JUNIPER NETWORKS | Engineering Simplicity

Guide électronique

Comprendre les éléments fondamentaux de la cybersécurité.

Par Trevor Pott
Responsable de la sécurité technique, Juniper Networks

Introduction

Ce document couvre les éléments fondamentaux de la sécurité de l'information, ce qu'elle fait et pourquoi elle est si importante.

Le terme sécurité de l'information, ou « infosec », décrit tout ce qui est lié à la protection de l'information : principes, outils, techniques, technologies, produits, services et pratiques. La sécurité de l'information commence et se termine avec les utilisateurs : les compromissions sont dues presque exclusivement à des manquements humains.

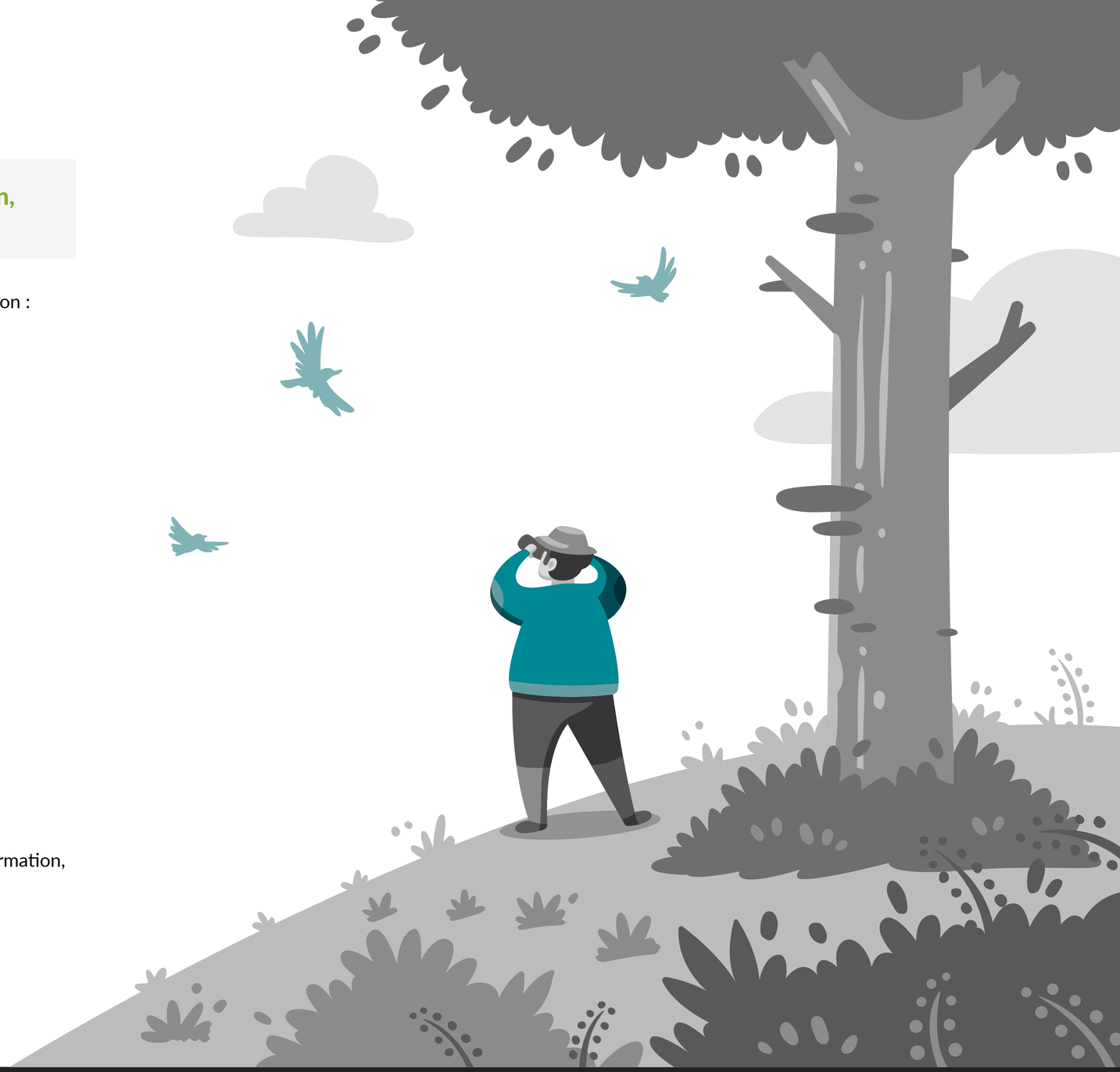
Il existe trois catégories principales de compromissions humaines : **l'ignorance, l'ingénierie sociale et la négligence.**

L'ignorance est un manque de connaissances qui peut présenter un risque de sécurité lorsqu'une personne pense, à tort, savoir quelque chose.

L'ingénierie sociale peut être aussi simple que l'appel d'un soi-disant « technicien Microsoft » ou aussi sophistiquée qu'un e-mail d'hameçonnage ciblé menant à un site Web frauduleux. Ces actions visent à vous faire divulguer des informations pour accéder à vos comptes.

Si nous pouvons tous être victimes d'ignorance ou d'ingénierie sociale, la négligence est un choix délibéré qui mène à un manquement (par exemple ne pas s'informer ou ne pas effectuer une tâche).

Heureusement, la technologie peut être utilisée pour éviter les compromissions de la sécurité de l'information, en bloquant les attaques, en envoyant des rappels aux opérateurs et en détectant des comportements malveillants, anormaux ou négligents.



Éléments fondamentaux de la sécurité de l’information

Données et métadonnées

La plupart des informations sont stockées sous forme de données sur des ordinateurs, que ce soit sous forme de fichiers ou de bases de données, ou encore d’images, de documents Word, d’enregistrements, etc.

Les informations sur les informations, appelées « métadonnées », sont également importantes.

Les photos contiennent souvent des métadonnées, telles que des coordonnées GPS ou les détails de l’appareil photo. Si ces métadonnées ne sont pas supprimées lorsque la photo est publiée sur un réseau social, un acteur malveillant peut les utiliser pour déterminer l’emplacement d’une cible, ou pour identifier le téléphone et la personne concernés.

Imaginons qu’une personne importe la photo de son repas sur un réseau social. Les métadonnées révèlent la position et l’heure de la prise de vue, que des voleurs peuvent utiliser pour déterminer s’ils ont le temps de cambrioler la personne avant qu’elle ne retourne chez elle.

Les métadonnées peuvent également révéler des secrets d’entreprise. Un électricien qui publie la photo d’un câblage qu’il vient de terminer dans un nouveau centre de données dont la construction n’a pas encore été annoncée, pourrait facilement divulguer son emplacement à toute personne qui examine les métadonnées. De même, les documents Word ont tendance à conserver l’historique de toutes les personnes qui ont travaillé dessus, ce qui peut avoir des conséquences juridiques.

Bien plus que des pare-feu et des logiciels anti-programmes malveillants

Les pare-feu classiques et logiciels anti-programmes malveillants ne sont en eux-mêmes pas particulièrement efficaces.

Un pare-feu classique peut empêcher une personne de contrôler votre PC à distance, mais il ne peut pas filtrer les e-mails d’hameçonnage contenant un lien qui, lorsqu’on clique dessus, télécharge une application de contrôle à distance qui fonctionnera derrière un pare-feu, ou peut reconfigurer votre pare-feu pour qu’il autorise l’accès à votre PC.

De même, bien que les logiciels anti-programmes malveillants soient très efficaces contre les fichiers malveillants connus, ils peinent face aux fichiers inconnus, et sont inefficaces contre les innombrables menaces qui peuvent s’introduire sur votre PC via un navigateur Internet.

Dans les entreprises, la plupart des produits et services d’infosec axent leurs efforts sur les données en transit, afin d’intercepter les problèmes avant qu’ils atteignent l’utilisateur ou quittent le réseau.

Sécurité de l’information de nouvelle génération

Les pare-feu applicatifs sont entrés en service dans les années 90, agissant comme des proxies entre les applications et le monde externe. Sont ensuite arrivés les pare-feu de nouvelle génération (NGFW), davantage intégrés dans l’infrastructure des organisations, et dotés de capacités avancées, comme l’application de stratégies en fonction de noms ou groupes d’utilisateurs, plutôt que sur de simples adresses IP.

De manière générale, un NGFW empêche les personnes mal intentionnées d’utiliser des attaques de base pour accéder à un réseau depuis l’extérieur, et offre également des capacités de filtrage des données en transit, par exemple pour déceler les tentatives d’hameçonnage dans les e-mails. Les NGFW peuvent protéger des milliers d’utilisateurs à la fois, et défendre les terminaux qui ne sont pas protégés par des antivirus, comme les imprimantes.

Les logiciels anti-programmes malveillants de nouvelle génération (NGAM), ou antivirus de nouvelle génération (NGAV), ne peuvent protéger que l’hôte sur lequel ils sont installés. Ils sont donc associés aux NGFW pour assurer une protection contre les attaques d’ingénierie sociale.

Un NGFW cherche à éviter que tout programme néfaste n’accède au PC, ce qui est le comportement le plus sûr.

Les NGAM (ou NGAV) tentent d’empêcher le programme néfaste de compromettre votre PC une fois infiltré. C’est la dernière ligne de défense.

Éléments fondamentaux de la sécurité de l’information

WAF et sécurité des applications

Les pare-feu applicatifs Web (WAF) représentent l’étape suivante. Un WAF est un pare-feu de couche applicative qui traite les applications HTTP et HTTPS, dont l’accès se fait généralement via Internet (au sein du réseau ou de manière externe).

Les WAF sont un rempart contre les vulnérabilités affectant une application donnée ou une classe d’applications. Par exemple, un WAF peut filtrer les commandes SQL malveillantes pour les éliminer et éviter leur exécution. Les WAF sont souvent utilisés en interne pour protéger contre les menaces internes et empêcher que la couche d’une application soit affectée par la compromission d’une autre.

La sécurité des applications ne s’appuie pas toujours sur des pare-feu, des logiciels anti-programmes malveillants ou sur tout autre produit ou service externe pour assurer la sécurité.

La sécurité des applications traditionnelle crée des couches de protection directement dans l’application elle-même. Comme les logiciels anti-programmes malveillants d’un PC, la sécurité des applications est la toute dernière ligne de défense des applications hébergées sur un serveur. Lorsqu’une attaque arrive à ce stade, c’est que le système de sécurité n’a pas correctement fonctionné.

Défense en profondeur

Aucun fournisseur ne peut protéger un réseau à lui tout seul contre les menaces actuelles, et personne ne dispose de la main-d’œuvre suffisante ou de la capacité de recherche et de développement nécessaire pour élaborer de nouvelles approches novatrices contre les menaces émergentes.

Le seul moyen réaliste de protéger un réseau moderne consiste à utiliser plusieurs produits provenant de différents fournisseurs qui fonctionnent étroitement ensemble pour offrir une défense multicouche en profondeur.

Chiffrement et DLP

Le chiffrement et la protection contre la perte des données (DLP) sont conçus pour empêcher toute fuite de données vers l’extérieur du réseau.

Les technologies de chiffrement permettent de s’assurer que seules les personnes ou applications qui disposent de la clé correcte peuvent accéder aux données.

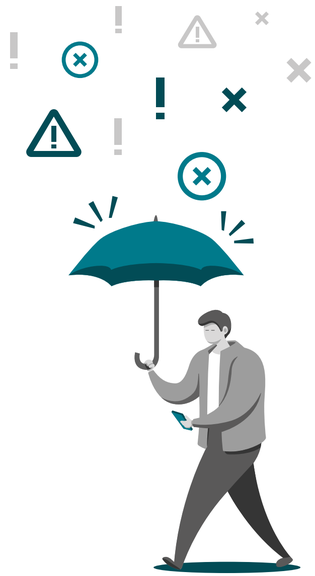
Par exemple, le vol de l’ordinateur portable d’un directeur commercial et des fichiers clients non chiffrés qu’il contient pourrait occasionner des dégâts considérables.

Les données sont chiffrées en transit pour s’assurer qu’aucune personne non autorisée ne puisse accéder aux données, ce qui est vital pour accéder à des services Internet ou utiliser un réseau sans fil (ces derniers ne pouvant pas être totalement sécurisés).

L’approche DLP standard consiste à analyser les données qui tentent de quitter le réseau, pour les arrêter si le comportement n’est pas autorisé. Par exemple, il n’est pas rare que les NGFW et NGAV bloquent la copie de certains contenus sur les clés USB ou dans les dossiers de stockage cloud (comme Dropbox).

La DLP est souvent intégrée dans les outils de sécurité, notamment CASB (Cloud Access Security Broker) et ATP (Advanced Threat Protection), qui sont ainsi capables de détecter l’envoi d’une feuille de calcul contenant des informations bancaires pour le bloquer ou générer une alerte.

Cependant, il existe beaucoup d’autres moyens d’exfiltrer des données d’un réseau : la DLP moderne a encore du mal à traiter les messageries instantanées, Slack et les réseaux sociaux.



Éléments fondamentaux de la sécurité de l’information – Défenses

Surveillance

Sans surveillance, les informaticiens n’auraient aucun moyen de savoir ce qui se passe, ni quels problèmes doivent être résolus. La plupart des produits de surveillance identifient les schémas à l’aide d’écarts et de corrélations.

Pour rechercher les écarts, il est nécessaire d’observer en temps réel le fonctionnement « normal » des charges des travail et des flux de données entre les systèmes afin d’établir une ligne de référence, puis d’identifier les écarts par rapport à cette norme.

La surveillance basée sur la corrélation identifie les événements simultanés ou successifs liés à un problème, généralement à l’aide des journaux d’événements des applications ou des composants de l’infrastructure.

Pour qu’un système de DLP basé sur la surveillance soit idéal, il doit examiner l’accès aux données sur toute l’infrastructure informatique de l’organisation, à la recherche d’anomalies. Par exemple, le système signale un comportement anormal si un directeur commercial, qui n’accède habituellement aux données que de quelques comptes par jour, extrait soudainement les données de tous les comptes de sa région. Pour que cette approche fonctionne, il faut que les produits provenant de divers fournisseurs puissent fonctionner de concert.

Cependant, la surveillance totale de toutes les données d’une organisation est souvent impossible. Les entreprises peuvent posséder des données dans des milliers d’endroits et de systèmes, tant sur site que dans un Cloud public.

Cependant, même si une organisation pouvait surveiller tous les accès aux données, il serait difficile de tirer des conclusions : un accès anormal peut correspondre à une tentative de vol en interne, à un événement de compromission en raison d’une attaque externe, ou simplement à un employé qui fait son travail. Le machine learning, qui se développe très rapidement, permet d’affiner ces schémas graduellement.

SIEM et ATP

Les produits de gestion des événements et des informations de sécurité (SIEM) se trouvent au cœur de la sécurité de l’information et sont de plus en plus intégrés aux produits ATP. Ils reçoivent des données issus de plusieurs produits et les plus utiles d’entre eux s’intègrent rapidement et facilement au principaux produits de plusieurs fournisseurs.

Les systèmes SIEM et les ATP les plus performants se basent principalement sur la corrélation. Exemple :

1. Le NGFW transmet les flux de données de courrier électronique à l’ATP, qui détecte des e-mails contenant des logiciels malveillants à l’intention d’un utilisateur donné.
2. L’ATP demande au pare-feu de stopper la distribution de ces e-mails.
3. Peu après, le NGAV du point de terminaison de l’utilisateur détecte un comportement étrange.
4. Le CASB détecte que le terminal tente de se connecter à des sites de stockage cloud et d’y importer des documents.

Individuellement, la gravité de chacune de ces alertes semble faible. Cependant, en corrélant ces événements, l’ATP peut déterminer qu’une attaque ciblée est probablement en cours, lui assigner le niveau de menace maximal et faire appel à un intervenant humain.

Les SIEM s’appuient principalement sur les données d’événements et de surveillance, et de nombreux fournisseurs commencent également à intégrer des capacités d’analyse, de DLP, ou à permettre l’intégration avec des applications tierces de DLP.

Éléments fondamentaux de la sécurité de l’information – Défenses

Contrôle d’accès, VPN et accès à distance

Grâce aux technologies de sécurité comme le chiffrement, il est possible de détenir un périphérique de stockage sans avoir accès aux données qui s’y trouvent. De même, le Cloud Computing permet aux organisations d’accéder à des produits, services et données partout dans le monde sans jamais avoir accès au matériel sous-jacent.

Presque tous les systèmes d’exploitation, infrastructures informatiques ou applications disposent d’un contrôle d’accès sous une forme ou une autre, dont les exemples les plus courants sont les réseaux privés virtuels (VPN) et l’accès à distance.

Les VPN sont des tunnels réseau chiffrés établis entre deux systèmes informatiques, qui permettent aux utilisateurs de se connecter de manière sécurisée au réseau privé de leur organisation et d’établir des liaisons sécurisées entre les sites. Ils utilisent le chiffrement pour empêcher les attaques d’espionnage.

L’accès à distance est un terme générique qui englobe toutes les technologies qui permettent à des utilisateurs d’accéder aux ressources organisationnelles sans utiliser de VPN.

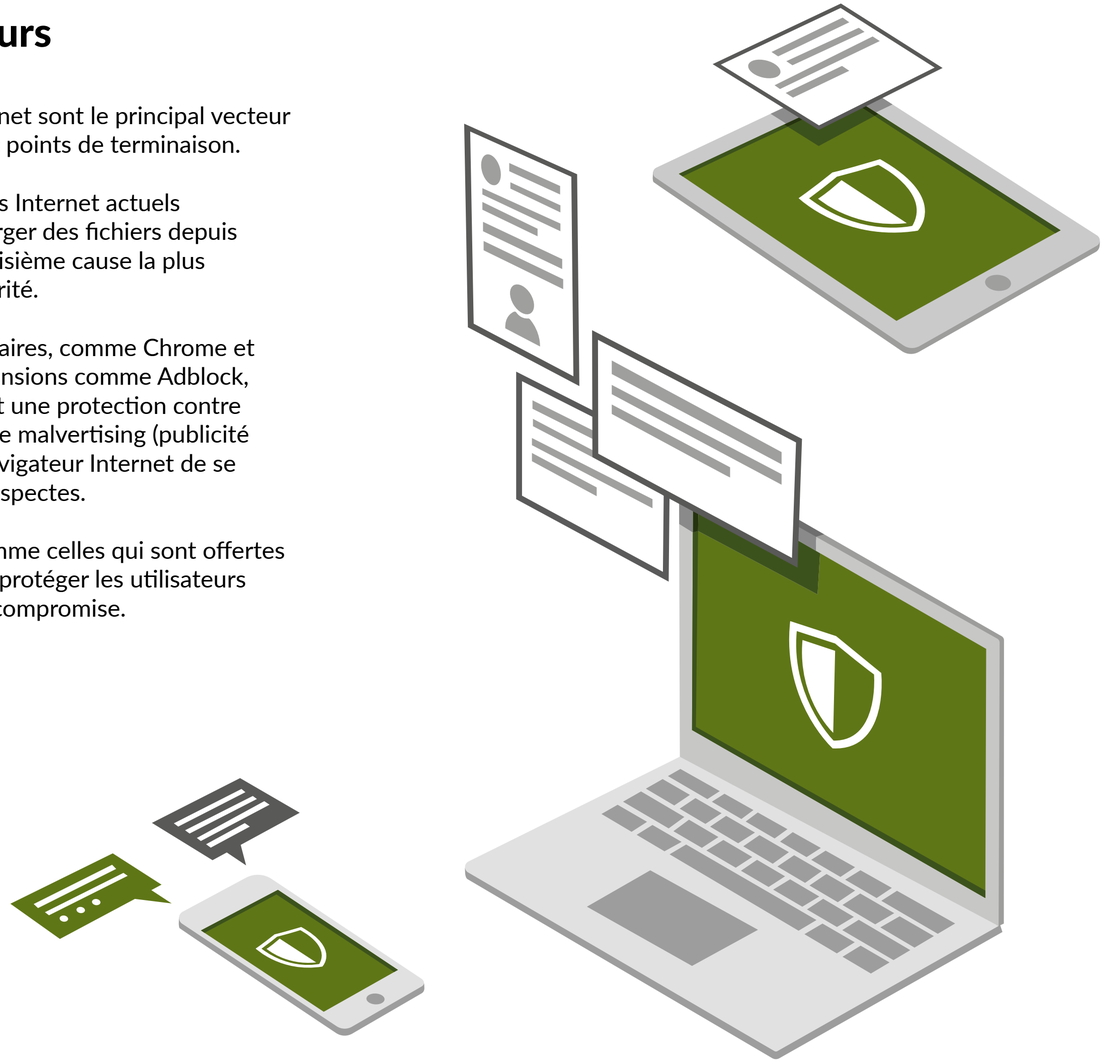
Défenses des navigateurs

Après les e-mails, les navigateurs Internet sont le principal vecteur de compromission des appareils et des points de terminaison.

Encore très vulnérables, les navigateurs Internet actuels permettent aux utilisateurs de télécharger des fichiers depuis Internet et de les exécuter : c’est la troisième cause la plus courante de compromission de la sécurité.

Les navigateurs Internet les plus populaires, comme Chrome et Firefox, permettent d’installer des extensions comme Adblock, Ghostery et Privacy Badger, qui offrent une protection contre différentes menaces Internet, comme le malvertising (publicité malicieuse), et visent à empêcher le navigateur Internet de se connecter à des ressources Internet suspectes.

D’autres extensions de navigateur, comme celles qui sont offertes par les fournisseurs NGAV, tentent de protéger les utilisateurs en interdisant l’accès à une ressource compromise.



Éléments fondamentaux de la sécurité de l’information – Défenses

MDM

Les produits de gestion des équipements mobiles (MDM) sont conçus pour les équipements qui se trouvent hors du périmètre de l’organisation, comme les téléphones portables, les tablettes et les ordinateurs portables. Ils appliquent des modèles, des profils et des stratégies de sécurité aux appareils à distance et mobiles et s’assurent qu’ils répondent aux exigences de sécurité de l’organisation avant d’autoriser la connexion aux ressources dans le périmètre.

La MDM assure la sécurité des applications par le biais de solutions comme les boutiques d’applications et les infrastructures de bureaux virtuels (VDI). Les produits MDM assurent également le contrôle d’accès, en veillant à ce que seuls les utilisateurs autorisés puissent utiliser l’équipement, et en permettant de le localiser et d’en effacer les données à distance en cas de perte ou de vol.

Authentification

Les technologies d’authentification centralisée et d’authentification unifiée (UA) s’appuient sur des services d’annuaire comme LDAP, SAML, ou Active Directory de Microsoft. L’authentification unique (SSO) est la technologie UA la plus courante. Elle permet aux utilisateurs d’utiliser un nom d’utilisateur et un mot de passe uniques pour accéder aux charges de travail et aux services de plusieurs fournisseurs, sur des infrastructures différentes.

Les systèmes d’authentification multifacteur (MFA) sont également largement utilisés, mais peuvent causer des complications s’ils doivent être différents en fonction du pays, par exemple. Par exemple, la vérification par SMS (une approche MFA courante) exige des utilisateurs qu’ils s’identifient à l’aide d’un code envoyé par message texte, mais de nombreux pays appliquent des restrictions sur les SMS qui affectent la fiabilité de cette méthode ou nécessitent des intégrations supplémentaires pour fonctionner correctement.

Automatisation

Aujourd’hui, les charges de travail gérées sont de plus en plus nombreuses et diverses, et le rythme du changement dans le domaine de l’IT ne cesse de s’accélérer. Les humains ne peuvent plus suivre la cadence sans assistance. C’est là qu’intervient l’automatisation.

L’automatisation est la plus importante défense dans le domaine de la sécurité de l’information.

Désormais, la sécurité de l’information doit être intégrée à tous les aspects de l’informatique, car les systèmes sont hautement interconnectés, les périmètres réseau s’effacent rapidement, et les menaces peuvent naître en leur sein. Chaque élément de l’infrastructure, chaque charge de travail et chaque appareil connecté au réseau doivent être pris en compte lors de la conception de la sécurité de l’information d’une organisation.

Anatomie d’une attaque

Définition de l’objectif

Prenons l’exemple de Robert (étant donné que, statistiquement, les pirates qui commettent le plus de crimes sont des hommes). Robert est un pirate. Il vise PotatoCom, son fournisseur d’accès Internet local. Depuis des années, PotatoCom refuse d’installer la fibre optique Internet, et Robert ne supporte plus sa connexion ADSL médiocre. Pour se venger, il veut compromettre le système financier de PotatoCom en empêchant la société d’accéder à sa propre base de données.

Pour gagner le contrôle du système et appliquer son plan, Robert n’a pas besoin d’être un expert, il lui suffit d’en apprendre suffisamment pour atteindre ses objectifs.

Connectivité

Robert doit trouver un moyen de réaliser ses activités illicites en ligne sans qu’on puisse l’identifier. Il peut utiliser une connexion Wi-Fi publique non sécurisée dans un café, mais il doit alors éviter toute caméra de surveillance, y compris sur son chemin. S’il ne peut pas éviter certaines caméras (ou s’il ne les a pas repérées), il peut se déguiser.

Pour lui, hors de question d’utiliser plusieurs fois le même point d’accès Wi-Fi ou le même mode de transport pour se rendre aux emplacements Wi-Fi gratuits, afin que ses activités ne constituent pas une habitude identifiable. S’il est suffisamment proche, Robert pourra même se connecter à un Wi-Fi gratuit sans avoir à se rendre dans le bâtiment qui le propose.

Robert doit également veiller à ce que les réseaux qu’il emprunte ne puissent pas détecter ses activités. Pour cela, il peut employer un ou plusieurs VPN, et louer une machine virtuelle (VM) ou un serveur privé virtuel pour préparer ses attaques. Pour masquer davantage son trafic Internet, il est susceptible d’utiliser TOR, I2P, ou toute autre méthode d’anonymisation et de chiffrement.

Dépenses

Chaque fois qu’il souhaite accéder à Internet, Robert doit acheter des clés USB, des ordinateurs portables et deux comptes VPN, et louer deux VM privées, le tout sans être identifié. Bien que ce soit difficile, c’est possible. Pour faire bref, Robert achète (légalement) une carte de crédit prépayée, intraçable et utilisable à tout endroit, avec de l’argent liquide.

Recherches

Robert doit identifier la base de données et les systèmes de sauvegarde qu’utilise PotatoCom, et les moyens d’y accéder. Il peut utiliser des outils techniques pour sonder l’infrastructure informatique de PotatoCom, ou encore user d’ingénierie sociale pour se faire passer pour un pair, discuter avec des employés de PotatoCom, et les encourager à exprimer leurs frustrations (ce qui marche souvent). Il peut également trouver ce dont il a besoin sur les réseaux sociaux, sur les pages des employés de PotatoCom qui se plaignent des outils qu’ils utilisent. Robert peut même tenter d’appeler les numéros d’assistance de certains fournisseurs en prétendant qu’il travaille chez PotatoCom, afin de confirmer que PotatoCom est bien l’un de leurs clients.

Anatomie d’une attaque

S’infiltrer dans le système

Le moyen le plus simple d’accéder à un système consiste à obtenir des identifiants par ingénierie sociale. Robert n’a pas besoin des identifiants d’un administrateur : tout utilisateur avec un accès basique à l’infrastructure convient, même sans droits de modification. Ensuite, il peut utiliser des outils d’analyse réseau pour sonder l’infrastructure, puis se déplacer latéralement pour attaquer les cibles faciles. Une fois plusieurs portes dérobées installées, Robert peut tenter d’accéder à la base de données et de la corrompre, s’il dispose de l’expertise nécessaire.

Robert n’a besoin que d’un mot de passe administrateur pour mettre la sécurité de PotatoCom en échec.

Toute l’infrastructure de PotatoCom se trouve sur le cloud d’un même fournisseur, et il est fort possible que les identifiants d’administration de l’environnement de production fonctionnent également pour les sauvegardes (une pratique de sécurité peu judicieuse, mais que l’on rencontre).

Apprendre à connaître la cible

Il est peu probable que Robert puisse tromper un administrateur pour obtenir ses identifiants, les administrateurs étant souvent plus au fait des questions de sécurité. Il identifie donc une cible et passe à la surveillance physique.

Robert se renseigne sa cible pour trouver la vulnérabilité qui le mènera, d’une manière ou d’une autre, aux identifiants d’administrateur qu’il recherche.

Il peut par exemple espionner la maison de sa cible, qui ne sera jamais aussi sécurisée que son bureau. Si la cible ne travaille pas depuis chez elle, où se trouve son bureau ? Avec l’ingénierie sociale, Robert peut s’y introduire pour y installer une caméra ou un enregistreur de frappe. Il peut également espionner par les fenêtres ou intercepter les signaux émis par un clavier sans fil.

Réfléchir comme un pirate

Une fois connecté à l’infrastructure de PotatoCom, Robert désactive la journalisation des modifications et corrompt la base de données, qu’il sauvegarde ensuite. Il supprime les autres sauvegardes, change le mot de passe de PotatoCom, et détruit toutes les preuves.

La base de données financière de PotatoCom est désormais inutilisable, et les employés ne peuvent pas accéder à leur compte pour déterminer ce qui s’est passé. Ils ne peuvent pas facturer les clients, payer les fournisseurs ou déclarer de revenus. En cas d’audit, ils seraient position difficile, ne pouvant pas accéder aux données nécessaires. La société pourrait même fermer ses portes.

Robert n’a rien fait de techniquement difficile. L’important, c’était son état d’esprit : il a tout fait pour éviter d’être identifié, et il a recherché le moyen d’accès le plus facile, l’élément le plus vulnérable d’un système étant généralement la faillibilité humaine. Cette logique, c’est celle d’un pirate.

Pour vaincre un pirate, un défenseur doit avoir le bon état d’esprit : la sécurité avant tout.

Un défenseur doit réfléchir comme un pirate pour rechercher les vulnérabilités exploitables, puis combler ces failles par la technologie, des processus d’entreprise, ou tout simplement en mettant des rideaux aux fenêtres. Les défenseurs doivent savoir ce qu’ils défendent avant de déterminer les outils qui conviennent. Tout comme avec les pirates, c’est l’état d’esprit qui compte.

Concepts avancés

Respect des réglementations

Aujourd'hui, il ne suffit plus d'implémenter des technologies de sécurité ou de réussir un audit en appliquant des stratégies de manière simpliste. Les organisations doivent démontrer qu'elles comprennent effectivement les éléments fondamentaux de l'infosec, et leur nécessité.

Le Règlement général sur la protection des données (RGPD) de l'Union européenne (UE), par exemple, exige que toute organisation qui participe au traitement de données à grande échelle dispose d'un délégué à la protection des données (DPD). Les DPD sont responsables de la conformité de l'organisation au RGPD et les conséquences personnelles et financières sont importantes si le DPD ou l'organisation pour laquelle il travaille négligent de sécuriser les données des ressortissants de l'UE.

Segmentation et microsegmentation

Les administrateurs réseau utilisent la segmentation et la microsegmentation pour empêcher le mouvement latéral de tout attaquant qui réussit à franchir les défenses périphériques du réseau. Chaque segment (ou microsegment, qui ne contient qu'une seule application) est défendu séparément. Ce type de cloisonnement protège contre les attaques latérales, ce qui est particulièrement important dans les environnements partagés, où les infrastructures informatiques accueillent plusieurs locataires, comme chez les fournisseurs de services cloud.

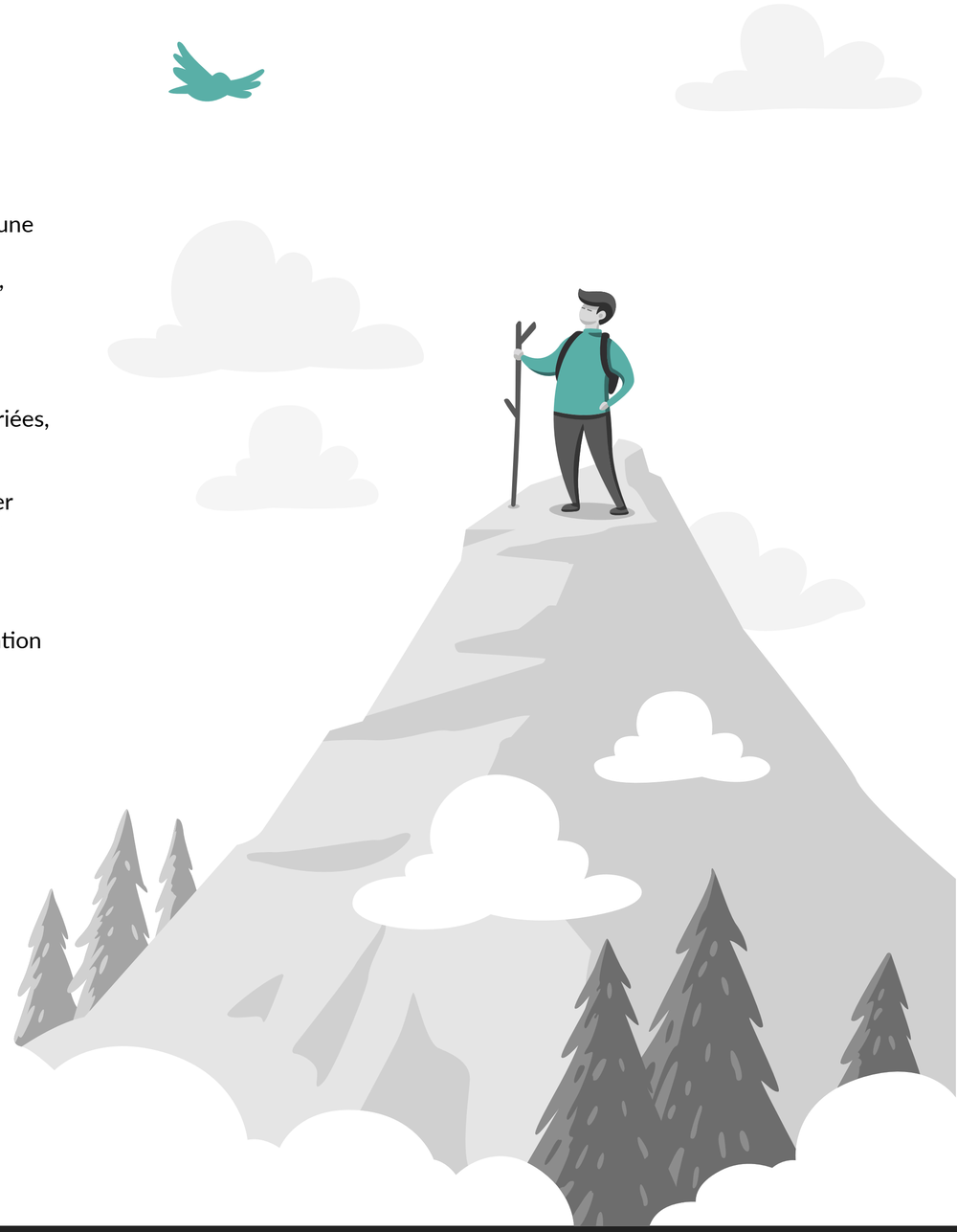
Par exemple, la microsegmentation serait un avantage dans un hôpital de recherche. Afin d'éviter que chaque projet de recherche doive acheter sa propre infrastructure informatique, il est possible d'utiliser des clouds privés, la microsegmentation et des mesures de sécurité adaptées, pour que chaque projet ait un accès locataire unique à l'infrastructure informatique partagée de l'hôpital.

Synthèse

Il est impossible de garantir que la sécurité de l'information d'une organisation ne sera jamais compromise. Cet état de fait ne remet cependant pas en cause les technologies de prévention, mais souligne l'importance des plans de réponse face aux compromissions.

Associée à des technologies de détection et d'atténuation, l'automatisation peut servir à déclencher des mesures appropriées, comme forcer un commutateur à déconnecter ou mettre en quarantaine un appareil compromis. Elle empêche ainsi toute propagation latérale et peut éviter aux entreprises de dépenser des dizaines ou même des centaines de millions de dollars par événement.

Les organisations doivent se soucier de quatre piliers liés à la sécurité de l'information : la prévention, la détection, l'atténuation et la réponse aux incidents ; sans oublier que la sécurité de l'information reste, au fond, une question d'état d'esprit.



Juniper Connected Security

La sécurité a besoin de couches

Pour protéger un réseau aujourd'hui, il faut protéger de tout ce qui s'y trouve, ce qui exige une approche de l'infosec encore peu adoptée par la plupart des organisations.

Les réseaux et la sécurité sont liés. Tenter de concevoir un réseau avec des solutions ponctuelles mène souvent à des résultats désastreux. Une sécurité réseau efficace s'appuie sur l'interconnexion de plusieurs couches de sécurité, réalisée en déployant plusieurs technologies offertes par différents fournisseurs.

Les commutateurs, les routeurs et les points d'accès Wi-Fi se combinent pour former Juniper Connected Security, qui fournit une visibilité approfondie du réseau et des points d'application des stratégies, depuis une interface centrale d'automatisation et d'orchestration. La protection latérale ainsi offerte aux organisations serait difficile à mettre en place autrement.

Bien que certains analystes suggèrent que la meilleure solution pour un segment donné soit celle d'un acteur spécialisé dans ce domaine, cette approche exige que les organisations utilisent plusieurs produits et les fassent tous fonctionner conjointement. Cela peut entraver l'automatisation et l'orchestration des défenses réseau, car les classements évoluent en permanence, et les implémentations de l'automatisation ont souvent un cycle de vie plus long que les produits à automatiser.

De nombreux fournisseurs possèdent un portefeuille diversifié de produits de mise en réseau et de sécurité de l'information, notamment des écosystèmes partenaires. De nombreux autres, comme Juniper, viennent en aide à des clients dont les opérations sont massives, et ils peuvent gérer les plus éclectiques et les plus démesurés des réseaux imaginables.

Juniper se distingue par son engagement envers l'interconnectivité, qui est littéralement au cœur de **Juniper Connected Security**. Juniper promeut l'intégration et l'orchestration, en encourageant l'utilisation de normes ouvertes, de protocoles ouverts et d'API ouvertes, et même en intégrant la prise en charge de produits concurrents. Notre objectif est d'aider les clients à utiliser au mieux ce qu'ils possèdent déjà, plutôt que de les pousser à jeter et remplacer.

L'utilisation d'un même système d'exploitation, Junos, sur l'ensemble du portefeuille de Juniper simplifie grandement la gestion centralisée et permet à Juniper d'offrir des plates-formes de gestion riches en fonctionnalités et des plans de gestion sur site, dans le cloud ou les deux. Avec Junos OS, l'ensemble du portefeuille peut être enrichi de fonctionnalités de manière économique.

Juniper Connected Security permet aux organisations de protéger les utilisateurs, les applications et l'infrastructure en étendant la sécurité à tous les points de connexion du réseau. Appliquer les stratégies au plus près des menaces réduit les risques de propagation. Grâce au machine learning, à l'analytique avancée et à l'automatisation, la réponse rapide aux incidents devient enfin une réalité.

Apprenez-en plus sur Juniper Connected Security en action.

Lire maintenant

Lisez le livre complet sur les éléments fondamentaux de la cybersécurité ici

JUNIPER NETWORKS | Engineering Simplicity

PN : 7400127-001-FR

Siège social et commercial
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089, États-Unis
Tél. : 888.JUNIPER (888.586.4737)
ou +1 408 745 2000
Fax : +1.408.745.2100
www.juniper.net

Siège EMEA et APAC
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, Pays-Bas
Téléphone : +31.0.207.125.700
Fax : +31.0.207.125.701