Les PME face au risque de ransomwares

Internet

Posté par : JerryG

Publié le : 18/12/2023 13:00:00

Dans son récent rapport Mission PME et cybersécurité, Michel Van Den Berghe, Président du Campus Cyber, souligne au ministre délégué chargé de la transition numérique et des télécommunications Jean-Noël Barrot, l'importance de la prévention et de la sensibilisation des PME au cyber-risque. Ces dernières sont en effet la cible de cyberattaques, y compris de ransomwares, qui font partie des attaques les plus courantes.

Selon Dirk Schader, Resident CISO (EMEA) et VP of Security Research chez Netwrix, les petites entreprises sous-estiment souvent le risque d'attaque auquel elles sont exposées. Elles pensent en effet que les cybercriminels ont tendance à cibler les grandes entreprises parce qu'elles stockent davantage de propriété intellectuelle et d'autres données sensibles. En réalité, le risque de cyberattaque est pratiquement le même quelle que soit la taille de l'entreprise :

« Chaque organisation possède des données précieuses, telles que des informations sur les clients et les employés, et constitue donc une cible pour les attaquants. De plus, les PME ne sont pas seulement une cible en elles-mêmes, mais aussi une voie d'accès vers les grandes entreprises avec lesquelles elles interagissent.

L'un des principaux défis auxquels sont confrontées les petites organisations est le manque de personnel. Il n'est pas rare que le seul administrateur informatique soit responsable de l'ensemble de l'infrastructure, y compris de sa sécurité.

L'externalisation des tâches liées à la sécurité auprès d'un fournisseur de services managés (MSP) ou d'un fournisseur de services de sécurité managés (MSSP) peut aider à relever ce défi. Toutefois, il est essentiel de veiller à ce que les éléments essentiels de la cybersécurité soient assurés en interne sur trois niveaux principaux : les données sensibles, les identités utilisées pour accéder à ces données et l'infrastructure en place.

Les informations d'identification, les comptes et les identités sont les connecteurs entre les données et l'infrastructure. Tant données que les ransomwares s'appuient souvent sur les droits d'accès du compte utilisateur qu'ils ont compromis, perpétuer l'application de principes de moindre privilège minimisera la quantité de données susceptibles d'être chiffrées lors d'une attaque.

En outre, l'accès en flux tendu conduit considérablement la surface d'attaque puisque le privilège n'est accordé que temporairement et pour l'exécution d'une tâche spécifique.

L'exfiltration ou le chiffrement des données ne se produit pas immédiatement ; ces deux phénomènes prennent du temps, et une détection et une réaction précoces peuvent contribuer à limiter les dégâts. L'audit d'activité qui détecte les anomalies dans le comportement des utilisateurs est le meilleur moyen de repérer une attaque à un stade précoce.

Enfin, le paiement d'une rançon n'est pas une option. Il n'y a aucune garantie qu'une PME obtienne la clé de chiffrement une fois l'argent versé. De plus, même en cas de réception de la clé, rien ne garantit que les opérations puissent être rétablies du jour au lendemain.

De plus, si les entreprises paient, rien n'empêche les pirates de les attaquer à plusieurs reprises, et chaque demande de rançon pourrait être plus élevée que la précédente. Les PME et leurs dirigeants gagneront ainsi à mieux se protéger des cybermenaces insistantes, et les gouvernements joueront un rôle décisif dans le combat contre les ransomwares, par le biais de l'éducation et de la prévention. »