Clément Arki

BTS SIO 2ème année

Veille Cybersécurité : White Hat Hackers

Sommaire :

Introduction :

J’ai choisi cette veille car c’est un sujet qui m’intéresse et dont j’ai déjà entendu parler dans un cours de cybersécurité pendant mon cursus. Mon intérêt est d’en apprendre un peu plus sur le sujet des hackers éthiques, notamment des White Hat Hackers. Par rapport à mon cursus de formation, le choix de cette veille sur les White Hat Hackers pourra me permettre d’approfondir ma compréhension sur les enjeux liés à la sécurité informatique.

Les outils de collecte que j'ai utilisés pour rassembler des informations pertinentes et à jour sur ce sujet incluent des newsletters provenant de sites tels que developpez.com, l'utilisation de l’outil Google Alerts, ainsi que des recherches effectuées sur internet.

I. White Hat Hackers : Éthique, Économie et Impact

1. Qu'est-ce qu'un White Hat Hackers ?

Un White Hat Hacker est une personne experte en sécurité informatique qui utilise des compétences de piratage pour identifier les vulnérabilités de sécurité du matériel, des logiciels ou des réseaux (essentiellement dans les entreprises). Ils agissent de manière légale et éthique.

Les White Hat Hackers ont émergé dans les années 1960 avec le développement des premiers systèmes informatiques. Ce terme a été popularisé plus tard dans les années 1970 et 1980 avec la montée de la culture hacker et les premiers groupes de sécurité informatique.

Contrairement aux pirates informatiques malveillants, les White Hat agissent en respectant les lois et règlements en vigueur en matière de piratage informatique.

L'inverse des White Hat sont les Black Hat hackers qui eux agissent de manière malveillante en exploitant les vulnérabilités pour des vols de données, des attaques de toute sortes (création de virus), des gains personnels ou nuire à des individus ou à des organisations.

Ces termes auraient pour origine des films de western ou le héros ou le shérif porte un chapeau blanc (White Hat) alors que le bandit porte un chapeau noir (Black Hat).

2. Rôle économique

Le rôle économique des White Hat Hackers se trouve dans la contribution à la sécurité en identifiant en corrigeant les vulnérabilités des systèmes informatiques. En détectant des attaques, les hackers éthiques aident les entreprises à renforcer leurs défenses en évitant ainsi des pertes financières et de réputation.

Les White Hat Hackers renforcent la sécurité numérique en fournissant des services de conseil en sécurité (à l'entreprise par exemple) et en participant à des programmes avec des primes conséquentes pour la découverte de failles.

Il contribue ainsi à instaurer la confiance et à stimuler la croissance de l'économique numérique. Aussi le salaire moyen d'un White Hat est de 74 450 € par an, mais ils peuvent aussi gagner jusqu'à 500 000 dollars par an grâce aux primes de bug.

Aussi, le salaire par mois d'un Hacker éthique est de 4000€ pour un débutant et 7500€ pour un salaire confirmé.

3. Impact utilisateur

L'impact des White Hat Hackers sur les utilisateurs contribuent à garantir la sécurité en ligne, ce qui renforce la confiance des utilisateurs dans les plateformes numériques.

Ils protègent des données personnelles lorsqu'ils découvrent des vulnérabilités. Les White Hat font en sorte de réduire les risques de piratage et de vol de données pour une utilisation plus sûre.

II. Analyse d'un White Hat Hackers

1. Avantages et inconvénients (tableau comparatif)

Avantages des White Hat Hackers	Inconvénients des White Hat Hackers
Sécurité : Contribuent à la sécurité en ligne en identifiant et en corrigeant les vulnérabilités.	**Divulgation :** Risque de divulgation d'informations sensibles lors de la découverte de failles.
Protection : Protègent les données personnelles et financières des utilisateurs.	**Pression :** Pression accrue pour résoudre rapidement les failles pour prévenir les attaques.
Confiance : Favorisent la confiance des utilisateurs envers les plateformes numériques.	**Attentes :** Attentes élevées de la part des parties prenantes pour éviter les violations de sécurité.
Prévention : Préviennent les cyberattaques et réduisent les risques de piratage.	**Complexité :** Peuvent être confrontés à des défis techniques complexes pour identifier les failles.
Sensibilisation : Sensibilisent à l'importance de la cybersécurité.	**Réputation :** Risque de perte de réputation en cas d'erreur.

2. Les compétences et les qualités d'un White Hat Hacker

Les compétences que doit avoir un White Hat Hacker dans ce domaine sont :

- Capacité de compréhension des menaces cybersécurité
- Capacité à exploiter des sources ouvertes de manière sécurisée
- Mise en place de plans de veille sur un ou plusieurs secteurs déterminés
- Détection, qualification et analyse d'informations pertinentes
- Le droit et les réglementations en vigueur en matière de cybersécurité

Les qualités que doit avoir un White Hat Hacker dans ce domaine sont :

- Rester éthique et légal
- Avoir un sens de la curiosité
- Être dynamisme et réactif
- Savoir faire preuve de créativité
- Pourvoir être disponibilité
- Avoir un sens de la confidentialité
- Aimer le travail en équipe et le goût du défi

3. Éthique dans le monde des White Hat Hackers

Les White Hat joue un rôle dans la sécurité informatique. Ils agissent pour le bien des organisations en trouvant les vulnérabilités. Les hackers éthiques contribuent activement à la protection des systèmes en identifiant les failles et en proposant des solutions pour les entreprises et les utilisateurs. Leur engagement éthique est essentiel pour la recherche de vulnérabilité et aussi pour la préservation de la sécurité.

Aussi, certains White Hat agissent de manière illégale (c'est-à-dire sans autorisation) en voulant agir pour le bien. Il garde donc quand même une éthique.

En revanche, il est fréquent que de nombreux hackers White Hat par le passé ait été impliqué dans des activités de piratage malveillant.

III. Responsabilités et Évolution des "White Hat Hackers"

1. Responsabilités envers la société

Les hackers éthiques portent une responsabilité importante envers la société en contribuant à la sécurité en ligne et à la protection des données.

Actuellement 84% des organisations font appel à des hackers éthique pour renforcer leur cybersécurité.

La responsabilité de l'hacker éthique est qu'il doit se conformer à un code de conduite et à une discipline stricte. Avant d'évaluer la sécurité du réseau d'une entreprise, l'hacker éthique sera soumis à une procédure qui sera :

- L'expert qui se met dans la peau d'un hacker malveillant pour identifier les vulnérabilités potentielles devra documenter le chemin d'attaque qu'il communique à l'organisation.
- L'hacker bienveillant devra signer un accord de confidentialité et traiter toutes les informations de l'entreprise avec la plus grande prudence.
- L'expert devra signaler immédiatement à l'organisation toute violation de sécurité.
- Toutes les traces de tests de vulnérabilités devront être effacées pour éviter toute exploitation malveillante des failles précédemment identifiées.

2. L'évolution du rôle

Le rôle des White Hat Hackers a évolué au fil du temps pour devenir essentiel dans la protection contre les cybermenaces. Centré sur la détection de vulnérabilité, leur rôle s'est élargi pour inclure la sensibilisation à la sécurité et la collaboration avec les entreprises. Ils travaillent à anticiper les failles, à renforcer les défenses et à former de nouveau experts en cybersécurité.

Aussi en termes d'évolution, les dépenses mondiales en logiciels, matériels et service de cybersécurité devraient franchir la barre des 300 milliards de dollars d'ici 2026.

Les principales causes de cette évolution sont la menace persistante des cyberattaques, les besoins liés à l'instauration d'un environnement de travail hybride sécurisé et les directives de protection et de gouvernance des données.

3. Exemples d'actions de White Hat Hackers

Attaque contre le secteur financier : Le responsable de l'attaque contre l'entreprise Ede Finance s'est avéré être un "White Hat". Dans cette attaque, où ils ont subi une perte de 580 000 dollars, l'hacker a dévoilé que les développeurs d'Ede Finance avaient mis en place une pratique douteuse en exploitant une vulnérabilité. Cette vulnérabilité leur permettait de forcer la vente des actifs détenus par les utilisateurs, en manipulant délibérément les prix dans le but de dérober leurs fonds. L'incident a révélé des pratiques douteuses des développeurs d'Ede Finance. En réponse, l'équipe a pris des mesures correctives, supprimant le contrat problématique et remboursant les pertes des utilisateurs avec leurs propres fonds.

Test de faille de sécurité chez FranceConnect : C'est une campagne lancée par le gouvernement pour attirer les meilleurs génies de l'informatique à venir tester la sécurité de son serveur France Connect**.** Le gouvernement promet d'offrir 20 000 € à ceux qui trouveront des failles de sécurité. Pour s'assurer de la sécurité de son serveur, la direction interministérielle du numérique (Dinum) a publié une annonce en ligne pour attirer les hackers susceptibles de repérer des « failles critique « sur son portail FranceConnect. Celui qui parviendra aura obtiendra 20 000 € offert. Une méthode visant aussi à valoriser le « hacking éthique ».

Histoire d'un Anonymous (de Black Hat à White Hat) : Un ancien membre de l'Anonymous, du nom d'Hector Monsegur, s'est reconverti du rôle de Black Hat à celui de White Hat. C'est personnage controversé sur la scène de la cybersécurité car il avait fondée et dirigée l'une des factions les plus célèbre d'Anonymous qui est LulzSec (dissolu en 2011). Arrêter par le FBI en 2011, il a servi d'informateur à l'agence pendant environ 10 mois pour identifier plusieurs membres de LulzSec ainsi que d'autre membre d'Anonymous. Après cela, il a eu une condamnation de 7 mois d'emprisonnement et l'accès à internet interdit pendant 2 ans. Après cela, il a décidé de se lancer en tant que chercheur indépendant dans l'industrie de la sécurité en adoptant une approche éthique en tant que White Hat.

Conclusion :

Je suis en faveur des White Hat Hackers car leur rôle est essentiel dans la sécurité informatique. Il détecte les vulnérabilités et les failles au sein des systèmes informatiques, ce qui contribue à renforcer leur résistance contre les cyberattaques.

Ce sont en général des personnes légales à qui on demande des services pour vérifier leur sécurité au sein d'une organisation par exemple. Parfois ils sont dans l'illégalité

mais ils gardent quand même une morale (une éthique) dans leurs actions. Ce ne sont pas des personnes malveillantes et ils agissent pour le bien.

A mesure que la cybersécurité évolue pour faire face aux nouvelles menaces, le rôle des White Hat Hacker devient de plus en plus important pour garantir la sécurité des systèmes et des données informatiques.

Sources :

https://fr.wikipedia.org/wiki/White_hat

https://www.techtarget.com/searchsecurity/definition/white-hat

https://coins.fr/curve-offre-recompense-contre-infos-hacker/

https://coins.fr/hackeur-curve-finance-restitue-20m-cryptos-volees/

https://www.sales-hacking.com/post/hacker-white-hat

https://www.glassdoor.fr/Salaires/ethical-hackers-salaire-SRCH_KO0,15.htm

28 mai 2023

https://www.channelnews.fr/croissance-de-124-du-marche-de-la-cybersecurite-prevue-en-2023-123484#:~:text=d%C3%A9penses%20informatiques-,Croissance%20de%2012%2C4%25%20du%20march%C3%A9%20de,la%20cybers%C3%A9curit%C3%A9%20pr%C3%A9vue%20en%202023&text=Les%20d%C3%A9penses%20mondiales%20en%20logiciels,du%20cabinet%20d'%C3%A9tudes%20IDC.

23 mars 2023

Grand I petit 2 :

https://guardia.school/metiers/hacker-ethique.html

19 janvier 2024

Grand III petit 3

https://www.developpez.com/actu/105766/De-black-hat-a-white-hat-un-ancien-membre-d-Anonymous-se-reconvertit-et-travaille-desormais-comme-chercheur-en-securite/

24 octobre 2016

Grand III petit 3

https://journalducoin.com/defi/arbitrum-hacker-sauve-utilisateurs-ede-finance-pratiques-douteuses-developpeurs/

31 mai 2023

Grand III partie 3

https://www.capital.fr/economie-politique/franceconnect-jusqua-20-000-euros-a-la-cle-si-vous-parvenez-a-pirater-la-plateforme-1487392

1 décembre 2023