



Nouvelles inquiétantes : la ville d'Anvers victime d'une attaque de ransomware

20 décembre 2022, 10:01

Tatiana Galibus

La semaine dernière, la ville d'Anvers a été victime d'une cyberattaque par ransomware. Le ransomware est un logiciel malveillant qui pratique l'extorsion. Il chiffre les données essentielles d'un utilisateur ou d'une entreprise en vue de bloquer l'accès aux fichiers, aux bases de données ou aux applications. Le paiement d'une rançon est alors exigé en échange du rétablissement de l'accès.

La plupart des services publics d'Anvers sont désormais paralysés, dont les services électroniques de l'administration, des musées et des bibliothèques. Cyber Play a revendiqué l'attaque sur son site sur le dark web. Ce groupe d'apparition relativement récente ne figure pas dans le rapport Kaspersky, qui épingle les huit ransomwares les plus dangereux au monde. C'est la preuve que même des cybercriminels de moindre envergure peuvent faire de gros dégâts et c'est symptomatique de la vitesse à laquelle les forces en présence peuvent évoluer et les menaces peuvent émerger dans la cybersphère.

La cybersécurité des entreprises belges peut-elle être aujourd'hui garantie ?

Non. La réponse a le mérite d'être simple. Nous savons que les groupes de ransomware sont bien organisés. Parfois mieux que les entreprises qu'ils ciblent. Ils adorent recourir aux technologies d'un autre âge : hameçonnage, spear phishing, clés USB, etc. Et comme l'illustre l'attaque de la semaine dernière, ces méthodes sont toujours efficaces.

Qu'est-ce qui explique leur succès ? Avec un groupe organisé de cette trempe, on n'a pas affaire à un simple programme ou script, mais à un réseau de cybercriminels bien rodés, dotés chacun de compétences spécifiques et tous centrés sur la réalisation d'un même objectif. Les célèbres fuites de données du gang Conti, « Panama Papers du ransomware » pour les intimes, ont révélé le modus operandi et les rouages de ces cybercriminels.

Saviez-vous qu'une entreprise belge fait face en moyenne à plus de 3.000 cyberattaques par an ? Rien qu'en 2022, on a observé une augmentation de 28 %. Il est donc temps d'agir.

La culture de la cybersécurité, un indispensable

Il est essentiel que les entreprises adoptent une culture claire et précise de la cybersécurité. Pour assurer cette protection dans un monde en pleine mutation, le manager que vous êtes doit être capable de répondre sans hésiter aux grandes questions suivantes.

- Tous mes collaborateurs ont-ils déjà entendu parler du phishing ou hameçonnage ? En connaissent-ils les rouages et les signes avant-coureurs ?
- Suis-je certain que dans mon entreprise, personne ne sera tenté par un clic dévastateur ou d'insérer une clé USB dans son ordinateur par curiosité ?
- Disposons-nous d'une stratégie et d'un contrôle clairs des accès ?
- Conservons-nous les données sensibles séparément sur un support de stockage chiffré ?

Vous avez une majorité de réponses négatives ? Vous hésitez beaucoup ? Il est grand temps de prendre conscience de l'urgence d'agir pour votre cybersécurité.

Sirris est à vos côtés

Dans les prochains mois, nous organiserons deux parcours de formation en [cybersécurité pour les services numériques](#) et [l'industrie manufacturière](#). Ces parcours d'apprentissage se composent de modules théoriques approfondis et de séances de mise en pratique personnalisées. Nous nous associons à des partenaires spécialisés en cybersécurité pour vous faire profiter des enseignements tirés et d'un partage d'expériences. En outre, vous bénéficierez de plusieurs **séances de microcoaching en fonction de vos besoins spécifiques**.

Auteurs



Tatiana Galibus