LETTRE INFORMATION CYBER - NOVEMBRE 2024

Cyberattaques en France : les dernières fuites de données et entreprises touchées

Les cyberattaques continuent de se multiplier en France. De nombreuses entreprises se sont retrouvées dans le viseur des cybercriminels. Ces attaques ont abouti au vol des données personnelles de la plupart des Français. Ci-dessous, on fait le point sur les dernières victimes et l'évolution de la situation.

Depuis quelques mois, les cyberattaques se multiplient en France. Les attaques informatiques se sont accélérées dès le début de l'année 2024, avec une pluie d'arnaques en ligne ou d'intrusions en tous genres. Une étude menée par Statista révèle que les cyberattaques devraient couter **plus de 129 milliards de dollars** à la France en 2024.

Au terme de la grande partie des cyberattaques recensées, **les données personnelles des Français** se sont retrouvées entre les mains des pirates. En règle générale, les données exfiltrées comprennent des noms complets, des adresses électroniques, des adresses postales ou des numéros de téléphone. Parfois, des coordonnées bancaires sont aussi récupérées par les pirates. C'était le cas lors du piratage de Free avec des millions d'IBAN qui se sont retrouvés dans la nature. **Pour toute question et demande de renseignement de ses clients, l'opérateur Free a mis en place un numéro vert (gratuit), disponible 7j/7 de 9h à 18h : 0 805 921 100**

Une fois dérobées, les données sont généralement revendues sur des marchés noirs. Bien souvent, c'est sur BreachForums, une plateforme très fréquentée par les cybercriminels en quête d'informations, que les enchères sont ouvertes. Une fois achetées, les données peuvent servir à orchestrer d'autres offensives, comme des attaques phishing personnalisées ou des tentatives d'usurpation d'identité.

À partir de là, on constate un effet boule de neige. Plus on trouve de données compromises, plus les hackers lancent des cyberattaques… qui aboutissent au vol d'autres informations. Pour Clément Domingo, chercheur en sécurité qui suit de près la situation en France, ce sont **les données de huit français sur dix** qui circulent sur des marchés noirs. C'est pourquoi les Français sont devenus les ciblés préférées des cybercriminels… La France s'est imposée comme **le pays d'Europe occidentale le plus touché** par les violations, démontre une étude de SurfShark.

La Banque de France dément une fuite de données, mais confirme une attaque

Des hackers revendiquent le piratage de la Banque de France. Le gang assure avoir dérobé des données sensibles, incluant les dossiers des employés et des clients, ainsi que des

documents stratégiques de la banque centrale. Les données sont en vente sur des marchés criminels…

La Banque de France affirme que ses données n'ont pas été dérobées par les pirates. Contactée par nos confrères d'Ouest-France, la banque assure qu'il *« n'y a pas eu d'attaque sur le système d'information sécurisé »* ayant permis d'exfiltrer des informations.

En revanche, la banque centrale a bien enregistré *« un accès extérieur occasionnel sur un extranet RH (ressources humaines) »*. Pour bloquer l'accès aux cybercriminels, cet extranet a été promptement fermé. Lors de l'intrusion, *« aucune donnée personnelle ou financière sensible n'a été compromise »*. Sur Telegram, les pirates continuent cependant de mettre en avant la base de données volées, dont un échantillon est disponible.

Apprendre à séparer ses usages pro-perso

La transformation numérique modifie en profondeur les usages et les comportements. Être connecté est devenu le quotidien. Le développement des technologies mobiles (PC portables, tablettes, smartphones) offre désormais la possibilité d'accéder, depuis presque n'importe où, à ses informations personnelles mais aussi à son système informatique professionnel : la frontière numérique entre la vie professionnelle et personnelle devient de plus en plus poreuse. Face à cette évolution, il est nécessaire d'adapter ses pratiques afin de protéger tant votre entreprise* ou votre organisation, que votre espace de vie privée. Voici 10 bonnes pratiques à adopter pour la sécurité de vos usages pro-perso.

1. Utilisez des mots de passe différents pour tous les services professionnels et personnels auxquels vous accédez.

2. Usages pro-perso : Ne mélangez pas votre messagerie professionnelle et personnelle

3. Ayez une utilisation responsable d'internet au travail

4. Maîtrisez vos propos sur les réseaux sociaux

5. Usages pro-perso : N'utilisez pas de services de stockage en ligne personnel à des fins professionnelles

6. Faites les mises à jour de sécurité de vos équipements

7. Utilisez une solution de sécurité contre les virus et autres attaques

8. Usages pro-perso : N'installez les applications que depuis les sites ou magasins officiels

9. Méfiez-vous des supports USB

10. Usages pro-perso : Évitez les réseaux Wi-Fi publics ou inconnus

LA SECURITE EST L'AFFAIRE DE TOUS.