Comment contenir les déplacements latéraux des hackers

Internet

Posté par : JerryG

Publié le : 23/8/2023 13:00:00

Selon le cabinet Asteris, il y aurait eu 385 000 cyberattaques réussies contre des organisations publiques et privées en France en 2022, pour un coût global de 2 milliards d'euros.

Les entreprises doivent donc admettre que, même en ayant mis en place une stratégie « Zero Trust » pour sécuriser leur réseau et leur infrastructure, un cybercriminel parviendra indubitablement à s'introduire dans un réseau, à y déployer un ransomware ou à causer d'autres dommages. C'est pourquoi il est nécessaire de connaître les menaces et de savoir comment s'en protéger.

Pour Dirk Schrader, Resident CISO (EMEA) and VP of Security Research chez Netwrix, les entreprises doivent comprendre le rôle clé des déplacements latéraux et agir pour les empêcher :

« Une attaque typique se déroule généralement en trois étapes. Tout d'abord, un cybercriminel compromet un compte utilisateur via une campagne d'hameçonnage, par exemple, ce qui lui permet de s'immiscer dans un terminal, un appareil IoT ou un système.

Ensuite, il se déplace latéralement à l'intérieur de l'appareil - dans l'environnement et escalade les privilèges jusqu'à obtenir l'accès à des ressources informatiques sensibles.

Cette étape peut durer des semaines, voire des mois, car l'hacker prend son temps pour étudier le réseau et les ressources de l'entreprise ciblée. On pense à tort que les mouvements latéraux se limitent aux réseaux sur site.

Or, ils peuvent se produire dans les environnements cloud, mais également entre les systèmes sur site et cloud. Enfin, le hacker exfiltre des données sensibles, déploie des ransomwares ou d'autres logiciels malveillants, et/ou endommage les systèmes pour stopper l'activité de l'organisation.

Pour empêcher ces déplacements latéraux, et donc contenir les attaques, il convient de mettre en œuvre les pratiques suivantes :

☛ Restreindre l'accès de l'administrateur local - Il est temps d'arrêter d'accorder des droits d'admin local à des utilisateurs standards : lorsqu'un compte est compromis, les cybercriminels tirent profit de ses droits d'accès ; ne pas disposer de tels droits bloque donc significativement la portée des cybercriminels.

☛ Appliquer le principe du moindre privilège - Il stipule que chaque utilisateur et chaque processus ne doit avoir accès qu'aux ressources du réseau dont il a strictement besoin pour accomplir les tâches qui lui sont assignées, et rien de plus. Sa compréhension initiale a évolué pour inclure un élément temporel : le privilège ne doit exister que tant qu'il est nécessaire pour une tâche donnée.

☛ Bloquer les attaques par ingénierie sociale - Les cybercriminels accèdent souvent à un environnement informatique cible par le biais d'une attaque d'ingénierie sociale au cours de

laquelle ils manipulent un utilisateur légitime pour qu'il fournisse ses identifiants. La sensibilisation à la sécurité est donc clé, car les employés restent encore trop souvent les maillons faibles de la chaîne de sécurité. Des outils de filtrage du courrier électronique et du web permettent également d'atténuer ces types d'attaques.

🔒 Protéger les mots de passe - Des mots de passe faibles permettent aux cybercriminels de voler facilement des identifiants. Il existe des outils qui permettent de s'assurer que des normes de complexité conformes aux meilleures pratiques sont exigées pour tous les mots de passe. Ces politiques sont à soutenir par des formations régulières à la cyber-hygiène pour tous les utilisateurs. En outre, la MFA (l'authentification multifacteurs) doit être appliquée à tous les comptes privilégiés.

🔒 Remplacer les comptes privilégiés permanents par un accès juste à temps et surveiller l'activité - Les droits admin sont les clés du royaume pour un hacker. La mise en œuvre d'une stratégie solide de gestion des accès privilégiés (PAM) est essentielle pour protéger les comptes privilégiés contre la compromission. Elle permet d'identifier ces derniers dans le parc informatique et de réduire la surface d'attaque en les remplaçant par un accès juste à temps limité à l'accomplissement de tâches spécifiques. En outre, cette technologie procure une visibilité sur ce que les utilisateurs privilégiés font dans l'environnement informatique et alerte l'équipe IT en cas de comportement suspect.

Les mouvements latéraux sont une technique courante des attaquants, qui leur permettent d'établir leur présence dans le réseau d'une entreprise et de parvenir à leurs fins. Il est donc essentiel de les empêcher et de contenir les actions des utilisateurs malveillants avec les stratégies, les techniques et les outils adéquats. »