Décrire les stratégies d’atténuation de base
Formation Microsoft Learn

Vous avez appris qu’il existe de nombreux types différents de cyberattaque.
Mais comment défendre votre organisation contre les cybercriminels ?
Il existe plusieurs façons de repousser les cyberattaquants, de l’authentification multifacteur à la sécurité améliorée du navigateur, et en informant et éduquant les utilisateurs.

Qu’est-ce qu’une stratégie d’atténuation ?

Une stratégie d’atténuation est une mesure ou une collection d’étapes qu’une organisation prend pour empêcher ou se défendre contre les cyberattaques.
Elle consiste généralement en l’implémentation de stratégies et processus technologiques et organisationnels conçus pour se protéger contre les attaques.
Voici quelques-unes des nombreuses stratégies d’atténuation différentes disponibles pour une organisation :

Authentification multifacteur

Traditionnellement, si un mot de passe ou un nom d’utilisateur est compromis, cela permet à un cybercriminel de prendre le contrôle du compte.
Mais l’authentification multifacteur a été introduite pour combattre ce phénomène.

L’authentification multifacteur fonctionne en demandant à un utilisateur de fournir plusieurs formes d’identification pour vérifier qu’il s’agit bien de celui qu’il prétend être.
La forme d’identification la plus courante utilisée pour vérifier ou authentifier un utilisateur est un mot de passe.
Cela représente une information que l’utilisateur connaît.

Les deux autres méthodes d’authentification fournissent une information sur qui l’utilisateur *est*, comme une empreinte digitale ou une analyse rétinienne (forme biométrique d’authentification), et sur ce que l’utilisateur *possède*, comme un téléphone, une clé matérielle ou un autre dispositif approuvé.
L’authentification multifacteur utilise au moins deux de ces types de preuve pour vérifier un utilisateur valide.

Par exemple, une banque peut exiger qu’un utilisateur fournisse des codes de sécurité envoyés à son appareil mobile, en plus de son nom d’utilisateur et de son mot de passe, pour accéder à son compte en ligne.

Sécurité du navigateur

Nous comptons tous sur des navigateurs pour accéder à Internet afin de travailler et d’effectuer nos tâches quotidiennes.
Comme vous l’avez appris précédemment, les attaquants peuvent compromettre la sécurité des navigateurs.
Un utilisateur peut télécharger un fichier malveillant ou installer un module complémentaire malveillant qui peut compromettre le navigateur, l'appareil et même se propager dans les systèmes d'une organisation.

Les organisations peuvent se protéger contre ces types d'attaques en implémentant des stratégies de sécurité qui :

- Empêchent l'installation d'extensions de navigateur ou de modules complémentaires non autorisés.
- Autorisent uniquement l'installation des navigateurs autorisés sur les appareils.
- Bloquent certains sites à l'aide de filtres de contenu web.
- Tiennent à jour les navigateurs.

Former les utilisateurs

Les attaques d'ingénierie sociale s'appuient sur les vulnérabilités humaines pour causer des dommages.
Les organisations peuvent se défendre contre les attaques d'ingénierie sociale en formant leur personnel.
Les utilisateurs doivent apprendre à reconnaître les contenus malveillants qu'ils reçoivent ou rencontrent, et savoir quoi faire lorsqu'ils repèrent quelque chose de suspect.
Par exemple, les organisations peuvent enseigner aux utilisateurs les conduites suivantes :

- Identifier les éléments suspects dans un message.
- Ne jamais répondre aux demandes externes d'informations personnelles.
- Verrouiller les appareils lorsqu'ils ne sont pas utilisés.
- Stocker, partager et supprimer uniquement les données conformément aux stratégies de l'organisation.

Informations sur les menaces

Le paysage des menaces peut être vaste.
Les organisations peuvent avoir de nombreux vecteurs d'attaque, qui sont autant de cibles possibles pour les cybercriminels.
Cela signifie que les organisations doivent prendre un maximum de mesures pour surveiller, prévenir et se défendre contre les attaques, et même identifier les éventuelles vulnérabilités avant que les cybercriminels ne les utilisent pour mener des attaques.
En bref, elles doivent utiliser le renseignement sur les menaces.

Le renseignement sur les menaces permet à une organisation de recueillir des informations sur les systèmes, des détails sur les vulnérabilités, des informations sur les attaques, etc.
Sur la base de sa compréhension de ces informations, l'organisation peut alors mettre en œuvre des politiques de sécurité, de dispositifs, d'accès des utilisateurs, et plus encore, pour se défendre contre les cyberattaques.
La collecte d'informations pour obtenir des insights et répondre aux cyberattaques est appelée « renseignement sur les menaces ».

Les organisations peuvent utiliser des solutions technologiques pour implémenter le renseignement sur les menaces dans leurs systèmes.
Il s'agit souvent de solutions intelligentes de lutte contre les menaces, capables de collecter automatiquement des informations, voire de chasser et de réagir aux attaques et aux vulnérabilités.

Ce ne sont là que quelques-unes des stratégies d'atténuation que les organisations peuvent adopter pour se protéger des cyberattaques.

Les stratégies d’atténuation permettent à une organisation d’adopter une approche robuste de la cybersécurité. La confidentialité, l’intégrité et la disponibilité des informations seront ainsi protégées.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20231023
"C'est ensemble qu'on avance"