Sécurité IT: les entreprises en France ne sont pas assez protégées

En ce mois d'octobre dédié à la sensibilisation à la cybersécurité et à la veille de l'ouverture des Assises de la sécurité à Monaco, **IDC** se fend d'une nouvelle étude consacrée à la sécurité informatique des entreprises en France et commandée par **Malwarebytes**.

Ce nouvel observatoire Cybersécurité révèle en premier lieu la prise de conscience des organisations face aux cybermenaces.

Un mal pour un bien ? Les déferlantes de ransomware Wannacry, Petya voire NotPetya au cours du premier semestre 2017 ont indiscutablement servi de sonnette d'alarme.

De fait, 76% des entreprises de plus de 500 salariés (dont 50% de plus de 1000 collaborateurs), tous secteurs confondus, la protection des données sensibles reste la principale préoccupation.

« Cela signifie que 34% d'entres elles ne le sont pas alors que les attaques en France ont explosé ces derniers mois », commente Justin Dolly, responsable sécurité chez l'éditeur américain de solutions de sécurité, rencontré par Silicon.fr en début de semaine.

Ce que confirment 51% des directions métiers sondées (58% dans les PME) qui déclarent avoir constaté une hausse des attaques au sein de leur organisation ces 12 derniers mois.

La majorité des entreprises mal protégées face aux ransomwares

Les conséquences de ces attaques sont diverses. Pour 39% des répondants, cela se traduit par une indisponibilité du site Web et, pour 27% d'entre eux, par un retard de livraison auprès des clients.

Dans des scénarios plus noirs, 23% des entités victimes ont dû interrompre la production tandis que 20% d'entre elles ont constaté une perte sur le chiffre d'affaires.

Certaines ne s'en cachent plus à l'image de Saint-Gobain qui, victime de NotPetya en juin dernier, a reconnu un manque à gagner de 250 millions d'euros.

Notons enfin que près d'un tiers des sondés (32%) déclarent ne pas constater d'impact suite à une attaque.

Peut-être s'agit-il des 37% des grandes entreprises et 25% des PME qui se déclarent capables de réagir en moins d'une heure à une charge malveillante. Un temps de réaction court qui limite drastiquement les dégâts.

Néanmoins, pour la majorité des cas (71% chez les PME, 16% des entreprises), il faut compter entre 1 et 5 heures après le déclenchement de l'assaut pour engager une parade.

Qui plus est, 59% des entreprises de plus de 1000 salariés considèrent ne pas être suffisamment protégées face aux ransomware. Lesquels se multiplient comme des petits pains.

« Il est beaucoup plus facile d'écrire des malware aujourd'hui qu'il y a 5 ans », affirme Justin Dolly. *« On trouve facilement en ligne des kits de développement exploitables par n'importe qui. C'est aussi simple que pour lancer des campagnes de spam il y a quelques années. »*

Eduquer les utilisateurs

Comment répondre à l'augmentation des attaques ?

Pour la majorité des répondants (46%), la réponse passe par l'éducation des utilisateurs.

« La politique de sécurité n'est désormais plus uniquement portée par le RSSI, elle est décloisonnée pour laisser une place de choix aux directions métiers, impactées en 1er lieu par les menaces de sécurité », illustre IDC dans son rapport.

La protection des données arrive en second (43%) des priorités. L'évolution de la législation avec l'application du RGPD en mai 2018 n'y est probablement pas étrangère.

« Le RGPD est une bonne chose, déclare notre interlocuteur, *ça va engendrer le changement. Et l'Europe est clairement en avance sur la protection de la donnée privée. »*

Rappelons que le RGPD (Règlement européen sur la protection des données ou GDPR en anglais) impose aux entreprises exerçant une activité en Europe des mesures de protection des données et risquent une amende jusqu'à 4% de leur chiffre d'affaires en cas de manquement à la réglementation.

5 milliards de malware éliminés

Or, les PME sont en retard sur le sujet. Selon IDC, seules 32% d'entre elles ont défini un calendrier de mise en conformité pour répondre aux évolutions réglementaires, contre 51% des grandes entreprises.

« Les grandes entreprises peuvent conduire le changement », avance le responsable sécurité de Malwarebytes. « *Par exemple, les banques peuvent imposer à leurs clientes PME à installer des systèmes sécurisés. »*

Le renforcement des systèmes d'analyse en temps réel s'inscrit d'ailleurs comme une des priorités majeures pour 36% des organisations sondées.

Un domaine dans lequel le fournisseur américain de solutions de sécurité IT, créé en 2008 par Marcin Kleczynski, excelle.

« Les solutions Malwarebytes ont permis d'éliminer plus de 5 milliards de malware ces trois dernières années », assure Doron Aronson, responsable communication du fournisseur de solutions de sécurité. Autrement dit, depuis que Malwarebytes se concentre sur le marché entreprises.

Aujourd’hui, l’éditeur revendique plus de 10 000 sociétés clientes.

Lire également

Lutte anti-ransomware : les entreprises françaises privilégient la sensibilisation

La France, 4eme pays le plus touché au monde par WannaCry

Mois européen de la cybersécurité : la France y participe (enfin) activement