Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 novembre 2024

Cyber-menaces : 75% des 18-24 ans utilisent leur mail professionnel à des fins personnelles

Un récent rapport Sailpoint effectué auprès d'employés de tout horizon dans plusieurs pays révèle leurs habitudes en matière de cyber-sécurité.

La récente étude* de Sailpoint, spécialiste de la sécurisation des échanges internet pour les entreprises, dans plusieurs pays met en exergue les bonnes mais aussi les mauvaises habitudes des employés en matière de cyber-sécurité à travers le monde. Les cyberattaques ont augmenté au cours de l'année dernière et nombreux sont ceux qui en prennent conscience. Plus d'un tiers (36 %) des Français interrogés ont été informées d'une violation de données susceptible d'exposer leurs informations au

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 novembre 2024

cours de la dernière année écoulée.

Les enjeux de la cybersécurité mieux compris
Les bonnes pratiques s'installent au sein des entreprises. En France, 87% des employés interrogés font désormais régulièrement une pause pour s'interroger sur la validité d'un e-mail avant de l'ouvrir, de peur qu'il s'agisse d'une tentative de 'phishing'. Et 27% d'entre eux ont reçu une formation sur le phishing au cours de l'année écoulée. Sur ce point, les Français ont pourtant encore une marge de progression conséquente. Nos cousins britanniques sont formés à hauteur de 50% et à 65% chez les Américains interrogés.

Un dangereux mélange entre vie personnelle et professionnelle
Pourtant, cela ne suffit pas à contrer les mauvaises habitudes. Beaucoup d'employés continuent tristement d'adopter un comportement risqué sur Internet. Près de la moitié (42%) des employés français ont déclaré qu'ils utilisaient leur adresse électronique professionnelle à des fins personnelles. Et ce chiffre monte jusqu'à 75% chez les Français de 18 à 24 ans. Que ce soit pour se connecter sur les réseaux sociaux ou à des publications d'actualités, recevoir des newsletters ou encore faire des achats en ligne, ces employés inconscients créent ainsi, sans le savoir, des lacunes de visibilité et des ouvrent les portes de l'infrastructure de leur entreprise aux cyber-malveillances.

Des réactions inappropriées face aux tentatives de phishing
Selon cette étude, 86% des Français interrogés sont confiants ou très confiants dans leur capacité à détecter un message de phishing. Pourtant, ils réagissent encore majoritairement mal aux messages de phishing. Moins d'un Français sur 5 sait comment réagir de manière appropriée à un message de phishing, soit en le transférant au service informatique.
Les Anglais et les Américains sont une fois de plus les meilleurs élèves puisque 29% d'entre eux les transfèrent au service de traitement informatique. Les travailleurs Japonais sont les moins bien formés à ce sujet puisqu'ils ne sont que 15% à avoir adopté cette bonne pratique.
Cette disparité entre la confiance en soi en matière de cyber sécurité et l'usage des bonnes pratiques est un réel danger pour les entreprises. Leurs employés sont persuadés de bien agir tout en mettant en péril la sécurité de l'entreprise. Augmenter le nombre de formations aux bons gestes et aux enjeux de la cyber sécurité en entreprise devient fondamental et devrait être une priorité.

**Enquête auprès de 3 000 répondants travaillant dans des entreprises de plus de 2 500 salariés. Étude réalisée dans les pays suivants : États-Unis, Royaume-Uni, France, Allemagne, Australie et Japon.*

Les cyberattaques les plus courantes contre

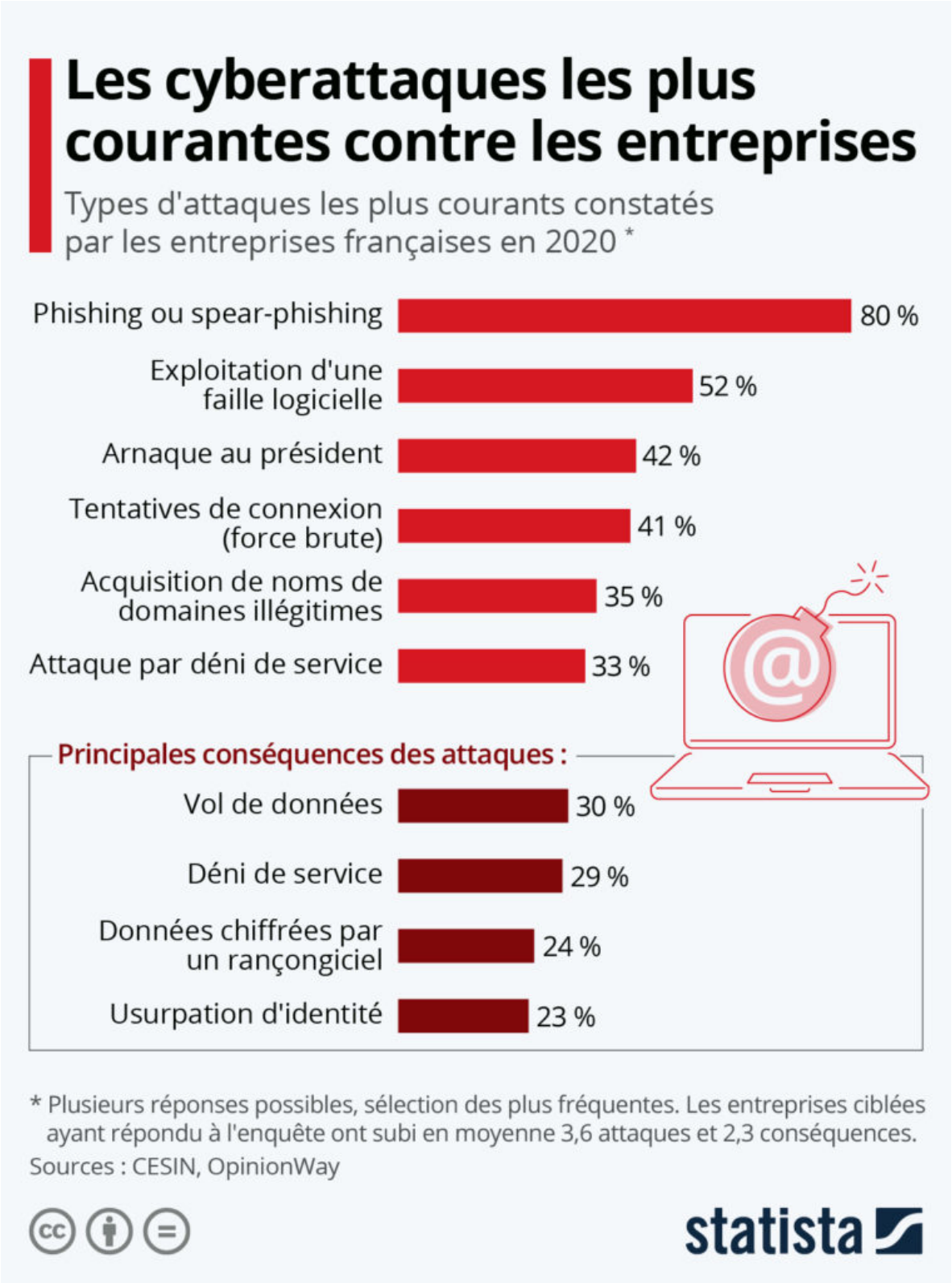
Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 novembre 2024

les entreprises françaises

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 novembre 2024



Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 novembre 2024

Samedi dernier, les Etats-Unis ont de nouveau été frappés par une cyberattaque massive. Des pirates informatiques ont ciblé la société américaine Kaseya, qui fournit des logiciels de gestion de réseaux, pour demander une rançon à potentiellement plus de 1 000 entreprises clientes du groupe. Les hackers ont utilisé un rançongiciel, un programme qui exploite une faille de sécurité pour paralyser un système informatique avant d'exiger une rançon pour le débloquer. L'une des conséquences a été la fermeture temporaire de 800 supermarchés en Suède, les caisses de l'enseigne ayant été mises hors service lors de l'attaque.

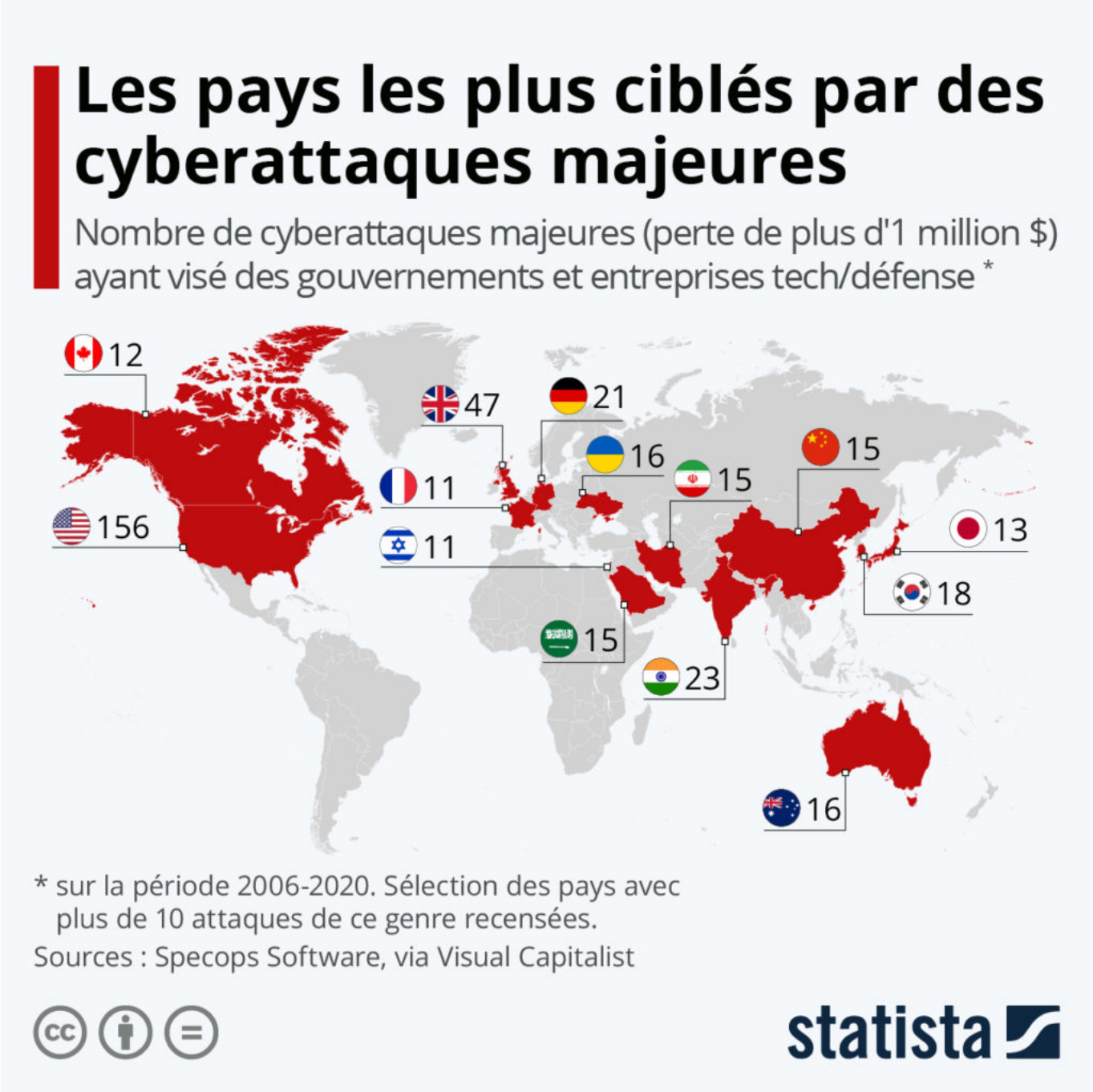
D'après le dernier baromètre de la cybersécurité publié par le CESIN, le vecteur d'attaques le plus courant constaté par les entreprises françaises reste le phishing ou spear-phishing, qui consiste à piéger des utilisateurs en leur envoyant un mail leur faisant croire qu'ils s'adressent à un tiers de confiance. Ce type d'attaque a été rapporté par 80 % des entreprises ciblées en 2020. Il est suivi par l'exploitation des failles logicielles, qui concerne un peu plus de la moitié des entreprises interrogées. Comme le montre également notre graphique, les principales conséquences de ces cyberattaques sont le vol de données (30 % des entreprises attaquées), le déni de service (29 %) ainsi que le chantage via un rançongiciel (24 %). Les auteurs de l'étude soulignent que la crise sanitaire a confronté les entreprises à de nouveaux cyber-risques, en lien notamment avec la généralisation du télétravail et l'usage d'applications et de services Cloud dont la sécurité fait défaut.

De Tristan Gaudiaut pour Statista

Les pays les plus ciblés par des cyberattaques majeures

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 novembre 2024



Des données publiées par Specops Software et reprises par le site Visual Capitalist révèlent les pays qui ont été les plus ciblés par des cyberattaques majeures au cours des deux dernières décennies. L'étude porte plus particulièrement sur la période 2006-2020 et recense les attaques informatiques visant des gouvernements ainsi que des entreprises technologiques et de défense qui ont causé des pertes supérieures à 1 million de dollars (environ 820 000 euros).

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 novembre 2024

Les États-Unis arrivent largement en tête des pays les plus touchés, avec 156 cyberattaques de ce genre documentées. Cela représente une moyenne de 11 attaques majeures par an, soit le même nombre que celui enregistré par la France en quinze ans. Parmi les cibles les plus souvent attaquées, on retrouve ensuite le Royaume-Uni (47), l'Inde (23) et l'Allemagne (21). Avec 11 cyberattaques d'envergure subies depuis 2006, l'Hexagone fait partie du top 15 des pays les plus ciblés, derrière le Canada (12) et à égalité avec Israël (11). Quant à la Russie, non sélectionnée dans ce graphique (moins de 10 attaques majeures), elle en a recensé 8 au total sur la période étudiée, soit deux fois moins que son voisin ukrainien.

L'Agence nationale de sécurité des systèmes d'information (ANSSI) a récemment alerté sur la hausse du niveau de menace cyber en France, en lien notamment avec le contexte de crise sanitaire. L'an dernier, les attaques informatiques contre des entreprises ou institutions françaises ont été multipliées par 4.

De Tristan Gaudiaut pour Statista

Nouvelle formation Bac+5 Manager en ingénierie informatique et Cybersécurité

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 novembre 2024

Le Centre de Formation des Apprentis de la Chambre de Commerce et d'Industrie de Vaucluse proposent, dès septembre, sur son Campus à Avignon, une nouvelle formation Bac+5 Manager en Ingénierie Informatique avec une spécialisation en Cybersécurité.

Ce titre de niveau 7 inscrit au RNCP (Registre Nationale des Certifications professionnelles) s'adresse aux candidats de moins de 29 ans, titulaires d'un Bac+2 ou Bac+3. En apprentissage, les candidats seront formés à la cybersécurité, à la sécurité des infrastructures, aux audits de sécurité, à la certification OSCP (certification de l'offensive Security), au Forensic, à la législation (normes ISO et IBIOS).

Trois ans de formation

Cette formation de trois ans forme des experts de la sécurité des réseaux, des infrastructures, des objets et des systèmes industriels connectés qui seront en mesure de détecter des attaques et de les stopper et de déceler toutes les failles d'un système et de les corriger.

Un diplôme sur-mesure

Ce diplôme a été conçu par le réseau des CCI, via l'ESIEE-IT l'école de l'expertise numérique créée par la

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 novembre 2024

CCI Paris Ile-de-France et spécialisée en informatique, robotique, électronique, domotique, transformation numérique, coding, applications, réseaux et sécurité, développement web mobile, lead developpement, ingénierie informatique, cyber sécurité, intelligence artificielle, big data, smart & green building.

Reconduction des aides aux entreprises pour l'embauche d'un apprenti

Pour la première année de chaque contrat d'apprentissage conclu entre le 1er juillet 2020 et le 31 décembre 2021 préparant à un diplôme jusqu'au master (bac + 5 – niveau 7 du RNCP) le montant de cette aide est de 8000 euros pour les majeurs de 18 à 30 ans, et de 5000 euros pour les mineurs de moins de 18 ans. Les entreprises bénéficieront ainsi de ces aides pour l'embauche d'un apprenti suivant cette nouvelle formation en ingénierie informatique.

Les infos pratiques

L'ensemble des informations est disponible sur le site du CFA de la CCI : cfa.vaucluse.cci.fr et la fiche est téléchargeable ici. Les inscriptions sont possibles dès maintenant directement sur le site. CFA Allée des Fenaisons à Avignon. 04 90 13 86 46.