beazley

Aperçu de l'industrie

Le danger des vulnérabilités exposées sur Internet: ce que les organisations doivent savoir

Un élément important du protocole de cybersécurité d'une organisation consiste à maintenir une vigilance continue en ce qui concerne les vulnérabilités exposées sur Internet. Une vulnérabilité est une faiblesse ou une faille qui permet à un auteur malveillant de rompre au moins l'un des trois principes de sécurité : confidentialité, intégrité et disponibilité. Une fois qu'une vulnérabilité de sécurité est décelée, les développeurs et les équipes de sécurité travaillent ensemble pour fournir un correctif, appelé correctif de sécurité.

De nouvelles vulnérabilités critiques à haut risque sont découvertes et publiées chaque jour, en moyenne jusqu'à 15 par jour au premier semestre 2022. Certaines de ces vulnérabilités ont été exploitées pendant des années avant d'être découvertes par la communauté de la sécurité et que des correctifs de sécurité efficaces soient mis à disposition. Il est donc très difficile pour les équipes informatiques de suivre et d'appliquer les correctifs de sécurité avant que les acteurs de la menace ne découvrent et n'exploitent les vulnérabilités. Le délai moyen de mise à jour des correctifs se situe entre 60 et 150 jours, mais des études ont montré que certaines vulnérabilités sont identifiées et exploitées par des acteurs malveillants 5 minutes après avoir été divulguées publiquement.

De plus, que les composants logiciels soient corrigés ou non, certaines applications sont vulnérables en raison de pratiques de développement logiciel non sécurisées, de l'utilisation de bibliothèques et de packages de développement compromis ou de configurations de sécurité faibles, en particulier dans les environnements cloud (avec l'hypothèse courante selon laquelle ces environnements sont " sécurisés par défaut »).

L'impact de l’exploitation réussie d'une vulnérabilité peut aller de la divulgation de données techniques ou d'un déni de service à la compromission totale d'un système, ce qui conduit souvent à une

infiltration du réseau. Heureusement, il y a des choses que les organisations peuvent faire pour se protéger contre ces attaques

Construisez des systèmes avec la « sécurité dès la conception »

Plusieurs pratiques peuvent aider à réduire le nombre de vulnérabilités dans vos systèmes. Tout d'abord, formez vos développeurs et programmeurs aux pratiques de sécurité et fournissez-leur des outils de révision du code source de sécurité. Deuxièmement, définissez une stratégie d'utilisation et de suivi des bibliothèques et du code open source. Et enfin, définissez des directives de renforcement de la configuration pour vos types d'actifs les plus utilisés et les plus critiques (en particulier pour les ressources cloud).

Réduisez votre surface d'attaque

Un bon moyen de protéger vos actifs est de ne pas les exposer à Internet. Ceci est particulièrement valable pour les protocoles d'administration et de gestion à distance. Idéalement, cela signifie limiter l'accès aux employés connectés à votre réseau d'entreprise, soit en étant physiquement sur site, soit en utilisant des procédures de connexion à distance sécurisées (par exemple, un VPN avec MFA). Cela s'applique également à l'accès aux applications et projets sensibles dans les environnements de développement ou de test où les fichiers de configuration ou de sauvegarde peuvent être facilement accessibles. Dans certains cas où un VPN n'est pas une option, limiter les connexions à des adresses IP source prédéfinies spécifiques peut également aider à limiter votre surface d'attaque.

Identifiez les vulnérabilités avant que les pirates ne le fassent

Il existe plusieurs méthodes pour identifier les vulnérabilités. Certaines d'entre eux peuvent être automatisées, tandis que d'autres nécessitent des interventions manuelles de la part de professionnels de la sécurité. Idéalement, une organisation utilisera une combinaison de méthodes, y compris des analyses de vulnérabilité régulières automatisées (idéalement mensuelles), des tests d’intrusion par des professionnels spécialisés (en commençant par les applications sensibles), des programmes de primes aux bogues, une surveillance de sécurité quotidienne ou automatisée et une chasse aux vulnérabilités.

Réduire la probabilité d'une exploitation réussie

Pour réduire la probabilité que des acteurs malveillants exploitent des vulnérabilités ou compromettent des systèmes, une organisation dispose d'un certain nombre d'options. Le plus critique est d'assurer une action immédiate pour appliquer des correctifs de sécurité ou une autre protection adéquate, comme limiter temporairement l'exposition

à Internet ou placer le service derrière un WAF correctement configuré en mode blocage. Il est également conseillé aux organisations de déployer l'EDR avec la correction automatique activée sur les serveurs exposés à Internet. Cela peut arrêter certaines tentatives d'exploitation dans leur élan. Et enfin, durcissez la configuration de vos serveurs susceptibles d'exposer des services et applications sur internet. Cela inclut la désactivation ou le masquage des services et fonctionnalités inutiles ou non sécurisés tels que les protocoles obsolètes.

Limiter l'impact d'une exploitation réussie

L'exploitation réussie d'une vulnérabilité ne conduirait pas nécessairement à une compromission complète d'un serveur ou à un mouvement latéral au sein du réseau. Il existe de nombreux contrôles qu'une organisation peut mettre en œuvre pour limiter l'impact de l'exploitation réussie d'une vulnérabilité exposée à Internet, y compris l'utilisation d'une architecture d'application à trois niveaux avec une DMZ pour les serveurs exposant des services à Internet, la ségrégation du réseau interne pour différents types d'actifs, limiter et contrôler l'accès sortant des serveurs à Internet.

Les organisations sont également encouragées à configurer les autorisations conformément aux principes du moindre privilège. Selon la recherche Unit 42 de Palo Alto Networks, Inc., 99 % des utilisateurs, rôles, services et ressources du cloud se voient accorder des autorisations excessives. Pour commencer, cela peut être résolu en séparant les groupes d'administration et en limitant leur portée. Ceci peut être réalisé en utilisant un modèle de hiérarchisation AD ou le modèle d'accès d'entreprise de Microsoft, par exemple. Les administrateurs de domaine ne doivent pas être autorisés à se connecter à distance à des actifs à haut risque tels que des serveurs exposant des services à Internet, et aucun service ne doit être exécuté à l'aide des accès administratifs sur ces actifs à haut risque. Utilisez des comptes de service dédiés avec le principe du moindre privilège pour vous assurer que les autorisations ne posent pas de problème.

Mettre en œuvre un renforcement de la sécurité et des restrictions sur les services exposés pour s'assurer qu'il n'y a pas d'exécution de scripts ou de logiciels non signés (par exemple, alignement sur les recommandations de référence CIS). Empêchez l'accès au processus "Lsass" qui stocke les mots de passe des utilisateurs localement sur les terminaux en appliquant la protection des informations d'identification, en réduisant le nombre d'informations d'identification mises en cache localement à 2 et en exécutant Lsass en tant que PPL.

Assurez-vous également de modifier les informations d'identification par défaut, en particulier pour les comptes d'administration/de gestion intégrés (par exemple, les ports iLO et iDRAC)

Il n'y a pas une seule activité ou un seul protocole qui puisse complètement protéger votre organisation contre la possibilité d'une cyberattaque. Mais en adoptant une approche à plusieurs volets pour identifier et traiter les vulnérabilités exposées, votre système et vos actifs seront bien mieux protégés.

beazley