learn.microsoft.com /fr-ca/training/modules/describe-basic-cybersecurity-threats-attacks-mitigations/3-describe-threat-landscape

Décrire le paysage des menaces
Formation Microsoft Learn

Vous en avez appris plus sur les cyberattaques, les cybercriminels et la cybersécurité. Toutefois, vous devez également comprendre les moyens que les cybercriminels peuvent utiliser pour effectuer des attaques et atteindre leurs objectifs.
Pour ce faire, vous allez découvrir des concepts tels que le paysage des menaces, les vecteurs d'attaque, les violations de sécurité et bien plus encore.

Quel est le paysage des menaces ?

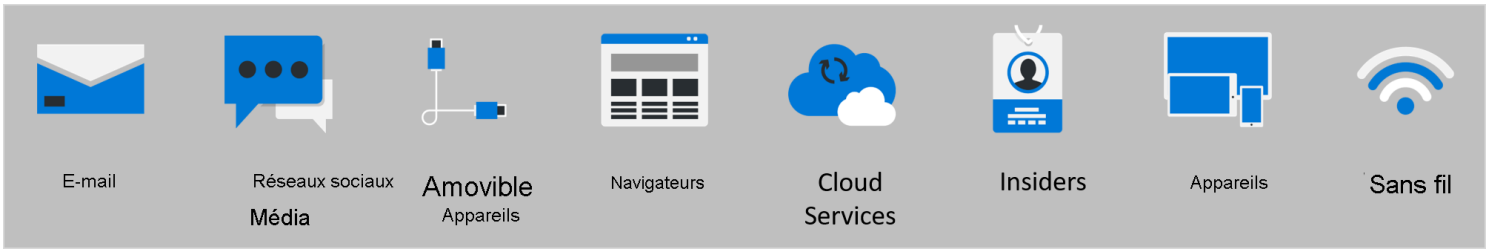
Qu'une organisation soit grande ou petite, l'intégralité du paysage numérique avec lequel elle interagit représente un point d'entrée pour une cyberattaque.
Ces stratégies peuvent inclure :

- Comptes de messagerie
- Comptes de réseaux sociaux
- Appareils mobiles
- L'infrastructure technologique de l'organisation
- Services cloud
- Personnes

Collectivement, on parle de « paysage des menaces ».
Notez que le paysage des menaces peut couvrir plus que simplement des ordinateurs et des téléphones mobiles.
Il peut inclure tous les éléments qui sont détenus ou gérés par une organisation, ou d'autres qui ne le sont pas.
Comme vous le découvrirez ensuite, les criminels utiliseront tous les moyens de préparer et d'effectuer une attaque.

Que sont les vecteurs d'attaque ?

Un vecteur d'attaque est un point d'entrée ou un itinéraire permettant à un attaquant d'accéder à un système.



L'e-mail est peut-être le vecteur d'attaque le plus courant.
Les cybercriminels envoient des courriels d'apparence légitime qui entraînent l'intervention des utilisateurs.
Cela peut inclure le téléchargement d'un fichier ou le clic sur un lien qui compromettra son appareil.

Un autre vecteur d'attaque courant est le passage par les réseaux sans fil.
Les acteurs malveillants écoutent souvent sur les réseaux sans fil non sécurisés dans des aéroports ou des cafés, recherchant des vulnérabilités dans les appareils des utilisateurs qui accèdent au réseau sans fil.
La surveillance des comptes de réseaux sociaux, ou même l'accès aux appareils qui sont laissés non sécurisés, sont d'autres itinéraires couramment utilisés pour les cyberattaques.
Toutefois, vous devez savoir que les attaquants n'ont pas nécessairement besoin de s'appuyer sur ces vecteurs.
Ils peuvent utiliser une variété de vecteurs d'attaque moins évidents.
Voici quelques exemples :

- **Support amovible**.
  Une personne malveillante peut utiliser des supports, comme des lecteurs USB, des câbles intelligents, des cartes de stockage et bien plus encore pour compromettre un appareil.
  Par exemple, les attaquants peuvent charger du code malveillant dans des périphériques USB, qui sont fournis par la suite aux utilisateurs en cadeau, ou laissés dans des espaces publics pour qu'on les trouve.
  Lorsqu'ils sont branchés, les dégâts sont faits.
- **Navigateur**.
  Les attaquants peuvent utiliser des sites web ou des extensions de navigateur malveillants pour laisser les utilisateurs télécharger des logiciels malveillants sur leurs appareils ou modifier les paramètres de leur navigateur.
  L'appareil peut alors devenir compromis, et fournir un point d'entrée au système ou au réseau à plus grande échelle.
- **Services cloud**.
  Les organisations s'appuient de plus en plus sur les services cloud pour les processus et activités du quotidien.
  Les attaquants peuvent compromettre des ressources ou des services mal sécurisés dans le cloud.
  Par exemple, une personne malveillante peut compromettre un compte dans un service cloud et prendre le contrôle de l'ensemble des ressources ou services accessibles à ce compte.
  Ils peuvent également obtenir l'accès à un autre compte avec encore plus d'autorisations.
- **Individus en interne**.
  Les employés d'une organisation peuvent servir de vecteur d'attaque dans une cyberattaque, intentionnellement ou non.
  Un employé peut devenir la victime d'un cybercriminel qui usurpe l'identité d'une personne pour obtenir un accès non autorisé à un système.
  Il s'agit d'une forme d'ingénierie sociale.
  Dans ce scénario, l'employé fait office de vecteur d'attaque non intentionnel.
  Dans certains cas, toutefois, un employé disposant d'un accès autorisé peut l'utiliser pour voler ou causer des dommages intentionnellement.

Que sont les violations de sécurité ?

Toute attaque entraînant l'obtention d'un accès non autorisé aux appareils, aux services ou aux réseaux est considérée comme une violation de sécurité.

Voyez une violation de sécurité comme un intrus (attaquant) parvenant à pénétrer dans un bâtiment (un appareil, une application ou un réseau).

Les violations de sécurité se présentent sous différentes formes, dont les suivantes :

Il est courant d'envisager les failles de sécurité comme l'exploitation d'une faille ou d'une vulnérabilité dans un service technologique ou un équipement.
De même, vous pouvez penser que les violations de la sécurité se produisent uniquement en raison de vulnérabilités dans la technologie.
Mais ce n'est pas le cas.
Les attaquants peuvent utiliser des attaques d'ingénierie sociale pour exploiter ou manipuler les utilisateurs afin d'obtenir un accès non autorisé à un système.

Dans le cadre de l'ingénierie sociale, les attaques d'emprunt d'identité se produisent lorsqu'un utilisateur non autorisé (l'attaquant) cherche à obtenir l'approbation d'un utilisateur autorisé en se faisant passer pour la personne d'autorité afin accéder à un système par une activité mal intentionnée.
Par exemple, un cybercriminel peut prétendre être un ingénieur du support technique pour inciter un utilisateur à révéler son mot de passe pour accéder aux systèmes d'une organisation.

Attaques de navigateur

Que ce soit sur un ordinateur de bureau, un ordinateur portable ou un téléphone, les navigateurs sont un outil d'accès important à Internet.
Les failles de sécurité dans un navigateur peuvent avoir un impact significatif en raison de leur omniprésence.
Supposons, par exemple, qu'un utilisateur travaille sur un projet important pour lequel l'échéance approche.
Il veut savoir comment résoudre un problème particulier pour son projet.
Il trouve un site web qui semble proposer une solution.

Le site web demande à l'utilisateur d'apporter des modifications aux paramètres de son navigateur pour pouvoir installer un module complémentaire.
L'utilisateur suit les instructions du site web.
À son insu, le navigateur est maintenant compromis.
Il s'agit d'une attaque de modificateur de navigateur, l'un des nombreux types différents utilisés par les cybercriminels.
Une personne malveillante peut désormais utiliser le navigateur pour voler des informations, surveiller le comportement de l'utilisateur ou compromettre un appareil.

Attaques de mot de passe

Une attaque de mot de passe se fait lorsqu'un utilisateur tente d'utiliser l'authentification pour un compte protégé par mot de passe pour obtenir un accès non autorisé à un appareil ou à un système.
Les attaquants utilisent souvent des logiciels pour accélérer le processus de piratage et de découverte des mots de passe.
Par exemple, supposons qu'une personne malveillante ait découvert un nom d'utilisateur pour son compte professionnel.

L’attaquant essaie alors un grand nombre de combinaisons de mots de passe possibles pour accéder au compte de l’utilisateur.
Le mot de passe ne doit être correct qu’une seule fois pour permettre à l’attaquant d’obtenir l’accès.
Il s’agit d’une attaque par force brute.
C’est l’une des nombreuses façons pour un cybercriminel d’utiliser des attaques de mot de passe.

Que sont les violations de données ?

Une violation de données se présente quand une personne malveillante parvient à accéder à ou à contrôler des données.
Pour reprendre l’analogie du cambrioleur, imaginez que cette personne obtient l’accès à ou vole des documents et des informations vitales dans le bâtiment :

Lorsqu’un pirate réussit une violation de sécurité, il souhaite souvent cibler les données, car elles représentent des informations vitales.
Une mauvaise sécurité des données peut entraîner l’accès et le contrôle des données par une personne

malveillante.
Cela peut entraîner des conséquences graves pour la victime, qu'il s'agisse d'une personne, d'une organisation ou même d'un gouvernement.
Cela est dû au fait que les données de la victime peuvent être abusées de nombreuses façons.
Par exemple, elles peuvent être conservées et rançonnées, ou utilisées pour causer des dommages financiers ou de réputation.

Unité suivante: Décrire les programmes malveillants

Continuer

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