WEBINAIRE SECURITE NUMERIQUE DES ENTREPRISES - POLICE NATIONALE - POLE EMPLOI NA - 18/10/2022	
Questions	**Réponses**
Pourra-t-on être informé du label ExpertCyber que vous allez mettre en place ?	Le label expert cyber est mis en place par le GIP ACYMA. Vous trouverez tous les renseignements utiles sur le lien : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/label-expertcyber/decouvrir-le-label-expertcyber
Est ce que les cookies présentent des risques ?	Les cookies sont des petits programmes informatiques qui permettent aux sites web de suivre les internautes. Certaines attaques informatiques peuvent se baser sur les cookies, mais il s'agit de techniques assez avancées. L'usage des cookies dans un navigateur web à jour est tout à fait acceptable.
Existe t-il une base de données publique recensant les vulnérabilités, accessible aux RSSI ou autre ?	Une base pragmatique est la liste des bulletin de vulnérabilités et d'alertes publiés par l'ANSSI (https://www.cert.ssi.gouv.fr/)
Quelles sont les entreprises les plus attaquées en France ? Public ou privé, taille, activité ?	La menace est systémique, tous les domaines sont concernés. On peut toutefois préciser que d'une manière globale, les entités diposant de moyens financiers conséquents seront certainement plus ciblés et exposés à une menace plus soutenue. Certains secteurs sont également plus sensibles comme la santé, l'administration territoriale, les entreprises innovantes ...
En cas de demande de rançon, faut-il la payer pour récupérer ses données ?	Le paiement n'est pas conseillé par défaut car il ne donne aucune certitude sur le fait de réellement récupérer les données et les systèmes attaqués, et cela peut pousser au crime, voire amener d'autres tiers malveillants à tenter de vous attaquer à nouveau.
Idem pour une commune l'envoi d'un mail à cybermenaces-bordeaux ?	L'adresse cybermenaces-bordeaux s'adresse aux entreprises, grandes ou petites, mais également aux associations, aux etablissements publics et aux collectivités territoriales. Dans tous les cas, nous vous apporterons une réponse et vous adresserons vers le bon guichet.
Existe-t-il des supports, publications accessibles pour informer rapidement les salariés des risques et des précautions de base afin que tous en soit conscients ?	Oui, cybermailveillance.gouv.fr, le site l'ANSSI (ssi.gouv.fr) ainsi que le sites de la CNIL
Lorsque j'ai des doutes avec un courriel, je le signale systématiquement sur signalspam, qu'en font-ils? Merci	Ils consolident des statistiques et peuvent opérer des actions auprès des acteurs télécoms.
Quelles sont les voies d'entrée des pirates: mail infecté, site internet de l'entreprise ?	Malheureusement, il en existe pleins. Mails les principales sont: le mail, les vulnérabilités techniques de composant informatiques exposées sur Internet, les défaut de protection des identifiants et mots de passe.
Existe t il une adresse afin de transférer les mails frauduleux à vos services ?	Non, les services de la DCPJ n'ont pas vocation à traiter les mails malveillants. Vous pouvez en revanche nous saisir en cas de cyberattaques avérée.
Pouvez-vous redonner le nom du site pour les fuites de données SVP ?	https://haveibeenpwned.com/

Est ce que vous ne pourriez pas faire une vidéo courte qui serait diffusée par les patrons à tous leurs salariés ? 10 minutes si possible ? ce serait vraiment utile. merci !	Ils existent de nombreux contenus pédagogiques (cf liens évoqués ci-dessus). Nous avons également transmis des videos à Pole Emploi qui vous les transmettra prochainement.
Bonjour, quel partage de la responsabilité dans le cas d'une attaque d'une application de gestion dédiée fournie et hébergée par le "développeur" ?	Dès lors qu'il y aura un tiers qui va traiter une vos données, c'est le contrat établi avec lui qui fera foi. Le cadre contractuel est donc très important.
J'ai un copain qui est intéressé pour travailler dans la cybersécurité, dans la police. Quelle est la démarche pour vous rejoindre ?	Nous recherchons des ingénieurs spécialisés dans l'analyse cybercriminelle ou des spécialistes en cryptomonnaie. Vous pouvez nous contacter sur l'adresse cybermenaces-bordeaux@interieur.gouv.fr
Quelle est l'adresse mail pour avertir et se faire aider?	cybermenaces-bordeaux@interieur.gouv.fr
Quelles sont les attaques qui "marchent bien" ces dernières semaines ?	Le ransomware (logiciel qui bloque tout) représente environ un fait de cyberattaque sur deux.
Quel est le site où nous pouvons trouver le guide ?	Site de l'ANSSI : https://www.ssi.gouv.fr/
Est-ce que lorsqu'on travaille avec un VPN on est en sécurité ? exemple Cyber Ghost ? ou ZDNET ?	Le VPN va permettre de sécuriser les données en transit entre votre ordinateur et le réseau sur lequel vous vous connectez. Il ne va pas apporter une sécurité sur les autres risques (phishing, intrusion…).
Bonjour, pour une commune, qui doit elle alerter en cas de cyberattaque ? Merci.	1 – votre responsable SSI 2 – votre prestataire informatique 3 – nous via notre adresse cybermenaces-bordeaux@interieur.gouv.fr concernant la nouvelle aquitaine. Des adresses similaires existent dans les autres régions françaises.
Doit-on déposer plainte pour une usurpation d'identité sur Facebook ? Que peut-on faire quand Facebook ne réagit pas ?	Oui, dès lors que vous êtes victime d'une atteinte à votre image numérique, un dépôt de plainte peut être opportun. Facebook,et d'une manière plus large, les acteurs importants du numérique, mettent normalement à disposition des formulaires pour les solliciter en cas d'attaque sur un service qu'ils proposent.
Je ne comprends pas ce que veut dire: couper le courant / débrancher en cas d'attaque.	En cas d'attaque, il est recommandé de déconnecter le poste victime du réseau Internet afin de couper toute capacité à l'attaquant de continuer ses méfaits. En revanche, il est pertinent de ne pas éteindre ce poste au risque de perdre les traces numériques associées à l'attaque.
Bonjour , Comment peut on repérer un mail malveillant ?	Quelques questions à se poser: 1/ est ce logique que je recoive ce mail, 2/ ce mail est il cohérent (langue, phrasé, …), 3/ les liens sont ils conformes (pointent ils bien vers les bons domaines) ? 4/ si infos sensibles demandées (mot de passe, code de carte de paiement…) --> attention
Bonjour, Est ce que cette organisation de la police judiciaire va rester la même ou évoluer avec la réforme ?	Les moyens dédiés à la lutte contre la cybercriminalité vont augmenter dans les années à venir, à la fois au niveau central et en région (recours à des ingénieurs, augmentation des policiers spécialisés).
Est ce que la guerre russie ukraine a un impact / cyberattaques contre les entreprises françaises ? Si oui lequel et comment ? En particulier pour les petites entreprises. merci	C'était une crainte au début du conflit. Pour l'instant, ce conflit n'a pas eu d'impact significative sur notre territoire. Les tensions grandissantes de ces dernières semaines pourraient amener à une évolution de cette situation.
Y a-t-il un numéro / mail à composer en cas de doute d'une cyberattaque ?	cybermenaces-bordeaux@interieur.gouv.fr
J'ai fait l'expérience d'un piratage de mes données et n'ai pas pu déposer plainte malgré les attaques répétées. La réponse fut qu'il n'y avait pas de cellule de cybercriminalité proche et donc rien à faire. C'est récent en nouvelle aquitaine?	Non, on vous a certainement fait une mauvaise réponse. Néanmoins, les moyens dédiés à ce type de criminalité restent encore limités et une priorisation est réalisée en fonction des typologies d'attaques et des chances de réussite.

Quel est aussi le budget moyen qu'il faut prévoir par salarié par an (formation, applis, etc.). Avez vous une idée du coût indicatif par salarié minimum	Un principe reconnu: 10 à 15% du budget informatique doit servir directement à la sécurité
Quelle est pour vous les meilleurs outils pour se protèger	Faire attention à ce qu'on publie sur Internet, avoir des mots de passe complexe et différenciée, stockés dans un coffre fort de mot de passe (ex KeePass)
Le coût matériel et logiciel pour la protection d'un réseau a un certain prix (pare-feu, VPN...). Des aides existent- elles pour des petites entreprises ou des associations pour pouvoir sécuriser leurs services ?	Je vous conseille de vous rapprocher du campus cyber de nouvelle Aquitaine, qui vous accompagnera sur ces questions.
S'il y avait une seule mesure gratuite que je pouvais faire appliquer immédiatement par mes gars pour fortement renforcer mon niveau de protection laquelle me conseillez vous ? Et si je devais prendre une deuxième mesure éventuellement payante, laquelle me conseillez vous?	Changer les mots de passe, faire des sauvegardes et les tester régulièrement
Comment sait on que nous sommes victime d'usurpation d'identité ?	C'est parfois complexe. Une solution peut être de se chercher régulièrement sur Internet.
Bonjour nous avons eu vent de remplacement «automatique» de pièces jointes dans les mails, notamment les fichiers nommés rib ou iban. avez vous déjà rencontré ce genre de menace ?	Oui, souvent, l'attaquant a compromis un des deux mails dans une conversation et va envoyer de manière opportuniste un nouveau RIB/IBAN. Une manière simple de se protéger est de mettre en place une processus de validation de changements de RIB passant par un autre canal de communication que le mail (ex appel de confirmation)
Avez-vous entendu d'escroquerie d'une action Porsche avec la banque Shine ?	non
Outre mots de passe, quels outils sont à mettre en place en priorité pour protéger son entreprise ?	Mise à jour régulière des systèmes, sauvegardes régulières avec test, sensibilisation du personnel, déploiement d'un antivirus à jour
Comment peux t'on savoir qu'on est victime d'usurpation d'identité numérique, merci ?	C'est parfois complexe. Une solution peut être de se chercher régulièrement sur Internet.