Veille technologique

REDIGE PAR SANDY CERRATO

Cyber criminalité : Les attaques par phishing.

| 2021-2022 |

https://www.proofpoint.com/fr/newsroom/press-releases/le-rapport-2022-de-proofpoint-sur-letat-du-phishing-revele-que-les-attaques#:~:text=83%20%25%20des%20personnes%20interrog%C3%A9es%20ont,ran%C3%A7ongiciel%20par%20email%20en%202021.

o

SOMMAIRE

2. Concernant votre boite mail.
3. Utiliser les plateformes de signalement.

L'IMPORTANCE D'UNE VEILLE DANS LE DOMAINE DE L'INFORMATIQUE.

La veille est utile quelque soit le domaine de compétence que nous avons choisit d'approfondir.

Il y a cependant des métiers pour lesquels elle est indispensable, c'est le cas de l'informatique.

En effet le domaine de l'informatique est en constante évolution et nécessite une rigueur en terme de mise a niveau de connaissance car sans cela il est impossible de se tenir informé de toutes les nouveautés disponibles dans le secteur, cependant il n'est pas toujours possible de consacrer plusieurs heures a la recherche de nouvelles informations.

J'ai donc fais le choix de m'abonner a diffèrent flux RSS tel que « google alert » et « Feedly » qui génèrent des alertes à chaque fois qu'un sujet correspondant à mes demandes apparait.

Je reçois directement les liens des articles dans ma boite mail.

Le sujet que je vais traiter dans ma veille informatique est celui des attaques par phishing.

J'ai commencé ma veille en décembre 2021 ce qui la rend assez complète, c'est un travail de mise a niveau quotidien mais indispensable, de plus j'ai pu mieux analyser certains mails suspect que j'ai reçu sur ma propre adresse , j'ai également pu observer dans le cadre de mon travail le manque d'informations des clients au sujet de ces mails infectés qui malheureusement bien trop souvent sont pris pour de vrais mails et amènent a des conséquences très handicapantes pour les entreprises.

Q'UEST-CE-QUE LE PHISHING ?

Le phishing par e-mail est la forme de base ou traditionnelle du phishing ou hameçonnage. C'est un type d'escroquerie en ligne où des criminels se font passer pour des organisations ou personnes légitimes par un moyen approprié pour voler à leurs cibles des données sensibles comme la date de naissance, les numéros de sécurité sociale, les numéros de téléphone, les détails de la carte de crédit, l'adresse du domicile et autres.

Munis de vos informations personnelles, les cybercriminels peuvent faire de nombreuses actions qui pourraient vous nuire, comme ouvrir des comptes bancaires à votre nom et demander des prêts, accéder à vos comptes bancaires déjà existants, faire des achats en ligne avec votre compte et bien d'autres encore.

Pour augmenter l'efficacité des attaques de phishing par email qu'ils mènent, les cybercriminels envoient une très grande quantité de mails généralement avec le même contenu. Il est en effet rare que le contenu des messages envoyés soit personnalisé.

LES ATTAQUES PAR PHISHING QUELQUES DONNEES SUR 2021.

- Les attaques par email dominent le paysage des menaces en France en 2021 : 88 % des personnes interrogées en France ont déclaré que leur organisation avait été confrontée à de vastes attaques de phishing en 2021. Par ailleurs, 80 % d'entre elles ont été confrontées à au moins une attaque de rançongiciel par email et 75 % à une ou plusieurs attaques de compromission d'emails professionnels (BEC).
- En plus d'être plus actifs, les cybercriminels ont eu plus de succès en 2021. 88 % des personnes interrogées en France ont déclaré que leur organisation avait subi au moins une attaque de phishing réussie.
- 81 % des organisations françaises ont déclaré avoir été confrontées à au moins une infection par rançongiciel provenant d'une charge utile directe d'un email, d'une livraison de logiciels malveillants de deuxième étape ou d'un autre exploitant - le taux le plus élevé de tous les pays étudiés dans le monde. Parmi ceux-ci, 56 % ont choisi de payer au moins une rançon. Pour aller plus loin, 69 % ont payé une rançon et obtenu l'accès à leurs données/systèmes, 20 % ont payé une rançon initiale et une ou plusieurs rançons complémentaires et ont obtenu l'accès aux données/systèmes, 4 % ont payé une rançon initiale, ont refusé de payer davantage et n'ont pas obtenu l'accès aux données et 7 % n'ont jamais eu accès aux données après avoir payé une rançon.

- Malgré le niveau élevé d'infections par rançongiciel en France, seulement 44 % de ces organisations couvrent les rançongiciels dans leur programme de formation à la sécurité.

- La France est le pays qui a le moins modifié son lieu de travail en raison de la pandémie. 47 % des travailleurs français ont déclaré que la pandémie n'avait pas eu d'impact sur leur lieu de travail (le pourcentage le plus élevé de tous les pays étudiés, la moyenne mondiale étant de 36 %). C'est peut-être pour cette raison que 32 % des travailleurs français sont les plus susceptibles de dire qu'ils n'utilisent pas d'appareils personnels pour des activités liées au travail (contre 26 % pour la moyenne mondiale).

- De nombreux travailleurs adoptent des comportements à risque et ne respectent pas les meilleures pratiques en matière de cybersécurité. 42 % ont déclaré avoir effectué une action dangereuse (cliquer sur un lien malveillant, télécharger un logiciel malveillant ou exposer leurs données personnelles ou leurs identifiants de connexion) en 2021. Et 56 % des personnes ayant accès à un appareil fourni par l'employeur (ordinateur portable, smartphone, tablette, etc.) ont autorisé leurs amis et leur famille à

utiliser ces appareils pour faire des choses telles que jouer à des jeux, diffuser des médias et faire des achats en ligne.

LES ATTAQUE PAR PHISHING : QUELQUES DONNEES

Les données présentés plus haut nous alerte sur le nombre de victimes de ces attaques . De nombreux employés mal informés ou peu formés ne différencient pas un mail frauduleux d'un mail réel, et il est donc très important de permettre aux employés de se former sur les risques encourus et les bonnes pratiques en matière de protections des données. De plus la venue du télétravail a fait exploser le compteur en terme de cyber attaques ; en effet le taux en 2021 est affolant, les réseaux des particuliers n'étant pas forcement sécurisés correctement un grand nombres d'entres eux ont subis de lourdes attaques ayant souvent pour but de leur soutirer de l'argent (« ransomware »). Face à une telle recrudescence de ces attaques et étant donné que le télétravail est voué a être une nouvelle norme et matière de travail il est primordial d'analyser ces attaques , leurs modes de fonctionnements et les cibles qu'elles visent afin de s'en protéger.

La plateforme Cybermalveillance.gouv.fr a enregistré en 2021 plus de 173 000 demandes d'assistance en ligne. Cela représente une augmentation de 65 % par rapport à l'année précédente, selon un rapport de 2021. Selon le rapport, 90 % des demandes d'assistance concernaient des particuliers, 8 % des entreprises et 2 % des collectivités. Plus de 10 300

entreprises ou associations et 2 100 collectivités ou administrations ont été aidées en ligne. Sur les 47 formes de cyber malveillance détectées, l'hameçonnage ou « phishing » arrive en tête des attaques rencontrées par les particuliers. Il a représenté 31 % des recherches d'assistance, soit une progression de 82 % en un an. Cette technique consiste à récupérer des données personnelles, comme des coordonnées bancaires, en envoyant des mails frauduleux.

LES PAYS LES PLUS TOUCHES.

Un virus à la propagation exponentielle le plus souvent transmit par mail. Le ransomware est un logiciel malveillant qui bloque l'accès à vos outils informatiques et à vos données en les chiffrant. Une fois cryptées, ces dernières peuvent être bloquées, détruites ou exploitées sur des marchés parallèles à prix d'or. Pour récupérer ces données, le cybercriminel demande le paiement d'une rançon en échange d'une clé de décryptage.

Menace importante en 2021, le ransomware constitue 60% des attaques observées par le CERT-Wavestone. La France est le 4ème pays le plus touché au monde après le Canada, le Royaume-Uni et les Etats-Unis. Dans 56% des cas, les victimes n'avaient pas anticipé être la cible potentielle d'une cyberattaque et dans 90% des cas, des données ont été perdues irrémédiablement.

COUT MOYEN ET CONSEQUENCES.

Le coût moyen d'une attaque par ransomware est estimé à 7 000€ pour une TPE et à 300 000€ pour une PME très affectée. Au-delà du coût de la rançon (222 000€ en moyenne) s'ajoutent des coûts indirects comme la réparation et le rachat de matériel, l'intervention d'équipes compétentes, et l'interruption de l'activité qui sont 5 à 10 fois plus élevés que le montant de la rançon.

En moins d'un an, le coût moyen de reprise d'activité après une attaque par ransomware a plus que doublé. Les organisations touchées subissent également une dégradation de leur réputation : 61% des utilisateurs ont perdu confiance en elles, et 31% ont mis fin à leurs relations avec elles.

L'HUMAIN AU CENTRE DES ENJEUX.

Le ransomware est majoritairement véhiculé par email et se cache dans une pièce-jointe vérolée ou derrière un lien malveillant. Les pirates informatiques exploitent des failles technologiques et humaines telles que le manque de connaissance en cybersécurité des collaborateurs. Ils misent également sur la détresse des victimes pour obtenir le paiement de la rançon. La sauvegarde de données, la mise à jour des outils digitaux et les technologies de protection de messagerie sont essentiels mais ne suffisent aujourd'hui plus à se prémunir de ce type d'attaque.

Dans 99 % des cas (Harvard Business Review), l'humain est la cible prioritaire des cyber attaquants. Avec plus de 80% des attaques qui transitent par email, la sensibilisation et la formation des collaborateurs sont essentielles à la pérennité des organisations. Des outils pédagogiques tels que des simulations d'attaques inopinées et régulières permettent de tester, d'éduquer et de faire prendre conscience aux collaborateurs des conséquences potentielles sur leur organisation.

CALCULATEUR EN LIGNE DU COUT D'UNE CYBER ATTAQUE EN FONCTION DE VOTRE ENTREPRISE.

Afin de vous faire une idée réelle du coût d'une cyber attaque je vous propose de vous rendre sur ce site et de renseigner les informations concernant votre entreprise vous serez en mesure de budgéter la perte financière qui incombe a une attaque de type ransomware.

J'ai renseigné des informations a propos d'une société fictive dans le secteur du commerce et de la vente au détail avec un chiffre d'affaire 500K/An.

Je vous laisse constater le cout d'une attaque sur cette entreprise.

https://www.hiscox.fr/calculateur-exposition-cyber-risques/

2. Renseignez les caractéristiques de votre entreprise

Choisissez les caractéristiques qui décrivent le mieux votre organisation.

Secteur d'activités	Région	Revenus (en devise locale)
Commerce et vente au détail	UE	Jusqu'à 500 K

3. Renseignez vos capacités en matière de sécurité

Notre calculateur se base sur des hypothèses selon votre secteur d'activité, votre situation géographique et vos revenus. Utilisez les curseurs ci-dessous pour ajuster ces hypothèses aux capacités de votre organisation et les comparer aux standards de votre secteur d'activité, afin de mieux comprendre les axes d'amélioration pour votre organisation.

Protection

Évaluez la capacité de votre organisation à se protéger contre les cyber-attaques (par ex. les firewalls, logiciels antivirus, correctifs réguliers appliqués sur les serveurs).

Détection

Évaluez la capacité de votre organisation à détecter une cyber-attaque (par ex. systèmes de détection des intrusions, centre des opérations de sécurité, surveillance du dark web).

Récupération

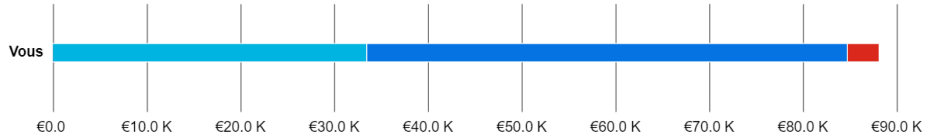
Évaluez la capacité de récupération de votre organisation après une cyber-attaque (par ex. plan de gestion de crise, assurance cyber, consultation d'experts de la cybersécurité).

L'estimation financière de votre exposition aux cyber-risques

€88.2 K

Ventilation de votre exposition aux cyber-risques

Nous avons défini quatre catégories de pertes distinctes qui couvrent les principales formes possibles de cyber incidents.



Type de cyber-risques

Interruption d'activités
Coûts induits du fait de l'indisponibilité des systèmes de gestion des activités et/ou des systèmes informatiques (par ex. attaque par ransomware chiffrant l'ensemble des systèmes informatiques)

Informations à caractère personnel
Coûts induits du fait de l'exposition des informations qui peuvent identifier une personne ou qui sont liées à une personne (par ex. le nom, les informations sur sa santé/son emploi, les informations financières, etc.)

Actifs immatériels
Coûts induits par le vol des ressources qui représentent une valeur pour une organisation et qui ne sont pas matérielles par nature (par ex. les licences, droits d'auteur, brevets, marques, etc.)

Perte financière
Coûts directs ou indirects résultant d'une fraude financière, de réclamations, d'amendes, d'exigences supplémentaires de reporting, etc.

Types de pirates susceptibles de cibler votre organisation

Les pirates informatiques se classent généralement en quatre grandes catégories :

Perturbation - 37%
Pirates motivés par des objectifs sociaux ou politiques plutôt que par l'argent.

Espionnage - 0%
Pirates informatiques très organisés, motivés par la récupération de données de propriété intellectuelle ou d'autres données commercialement sensibles.

Attaque de masse - 63%
Pirates motivés par l'argent qui ont tendance à attaquer un groupe de victimes large et de façon aléatoire.

Arnaque organisée - 0%
Groupes de pirates organisés qui ciblent des personnes ou des groupes d'organisation avec l'intention particulière de commettre une arnaque financière de grande ampleur.

Comme vous pouvez le constater cet outil est assez complet et vous permet de mettre des chiffres adaptés a votre entreprises afin de visualiser l'importance d'une cyber sécurité active et le poids de la formations des équipes en matière de bonne pratique.

COMMENT SE PROTEGER ?

De manière générale :

Ne partagez jamais vos informations, soyez prudent lorsque vous partagez des informations personnelles ou professionnelles ; Ne vous connectez jamais ailleurs que sur le site internet de votre véritable administration, institution, organisation…Observez bien l'URL du lien, toute faute d'orthographe ou irrégularité doit attirer votre attention .Vérifiez que le site est sécurisé : un cadenas doit être présent dans l'URL et l'adresse du site doit commencer par HTTPS (et non HTTP) .Saisissez vos noms d'utilisateur et mots de passe uniquement quand vous utilisez une connexion sécurisée.

Concernant votre boite mail :

Certes, il arrive que le manque de temps et la fatigue engendrent une baisse de vigilance. Toutefois, prenez le temps de vous poser les bonnes questions. Par exemple, est-ce que cet e-mail m'est réellement destiné ? Ce message évoque un dossier, une facture, un thème qui ne me parle pas ? Est-ce que je connais cet expéditeur ? Son contenu est inquiétant, déconcertant, inattendu ? Pourquoi cet expéditeur me somme-t-il de répondre dans de si brefs délais ? En cas de doute, ne cliquez pas sur "répondre" ou "transférer". De plus, ne cliquez jamais sur les liens ou pièces jointes des emails. Ils dirigent souvent vers une fausse page qui ressemble au site d'origine ou téléchargement d'un logiciel malveillant.

Utiliser les plateformes de signalement :

Les tentatives d'escroquerie par phishing peuvent être signalées sur la plateforme PHAROS (www.internet-signalement.gouv.fr), portail officiel de signalement des contenus illicites de l'Internet ou sur le site www.phishing-initiative.com.

Le gouvernement met également a disposition des fiches « reflexes » concernant le phishing..

Elles sont consultable ici : https://www.cyberveille-sante.gouv.fr/sites/default/files/documents/fiches-reflexes/Fiches_reflexes-Phishing_v1.6.pdf

SOURCES

https://www.groupe-delta.com/communication/cybersecurite-10-statistiques-choc-a-retenir-en-2021/#:~:text=Google%20a%20d%C3%A9couvert%20plus%20de,d%C3%A9jouer%20ce%20type%20de%20menaces.

https://securite.developpez.com/actu/329999/Les-attaques-par-ransomware-ont-augmente-de-250-pourcent-au-cours-du-premier-semestre-de-2021-les-utilisateurs-seront-confrontes-a-une-attaque-toutes-les-11-secondes-au-cours-du-second-semestre/

https://www.allianz-trade.fr/content/dam/onemarketing/aztrade/allianz-trade_fr/news/150921/cp-etude-fraude-2021.pdf

https://www.sudouest.fr/sciences-et-technologie/cyberattaques-les-demandes-d-assistance-en-ligne-en-hausse-de-65-en-un-an-en-france-9564561.php

https://www.carnetdebord.info/06-types-dattaques-de-phishing-les-plus-courants-en-2021/#1-_Le_phishing_par_e-mail

https://www.hiscox.fr/calculateur-exposition-cyber-risques/#results

https://www.zdnet.fr/actualites/comment-resister-au-raz-de-maree-de-la-cybercriminalite-en-2022-39935225.htm

https://www.cnil.fr

https://www.cyberveille-sante.gouv.fr/sites/default/files/documents/fiches-reflexes/Fiches_reflexes-Phishing_v1.6.pdf