Bitdefender

Des barrières améliorées pour renforcer le dernier rempart : gestion des patchs et chiffrement

Dans un environnement de plus en plus hostile où des cyberattaques massives font la une des journaux pratiquement tous les mois, les entreprises commencent à modifier leur modèle de défense pour avoir une meilleure visibilité sur la manière dont ces attaques sont orchestrées, et pour comprendre pourquoi elles les ont ciblées. Une fois convaincus qu'une violation est inévitable, et après avoir adopté des outils de détection et de réponse utiles, les RSSI se concentrent sur la réduction de la surface d'attaque tout en ajoutant des protections supplémentaires à leur infrastructure. C'est là où la gestion des patchs et le chiffrement peuvent faire la différence.

MAINTENIR LES BIENS PRÉCIEUX HORS DE VUE

Une enquête de Bitdefender réalisée auprès de 1 051 professionnels de la sécurité chargés des achats de solutions en Europe et aux États-Unis a révélé que selon 4 RSSI sur 5, le chiffrement est le dispositif le plus efficace pour protéger les données, suivi des logiciels de sécurité et des sauvegardes. Si on étudie leur répartition géographique, on constate que le chiffrement est la méthode privilégiée en Italie, au Royaume-Uni et aux États-Unis ; mais en moyenne seule une entreprise sur six chiffre toutes ses données.
Trois preneurs de décisions en matière de sécurité informatique sur quatre citent les coûts et l'atteinte à la réputation de leur entreprise comme les pires conséquences auxquelles ils auraient à faire face si une menace avancée réussissait à accéder aux « joyaux de la couronne ».
Les données critiques relevant de la propriété intellectuelle doivent être enregistrées sur site, avoir un accès restreint et n'être accessibles que par le personnel autorisé. Toutes les données stockées en local ou dans le cloud doivent également être chiffrées pour empêcher les cybercriminels de les lire en cas de violation de données ou d'accès non autorisé.

Les RSSI devraient se prémunir contre le risque de perte de données et se conformer aux réglementations en chiffrant intégralement le disque dur de leurs endpoints mobiles.

GravityZone Full Disk Encryption protège l'intégralité des données situées sur le disque dur de l'endpoint en tirant profit des systèmes de chiffrement fournis par Windows (BitLocker) et par Mac (FileVault). La fonctionnalité s'appuie sur des systèmes de chiffrement natifs des appareils pour assurer une compatibilité totale et des performances maximales. GZ Full Disk Encryption est intégré à la console et à l'agent GravityZone, sans avoir à déployer d'agent supplémentaire ni à installer de serveur de gestion des clés. L'utilisation de l'infrastructure de sécurité des endpoints existante pour gérer Full Disk Encryption permet un déploiement intégralement centralisé, ce pour un minimum d'effort d'administration.

COMBLER LES LACUNES

Tandis que les systèmes obsolètes sont source d'attaques de malwares et de violations de données pour les organisations, la moitié des RSSI interrogés admettent également que l'expansion de leur infrastructure a augmenté la surface d'attaque de leur entreprise. Les spécialistes de la sécurité conseillent fortement aux RSSI de veiller à ce que tous leurs logiciels soient toujours à jour. Une tâche rendue plus simple par les outils de gestion des patchs, qui aident ainsi les entreprises à éviter tout événement néfaste, comme les tristement célèbres épidémies WannaCry et GoldenEye.

Le module GravityZone Patch Management permet d'installer les patchs automatiquement ou manuellement. Grâce à lui, les entreprises peuvent gérer les patchs de manière plus souple et plus efficace. Il permet de créer un inventaire des patchs, de planifier des analyses des patchs, de limiter les mises à jour aux applications sélectionnées par l'administrateur, d'adapter le planning pour les patchs liés ou non à la sécurité, et de reporter le redémarrage après les installations en nécessitant un. Dans le contexte actuel en matière de cybersécurité, l'application de patchs sur les systèmes d'exploitation et les applications est devenue une priorité pour les services informatiques, pour des raisons de sécurité mais aussi de conformité. GravityZone Patch Management peut vérifier l'état des patchs de l'ensemble de l'entreprise, conformément aux politiques et réglementations.