MINISTÈRE DE L'INTÉRIEUR
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

DSIC
Direction des Systèmes d'Information et de Communication

DIRECTION DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION

DIRECTION
des systèmes d'information
et de communication Est

SSI

Lettre d'information SSI n°64

Pôle Défense et Sécurité des Systèmes d'Information

Notes d'information technique

Edition ► Décembre 2020

I – Cybercriminalité et attaques informatiques

Dans le MONDE

- **AstraZeneca ciblé par des cyberpirates nord-coréens.**
  Des pirates informatiques recourant à des outils déjà utilisés par des groupes nord-coréens ont tenté de pénétrer dans les systèmes informatiques du groupe pharmaceutique AstraZeneca en se faisant passer pour des recruteurs. Source LMI
- **Fuite de données médicales au Brésil : 16 millions de patients touchés dont Jair Bolsonaro.**
  Les deux bases de données concernées sont utilisées pour recenser les Brésiliens touchés par le Coronavirus. Source Siècle Digital – ZDNet – UD
- **Le fabricant d'armes Smith&Wesson piraté.**
  Comme les autres labos impliqués dans la recherche d'un vaccin contre la Covid-19, la firme Johnson & Johnson est aujourd'hui sous le feu des attaques informatiques.
  Source ZDNet – ZDNet – ZDNet – UD – Numerama
- **Covid-19 : L'EMA, en charge d'approuver les vaccins, victime d'une cyberattaque.**
  L'agence européenne des médicaments a récemment été victime d'un piratage. Les vaccins contre la Covid-19 pourraient avoir été la cible, même si l'agence n'a pas donné de détails sur l'attaque pour le moment. Source ZDNet – SN – LMI – Siècle Digital
- **Des pirates informatiques divulguent les données d'Embraer, troisième avionneur mondial.**
  La société brésilienne a été victime d'une attaque avec demande de rançon le mois dernier, en novembre. Source ZDNet
- **Cyberattaques massives à l'encontre du Canada.**
  De nombreuses pannes informatiques ont impacté des dizaines d'entreprises canadiennes ces 15 derniers jours. Un groupe de pirates du nom d'Everest revendiquent plusieurs cyberattaques à l'encontre de plusieurs compagnies du BTP du pays. Air Canada et l'Aéroport International de Vancouver sont concernés. Source Zataz
- **Les gangs derrière les rançongiciels font sonner le téléphone des victimes qui les ignorent.**
  Les cybercriminels continuent de développer à un rythme effrayant leurs méthodes de pression sur leurs victimes. Après les menaces de fuite, voilà le démarchage téléphonique…
  Source Numerama – ZDNet
- **Une rançon à près de 35M$ contre Foxconn au Mexique.**
  Fin novembre 2020, le site mexicain du géant de la sous-traitance informatique Foxconn a été victime du rançongiciel DoppelPaymer. 1 200 serveurs et 100 Go de données auraient été chiffrés et jusqu'à 30 To de sauvegardes effacées. Source LMI – ZDNet – Numerama – UD – Siècle Digital
- **FireEye, géant américain de la sécurité, victime d'une attaque informatique.**
  FireEye soupçonne que les auteurs de l'attaque sont liés à un gouvernement étranger. L'attaque a notamment visé les outils utilisés par FireEye pour ses tests d'intrusion.
  Source ZDNet – Numerama – UD – SN – Siècle Digital – LMI
- **Le croisiériste Hurtigruten sabordé par un ransomware.**
  Après Carnival ou CMA-CGM, le monde maritime affiche une autre victime de ransomware : Hurtigruten. La firme norvégienne a vu son système d'information tomber. Source LMI
- **La Cour européenne des droits de l'homme cible d'une cyberattaque à la suite d'une décision condamnant la Turquie.**
  Des hackers s'en sont pris au site web de la Cour de justice des droits de l'homme, le rendant indisponible pendant plusieurs heures. La juridiction strasbourgeoise, gardienne des libertés au niveau européen, accuse la Turquie d'être derrière cet incident. Source UD – ZDNet – SN

En FRANCE

Cybersécurité

TousAntiCovid : Un phishing imite le SMS gouvernemental.
Le gouvernement a lancé une campagne de sensibilisation par SMS pour la nouvelle version de son application TousAntiCovid. Mais une campagne de phishing par SMS imite cette campagne afin de diffuser un logiciel malveillant sur Android. Source ZDNet – Numerama – Numerama – L'1FO

« Nous avons essayé de livrer votre colis » : attention à ce faux SMS de UPS.
Un SMS vous indique de payer 2 euros pour valider une livraison de colis ? Ignorez-le, c'est un phishing. Source Numerama

Augmentation des tentatives de phishing imitant les banques et les services de paiement en ligne.
En effet, les cybercriminels ont utilisé le thème du coronavirus pour adapter leurs attaques par phishing tout au long de l'année. Mais avec les confinements et restrictions que nous traversons, l'intensification des achats en ligne et la hausse des transactions numériques sont des opportunités pour les pirates. Les Français n'ont pas été épargnés. Source UnderNews

Randstad victime du ransomware Egregor.
Le géant du travail par intérim Randstad a révélé une cyberattaque par rançongiciel ayant impacté un nombre limité de ses serveurs. Des données issues de ses activités en France ont notamment été volées. Source LMI

L'éditeur Dedalus mise sur une thérapie rapide.
Dedalus a été victime d'une cyberattaque. Un rançongiciel, Lockbit, a bloqué un site basé à Mérignac de l'éditeur de logiciels de santé. Il annonce avoir pris l'incident à temps et ne pas avoir eu de pertes de données. Source LMI

Dassault Falcon Jet victime du ransomware Ragnar Locker.
La filiale américaine de Dassault Aviation en charge de la commercialisation de jets privés a été touchée par une attaque par rançongiciel revendiquée par l'opérateur malveillant derrière Ragnar Locker. Ce dernier menace de mettre aux enchères des données concernant le tout dernier Falcon 6X. Source LMI – Zataz – ZDNet – Zataz

Un hôpital savoyard fonctionne au ralenti à la suite d'un ransomware.
L'hôpital d'Albertville, en Savoie, a été touché par un rançongiciel qui affecte l'accès aux dossiers patients et à un certain nombre d'équipements médicaux. En revanche, les plateaux d'imagerie et les blocs opératoires fonctionnent normalement d'après la direction hospitalière, qui a décidé de porter plainte. Source UD

Cyberattaque à Pantin : l'expansion des menaces envers les villes françaises.
Après plusieurs villes ces derniers mois telles que Vincennes ou Alfortville, ce sont les services municipaux de la ville de Pantin qui tournent au ralenti. La cause ? Une cyberattaque qui aurait été menée précédemment à Bondy mi-novembre. Source Globb Security – UnderNews

Fuite de Ledger : un hacker publie l'intégralité des données volées cet été.
[startup française spécialisée dans la sécurisation des portefeuilles de cryptomonnaie]
Un utilisateur du forum de hacker le plus connu a mis en ligne deux fichiers issus de la fuite de Ledger. Source Numerama

Cyberdéfense

Quel avenir pour la cybersécurité en France ? - [Enquête Proofpoint auprès de RSSI français]
Proofpoint dévoile aujourd'hui les conclusions d'une enquête menée auprès de 150 Responsables de la Sécurité des Systèmes d'Information (RSSI) français. Le rapport met en lumière la manière dont les organisations abordent la cybersécurité dans le contexte de la pandémie et comment elles anticipent l'avenir. Source UnderNews – Proofpoint

Cybercriminalité : Mais que fait la police ?
On lit tous les jours des témoignages d'entreprises, grands comptes ou PME, frappés par des attaques informatiques – allant du simple hameçonnage au ransomware. Et souvent, la question revient : « que fait la police ? » Car bien souvent, les entreprises ont la sensation d'être esseulées face à une cybercriminalité qui se permet aujourd'hui de publier des communiqués de presse et d'afficher fièrement ses tableaux de chasse. Source ZDNet

L'ANSSI et le BSI alertent sur le niveau de la menace cyber en France et en Allemagne dans le contexte de la crise sanitaire.
Pour la 3e édition du rapport franco-allemand « Common Situational Picture », l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et son homologue, le Bundesamt für Sicherheit in der Informationstechnik (BSI), font le constat d'un accroissement très rapide du niveau de la menace cyber en France et en Allemagne. Dans la continuité d'une trajectoire initiée en 2019, le nombre de cyberattaques a explosé : le nombre de victimes a ainsi été multiplié par 4 en un an. Cela est particulièrement préoccupant, notamment dans un contexte où toute cyberattaque est susceptible d'avoir un impact exacerbé du fait de la crise sanitaire. Source ANSSI – LMI – ZDNet

L'ANSSI continue de s'investir dans les travaux de l'appel de Paris à l'OCDE.
La France a fait le choix de l'OCDE (Organisation de coopération et de développement économique), dont la voix est portée par Yves Verhoeven depuis 2019, pour mettre en œuvre le volet relatif à la responsabilité des acteurs privés de l'Appel de Paris pour la confiance et la sécurité dans le cyberespace. Source ANSSI – ANSSI

Recommandations pour la protection des systèmes d'information essentiels.
Ce guide s'adresse en particulier aux opérateurs de services essentiels, pour mettre leurs systèmes d'information en conformité avec ces règles de sécurité. Ce guide peut également servir aux fournisseurs de services numériques (FSN) pour définir et mettre en œuvre leurs propres mesures de sécurité. Ce guide constitue enfin un recueil de bonnes pratiques pour les opérateurs d'importance vitale (OIV) et pour toute entité ayant des besoins de protection de ses SI, et pour leurs prestataires tels que les entreprises de services numériques (ESN).
Source ANSSI – ANSSI – ANSSI – ANSSI

Recommandations pour les architectures des systèmes d'information sensibles ou Diffusion Restreinte.
L'instruction interministérielle n° 901/SGDSN/ANSSI (II 901) du 28 janvier 2015 définit les objectifs et les mesures de sécurité minimales relatifs à la protection des informations sensibles, notamment celles relevant du niveau Diffusion Restreinte (DR). Le présent guide donne des recommandations pour la conception de l'architecture des systèmes d'information (SI) qui hébergent des informations sensibles ou DR. De manière générale, il apporte des conseils techniques pour la mise en pratique de l'II 901. Source ANSSI – ANSSI – ANSSI – Legifrance

II – Actualités

Brèves

Cybersécurité

Les deux meilleures pratiques pour une cybersécurité réussie.
Cisco vient de dévoiler les résultats de sa nouvelle étude sur la cybersécurité intitulée « Security Outcomes Study ». Celle-ci offre aux équipes informatiques une vision claire des sujets de sécurité à prioriser pour 2021. Menée auprès de 4 800 professionnels de la sécurité, des technologies de l'information et de la protection de la vie privée dans 25 pays, elle met en lumière les meilleures pratiques assurer la réussite des programmes de sécurité.
Source GlobalSecurity – SN

Le risk manager, un combattant des phénomènes étranges !
[Par Anne Lupfer, Responsable de l'offre Gestion des risques de l'information chez Almond]
En conduisant des études de risques, les risk managers s'aperçoivent fréquemment que les personnes sollicitées dépriorisent, dévalorisent voire ignorent le critère intégrité. Et ce, quel que soit leur secteur d'activité et quelle que soit l'étape de l'appréciation des risques (identification des besoins de sécurité ou évaluation des impacts d'un risque). Ainsi, viennent en tête les deux autres critères : la confidentialité (39 %) et la disponibilité (42 %) bien devant l'intégrité (16 %).
Source GlobalSecurityMag

Bien réagir aux attaques ransomware pour mieux survivre.
Qu'elles soient préméditées ou opportunistes, les attaques par ransomware font des dégâts conséquents. Zoom sur les points de fragilité, techniques utilisées et réactions à adopter pour essayer de parer au pire et limiter la casse. Source LMI

Ransomware : une menace sans fin ?
[Par Christophe Lambert – Directeur Technique France et EMEA Cohesity]
Se défendre contre cette menace en constante évolution n'est certes pas une mince affaire, mais un bon point de départ consiste à comprendre où se situent les points faibles et comment ils sont exploités. Source Silicon

Cybermenaces 2021, la tendance sera aux attaques d'exfiltration de données.
La cybercriminalité va s'intensifier en 2021 avec des criminels qui délaisseront les attaques de chiffrement des données au profit d'attaques d'exfiltration de données, selon ce que prévoit l'éditeur Acronis. Source SN

Cybercriminalité : un coût élevé pour l'économie mondiale.
Le coût de la cybercriminalité a augmenté de moitié en deux ans pour atteindre 1 trillion de dollars, selon McAfee et le CSIS. Source Silicon – UD

Arnaque: « Bonjour, ici Microsoft ».
Des appels téléphoniques aux couleurs de Microsoft vous annoncent un problème dans votre parc informatique. Ne répondez pas au risque d'avoir de vrais ennuis, ensuite. Source Zataz

2020 … une année cyber catastrophique.
Une année d'enquête concernant les cyberattaques de type prise d'otage numérique, il ne faut pas oublier les autres catastrophiques malveillances qui ont égrainé l'année 2020. Voici le récapitulatif, non exhaustif d'une année cyber catastrophique. Source Zataz

Les attaques DDoS explosent et ciblent les jeux en ligne.
Avec la crise sanitaire, les campagnes en déni de service se sont fortement multipliées au troisième trimestre 2020. Pendant le confinement, les jeux en ligne ont particulièrement été visés par des attaques DdoS. Source LMI

Une intrusion ne doit pas être considérée comme un événement ponctuel.
D'après les chiffres de CrowdStrike, 68 % des organisations ayant subi une attaque, ont connu d'autres tentatives d'intrusion. Plutôt que de considérer la réponse aux intrusions comme une activité d'urgence ponctuelle, les organisations doivent prévoir une surveillance et une réponse en temps réel et en continu. Source IT Social

Comment modéliser les cyber-risques pour mieux s'en prémunir ?
Le risque cyber, qui peut prendre la forme d'un piratage de site, d'un vol de données ou d'une usurpation d'identité, est devenu un risque assurantiel à part entière pour les entreprises, qui sont de plus en plus conscientes de la nécessité de le garder à l'œil et d'apprendre à le gérer efficacement. Source IT Social

Les 10 Cyberattaques qui ont marqué l'année 2020.
Exceptionnelle à tous égards, l'année 2020 a marqué une nouvelle étape dans l'essor des cyber risques : face à des hackers exploitant les failles nées de la crise sanitaire, les entreprises ont été exposées à un niveau de menace inédit et des cyberattaques d'ampleur.
Source GlobalSecurityMag

10 prévisions pour aider les RSSI à traverser les incertitudes de 2021.
Netskope, une société américaine spécialisée dans les solutions de cybersécurité dans le Cloud, livre ici ses 10 prévisions afin d'aider ses pairs RSSI à se préparer à entrer en zone inconnue en 2021. Source SN

Microsoft et FireEye confirment la cyberattaque de SolarWinds.
Les systèmes du fournisseur de logiciels SolarWinds ont été compromis suite à une cyberattaque perpétrée par un groupe de pirates parrainés par un État.
Source ZDNet – UD – InformatiqueNews – LMI – ZDNet – LMI – Silicon – Numerama

Cybersécurité de l'industrie

Les entreprises préoccupées par la sécurité de la 5G.
Une étude de Deloitte montre que les entreprises s'inquiètent du volet sécurité de la 5G. Son déploiement nécessitera des compétences en cybersécurité pour diminuer les risques et le recours à l'IA. Source LMI

Les terminaux d'imagerie médicale de GE Healthcare exposés au piratage.
[GE Healthcare – filiale de General Electric (USA)]
Une vulnérabilité donne aux pirates un moyen d'accéder à des données sensibles et d'exécuter des codes malveillants sur les appareils d'imagerie médicale de GE Healthcare. Avec à la clé une capacité d'altérer leur fonctionnement. Source LMI

Doctrine de détection pour les systèmes industriels.
Une supervision à partir de systèmes de contrôle et d'acquisition de données (Supervisory Control And Data Acquisition, SCADA) existe sur la majorité des installations industrielles. Elle permet notamment de piloter et de veiller au bon fonctionnement du procédé industriel. En revanche, cette supervision n'est ni prévue ni adaptée pour la détection d'incidents de sécurité, notamment induits par l'ouverture de ces systèmes et par leur interconnexion avec des réseaux largement connectés. Source ANSSI – ANSSI

Sécurité numérique

Les entreprises françaises ont encore du chemin à parcourir pour atteindre l'Intelligence Active en temps réel.
Ces dernières années, les entreprises françaises ont travaillé à l'élaboration d'une stratégie d'analytique permettant de transformer leurs données en enseignements de valeur. Toutefois, il semblerait que la mise en pratique de cette stratégie représente encore un défi pour une majorité d'entre elles, comme le démontre le rapport « Les données : Le nouvel or bleu. La nécessité d'investir dans des pipelines de données et d'analyse » mené conjointement par Qlik et IDC. Source GlobalSecurityMag

Pourquoi l'externalisation va s'imposer.
Confier au moins en partie la sécurité du système d'information de l'entreprise est une tendance forte du marché. Complexité des technologies, maîtrise des coûts, mais aussi le manque de ressources humaines explique un mouvement de fond des entreprises vers l'externalisation. Source Silicon

L'importance de la périphérie réseau pour sa sécurité.
L'investissement dans la périphérie du réseau permet aux FAI de proposer de nouveaux services et de réaliser des économies. Cependant, le paysage des DDoS étant plus imprévisible que jamais, ils devront ouvrir un nouveau chapitre de leur stratégie de sécurité pour 2021 explique Darre Anstee, de NETSCOUT. Source ZDNet

Gestion des accès à privilèges de nouvelle génération : un atout pour les équipes.
[Par Hicham Bouali – Architecte IAM Solutions One Identity]
Le PAM de nouvelle génération offre désormais une vue holistique et tient compte des besoins inhérents aux accès à privilèges, tout en intégrant la redoutable adaptabilité dont peuvent hélas faire preuve les personnes malveillantes, et leurs tentatives de compromission sur des comptes à privilèges. Source Silicon

Dell annonce de nouvelles protections pour ses PC et serveurs.
Dell va utiliser des scellés inviolables pendant le transport des appareils et fournir une fonction de réinitialisation logicielle pour effacer les disques durs avant leur déploiement chez les clients. Source ZDNet

À quoi sert Tor ? Presque pas à aller sur le dark web.
Une équipe de chercheurs académiques a essayé de déterminer quel pourcentage des utilisateurs du réseau anonyme Tor s'en servait pour visiter des sites « illicites » ou du moins « cachés ». D'après eux, seuls 7 % visitent les sites du dark web (ceux en. onion), tandis que les autres se servent de Tor uniquement comme protection sur le web traditionnel.
Source Numerama

Comment sécuriser son réseau informatique ?
Dans un contexte où les attaques informatiques sont de plus en plus fréquentes et engendrent des dommages importants, il est indispensable pour chaque entreprise de mettre en place une stratégie efficace afin de sécuriser son réseau. Il existe aujourd'hui des solutions permettant de profiter au maximum de la technologie, tout en se protégeant du piratage. Source Zataz

L'externalisation en question.
[Par Alain Bouillé, délégué général du Cesin (Club des experts de la sécurité de l'information et du numérique) – Arnaud Hess, responsable du Business Development chez Advens – Laurent Célerier, CTO d'Orange Cyberdéfense.]
La complexité croissante des technologies, le besoin de maîtrise des coûts et le manque de ressources humaines sont les principaux critères qui plaident pour un recours à l'externalisation de la cybersécurité. Points de vue croisés de trois spécialistes. Source Silicon

Des réseaux plus sûrs à la maison : Comment travailler à distance en 2021.
Le travail à domicile à temps plein présente un ensemble unique de défis. Cependant, il y a un aspect qu'il est facile de négliger : la sécurité de votre réseau domestique. Source ZDNet

La continuité d'activité n'est pas garantie sans contrôle régulier.
Les DSI devraient renforcer la sécurité des systèmes de sauvegarde pour éviter les activités malveillantes menées par des loups solitaires. Source Reseaux-Telecoms

« C'est compliqué d'ouvrir et de sécuriser au maximum le SI »
[Par Rémi Grivel, vice-président du Clusir Rhône-Alpes – directeur général du groupe Ciril. (crédit : Ciril)] - Réunissant plus de 150 membres DSI, RSSI et DPO, le Clusir Rhône-Alpes Auvergne constitue un point de rencontres incontournable au niveau régional pour échanger autour de la sécurité des SI. Comment ses membres traversent la crise sanitaire ? À quelles menaces sont-ils confrontés ? Le point avec son vice-président Rémi Grivel. Source LMI

Effacer ses données d'un ordinateur, d'un téléphone ou d'une tablette avant de s'en séparer.
Vous souhaitez vendre, donner ou jeter votre ordinateur personnel, votre téléphone ou votre tablette ? Pensez à bien effacer les données qui s'y trouvent pour que celles-ci ne soient pas réutilisées par d'autres personnes. Source CNIL

« Des Hommes de bonne volonté contre le temps qui passe… »
[Par Fabien MIQUET, Product & Solution Security Officer chez Siemens Digital Industries France] - [CyberCercle – un cercle de réflexion, d'expertise et d'échanges sur les questions de confiance et de sécurité numériques]
Force est de constater que la cybersécurité des systèmes industriels et urbains, enjeu majeur s'il en est, n'est pas encore un sujet mature au sein des donneurs d'ordre, alors même que dix années se sont écoulées depuis STUXNET. Source CyberCercle

Hameçonnage, demande d'argent et virus informatique : le top 3 des menaces cyber en 2020 pour les Internautes.
Cette étude, menée en juillet dernier par l'Institut National de la Consommation (INC), dévoile que plus de 90 % des internautes sondés ont déjà été victimes au moins une fois d'un acte de cybermalveillance, alors que pourtant 80 % des personnes interrogées se disent suffisamment sensibilisées et informées sur les risques liés à Internet.
Source cybermalveillance – cybermalveillance – cybermalveillance

La fraude à la carte bancaire.
La fraude à la carte bancaire désigne l'utilisation frauduleuse des coordonnées de la carte bancaire d'une personne à son insu alors que celle-ci est pourtant toujours en possession de sa carte. Source cybermalveillance

Le référentiel d'exigences applicables aux prestataires de vérification d'identité à distance (PVID).
Le besoin de disposer de services de vérification d'identité à distance s'est accru en France et en Europe au cours des dernières années et a été mis en lumière directement par la crise sanitaire. Aussi, l'ANSSI a élaboré un référentiel pour les prestataires de vérification d'identité à distance. Ce nouveau référentiel d'exigences, valorisé à terme par un visa de sécurité ANSSI, permettra d'identifier les prestataires fournissant un service de vérification d'identité à distance avec un niveau de garantie substantiel ou élevé. Source ANSSI – ANSSI

Sûreté

Classement 2020 des pires élèves en matière de mots de passe : les utilisateurs de Zoom et les employés de Twitter.
Les utilisateurs de Zoom et les employés de Twitter sont les « Pires élèves en matière de mots de passe » selon le classement 2020 de Dashlane. Experian, Nintendo et Marriott figurent aussi dans la cinquième édition de ce classement annuel. Source UnderNews

Sonnettes connectées, nids à vulnérabilités.
Pratique au quotidien, l'usage de sonnettes connectées peut présenter un véritable risque en termes de cybersécurité. Source LMI

IoT (objets connectés) / IA

Comment réduire l'impact environnemental des projets IoT ?
[par Georges Ouffoué, docteur en informatique, responsable « Lab by APL », APL Data Center]
Si dans certains cas les objets connectés et applications associées permettent de réaliser des gains opérationnels, économiques et/ou environnementaux, leur utilisation est loin d'être neutre sur le plan environnemental. L'analyse du cycle de vie (ACV) complet des projets IoT, pour mesurer leur balance environnementale, reste le moyen le plus efficace de s'assurer que les gains attendus seront bien au rendez-vous. Source GlobalSecurityMag

IA : 2021 promet d'être une année riche en défis technologiques.
Il ne fait aucun doute que l'épidémie de Covid-19 bouleverse la vision du monde que se font les individus, les citoyens du monde ainsi que les professionnels de la technologie. Ses effets sur le secteur technologique sont au cœur des réflexions : quelles innovations vont en découler ? Quelles seront les nouvelles attentes des utilisateurs ? Quelle transformation numérique les entreprises devront-elles opérer en conséquence ? Source GlobalSecurityMag

Intelligence Artificielle, accélérateur de croissance en Occitanie.
La cartographie réalisée référence plus de 120 acteurs de l'IA en région par expertise IA (analyse de texte, analyse médicale, cybersécurité, IoT, maintenance prédictive, chatbot, traitement d'image, architecture et hébergement de données…), localisation géographique et secteur d'activité (relation client, santé, aéronautique et spatial, agriculture et agroalimentaire, BTP, chimie et pharmacie, éducation, Smart – City…). Source Alliancy

L'intelligence artificielle pour une gestion sanitaire plus résiliente ?
Alors que la deuxième vague de la pandémie a très vite submergé nos services hospitaliers, nous obligeant une fois encore à se confiner, beaucoup se demandent si ce deuxième épisode épidémique aurait pu être évité. Au point de remettre en cause la faculté des pouvoirs publics à anticiper et gérer les crises. Alliancy s'est penché sur la question pour savoir si la technologie, et en particulier l'intelligence artificielle, aurait pu – ou pourrait à l'avenir – aider à rendre notre système de santé plus résilient. Source Alliancy

L'IA va-t-elle supplanter l'humain sur la cybersécurité en 2030 ?
Selon une étude menée par Trend Micro sur le futur de la cybersécurité d'ici 2030, une partie des responsables IT pensent qu'à l'avenir cette fonction sera réalisée uniquement par une IA.
Source LMI

LOGICIELS MALVEILLANTS

Malware – Ransomwares

Ransomware : une menace sans fin ?
[Par Christophe Lambert – Directeur Technique France et EMEA chez Cohesity]
Se défendre contre cette menace en constante évolution n'est certes pas une mince affaire, mais un bon point de départ consiste à comprendre où se situent les points faibles et comment ils sont exploités. Source Silicon

DoppelPaymer : ce ransomware « discret » qui n'épargne pas la France.
Il n'a pas l'aura de Maze, d'Egregor ou de Ryuk. Mais le ransomware DoppelPaymer sévit en France, avec une dizaine de victimes revendiquées. Source Silicon

« Sunburst » : une nouvelle attaque ultra sophistiquée menace des milliers d'organisations.
« Sunburst ». Retenez ce nom, il devrait revenir dans l'actualité de la fin d'année 2020. C'est ainsi que le géant de la sécurité FireEye a baptisé un malware jusqu'ici inconnu, dont lui-même a été victime en ce début de décembre 2020. Des « hackers très sophistiqués », l'exploiteraient au moins depuis le printemps dans des manœuvres d'espionnage contre des organisations gouvernementales ou proches de celles-ci.
Source Numerama – GlobalSecurityMag – Numerama

Ransomware : Le FBI s'inquiète des nouveaux moyens de pression visant les entreprises.
Selon le FBI, le groupe DoppelPaymer a été l'un des premiers à appeler les victimes de ransomware, en les menaçant d'envoyer des personnes chez elles si elles ne payaient pas la rançon. Source ZDNet

Le malware Emotet refait surface pour les fêtes de fin d'année.
Le malware prolifique vient de refaire surface, cette fois pour les fêtes de fin d'année, via des campagnes de phishing. Source SN

Le logiciel Orion ciblé par un autre malware. [SolarWinds]
Microsoft a découvert son existence, et affirme qu'il provient d'un autre groupe de hackers.
Source Siècle Digital

ACTUALITES JURIDIQUES - Législation et jurisprudences

CNIL

Informatique et Libertés : retour sur la création de la CNIL pendant le mandat du Président Valéry Giscard d'Estaing.
Face au débat relatif aux enjeux émergents pour la vie privée et les libertés individuelles suite, notamment, à l'annonce du projet SAFARI, la loi Informatique et Libertés est votée en 1978.
Source CNIL – CNIL

La CNIL et l'ADF renouvellent leur partenariat pour accompagner les collectivités dans leur démarche de protection des données personnelles.
Afin de poursuivre l'accompagnement des Départements dans leur mise en conformité au règlement européen sur la protection des données, la CNIL et l'ADF (Assemblée des Départements de France) ont signé une nouvelle convention de partenariat pour une durée de trois ans. Source CNIL

Recherches médicales liées à la COVID-19 : la CNIL mobilisée aux côtés de l'Institut Pasteur.
Des informations erronées étant parues récemment dans des médias, la CNIL et l'Institut Pasteur ont souhaité affirmer publiquement leur parfaite coopération dans le cadre de la lutte contre la COVID-19. Source CNIL

Cookies : sanction de 60 millions d'euros à l'encontre de GOOGLE LLC et de 40 millions d'euros à l'encontre de GOOGLE IRELAND LIMITED.
Le 7 décembre 2020, la formation restreinte de la CNIL a sanctionné les sociétés GOOGLE LLC et GOOGLE IRELAND LIMITED d'un montant total de 100 millions d'euros d'amende, notamment pour avoir déposé des cookies publicitaires sur les ordinateurs d'utilisateurs du moteur de recherche google.fr sans consentement préalable ni information satisfaisante. Source CNIL – Legifrance – ZDNet

Cookies : sanction de 35 millions d'euros à l'encontre d'AMAZON EUROPE CORE.
Le 7 décembre 2020, la formation restreinte de la CNIL a sanctionné la société AMAZON EUROPE CORE d'une amende de 35 millions d'euros pour avoir déposé des cookies publicitaires sur les ordinateurs d'utilisateurs à partir du site amazon.fr sans consentement préalable et sans information satisfaisante. Source CNIL

RGPD – (Règlement général sur la protection des données)

Certification des compétences du DPO : la CNIL lance une consultation publique pour mettre à jour ses référentiels.
La CNIL peut agréer des organismes en vue de délivrer une certification des compétences du délégué à la protection des données (DPO) sur la base de référentiels. Afin d'évaluer ces derniers, la CNIL publie une consultation jusqu'au 6 janvier 2021. Source CNIL

Violations de données de santé : la CNIL sanctionne deux médecins.
Le 7 décembre 2020, la formation restreinte de la CNIL a prononcé deux amendes de 3 000 € et 6 000 € à l'encontre de deux médecins libéraux pour avoir insuffisamment protégé les données personnelles de leurs patients et ne pas avoir notifié une violation de données à la CNIL. Source CNIL – UD

Violation de données : Twitter condamné à 450 000 euros d'amende par la CNIL irlandaise.
Twitter doit payer 450 000 euros pour avoir incorrectement notifié une violation de données intervenue en 2018 qui a rendu public des tweets protégés. Il devient ainsi la première grande entreprise américaine à être condamné par la CNIL irlandaise au titre du RGPD. Source UD

Quelles sont les conséquences du RGPD sur les dispositifs médicaux ? -[Par Amanda Dubarry] - Un consortium international de plus de 250 journalistes a enquêté pendant plus d'un an sur la mise sur le marché des dispositifs médicaux. Les journalistes ont alors constaté des défaillances concernant la sécurité, la traçabilité et l'efficacité des dispositifs médicaux. Au-delà des préoccupations sociétales et sanitaires, cette enquête est l'occasion de se pencher sur l'encadrement des dispositifs médicaux au regard du règlement général sur la protection des données du 26 avril 2016 (RGPD) Source HAAS Avocats – HAAS Avocats

Droit des TIC

L'Europe s'accorde pour supprimer les contenus terroristes sur Internet en une heure.
La Commission, le Parlement et le Conseil ont trouvé un accord politique pour aboutir à un nouveau cadre contre la propagande terroriste sur Internet. Le principal axe consiste à obtenir le retrait des contenus en moins d'une heure. Source Numerama

Le Legal design va s'imposer au cœur des projets informatiques.
[Par Stéphane Astier et Anne-Charlotte Andrieux]
Cette fin d'année 2020 est l'occasion d'une réflexion essentielle sur la place du droit dans la gestion générale des projets informatiques. Que l'on se place côté client ou côté prestataire, l'introduction d'une démarche de legal design visant à placer le droit au cœur de cette gestion est en effet une pratique ayant vocation à s'imposer à l'avenir. Source HAAS Avocats

Définitions DSA x DMA | Zoom sur le Digital Services Act et le Digital Market Act.
[Par Eve Renaud-Chouraqui]
Ces deux règlements, d'application directe, ont vocation à remettre de l'ordre dans ce que Thierry Breton a qualifié de « far west » numérique. Le DSA sera applicable à tout intermédiaire en ligne et visera à imposer de nouvelles obligations et responsabilités par rapport aux contenus qu'il héberge. Le DMA viendra, quant à lui, cibler les comportements économiques des acteurs systémiques du numérique et les abus et dérives constatées à l'encontre de leurs concurrents et de leurs clients. Source HAAS Avocats – HAAS Avocats

Les nouvelles actions de groupe : comment ça marche ? - [Par Gérard Haas et Kate Jarrard]
Les projets de réforme de l'action de groupe ont le vent en poupe depuis plusieurs mois. Le 15 septembre 2020, la proposition de loi n°3329 pour un nouveau régime de l'action de groupe a été déposée à l'Assemblée nationale. Celle-ci vise à créer un nouveau cadre juridique commun à l'ensemble des actions de groupe. Deux mois plus tard, le 25 novembre, le Parlement européen a adopté la version finale d'une proposition de directive visant à instaurer un régime de « class action » en matière de protection des consommateurs.
Source HAAS Avocats – Assemblée nationale – UE

Score de productivité de Microsoft : une surveillance permanente du salarié ?
[Par Amanda Dubarry et Lucie Brecheteau]
En octobre dernier, le géant Microsoft a présenté un nouvel outil destiné aux entreprises : le « score de productivité », dont l'objectif affiché est d'évaluer la production de chaque salarié. Au cœur de ces informations figurent notamment le nombre de mails envoyés par le salarié ainsi que la fréquence d'envoi, ou encore le temps passé sur des applications telles que Teams ou Skype. Source HAAS Avocats

Juridique

L'adresse IP d'un salarié peut constituer une preuve illicite.
Le Tribunal de commerce de Paris a jugé que la « difficulté de s'accorder sur des prestations » n'est pas anormale en cas de recours à la méthode Agile et en l'absence d'un cahier des charges. En outre, la responsabilité du prestataire ne pouvait être engagée pour défaut de vérification de la conformité des produits aux attentes du client, cette obligation incombant au client. Celui-ci n'avait d'ailleurs pas exprimé ses besoins et avait signé le procès-verbal de recettes sans réserve et réglé le solde des factures, confirmant ainsi son accord aux produits délivrés. Source Cyberdroit – Legalis

Litiges informatiques : attention aux délais de constats d'huissier à respecter.
Un litige entre une PME et une agence web vient rappeler que constater par exploit d'huissier un dysfonctionnement ne suffit pas. Source LMI – Legalis

Législation

Publication des décrets relatifs aux fichiers PASP, GIPASP et EASP : la CNIL précise sa mission d'accompagnement.
La CNIL a rendu trois avis, sur les modifications des fichiers PASP (Prévention des atteintes à la sécurité publique) GIPASP (Gestion de l'information et Prévention des atteintes à la sécurité publique) et EASP (Enquêtes administratives liées à la sécurité publique). Elle rappelle, à cette occasion, les conditions dans lesquelles elle exerce sa mission d'accompagnement des pouvoirs publics. Source CNIL – Legifrance – Legifrance – Legifrance

Cryptomonnaies : La France ne veut plus d'anonymat.
Le ministère de l'Économie a annoncé hier la parution d'une ordonnance visant à étendre les obligations pesant sur les acteurs du secteur des cryptomonnaies. Le gouvernement entend imposer les mêmes obligations de contrôle d'identité à l'ensemble des sociétés françaises.
Source ZDNet

DSA, DMA, l'Europe revoit sa régulation numérique.
Au travers de deux textes en préparation depuis plus d'un an, le Digital Services Act et le Digital Market Act, la Commission européenne entend mettre à jour son cadre réglementaire en vigueur sur le numérique. Source ZDNet

III - Avis Cert-FR (les 20 plus récents) - Etat de vulnérabilités et les moyens de s'en prémunir !

Référence	Titre	Date
CERTFR-2020-AVI-846	Multiples vulnérabilités dans les produits QNAP	(31 décembre 2020)
CERTFR-2020-AVI-845	Vulnérabilité dans SolarWinds Orion API	(28 décembre 2020)
CERTFR-2020-AVI-844	Multiples vulnérabilités dans les produits Qnap	(23 décembre 2020)
CERTFR-2020-AVI-843	Multiples vulnérabilités dans les produits Treck	(23 décembre 2020)
CERTFR-2020-AVI-842	Multiples vulnérabilités dans Asterisk	(23 décembre 2020)
CERTFR-2020-AVI-841	Multiples vulnérabilités dans le noyau Linux de Red Hat	(23 décembre 2020)
CERTFR-2020-AVI-840	Multiples vulnérabilités dans Tenable Tenable.sc	(22 décembre 2020)
CERTFR-2020-AVI-839	Multiples vulnérabilités dans Trend Micro InterScan Web Security Virtual Appliance	(22 décembre 2020)
CERTFR-2020-AVI-838	Multiples vulnérabilités dans Aruba ArubaOS	(21 décembre 2020)
CERTFR-2020-AVI-837	Multiples vulnérabilités dans le noyau Linux de SUSE	(21 décembre 2020)
CERTFR-2020-AVI-836	[SCADA] Multiples vulnérabilités dans les produits Schneider Electric	(21 décembre 2020)
CERTFR-2020-AVI-835	Vulnérabilité dans F5 BIG-IP	(21 décembre 2020)
CERTFR-2020-AVI-834	Multiples vulnérabilités dans le noyau Linux de Debian LTS	(21 décembre 2020)
CERTFR-2020-AVI-833	Multiples vulnérabilités dans Wireshark	(21 décembre 2020)
CERTFR-2020-AVI-832	Multiples vulnérabilités dans F5 BIG-IP	(18 décembre 2020)
CERTFR-2020-AVI-831	Vulnérabilité dans les produits VMware	(18 décembre 2020)
CERTFR-2020-AVI-830	Vulnérabilité dans le noyau Linux de SUSE	(18 décembre 2020)
CERTFR-2020-AVI-829	Multiples vulnérabilités dans F5 BIG-IP	(17 décembre 2020)
CERTFR-2020-AVI-828	Vulnérabilité dans Zimbra	(17 décembre 2020)
CERTFR-2020-AVI-827	Multiples vulnérabilités dans Mozilla Thunderbird	(16 décembre 2020)

- **Alertes (les 5 plus récentes)** - **Destinées à prévenir d'un danger immédiat**

Référence	Titre	Date
CERTFR-2020-ALE-026	Présence de code malveillant dans SolarWinds Orion	Alerte en cours le 14/12/2020
CERTFR-2020-ALE-025	Vulnérabilité dans Fortinet FortiOS SSL-VPN	Alerte en cours le 27/11/2020
CERTFR-2020-ALE-024	[MaJ] Vulnérabilité dans les produits VMware	Alerte en cours le 24/11/2020
CERTFR-2020-ALE-022	[MàJ] Vulnérabilité dans Oracle Weblogic	Alerte en cours le 30/10/2020
CERTFR-2020-ALE-020	Vulnérabilité dans Microsoft Netlogon	Alerte en cours le 15/09/2020

- **Bulletins d'actualité** - **Une illustration par l'actualité récente de certaines mesures pragmatiques à appliquer - (les 5 plus récentes)**

Référence	Date
CERTFR-2020-ACT-018	(28 décembre 2020)
CERTFR-2020-ACT-017	(21 décembre 2020)
CERTFR-2020-ACT-016	(14 décembre 2020)
CERTFR-2020-ACT-015	(07 décembre 2020)
CERTFR-2020-ACT-014	(30 novembre 2020)

- **Indicateurs de compromission** - **Les indicateurs de compromission, qualifiés ou non par l'ANSSI, sont partagés à des fins de préventions**

Référence	Titre	Date
CERTFR-2020-IOC-006	Le rançongiciel Egregor	(18 décembre 2020)
CERTFR-2020-IOC-005	Le Rançongiciel Ryuk	(30 novembre 2020)
CERTFR-2020-IOC-004	Le groupe cybercriminel TA505	(22 juin 2020)
CERTFR-2020-IOC-003	Le code malveillant Dridex	(25 mai 2020)
CERTFR-2020-IOC-002	Le groupe cybercriminel SILENCE	(07 mai 2020)

- **Menaces et incidents** - **Les rapports des Menaces et Incidents détaillent l'état des connaissances et les investigations de l'ANSSI en analyse de la menace et traitements d'incidents (les plus récentes).**

Référence	Titre	Date
CERTFR-2020-CTI-012	Le rançongiciel Egregor	(18 décembre 2020)
CERTFR-2020-CTI-011	Le rançongiciel Ryuk	(30 novembre 2020)
CERTFR-2020-CTI-010	Le malware-as-a-service Emotet	(02 novembre 2020)
CERTFR-2020-CTI-006	Évolution de l'activité du groupe cybercriminel TA505	(22 juin 2020)
CERTFR-2020-CTI-005	Le code malveillant Dridex : origines et usages	(25 mai 2020)

- **Durcissement et recommandations et incidents** - **(Un ensemble de points de contrôle visant à identifier des faiblesses potentiellement exploitables sur un système d'information sont proposés ; une série de recommandations opérationnelles complètent ces points d'audit afin de durcir le niveau de sécurité du système d'information)**

Référence	Titre	Date
CERTFR-2020-DUR-001	Points de contrôle Active Directory	(02 juin 2020)

IV – Etat des mises à jour de sécurité – *Pour le périmètre du Ministère de l'Intérieur (MI)*

Logiciel	Version	Dernières vulnérabilités identifiées sur versions antérieures		
		Avis CERT-FR	Référence Editeur	Alerte C2MI
Libre Office MIMO	6.2.8.2 M1			
	Antérieures	CERTFR-2020-AVI-347	CVE-2020-12802	
Mozilla Firefox	78.6.0 ESR			
	Antérieures	CERTFR-2020-AVI-826	Mfsa2020-54	2020_12_18
Client officiel Pablo *	3.1.20	Multiples vulnérabilités		
Adobe Reader	11.0.23			
	Antérieures	CERTFR-2020-AVI-814	apsb20-75	2019_052_01
Adobe Flash Player	32.0.0.192			
	Antérieures	CERTFR-2020-AVI-644	apsb20-58	2019_083_01
Adobe Shockwave player	12.3.3.204			
	Antérieures	CERTFR-2017-AVI-415	apsb17-40	2017_191_01
McAfee EPO	5.3			
	Antérieures	CERTA-2013-AVI-278	SB10042	
McAfee Agent	5.0.5			
McAfee ViruScan	8.8.0.P7			
7-zip	18.05			2018_78_01
	Antérieures	CERTFR-2018-AVI-214	7-zip.org	
Foxit Reader	10.1.0.37527			
	Antérieures	CERTFR-2020-AVI-813	Bulletin de sécurité Foxit du 09 décembrel 2020	
VLC	3.0.7.1			
	Antérieures	CERTFR-2019-AVI-291	CVE-2019-5439	

	Version conseillée		Version non corrigée nécessitant des mesures de contournement		Version présentant un risque élevé

**** pablo : client de messagerie Thunderbird pour le Ministère de l'Intérieur***