Penser comme un hacker pour lutter contre la cybercriminalité

Les pirates virtuels sont de plus en plus présents sur les réseaux et n'hésitent pas à hacker les systèmes afin d'avoir accès aux bases de données sensibles, allant de particuliers aux entreprises en passant par le secteur privé comme public en vue de perpétrer leur forfait.

La problématique de la sécurité des données et des échanges de celles-ci devient un problème de plus en plus récurrent dans le contexte actuel. Il y a de cela quelques jours, le CNED plateforme instituée par le ministère de l'Education Nationale dans le but de permettre de suivre des cours à distance à la maison a été victime de cyberattaque notamment de vols de données. Ce n'est pas la seule plateforme à s'être faite pirater. Plusieurs autres entreprises, qu'elles fassent partie du secteur privé comme public sont également victimes de ces pirates virtuels. Les différentes malversations de nature criminelle ou délictuelle opérées dans la vie réelle vont trouver une déclinaison dans le monde virtuel qu'il soit question de vol, d'escroquerie et autres.

Avant la période relative à la crise sanitaire, les pirates opéraient d'une certaine façon. Ils visaient dans la majorité des cas les grandes entreprises. Depuis la crise sanitaire, leur mode opératoire s'est semble-t-il ouvert à d'autres victimes. L'on dénote une montée en puissance des attaques sur internet touchant à la fois les particuliers personnes physiques comme les personnes morales de droit privé et public. En 2020 par exemple, la plateforme Doctolib a été victime d'un piratage informatique portant sur les données de près de 6000 patients ayant permis de recueillir des informations sur leur nom, prénom, âge, sexe, numéro de téléphone, adresse e-mail dans un but a minima de revendre les données personnelles

recueillies.

Les conséquences de ces attaques sont multiples et peuvent aller jusqu'à la perte financière surtout lorsque la réputation, l'image de l'entreprise sont en jeu. Ces attaques massives deviennent un enjeu de sécurité nationale. Rien qu'en 2019, selon le Center for Strategic and International Studies la cybersécurité était estimée à plus de 600 milliards de dollars en termes de détournement de données, demandes de rançons et cetera, soit 1 % du PIB mondial détourné.

Les répercussions de ces attaques sur les entreprises peuvent être désastreuses surtout pour les TPE et PME dont 60% ne survit pas à ce type d'attaques. Plusieurs outils sont utilisés afin d'amener la victime à commettre une erreur qui lui sera à coup sûr préjudiciable.

Selon le directeur technique de SEKOIA, entreprise spécialisée dans la cybersécurité, David Bizeul, toute personne est intéressante et donc une cible pour le hacker car nous avons tous des choses monétisables. Ces derniers agissant seuls ou à plusieurs ont un arsenal d'attaques constitué. Ils peuvent ainsi passer par du phishing (ou hameçonnage) afin d'obtenir la communication d'informations personnelles sur un individu ; le trojan (ou cheval de troie), dont le but est de récupérer les données de type identifiants bancaires, secret de navigation ; les rançongiciels qui consistent à chiffrer les fichiers, disques des victimes et de leur demander une rançon en retour si ces dernières souhaitent récupérer leurs données. Ce mode de procédé vise les salariés en télétravail, les entreprises ou hôpitaux ; des attaques pouvant viser par ailleurs spécifiquement des organisations de santé dans un but d'espionnage ou pour tenter de dérober les secrets de la recherche médicale sur le vaccin.

En règle générale, afin de brouiller toute piste, les hackers préfèrent utiliser des bitcoins pour se faire payer ; ce qui rend la traçabilité des opérations et l'identification des coupables pour ainsi dire impossibles.

Le développement soudain de la cybercriminalité dans le contexte actuel s'expliquerait non seulement par un changement de cadre de travail des salariés, un comportement des victimes, une amplification des usages numériques et la période anxiogène sont autant de facteurs favorables au hacker. L'attaquant n'hésite pas à profiter des nouveaux outils mis en place dans la gestion du télétravail afin de s'immiscer à la fois dans la vie de l'entreprise et celle du

salarié. Par exemple, lorsque le salarié utilise pour son travail ses outils personnels et inversement, il ouvre ainsi involontairement la brèche à l'attaquant qui n'hésitera pas à user de cette faille pour recueillir à tout le moins les données dont il a besoin afin de les revendre, ce qui peut salir l'image de l'entreprise et qui peut impacter son chiffre d'affaire.

Se prémunir contre les différentes attaques

Il est important de savoir se prémunir contre ces diverses attaques en cette période d'urgence. Pour cela, il faut se conditionner à la situation de crise afin de lutter contre *l'infodemic,* terme anglais désignant la diffusion d'informations mensongères. Les hackers profitent de ce climat incertain en se servant de l'actualité ayant engendré ce sentiment de peur pour attaquer. Ils peuvent procéder ainsi : par la création de sites ressemblant aux sites officiels ; c'est le cas par exemple de l'appli Covid en 2020. Selon l'entreprise Palo Alto Networks, plus de 1700 noms de domaines ont été créés quotidiennement sur la période mars-avril 2020. Plus de 86000 sur 1,2 millions de noms de domaines recensés liés au Covid ont été catalogués comme étant dangereux car visant des procédés de phishing et autres.

Qu'il soit question de personnes physiques ou morales, l'appel à la vigilance est primordial. S'agissant des entreprises types start-up, TPE, PME, il est important de sensibiliser les personnes travaillant dans l'entreprise mais aussi de mettre en place une surveillance des communications réseaux entrantes et sortantes de l'entreprise. Préparer en amont une stratégie efficace afin d'anticiper les attaques, le but étant de préserver les actifs de ces entités : hôpitaux, entreprises, collectivités. S'agissant des grandes entreprises il est d'autant plus important de prévoir un plan de continuité du service. L'ANSSI, Agence nationale de la sécurité des systèmes d'information a également mis au point un guide d'accompagnement technique dans le but d'aider les particuliers et entreprises à se prémunir de ces différents types d'attaques. La CNIL, Commission nationale de l'informatique et des libertés, veille également au respect de la réglementation à travers le respect du règlement général en matière de protection de données, le RGPD, entré en vigueur et applicable depuis 2018 en France visant à sanctionner tout manquement en la matière.

La justice se mobilise elle aussi pour lutter contre ce fléau en vertu de la loi du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur

financement et améliorant l’efficacité ainsi que les garanties de la procédure pénale. L’article 706-72-1 du code de procédure pénale attribue compétence au procureur de la République, au pôle de l’instruction, au tribunal correctionnel ainsi qu’à la cour d’assises de Paris une compétence concurrente s’agissant d’atteintes aux systèmes de traitement automatisé de données et dans le cadre de cyber sabotage préjudiciable pour les intérêts fondamentaux de la Nation. Quoi qu’il en soit, tout le monde peut être la cible d’une cyberattaque.