Les PME face au risque de ransomwares
Internet
PostÃ© par : JerryG
PubliÃ©e le : 18/12/2023 13:00:00

Dans son rÃ©cent rapport Mission PME et cybersÃ©curitÃ©, Michel Van Den Berghe, PrÃ©sident du Campus Cyber, souligne au ministre dÃ©lÃ©guÃ© chargÃ© de la transition numÃ©rique et des tÃ©lÃ©communications Jean-NoÃ«l Barrot, lâ□□importance de la prÃ©vention et de la sensibilisation des PME au cyber-risque. Ces derniÃ¨res 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 exposÃ©es. Elles pensent en effet que les cybercriminels ont tendance Ã cibler les grandes entreprises parce qu'elles stockent davantage de propriÃ©tÃ© intellectuelle et d'autres donnÃ©es sensibles. En rÃ©alitÃ©, le risque de cyberattaque est pratiquement le mÃªme quelle que soit la taille de l'entreprise :

Â« Chaque organisation possÃ¨de des donnÃ©es prÃ©cieuses, telles que des informations sur les clients et les employÃ©s, et constitue donc une cible pour les attaquants. De plus, les PME ne sont pas seulement une cible en elles-mÃªmes, mais aussi une voie d'accÃ¨s vers les grandes entreprises avec lesquelles elles interagissent.

L'un des principaux dÃ©fis auxquels sont confrontÃ©es 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 sÃ©curitÃ©.

L'externalisation des tÃ¢ches liÃ©es Ã la sÃ©curitÃ© auprÃ¨s d'un fournisseur de services managÃ©s (MSP) ou d'un fournisseur de services de sÃ©curitÃ© managÃ©s (MSSP) peut aider Ã relever ce dÃ©fi. Toutefois, il est essentiel de veiller Ã ce que les Ã©lÃ©ments essentiels de la cybersÃ©curitÃ© soient assurÃ©s en interne sur trois niveaux principaux : les donnÃ©es sensibles, les identitÃ©s utilisÃ©es pour accÃ©der Ã ces donnÃ©es et l'infrastructure en place.

Les informations d'identification, les comptes et les identitÃ©s sont les connecteurs entre les donnÃ©es et l'infrastructure. Ã□tant donnÃ© que les ransomwares s'appuient souvent sur les droits d'accÃ¨s du compte utilisateur qu'ils ont compromis, perpÃ©tuer lâ□□application de principes de moindre privilÃ¨ge minimisera la quantitÃ© de donnÃ©es susceptibles d'Ãªtre chiffrÃ©es lors d'une attaque.

En outre, l'accÃ¨s en flux tendu rÃ©duit considÃ©rablement la surface d'attaque puisque le privilÃ¨ge n'est accordÃ© que temporairement et pour l'exÃ©cution d'une tÃ¢che spÃ©cifique.

L'exfiltration ou le chiffrement des donnÃ©es ne se produit pas immÃ©diatement ; ces deux phÃ©nomÃ¨nes prennent du temps, et une dÃ©tection et une rÃ©action prÃ©coces peuvent contribuer Ã limiter les dÃ©gÃ¢ts. L'audit d'activitÃ© qui dÃ©tecte les anomalies dans le comportement des utilisateurs est le meilleur moyen de repÃ©rer une attaque Ã un stade prÃ©coce.

Enfin, le paiement d'une ranÃ§on n'est pas une option. Il n'y a aucune garantie quâ□□une PME obtienne la clÃ© de chiffrement une fois l'argent versÃ©. De plus, mÃªme en cas de rÃ©ception de la clÃ©, rien ne garantit que les opÃ©rations puissent Ãªtre rÃ©tablies du jour au lendemain.

De plus, si les entreprises paient, rien n'empÃªche les pirates de les attaquer Ã plusieurs reprises, et chaque demande de ranÃ§on pourrait Ãªtre plus Ã©levÃ©e que la prÃ©cÃ©dente. Les PME et leurs dirigeants gagneront ainsi Ã mieux se protÃ©ger des cybermenaces insistantes, et les gouvernements joueront un rÃ´le dÃ©cisif dans le combat contre les ransomwares, par le biais de lâ□□Ã©ducation et de la prÃ©vention. Â»