PAYS :France
PAGE(S) :58-59
SURFACE :62 %
PERIODICITE :Trimestriel

JOURNALISTE :Ivan Kwiathowski

► 14 septembre 2021

Cliquez ici pour voir la page source de l'article

PUBLI INFO

ÉDUIRE LA VULNÉRABILITÉ ET RENFORCER A SÉCURITÉ NUMÉRIQUE DES TPE/PME

ragilisées par la crise sanitaire, les petites et moyennes structures ont longtemps craint pour leur survie et la érennité de leurs activités. Soutenues par le gouvernement dans le cadre du plan France Relance, elles ont pu énéficier de 25 milliards d'euros pour engager leur transition numérique, accélérer leur développement et réparer l'avenir à l'horizon 2030. Ce plan de soutien devrait leur permettre de dessiner une sortie de crise et trouver un niveau d'activité quasi normal, à condition de tout mettre en oeuvre pour renforcer leur sécurité umérique.

s TPE et PME, cibles vilégiées des hackers

cybermenace ne cesse de croître depuis 8, la pandémie de Covid-19 a été un eur aggravant pour les entreprises de tes tailles. La crise sanitaire a entraîné hausse des usages numériques liés aux finements, et notamment au recours sif au télétravail. Selon l'ANSSI, le nombre victimes de cyberattaques a été multiplié quatre en 2020. La même année, la plarme cybermalveillance.gouv.fr qui a pour sion d'assister les victimes de cyberattaques registré une hausse de sa fréquentation +155% par rapport à 2019 !

antage exposées aux risques cyber, les et PME sont une cible privilégiée pour attaques de type ransomware, l'espione, les pannes d'activité ou encore le vol données sensibles. Selon le Syntec Nuique, 77% d'entre elles sont victimes de erattaques.

s leur guide cybersécurité 2021 à destion des dirigeants de TPE, PME et ETI, rmalveillance.gouv.fr et Bpifrance publient yberattaques les plus fréquentes et leurs acts. Ainsi, 22% d'entre elles concernent ransomware, 20% les intrusions dans ystèmes d'information, 14% les piratages compte, 10% les usurpations d'identité % les hameçonnages (phishing).

onstat est sans appel : ces structures ne pas suffisamment sécurisées. Si leurs jeants affirment avoir conscience des séquences dramatiques d'une cyberatie, on note un décalage entre leur perion de la réalité et les actions menées se protéger. Les raisons invoquées dans anque de sécurité informatique sont ent les mêmes : manque de temps, de ources ou encore d'intérêt ("je ne suis ne petite structure, personne ne me aît, je suis à l'abri").

Le coût estimé des cyberattaques

Des infrastructures informatiques fragiles et non sécurisées entraînent de lourdes conséquences financières pour les petites et moyennes entreprises. Celles-ci sont les plus touchées en ce qui concerne le montant des pertes proportionnellement à la taille de l'entreprise. En 2021, pour les microentreprises de moins de dix salariés, le coût médian des attaques était d'environ 7273 €. Certaines structures ont subi des pertes de 280 000 €. Une entreprise de services allemande a même subi des failles représentant un coût de 430 909 € par salarié ! Ajoutons à cela que lorsqu'un hacker parvient à mettre la main sur des données personnelles, l'entreprise s'expose à une amende pouvant aller jusqu'à 4% de son chiffre d'affaires. Les attaques fragilisent la pérennité de l'activité des TPE/PME puisque ces structures risquent la faillite dans les trois mois suivants un incident de sécurité ou une cyberattaque.

Toutefois, si les coûts immédiats d'une cyberattaque sont bien connus, les coûts cachés sont moins facilement mesurables. Parmi les conséquences d'une attaque, la réputation de l'entreprise affectée, les interruptions d'activité ou encore la perte de données sensibles ne doivent pas être oubliées.

Des solutions de cybersécurité adaptées à tous les budgets

Dans ce contexte, la question n'est plus de savoir si l'attaque aura lieu un jour mais quand elle se produira. Il devient indispensable pour les TPE et PME d'investir dans la cybersécurité pour assurer leur pérennité, rester compétitives, mais surtout sereines.

Le budget restreint étant l'argument le plus souvent évoqué par les petites et moyennes structures pour justifier le manque d'investissement en cybersécurité, des solutions ont été développées pour les aider à se protéger sans se ruiner.

Wooxo propose un pack cybersécurité, une solution française et souveraine de prévention des cyberattaques et de reprise instantanée d'activité, spécialement conçue pour les TPE et PME. Le pack comprend une sauvegarde sécurisée contre les ransomware, le respect de la règle de sauvegarde du 3-2-1, une reprise d'activité instantanée en cas d'attaque, une restauration sur site ou hors site et une restauration autonome en moins d'une minute.

Adaptés à chaque budget, les services clé en main du pack cybersécurité garantissent zéro perte de données et zéro interruption d'activité. Un investissement justifié au regard de l'actualité, capital pour préserver ce que les entreprises ont de plus précieux : leurs données.

PAYS :France
PAGE(S) :58-59
SURFACE :62 %
PERIODICITE :Trimestriel

JOURNALISTE :Ivan Kwiathowski

► 14 septembre 2021

Cliquez ici pour voir la page source de l'article

Ivan Kwiathowski, Kaspersky

arbitraire sur le contrôleur de domaine. La seconde, baptisée PetitPotam et publiée plus tard courant juillet, est exploitable via le protocole MS-EFSRPC accessible sur le port TCP/445. Elle donne la possibilité à un attaquant non authentifié de forcer un serveur à se connecter à un autre serveur spécifique, lui permettant ainsi d'effectuer une attaque de type NTLM Relay.

SolarWinds, après les déboires de la fin d'année, a lui aussi été concerné par une vulnérabilité activement exploitée par les attaquants et qui a touché la gamme de produits Serv-U.

On a également beaucoup parlé de l'affaire Pegasus récemment, mais sans grand lien avec la cybercriminalité. Cette affaire qui semble toute tirée d'un roman a surtout mis en exergue une tendance toujours plus présente : le cyberespionnage. Au-delà de confirmer le rôle grandissant des États dans les cyberattaques récentes, cette affaire confirme également le passage à l'offensive de nombreux gouvernements sur les sujets d'espionnage. Israël, pays dont l'entreprise qui revendait le logiciel d'espionnage incriminé est originaire, a d'ailleurs dû envoyer une délégation à Paris pour tenter de limiter les dégâts et reprendre le sujet sur un volet plus diplomatique. Le cyberespionnage est un sujet qui prend de plus en plus de place, jusqu'au plus haut sommet de l'État français. Le gouvernement met d'ailleurs en garde ses entreprises quant à ces risques au travers de publications régulières de la DGSI. Le volet cyber semble donc prendre une place prépondérante dans les relations diplomatiques et même économiques entre les États. »

Enfin, pour Ivan Kwiatkowski, chercheur en cybersécurité, Kaspersky, l'évènement marquant de cet été dans le domaine de la cybersécurité concerne également la série d'articles et de révélations sur NSO Group et son malware commercial, Pegasus. Si l'existence de vulnérabilités 0day « zéro clic » pour téléphones mobiles n'était une surprise pour personne, cela a été l'occasion, selon lui, pour la société civile de découvrir la relative facilité d'accès à ce type d'outils, ainsi que la diversité des cibles de telles attaques : membres de gouvernements bien sûr, mais aussi journalistes, militants, activistes et défenseurs des droits de l'Homme. « Ces dernières années, l'industrie de la cybersécurité s'est beaucoup concentrée sur la problématique des ransomwares, qui touche avant tout les entreprises. Cette affaire rappelle que les individus et les personnalités sont eux aussi susceptibles d'être victimes d'attaques informatiques aux conséquences gravissimes (pouvant aller jusqu'à la mort !). Mon espoir est que ces découvertes remettront la problématique de la prolifération des outils offensifs sur le devant de la scène et donneront lieu au débat de société qu'elle mérite. », conclut-il. ■■■

[1] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855
[2] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26857
[3] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26858
[4] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27065
[5] https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups
[6] https://www.welivesecurity.com/author/zhromcova
[7] https://www.welivesecurity.com/author/acherepanov
[8] https://www.welivesecurity.com/2021/08/06/anatomy-native-iis-malware
[9] https://www.welivesecurity.com/?s=iis