LA VEILLE EN CYBERSÉCURITÉ

1)

La veille technologique implique de se tenir régulièrement informé des avancées dans le domaine de la technologie et du numérique, notamment de leur disponibilité sur le marché.

La veille technologique consiste à surveiller les progrès techniques et les innovations dans un secteur spécifique. Elle englobe la collecte, le partage et la diffusion d'informations pour anticiper ou se renseigner sur les changements liés à la recherche, au développement, aux brevets, aux nouveaux produits, aux matériaux, aux processus, aux concepts et aux innovations de fabrication. Son objectif est d'évaluer leur impact sur l'environnement et l'organisation.

2)

Il existe différents types de veille :

Veille concurrentielle : Observer ce que font les concurrents pour s'améliorer.

La veille juridique : Surveillance et collecte d'informations sur les changements dans la législation, les règlements et les décisions judiciaires pertinents pour une organisation. Son but est d'assurer la conformité et d'anticiper les impacts sur les activités.

Veille informationnelle : Collecte d'informations pertinentes auprès de diverses sources telles que les médias, les publications spécialisées, etc., pour rester à jour sur les développements et les événements dans un domaine spécifique.

Veille Technologique : Suivre les nouvelles inventions et avancées techniques.

Veille Stratégique : Prédire les grandes tendances qui pourraient affecter l'entreprise à long terme.

Veille Sociale : Surveiller ce que disent les gens sur l'entreprise sur les réseaux sociaux.

Veille Marketing : Observer ce que font les concurrents pour mieux vendre.

Veille environnementale : Suivre les changements dans l'environnement comme le climat ou les règles écologiques. Chaque type de veille aide à prendre de bonnes décisions pour l'entreprise.

3)

Il est crucial pour les entreprises de prendre la cyber sécurité au sérieux et de mettre en place tous les contrôles nécessaires pour prévenir les cyberattaques, surtout celles qui manipulent des données sensibles. Cette prise de conscience généralisée ouvre de nombreuses opportunités professionnelles dans le domaine de la cybersécurité.

De nos jours, les cyberattaques font partie intégrante de notre quotidien. Des termes comme "ransomware", "phishing" ou "virus" sont devenus courants. En plus de ces attaques, les appareils que nous utilisons au quotidien, tels que les téléphones, les ordinateurs, les tablettes, les imprimantes, etc., peuvent présenter des vulnérabilités. Une fois découvertes, ces vulnérabilités peuvent être exploitées à des fins malveillantes en peu de temps.

Pour assurer la pérennité d'une entreprise, il est crucial de corriger rapidement les failles découvertes. Il est donc essentiel de rester informé sur les menaces et les failles existantes. Cela permet de sécuriser au mieux l'infrastructure et les données de l'entreprise.

La technologie évolue rapidement, de même que l'ingéniosité des chapeaux noirs . Il est recommandé d'avoir plusieurs sources d'informations pour détecter les alertes le plus tôt possible.

4)

En mettant en place ces stratégies et ces outils, nous pouvons améliorer la sécurité de notre entreprise et réduire les chances d'avoir des failles .

Formation (sensibiliser) : Sensibiliser nos collaborateurs à la sécurité informatique en fournissant une formation régulière sur les bonnes pratiques de sécurité, les risques potentiels et les mesures à prendre en cas d'attaque.

Détecter les dangers : On utilise des outils de détection de dangers pour surveiller les activités suspectes sur notre réseau, pour éviter les attaques malveillantes , et les tentatives d'intrusion, etc.
outil : SIEM (Système de Gestion des Informations et des Événements de Sécurité)

Analyser les vulnérabilités : Vérifier régulièrement nos systèmes et applications pour repérer les points faibles. En les trouvant, nous pouvons les réparer avant que des chapeaux noirs ne les exploitent pour attaquer.
Outil: Nessus

Veille sur les dangers: Se tenir informé des nouvelles méthodes d'attaque et des dangers actuels des chapeaux noirs en lisant les publications des experts, les rapports de sécurité et en participant aux discussions sur les forums en ligne dédiés à la sécurité.
outil : Recorded Future

Surveillance des Activités : Utilisez des logiciels qui gardent un œil sur ce qui se passe sur notre réseau en enregistrant les événements. Cela nous aide à remarquer les actions étranges ou les attaques qui pourraient être en cours.

outil: IPFIRE

Intelligence Artificielle : On l'utilise pour des services qui nous fournissent des informations sur les attaques en cours, les chapeaux noirs et les outils utilisés.
outil: Darktrace

Tests d’intrusion : Faire des tests de pénétration de manière régulière pour voir si nos systèmes et réseaux résistent face aux attaques, et pour repérer les failles.
outil: Burp Suite
.

5)

Le VPN = Virtual Private Network

Un VPN est un réseau privé virtuel, établit une connexion sécurisée entre des appareils via Internet. C’est un système qui établit une connexion directe entre des ordinateurs éloignés les uns des autres. Ce terme est souvent utilisé dans le contexte du travail à distance.

6)

Le VPN est un outil utilisé pour sécuriser les communications en ligne en établissant une connexion protégée entre des ordinateurs distants via Internet. Cela aide à chiffrer les données échangées et à masquer les adresses IP des utilisateurs pour prévenir l'interception d'informations sensibles. Cependant, bien que les VPN offrent une protection contre certaines cyberattaques, ils ne garantissent pas une sécurité totale et doivent être utilisés avec d'autres mesures de sécurité telles que la vigilance contre le phishing et les logiciels malveillants. Parfois, les chapeaux noirs peuvent également utiliser des VPN pour dissimuler leurs activités malveillantes .En résumé, les VPN sont utiles pour renforcer la sécurité en ligne, mais ils ne sont pas une solution complète contre les cybermenaces.

7)

Les menaces:

- **Attaques basées sur l'IA et la Machine Learning**: Les chapeaux noirs exploitent l'IA et le ML pour automatiser les attaques plus précises et travaillées , et peut éviter certaines détections

- **Les attaques DDOS**: Les attaques DDOS submergent les sites Web et les réseaux avec un trafic, les rendant inaccessibles aux utilisateurs.

- **Les ransomwares**: Les chapeaux noirs chiffrent les données des victimes et exigent un paiement pour les déverrouiller.

- **le vol d'identité :** Les chapeaux noirs exploitent des données dérobées comme des identifiants de connexion, des mots de passe ou des données personnelles pour se faire passer pour une autre personne sur internet.

- **Le spear phishing :** C'est du phishing mais de façon plus ciblée , où les chapeaux noirs adaptent leurs attaques en utilisant des renseignements précis sur la cible, ce qui augmente leur probabilité de réussite.

Stratégies pour combattre les attaques :

- **Contre les attaques basées sur l'IA et le ML**: On utilise des outils de détection d'anomalies qui exploitent l'intelligence artificielle et des méthodes d'analyse pour repérer les comportements suspects et les activités malveillantes.

- **Contre les attaques DDOS**: On met en place des dispositifs pour équilibrer la charge pour répartir efficacement le trafic entre les serveurs, ce qui assure une performance optimale du système.

- **Vol d'identité** : On renforce la sécurité en utilisant l'authentification à deux facteurs (2FA) ou multifactorielle (MFA), qui nécessite une seconde vérification en plus des identifiants de connexion pour réduire les risques d'accès non autorisé aux comptes.

- **Spear phishing :** On améliore la sécurité en utilisant des méthodes de sensibilisation et d'entraînement pour éduquer les utilisateurs sur la détection du phishing, réduisant ainsi les risques de tomber dans des attaques de spear phishing.

- **Contre les ransomwares**: On utilise des solutions de sauvegarde et de récupération des données pour pouvoir restaurer nos données en cas d'attaque.