MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES

Liberté
Égalité
Fraternité

DIRECTION DES RESSOURCES HUMAINES

SOUS-DIRECTION DE L'ATTRACTIVITÉ ET DES RECRUTEMENTS

Bureau des concours et examens professionnels

Concours interne et 3ème concours pour le recrutement dans le grade d'adjoint administratif principal de 2ème classe de chancellerie

Section numérique

Sujet V0

Epreuve unique d'admissibilité

Durée totale de l'épreuve : 2 heures – coefficient 3

Rédaction d'un écrit professionnel fondé sur la base d'un dossier complétée par la réponse à un questionnaire à choix multiple, dans la section choisie au moment de l'inscription. Certaines questions ou documents pourront être proposés en anglais.

Sujet au verso

1/ Cas pratique

Vous êtes agent ressource à l'ambassade de France en Syldavie, l'ambassadeur vous demande de préparer un mail, à sa signature, adressé à l'ensemble des agents pour les sensibiliser à la sécurité de l'information et des communications au sein de l'ambassade en développant les points qui vous semblent incontournables pour le réseau diplomatique et consulaire. Vous vous appuierez sur les documents joints pour préparer votre projet.

2/ Questions à choix multiples (cochez la ou les bonnes réponses) :

1. Sélectionner les enjeux de la cyber sécurité :

   ☐ augmenter les risques pesant sur le système d'information

   ☐ révéler les secrets

   ☐ rendre difficile la vie des utilisateurs en ajoutant plusieurs contraintes comme les mots de passe longs et complexes

   ☐ protéger le système d'information

2. Choisir la ou les réponses correctes :

   ☐ le chiffrement permet de garantir que la donnée sera toujours disponible/accessible

   ☐ la sécurité physique permet d'assurer la disponibilité des équipements et des données

   ☐ la signature électronique permet de garantir la confidentialité de la donnée

   ☐ les dénis de service distribués (DDoS) portent atteinte à la disponibilité des données

3. Select attacks that are usually of type "targeted":

   ☐ phishing ou hameçonnage ;

   ☐ ransomware ou rançongiciel ;

   ☐ social engineering ou ingénierie sociale ;

   ☐ spear phishing ou « l'arnaque au président ».

4. In France, cybersecurity is ponly for private companies and persons :

   ☐ yes
   ☐ no

5. Dans un réseau, qu'est-ce qu'on entend par une zone de confiance ?

   ☐ le hotspot wifi offert aux visiteurs, par exemple dans une gare SNCF

   ☐ le réseau interne (où sont hébergés les postes des utilisateurs et les serveurs) ;

   ☐ le réseau Internet ;

   ☐ une zone démilitarisée (DMZ) ;

6. Entourer la (ou les) proposition(s) vraie(s) lors de l'usage d'un hotspot Wifi

   ▢ les autres personnes connectées peuvent voir mes communications ;

   ▢ je suis protégé des personnes malveillantes ;

   ▢ je suis sur un réseau de confiance, je peux désactiver mon pare-feu ;

   ▢ il peut s'agir d'un faux point d'accès ;

Méthodes de travail : les atouts de l'Agilité

Incontournable dans la gestion de projets en matière informatique, l'approche dite "Agile" a été adoptée par la DNUM du MEAE pour développer ses applications à partir de 2013. Au-delà de ses résultats probants dans ce secteur, l'agilité est une source d'inspiration pour renouveler les méthodes de travail en mode projet ou en équipe, en faisant la part belle à l'humain, à l'engagement collectif et à une circulation fluide de l'information. Retour sur une pratique qui gagne à être connue.

Qu'est-ce que l'agilité dont tout le monde a plus ou moins entendu parler ?

L'agilité se traduit concrètement au travers d'une **famille de pratiques d'organisation et de réalisation de projets** (dont font partie la méthode Extreme programming -XP- ou Scrum). Leur émergence dans les années 1990-2000 a conduit à la rédaction du **"Manifeste du développement agile de logiciels"**, en 2001, par des experts américains. Le terme s'est rapidement imposé pour s'étendre du domaine projet aux organisations elles-mêmes.

Se voulant **plus pragmatiques que les méthodes traditionnelles,** elles impliquent au maximum le demandeur (client) et permettent une grande réactivité à ses demandes. Face à un environnement complexe et changeant, une pratique agile cherchera ainsi à s'adapter en permanence en vue de répondre rapidement et efficacement aux attentes des utilisateurs.

Une place majeure faite à l'humain et à la manière de travailler ensemble

Dans le domaine des systèmes d'information (SI), l'approche Agile repose sur un **style de conduite de projet itératif, incrémental (par palliers) et adaptatif** centré sur l'autonomie des ressources humaines impliquées de bout en bout dans la production d'une application. Elles doivent **respecter les quatre valeurs fondatrices du Manifeste** :

• **Les individus et leurs interactions** plus que les processus et les outils ;
• **Des logiciels opérationnels** plus qu'une documentation exhaustive ;
• **La collaboration avec les clients** plus que la négociation contractuelle ;
• **L'adaptation au changement** plus que le suivi d'un plan.

De ces quatre valeurs découlent **douze principes (voir encadré ci-dessous)** qui prônent **respect, transparence, communication, confiance, simplicité, amélioration continue, motivation, courage** dans le travail d'équipe et la conduite de projets.

Une boîte à outils universelle

Rappelons qu'apparues dans l'industrie du logiciel, ces pratiques agiles ont su convaincre **d'autres métiers en lien avec la transformation numérique,** tels que le marketing ou la gestion des ressources humaines... N'oublions pas qu'une autre pratique Agile, le "Lean" vient de l'industrie automobile (Toyota).

L'approche, basée sur le bon sens et le pragmatisme, peut être très inspirante pour conduire une activité en mode projet ou travailler en équipe. Il peut être enrichissant pour une équipe de piocher dans **la « boîte à outils Agile » :**

- Prioriser la liste des choses à faire selon la valeur qu'elles apportent ;
- Suivre l'avancement des tâches sur un tableau à trois colonnes : « à faire », « en cours », « fait » ;
- Limiter le nombre de travaux « en cours » ;
- Instaurer un point d'avancement quotidien (« Daily stand-up ») au sein d'une équipe, de 15 minutes maximum, ou chacun, debout, répond à trois questions (sans déborder) : Qu'ai-je fait depuis le dernier point ? Que ferai-je jusqu'au prochain ? Quelles difficultés ai-je rencontrées ?

- Rétrospective : faire régulièrement un exercice d'introspection pour déterminer les axes d'améliorations et un plan d'actions immédiates ;
- Favoriser le management visuel…

Il existe même des retours d'expériences réussies sur la rénovation d'une maison en approche Agile ou encore la priorisation d'une lettre au Père Noël… Regardez, essayez, un outil Agile pourrait peut-être vous rendre service !

Les douze principes de l'Agilité :

1. "Notre plus haute priorité est de satisfaire le client en livrant rapidement et régulièrement des fonctionnalités à grande valeur ajoutée ;
2. Accueillez positivement les changements de besoins, même tard dans le projet. Les processus Agiles exploitent le changement pour donner un avantage compétitif au client ;
3. Livrez fréquemment un logiciel opérationnel avec des cycles de quelques semaines à quelques mois et une préférence pour les plus courts ;
4. Les utilisateurs ou leurs représentants et les développeurs doivent travailler ensemble quotidiennement tout au long du projet ;
5. Réalisez les projets avec des personnes motivées. Fournissez-leur l'environnement et le soutien dont elles ont besoin et faites-leur confiance pour atteindre les objectifs fixés ;
6. La méthode la plus simple et la plus efficace pour transmettre de l'information à l'équipe de développement et à l'intérieur de celle-ci est le dialogue en face-à-face ;
7. Un logiciel opérationnel est la principale mesure d'avancement ;
8. Les processus Agiles encouragent un rythme de développement soutenable. Ensemble, les commanditaires, les développeurs et les utilisateurs devraient être capables de maintenir indéfiniment un rythme constant ;
9. Une attention continue à l'excellence technique et à une bonne conception renforce l'Agilité ;
10. La simplicité – c'est-à-dire l'art de minimiser la quantité de travail inutile – est essentielle ;
11. Les meilleures architectures, spécifications et conceptions émergent d'équipes auto-organisées ;
12. À intervalles réguliers, l'équipe réfléchit aux moyens de devenir plus efficace, puis règle et modifie son comportement en conséquence."

https://cyber.gouv.fr/tendances-les-cybermenaces

Quelles sont les principales motivations des attaquants ?

Les motivations des attaquants sont multiples. Les cyberattaques peuvent être catégorisées selon leurs finalités : la recherche de gains financiers, l'espionnage et la déstabilisation. Le Cert-Fr traite et porte une attention particulière à l'ensemble de ces catégories de menaces, puisqu'elles sont susceptibles d'affecter ses bénéficiaires des secteurs publics et privés, et plus généralement les intérêts fondamentaux de la Nation.

L'appât du gain
Les attaques à but lucratif visent à générer un gain financier de façon directe ou indirecte. Elles sont le plus souvent réalisées par des groupes de cybercriminels organisés. La cybercriminalité affecte un large panel d'entités qui se voient ciblées souvent de manière opportuniste par les attaquants. De par ses effets systémiques sur la société et en particulier lorsqu'elle porte atteinte aux intérêts de la Nation, la cybercriminalité fait l'objet d'un traitement par l'ANSSI.

Le pré-positionnement stratégique
Après être parvenu à infiltrer un système d'information, l'attaquant peut décider de s'y installer. C'est ce que l'on appelle le pré-positionnement. Généralement, cela précède une attaque de longue durée dont la finalité n'est pas clairement établie. Ce pré-positionnement peut permettre à l'attaquant de conduire dans un second temps des actions de sabotage ou d'espionnage.

L'espionnage
Les cyberattaques ayant une finalité de renseignement étatique ou économique sont le plus souvent réalisées en infiltrant les systèmes d'information d'une organisation ou d'un individu pour s'emparer des données qui y sont conservées et les exploiter.
L'objectif de telles opérations est de conserver un accès discret et durable au système infiltré afin de capter toute information stratégique d'intérêt. De fait, il faut parfois des années à une organisation pour s'apercevoir qu'elle a été victime d'espionnage.
Un certain nombre de secteurs industriels (armement, spatial, aéronautique, industrie pharmaceutique, énergie, etc.) ou encore certaines activités de l'État (économie, finances, affaires étrangères, défense, etc.) sont particulièrement exposés à ce type de menace.

La déstabilisation
Les opérations de déstabilisation peuvent prendre plusieurs formes.
Certaines opérations d'influence reposent sur la compromission de contenus légitimes (boîtes mails, sites internet) afin de pouvoir les utiliser lors de campagne de diffusion de fausses informations. Ces contenus peuvent être altérés volontairement et diffusés publiquement.
Pour les auteurs de ces opérations, il s'agit avant tout de modifier les perceptions d'une population ou de déstabiliser un acteur donné ou un processus démocratique.
Une cyberattaque peut également être un moyen de porter atteinte à l'image d'autrui. Si elles sont souvent le fait d'« *hacktivistes* », les attaques défigurant un site internet ou le saturant de connexions automatisées peuvent être commises par des concurrents, des employés mécontents, voire par des organisations étatiques afin de décrédibiliser leur cible.
Enfin, certaines cyberattaques peuvent prendre la forme d'actions de sabotage informatique qui consistent à rendre inopérant tout ou partie du système d'information (y compris les systèmes industriels) d'une organisation *via* une cyberattaque.
Certains attaquants cherchent à se prépositionner sur des systèmes d'informations stratégiques dans la longue durée. La finalité de ces intrusions est souvent peu claire, entre espionnage et préparation d'actions de sabotage.

Quelles sont les capacités et techniques des attaquants ?

Les attaques se limitent rarement à une seule technique et sont perpétrées par une large palette d'acteurs, de l'individu isolé aux organisations offensives étatiques.

Les acteurs cybercriminels, bien qu'animés par une recherche du meilleur ratio coût/bénéficie, peuvent parfois adopter des modes opératoires semblables à ceux d'acteurs soutenus par des gouvernements, en préparant minutieusement leurs opérations, en persistant sur les réseaux de leurs victimes pendant de longues périodes à la recherche de ressources d'intérêt et parfois en exploitant des vulnérabilités inconnues (0-Day). Par ailleurs, cette mise à disposition d'outils et services malveillants prêts à l'emploi peut profiter à d'autres types d'attaquants, notamment motivés idéologiquement tels que les hacktivistes.

Les attaquants étatiques peuvent avoir des capacités sophistiquées et développer des codes et des méthodes d'attaques très spécifiques. Ils s'inspirent également des méthodes cybercriminelles en s'appropriant des codes et outils traditionnellement utilisés par les attaquants cybercriminels tels que des rançongiciels. Pour se dissimuler, ils peuvent exploiter des outils légitimes présents sur les réseaux des victimes, échappant ainsi à la détection (selon la technique du *living-off-the-land* - LotL). Le développement de capacités offensives par des entreprises privées telles que NSO Group rend accessibles des capacités parfois de pointe à des acteurs n'ayant pas les moyens de les développer ou souhaitant maintenir une possibilité de déni plausible.

Afin de conduire leurs campagnes offensives, les attaquants peuvent utiliser plusieurs types d'attaques tels que :

Les attaques sur la chaine d'approvisionnement (*supply chain attack*) :

Ce type d'attaque consiste à compromettre un tiers, comme un fournisseur de services logiciels ou un prestataire, afin de cibler la victime finale. Cette technique est éprouvée et exploitée par plusieurs acteurs étatiques et cybercriminels depuis au moins 2016. Cette méthode présente un risque de propagation rapide d'une attaque qui peut parfois concerner un secteur d'activité entier ou une zone géographique précise notamment lorsque l'attaque cible un fournisseur de logiciels largement répandus, une entreprise de service numérique (ESN) locale ou spécialisée dans un secteur d'activité particulier.

Attaque par rançongiciel

Les attaques de type « rançongiciel » (*ransomware*) ciblent tous types d'organisations, y compris les acteurs publics et les services gouvernementaux. Très répandus, les rançongiciels sont des logiciels malveillants qui chiffrent l'ensemble des données, outils et applications de la victime (fichiers, messagerie, SAP, *etc*.). Pour les récupérer, cette dernière se voit demander le paiement d'une rançon en échange de la clé de déchiffrement. Les cybercriminels exfiltrent parfois les données internes de leur cible avant l'attaque, afin d'augmenter leur pression en menaçant de les publier.

Attaques par point d'eau

L'attaque par point d'eau (*watering hole*) consiste à piéger un site internet légitime afin d'infecter les équipements informatiques des visiteurs. Elle peut aussi bien être employée contre des entreprises privées que des institutions travaillant sur des secteurs sensibles et qui disposent de systèmes informatiques hautement protégés et difficiles à attaquer.

Défiguration de sites internet

Ce type d'attaque peut viser tout type d'organisation et exploite souvent des vulnérabilités connues mais non corrigées, pour ajouter ou modifier des informations dans une page web à des fins de revendications. Ces opérations sont généralement revendiquées par des hacktivistes pour motifs politiques ou idéologiques, ou à des fins de défi technique entre attaquants.

Quels sont les profils des attaquants ?

Les auteurs de cyberattaques affichent des profils d'une grande diversité. Selon ces profils, les motivations varieront. L'ANSSI constate cependant une tendance à la collaboration entre certaines catégories d'attaquants aux objectifs proches.

Etats et agences de renseignement

Les Etats et agences de renseignements ont la capacité de réaliser une opération offensive de longue durée (ressources stables, procédures, *etc*.) et d'adapter leurs outils et méthodes à la typologie de la cible.

Organisations criminelles

Du fait de la prolifération des *kits* d'attaques facilement accessibles en ligne et d'une spécialisation de l'offre technique sur le *darknet*, les organisations criminelles mènent des opérations de plus en plus sophistiquées et organisées, à des fins lucratives ou de fraude.

Hacktivistes

Cette catégorie d'attaquant se distingue généralement par des attaques peu sophistiquées. L'objectif de ces individus est ainsi de véhiculer des messages et idéologies en ayant recours à différentes méthodes pour amplifier l'écho de leur action.

Entreprises spécialisées dans la vente de prestations et de services cyber-offensifs

Ces officines sont généralement dotées de capacités informatiques élevées sur le plan technique et proposent de véritables services de piratage à leurs clients. Plusieurs offres de services sont possibles : des outils clé en main, de l'expertise humaine ou encore des capacités telles que des méthodes d'exploitation de vulnérabilités 0-Day. Si ces services sont généralement réservés à des clients étatiques dans le cadre de la lutte contre le terrorisme et la criminalité organisée, ils peuvent être détournés à des fins d'espionnage stratégique et politique à l'encontre d'autres cibles telles que des journalistes, des défenseurs des droits de l'Homme et de hauts responsables ainsi que d'entreprises détenant des données à caractère personnel ou stratégiques.

Amateurs

Également appelés « *script-kiddies* », ces attaquants sont dotés de connaissances informatiques et motivés par une quête de reconnaissance sociale, d'amusement, de défi. Ils conduisent généralement des attaques basiques mais sont parfois à même d'utiliser les *kits* d'attaques proposés en ligne.

Menace interne

Cette typologie d'attaquant peut être guidée par un esprit de vengeance aigu ou un sentiment d'injustice. Il peut par exemple s'agir d'un salarié licencié ou encore d'un prestataire mécontent suite au non renouvellement d'un marché.

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-usages-pro-perso

Apprendre à séparer ses usages pro-perso

La transformation numérique modifie en profondeur les usages et les comportements. Être connecté est devenu le quotidien. Le développement des technologies mobiles (PC portables, tablettes, smartphones) offre désormais la possibilité d'accéder, depuis presque n'importe où, à ses informations personnelles mais aussi à son système informatique professionnel : la frontière numérique entre la vie professionnelle et personnelle devient de plus en plus poreuse. Face à cette évolution, il est nécessaire d'adapter ses pratiques afin de protéger tant votre entreprise* ou votre organisation, que votre espace de vie privée.
Voici 10 bonnes pratiques à adopter pour la sécurité de vos usages pro-perso.

**Le terme « entreprise » employé dans ce document regroupera toutes les organisations professionnelles qu'elles soient à caractère privé, public ou associatif.*

1. Utilisez des mots de passe différents pour tous les services professionnels et personnels auxquels vous accédez

L'affichage du contenu tiers "dailymotion" a été bloqué conformément à vos préférences.

Si vous ne le faites pas et qu'un des services auquel vous accédez se fait pirater, le vol de votre mot de passe permettra à une personne malveillante d'accéder à tous vos autres services y compris les plus critiques (banque, messagerie, sites marchands, réseaux sociaux…). Si vous utilisez ce même mot de passe pour accéder au système informatique de votre entreprise, c'est elle que vous mettez aussi en péril, car un cybercriminel pourrait utiliser vos identifiants de connexion pour voler ou détruire des informations.

2. Usages pro-perso : Ne mélangez pas votre messagerie professionnelle et personnelle

Ce serait, en effet, le meilleur moyen de ne plus s'y retrouver et de commettre des erreurs, notamment des erreurs de destinataires. Celles-ci pourraient avoir pour conséquences de voir des informations confidentielles de votre entreprise vous échapper vers des contacts personnels qui pourraient en faire un mauvais usage, ou à l'inverse de voir un message trop personnel circuler dans votre environnement professionnel alors que vous ne le souhaiteriez pas. Enfin, comme votre messagerie personnelle est généralement bien moins sécurisée que votre messagerie professionnelle, vous faire pirater votre compte pourrait mettre en danger votre entreprise si un cybercriminel accédait à des messages professionnels confidentiels que vous auriez gardés dans votre messagerie personnelle.

3. Ayez une utilisation responsable d'internet au travail

Si l'utilisation d'une connexion Internet professionnelle à des fins personnelles est tolérée, il est important d'avoir à l'esprit que votre utilisation peut mettre en cause votre entreprise qui pourra se retourner contre vous si vous commettiez des actes répréhensibles comme du téléchargement illégal, de l'atteinte au droit d'auteur ou si vous publiez des propos qui pourraient être condamnables. De plus, vous devez avoir à l'esprit que votre entreprise est en droit de contrôler votre utilisation de la connexion qu'elle met à votre disposition. N'utilisez donc pas votre connexion professionnelle pour des choses qui n'ont, selon vous, pas à être connues de votre entreprise.

4. Maîtrisez vos propos sur les réseaux sociaux

L'affichage du contenu tiers "dailymotion" a été bloqué conformément à vos préférences.

Quand vous parlez de votre travail ou de la vie de votre entreprise (ambiance, nouveaux projets…) sur les réseaux sociaux, même si vos propos ne sont pas négatifs, vous ne contrôlez pas vos lecteurs :

la rediffusion ou l'interprétation qu'ils peuvent faire de vos informations pourraient nuire à votre entreprise. À l'inverse, et pour les mêmes raisons, vous n'avez pas forcément envie que certains propos que vous pouvez tenir sur les réseaux sociaux et qui concernent votre vie privée puissent être connus de votre entreprise. Sur les réseaux sociaux, veillez ainsi à séparer vos usages pro-perso : verrouillez votre profil pour que tout ne soit pas public et avant de poster, demandez-vous toujours si ce que vous communiquez ne pourra pas vous porter préjudice, ou à votre entreprise, si d'aventure vos propos ou messages étaient relayés par une personne malintentionnée.

5. Usages pro-perso : N'utilisez pas de services de stockage en ligne personnel à des fins professionnelles

Ou du moins pas sans l'autorisation de votre employeur et sans avoir pris les mesures de sécurité qui s'imposent. Ces services de stockage en ligne d'informations (*Cloud* en anglais) généralement gratuits pour les particuliers sont certes pratiques, mais d'un niveau de sécurité qui ne se prête pas forcément aux exigences des entreprises pour protéger leurs informations. Ils ne sont pas conçus pour cela. Pour les besoins des entreprises, il existe des solutions professionnelles et sécurisées.
L'utilisation d'un service de stockage en ligne personnel pour des usages professionnels pourrait mettre en danger votre entreprise si votre compte d'accès à ce service était piraté alors qu'il contenait des informations confidentielles.

6. Faites les mises à jour de sécurité de vos équipements

Sur vos moyens informatiques personnels (ordinateur, téléphone, tablette), mais également sur vos moyens professionnels si cela relève de votre responsabilité, il est important d'installer sans tarder les mises à jour dès qu'elles sont publiées. Elles corrigent souvent des failles de sécurité qui pourraient être exploitées par des cybercriminels pour prendre le contrôle de votre appareil et accéder à vos informations ou à celles de votre entreprise.

7. Utilisez une solution de sécurité contre les virus et autres attaques

Sur vos moyens informatiques personnels (ordinateur, téléphone, tablette), mais également sur vos moyens professionnels si cela relève de votre responsabilité, utilisez une solution antivirus et tenez-la à jour. Même si aucune solution n'est totalement infaillible, de nombreux produits peuvent vous aider à vous protéger des différentes attaques que peuvent subir vos équipements comme les virus, les rançongiciels (*ransomware*), l'hameçonnage (*phishing*)… Si un cybercriminel prenait le contrôle de vos équipements personnels, il pourrait accéder à toutes vos informations, mais aussi au réseau de votre entreprise si vous vous y connectez avec ce matériel.

8. Usages pro-perso : N'installez les applications que depuis les sites ou magasins officiels

Que ce soit pour vos usages personnels ou professionnels si cela relève de votre responsabilité, et même s'ils ne sont pas infaillibles, seuls les sites ou magasins officiels vous permettent de vous assurer au mieux que les applications que vous installez ne sont pas piégées par un virus qui permettrait à un cybercriminel de prendre le contrôle de votre équipement.
Méfiez-vous des sites « parallèles » qui ne contrôlent pas les applications qu'ils proposent ou qui offrent gratuitement des applications normalement payantes en téléchargement illégal : elles sont généralement piégées. Consultez le nombre de téléchargements et les avis des autres utilisateurs avant d'installer une nouvelle application. Au moindre doute, ne l'installez pas et choisissez-en une autre.

9. Méfiez-vous des supports USB

Vous trouvez ou on vous offre une clé USB (ou tout autre support à connecter). Partez du principe qu'elle est piégée et que même les plus grands spécialistes pourraient avoir du mal à s'en apercevoir.

Ne la branchez jamais sur vos moyens informatiques personnels et encore moins sur vos moyens informatiques professionnels au risque de les compromettre en ouvrant un accès à un cybercriminel. Utilisez une clé USB pour vos usages personnels et une autre pour vos usages professionnels afin d'éviter que la compromission de l'une ne puisse infecter l'autre.

10. Usages pro-perso : Évitez les réseaux Wi-Fi publics ou inconnus

L'affichage du contenu tiers "dailymotion" a été bloqué conformément à vos préférences.

Ces réseaux peuvent être contrôlés par des cybercriminels qui peuvent intercepter vos connexions et ainsi récupérer au passage vos comptes d'accès et vos mots de passe personnels ou professionnels, vos messages, vos documents ou même vos données de carte bancaire… afin d'en faire un usage délictueux. Depuis un réseau Wi-Fi public ou inconnu, n'échangez jamais d'informations confidentielles.

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/piratage-systeme-informatique-pro

Piratage d'un système informatique professionnel, que faire ?

L'intrusion dans un système informatique (serveur, réseau…) se définit comme l'accès illicite à ce système par un cybercriminel, ce qui peut entraîner le vol, voire la perte totale, des informations du système touché. Que faire en cas de piratage d'un système informatique ? Confiner les équipements concernés, préserver les preuves, identifier les origines de l'intrusion, déposer plainte, signaler à la CNIL…

1. En quoi consiste le piratage d'un système informatique professionnel ?

Un système informatique (ou système d'information) désigne tout appareil, équipement ou ensemble de ces matériels, permettant de traiter et stocker des données. L'intrusion dans un système informatique se définit comme l'accès non autorisé à ce système par un tiers. Cela peut concerner un ordinateur, un appareil mobile, un objet connecté, un serveur ou le réseau d'une organisation. En pratique, les pirates peuvent recourir à différentes méthodes pour s'introduire dans un système informatique comme l'utilisation d'une faille de sécurité ; la mauvaise configuration d'un logiciel ou d'un équipement ; l'infection par un logiciel malveillant (virus informatiques) ; la récupération d'identifiants de connexion par le biais d'un appel ou d'un message frauduleux (hameçonnage) ; etc. L'origine de l'intrusion peut être interne (un collaborateur mécontent ou négligeant ou bien encore un prestataire) ou bien externe (cybercriminels). Par la suite, le cybercriminel peut chercher à se propager dans les autres équipements du réseau attaqué. Le piratage d'un système informatique peut donc être d'une grande gravité pour l'organisation qui en est victime puisqu'elle peut entraîner le vol, voire la perte totale, des informations du système touché.

Le piratage d'un système informatique vise à prendre le contrôle ou utiliser les ressources d'un appareil ou d'un équipement pour en faire un usage frauduleux : gain d'argent, espionnage, sabotage, revendication, chantage ou vandalisme.

2. Comment assurer la protection de mon système informatique ?

- Utilisez, paramétrez et mettez à jour régulièrement votre antivirus et les équipements de sécurité de votre système informatique (pare-feu, etc.).
- Mettez à jour régulièrement les appareils, les systèmes d'exploitation ainsi que les logiciels installés de vos équipements.
- N'installez pas de logiciels, programmes, applications ou équipements « piratés » ou dont l'origine ou la réputation est douteuse.

- N'utilisez les comptes administrateurs qu'en cas de nécessité.
  - Limitez les privilèges et les droits des utilisateurs au strict nécessaire.
  - Vérifiez régulièrement les fichiers de journalisation de vos équipements afin d'identifier toute activité inhabituelle.
- Utilisez des mots de passe suffisamment complexes et changez-les au moindre doute.
  - Faites des sauvegardes régulières et déconnectées de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine au besoin.
  - N'ouvrez pas les messages suspects, leurs pièces jointes et ne cliquez pas sur les liens provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu mais dont le contenu est inhabituel ou vide.

3. Victime du piratage d'un système informatique, que faire ?

1. **Confinez, déconnectez du réseau et mettez en quarantaine les postes ou équipements informatiques concernés par l'incident**. Coupez tous les accès réseaux pour stopper l'incident. De même, écartez et conservez les supports informatiques concernés par l'incident (clefs USB, disques durs, CD, DVD, etc.).

2. **Identifiez les origines possibles de l'intrusion** au niveau des équipements touchés par l'attaque et prenez les mesures nécessaires pour qu'elle ne puisse pas se reproduire. L'intrusion peut, par exemple, provenir du piratage d'un de vos comptes d'administration suite à un message d'hameçonnage ou d'identifiants de connexion trop faibles, ou encore, par l'utilisation d'un mot de passe par défaut qui n'aurait pas été changé. Elle peut également être la résultante de l'ouverture d'une pièce jointe, d'un clic sur un lien malveillant contenu dans un message (mail) ou bien encore de la navigation sur un site malveillant. Il peut également s'agir d'un logiciel ou d'un équipement non mis à jour d'une faille de sécurité qui aurait été utilisée par des cybercriminels. Cela peut également provenir d'une mauvaise configuration de l'équipement touché (port serveur non fermé ou peu sécurisé, mots de passe trop simples, etc.), etc. Enfin, si l'origine de l'intrusion est interne, identifiez les personnes ayant accès aux données et aux équipements concernés.

3. **Identifiez toute activité inhabituelle** au sein de votre système informatique. Ces activités inhabituelles peuvent être de différentes natures : création de comptes administrateurs, ajout d'un fichier dans le système, lancement et/ou exécution de programmes ou de processus inconnus, existence d'une activité réseau inhabituelle ou inconnue, modification suspecte du registre Windows, etc.

4. **Évaluez et vérifiez l'étendue de l'intrusion** à d'autres appareils ou équipements de votre système informatique. Par ailleurs, mesurez les dégâts causés et identifiez les éventuelles informations perdues ou compromises.

5. **Récupérez les fichiers de journalisation** (logs) de vos pare-feux, des serveurs mandataires (proxys), des postes ou serveurs touchés qui seront des éléments d'investigation. Ces éléments peuvent permettre d'obtenir des « traces » du cybercriminel dans le cadre de l'analyse de l'attaque. Ils peuvent également constituer des preuves à valeur juridique en cas de procédures ultérieures.

6. **Réalisez une copie complète** (copie physique) de la machine attaquée et de sa mémoire. Effectuez la même opération sur tous les équipements qui ont été touchés. Si vous n'êtes pas en mesure de réaliser une copie physique des équipements touchés, conserver leurs disques durs à disposition des enquêteurs car ils seront utiles pour leurs investigations.

7. En parallèle de vos investigations techniques, **déposez plainte** au commissariat de police ou à la brigade de gendarmerie ou encore par écrit au procureur de la République du tribunal judiciaire dont vous dépendez. Tenez à disposition des enquêteurs tous les éléments de preuves techniques en votre possession. Il est important de garder à l'esprit que le dépôt de plainte doit intervenir avant la réinstallation des appareils touchés, de manière à conserver les preuves techniques de l'incident et pouvoir les fournir aux enquêteurs.

8. **Réalisez une analyse antivirale complète (scan)** des équipements touchés avec votre antivirus afin de vérifier qu'ils ne sont pas confrontés à un virus informatique. Au préalable, n'oubliez pas de mettre à jour votre antivirus. Si votre antivirus a détecté des logiciels malveillants sur vos appareils, il vous proposera de les « mettre en quarantaine », c'est-à-dire de les empêcher d'agir, ou mieux, de les supprimer directement lorsque cela est possible. Redémarrez vos équipements après cette opération.

9. **Supprimez les fichiers malveillants** installés par le cybercriminel si l'antivirus ne les a pas détectés et que vous en avez découvert, ainsi que les accès aux comptes impliqués dans l'incident.

10. **Réinstallez le système** à partir de sauvegardes antérieures à l'incident et réputées saines.

11. **Changez au plus vite tous les mots de passe** d'accès aux équipements suspectés touchés. Modifiez également tous les mots de passe des utilisateurs ayant accès au système et qui ont pu être compromis.

12. Après la réinstallation de votre système et avant de le remettre en service, **mettez à jour l'ensemble de vos logiciels et de vos équipements** au plus vite pour sécuriser votre système informatique et éviter une nouvelle intrusion. Appliquer les mises à jour de sécurité est indispensable si le cybercriminel a utilisé une faille de sécurité connue.

13. En cas de violation de données à caractère personnel et selon les risques pour les personnes dont les données ont été compromises, **vous pourriez être dans l'obligation de notifier l'incident à la CNIL**. Vous devrez notamment préciser :
– la nature de la violation,
– les catégories et le nombre approximatif de personnes concernées par la violation,
– les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés,
– les conséquences probables de la violation de données,
– les mesures prises ou que vous envisagez de prendre pour éviter que cet incident se reproduise ou atténuer les éventuelles conséquences négatives.

14. **Faites-vous assister au besoin par des professionnels qualifiés**. Vous trouverez sur www.cybermalveillance.gouv.fr des professionnels en cybersécurité susceptibles de vous apporter leur assistance technique.