Techniques et outils de sécurisation des postes

Sécurité des postes : notions clés

En premier, je définis les 2 types de menaces majeures.

1. Les menaces internes

-**Intentionnel** : Une personne agit délibérément pour nuire à une organisation, souvent par frustration ou pour des raisons financières.

-**Non intentionnel** : Erreurs humaines ou négligences qui entraînent des fuites de données ou des failles de sécurité, comme l'envoi d'informations sensibles à la mauvaise personne ou l'usage de mots de passe faibles.

-**Menaces tierces** : Partenaires commerciaux ou sous-traitants dont les actions compromettent involontairement ou intentionnellement la sécurité de l'organisation.

-**Menaces malveillantes** : Employés ou acteurs internes qui cherchent à causer du tort par vengeance ou pour des gains personnels, comme le vol de données ou le sabotage.

-**Menaces collusoires** : Collaborations entre un employé et un acteur externe (comme un cybercriminel) visant à nuire à l'organisation, souvent pour des raisons financières.

2. Les menaces externes

-**Logiciels malveillants** (malware) : Regroupe divers programmes nuisibles comme les rançongiciels, chevaux de Troie, logiciels espions et cryptojacking.

-**Phishing** : Tromperie incitant les victimes à fournir des informations sensibles ou à cliquer sur des liens dangereux :

-Spear phishing : Phishing ciblé sur des individus ou groupes spécifiques.

-Smishing : Phishing via SMS.

-Vishing : Phishing par téléphone.

-**Attaques par injection SQL** (SQLI) : Exploitent des failles pour insérer des commandes malveillantes dans une base de données.

-**Exécution de code à distance** (RCE) : Permet à un attaquant de manipuler un système à distance.

-**Cross-Site Scripting** (XSS) : Injection de scripts malveillants dans des pages web pour voler des données ou exécuter du code.

-**Attaques contre la chaîne d'approvisionnement** : Exploitent les relations entre une organisation et ses partenaires externes pour infiltrer ses systèmes.

3. Leur différence

-Menaces internes :

-Elles proviennent de l'intérieur de l'organisation (employés, sous-traitants, partenaires).

-Elles peuvent être intentionnelles (espionnage, sabotage) ou non intentionnelles (négligence, erreurs humaines).

-Menaces externes :

-Elles viennent de l'extérieur de l'organisation (hackers, cybercriminels, groupes malveillants).

-Elles visent à infiltrer, manipuler ou perturber un système sans accès privilégié.

Ensuite, les types d'attaques pouvant cibler les postes :

Type de menace	**Catégorie**	**Exemples de menaces**	**Origine/Provenance**
Menace interne	Intentionnelle	Sabotage, vol de données, espionnage	Employés, sous-traitant, partenaires
Menace interne	Non intentionnelle	Négligence, erreurs humaines, failles de sécurités	Employés, partenaires
Menace interne	Tierce	Compromission par un sous-traitant ou partenaire	Partenaires externes

Menace interne	Malveillants	Sabotage, fuite d'informations, cybercriminalité interne	Employés malveillants
Menace interne	Collusoire	Complicité avec un cybercriminel externe	Employés recrutés par des hackers
Menace externe	Logiciels malveillants	Virus, ransomwares, chevaux de Troie, keyloggers	Hackers, groupe malveillants
Menace externe	Phishing	E-mails frauduleux, spear phishing, smishing, vishing	Cybercriminels, escrocs
Menace externe	Injection SQL	Exploitation de bases de données vulnérables	Hackers, pirates informatiques
Menace externe	Exécution de code à distance (RCE)	Prise de contrôle d'un système à distance	Hackers, cybercriminels
Menace externe	Cross-Site Scripting (XSS)	Injection de scripts malveillants sur des sites web	Hackers, attaquants externes
Menace externe	Attaques contre la chaine d'approvisionnement	Compromission via fournisseurs ou partenaires	Hackers, espionnage économique

Puis, pour s'en prémunir, la défense en profondeur (ou élastique) repose sur plusieurs couches de sécurité pour une protection optimale contre les cybermenaces, tel que :

-**Antivirus** : Détecte et élimine les logiciels malveillants connus
-**Pare-feu** : Filtre le trafic réseau, bloque les connexions suspectes et protège contre les intrusions.
-**EDR** (Endpoint Detection & Response) : Analyse en temps réel les activités sur les terminaux, détecte et répond aux menaces avancées.
-**Antimalware** : Protège contre tous types de logiciels malveillants, grâce à l'analyse heuristique et comportementale.

Finalement, en tant que TAI, on joue un rôle clé en cybersécurité, à la fois dans la prévention des incidents et la remédiation après une attaque :

-Prévention :

-Met en place des solutions de sécurité (*antivirus, pare-feu, EDR, antimalware*).
-Sensibilise les utilisateurs aux bonnes pratiques (*gestion des mots de passe, détection des emails frauduleux*).

-Effectue des mises à jour régulières pour corriger les vulnérabilités.
-Surveille les systèmes pour détecter des comportements anormaux.

-Remédiation :

-Analyse et diagnostique les incidents de sécurité.
-Met en quarantaine et supprime les menaces détectées (*virus, ransomwares, chevaux de Troie*).
-Restaure les systèmes affectés et sécurise les données compromises.
-Met en place des mesures correctives pour éviter une récidive.