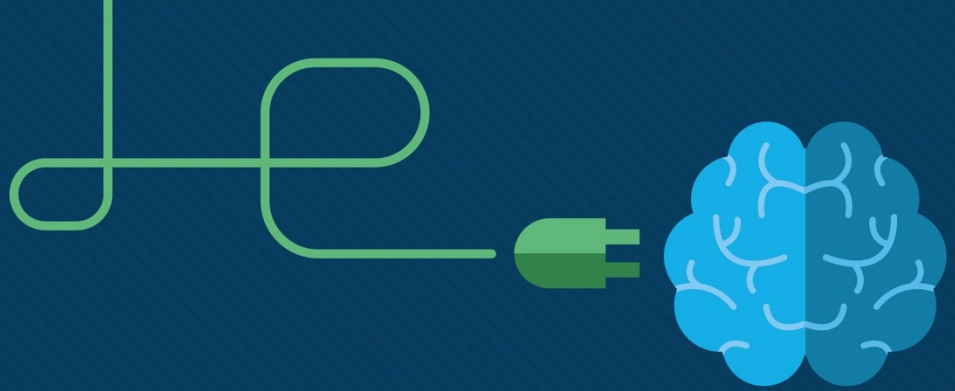


Module 18: Comprendre les mécanismes de défense

CyberOps Associate v1.0

Objectifs du module

Titre du Module: Comprendre les mécanismes de défense

Objectif du Module: Expliquer les approches en matière de protection du réseau.

Titre du Rubrique	Objectif du Rubrique
Défense en profondeur	Expliquer comment la stratégie de défense approfondie protège les réseaux.
Les politiques de sécurité, les réglementations et les standards	Présenter les standards, les réglementations et les politiques de sécurité en vigueur.

18.1 Une défense en profondeur

Ressources, vulnérabilités, menaces

- Les analystes en cybersécurité doivent se préparer pour tous types d'attaques. Leur mission est d'assurer la protection des ressources du réseau de l'entreprise.
- Pour ce faire, les analystes en cybersécurité doivent tout d'abord identifier les éléments suivants :
  - **Ressources** - Tout élément de valeur pour une entreprise devant faire l'objet d'une protection, à savoir les serveurs, les appareils d'infrastructure, les terminaux et surtout, les données.
  - **Vulnérabilités** - Une faiblesse dans un système ou sa conception susceptible d'être exploitée par un acteur de menace.
  - **Menaces** - Tout danger potentiel auquel est exposée une ressource.

Identifier les ressources

- L'ensemble des appareils et des informations que détient ou gère l'entreprise représentent les ressources.
- il est par conséquent nécessaire de les inventorier et de les évaluer pour déterminer le niveau de protection nécessaire et contrer les attaques potentielles.
- La gestion des ressources consiste à inventorier l'ensemble des ressources, puis à développer et à mettre en œuvre des politiques et des procédures pour les protéger.
- Cette tâche peut s'avérer colossale car de nombreuses entreprises doivent protéger les utilisateurs et les ressources internes, les travailleurs mobiles ainsi que les services virtuels basés dans le cloud.
- Les entreprises doivent par ailleurs identifier les emplacements de stockage des ressources d'informations critiques ainsi que les modes d'accès à ces données.
- Il existe autant de ressources d'informations différentes que de menaces qui pèsent sur elles. Chacune de ces ressources peut attirer des acteurs de menace avec différents niveaux de compétence et mus par des motivations diverses.

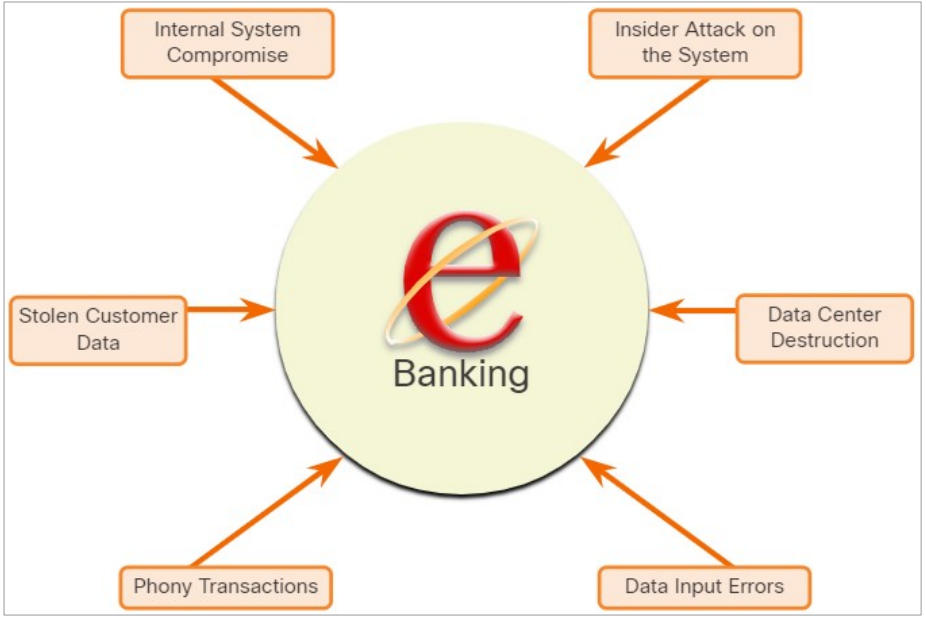
Identifier les vulnérabilités

- L'identification des menaces permet aux entreprises de dresser une liste des menaces potentielles dans un environnement particulier.
- Lors de l'identification des menaces, il est important de se poser plusieurs questions :
  - Quelles sont les vulnérabilités auxquelles est exposé un système ?
  - Qui peut souhaiter exploiter ces vulnérabilités pour accéder à des ressources d'informations spécifiques ?
  - Quelles sont les conséquences d'une exploitation des vulnérabilités du système et de la perte des ressources ?

Identifier les vulnérabilités (Suite)

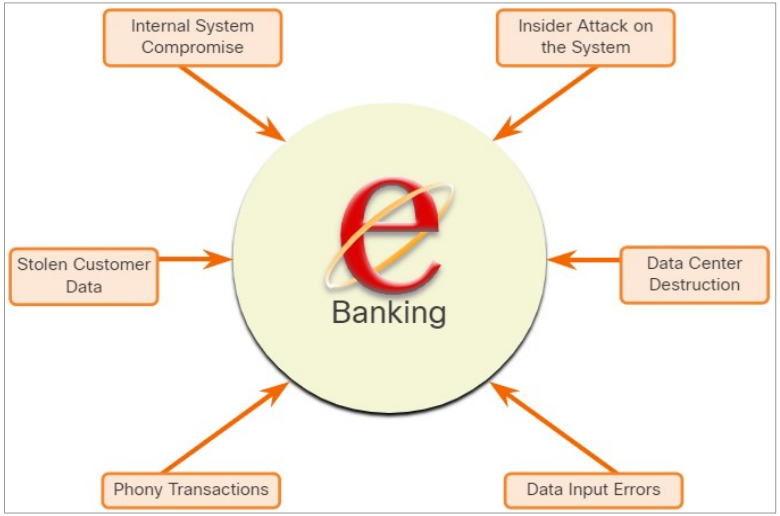
L'identification de menace d'un système de banque en ligne révèle les vulnérabilités suivantes:

- **Mise en danger du système interne** - L'attaquant utilise les serveurs de banque en ligne exposés pour pénétrer dans un système bancaire interne.
- **Vol des données client** - Un attaquant dérobe des données personnelles et financières sur les clients de la banque dans la base de données client.
- **Opérations bancaires frauduleuses depuis un serveur externe** - Un attaquant modifie le code de l'application de la banque en ligne et effectue des opérations en se faisant passer pour un utilisateur légitime.



Identifier les vulnérabilités (Suite)

- **Opérations bancaires frauduleuses à l'aide d'un code PIN ou d'une carte à puce volés** - Un attaquant usurpe l'identité d'un client et effectue des opérations malveillantes depuis le compte compromis.
- **Erreurs de saisie de données** - Un utilisateur saisit des données incorrectes ou effectue des demandes de transaction non valides.
- **Destruction du data center** - Un événement cataclysmique endommage gravement ou détruit le data center.



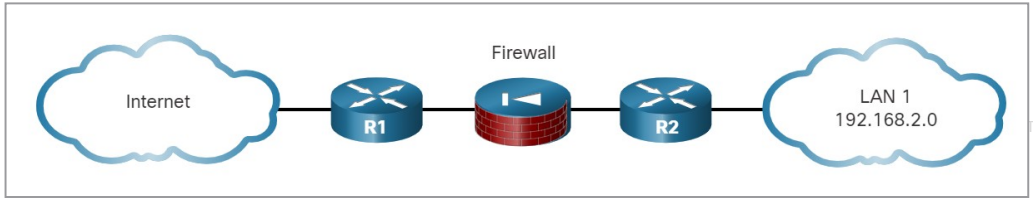
- Pour identifier les vulnérabilités sur un réseau, il est nécessaire de comprendre les applications principales utilisées ainsi que les différentes vulnérabilités associées à ces applications et au matériel. Cela peut représenter des heures de recherche de la part de l'administrateur réseau.

Identifier les menaces

- Les entreprises doivent adopter une approche de défense en profondeur pour identifier les menaces et protéger les ressources vulnérables.
- Cette approche utilise plusieurs couches de sécurité à la périphérie du réseau, sur le réseau et sur les terminaux connectés au réseau.
- Un routeur analyse le trafic avant de le transmettre à une appliance de pare-feu dédiée, par exemple Cisco ASA.
- Les routeurs et les pare-feu ne sont pas les seuls dispositifs utilisés dans une approche de défense en profondeur.
- D'autres dispositifs de sécurité sont disponibles, notamment des systèmes de protection contre les intrusions, des solutions de protection avancée contre les malwares, des systèmes de sécurité de contenu web et e-mail, des services d'identité, des contrôles d'accès réseau, etc.
- Dans une approche de sécurité de défense en profondeur multicouche, les différentes couches s'unissent pour créer une architecture de sécurité dans laquelle l'échec d'un système de protection n'a pas d'incidence sur l'efficacité des autres systèmes de protection.

Identifier les menaces (Suite)

- La figure illustre une topologie simple d'une approche de défense en profondeur:
  - **Routeur de périphérie -** La première ligne de défense est appelée routeur de périphérie (R1 dans la figure). Le routeur de périphérie dispose d'un ensemble de règles qui définissent le type de trafic autorisé ou refusé. Il transmet au pare-feu toutes les connexions destinées au réseau local interne.
  - **Pare-feu -** La deuxième ligne de défense est le pare-feu. Le pare-feu est un dispositif de contrôle qui effectue un filtrage supplémentaire et assure le suivi de l'état des connexions. Il empêche toute connexion entre les réseaux externes (non approuvés) et les réseaux internes (approuvés), et permet aux utilisateurs internes d'établir des connexions bidirectionnelles aux réseaux non approuvés.
  - **Routeur interne -** Le routeur interne constitue une autre ligne de défense (R2 dans la figure). Il peut appliquer des règles de filtrage finales avant d'acheminer le trafic vers sa destination.

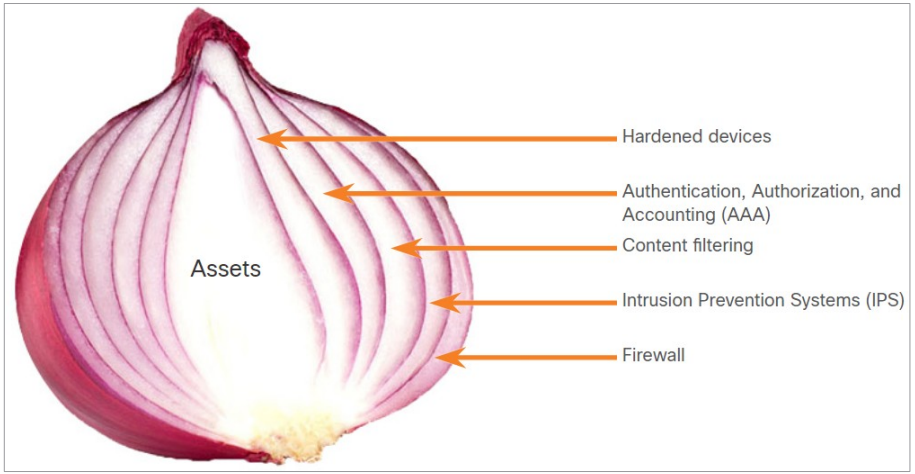


La Security Onion et l'artichaut de sécurité

Il existe deux analogies communes qui sont utilisées pour décrire une approche défensive en profondeur.

Security Onion

- Pour illustrer une approche de défense en profondeur, on utilise souvent l'image d'un oignon.
- Comme le montre la figure, un acteur de menace démonte les mécanismes de défense d'un réseau couche par couche de la même façon que l'on épluche un oignon.
- Ce n'est qu'après avoir pénétré dans chaque couche que l'acteur de la menace atteindra les données ou le système cible.

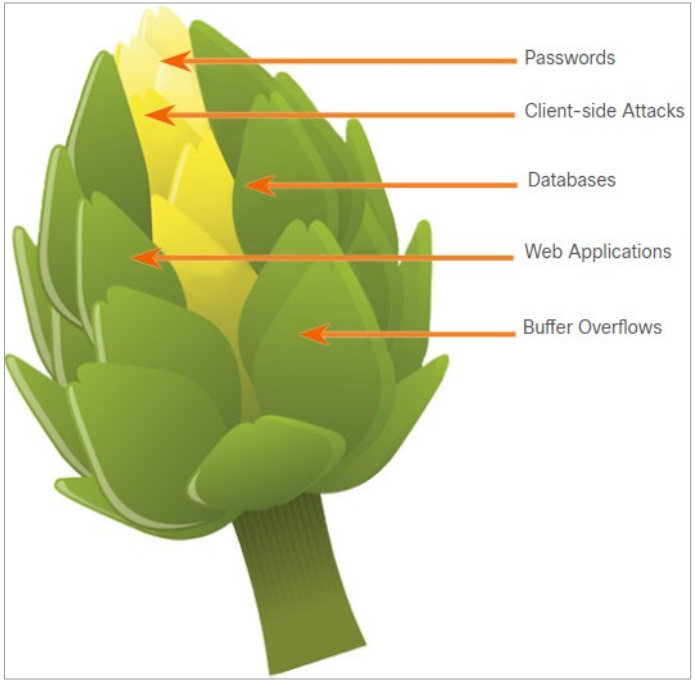


Remarque: *L'approche Security Onion décrite sur cette page est un moyen de visualiser la défense en profondeur. Il ne faut pas la confondre avec la suite d'outils de sécurité réseau appelée Security Onion.*

La Security Onion et l'artichaut de sécurité (Suite)

Artichaut de sécurité

- L'évolution des réseaux sans frontières a changé l'analogie avec l'"artichaut de la sécurité", qui profite à l'acteur de menace.
- Comme le montre la figure , les acteurs de menace n'ont plus besoin d'enlever chaque couche. Il leur suffit de retirer certaines «feuilles d'artichaut».
- Chaque «feuille» du réseau peut révéler des données sensibles qui ne sont pas correctement sécurisées.
- Afin d'atteindre le cœur de l'artichaut, le pirate s'attaque au blindage de sécurité le long du périmètre.
- Alors que les systèmes connectés à Internet sont très bien protégés, les pirates informatiques persistants trouvent une lacune dans cet extérieur dur par lequel ils peuvent entrer.



18.2 Les politiques de sécurité, les réglementations et les standards

Politiques d'entreprise

- Les politiques d'entreprise sont des lignes directrices élaborées par une entreprise qui régissent ses actions.
- Les politiques définissent des standards de comportement pour l'entreprise et ses employés.
- Dans un réseau, les politiques définissent les activités autorisées sur le réseau ;
- elles fournissent donc des consignes d'utilisation acceptable. Si un comportement allant à l'encontre des politiques d'entreprise est détecté sur le réseau, il est possible qu'une faille de sécurité se soit produite.

Politiques d'entreprise (Suite)

Une entreprise peut définir plusieurs politiques, comme indiqué dans le tableau.

Politique	Description
Politique de l'entreprise	• Il établie les règles de conduite ainsi que les responsabilités des employés et des employeurs. • Il protège les droits des travailleurs et les intérêts des employeurs. • Selon les besoins de l'entreprise, diverses politiques et procédures établissent des règles relatives au comportement, à la participation, au code vestimentaire et à la vie privée des employés, ainsi qu'à d'autres domaines liés aux conditions générales d'emploi.
Politiques pour les employés	• Ces politiques sont créées et gérées par le département des ressources humaines pour déterminer le salaire des employés, la grille de rémunération, les bénéfices sociaux, les horaires de travail, les congés, etc. • En règle générale, ces politiques doivent être approuvées et signées par les employés.
Politiques de sécurité	• Ces politiques regroupent les différents objectifs de sécurité définis par une entreprise, définissent les règles de comportement à l'intention des utilisateurs et des administrateurs, et spécifient la configuration système requise. • Ces objectifs, ces règles et ces configurations régissent ensemble la sécurité du réseau et des systèmes informatiques d'une entreprise. • Une politique de sécurité est un document qui évolue constamment en fonction des changements dans l'environnement des menaces, des vulnérabilités et des exigences des employés et des entreprises.

Politique de sécurité

- Les politiques de sécurité informent les utilisateurs, le personnel et les dirigeants des exigences de l'entreprise quant à la protection des ressources d'informations et technologiques.
- Une politique de sécurité globale présente un certain nombre de bénéfices, y compris:
  - Elle manifeste l'engagement de l'entreprise envers la sécurité.
  - Elle définit les normes de conduite.
  - Elle garantit la cohérence des opérations du système, de l'achat et de l'utilisation de composants matériels et logiciels ainsi que de la maintenance.
  - Elle définit les conséquences juridiques des infractions.
  - Elle garantit à l'équipe en charge de la sécurité le soutien des dirigeants.
- Une politique de sécurité spécifie également les mécanismes nécessaires pour répondre aux exigences de sécurité, et constitue une référence pour acquérir, configurer et assurer la conformité des systèmes informatiques et des réseaux.

Politiques de sécurité (Suite)

Le tableau suivant répertorie les stratégies pouvant être incluses dans une stratégie de sécurité :

Politique	Description
Politique d'identification et d'authentification	Elles spécifient les personnes autorisées à accéder aux ressources réseau et décrivent les procédures de vérification.
Politiques de mot de passe	Elles garantissent que les mots de passe remplissent les conditions minimales requises et sont changés régulièrement.
Politique d'utilisation acceptable (AUP)	Elles identifient les applications réseau et les utilisations acceptables pour l'entreprise Elles peuvent également permettre d'identifier les responsables d'une infraction.
Stratégie d'accès à distance	Elles définissent comment les utilisateurs distants peuvent accéder au réseau et les éléments qui sont accessibles via une connectivité à distance.
Politique de maintenance du réseau	Elles spécifient les procédures de mise à jour des systèmes d'exploitation des périphériques réseau et des applications.
Procédures de gestion des incidents	Elles décrivent comment les incidents de sécurité doivent être gérés.

Politiques BYOD

- BYOD permet aux employés d'utiliser leurs propres terminaux mobiles pour accéder aux systèmes, logiciels, réseaux ou informations de l'entreprise.
- Elle apporte des avantages clés aux entreprises, notamment une productivité accrue, une réduction des coûts, une meilleure mobilité des employés, etc. Ces bénéfices impliquent toutefois un risque accru pour la sécurité, car les politiques BYOD peuvent entraîner des failles de données et une plus grande responsabilité pour l'entreprise.
- Une politique de sécurité BYOD doit être mise en place pour atteindre les objectifs suivants:
  - Préciser les objectifs du programme BYOD
  - Identifier les employés susceptibles d'utiliser leurs propres appareils
  - Identifier les appareils pris en charge
  - Identifier le niveau d'accès accordé aux employés lors de l'utilisation d'appareils personnels
  - Décrire les droits d'accès et les activités autorisées au personnel de sécurité
  - Identifier les règles à respecter lors de l'utilisation d'appareils personnels
  - Identifier les systèmes de protection à mettre en place lorsqu'un appareil est exposé à un risque

Politiques BYOD (Suite)

Le tableau répertorie les meilleures pratiques de sécurité BYOD pour aider à atténuer les vulnérabilités BYOD.

Meilleure pratique	Description
Accès protégé par mot de passe	Utiliser des mots de passe uniques pour chaque périphérique et compte.
Contrôle manuel de la connectivité sans fil	Désactiver les connexions Wi-Fi et Bluetooth lorsqu'elles ne sont pas utilisées. Connectez-vous uniquement aux réseaux approuvés.
Rester à jour	Veiller à ce que le système d'exploitation des périphériques et les autres logiciels soient à jour. Les mises à jour logicielles contiennent généralement des correctifs de sécurité permettant de maîtriser les menaces et exploits les plus récents.
Sauvegarder vos données	Sauvegardez régulièrement les données de l'appareil dans le cas d'une perte ou d'un vol.
Activer «Rechercher mon appareil»	S'abonner à un service de localisation de périphériques avec une fonctionnalité d'effacement à distance.
Utiliser un logiciel antivirus.	Fournir un logiciel antivirus pour les dispositifs BYOD approuvés.
Utiliser le logiciel de Gestion des périphériques mobiles (MDM)	Le logiciel MDM permet aux informaticiens de mettre en place des paramètres de sécurité et des configurations logicielles sur tous les appareils qui se connectent aux réseaux d'entreprise.

Conformité à la réglementation et aux normes

- Il existe également des réglementations externes quant à la sécurité du réseau.
- Les professionnels de la sécurité du réseau doivent connaître les lois et les codes de déontologie en matière de sécurité des systèmes d'information (INFOSEC).
- De nombreuses entreprises sont chargées de développer et de mettre en œuvre des politiques de sécurité.
- Les règles de conformité définissent les responsabilités des entreprises et les sanctions en cas de manquement à ces règles.
- Les règles de conformité que doit respecter une entreprise dépendent du type d'entreprise et des données qu'elle gère.

18.3 Récapitulation de comprendre les mécanismes de défense

Qu'est-ce que j'ai appris dans ce module?

- Le point de départ de la défense du réseau est l'identification des actifs, des vulnérabilités et des menaces.
- Tout élément de valeur pour une entreprise devant faire l'objet d'une protection, à savoir les serveurs, les appareils d'infrastructure, les terminaux et surtout, les données.
- Les vulnérabilités sont des faiblesses dans un système ou sa conception susceptible d'être exploitée par un acteur de menace.
- Les menaces sont tout danger potentiel auquel est exposée une ressource.
- Les entreprises doivent adopter une approche de défense en profondeur pour identifier les menaces et protéger les ressources vulnérables.
- Les entreprises doivent également mettre en place des politiques qui définissent les activités autorisées sur le réseau,
- Les politiques de l'entreprise définissent des standards de comportement pour l'entreprise et ses employés.

Qu'est-ce que j'ai appris dans ce module? (suite)

- Les politiques de sécurité informent les utilisateurs, le personnel et les dirigeants des exigences de l'entreprise quant à la protection des ressources d'informations et technologiques.
- L'objectif d'une politique BYOD (Bring Your Own Device) est de permettre aux employés d'utiliser leurs propres appareils mobiles pour accéder aux systèmes, logiciels, réseaux ou informations de l'entreprise.
- Les règles de conformité que doit respecter une entreprise dépendent du type d'entreprise et des données qu'elle gère.


CISCO