Cybersécurité : les prévisions de Sophos pour 2018

2018 ne sera pas l'année d'un « Pearl Harbor numérique » (une attaque informatique capable de paralyser tout un pays), mais de l'industrialisation des malwares, selon Sophos.

L'éditeur britannique de logiciels met en exergue six prévisions de cybersécurité :

1. Attaques « sans fichier »

Sophos prévoit une augmentation des attaques utilisant des malwares et chevaux de Troie « sans fichier ». Des programmes qui tournent en mémoire de systèmes, comme l'ont fait Poweliks, Angler, Kovter et, plus récemment, Powmet.

« À ce jour, les attaques 'sans fichier' ont été assez isolées, mais elles semblent prendre de plus en plus d'importance. Il s'agit d'une réponse au déploiement à grande échelle de l'apprentissage automatique (machine learning) », a expliqué par voie de communiqué Fraser Howard, chercheur principal en charge des menaces informatiques chez l'éditeur.

L'utilisation malvaillante de l'interpréteur de ligne de commande Windows PowerShell de Microsoft devrait encore gagner du terrain, a ajouté Sophos.

2. Tests à données aléatoires

Par ailleurs, l'éditeur de logiciels d'origine britannique s'attend à une amélioration de la sophistication des tests à données aléatoires (fuzzing) de logiciels.

« Le fuzzing peut être utilisé pour créer automatiquement des milliards de tests 'stupides'. Le prochain défi consistera à rendre ces tests plus intelligents. Et ce en alimentant le processus de création du test en connaissances additionnelles sur les principes de fonctionnement d'un programme », a souligné Stephen Edwards, chercheur en sécurité chez Sophos.

« Cependant l'exploration automatique du code est difficile. Les techniques hybrides tentent par conséquent d'équilibrer la vitesse des tests 'stupides' avec l'efficacité d'autres tests intelligents'. Et ce tout en évitant de se perdre dans une trop grande quantité de choix », a-t-il ajouté.

3. Gestion du risque

Alors que s'estompent les frontières entre un réseau classique et internet, *« nous devons déterminer le risque en fonction de l'identité et des ressources (assets) associées à cette identité »*, a commenté Mark Lanczak-Faulds, chercheur en cybersécurité de l'éditeur.

« Lorsqu'une alerte est déclenchée en tenant compte de ces facteurs, les DSI sont conscients des enjeux et peuvent agir de manière appropriée et rapidement », a-t-il ajouté.

4. Atténuation des exploits

Pour Sophos, l'installation des correctifs/patchs est un élément clé de la cybersécurité. La détection de menaces et fichiers PE (Portable Executable) basée sur l'apprentissage automatique, ne devrait pas retarder cette installation de correctifs.

5. Ransomware multi-plateforme

Le rançongiciel (ransomware) évolue. Si les ransomwares (WannaCry, Petya, Cerber, Locky…) ont surtout ciblé les systèmes Windows l'an dernier, les plateformes Android, Linux et MacOS n'ont pas non plus été épargnées (rapport SophosLabs).

La diffusion multi plateformes de ransomwares devrait se confirmer en 2018.

Par ailleurs, pour déjouer les protections de cybersécurité, les ransomwares changent. Ils peuvent être utilisés pour dissimuler d'autres programmes malveillants, des enregistreurs de frappe ou des mineurs de crypto-monnaies, par exemple.

6. Protection des données

Le Règlement général sur la protection des données (RGPD) entre en vigueur le 25 mai 2018 dans l'Union européenne. Toutes les entreprises (responsables de traitement et sous-traitants) traitant des données personnelles de résidents devront s'y conformer.

« Je m'attends à passer beaucoup de temps à supprimer des données inutiles et à faire très attention aux données stockées et où elles le sont », a déclaré Ross McKerchar, directeur cybersécurité chez Sophos.

En stockant moins de données, les DSI peuvent donc limiter les risques.

Lire également :

Cybersécurité : Proofpoint livre ses prédictions pour 2018

Sécurité : la logistique fortement menacée en 2018, selon Kaspersky

crédit photo © Shutterstock