Options de configuration : cinq conseils pour éviter les failles de sécurité

Pour les pirates informatiques, l'environnement idéal pour une attaque est celui qui demande aussi peu d'effort que possible à infiltrer. Ces opportunités s'expliquent par des systèmes peu ou mal configurés et entraînent une vulnérabilité totale de l'environnement et de ses données.

Voici les cinq principales erreurs de configuration qui peuvent entraîner des failles de sécurité.

1. Ne pas reconfigurer les identifiants par défaut

L'une des erreurs les plus courantes, et pourtant les plus évidentes, consiste à ne pas reconfigurer les noms d'utilisateur et les mots de passe par défaut des bases de données, des installations et des équipements. C'est un problème tellement basique qu'il est comparable à des clés laissées sur une porte verrouillée. Et quand cela arrive, les informations d'identification par défaut sont l'une des erreurs de configuration les plus faciles à exploiter.

Les scanners de vérification des mots de passe peuvent en effet permettre aux hackers d'accéder aux équipements clés du réseau, comme les pare-feu et les routeurs. Même les systèmes d'exploitation peuvent se trouver exposés à cause d'informations d'identification par défaut. Les attaques de force brute scriptées peuvent également fournir accès aux divers équipements en ciblant des noms d'utilisateur et des mots de passe par défaut, ou des options basiques comme « 12345 », « azerty » ou « password ».

Le processus est également automatisé jusqu'à un certain point. Les chercheurs ont récemment découvert un scanner web en Python appelé Xwo, en mesure de balayer facilement le web à la recherche de services web exposés et de mots de passe par défaut.
Après avoir collecté les informations d'identification par défaut pour MySQL, MongoDB, Postgre SAL et Tomcat, le scanner transfère les résultats à un serveur de commande et contrôle pour poursuivre son action.

2. Retarder la mise à jour des logiciels

Les prestataires technologiques et les spécialistes de la sécurité répètent ce message essentiel à la sécurité depuis des années. Pourquoi ? Parce que c'est efficace. Des systèmes d'exploitation mis à jour à l'aide des derniers correctifs peuvent avoir un impact crucial sur la prévention des failles.

Certes, il peut être difficile de suivre le rythme des correctifs. Ces éléments peuvent changer tous les jours, et le défi s'étoffe à mesure que les environnements se complexifient. Mais si les administrateurs n'assurent pas une maintenance correcte sur le plan des correctifs, ils ne font qu'attendre un accident inévitable.

Et les attaquants continueront à exploiter les vieux bugs tant qu'ils seront efficaces. Bien que la détection et la prévention des vulnérabilités de type « Zéro Day » suscitent une attention justifiée,

les vulnérabilités les plus couramment exploitées remontent, par comparaison, à l'âge de pierre du numérique.

3. Appliquer les mêmes mots de passe sur différents périphériques

Bien que des mots de passe forts et complexes constituent l'un des piliers de toute stratégie de sécurité basique, même lorsqu'ils sont mis en place, leur utilisation est discutable. Les environnements utilisent souvent le même compte utilisateur et le même mot de passe sur tous les périphériques d'un parc de terminaux.

L'une des principales raisons est que cela facilite la gestion. Mais, et c'est un inconvénient majeur, c'est également pratique pour les hackers, et cela peut leur permettre de compromettre toutes les machines à partir d'une faille sur une seule d'entre elles. À partir de là, ils peuvent utiliser des programmes d'extraction des informations d'identification pour révéler les mots de passe, voire leurs hachages. C'est alors que les vrais problèmes commencent.

La réutilisation des mots de passe doit être évitée à tout prix, et les comptes non indispensables doivent être désactivés avant de pouvoir fournir un accès.

4. La mauvaise configuration des interfaces à distance

Tout appareil en contact avec l'extérieur et connecté à Internet doit faire l'objet d'une protection particulièrement soignée. Des services tels que le protocole propriétaire RDP (Remote Desktop Protocol) développé par Microsoft peuvent fournir aux administrateurs une interface permettant de contrôler les ordinateurs à distance. Mais leur mauvaise configuration offre aux cybercriminels une possibilité d'accéder aux systèmes.

Par exemple, des ransomwares tels que CrySiS et SamSam ont déjà ciblé les entreprises via des ports RDP ouverts, en utilisant des attaques par force brute et par dictionnaire. Les administrateurs doivent utiliser une combinaison de mots de passe forts et complexes, de pare-feu et de listes de contrôle d'accès pour réduire le risque de compromission.

5. Désactiver la journalisation ou la cape d'invisibilité des hackers

Bien que la désactivation de la journalisation ne permette pas nécessairement à un attaquant d'accéder à un système, cela lui permet d'agir en restant inaperçu sur la machine. Lorsque la journalisation est désactivée, les pirates informatiques peuvent se déplacer latéralement sur un réseau à la recherche de données ou d'actifs à exploiter, sans laisser de trace de leur activité.

Cela complique énormément le travail des analystes judiciaires et des intervenants en cas

d’incident lorsqu’ils doivent reconstituer ce qui s’est produit lors d’un incident ou d’une intrusion. En revanche, il peut être très bénéfique d’activer la journalisation et d’en envoyer les données vers un emplacement centralisé, par exemple une plateforme de gestion des informations et des événements de sécurité (SIEM). Ces données fourniront les indices nécessaires aux analystes judiciaires lors d’une enquête pour reproduire l’attaque et comprendre l’ampleur de l’intrusion.

Tout périphérique, toute plateforme laissé(s) dans un état par défaut ou mal configuré facilite d’autant le travail d’un criminel. Bien que ces vulnérabilités n’entraînent pas nécessairement de problèmes tout de suite, les pirates informatiques les découvriront probablement à un moment donné et les exploiteront pour obtenir un accès non autorisé.

La mise en place de configurations de sécurité appropriées pour protéger les applications, les serveurs et les bases de données peut aider les entreprises à préserver leurs données et leur éviter de devenir une cible facile.