BTS SIO - Epreuve E4

Mettre en œuvre des outils et stratégies de veille informationnelle

Rédacteur(s)	Version	Date	Nb pages
	1.1	30/11/2021	10

Mon sujet

.....

SOMMAIRE

1 Introduction

La veille, dans le contexte professionnel, est une activité qui consiste à surveiller et à recueillir des informations pertinentes dans un domaine spécifique, afin de les analyser et d'identifier des tendances et des opportunités pour les entreprises. Elle permet de se tenir informé des évolutions du marché, des innovations technologiques, des changements réglementaires, des nouvelles méthodes de travail...

Les différents domaines de veille sont nombreux et peuvent varier en fonction de l'activité professionnelle de chaque personne. On peut citer par exemple la veille concurrentielle, la veille réglementaire, la veille marketing, la veille technologique, la veille environnementale, la veille stratégique, la veille juridique....

Il est important de faire de la veille dans le cadre de son métier pour plusieurs raisons. Tout d'abord, cela permet de rester compétitif et de s'adapter rapidement aux changements du marché. La veille permet également de prendre des décisions éclairées et d'anticiper les évolutions futures. Elle peut aussi aider à détecter des opportunités de développement ou de croissance pour son entreprise.

La veille technologique est particulièrement importante dans le domaine de l'informatique car les technologies évoluent très rapidement. Il est donc essentiel de se tenir informé des dernières innovations et des tendances du marché pour rester compétitif et proposer des solutions innovantes à ses clients. La veille technologique permet également de détecter des opportunités de développement de nouveaux produits ou services, ou encore d'améliorer les processus internes de l'entreprise en utilisant des technologies plus efficaces.

1.1 Mes sources

Dark Reading: https://www.darkreading.com/

SC Magazine : https://www.scmagazine.com/

Infosecurity Magazine: https://www.infosecurity-magazine.com/

Gartner: https://www.gartner.com/en/information-technology/cybersecurity

Forrester: https://go.forrester.com/blogs/category/security-risk/

IDC: https://www.idc.com/research/security

Centre national de cybersécurité (CNC): https://www.cybermalveillance.gouv.fr/

Centre canadien pour la cybersécurité: https://www.cyber.gc.ca/fr/

Center for Internet Security (CIS): https://www.cisecurity.org/

Symantec: https://www.symantec.com/security-center

McAfee: https://www.mcafee.com/enterprise/en-us/security-awareness.html

Trend Micro: https://www.trendmicro.com/en_us/business.html

2 Mon sujet de veille

2.1 Introduction

Afin de me tenir informé des dernières évolutions technologiques et de perfectionner mes compétences en matière de sécurité informatique, j'ai choisi de réaliser une veille sur les nouvelles tendances en matière de cybersécurité.

La cybersécurité est devenue un enjeu crucial pour les entreprises et les organisations du monde entier. Les attaques informatiques sont de plus en plus sophistiquées et les cybercriminels utilisent des techniques de plus en plus avancées pour voler des données sensibles ou perturber le fonctionnement des systèmes informatiques. Dans ce contexte, il est essentiel de se tenir informé des dernières tendances en matière de cybersécurité pour protéger les systèmes et les données des attaques malveillantes.

Mon sujet de veille portera sur les nouvelles tendances en matière de cybersécurité. Je vais me concentrer sur les dernières méthodes de piratage, les vulnérabilités découvertes sur les systèmes d'exploitation ou les applications populaires, et les meilleures pratiques de sécurité pour les réseaux d'entreprise.

La problématique qui se pose est comment rester à jour sur les dernières tendances en matière de cybersécurité et comment appliquer ces nouvelles connaissances pour renforcer la sécurité des systèmes informatiques. Les cybercriminels sont en constante évolution, ce qui signifie que les méthodes de sécurité informatique doivent également évoluer pour répondre à ces menaces. Il est donc crucial de se tenir informé des dernières tendances et de trouver des moyens efficaces pour les appliquer dans les environnements informatiques des entreprises et des organisations.

En résumé, ma veille sur les nouvelles tendances en matière de cybersécurité vise à m'informer sur les dernières évolutions dans ce domaine et à trouver des solutions pour renforcer la sécurité informatique dans les environnements professionnels.

2.2 Historique

L'histoire de la cybersécurité remonte aux débuts de l'ère informatique, lorsque les ordinateurs étaient utilisés principalement à des fins militaires et gouvernementales. Depuis lors, l'utilisation des ordinateurs et d'Internet s'est répandue dans le monde entier, entraînant une explosion de la cybercriminalité et la nécessité de développer des mesures de sécurité pour protéger les systèmes informatiques.

Voici les grandes dates clés et étapes de l'histoire de la cybersécurité :

1970 : le premier virus informatique, appelé "Creeper", est créé. Il s'agit d'un programme qui se propage automatiquement d'un ordinateur à l'autre via un réseau.

1983 : le protocole de communication TCP/IP est développé, fournissant les bases de l'Internet moderne.

1988 : le premier virus informatique à grande échelle, appelé "Morris Worm", est créé. Il a infecté plus de 6 000 ordinateurs à travers le monde.

1991 : le premier pare-feu est développé pour protéger les réseaux informatiques contre les attaques externes.

1995 : le terme "cybersécurité" est utilisé pour la première fois dans un article du Wall Street Journal.

2000 : l'attaque informatique appelée "ILOVEYOU" infecte des millions d'ordinateurs dans le monde entier.

2002 : le gouvernement des États-Unis crée le Department of Homeland Security pour coordonner les efforts de sécurité intérieure, y compris la cybersécurité.

2008 : le ver informatique "Conficker" infecte des millions d'ordinateurs dans le monde entier.

2010 : Stuxnet, un logiciel malveillant sophistiqué, est découvert. Il a été développé pour attaquer les systèmes de contrôle industriels.

2013 : les révélations d'Edward Snowden sur les programmes de surveillance de la NSA américaine ont mis en lumière l'importance de la protection de la vie privée en ligne.

2017 : la cyberattaque WannaCry infecte des centaines de milliers d'ordinateurs dans le monde entier.

2020 : la pandémie de COVID-19 entraîne une augmentation significative des attaques de phishing et des cyberattaques.

Cette chronologie montre que la cybersécurité est un domaine en constante évolution, avec des menaces de plus en plus sophistiquées qui nécessitent des mesures de sécurité de plus en plus avancées pour les contrer. En restant informé des dernières tendances en matière de cybersécurité, il est possible de mieux protéger les systèmes informatiques des entreprises et des organisations.

2.3 Problématique que la techno a rencontré durant son dev

La cybersécurité est un domaine qui a connu de nombreux défis au cours de son développement. Les principales problématiques rencontrées sont les suivantes :

Complexité croissante des systèmes informatiques : avec l'expansion rapide des réseaux et des systèmes informatiques, la complexité des systèmes a augmenté de manière exponentielle. Cela a rendu la tâche de sécurisation des systèmes de plus en plus difficile, car les vulnérabilités potentielles sont devenues plus nombreuses et plus difficiles à identifier.

Évolution constante des menaces : les cybercriminels utilisent des techniques sophistiquées pour exploiter les vulnérabilités des systèmes informatiques, et ils sont constamment à la recherche de nouvelles façons d'attaquer. La complexité et la diversité des menaces ont rendu la protection des systèmes informatiques encore plus difficile.

Manque de normes de sécurité communes : il n'y a pas de normes de sécurité universelles pour les systèmes informatiques, ce qui rend difficile la coordination des efforts de cybersécurité entre les pays et les organisations. Les normes de sécurité varient considérablement d'un pays à l'autre, et même d'une organisation à l'autre, ce qui peut entraîner des lacunes dans la protection des systèmes informatiques.

Coût élevé de la mise à niveau des systèmes : les entreprises et les organisations doivent constamment mettre à jour leurs systèmes pour se protéger contre les dernières menaces de cybersécurité. Cependant, cela peut être très coûteux, en particulier pour les petites entreprises qui n'ont pas les ressources nécessaires pour investir dans des mesures de sécurité de pointe.

Problèmes de confidentialité : certaines mesures de cybersécurité, telles que la surveillance des communications en ligne, peuvent poser des problèmes de confidentialité pour les utilisateurs. Il est important de trouver un équilibre entre la protection des systèmes informatiques et le respect de la vie privée des utilisateurs.

Ces problématiques montrent que la cybersécurité est un domaine complexe et en constante évolution, qui nécessite une attention constante pour s'assurer que les systèmes informatiques sont protégés contre les menaces croissantes de cybercriminalité.

2.4 Avantages / inconvénients <> points forts / points faibles

Les nouvelles tendances en matière de cybersécurité offrent de nombreux avantages pour les entreprises et la société dans son ensemble. Voici quelques-uns des points forts :

Amélioration de la sécurité des données : les nouvelles technologies de cybersécurité offrent des niveaux de sécurité plus élevés pour les données des entreprises et des utilisateurs. Cela peut aider à prévenir les pertes de données et les violations de données, qui peuvent causer des dommages importants aux entreprises et à leurs clients.

Détection plus rapide des menaces : certaines nouvelles technologies de cybersécurité utilisent l'intelligence artificielle et l'apprentissage automatique pour détecter les menaces plus rapidement et plus efficacement. Cela permet aux entreprises de réagir plus rapidement aux menaces de sécurité et de minimiser les pertes potentielles.

Réduction des coûts : en améliorant la sécurité des données, les entreprises peuvent réduire les coûts associés aux pertes de données et aux violations de données. Les nouvelles technologies de cybersécurité peuvent également aider à réduire les coûts liés à la gestion de la sécurité des données en automatisant certaines tâches et en améliorant l'efficacité globale de la sécurité des données.

Cependant, il y a aussi des inconvénients et des freins associés à la mise en place de nouvelles tendances en matière de cybersécurité. Voici quelques-uns des points faibles :

Coûts initiaux élevés : la mise en place de nouvelles technologies de cybersécurité peut être coûteuse, en particulier pour les petites entreprises qui ont des budgets limités. Les coûts peuvent inclure l'achat de nouveaux logiciels, la formation du personnel et la mise à niveau des systèmes informatiques existants.

Risques de compatibilité : certaines nouvelles technologies de cybersécurité peuvent ne pas être compatibles avec les systèmes informatiques existants de l'entreprise. Cela peut nécessiter des mises à niveau supplémentaires ou des modifications des systèmes existants pour garantir la compatibilité.

Risques juridiques : la mise en place de nouvelles technologies de cybersécurité peut entraîner des risques juridiques pour les entreprises, notamment en ce qui concerne la confidentialité des données des clients et la conformité aux lois et réglementations en matière de protection des données.

Résistance humaine : les employés peuvent résister à l'utilisation de nouvelles technologies de cybersécurité en raison de préoccupations liées à la confidentialité et à la complexité du système. Il est important de fournir une formation adéquate et de communiquer clairement les avantages de la mise en place de nouvelles technologies de cybersécurité pour aider à surmonter cette résistance.

Ces avantages et inconvénients montrent que la mise en place de nouvelles tendances en matière de cybersécurité est une décision importante qui doit être bien réfléchie et planifiée pour maximiser les avantages et minimiser les risques.

2.5 Dimension juridique

La dimension juridique est essentielle dans le domaine de la cybersécurité. En effet, les données qui transitent sur les réseaux sont souvent soumises à des réglementations strictes en matière de confidentialité, d'intégrité et de disponibilité. Ainsi, les entreprises et les organisations qui collectent, traitent ou stockent des données personnelles doivent se conformer aux lois et aux réglementations en vigueur, telles que le RGPD (Règlement Général sur la Protection des Données) en Europe.

Par ailleurs, la dimension juridique de la cybersécurité englobe également les aspects liés à la responsabilité civile et pénale en cas d'incident de sécurité. Les entreprises peuvent être tenues responsables si elles ne mettent pas en place les mesures de sécurité adéquates pour protéger les données qu'elles traitent. En outre, les États peuvent engager des poursuites pénales contre les auteurs d'attaques informatiques, qu'il s'agisse de cybercriminels, d'espions industriels ou de groupes de hackers.

Enfin, la dimension juridique de la cybersécurité concerne également les accords internationaux de coopération entre les États en matière de lutte contre la cybercriminalité. Les accords de ce type permettent aux pays de partager des informations, de coordonner des enquêtes et de poursuivre les auteurs d'infractions au niveau international.

2.6 L’avis des experts

Parmi les experts reconnus du domaine, on peut citer Bruce Schneier, chercheur en sécurité informatique et cryptographe renommé, qui a notamment publié de nombreux ouvrages sur la cybersécurité. On peut également mentionner Brian Krebs, journaliste spécialisé dans la sécurité informatique, qui a révélé plusieurs grandes affaires de piratage et de cybercriminalité.

En France, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'expert national en matière de cybersécurité. Elle conseille les entreprises et les administrations publiques sur les mesures de sécurité à mettre en place et coordonne la réponse aux incidents de sécurité.

Il est important de prendre en compte l'avis des experts du domaine pour prendre des décisions éclairées en matière de cybersécurité, que ce soit pour l'adoption de nouvelles technologies ou pour la mise en place de mesures de sécurité efficaces.

2.7 Etat actuel

Actuellement, la cybersécurité est un domaine en constante évolution, en réponse à l'émergence de nouvelles menaces et à l'évolution des technologies. Les entreprises et les organisations sont de plus en plus conscientes de l'importance de la sécurité informatique et cherchent à mettre en place des mesures de protection efficaces.

Les technologies de cybersécurité telles que les firewalls, les antivirus, la détection d'intrusion ou encore la gestion des identités et des accès sont de plus en plus sophistiquées et intégrées dans des solutions globales de sécurité. De même, la technologie blockchain est de plus en plus utilisée pour assurer la sécurité des transactions et des échanges de données.

En parallèle, les cyberattaques sont de plus en plus nombreuses et sophistiquées, avec l'émergence de nouvelles formes de cybercriminalité telles que le ransomware ou les attaques par déni de service distribué (DDoS).

Dans l'ensemble, la cybersécurité est en phase de démocratisation, avec une prise de conscience croissante de son importance et une généralisation de son usage. Cependant, la complexité des enjeux et la diversité des menaces rendent la tâche difficile et nécessitent une approche globale et coordonnée de la sécurité informatique.

2.8 Evolution

Il est difficile de prédire avec certitude l'évolution de la technologie de la cybersécurité dans les années à venir, mais certaines tendances se dessinent.

Tout d'abord, on peut s'attendre à une évolution continue des technologies de sécurité, avec une intégration croissante de l'intelligence artificielle et de l'apprentissage automatique pour détecter et prévenir les menaces. Les systèmes de sécurité deviendront également de plus en plus adaptatifs et capables de s'autoréparer en cas d'attaque.

Parallèlement, la technologie blockchain continuera de se développer et de s'étendre à de nouveaux secteurs, avec une utilisation croissante pour sécuriser les échanges de données et de transactions.

Cependant, les cybercriminels ne resteront pas inactifs et continueront de développer de nouvelles techniques d'attaque. Les ransomwares, les attaques par phishing et les attaques par déni de service restent des menaces importantes, et de nouvelles formes d'attaques émergeront sans aucun doute.

Enfin, la cybersécurité deviendra de plus en plus un enjeu stratégique pour les entreprises et les organisations, avec une implication croissante des gouvernements dans la régulation et la protection des infrastructures critiques.

3 Bilan de ma veille

Grâce à cette veille sur les nouvelles tendances en matière de cybersécurité, j'ai pu acquérir plusieurs compétences et connaissances importantes.

Tout d'abord, j'ai approfondi ma compréhension des enjeux de la cybersécurité dans un contexte en constante évolution. J'ai pu prendre connaissance des dernières technologies et tendances, ainsi que des défis et des risques associés à leur utilisation.

Ensuite, j'ai pu découvrir les différentes dimensions de la cybersécurité, y compris les aspects juridiques et les opinions des experts du domaine. J'ai également appris à analyser les avantages et les inconvénients d'une technologie ou d'une pratique de sécurité spécifique, ainsi qu'à évaluer son évolution future.

Dans mon futur métier ou projet professionnel, ces compétences et connaissances seront essentielles pour mener à bien des projets de sécurité informatique. Je serai en mesure d'analyser les menaces et les risques, de sélectionner les meilleures pratiques et technologies de sécurité pour répondre à ces défis, et de communiquer efficacement avec les parties prenantes pour assurer une mise en œuvre réussie.

En somme, cette veille m'a permis d'acquérir des connaissances précieuses qui me seront utiles tout au long de ma carrière dans le domaine de la cybersécurité.