Question 3 :

L’organisation peut éduquer son personnelle via des formations de cybersécurité ou l’intervention de personne qualifiée pour leur apprendre a se protéger.Il faut aussi que les programmes et vidéos proposer soif a jour et il faut tenter de divertir tous en apprenant car sinon les employers ne ferrons pas attention a ce qui est dit par la personne ou la vidéo, donc cela ne servira a rien.

Question 4 :

Le RGPD est un règlement qui vise les entreprises et qui a pour but d’assurer la protection des données à caractère personnel.

Question 5 :

Les menaces qui pèsent sur les entreprises sont des amendes de 20 millions de dollars ou jusqu’à 4% du chiffre d’affaire de l’entreprise. Il y a aussi de menace de piratage car maintenant a la place de bloquer les donnée il les rendent publique et les tramsmet au CNIL pour qu’il recoive l’amende.

Question 6 :

-La cybercriminalité est un problème majeur pour les entreprises, avec 8 entreprises sur 10 en France étant touchées par des cyberattaques chaque année. Le phishing (hameçonnage) et l'arnaque au président sont parmi les attaques les plus courantes en 2018.

-Les conséquences des cyberattaques sur les entreprises incluent un ralentissement de la production, l'indisponibilité des sites Web, des retards de livraison, des pertes de chiffre d'affaires, et d'autres effets négatifs.

-La transformation numérique, y compris l'utilisation du cloud et de l'Internet des objets (IoT), a un impact sur la sécurité des données des entreprises.

-Les PME sont également des cibles fréquentes, avec 43% des cyberattaques les visant.Les principales méthodes d'attaque sont le phishing, les malwares, les rançongiciels et la fraude au président.La sensibilisation des employés aux risques informatiques est essentielle, mais seulement 17% des PME sont assurées contre les attaques informatiques.

-Les coûts des attaques informatiques sont élevés, avec le coût moyen d'une attaque de malware de 2,4 millions de dollars en 2017.

-Malgré la progression de la cybercriminalité, les dépenses en cybersécurité ne devraient augmenter que de 9% par an et par entreprise d'ici à 2023 ce qui est largement insuffisant.

-La France dispose de ressources telles que 500 investigateurs cybers et 2 000 enquêteurs sur Internet pour lutter contre la cybercriminalité.

-Les solutions de cybersécurité évoluent pour faire face à ces menaces, notamment avec l'architecture SASE (Secure Access Service Edge) et le SOC (Security Operation Center) nouvelle génération.

-Le SASE vise à gérer toute la cybersécurité de l'entreprise depuis une plateforme Cloud unique, simplifiant ainsi la protection de la surface d'exposition croissante.

-L'EDR (Endpoint Protection & Response) offre une protection avancée des terminaux, tandis que le XDR (Extended Detection Response) étend cette protection à d'autres points d'accès.

-Le Next Gen SOC (Security Operation Center) est plus agile et réactif, capable de réagir de manière automatisée pour contrer les menaces.

Question 7 :

 l'utilisation préméditée des activités perturbatrices, ou la menace de celle-ci, contre des ordinateurs et / ou réseaux, dans l'intention de causer un préjudice de nature sociale, idéologique, religieuse, politique, ou autres objectifs. Ou pour intimider toute personne dans la poursuite de tels objectifs

La grande différence ces que la cybercriminaliter a un but lucratif et vise tous le monde tandis que le cyberterrorisme a pour but de causer du tord a certainne personne en particulier

Question 8 :

Attaque de SolarWinds (2020) : Des cybercriminels ont compromis le logiciel de gestion des réseaux de SolarWinds, ce qui a permis de pénétrer dans de nombreuses agences gouvernementales américaines et entreprises du secteur privé. Les conséquences incluent la collecte d'informations sensibles et la compromission de la sécurité nationale, avec des allégations d'implication russe.

WannaCry (2017) : Ce ransomware a touché des organisations dans le monde entier, paralysant des systèmes informatiques essentiels. Bien que WannaCry ait été attribué à un groupe de pirates nord-coréen, il n'a pas eu de conséquences directes sur la sécurité mondiale, mais a montré la vulnérabilité des infrastructures critiques.

Attaque de l'électricité en Ukraine (2015 et 2016) : Des groupes de hackers, ont réussi à couper l'électricité dans certaines parties de l'Ukraine, provoquant des perturbations majeures.

Ces incidents ont eu des conséquences variées sur la sécurité mondiale, allant de la mise en évidence des vulnérabilités des infrastructures critiques à l'accroissement des tensions entre États. Ils ont également conduit à des appels à renforcer la cybersécurité et à élaborer des normes internationales pour prévenir de futures attaques. La cybermenace est devenue un enjeu majeur de sécurité mondiale, avec une surveillance accrue et des efforts pour dissuader les acteurs malveillants.

L’onde de choc STUXNET (2010) : c’est un ver informatique découvert dans les installations nucléaire iraniennes qui avait pour but d’espionner et de détruire les systèmes industriels, ce malware a été conçue par les Américains dans le but de ralentir le programme nucléaire des Iraniens.

Le piratage de SONY Entertainment (2011) : Intrusion dans les servers de sony ce qui a pour effets une vole de millions de donnée personnelles et un arrêt des services en ligne pendant plusieurs mois.

Question 9 :

Les stratégies utiliser sont la surveillance d’internet, la collaboration avec des grandes entreprises et au niveau européen la mise en place d’un **Centre européen de lutte contre la cybercriminalité.**

Question 1 et 2

<https://www.gloomaps.com/EElHNWpAYl>

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement