WEBINAIRE SECURITE NUMERIQUE DANS L'INDUSTRIE DU 29/11/2022 GENDARMERIE NATIONALE - POLEMETAL2S - POLE EMPLOI NA	
Questions	**Réponses**
Mon Colonel, les sanctions sont-elles suffisantes pour dissuader l'assaillant ?	un accès frauduleux à un système de traitement automatisé de données (STAD), infraction la plus communément retenue, c'est passible de 2 ans d'emprisonnement et 60000€ d'amende qui peut monter à 3 ans et 100000€ s'il y a altération des données ou du fonctionnement. La collecte de données par un moyen frauduleux c'est 5 ans et 300000€. En comparaison le trafic de stupéfiant (art 222-37 du cp) c'est 10 ans et 7500 000€… Précision : il s'agit ici des peines maximum … très rarement prononcées. Ce qui peut avoir un réel impact, ce sont les peines complémentaires, qui peuvent entraîner la confiscation du matériel et des biens acquis grâce aux gains frauduleux et certaines interdictions qui peuvent être lourdes de conséquences (interdiction de droits civiques, interdiction de séjour, etc.)
Que pensez vous, pour suppléer le mot de passe, de la double authentification ?	La double authentification comme la multi authentification ne supplée pas le mot de passe. Il faut utiliser les 2. Nous conseillons d'ailleurs d'utiliser les multi authentifications dès qu'elles vous sont proposées.
Pour un pirate informatique, quelle sanction maximum pour lui (pour comparer risques et gains)?	voir réponse au dessus Précision : les gains de la cybercriminalité peuvent être rapidement très importants. En l'absence de législation commune mondiale, malgré le renforcement de la coopération internationale, il est compliqué d'identifier un cyberdélinquant. Et lorsqu'il s'agit uniquement d'atteintes aux biens (escroqueries), il y a peu de chances que les peines prononcées soient fortes.
Donner la principale menace qui affecte les TPE industrielles ? Ex sous traitant chaudronnerie de chantier naval avec utilisation applicatifs clients…	Le secteur industriel est le secteur le plus touché par les rançongiciels

Dommage qu'un dépot de plainte ne génère pas automatiquement d'enregistrement à la CNIL ou autre organisme	Effectivement, dès qu'une perte ou vol de données est constaté, il faut le signaler à la CNIL tel que prévu par la loi, mais c'est un autre canal que la plainte qui elle va servir les services judiciaires, déclencher l'enquête et permettre le recoupement d'informations.
Les assurances assurent elles une couverture aux attaques cyber ? un partenariat avec l'Etat?	Oui, et elles conditionnent généralement leur couverture à une élévation du niveau de sécurité informatique de l'entreprise. Actuellement des discussions sont en cours au Parlement sur le rôle des assurances en matière cyber et cela sera acté dans la LOPMI. Je vous invite à vous rapprocher de votre assureur pour en discuter car son rôle sera essentiel en cas d'attaque.
Ou d'aider à financer ces formations ? Et d'ailleurs est-ce nécessaire ou les guides et ressources que vous proposez sont suffisants ?	Les guides sont déjà une bonne chose mais la prévention passe par la répétition des conseils. Il existe beaucoup d'évènements en accès gratuit, comme ce webinaire. Des actions peuvent être régulièrement organisées au sein des entreprises, par les responsables informatiques. Ces actions peuvent être appuyées par des supports produits par l'ANSSI ou Cybermalveillance. Ex : le MOOC de l'ANSSI très bien fait.
Est-ce que l'état a prévu de financer des formations cyber pour former nos collaborateurs ? Cpf ?	Oui, voici plusieurs liens utiles qui parle aussi du CPF https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/formation-cybersecurite https://www.ffcybersecurite.org/formation
Comment définiriez-vous le profil d'une Tpe industrielle bien protégée ? En quelques mots concrètement Merci !	Difficile de répondre à cette question, le mieux étant de respecter au plus près les règles de bonnes pratiques mais aussi de sécurité proposées dans les guides du clusif et de l'anssi. Par ailleurs, il vaut mieux aussi mettre en place une organisation qui permette de revoir régulièrement ces règles.

Faut-il communiquer ou éviter de communiquer pour se protéger ? Comment intégrer le risque cyber à son marketing et sa e communication?	Procédez en fonction des différentes phases : avant, pendant, après la crise. Associez vos collaborateurs très en amont à la cybersécurité (formation, exercices etc.) afin qu'ils deviennent le maillon fort, prévoyez un plan de communication en cas de crise surtout vis à vis de l'extérieur, et enfin ne laissez pas dans le flou après la crise, le temps de la remédiation vos collaborateurs et vos partenaires. En terme de marketing, même si ce n'est pas forcément notre coeur de métier, il me semble que si vous communiquez sur un niveau important de sécurité informatique ou au moins que le risque est bien pris en compte, c'est un gage de confiance pour vos clients. Précision : Vous n'aurez parfois pas le choix de communiquer sur vos technologies ou vos marchés. Vous devez alors prendre en compte qu'en le faisant, vous donnez peut-être des informations qui permettront à un attaquant de savoir par où passer. Si vous en avez conscience, vous pouvez prendre de mesures de contrôle renforcées, spécifiques à ces risques.
La médiatisation n'est-elle pas dangereuse pour la pérennité de l'entreprise. Quel client va encore faire confiance à cette société ?	Oui c'est un risque mais n'oubliez pas que vous êtes une victime. Que la clareté et l'honneteté sont aussi un signe de confiance et qu'enfin, si vous ne communiquez pas, d'autres le feront à votre place et vous ne maîtriserez plus ce qui se dit. Par ailleurs vous avez aussi des obligations légales notamment vis à vis de la CNIL en cas de perte ou vol de données. Voici à quoi pourrait ressembler une communication qui montre que vous êtes victimes mais que vous assumez et que vous gérez : *« Depuis cette nuit, nous sommes victimes de (….). Nos équipes sont mobilisées pour limiter les impacts et relancer notre activité … etc. Nous avons fait appel à une société spécialisée … etc. Nous avons porté plainte et une enquête est ouverte par la gendarmerie.* *Nous demandons aux clients qui disposent d'un compte sur notre site internet de vérifier qu'ils en ont toujours l'accès et de modifier au plus vite leur mot de passe. Pour toute difficulté, vous pouvez contacter le numéro (…) ».* Ça fait partie des choses auxquelles vous devez penser avant que cela n'arrive.
Est-ce que les données personnelles des salariés doivent être cryptées ?	Ce n'est pas une obligation mais par contre il faut les protéger au mieux ce qui peut passer par du chiffrement

Que faire avec ses collaborateurs pour les former en peu de temps ?	Des séances d'informations et de mise en situation régulières (tous les 6 mois). Pour commencer plein de formations sont disponibles sur les sites de cybermalveillance et anssi Précision : cela ne se fera, malgré tout, pas en peu de temps … Deux actions peuvent cependant être réalisées facilement, qui permettent de sensibiliser et d'impliquer les collaborateurs : 1/ leur faire signer une charte d'utilisation des systèmes d'information et de communication en expliquant leurs responsabilités. 2/ coller des affiches de prévention au risque cyber aux endroits stratégiques (près de la machine à café, dans les vestiaires, dans les toilettes, …)
bonjour , quel est le niveau de sécurité des données hébergées dans le cloud pour les applications 365 (sharepoint, onedrive , outlook , ...) ?	Aucun système n'est sur à 100 %, le mieux est donc d'appliquer une bonne politique de sauvegarde sur plusieurs supports, à différents endroits et de pouvoir les tester régulièrement. Précision : le cloud permet de transférer certaines responsabilités au fournisseur de service (ici Microsoft) mais il faut bien avoir conscience que mettre des données sur le cloud, c'est mettre ses données en ligne. Et c'est aussi confier ses données à une autre entreprise qui pourrait être intéressée par ces données. Microsoft, par exemple, ce n'est pas français.
Quelle est le geste le plus important ?	La gestion des sauvegardes mais ce n'est pas suffisant. Appliquez les 4 pts que l'on a cité : - cyber bon sens - gestion des mots de passe - gestion des accès (compte) - gestion de la sauvegarde
BONJOUR sur quel support pouvons nous ranger nos Mdp ?	Le plus simple est d'utiliser un gestionnaire de mots de passe. En plus de les stocker, il pourra même vous les créer. Il existe des tas de produits sur le marché ; des payants et des gratuits. Certains citent KEEPASS en expliquant qu'il est certifié par l'ANSSI. C'est vrai, pour la version 2.10 portable de 2010, certifiée en 2011 … Ça reste tout de même un très bon produit. Il en existe d'autres qui sont régulièrement cités par des sites spécialisés : NordPass, LastPass, Dashlane, 1Password, etc. L'inconvénient du gestionnaire, c'est que s'il est attaqué, le cyberdélinquant aura accès à tous vos mots de passe … Vous pouvez utiliser des méthodes alternatives pour créer et mémoriser des mots de passe solides. Je pense que vous pouvez retrouver cela sur des replay de webinaires que nous avons faits, sur le site de Pôle Emploi Nouvelle Aquitaine.

Les vulnérabilités peuvent-elles venir des fournisseurs (exemple dans l'actualité avec l'ARS Ile de France). Quels conseils pour les sociétés en marché (il faut respecter le code des marchés + quels autres éléments)?	Oui, il faut avoir un vrai point d'attention sur ce qu'on appel la supply chain (les chaines d'approvisionnement) qui servent souvent de porte d'accès et/ou de rebond. Il faut donc les prendre en compte dans une analyse de risque. Par contre je ne peux vous répondre sur les stè en marché si ce n'est de toujours vérifier les origines des mails, demandes diverses et variées et d'avoir des mécanismes internes de contrôle notamment s'il s'agit d'ordre de virement.
Si les mots de passe sont sauvegardés sur l'ordinateur est-ce grave	S'ils sont stockés de manière sécurisée (chiffrement), ce n'est pas un problème : par exemple avec un gestionnaire de mots de passe. Mais s'ils sont enregistrés par votre navigateur ou inscrits dans un fichier texte ou autre, non chiffré, alors oui, c'est problématique. Si un attaquant parvenait à entrer sur votre système, il aurait la possibilité de lire ce fichier et d'accéder à tout.
Est il possible de prévenir "80%" des attaques avec 2 ou 3 gestes ? Lesquels ?	Peut-être pas 80 % mais en tout cas de réduire significativement les risques oui. En appliquant les 4 pts cités plus haut, à la ligne 20.
Dans la motivation des attaquants, pouvons-nous penser que le risque de sanctions qu'ils encourent peuvent rentrer dans cette catégorie (extradition impossible à l'autre bout du monde) ?	Evidemment cela joue comme par exemple certains groupes cybercriminels qui demandent à ne pas cibler dans les attaques tels ou tels pays pensant ainsi limiter l'impact des enquêtes internationales. De plus, la mise en œuvre d'une procédure de coopération internationale nécessite un certain niveau de criminalité. Elle ne sera pas mise en œuvre pour quelque milliers (ou même dizaines de milliers) d'euros. Et certains procureurs de la République classent même sans suite toute procédure dont le préjudice ne dépasse pas une certaine somme … Il est très facile de faire 1 million d'escroqueries à 1€ … Personne n'ira porter plainte pour 1€ et s'il y a plainte, il n'y aura probablement pas d'enquête.
Recommanderiez-vous de prendre une assurance contre les cyberattaques ?	Les assurances ont effectivement un grand rôle à jouer mais peuvent conditionner leurs prises en charges à votre niveau de sécurité informatique. Il faut bien en discuter avec elles