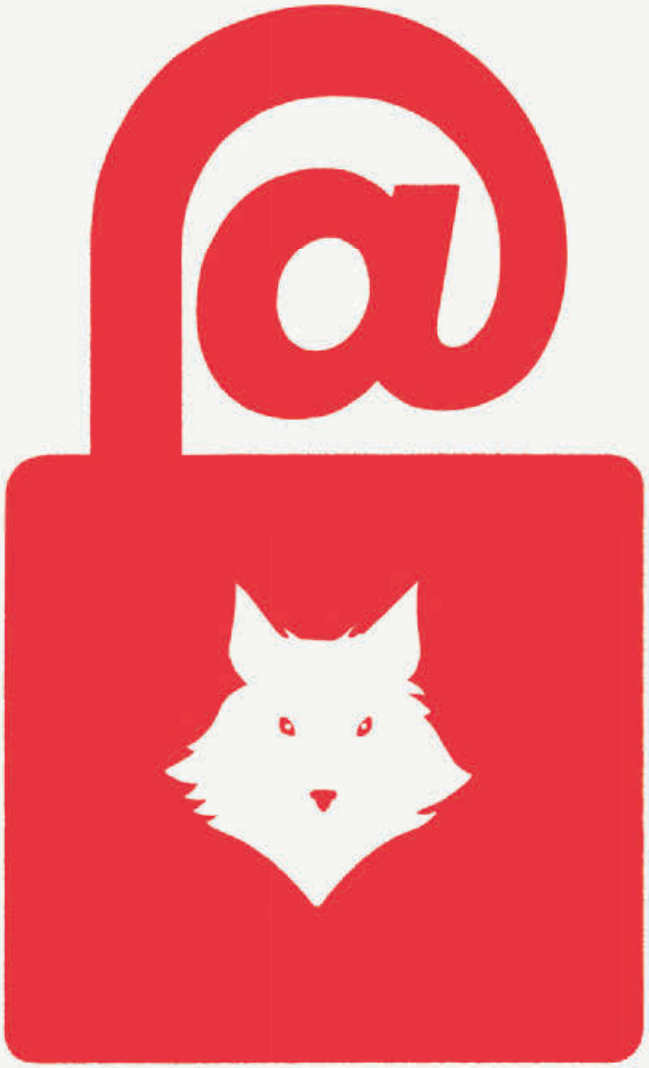
CYBERSÉCURITÉ

COMMENT SE PRÉPARER À UNE **CYBERMENACE MAJEURE** ?



Les chiffres sont sans appel : près de la moitié des entreprises belges ont déjà été victimes de cybercriminalité. Tous les secteurs sont touchés, mais certains plus que d'autres, tels que le secteur de la santé, suivi par celui des institutions financières. Quelles actions prioritaires les entreprises doivent-elles déployer pour renverser la tendance et transformer leur vulnérabilité en une véritable cyberrésilience ?

UNE VULNÉRABILITÉ GÉNÉRALISÉE ET UN COÛT FINANCIER CONSIDÉRABLE

Selon le baromètre Skyforce 2024 de la cybersécurité pour les TPE et PME belges[1], 66 % des entreprises ont subi une attaque au cours des deux dernières années, et 87 % d'entre elles ont connu des pertes financières ou une atteinte à leur réputation. Plus alarmant encore, 28 % craignent que le niveau de risque cyber les mène à la faillite.

Le Centre pour la Cybersécurité Belgique (CCB) confirme cette tendance : en 2024, le nombre de cyberincidents signalés a augmenté de 80 %. Les modalités d'attaque sont variées. Le phishing et le ransomware restent les principales menaces. Les statistiques révèlent une sophistication croissante des méthodes employées et une capacité d'adaptation constante des cybercriminels.

L'impact économique des cyberattaques dépasse largement les seuls coûts techniques de remédiation. Pour les PME, le coût moyen d'une cyberattaque atteint 1,2 million EUR par incident, un montant susceptible de compromettre gravement leur viabilité financière. Le coût moyen d'une violation de données s'élève à environ 58.600 EUR, montant qui peut exploser selon la gravité de l'incident.

Au-delà des coûts directs, les entreprises subissent des pertes indirectes majeures : perte de prospects et de clients suite à une attaque. La réputation, cet actif immatériel si difficile à construire, peut être irrémédiablement endommagée en quelques heures.

1 Cybersécurité - TPE et PME belges, baromètre annuel 2024 - vhttps://www.skyforce.be/wp-content/uploads/2024/05/BAROMETRE_2024_FR.pdf

LE FACTEUR HUMAIN : TALON D'ACHILLE DE LA CYBERSÉCURITÉ

Paradoxalement, malgré la sophistication croissante des technologies de protection, 46 % des attaques exploitent des erreurs humaines. Ce constat souligne l'importance cruciale de la sensibilisation et de la formation du personnel.

À cet égard, la prévention doit constituer une priorité stratégique. Cela implique, d'une part, d'identifier et de protéger les actifs critiques (quels les systèmes et les processus dont l'indisponibilité paralyserait l'entreprise ?) et, d'autre part, de mettre en place des défenses techniques robustes (pare-feu de dernière génération, authentification multifactorielle, chiffrement des données sensibles, sauvegardes régulières et testées).

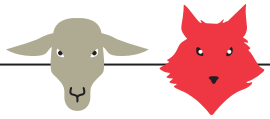
La formation continue du personnel constitue un investissement rentable. Un collaborateur capable d'identifier un email de phishing peut éviter à son entreprise des pertes considérables. Les simulations d'attaques et les exercices pratiques renforcent la vigilance collective.

ANTICIPER EST LA CLÉ DE LA CONTINUITÉ

La préparation est aussi importante que la prévention. Pour accompagner les entreprises victimes d'un cyberincident, la FEB a développé, en collaboration avec le CCB et le monde des entreprises, la « Cyber Incident Roadmap » qui définit les différentes étapes de prise en charge de l'incident, depuis le repérage jusqu'à la normalisation complète.

Enfin, pour renforcer la résilience des entreprises/organisations en matière de cybersécurité, le CCB a développé un cadre de référence gratuit – les CyberFondamentaux – pour les aider à mettre en œuvre des mesures appropriées et pertinentes. Une « certification selon ce cadre » est même possible, qui permet aux entreprises/organisations (même celles qui ne sont pas soumises à la réglementation NIS2) de démontrer qu'elles ont pleinement assumé leurs responsabilités en matière de cybersécurité. □

« L'IMPACT ÉCONOMIQUE DES CYBERATTAQUES VA BIEN AU-DELÀ DES COÛTS TECHNIQUES DE RÉPARATION »



DO'S-AND -DON'TS

Prévention
- Mettre en place une culture de la cybersécurité avec des formations, des trainings, des évaluations...
- Instaurer une politique de défense intelligente permettant une détection et un confinement rapides.

Gestion
- Impliquer tous les départements dans le plan de gestion de crise. La cybersécurité n'est pas juste une question IT.
- Prendre toute cybermenace au sérieux. Toute entreprise est une victime potentielle, quelles que soient sa taille et son activité.

Vous trouverez plus de do's-and-don'ts pour renforcer votre cybersécurité en situation de crise dans le toolkit 'BE PREPARED - Building Business Resilience in a Disruptive World'.
www.vbo-feb.be/fr/beprepared

LA CYBERASSURANCE : UN MAILLON INDISPENSABLE DANS LA STRATÉGIE DE SÉCURITÉ

La cyberassurance est un des outils essentiels d'une stratégie cybernétique solide. Elle couvre non seulement les coûts directs d'un incident (expertise judiciaire, assistance juridique, récupération du système, etc.), mais aussi les dommages indirects (perte de revenus, perte de réputation et réclamations en responsabilité civile, etc.). Pour de nombreuses PME, cela peut faire la différence entre la reprise et l'effondrement.

De plus, les assureurs donnent souvent accès à des équipes de crise spécialisées et à un soutien en cas d'incident. Cela permet aux entreprises de réagir plus rapidement et plus efficacement, avec moins d'impact sur la continuité de leurs activités.

Assurer la résilience des paiements face aux cyberattaques
Une interruption totale du système de paiement expose les entreprises à des pertes financières majeures, à la perte de clients et à une atteinte à la réputation. C'est pourquoi le secteur financier belge combine des mesures réglementaires, des investissements techniques tels que l'authentification multifactorielle (MFA), des plans de continuité, des formations, et une collaboration renforcée avec les autorités et les acteurs sectoriels pour garantir la résilience des paiements face aux cyberattaques.