalisables et immédiatement applicables, qui vous permettront d'améliorer sensiblement la cybersécurité dans votre entreprise. En appliquant correctement ces 30 mesures, vous atteindrez déjà un très bon équilibre entre le risque encouru et l'investissement consenti dans la cybersécurité.

Pour une entreprise manufacturière, comment s'y retrouver dans la cybersécurité ?

Pour nombre d'entreprises de production, la cybersécurité est un thème très complexe. Les failles de cybersécurité peuvent entraîner des pertes de données et d'argent, une baisse de fiabilité et une réputation ternie. Le [webinaire « La cybersécurité pour les entreprises manufacturières »](#) présente les solutions de cybersécurité les plus importantes et explique les meilleures pratiques pour améliorer la cybersécurité dans l'industrie manufacturière, tant du point de vue des technologies de l'information que de celui des ateliers connectés. Le webinaire se concentre sur des solutions pragmatiques simples qui sont également réalisables pour les PME.

La [masterclass « La cybersécurité pour les entreprises manufacturières »](#) vous apprendra comment progresser en toute sécurité vers Industrie 4.0 grâce à une feuille de route exécutable, étape par étape, qui mène à une cybersécurité résiliente. Nous vous fournissons les connaissances dans un format pratique et pragmatique afin de vous donner une compréhension approfondie de tous les aspects de sécurité de votre transition vers Industrie 4.0.

Sur la base des résultats de l'étude « [La sécurité industrielle dans l'industrie manufacturière](#) », Sirris et Agoria ont décidé de réunir des entreprises manufacturières au sein d'un [réseau d'apprentissage consacré à la cybersécurité dans les technologies d'exploitation](#), et plus particulièrement à la capacité à détecter les menaces et les anomalies dans l'environnement de production. En effet, l'amélioration significative des capacités de détection est dans de nombreux cas l'un des moyens les moins invasifs d'accroître sensiblement la cyberrésilience de l'environnement de production.

Comment survivre aux évaluations de sécurité pour une start-up ou une scale-up numérique ?

Vous travaillez dans une start-up ou une scale-up ? Après des mois de démonstrations, vous avez reçu des avis négatifs de la part d'évaluateurs TPSA au sein d'une grande entreprise ? La gestion des risques et la « décision de confiance » interviennent trop souvent à la fin du parcours de l'acheteur. Le manque de confiance est alors la principale raison pour laquelle les choses finissent par mal tourner. Il reste encore beaucoup à apprendre dans ce domaine « TPSA », tant entre nous que du point de vue de l'évaluateur. C'est la raison pour laquelle nous rassemblons un groupe d'entreprises de produits et services numériques au sein d'un [réseau d'apprentissage consacré à](#)

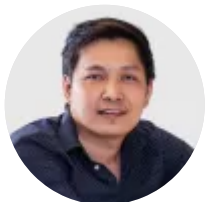
[la survie à une telle évaluation de sécurité.](#)



(Source image banner: iStock)

]]>

Auteurs



Annanda Rath



Tatiana Galibus