CONCOURS EXTERNE, INTERNE ET DE 3ème VOIE DE TECHNICIEN PRINCIPAL TERRITORIAL DE 2ème CLASSE

SESSION 2018

ÉPREUVE DE RAPPORT AVEC PROPOSITIONS OPÉRATIONNELLES

ÉPREUVE D'ADMISSIBILITÉ :

La rédaction d'un rapport technique portant sur la spécialité au titre de laquelle le candidat concourt. Ce rapport est assorti de propositions opérationnelles.

Durée : 3 heures
Coefficient : 1

SPÉCIALITÉ : INGÉNIERIE, INFORMATIQUE ET SYSTÈMES D'INFORMATION

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni initiales, ni votre numéro de convocation, ni le nom de votre collectivité employeur, de la commune où vous résidez ou du lieu de la salle d'examen où vous composez, ni nom de collectivité fictif non indiqué dans le sujet, ni signature ou paraphe.
- Sauf consignes particulières figurant dans le sujet, vous devez impérativement utiliser une seule et même couleur non effaçable pour écrire et/ou souligner. Seule l'encre noire ou l'encre bleue est autorisée. L'utilisation de plus d'une couleur, d'une couleur non autorisée, d'un surligneur pourra être considérée comme un signe distinctif.
- L'utilisation d'une calculatrice de fonctionnement autonome et sans imprimante est autorisée.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 22 pages.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.

S'il est incomplet, en avertir le surveillant.

Vous êtes technicien principal territorial de 2ème classe, responsable de la sécurité des systèmes d'information (R.S.S.I.), au sein de la direction des systèmes d'information de la ville Techniville (50 000 habitants).

Dans un premier temps, le directeur des systèmes d'information vous demande de rédiger à son attention, exclusivement à l'aide des documents joints, un rapport technique sur les attaques virales de type « Ransomware ».

10 points

Dans un deuxième temps, il vous demande d'établir un ensemble de propositions opérationnelles permettant une meilleure continuité des services publics en cas d'attaque virale de type " Ransomware ".

10 points

Pour traiter cette seconde partie, vous mobiliserez également vos connaissances

Liste des documents :

Document 1 : **Une cyberattaque massive bloque des ordinateurs dans des dizaines de pays.**
lemonde.fr - Nathalie Guibert, Damien Leloup et Philippe Bernard - Mai 2017.
(3 pages)

Document 2 : **Plus agressif, le Ransomware Petya gagne aussi en efficacité.**
Le monde informatique - George Nott - Juin 2017.
(1 page)

Document 3 : **Le Ransomware, le nouveau fléau des ordinateurs ?**
Le monde de l'informatique - Stéphane Manhes - Décembre 2016.
(3 pages)

Document 4 : **Attaque WannaCry via SMB et Jaff par email.**
altospam.com - Stéphane Manhes - Mai 2017.
(1 page)

Document 5 : **Comment fonctionne un "Ransomware", virus à l'origine des dernières cyberattaques.**
huffingtonpost.fr - Jade Toussay / Gregory Rosière - Juin 2017.
(2 pages)

Document 6 : **Le "Rançongiciel", fléau international en pleine expansion** (extrait)**.**
lagazettedescommunes.com - Pierre-Alexandre Conte - Février 2017.
(1 page)

Document 7 : **L'expérience traumatisante d'une commune piratée.**
lagazettedescommunes.com - Pierre-Alexandre Conte - Février 2017.
(1 page)

Document 8 : **Inculquer le virus de la sécurité informatique.**
Club Techni.Cités - Emmanuelle Lesquel - Février 2017.
(2 pages)

Document 9 : **Guide d'hygiène informatique Version 2.0.**
ssi.gouv.fr - anssi - Septembre 2017.
(1 page)

Document 10 : **Cyberattaque mondiale : cinq choses que vous devez absolument savoir.**
L'union - Juin 2017.
(2 pages)

Document 11 : **Ce que le RGPD dit à propos des ransomware.**
business.f-secure.com - Olivier QUINIOUT - Août 2017
(2 pages)

Certains documents peuvent comporter des renvois à des notes ou à des documents non fournis car non indispensables à la compréhension du sujet.

DOCUMENT 1

Une cyberattaque massive bloque des ordinateurs dans des dizaines de pays.

lemonde.fr - Nathalie Guibert, Damien Leloup et Philippe Bernard - Mai 2017.

Les attaques ont notamment perturbé les hôpitaux britanniques, le ministère de l'intérieur russe et le constructeur automobile français Renault.

Les « rançongiciels » bloquent l'accès aux données d'un ordinateur, tant qu'une rançon n'est pas payée.

Royaume-Uni, Russie, Espagne, Portugal, France, Mexique… Vendredi 12 mai, des dizaines de milliers d'ordinateurs, dans au moins 99 pays, ont été infectés par un logiciel malveillant bloquant leur utilisation, dans ce qui semble être l'une des plus importantes campagnes de diffusion d'un logiciel de ce type depuis des années.

Outre-Manche, c'est le système de santé qui a été largement perturbé par ce virus informatique. Examens médicaux annulés ou perturbés, communications téléphoniques affectées, accès aux données bloqués… le Service national de santé (NHS) britannique, qui englobe médecins de ville, hôpitaux et ambulances, a été largement déstabilisé vendredi après-midi par ce logiciel qui prend en otage les usagers des ordinateurs en bloquant l'accès à leurs fichiers.

« Oups, vos fichiers ont été encodés », signale l'écran parasite, qui exige le paiement de 300 dollars (275 euros) sous peine d'effacement des contenus. Selon le NHS, qui a ouvert une enquête, l'attaquant a utilisé WannaCry, un virus de type « ransomware » (« rançongiciel ») qui se diffuse par le biais des courriels mais qui n'aurait pas pu accéder aux données personnelles des patients.

L'attaque aurait été renforcée par l'utilisation d'Eternal Blue, un outil de piratage mis au point par les services de renseignement américains et qui aurait été volé à l'Agence nationale de sécurité (NSA), affirme le quotidien britannique Financial Times. Il facilite la dissémination du virus à travers les systèmes de partage de fichiers couramment utilisés par les entreprises et les administrations.

NHS Digital, la structure qui centralise les usages médicaux de l'informatique par le système public de santé britannique, assure que le NHS n'était pas spécifiquement ciblé. Le centre national britannique de cybersécurité, une branche du Government Communications Headquarters, l'équivalent britannique de la NSA, a été mis en alerte.

Le ministère russe de l'intérieur affecté

Le NHS n'a pas été la seule cible touchée par les pirates. La première ministre britannique, Theresa May, a déclaré dans la soirée que la cyberattaque contre le service public de santé était « une attaque internationale » touchant « plusieurs pays et organisations ».

Ainsi, Telefonica, le géant espagnol des télécommunications, et plusieurs autres entreprises du pays ont été victimes d'un virus similaire. « L'attaque a touché ponctuellement des équipements informatiques de travailleurs de différentes entreprises » et « n'affecte donc pas la prestation de services, ni l'exploitation des réseaux, ni l'usager de ces services », a assuré le ministère de l'énergie.

Le Centre cryptologique national espagnol – la division des services de renseignement chargée de la sécurité des technologies de l'information – a évoqué une «attaque massive de ransomware» qui «touche les systèmes Windows en cryptant tous leurs fichiers et ceux des réseaux en partage».

Des opérateurs téléphoniques portugais et l'entreprise américaine de livraison FedEx ont également été touchés, de même que le ministère de l'intérieur russe, qui a indiqué, vendredi soir, que ses ordinateurs avaient été la cible d'une « attaque virale ».

L'attaque, à ce stade, semble d'ampleur limitée en France, mais le secrétariat général pour la défense et la sécurité nationale estime qu'il n'y a aucune raison que le pays soit épargné. Pour les autorités, la nouveauté tient dans la très forte capacité de propagation du logiciel malveillant, en dépit des correctifs déjà apportés par Microsoft en mars.

Outre le constructeur automobile Renault, le ministère de l'éducation nationale a été touché. Le ministère de la défense n'a pas repéré de problème et a pris des mesures dans la nuit de vendredi à samedi pour mettre à jour ses passerelles en fonction du virus, notamment au sein du service de santé des armées.

L'Agence nationale de sécurité des systèmes d'information diffuse des messages de bonnes pratiques. Le rendez-vous de lundi matin sera un test, dans les entreprises et les administrations, quand les personnels reprendront le travail. Selon la police française, plus de 75 000 ordinateurs ont été infectés dans le monde et ce nombre « devrait très vraisemblablement s'alourdir dans les jours qui viennent ». Cela en fait déjà la plus importante diffusion d'un logiciel de ce type de l'histoire.

Failles dites « zero day »

D'après les premières constatations des experts, ce logiciel malveillant tire parti d'une faille de sécurité informatique, dont l'existence a été révélée à la mi-avril par un mystérieux groupe se faisant appeler The Shadow Brokers. Celui-ci avait rendu publique une série d'outils de piratage présentés comme faisant partie de l'arsenal de la NSA. La faille en question a été depuis corrigée par Microsoft, mais les ordinateurs dont le système d'exploitation n'est pas à jour restent vulnérables.

Edward Snowden, le lanceur d'alerte qui avait révélé l'existence des programmes secrets de surveillance du Web de la NSA, a estimé que l'agence américaine avait une importante part de responsabilité dans la diffusion de ce virus. « S'ils avaient révélé l'existence de cette faille de sécurité lorsqu'ils l'ont découverte, (...) tout cela ne serait pas arrivé », écrit-il sur son compte Twitter.

La NSA, comme d'autres agences de renseignement dans le monde, conserve généralement pour son propre usage les failles de sécurité que ses experts découvrent, ce qui lui permet de mener des piratages offensifs. Une pratique dénoncée par de nombreux experts en sécurité informatique, qui estiment que ces failles dites « zero day » – qui n'ont encore jamais été découvertes – doivent être corrigées dès leur découverte, car elles sont une source de danger pour tous les utilisateurs.

Lire aussi : Entre les Etats-Unis et la Russie, des relents de guerre froide dans le cyberespace

Fragilités britanniques

Cette problématique est particulièrement cruciale pour les ordinateurs équipés de Windows XP – un système d'exploitation ancien, pour lequel Microsoft ne propose plus de mises à jour mais qui équipe encore de nombreux ordinateurs. Notamment au sein du NHS britannique, comme dans d'autres administrations.

Au Royaume-Uni, le choc est particulièrement ressenti parce que le NHS est une institution très populaire, une source de fierté et un sujet ultrasensible du débat politique, en particulier dans la campagne actuelle pour les élections législatives, prévues le 8 juin. Cette administration tentaculaire, soumise à l'austérité budgétaire, souffre de faiblesses, notamment au niveau de son gigantesque système informatique, déjà visé par des attaques.

Dans un article publié le 10 mai par le prestigieux British Medical Journal, Krishna Chinthapalli, un neurologue exerçant dans un hôpital londonien, écrivait : « Nous devons nous préparer. D'autres hôpitaux vont presque certainement être paralysés par des "rançongiciels" cette année. » En 2016, quatre établissements hospitaliers anglais avaient déjà été paralysés plusieurs jours par un logiciel de ce type.

Selon ce médecin, les hôpitaux constituent des « cibles idéales » pour les maîtres chanteurs car ils détiennent des données uniques et sont « plus enclins » que d'autres institutions à payer pour récupérer rapidement leurs données. Krishna Chinthapalli rapporte qu'une attaque similaire a aussi visé un hôpital de Los Angeles l'an dernier. Une rançon de 3,4 millions de dollars avait été exigée. Selon des informations démenties par l'établissement, ce dernier a dû acquitter la somme de 17 000 dollars pour récupérer les données de ses patients.

Des logiciels prisés des réseaux criminels

Les rançongiciels ont connu un développement exponentiel ces trois dernières années. Ils sont généralement conçus par des groupes criminels, et touchent le plus souvent les petites et moyennes entreprises, auxquelles ils extorquent des sommes variant entre quelques dizaines et quelques centaines d'euros par machine infectée – le paiement s'effectue en bitcoins, une monnaie virtuelle anonyme.

La plupart des victimes ne portent pas plainte. « Les entreprises pensent qu'en portant plainte elles terniront leur image et ne récupéreront pas nécessairement leurs données. Elles pensent aussi que payer la rançon coûtera moins cher que de payer une entreprise pour nettoyer leurs réseaux informatiques et installer des protections plus solides », regrettait, en 2016, dans un entretien au Monde, le commissaire François-Xavier Masson, chef de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.

L'ampleur et la rapidité de diffusion de ce nouveau rançongiciel ont cependant accru l'inquiétude des services de sécurité. Pour l'instant, rien ne permet de lier ce logiciel malveillant à un acteur étatique, et l'hypothèse d'un acte criminel classique, mené par des personnes ayant exploité les failles dévoilées par The Shadow Brokers, est la piste la plus logique. Mais dans un contexte marqué par plusieurs piratages d'ampleur, dont la publication, à la veille du deuxième tour de la présidentielle française, de courriels piratés de la campagne d'Emmanuel Macron, les services de sécurité informatique des pays les plus touchés mènent l'enquête.

En France, des mesures de sécurité ont été prises, notamment pour protéger le réseau des hôpitaux militaires. Les services gouvernementaux restent prudents, car il faudra du temps pour analyser le logiciel et sa diffusion, pour savoir s'il visait des organisations spécifiques, comme l'affirme Mme May, ou si sa prolifération était opportuniste. Et il en faudra encore plus pour espérer retrouver ses concepteurs.

DOCUMENT 2

Plus agressif, le ransomware Petya gagne aussi en efficacité.

Le monde informatique - George Nott - Juin 2017.

Les entreprises du monde entier ont été victimes d'une nouvelle attaque de ransomware exploitant la vulnérabilité Eternal Blue déjà utilisée par les pirates lors de la précédente infection à grande échelle WannaCry.

Le spécialiste en sécurité Dr Web a expliqué de façon très détaillée le mode opératoire de Petya.

Selon les experts en sécurité informatique de McAfee, le ransomware baptisé NotPeya est une « très méchante variante qui crypte les fichiers et la zone d'amorce MBR de l'ordinateur, rendant la machine inutilisable ». Alors que l'attaque de WannaCry, il y a quelques semaines, avait incité de nombreux utilisateurs à appliquer les derniers correctifs de Windows pour se protéger, NotPetya s'est doté « d'un nombre de mécanismes de diffusion encore plus importants pour réussir son attaque », a ajouté McAfee. Selon le spécialiste de la sécurité Symantec, NotPetya, une variante de Petya, se propage comme WannaCry en exploitant la vulnérabilité MS15-010 par SMB, également connue sous le nom Eternal Blue.

Comme l'indique Dr Web dans un communiqué, « la propagation massive du ransomware Trojan.Encoder.12544 a commencé dans la première moitié de la journée du 27.06.2017. Lors de son démarrage sur un ordinateur attaqué, le ransomware utilise plusieurs moyens pour trouver des PC accessibles dans le réseau local, puis selon une liste d'adresses IP reçue, commence à scanner les ports 445 et 139. Après avoir détecté dans le réseau les machines sur lesquelles ces ports sont ouverts, Trojan.Encoder.12544 tente de les infecter à l'aide de la vulnérabilité largement connue du protocole SMB (MS17-10) ».

Une méthode d'infection très efficace

Créée par la NSA, l'agence de sécurité nationale américaine, la vulnérabilité Eternal Blue a été rendue publique par le groupe de pirates Shadow Brokers en avril 2017. « Le ransomware NotPetya est à nouveau impliqué dans une attaque mondiale dévastatrice dont les dégâts pourraient dépasser ceux de WannaCry », a déclaré Kobi Ben Naim, directeur senior de la cyber recherche chez CyberArk Labs. « NotPetya se répand en utilisant une méthode d'infection terriblement efficace utilisée par WannaCry. L'attaque s'appuie sur un ver qui répand rapidement le ransomware en utilisant la vulnérabilité SMB dans les systèmes Microsoft. La combinaison est puissante et les dégâts massifs pourraient atteindre un niveau jamais connu auparavant ».

Les chercheurs de CyberArk Labs ont révélé que NotPetya avait besoin d'acquérir des droits d'administration pour fonctionner. Par conséquent, si un utilisateur clique sur un lien diffusé lors de la campagne de phishing, le ransomware pourra encore infecter le réseau. « En plus de l'application des correctifs, les entreprises doivent impérativement protéger leurs identifiants et renforcer leurs privilèges d'accès aux points d'extrémités afin d'éviter qu'ils ne soient détournés pour exécuter cette attaque », a ajouté Kobi Ben Naim. Enfin, le cabinet de sécurité informatique ESET vient de déclarer que le paiement de la rançon par courrier électronique n'était plus possible, car l'adresse de messagerie pour envoyer l'identifiant du portefeuille Bitcoin et la « clé d'installation personnelle » a été bloquée par le fournisseur.

DOCUMENT 3

Le Ransomware, le nouveau fléau des ordinateurs ?

Le monde de l'informatique - Stéphane Manhes - Décembre 2016.

L'arrivée d'internet a été une révolution pour tout le monde. Les moyens de communication sont devenus plus faciles, notamment grâce aux réseaux sociaux tandis que les démarches administratives ont gagné en simplicité. Seulement, internet n'a pas apporté que des bénéfices. En effet, internet a aussi été l'occasion de créer toutes sortes de virus infectant les ordinateurs. Certains virus sont assez banals et ne posent que peu de problèmes tandis que d'autres sont redoutables et peuvent causer des dégâts irréversibles à vos ordinateurs. Dans ce cas, il faut savoir se prémunir de ces logiciels malveillants et surtout bien faire la différence entre de vraies ou fausses recommandations. Parmi ces virus, il y a le ransomware, également connu sous le nom de rançongiciel ou logiciel de rançon. Mais quel est ce type de virus exactement ? Est-il plus agressif que d'autres ? Et comment faire pour éviter de recevoir des ransomwares ?

Qu'est-ce qu'un ransomware ?

Le domaine des virus informatiques ne cesse d'évoluer. Chaque année de nouveaux virus apparaissent, toujours plus agressifs et difficiles à contrer. Les ransomwares ne sont pas vraiment nouveaux puisque le tout premier a fait son apparition en 1989. Toutefois, depuis quelques années, on note une recrudescence des ransomwares. À ce propos, un célèbre éditeur de logiciels de sécurité a dévoilé qu'au second trimestre 2012, pas moins de 120 000 nouveaux ransomwares avaient été enregistrés. Ce chiffre est tout de même quatre fois supérieur par rapport à l'année précédente à la même période. Et cela ne va pas en s'arrangeant puisqu'en septembre 2016, le taux de virus était de 26,45 % alors qu'entre 2008 et 2013, ce chiffre stagnait aux alentours de 0,34 %. Parmi ces données chiffrées, on retrouve énormément de ransomwares.

Mais quel est ce virus exactement ? Un ransomware est un logiciel malveillant qui va prendre en otage votre ordinateur ou certaines de vos données en les chiffrant. Ensuite, vous recevrez un message d'alerte vous demandant de payer une rançon, d'où le nom de ce virus, afin de pouvoir recevoir la clé permettant de décrypter vos données. Si, à l'époque les ransomwares n'étaient pas spécialement perfectionnés et plutôt simples à contrer, l'évolution technologique a permis d'en façonner des plus coriaces provenant de Russie, d'Allemagne ou des États-Unis, entre autres.

Le fonctionnement d'un ransomware est à peu près similaire à un cheval de Troie et le but est d'extorquer de l'argent à l'utilisateur de l'ordinateur. Certains ransomwares sont tellement bien construits que beaucoup de personnes « tombent dans le panneau » et payent la rançon demandée. Les paiements sont généralement faits par virements bancaires, sous la forme de SMS surtaxés ou encore via des plateformes de paiements telles que Paypal.

Les différentes formes de ransomwares

La particularité des ransomwares est qu'ils évoluent et se renouvellent constamment. De plus, ils peuvent revêtir différentes formes pour tromper les utilisateurs. Tout d'abord, il existe le ransomware policier. Ce dernier a fait son apparition en 2011 et vous demande de payer une amende. Soit le ransomware bloque votre ordinateur, soit il bloque votre navigateur internet. Dans les deux cas, un message de l'État, de la police ou de la gendarmerie nationale s'affiche au démarrage de votre ordinateur et vous demande de régulariser une amende impayée afin de récupérer l'accès à votre PC.

Il y a aussi les crypto-ransomwares. Ces derniers chiffrent certaines données de votre ordinateur et vous réclament une rançon pour pouvoir obtenir une clé de déchiffrage. La difficulté avec ce ransomware est que lorsque les données ont été chiffrées, il est impossible de les décrypter et donc de les récupérer. À la fin de l'année 2015 ainsi qu'en janvier 2016, une grande campagne de crypto-ransomwares a été déployée via des emails contenant des pièces

jointes en .zip ou avec un document Word. Bien évidemment, ces pièces jointes ne doivent surtout pas être ouvertes sous peine d'installer, contre votre volonté, le virus qui va automatiquement chiffrer vos données.

Aux mois de mars, avril et mai 2016, un tout nouveau type de crypto-ransomware est né. Celui-ci chiffre tous vos documents possédant une extension en .crypt. Le dernier type de ransomware est celui qui bloque totalement l'accès à votre ordinateur et vous demande de cliquer sur des publicités. Ce ransomware ne semble pas trop nuisible, cela dit, l'auteur du virus reçoit de l'argent à chaque clic effectué sur la publicité en question.

Comme vous l'aurez compris, tout le monde est susceptible d'être attaqué, un jour ou l'autre, par un ransomware. Il est donc nécessaire de prendre diverses précautions.

Comment se prémunir face aux ransomwares ?

La meilleure façon de lutter contre les ransomwares est de prévenir plutôt que de guérir. En effet, une fois le virus installé sur votre ordinateur, il est particulièrement difficile de s'en débarrasser. Lutter contre les ransomwares se passe en deux étapes : avant d'être infecté et après.

Se prémunir pour ne pas être infecté

Malheureusement, comme expliqué, tout le monde peut être infecté par un ransomware. Par conséquent, vous devrez mettre toutes les chances de votre côté afin d'éviter d'être exposé. La première chose à faire est de réaliser des sauvegardes de l'ensemble du contenu de votre ordinateur. Faites des sauvegardes sur le cloud et même sur une clé USB pour pouvoir retrouver vos données dans le cas où elles seraient irrécupérables suite à l'infection. Ces sauvegardes doivent être faites régulièrement pour ne perdre aucune donnée.

Ensuite, paramétrez correctement votre antivirus. Si vous n'en possédez pas, faites-en l'acquisition au plus vite. C'est une action obligatoire si vous possédez un ordinateur qu'il soit portable ou pas. Par ailleurs, beaucoup de ransomwares se trouvent dans les pièces jointes de certains mails. N'ouvrez jamais un mail si vous ne connaissez pas l'expéditeur et utilisez un service perfectionné de protection des emails comme Altospam.

Si vous êtes un adepte des réseaux sociaux ou des jeux vidéo en ligne, ne cliquez jamais sur un lien même s'il est envoyé par un de vos amis. En effet, ce n'est pas parce que le lien vous est conseillé par un ami qu'il est sûr. Le compte de votre ami a pu, tout simplement, être piraté. À côté de cela, n'oubliez jamais de faire les mises à jour que l'on vous propose, que ce soit pour votre navigateur, vos périphériques, votre antivirus… Les ransomwares aiment bien se glisser là où sont les failles donc fermez-leur les portes de votre ordinateur en faisant toutes les mises à jour dont votre ordinateur a besoin.

Si vous pensez avoir été infecté

Si vous voyez une application ou un logiciel installé sur votre ordinateur alors que vous ne le connaissez pas, désactivez votre connexion internet puis supprimez ce logiciel au plus vite. Le virus n'aura peut-être pas eu le temps de s'être correctement installé et vos données ne seront donc pas en danger.

Si vous avez été infecté

Si vous êtes sûr d'avoir été infecté, notamment parce que vous avez un message affiché à l'écran vous demandant de payer une rançon, dans ce cas, vous disposez de peu d'alternatives. Si vous avez bien sauvegardé vos données sur un périphérique externe, alors ne payez surtout pas la rançon et essayez de contacter la police, car certains commissariats possèdent des experts en cybercriminalité qui pourront traquer l'auteur du ransomware.

Si vos données étaient très importantes pour vous et que vous n'aviez pas effectué de sauvegarde au préalable, dans ce cas c'est à vos risques et périls. Vous pouvez payer la rançon demandée en espérant pour que vos données soient rétablies (mais c'est peu probable). Toutefois, sachez que chaque fois que quelqu'un paye la rançon, c'est comme si vous financiez les prochaines attaques.

Lorsque l'on a été infecté par un ransomware, il n'existe que très peu de solutions pour s'en débarrasser. Vous pouvez nettoyer vous-même votre ordinateur en espérant que le ransomware n'ait pas une version trop expérimentée, essayer des procédures de nettoyage, sinon vous pouvez confier votre ordinateur à un informaticien afin que ce dernier essaie de restaurer vos données.

Depuis quelques années, les ransomwares sont devenus particulièrement agressifs et les attaques nombreuses. Ces dernières sont généralement faites par vague et il est souvent difficile d'en déterminer la provenance et l'auteur. Le mieux est, bien évidemment, de ne pas être infecté donc armez votre ordinateur contre ce fléau, faites des sauvegardes régulièrement et vérifiez votre antivirus. Les ransomwares font partie des cyberattaques les plus dangereuses actuellement, il est très compliqué de s'en débarrasser et de récupérer ses données. N'oubliez pas, sur internet, ne faire confiance en personne. N'ouvrez jamais de mail dont vous ne connaissez pas la provenance et ne cliquez sur aucun lien suspect. Malheureusement, même en prenant toutes ces précautions, vous n'êtes pas à l'abri. En effet, vous pouvez infecter votre ordinateur simplement en allant sur un site internet dont les scripts seraient endommagés. Internet a été l'une des plus grandes révolutions de ces dernières années, mais cela a aussi apporté son lot de contraintes et de dangerosité

DOCUMENT 4

Attaque WannaCry via SMB et Jaff par email.

altospam.com - Stéphane Manhes - Mai 2017.

Selon toute vraisemblance, le virus qui fait tant parler de lui depuis quelques jours ne s'est pas propagé par les emails. Vincent Nguyen, le directeur du CERT de Wavestone, précise que « Tout le monde cherche ce fameux e-mail initial et, en quatre jours, aucune équipe n'est parvenue à mettre la main dessus ». Nous confirmons de notre côté, qu'aucun de nos clients n'a pour l'heure été victime de ce virus et que nos 6 antivirus ne l'ont pas détecté pendant sa période de diffusion.

Il est fort probable que les pirates aient identifié des postes « patients zéro » susceptibles de servir de base à une propagation par l'intermédiaire d'une autoréplication. Ce virus utilise une faille dans le protocole SMB (Server Message Block) de Windows, présente sur les anciens systèmes d'exploitation Microsoft, pourtant corrigée par un patch MS17-010 pour combler cette vulnérabilité. Cela rappelle donc l'importance des mises à jour. Cette attaque, qui a touché plus de 230000 ordinateurs dans plus de 150 pays selon Europol, serait à mettre sur le compte de hackers Nord-Coréens soupçonnés d'appartenir au collectif Lazarus Group.

Cependant, parallèlement, il y a toujours des attaques via la messagerie. Actuellement, Jaff, une variante récente de Locky continue de sévir, créant peut-être une confusion. Ce virus est propagé par l'intermédiaire d'emails contenant des pièces jointes au format PDF. Ce document PDF contient une macro malveillante, par l'intermédiaire d'un script embarqué au format DOCM, lançant le téléchargement et l'exécution du ransomware. L'alerte CERTFR-2017-ALE-011 détaille le mécanisme. Grâce aux 6 antivirus intégrés et au système d'analyse sandboxing statique des PDF (notamment), Altospam bloque parfaitement ces malwares.

Pour se protéger, 4 règles simples sont essentielles : mise à jour, sauvegarde, protection et sensibilisation. L'attaque WannaCry est la preuve que les systèmes d'exploitation (et les logiciels) doivent être mis à jour. Il est primordial de mettre en place des procédures de mises à jour strictes dans les entreprises. De plus, les sauvegardes sont essentielles, à la fois pour corriger l'erreur humaine, mais également pour être en mesure de rétablir un système en cas d'attaque. La protection est liée évidemment aux firewalls, proxy, sécurité du poste utilisateur, mais surtout à la mise en place d'un système de protection de la messagerie performant tel qu'Altospam. Aujourd'hui les attaques par emails restent le principal vecteur de virus car ils permettent d'être très rapide. Dernier point fondamental, la sensibilisation des utilisateurs. Cette attaque très médiatisée aura eu le mérite de jouer ce rôle.

DOCUMENT 5

Comment fonctionne un "Ransomware", virus à l'origine des dernières cyberattaques.

huffingtonpost.fr - Jade Toussay / Gregory Rosière - Juin 2017.

NotPetya et Wannacry ont un point commun: les données piratées ne sont pas volées, mais chiffrées afin d'être inutilisables... à moins de payer une rançon.

PIRATAGE - Bis repetita. Après l'impressionnante cyberattaque Wannacry en mai, un nouveau virus a frappé les entreprises de la planète, notamment en Ukraine et en Russie, ce mardi 27 juin.

Surnommé NotPetya, ce programme utilise le même mode d'attaque que Wannacry et bien d'autres virus, que l'on appelle "ransomware" ou "rançongiciel" en français.

Son mode de fonctionnement? Le logiciel malveillant verrouille et chiffre les fichiers des utilisateurs et les force à payer une rançon allant de centaines à plusieurs milliers de dollars, sous forme de monnaie virtuelle bitcoin.

Pour NotPetya, le virus exhortait les utilisateurs à débourser 300 dollars pour avoir une chance (improbable) de retrouver leurs données. Si tous les experts du secteur déconseillent de payer, NotPetya a déjà accumulé 8000 dollars en moins de 24 heures.

Les attaques de type "ransomware" ont explosé en 2016, confirmant les craintes des experts en cybersécurité. Le HuffPost fait le point sur ce virus d'un nouveau genre, qui affecte aussi bien les multinationales que les particuliers.

D'où vient ce logiciel?

Pour Wannacry comme pour NotPetya, c'est une faille de Windows, dévoilée en avril par le groupe de pirates "Shadow Brokers", qui est utilisée, précise Kaspersky. Celle-ci avait à l'origine été trouvée et gardée secrète par la NSA, l'agence d'espionnage américaine. Ce sont ces "failles" qui permettent aux hackers d'accéder aux contenus de l'ordinateur, avant de les chiffrer (ou d'en faire ce qu'ils veulent).

De manière générale et depuis quelques années également, des hackers proposent sur le dark web des "ransomware" prêts à l'emploi, et donc accessibles à tous. De quoi favoriser l'expansion de ce nouveau mode de piratage, désormais à la portée de tout le monde.

Qui peut être touché?

Absolument tout le monde. Des entités d'Etat aux particuliers, en passant par les collectivités locales ou encore les PME. Ces dernières sont d'ailleurs de plus en plus visées par les pirates, car plus avantageuses que les grosses entreprises.

Les PME "sont bien souvent moins préparées et ont des ressources informatiques plus limitées, ce qui favorise les cyber-attaques", analyse ainsi Laurent Heslault, directeur des stratégies de sécurité Symantec Corporation, dans une tribune publiée sur LeHuffPost. "Bien souvent également, les PME sont ciblées car elles font partie d'une "supply chain" économique permettant aux cyber-attaquants de toucher ou tout du moins de cibler in fine leurs clients ou sous-traitants, qui sont des entreprises de taille supérieure, voire des grands groupes ou même le secteur public. Une fois hackée, la PME se transforme alors en un véritable point d'entrée vers ceux-ci."

Autre "avantage" des PME pour les pirates: la propension de ces entreprises à payer plus rapidement les rançons. Une mise à l'arrêt prolongée entraînerait en effet des pertes bien plus difficiles à gérer que dans une grande entreprise. C'est d'ailleurs ce qui s'est produit

en avril 2016 pour une petite entreprise béarnaise, contrainte de verser "une somme à quatre chiffres", après la prise en otage de ses données pendant cinq jours.

La société Kaspersky Lab estime qu'au premier semestre 2016, une entreprise était visée par une attaque de ce type toutes les deux minutes. Au troisième trimestre, cette estimation s'était réduite à une attaque toutes les 40 secondes.

Comment s'en protéger

Evidemment, les pirates abusent le plus souvent de la naïveté des internautes. Comme le souligne Laurent Heslault, "avoir conscience" de la possibilité de ces cyberattaques est "un premier pas, qui doit être suivi par quelques foulées supplémentaires". Une fois encore donc, mieux vaut éviter de cliquer sur des liens inconnus, ou de télécharger des pièces jointes suspectes.

La mise à jour des systèmes et logiciels antivirus est également cruciale. Il y a quelques mois, Microsoft a ainsi publié un patch de sécurité pour réparer la faille à l'origine des cyberattaques Wannacry et NotPetya. Seul problème, de nombreux systèmes n'ont toujours pas été mis à jour.

C'est donc surtout en amont que les grands groupes informatiques doivent travailler à résoudre les "failles" qui permettent aux hackers de pirater les systèmes, comme l'a souligné Edward Snowden en mai. "Si la NSA avait discuté en privé de cette faille utilisée pour attaquer des hôpitaux quand ils l'ont 'découverte', plutôt que quand elle leur a été volée, ça aurait pu être évitée".

DOCUMENT 6

Le « Rançongiciel », fléau international en pleine expansion (extrait).

lagazettedescommunes.com - Pierre-Alexandre Conte - Février 2017

Extorsion : Tout le monde ou presque a entendu parler de Locky.

Ce « ransomware » – « rançongiciel » en français – s'est rendu populaire en faisant de nombreuses victimes au cours de l'année passée. Une fois activé sur l'ordinateur de la personne visée, ce dernier chiffre les données et demande une somme d'argent en échange de leur restitution. S'il reste l'exemple le plus connu, Locky n'est pas un cas unique. Loin de là.

290 millions de dollars – Le FBI estime que durant le premier trimestre de l'année 2016, environ 209 millions de dollars ont été extorqués par le biais de « rançongiciels ». Aux Etats-Unis, le Hollywood Presbyterian Medical Center a fait partie des victimes au mois de février 2016. Paralysé pendant plus d'une semaine, il avait fini par débourser la somme de 17 000 dollars pour reprendre une activité normale. Et ce, après avoir dû envoyer de nombreux patients vers d'autres établissements.

Une mésaventure similaire est arrivée trois mois plus tard au Kansas Heart Hospital. Mais cette fois, après avoir payé la rançon, l'hôpital n'a pas pu récupérer ses fichiers. Pire, une seconde somme d'argent lui a été demandée. Fin janvier, c'est la police de Washington qui s'est aperçue que le réseau de vidéosurveillance de la ville ne fonctionnait plus correctement. Avant de prendre connaissance du problème : depuis le 12 janvier, un « ransomware » avait commencé à faire son œuvre, paralysant 123 des 187 caméras utilisées. En cherchant la source du dysfonctionnement, des enquêteurs sont tombés un peu plus tard sur un message les invitant à payer une somme.

Ce qui n'a pas été fait. Le réseau a été réinstallé dans l'urgence.

DOCUMENT 7

L’expérience traumatisante d’une commune piratée.

lagazettedescommunes.com - Pierre-Alexandre Conte - Février 2017.

Chaque jour ou presque, des collectivités découvrent qu’elles ont été victimes d’une attaque informatique. Mais difficile de témoigner à visage découvert. Voici ce qu’une victime raconte, sous couvert d’anonymat : « Nous sommes arrivés un matin et nos postes informatiques étaient bloqués, explique cette directrice générale des services. Impossible de travailler dans ces conditions. Sur les écrans était affiché un message énigmatique et surtout, une demande de rançon. »

Si la police a rapidement été prévenue, la commune a dû se résoudre à trouver une solution au plus vite pour reprendre une activité normale. « Nous ne pouvions pas payer la somme, explique-t-elle. Nous avons appelé notre prestataire informatique qui a fait le déplacement et nous a indiqué qu’une grande partie de nos données, notamment les plus récentes, étaient perdues.

Personne n’avait anticipé le problème. Cela a créé beaucoup de remous au sein de la collectivité, dans la mesure où nous ne savons pas qui est responsable de l’attaque. L’enquête est toujours en cours. Plusieurs pistes ont été évoquées, dont des personnes hostiles à certaines décisions locales. C’est une expérience qui reste encore assez traumatisante pour nous. »

Si le prestataire informatique a fourni une solution d’appoint pour que les données soient plus fréquemment sauvegardées, aucun changement en profondeur, en termes de sécurité, n’a été apporté à ce jour.

DOCUMENT 8

Inculquer le virus de la sécurité informatique.

Club Techni.Cités - Emmanuelle Lesquel - Février 2017.

Comment faire en sorte que les agents aient les bons réflexes en matière de sécurité informatique ? Pour répondre à cette question, le conseil départemental de l'Aisne a décidé de proposer, depuis plusieurs années, une sensibilisation largement menée de façon ludique. Une stratégie qui obtient de bons résultats.

Sécurité informatique : comment se protéger ?

L'ouverture d'un seul document malveillant contenu dans un email peut infecter et bloquer tous les ordinateurs et données d'une collectivité. La protection des données informatiques et des systèmes d'information dans leur ensemble nécessitent une participation sans failles de tous les agents.

Pour obtenir cette participation, les mesures de précaution comme la non-ouverture et le signalement d'emails douteux ou des contraintes comme les mots de passe doivent être comprises. Pour inculquer les bons réflexes, le département de l'Aisne a mis en place depuis plusieurs années une sensibilisation importante et régulière, notamment par des méthodes ludiques allant du jeu de l'oie au jeu de rôle, en passant par le jeu concours et le quiz.

Jeu concours

Dès 2009, un premier grand jeu concours sur ce thème a mobilisé 500 agents sur les 1 200 alors connectés au réseau. Pour expliquer les risques et les bons réflexes, la quasi-totalité des agents a pu bénéficier de temps de formation collectifs en salle. Ces formations sont complétées par un outil d'e-learning ludique auquel ils peuvent accéder quand ils le souhaitent.

« Quiz, saynète, ou format vidéo interactif type « motion pictures » ; j'utilise comme support de formation des serious game que j'ai moi-même créés mais je pioche aussi dans des outils très bien faits comme ceux réalisé par la Cnil », détaille Hervé Fortin, responsable sécurité des systèmes d'information (SSI) du département de l'Aisne.

Hervé Fortin estime qu'il faut compter trois ans pour que les comportements deviennent réellement réflexes : « Ensuite, il faut continuer à entretenir ces bons réflexes par des piqûres de rappel régulières. Ce que nous faisons par email et via le magazine interne. Il faut trouver le bon dosage ».

Formation personnelle très professionnelle

Paiement en ligne, réseaux sociaux, ou utilisation d'internet par les enfants, le responsable forme aussi les agents qui le souhaitent aux questions qui les intéressent dans leur vie personnelle : « Par ce biais, qui les interpelle souvent plus qu'une formation sur la sécurité des données sensibles à leur travail, ils sont plus réceptifs. Les bons réflexes acquis chez eux le sont aussi au niveau professionnel ».

Ce mode de sensibilisation semble aujourd'hui porter ses fruits. « Je constate réellement un changement des comportements. Ainsi, très peu d'agents ont ouvert les emails malveillants que nous avons reçus en abondance cet été. Ils étaient pourtant rédigés en bon français et avec des adresses de contacts piratés. Et ceux qui les ont ouverts ont eu les bons réflexes en se coupant du réseau et en nous prévenant », se félicite Hervé Fortin.

3 questions à Hervé Fortin, responsable de la sécurité des systèmes d'information (SSI) du conseil départemental de l'Aisne

Quel est le préalable indispensable pour faire évoluer les mentalités ?

Il s'agit avant tout de mettre en place une charte informatique. La politique générale de sécurité doit être écrite de façon succincte. Elle doit être juridiquement viable sans être trop technique et bien sûr elle doit bénéficier d'un soutien actif de la direction des élus, et des représentants des salariés. Ensuite, les outils peuvent être déployés.

La prévention passe-t-elle avant tout par des outils techniques ou de la sensibilisation ? Mener de front sensibilisation et mise en place des outils techniques est à mon avis la meilleure solution.

Chez nous, les outils techniques sont mis en place depuis longtemps. Nous pouvons donc nous concentrer sur la sensibilisation qui est vraiment essentielle et qui, aujourd'hui, porte ses fruits. Pour aller plus loin, nous allons définir des référents SSI par direction métier (il existe plus de 120 métiers différents au département de l'Aisne). Ils pourront ainsi être mon relais, me signaler les mouvements de personnel ou informer les nouveaux venus de l'existence de la charte et du portail de formation.

Des métiers sont-ils plus exposés que d'autres ?

Tout à fait. Par exemple, j'interviens régulièrement auprès des travailleurs sociaux, souvent à leur demande d'ailleurs, car ils cumulent de nombreux risques : mobilité, gestion de données sensibles, jeunes publics, etc.

DOCUMENT 9

GUIDE D'HYGIÈNE INFORMATIQUE Version 2.0.

ssi.gouv.fr – anssi – Septembre 2017.

Protéger sa messagerie professionnelle

La messagerie est le principal vecteur d'infection du poste de travail, qu'il s'agisse de l'ouverture de pièces jointes contenant un code malveillant ou du clic malencontreux sur un lien redirigeant vers un site lui-même malveillant.

Les utilisateurs doivent être particulièrement sensibilisés à ce sujet : l'expéditeur est-il connu ? Une information de sa part est-elle attendue ? Le lien proposé est-il cohérent avec le sujet évoqué ? En cas de doute, une vérification de l'authenticité du message par un autre canal (téléphone, SMS, etc.) est nécessaire.

Pour se prémunir d'escroqueries (ex : demande de virement frauduleux émanant vraisemblablement d'un dirigeant), des mesures organisationnelles doivent être appliquées strictement.

Par ailleurs, la redirection de messages professionnels vers une messagerie personnelle est à proscrire car cela constitue une fuite irrémédiable d'informations de l'entité. Si nécessaire des moyens maîtrisés et sécurisés pour l'accès distant à la messagerie professionnelle doivent être proposés.

Que l'entité héberge ou fasse héberger son système de messagerie, elle doit s'assurer : de disposer d'un système d'analyse antivirus en amont des boîtes aux lettres des utilisateurs pour prévenir la réception de fichiers infectés ; de l'activation du chiffrement TLS des échanges entre serveurs de messagerie (de l'entité ou publics) ainsi qu'entre les postes utilisateur et les serveurs hébergeant les boîtes aux lettres.

SÉCURISER LE RÉSEAU

Il est souhaitable de ne pas exposer directement les serveurs de boîte aux lettres sur Internet. Dans ce cas, un serveur relai dédié à l'envoi et à la réception des messages doit être mis en place en coupure d'Internet.

Alors que le spam - malveillant ou non - constitue la majorité des courriels échangés sur Internet, le déploiement d'un service anti-spam doit permettre d'éliminer cette source de risques.

Enfin, l'administrateur de messagerie s'assurera de la mise en place des mécanismes de vérification d'authenticité et de la bonne configuration des enregistrements DNS publics liés à son infrastructure de messagerie (MX, SPF, DKIM, DMARC).

DOCUMENT 10

Cyberattaque mondiale : cinq choses que vous devez absolument savoir.

L'union - Juin 2017.

Que s'est-il passé ?

Une vague massive de cyberattaques au ransomware, rappelant le mode opératoire du virus WannaCry en mai, a touché des multinationales et des sociétés et services européens et américains, après avoir frappé en Ukraine et en Russie.

Après avoir obligé mardi le géant pétrolier russe Rosneft à passer sur un serveur de secours et la centrale nucléaire ukrainienne de Tchernobyl à revenir à des mesures manuelles du niveau de radioactivité, le «ransomware» (rançongiciel) Petrwrap causait des pannes informatiques chez le transporteur maritime Maersk, coupait le courant chez le propriétaire des biscuitsLu et Oreo, contraignait des salariés allemands de Nivea à cesser le travail...

Le virus «se répand dans le monde entier, un grand nombre de pays sont affectés», a prévenu sur Twitter Costin Raiu, chercheur du laboratoire russe Kaspersky. Le laboratoire pharmaceutique Merck est devenu sa première victime connue aux Etats-Unis, son système informatique ayant été «compromis».

Que réclament les attaquants ?

Plusieurs entreprises ont fait état d'un virus faisant apparaître une demande de rançon de 300 dollars sur l'écran de leurs ordinateurs.

Quelles sont les conséquences concrètes ?

A cause de cette attaque, ce mardi, les passagers du métro de Kiev ne pouvaient pas payer par carte bancaire, les panneaux d'affichage de l'aéroport de Kiev ne fonctionnaient plus et des banques ukrainiennes devaient mettre en pause certains des services proposés à leurs clients.

Selon la société spécialisée en sécurité informatique Group-IB, «environ 80 entreprises ont été visées» en Russie et en Ukraine. Parmi elles, Rosneft et de grosses banques ukrainiennes, mais aussi Mars, Nivea, Auchan et des structures gouvernementales ukrainiennes. L'assureur français MAIF a communiqué sur Twitter.

Touchée également, la SNCF a réussi à se défendre contre le virus qui ne s'est pas propagé dans le système informatique de l'entreprise ferroviaire. Aucun incident n'a affecté les trains ce mardi soir. La vigilance reste de rigueur !

En France, les sites officiels du groupe Saint-Gobain n'étaient pas accessibles. «Saint-Gobain a fait l'objet d'une cyberattaque. Par mesure de sécurité, afin de protéger nos données nous avons isolé nos systèmes informatiques. C'est en cours de résolution», a déclaré une porte-parole du groupe français de matériaux.

Il est encore «trop tôt» pour connaître l'ampleur des dégâts éventuels, différentes polices au niveau mondial devant d'abord enquêter ensemble, comme cela s'est passé lors de l'attaque causée par le virus Wannacry en mai.

Le parquet de Paris a ouvert une enquête.

En Allemagne, selon la chaîne de télé régionale NDR, «plus rien ne fonctionne au siège» de Beiersdorf, qui fabrique la crème Nivea. De nombreux salariés ont dû rentrer chez eux. D'autres

entreprises allemandes ont été frappées, selon l'Office pour la sécurité des techniques d'information (BSI).

En Suisse, c'est Admeira, principale régie publicitaire de la confédération, qui a indiqué sur twitter avoir été touchée, et son site internet n'était plus accessible.

En Asie, un responsable du Centre d'alerte informatique de l'Inde a affirmé n'avoir encore reçu aucune plainte concernant cette attaque. Mais des consignes vont être données au cas où.

Comment se protéger du virus ?

La menace se propage sous forme de mail incitant à ouvrir un fichier joint. C'est lui qui contient le « ransomware » ou « cryptovirus ».

Le mail qui propage la menace semble légitime, transmis en apparence par une entreprise ou une institution connue. Il faut donc être particulièrement attentif quant à l'émetteur du mail. Si vous ne vous sentez pas concerné par le message, n'ouvrez surtout pas la pièce jointe ! Supprimez directement le courriel.

Il est, par ailleurs, conseillé de bien effectuer les mises à jour de sécurité et de faire des sauvegardes sur des supports non connectés à Internet.

Que se passe-t-il si le fichier est ouvert ?

Ce type de virus comporte un logiciel qui peut compresser vos fichiers et placer un mot de passe sur chacun d'entre eux. Il n'est ensuite plus possible de les décompresser. Vous risquez de perdre l'ensemble des fichiers sur votre ordinateur !

Seul une restauration de sauvegarde permet de revenir à un état de fonctionnement normal.

En cas d'infection, l'Agence nationale de la sécurité des systèmes d'information (Anssi) conseille sur son site de stopper immédiatement toute connexion Internet de l'ordinateur, de ne pas payer la rançon, de restaurer l'ordinateur en réinstallant un système sain, puis de porter plainte.

DOCUMENT 11

Ce que le RGPD dit à propos des ransomware.

business.f-secure.com - Olivier QUINIOUT - Août 2017

Les récentes attaques Petya et WannaCry ont attiré l'attention des entreprises sur le danger que représentent les ransomware. Il semble que l'Union européenne les ait pris en considération lorsqu'a été rédigé le RGPD.

L'entrée en vigueur du RGPD approche à grands pas. Et de nombreuses entreprises s'évertuent désormais à mieux connaître ce nouveau règlement pour s'assurer d'être en conformité avec celui-ci.

Les professionnels déjà familiers du RGPD ont bien compris que l'objectif de l'UE est de fournir aux entreprises un cadre pour mieux gérer les données personnelles collectées auprès des clients. Les organisations doivent mieux sécuriser ces données, et savoir comment réagir au cas où elles en perdraient le contrôle.

L'essentiel ? Éviter les intrusions informatiques, et être en mesure d'intervenir au cas où elles se produiraient.

Le RGPD est un document juridique : il est donc important de bien saisir la définition d'une « violation de données à caractère personnel ». La voici : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.»

Les entreprises ont tendance à assimiler l'expression « violation de données » avec la perte de contrôle d'informations confidentielles. Mais la définition du RGPD est bien plus large. Cette définition inclut notamment les différents incidents de sécurité, comme les infections ransomware.

Qu'implique donc une telle définition pour les entreprises ? Selon Erka Koivunen, CISO chez F-Secure, les organisations ont l'obligation de faire état d'éventuelles infections ransomware auprès des autorités ainsi qu'auprès des clients affectés.

Vous aboutirez rapidement à la conclusion qu'une infection par ransomware (ou par tout autre malware) affectant un nombre important des systèmes centraux liés au traitement des données personnelles constituera un cas de violation des données personnelles au regard du RGPD et entraînera ainsi l'obligation de notification des intrusions prévue dans les articles 33 et 34 , explique Erka.

Les articles 33 et 34 contraignent les organisations à prévenir les autorités et les personnes dont les données personnelles auraient été subtilisées. Toutefois, cela n'est nécessaire que lorsque la violation de données constitue un risque « pour les droits et libertés des personnes physiques. »

Comment l'infection des systèmes d'une entreprise par un ransomware peut-elle affecter les individus si les données stockées les concernant ont été chiffrées (ou rendues inaccessibles) ? Répondre à cette question n'a rien d'aisé et c'est justement le type d'interrogations auxquelles les entreprises doivent être capables de répondre avec le RGPD.

« Si vous en êtes au stade où un ransomware affecte les données privées que vous avez collectées, il ne faudra pas seulement vous inquiéter de la fuite de ces données (comme c'est souvent le cas). Vous devrez aussi récupérer le contrôle de vos systèmes et données pour rétablir vos opérations. Si vous ne disposez pas de sauvegardes de qualité, les efforts que vous devrez réaliser exigeront une énergie colossale », explique Hannes Saarinen, Privacy Officer chez F-Secure. « Si vous n'êtes pas préparé et si vous avez besoin de collecter

à nouveau toutes vos données, vous devrez sans doute faire état de ce cyber incident, même si les données ont été détruites, plutôt que volées. »

La capacité à réagir en cas de cyber incident sera pour les entreprises l'un des éléments-clés de leur conformité à ce nouveau règlement.

Concrètement, les plans de réponse aux cybers incidents doivent être actualisés et inclure des vérifications permettant de déterminer dans quels cas la notification de l'attaque réclamée par le RGPD devient nécessaire, explique Hannes.