Stemy
AHEAD IN BUSINESS SOLUTIONS

Memo - Bruxelles, Septembre 2025

Tendances de la Cybersécurité 2025 : Anticiper les Menaces de Demain

À l'aube de 2025, la cybersécurité s'impose plus que jamais comme un enjeu stratégique pour les entreprises, les institutions publiques et même les particuliers. La digitalisation croissante, l'essor de l'intelligence artificielle et la multiplication des objets connectés redessinent un paysage où les menaces évoluent rapidement et deviennent de plus en plus sophistiquées.
Chez **Stemy**, nous surveillons de près ces tendances afin d'aider nos clients à renforcer leur résilience et à protéger durablement leurs actifs numériques.

L'IA au cœur de la cybersécurité… et des attaques

L'intelligence artificielle devient une arme à double tranchant. Si elle renforce la détection d'anomalies et la réponse automatisée aux incidents, elle est également exploitée par les cybercriminels pour lancer des attaques plus rapides, plus ciblées et plus difficiles à détecter. En 2025, la bataille se jouera dans la capacité à maîtriser l'IA défensive avant que l'IA offensive ne prenne l'avantage.

Le ransomware continue d'évoluer

Les attaques par rançongiciel restent une menace majeure, mais leur mode opératoire évolue : au-delà du simple chiffrement de données, les cybercriminels misent sur l'extorsion multiple (vol de données sensibles, menaces de divulgation publique, perturbations ciblées). La prévention, la sauvegarde cloud sécurisée et la préparation de plans de réponse deviennent indispensables.

Cybersécurité et télétravail hybride

Avec la généralisation du travail hybride, les périmètres de sécurité traditionnels s'effacent. La protection doit désormais s'étendre aux collaborateurs à distance, aux terminaux mobiles et aux connexions domestiques. Les entreprises adoptent de plus en plus le modèle **Zero Trust**, où chaque accès doit être continuellement vérifié, quel que soit l'utilisateur ou l'appareil.

La sécurité du cloud et des chaînes logistiques

En 2025, les environnements multicloud et l'interconnexion des systèmes augmentent les surfaces d'attaque. Les cybercriminels ciblent aussi les fournisseurs tiers pour compromettre toute une chaîne de valeur. Les audits réguliers, la surveillance en continu et les solutions de sécurité intégrées au cloud deviennent incontournables.

La réglementation et la conformité en première ligne

Les autorités renforcent leurs exigences en matière de cybersécurité. Qu'il s'agisse du **RGPD**, des normes **ISO** ou de nouvelles régulations sectorielles, les entreprises doivent non seulement se protéger contre les cyberattaques, mais aussi prouver leur conformité. La gouvernance des données devient un enjeu aussi important que la protection elle-même.

Se préparer pour 2025 et au-delà

La cybersécurité n'est plus une fonction de support : c'est un pilier stratégique de la pérennité des entreprises. En 2025, la clé réside dans une approche **proactive, intégrée et évolutive** : combiner technologies avancées, formation des équipes et partenariats stratégiques.

Chez **Stemy**, nous accompagnons nos clients dans cette transition en leur apportant expertise, veille technologique et solutions adaptées aux défis de demain.

Protégez aujourd'hui, innovez demain : faisons de la cybersécurité un moteur de confiance et de croissance.

+32 484 836 390
HQ Stemy Belgium
contact@stemy.be
www.stemy.be