RSECURE

# Accompagnement cyber pour les TPE

Protégez votre business avec nos services sur mesure !


MADE IN LUXEMBOURG

## LA CYBERSÉCURITÉ, EST-CE BIEN UTILE POUR LES TPE ?

La cybersécurité ne concerne plus uniquement les grandes entreprises ou les institutions publiques. Les très petites entreprises (TPE), souvent perçues comme des cibles moins exposées, se retrouvent pourtant de plus en plus dans la ligne de mire des cybercriminels.
Avec des ressources limitées, une protection parfois rudimentaire et une prise de conscience encore inégale, les TPE représentent une porte d'entrée facile pour les attaques informatiques. Pourtant, une simple faille de sécurité peut avoir des conséquences dévastatrices : perte de données clients, interruption de service, atteinte à la réputation, voire la fermeture de l'entreprise.
Alors, face à ces menaces bien réelles, la cybersécurité est-elle un luxe ou une nécessité pour les TPE ?

### LES CHIFFRES CYBER AU LUXEMBOURG

- 1,466 attaques par semaine
- + 82% d'augmentation du nombre d'attaques depuis le dernier quadrimestre
- 62% des failles sont liées à une fuite d'information
- 18 645 € : Coût moyen d'une cyberattaque pour une société
- 1 société sur 8 rapporte que les attaques ont représenté un coût supérieur à 230.000€

Rsecure SARL / www.rsecure.lu
38-40, Parc d'Activités de Capellen L-8308 - Luxembourg

## LES SERVICES COMPRIS


Sensibilisation


Campagne de phishing


Monitoring


Veille cybersécurité


Accompagnement audit

- **SENSIBILISATION DES EMPLOYÉS :** la formation et la sensibilisation de vos collaborateurs aux divers risques liés à la cybersécurité jouent un rôle essentiel dans la protection de vos systèmes informatiques. La formation permet d'apprendre à reconnaître les menaces les plus courantes et développe la vigilance des employés.
- **CAMPAGNE DE PHISHING :** une fois la sensibilisation des employés faite, il est primordial de tester leurs réflexes régulièrement grâce à des campagnes de phishing adaptées et personnalisées. Savent-ils détecter les signaux d'alerte tels que les adresses d'expéditeurs douteuses, les fautes d'orthographe, les pièces jointes "urgentes", ..... ?
- **MONITORING :** est un processus de surveillance continue et proactive des dispositifs de sécurité informatiques de l'entreprise, incluant les antivirus, pare-feu, solutions cloud comme Microsoft 365, systèmes de détection d'intrusion, et autres outils de protection. Il ne s'agit pas simplement de vérifier leur bon fonctionnement, mais d'analyser les journaux d'activité, les alertes, et les comportements réseau pour anticiper les menaces et réagir rapidement aux incidents.
- **VEILLE CYBERSÉCURITÉ :** consiste à surveiller en continu l'évolution du paysage des cybermenaces, notamment les nouvelles techniques d'attaque, les failles émergentes, les vulnérabilités logicielles, et les tendances de cybersécurité. Lors de nos réunions, nous vous partageons les éléments les plus pertinents et les plus récents, accompagnés de recommandations ciblées et pragmatiques afin de renforcer votre posture de sécurité.
- **ACCOMPAGNEMENT :** parce que le monde cyber est en constante évolution, et que les règlementations nationales et européennes deviennent toujours plus nombreuses et pointues, nos experts vous accompagnent pour les audits de conformité, et également pour toutes vos questions liées à la cybersécurité.

# LES OPTIONS

- Plateforme de formation en ligne avec bouton d'alerte de phishing
- "SOC tranquility" : Security Operation Center en 24/7 (service qui traque et bloque les attaques sur les appareils connectés au réseau de l'entreprise)
- Mise en place de politique de sécurité adaptée aux TPE : charte informatique, gestion des incidents, .....

Rsecure SARL / www.rsecure.lu
38-40, Parc d'Activités de Capellen L-8308 - Luxembourg