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°68

Pôle Défense et Sécurité des Systèmes d'Information

Notes d'information technique

Edition ► Avril 2021

I – Cybercriminalité et attaques informatiques

Dans le MONDE

- **533 millions de données utilisateurs de Facebook compromises.**
  Une compilation de 533 millions d'enregistrements d'utilisateurs Facebook incluant des noms, numéros de téléphones et e-mails s'est retrouvée sur RaidForums. Source LMI – Zataz
- **Le pétrolier SHELL pris en otage par un chantage numérique.**
  La compagnie pétrolière anglo-néerlandaise Shell et ses 83 000 employés pris en otage par un rançonnage numérique signé par le groupe Cl0P. Source Zataz
- **En Iran, une cyberattaque vise la centrale de Natanz.**
  Déjà ciblée par un acte de sabotage en juillet dernier, la centrale d'enrichissement d'uranium de Natanz aurait cette fois fait les frais d'une cyberattaque. Cette-dernière est intervenue dimanche après l'inauguration officielle des dernières centrifugeuses plus performantes. Source LMI
- **La Commission européenne visée par une cyberattaque.**
  Plusieurs organes de l'Union européenne ont été visés par une série d'attaques. Nous ne connaissons pour le moment ni l'origine des hackers, ni les dégâts causés par ces intrusions. Source Siècle Digital
- **Affaire SolarWinds : 4 mois plus tard, l'Europe admet faire partie des victimes.**
  Le gouvernement américain n'est pas la seule victime de l'affaire SolarWinds. 4 mois après la découverte de l'attaque, l'Union européenne déclare que plusieurs de ses institutions ont été touchées par la campagne de cyberespionnage. Source Numerama
- **Huawei accusé d'espionnage aux Pays-Bas.**
  Huawei aurait accédé aux données de 6,5 millions d'abonnés de l'opérateur néerlandais KPN.
  Source Siècle Digital
- **13 millions de clients de Phone House Espagne dans les mains de pirates.**
  Les pirates informatiques du groupe Babuk ont réussi à infiltrer l'informatique de l'opérateur téléphonique Phone House Espagne. Les cybercriminels viennent de diffuser une partie des données volées. Source Zataz
- **Québec : le numéro 1 du voyage piraté.**
  Le site web Québécois Express Voyage infiltré. Une base de données de plusieurs milliers de Québécois commercialisée par le pirate. Source Zataz

En FRANCE

Cybersécurité

Attention aux mails frauduleux semblant provenir de Service-Public.fr !
Vous avez reçu un mail qui utilise le logo de Service-Public.fr et qui vous alerte sur une nouvelle version de la carte vitale ? Ce courriel vous invite à cliquer sur une page et à renseigner vos données personnelles pour obtenir votre nouvelle carte vitale ? Soyez vigilant, ces mails n'émanent pas de Service-Public.fr et il ne faut en aucun cas y donner suite. Source service-public

Fuite des numéros de 20 millions de Français depuis Facebook : tout ce qu'il faut savoir.
Les numéros de téléphone de 533 millions d'utilisatrices et utilisateurs de Facebook ont été publiés, librement et illégalement, sur le web. Source Numerama – Numerama – Numerama – Numerama – UD

Pierre Fabre touché par une cyberattaque.
Le groupe pharmaceutique et de dermo-cosmétiques Pierre Fabre a été touché par une attaque informatique de grande ampleur. Ses systèmes informatiques seraient à l'arrêt depuis mercredi matin. Ses sites web et son standard téléphonique sont tombés. Source LMI – LMI – Zataz – ZDNet – UD – Siècle Digital

École à la maison : enquête en cours après cyberattaques.
Suite à l'indisponibilité du service d'enseignement à distance CNED, une plainte a été déposée près le parquet de Paris et instruite par l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. L'implication d'un acteur étranger de puissance étatique est loin de couler de source.
Source LMI – ZDNet – UD – UD – SN

Plus de deux millions de clients Yves Rocher ressortent dans le black market.
En 2019, une fuite de données est annoncée par un vendeur de VPN. Un an et demi plus tard, deux millions de données clients de la marque Yves Rocher apparaissent dans plusieurs blackmarket surveillés par ZATAZ. Plus de deux millions de clients canadiens sont concernés. Source Zataz

Diffusion d'une base de données volée à la société UCAR.
Identités, téléphones, adresses physiques et électroniques. Un pirate diffuse plus de 130 000 comptes clients courant de 2018 à fin 2020. Source Zataz – LMI

Quand un reportage TV sur la fuite des infirmières au Luxembourg fait fuiter un mot de passe d'un hôpital.
La fuite de mot de passe, de mail… En vous en parle souvent. Mais quand il s'agit d'une fuite via un reportage TV, on peut se dire que l'éducation sur le sujet du contrôle de son environnement a encore de beaux jours devant elle ! Source Zataz

L'hôpital de Saint-Gaudens touché par un ransomware, les tests Covid-19 interrompus.
Après Dax, Oloron-Sainte-Marie et Villefranche-sur-Saône, c'est au tour du centre hospitalier de Saint-Gaudens en Haute-Garonne d'être pris pour cible par des cybercriminels. Les prélèvements Covid-19 et les bilans biologiques externes ont été interrompus. Seule la téléphonie a été remise en place depuis l'attaque informatique. Une plainte a été déposée. Source UD

Depuis un an, 18 millions de Français ont été victimes de la cybercriminalité.
Les Français se sentent plus vulnérables aux attaques informatiques depuis la pandémie de Covid-19. Ils remarquent, à juste titre, que leur temps de présence en ligne a augmenté. Un sentiment renforcé par les chiffres de la cybercriminalité : au cours des 12 derniers mois, 18 millions de personnes ont été victimes d'une attaque en France, d'après une étude menée par Norton. Source UD

Un groupement hospitalier des Hauts-de-France victime d'une cyberattaque.
Un groupement d'établissements hospitaliers situés dans les Hauts-de-France a été victime d'une cyberattaque, a-t-on appris vendredi auprès de la direction de la Fondation Hopale qui a décidé de ne pas ouvrir son centre de vaccination de Berck-sur-Mer (Pas-de-Calais) ce week-end. Source SN

Une attaque informatique cloue les téléservices de la CNIL ?
Nos petits yeux saignent ! Un message laconique sur le site de la Commission Nationale de l'Informatique et des Libertés annonce une cyberattaque à l'encontre de la grande dame de la protection de nos données personnelles. Source Zataz

Des pirates s'attaquent à un fleuron de la thérapie française.
Des pirates informatiques ont lancé une cyber attaque à l'encontre d'un des leaders européen des recherches sur les thérapies et traitements contre les troubles génétiques, le français Yposkesi. Des données ont commencé à fuiter. Source Zataz

Le centre de vaccination contre le Covid-19 de Berck-sur-Mer ferme à la suite d'une cyberattaque.
Le centre de vaccination contre le Covid-19 de Berck-sur-Mer est contraint de fermer à la suite d'une attaque informatique qui a touché son gestionnaire, la Fondation Hopale. La direction promet qu'aucun créneau de vaccination n'a besoin d'être reporté. Mais cette fermeture ralentit tout de même la campagne de vaccination, seule sortie de crise. Source UD

Cyberattaque à l'encontre du 1er acteur indépendant du tourisme français.
La société Marietton Développement face à une cyberattaque qui a permis aux pirates du groupe Babuk de mettre la main sur 140Gb des données internes sensibles. Source Zataz

Impôts : vagues de cyberattaques en France et dans le monde.
Pas de répit depuis le début d'année en matière de cybermenaces. Les attaquants sont à l'affût et continuent d'exploiter des leurres liés à l'actualité afin de cibler les utilisateurs par le biais de campagnes de mails malveillants. Source UnderNews

Hausse de 73 % de l'utilisation des logiciels espions depuis le début du confinement en France.
Avast, spécialiste mondial des produits de sécurité et de la confidentialité en ligne, révèle que l'utilisation des logiciels espions (spywares et stalkerwares) a augmenté en janvier et février. Ces applications sont des logiciels de localisation contraires à l'éthique. Source UnderNews

La fondation santé des étudiants de France victime d'un ransomware.
En fin de semaine dernière, la FSEF qui gère un réseau de 13 cliniques françaises prodiguant des soins pour jeunes a été touchée par un rançongiciel. La reconstruction du SI est en cours et son rétablissement devrait intervenir d'ici quelques jours. Source LMI

Recrudescence de cryptolocker, nouveau Ransomware dans le secteur médical.
[Par Stéphane Astier et Anne-Charlotte Andrieux] - Vingt-sept cyberattaques ont ciblé des hôpitaux français en 2020, et environ une attaque par semaine est recensée depuis le début de l'année 2021. Source HAAS Avocats

Cyberdéfense

Levée de la mise sous observation des produits Stormshield.
L'ANSSI avait décidé le 4 février 2021 de placer les qualifications et agréments des produits SNS et SNI de Stormshield sous observation pour la durée des investigations. Source ANSSI – ANSSI – ANSSI

Le Conseil de l'Economie et de l'Information du Digital (CEIDIG) édite un nouveau guide pour les dirigeantes et dirigeants.
Le CEIDIG publie, ce jeudi 1er avril 2020, le guide « L'essentiel de la sécurité numérique pour les dirigeantes et les dirigeants – 2e édition » issu d'une collaboration inédite d'experts du monde numérique, de grandes entreprises et de partenaires institutionnels. La soirée de lancement sera l'occasion pour Guillaume Poupard de présenter les grands enjeux de la cybersécurité pour les membres du comité exécutif des entreprises. Source ANSSI – CEIDIG – Cigref

L'État s'attaque-t-il vraiment aux cybercriminels ?
La table-ronde organisée le 15 avril à Paris par le Sénat a mis en lumière les moyens importants, bien qu'encore assez faibles, déployés par l'État pour prévenir et combattre la cybercriminalité visant les entreprises, et tout particulièrement les plus vulnérables, les PME et les collectivités locales. Source SN

La cybersécurité, variable d'ajustement pour les décideurs ?
[par Mounir Chaabane – Conférencier Sécurité et Stratégie IT]
L'amorce d'un changement de ton pour faire du sujet un traitement non-négociable ? Source Alliancy

Collectivités territoriales : face à la menace, saisissez-vous des enjeux cyber.
Alors que la menace cyber est plus importante que jamais, les collectivités territoriales sont les cibles privilégiées des attaques cyber. Un cadre réglementaire leur impose la mise en place de différentes mesures destinées à sécuriser leurs systèmes d'information, leurs services numériques, et à protéger les données à caractère personnel de leurs administrés. Une infographie réalisée par Camille Dubedout, doctorante à l'ANSSI, et Valentin Schabelman, doctorant chez Examin, permet de saisir les contours de ce cadre juridique. Source ANSSI – ANSSI

Atos et l'Inria concluent un accord d'envergure dans le domaine de la recherche.
Atos et l'Inria viennent de conclure un partenariat stratégique pour répondre aux besoins des acteurs industriels de demain. Source ZDNet

Évolutions concernant les processus de certification de sécurité.
Conscient de l'évolution rapide et constante des menaces, le centre de certification national au sein de l'ANSSI propose maintenant un processus permettant de garantir, de manière continue, la sécurité des produits certifiés selon les Critères Communs. Source ANSSI

II – Actualités

Brèves

Cybersécurité

Le nouveau rapport de Bitdefender met en lumière les principales cybermenaces mondiales.
Bitdefender publie son Rapport 2020 sur le paysage des menaces ciblant les particuliers, présentant les principales menaces de cybersécurité, leur fréquence et les tendances en matière de cybercriminalité en 2020. Source GlobalSecurityMag

Tous les œufs dans le même panier ? 44 % des entreprises ont une équipe sécurité dédiée au sein de leur département informatique.
Pour la moitié (52 %) des entreprises interrogées dans le cadre de l'étude IT Security Economics de Kaspersky, leur département informatique bénéficie d'une équipe dédiée à la cybersécurité. Pourtant seules 20 % des entreprises disposent d'un centre opérationnel de sécurité (SOC) interne chargé de la surveillance et de la réponse aux incidents de sécurité. Le développement de l'expertise en cybersécurité en interne arrive en deuxième position lorsqu'on évoque les raisons qui les pousseront à augmenter le budget dédié la sécurité informatique au cours des prochaines années. Source GlobalSecurityMag

Détection et restauration des données : les éléments indispensables d'une cybersécurité efficace.
Les conséquences des attaques très médiatisées comme les rançongiciels ont de quoi donner quelques sueurs froides aux responsables de la sécurité informatique. Le risque d'être victime de ces attaques ne fait que croître, car les cybercriminels multiplient les tentatives et développent des méthodes de plus en plus sophistiquées. Source Silicon

La Formule 1, une vitrine technologique… et une vitrine cybercriminelle.
Dimanche 28 mars, l'extinction des feux du Grand Prix de Bahreïn a lancé la saison 2021 de F1. L'occasion pour la catégorie reine du sport automobile de faire montre de la véritable vitrine technologique qu'elle est devenue pour l'industrie automobile. Pourtant, cette rentrée des classes ne s'est pas effectuée sans heurts, loin de là, car la technologie omniprésente en F1 peut se retourner contre elle. Trois des 10 équipes de F1, que sont Williams, Aston Martin et Ferrari ont en effet été piratées au mois de février, avant le lancement de leurs nouvelles voitures, mettant en évidence la vulnérabilité et la technologie de pointe de ceux qui sont prêts à mener de telles attaques. Source GlobalSecurityMag

Êtes-vous sûr de la sécurité de ce QR code ?
[par Bastien Bobe Security Sales Engineer Europe du Sud chez Lookout]
Alors que les entreprises tentent de créer une expérience sans contact dans le contexte de la pandémie de coronavirus, beaucoup se sont tournées vers les QR codes. Nous voyons beaucoup de restaurants les utiliser pour afficher leurs menus sur les smartphones et sur les reçus pour une option de paiement sans contact. Source GlobalSecurityMag

Les cyberattaques perpétrées par les États-nations ont doublé en trois ans, d'après une étude.
Les cyberattaques menées par les acteurs étatiques explosent, rapporte le criminologue Mike McGuire dans une étude réalisée pour le compte de HP. Ainsi, en seulement trois ans, elles ont été multipliées par deux. Les entreprises à forte valeur ajoutée sont les premières victimes de ces campagnes malveillantes. Si l'adoption d'un traité international semble être l'une des solutions les plus séduisantes pour y remédier, elle se heurte cependant à la réalité du terrain. Source UD – SN

Le secteur bancaire a connu une recrudescence d'attaques informatiques en 2020.
Depuis un an maintenant, le télétravail a réinventé la donne et a drastiquement complexifié la sécurité des systèmes informatiques, tous secteurs confondus. Désormais sur un système ouvert, l'infrastructure est fragilisée et le secteur bancaire a dû faire face à un nombre exponentiel de cyberattaques dès le premier confinement. Source UnderNews

Les États-Unis restent la principale cible des cyberattaques.
Selon les agences de renseignement américaines, au cours des prochaines décennies, des groupes de pirates soutenus par des États-nations vont passer de plus en plus à l'action. Avec à la clé une hausse des cyberattaques, campagnes de désinformation et de cyberespionnage, ainsi que des vols de propriété intellectuelle. Source LMI

60 % des établissements scolaires ont été victimes d'attaques de phishing visant les données du cloud.
Fournisseur de cybersécurité qui simplifie la sécurité des données, Netwrix a publié son rapport mondial 2021 sur la sécurité des données dans le cloud pour le secteur de l'éducation. Source IT Social

Cybersécurité de l'industrie

Retail, administrations, industries critiques peinent à sécuriser leur cloud durant la pandémie.
La pandémie actuelle a causé la plus grande migration vers le travail à distance de l'histoire. Un peu partout dans le monde, les entreprises ont œuvré pour migrer rapidement vers le cloud et sécuriser les accès de leurs employés travaillant à domicile. Aujourd'hui, l'Unit 42 (l'unité de recherche sur la cybercriminalité de Palo Alto Networks) dévoile une nouvelle étude qui montre comment la montée en puissance de l'adoption du cloud a créé des failles de sécurité facilitant l'augmentation des cyberattaques l'année passée. Source GlobalSecurityMag

Cybersécurité et empreinte carbone : une relation encore difficile.
Qu'en est-il de l'empreinte carbone dans nos entreprises ? Quel est l'impact de l'informatique et de la cybersécurité sur cette empreinte, et surtout quel impact a pu avoir le récent passage au télétravail d'une grande partie de la population ? Source Silicon

Schneider Electric appelle à transformer l'industrie avec l'« Universal Automation ».
Transformer le secteur industriel avec le lancement d'une technologie ouverte et durable EcoStruxure™ Automation Expert, fondée sur la norme IEC61499. Source GlobalSecurityMag

Les entreprises prévoient d'investir dans l'automatisation et les systèmes de sécurité enfouis.
Le domaine de la cybersécurité est un espace où l'évolution des techniques de guérilla signifie que les entreprises ne savent pas où vont frapper les attaquants. Logiciel, matériel ou micrologiciel, les entreprises entendent sécuriser les trois, avec toutefois une priorité pour le logiciel. Source IT Social

Sécurité numérique

Sauvegarde des données fichiers à grande échelle : Trois conseils clés.
[par Vincent Gibert, Sales Manager France chez Qumulo]
Que ce soit face à l'accélération des attaques ransomwares et des cybermenaces en général, ou pour parer à tout incident impliquant les installations, la reprise après sinistre et la continuité des activités sont plus que jamais d'actualité. Source GlobalSecurityMag

La sauvegarde des données ne doit plus être une option.
Selon une étude réalisée par Vanson Bourne pour Veeam, 58 % des sauvegardes informatiques échouent, mettant en danger le patrimoine data. Source LMI

Des droits d'accès mal gérés dans le secteur de la santé.
Dans une étude réalisée in situ par Varonis, le prestataire a montré combien les droits d'accès aux données sensibles étaient excessifs dans la santé. Source LMI

4 points essentiels pour rehausser le niveau de cyber-protection des professionnels de santé.
[par Laurent Ostrowski – Responsable Digital Workspace chez Cegedim Outsourcing]
La recrudescence des cyberattaques que subissent les professionnels de santé depuis maintenant plus d'un an est fortement préoccupante. 475 %, c'est le bond des cyberattaques ciblant les hôpitaux depuis le début de la crise de la Covid-19 soit 5 fois plus qu'habituellement (Source Stormshield.) et 60 % des signalements des établissements de santé, du service santé des armées (SSA) et établissements médico-sociaux portaient sur des incidents d'origine malveillante (Source ANS). Source GlobalSecurityMag

Prenez 2 minutes pour activer la double authentification sur votre compte LinkedIn.
Votre compte LinkedIn est votre carte de visite professionnelle, protégez-le. Source Numerama

Trois conseils pour protéger les réseaux en 2021.
Face à cette multiplication des risques, les entreprises doivent répondre à plusieurs défis afin de protéger leurs réseaux. Source IT Social

8 DSI sur 10 estiment qu'il est essentiel de maintenir la sécurité et le contrôle les applications des utilisateurs.
Un rapport de Cisco identifie les priorités essentielles des services informatiques : se concentrer sur la sécurité et la collaboration en mode hybride, offrir la meilleure expérience à l'utilisateur final, favoriser l'innovation et la sécurité dans un monde où le cloud est roi. Source IT Social

WiFi : vers une surveillance sans fil tous azimuts en 2025 ?
L'Institute of Electrical and Electronics Engineers (IEEE) travaille sur une norme qui pourrait permettre au WiFi de suivre les utilisateurs à travers les murs, et jusqu'à tout ce qu'il tape sur son clavier.
Source LMI – Reseaux-Telecoms

Rapport d'activité 2020 de Cybermalveillance.gouv.fr : le nombre de recherches d'assistance par les entreprises sur les ransomwares a progressé de 30 %.
La plateforme gouvernementale d'aide aux particuliers et petites entreprises cybermalveillance.gouv.fr vient de dévoiler son rapport d'activité 2020. En 2020, le nombre de recherches d'assistance d'entreprises ou d'administrations sur cette menace a progressé de 30 %.
Source SN – cybermalveillance – LMI – UnderNews

"La page des toqués des tic, quelques réflexions sur les termes informatiques".
[par Cédric CARTAU, RSSI & DPO, CHU de Nantes, GHT44]
La cybersécurité est pleine d'acronymes et de termes anglais, qui rendent cette discipline déjà vue comme très technique, encore plus nébuleuse et réservée à des initiés… D'où l'idée qu'utiliser des termes français la rendrait plus accessible… Las… cet exercice se révèle parfois contre – productif… voire franchement ridicule… Source CyberCercle

Photos, fichiers, messages… : comment protéger ses données numériques grâce aux sauvegardes ?
Vous est-il déjà arrivé de vous faire voler un appareil dans lequel étaient stockés toutes vos photos ou contacts ? Ou d'endommager la clé USB contenant l'unique copie d'un fichier sur lequel vous avez longuement travaillé ? Ou pire, d'oublier votre ordinateur portable ou téléphone dans un lieu public, perdant ainsi l'intégralité des documents qu'ils contiennent ? Des situations pénibles, frustrantes, voire critiques selon les contextes, d'autant plus lorsqu'elles auraient pu être évitées grâce à la sauvegarde des données. Source cybermalveillance – cybermalveillance

Le modèle Zero Trust.
Le modèle Zero Trust exerce un attrait croissant, car il est promu comme une garantie d'accès sécurisé aux ressources informatiques dans les contextes d'usages mixtes (télétravail, BYOD/AVEC) et fait l'objet d'un engouement de la part d'éditeurs de solutions technologiques et de sécurité qui y voient la perspective de nouveaux gains. Or, à ce jour, le recours à ces solutions est ardu, faute de maturité : le déploiement est susceptible d'entraîner des erreurs d'installation ou de configuration, d'accroître la vulnérabilité des systèmes d'information et de donner aux entreprises un faux sentiment de sécurité.
Source ANSSI – ANSSI

Recommandations pour une configuration sécurisée d'un pare-feu Stormshield Network Security (SNS) en version 3.7.17.
Ce document a pour objectif de présenter les bonnes pratiques relatives à la sécurisation des pare-feux Stormshield Network Security (SNS), en version physique ou en version virtuelle. Source ANSSI – ANSSI

Sûreté

Le slicing 5G pourrait exposer à de sérieuses failles de sécurité.
Des manquements dans les étapes de validation de la sécurité dans le découpage du réseau 5G exposent à un risque grave de violations de la vie privée et de la sécurité. Source LMI

Cybersécurité et 5G : quels enjeux ?
Véritable révolution de la mobilité digitale, la 5G va permettre le développement de nouveaux usages dans des domaines aussi divers que la santé, les transports, le divertissement et l'industrie. Mais ces nouveaux services vont indéniablement soulever des enjeux en matière de cybersécurité. Des défis sécuritaires se posent notamment pour les entreprises et les professionnels. Source Zataz

L'urgence de protéger efficacement les infrastructures électriques.
[par Stéphane Prevost chez Stormshield]
L'accélération fulgurante des cyberattaques contre les opérateurs de service, organisations et entreprises stratégiques est aujourd'hui une réalité préoccupante qui nécessite de prendre des mesures d'urgence pour se protéger. Source GlobalSecurityMag

Vulnérabilité critique sur Zoom : Exécution de code à distance.
Une vulnérabilité de type "zero-day" dans Zoom, qui peut être utilisée pour lancer des attaques par exécution de code à distance (RCE – remote code execution), a été révélée par des chercheurs en cybersécurité. Source ZDNet

IoT (objets connectés) / IA

100 millions d'objets connectés ont une de ces failles : les réparer toutes s'annonce impossible.
Des chercheurs ont découvert un lot de vulnérabilités qui permettraient à des criminels de prendre le contrôle d'une chaîne de production ou de paralyser un hôpital. Ces failles ont déjà des correctifs, mais ils risquent de n'être déployés qu'à petite échelle. Source Numerama – Siècle Digital

Les appareils connectés sont aussi vulnérables : comment bien se protéger ?
La sensibilisation passe aussi par la prise de conscience que tout ce qui est connecté est potentiellement exposé et ainsi, les ordinateurs et les téléphones ne sont pas les seuls appareils à être vulnérables et à pouvoir fait l'objet d'une attaque. Source GlobalSecurityMag

Objets connectés en pratique sportive de plein air : des compagnons à choyer !
[par Benoit Grunemwald Expert en Cyber sécurité, ESET France]
Devenus nos meilleurs amis lors de nos pratiques sportives de plein air, les objets connectés (IoT) figurent également parmi les plus perméables aux cyber-attaques. Gros plan sur les bons réflexes à avoir.
Source GlobalSecurityMag

LOGICIELS MALVEILLANTS

Malware – Ransomwares

« Votre colis a été envoyé » : attention à ce SMS, il cache un malware.
Le phishing au colis est de retour. Mais cette fois, il embarque un malware capable de dépouiller votre compte bancaire. Source Numerama

Détection d'un Trojan dissimulé dans le Store de téléchargement d'applications Android, APKPure.
[APKPure est une alternative pour télécharger des applications Android]
Il est recommandé aux propriétaires d'appareils Android, ayant déjà installé l'application APKPure de la supprimer temporairement pour se débarrasser du Trojan. Source Zataz

Microsoft reste la marque la plus usurpée dans les tentatives de phishing au premier trimestre 2021.
Check Point® Software Technologies Ltd. publie son nouveau rapport de phishing des marques pour le premier trimestre 2021. Il met en évidence les marques les plus fréquemment imitées par les criminels pour essayer de voler les informations personnelles ou les identifiants de paiement des particuliers en janvier, février et mars. Source GlobalSecurityMag

Ce malware manipule les copier/coller pour détourner des cryptomonnaies.
Les victimes du malware Hack Boss pensent envoyer des cryptomonnaies vers l'adresse de leur choix, mais elle les envoie en réalité à des malfaiteurs. Source Numerama

Un rançongiciel menace d'organiser une spéculation à la baisse sur le cours des actions de ses victimes.
Toujours plus ! Un rançongiciel (ou ransomware) teste encore un nouveau levier pour mettre ses victimes sous pression. Source Numerama

ACTUALITES JURIDIQUES - Législation et jurisprudences

CNIL

Radars-tronçons : clôture de la mise en demeure du ministère de l'Intérieur.
Par décision du 25 mars 2021, la Présidente de la CNIL a décidé de procéder à la clôture de la mise en demeure du 12 novembre 2019 adressée au ministère de l'Intérieur. Source CNIL – Legifrance

Nouvelles règles pour les cookies et autres traceurs : bilan de l'accompagnement de la CNIL et actions à venir.
Le délai accordé pour mettre en conformité les sites et applications mobiles aux règles en matière de traceurs a pris fin le 31 mars 2021. La CNIL rappelle les éléments clés de la réglementation sur lesquels elle a focalisé ses efforts d'accompagnement pendant cette période et présente les actions à venir.
Source CNIL

Fuite de données Facebook : comment protéger vos données ?
Un fichier comprenant des données de près de 533 millions d'utilisateurs de Facebook, dont 20 millions de Français, est actuellement accessible sur internet. La CNIL rappelle quelques conseils pour limiter les conséquences pour vos informations personnelles. Source CNIL

Scènes de la vie numérique : la CNIL publie son 8e cahier Innovation & Prospective.
Des situations problématiques du quotidien aux chemins du droit, la CNIL explore, dans son nouveau cahier Innovation & Prospective, le rapport des personnes à la protection de leurs données et à leur vie privée. Source CNIL – CNIL

Quelles mutations dans le monde du travail?
Dans le cadre de sa mission éthique, la CNIL publie le cahier air 2020. Ce nouveau format éditorial synthétise les moments saillants du colloque air 2020, organisé en novembre dernier, en abordant les nouveaux rapports et les enjeux qui lient le travail aux technologies. Source CNIL – CNIL

Multiplication des attaques par rançongiciel : comment limiter les risques ?
Alors que les attaques par rançongiciel sont de plus en plus nombreuses, la CNIL rappelle quelques points de vigilance. Source CNIL – CNIL

◆ RGPD – (Règlement général sur la protection des données)

COVID-19 : le CEPD et le Contrôleur européen de la protection des données rendent un avis sur la proposition de certificat vert numérique.
Le Comité européen de la protection des données et le Contrôleur européen de la protection des données ont publié, le 6 avril 2021, un avis conjoint sur la proposition de règlement relatif au certificat vert numérique (Digital Green Certificate) de la Commission européenne. Il revient sur les garanties que ce dispositif doit apporter pour les droits et libertés fondamentaux des personnes. Source CNIL

La Cnil irlandaise poursuit Facebook pour sa fuite de données concernant 533 millions de personnes.
La Data Protection Commission (DPC) ouvre une enquête sur la fuite de données qui a touché 533 millions utilisateurs Facebook. Elle souhaite savoir si les obligations du RGPD ont été respectées par l'entreprise américaine qui est qualifiée de responsable de traitement au sens de ce texte. Si tel n'est pas le cas, elle risque une amende pouvant aller jusqu'à 4 % de son chiffre d'affaires. Source UD

Clubhouse : les données de 1,3 million d'utilisateurs en accès libre.
Le document contient le nom d'utilisateur, la date de création du compte, l'URL de la photo, le nombre d'abonnés et d'abonnements, mais également les comptes Twitter et Instagram reliés à un profil Clubhouse. Source Siècle Digital

Les Clubs Utilisateurs SAP et Oracle publient une série de Fiches Réflexes autour du RGPD.
Afin de continuer à accompagner les utilisateurs de progiciels dans leur mise en application du RGPD, les clubs utilisateurs des solutions Oracle (AUFO – Association des Utilisateurs Francophone d'Oracle, Groupe Francophone des Utilisateurs J.D. Edwards, et Club des Utilisateurs PeopleSoft), et l'USF (Utilisateurs SAP Francophones), rédigent en commun et mettront à disposition de leurs membres, une série d'une dizaine de Fiches Réflexes pour les accompagner dans les actions à mener, les points de vigilance et les risques à éviter dans diverses situations. Source Alliancy – AUFOUSF – AUFOUSF

La CNIL va intensifier ses contrôles de conformité au RGPD, suite à l'entrée en vigueur des nouvelles règles sur les cookies.
Quelques jours après l'entrée en vigueur de nouvelles règles concernant les cookies traceurs, la CNIL menace de lourdes sanctions les entreprises qui ne s'y conforment pas. Source IT Social

Secteur social : le nouveau référentiel CNIL est publié.
[Par Stéphane Astier et Anne-Charlotte Andrieux]
L'objet de ce référentiel est de donner aux acteurs du secteur social des indications utiles et opérationnelles pour paramétrer leurs différents traitements métiers intégrant des données à caractère personnel. Nouvelle bible du Délégué à la Protection des Données (DPO) cette version définitive permet de souligner quelques modifications importantes. Source HAAS Avocats – CNIL – Legifrance

AIPD : vers la fin de la période de tolérance.
[Par Gérard Haas et Amanda Dubarry]
Depuis le 25 mai 2018, date de l'entrée en application du règlement général sur la protection des données (RGPD), les organismes mettant en place des traitements de données dits « à risque » doivent réaliser une analyse d'impact sur la vie privée (AIPD) Cette nouvelle obligation sera pleinement effective pour les traitements précédents l'entrée en application du règlement au 24 mai 2021. La CNIL avait en effet accordé aux responsables de traitement une période de tolérance de 3 ans afin qu'ils puissent se mettre en conformité. Source HAAS Avocats – CNIL

◆ Droit des TIC

La CNIL précise les garanties que doit respecter la fonctionnalité TousAntiCovid-Carnet.
La nouvelle fonctionnalité « carnet », intégrée à l'application TousAntiCovid, permet de stocker les certificats de résultats de test et, très prochainement, de vaccination afin de « favoriser les déplacements nécessitant un contrôle sanitaire […] notamment lors des passages aux frontières ». La CNIL est vigilante quant à son déploiement afin que les garanties pour les personnes soient respectées. Source CNIL

Quels experts pour la protection des données ?
Depuis les attaques de l'administration estonienne de 2007, les entreprises et administrations du monde entier font face à des effractions d'un nouveau genre, les cyber attaques. Pour assurer la sécurité optimale des données, il est important de mutualiser les compétences des experts en cybersécurité et des professionnels de la protection des données qui sont de plus en plus recherchés sur le marché du travail.
Source Siècle Digital

Détournement de données par une entreprise concurrente : que faire ?
[Par Gérard Haas et Marie Torelli]
Qu'il s'agisse des méthodes, des techniques, des procédés ou des algorithmes, de nombreux éléments composant le savoir-faire des entreprises ne sont pas susceptibles d'être protégés par le droit d'auteur. Pourtant, ils constituent des actifs immatériels présentant des enjeux cruciaux pour les entreprises.
Source HAAS Avocats

La difficile levée d'anonymat sur internet.
[Par Pierre Roquefeuil, Avocat.]
L'anonymat sur Internet pose depuis longtemps question. Au début d'internet, cet anonymat était plutôt vécu comme une nouvelle liberté, chacun pouvant désormais s'exprimer sans contrainte, avec une audience potentiellement illimitée. Source Village de la Justice

Juridique

La CEDH précise le droit à la liberté d'expression de l'employeur.
[Par Kate Jarrard et Jean Edouard Poux]
Dans un arrêt rendu le 25 mars dernier, la Cour européenne des droits de l'homme (CEDH) estime que la condamnation à une peine d'emprisonnement avec sursis pour diffamation d'un employeur envers une ancienne salariée est contraire à l'Article 10, relatif à la liberté d'expression, de la Convention européenne de sauvegarde des Droits de l'homme et des Libertés fondamentales. Source HAAS Avocats – CEDH

Non-respect d'une licence : quel fondement juridique ?
[Par Claudia Weber et Céline Dogan, Avocats.]
Question régulièrement débattue depuis plusieurs années : en cas de violation d'un contrat de licence portant sur un droit de propriété intellectuelle, le titulaire du droit peut-il agir en contrefaçon (responsabilité délictuelle) ou doit-il agir en responsabilité contractuelle ? Source Village de la Justice

Photographies et droits d'auteur.
[Par Philippe Bessis, Avocat]
La Cour d'Appel de Versailles, dans un arrêt du 30 mars 2021 statue sur le droit d'auteur en matière photographique. Source Village de la Justice

Législation

Le Conseil d'État recale l'interconnexion de GendNotes à des fichiers tiers.
Le projet du ministère de l'Intérieur d'interconnecter l'application de prise de notes utilisée par la Gendarmerie Nationale sur le terrain avec des fichiers tiers a du plomb dans l'aile. En tout cas jusqu'à des précisions de finalité de traitement qui sont pour l'instant aussi floues que fourre-tout.
Source LMI – Legalis – Legalis

"Souveraineté numérique : passer du discours aux actes".
[par Catherine MORIN-DESAILLY, sénatrice de la Seine-Maritime]
La souveraineté numérique est au cœur de la réflexion de l'État, que ce soit au niveau du Parlement ou de l'exécutif – rapports parlementaires parus ou en cours, plan de relance cybersécurité, perspectives de la présidence française de l'Union européenne – et de l'Union européenne – DMA, DSA portés avec volontarisme par Thierry BRETON. Source CyberCercle

Des algorithmes contre le terrorisme.
Un nouveau texte de loi sur l'anti-terrorisme est dans les cartons du ministère de l'Intérieur et prévoit d'actualiser et de pérenniser le traitement automatisé des données de connexion par la DGSI.
Source L'1FO

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

Référence	Titre	Date
CERTFR-2021-AVI-331	Multiples vulnérabilités dans Microsoft Edge	(30 avril 2021)
CERTFR-2021-AVI-330	Multiples vulnérabilités dans PHP	(30 avril 2021)
CERTFR-2021-AVI-329	Multiples vulnérabilités dans le noyau Linux de SUSE	(30 avril 2021)
CERTFR-2021-AVI-328	Vulnérabilité dans Samba	(29 avril 2021)
CERTFR-2021-AVI-327	Multiples vulnérabilités dans F5 BIG-IP	(29 avril 2021)
CERTFR-2021-AVI-326	Multiples vulnérabilités dans Cisco ASA et FTD	(29 avril 2021)
CERTFR-2021-AVI-325	Multiples vulnérabilités dans BIND	(29 avril 2021)
CERTFR-2021-AVI-324	Multiples vulnérabilités dans le noyau Linux de Red Hat	(28 avril 2021)
CERTFR-2021-AVI-323	Vulnérabilité dans le noyau Linux de SUSE	(28 avril 2021)
CERTFR-2021-AVI-322	Multiples vulnérabilités dans GitLab	(28 avril 2021)
CERTFR-2021-AVI-321	Vulnérabilité dans Citrix ShareFile storage zones controller	(28 avril 2021)
CERTFR-2021-AVI-320	Vulnérabilité dans Fortinet FortiWAN	(28 avril 2021)
CERTFR-2021-AVI-319	[SCADA] Multiples vulnérabilités dans Moxa NPort	(28 avril 2021)
CERTFR-2021-AVI-318	Multiples vulnérabilités dans Zimbra	(27 avril 2021)
CERTFR-2021-AVI-317	Multiples vulnérabilités dans Google Chrome	(27 avril 2021)
CERTFR-2021-AVI-316	Vulnérabilité dans Kaspersky Password Manager	(27 avril 2021)
CERTFR-2021-AVI-315	Multiples vulnérabilités dans IBM DB2	(27 avril 2021)
CERTFR-2021-AVI-314	Multiples vulnérabilités dans les produits Apple	(27 avril 2021)
CERTFR-2021-AVI-313	Multiples vulnérabilités dans Stormshield Management Center	(26 avril 2021)
CERTFR-2021-AVI-312	Multiples vulnérabilités dans le noyau Linux de Red Hat	(26 avril 2021)

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

Référence	Titre	Date
CERTFR-2021-ALE-007	Vulnérabilité dans Pulse Connect Secure	Alerte en cours le 20/04/2021
CERTFR-2021-ALE-006	Vulnérabilité dans F5 BIG-IP	Clôturée le 15/04/2021
CERTFR-2021-ALE-005	Multiples vulnérabilités dans Microsoft DNS server	Alerte en cours le 12/03/2021
CERTFR-2021-ALE-004	Multiples vulnérabilités dans Microsoft Exchange Server	Alerte en cours le 03/03/2021
CERTFR-2021-ALE-003	Vulnérabilité dans VMWare vCenter Server	Alerte en cours le 25/02/2021

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

Référence	Date
CERTFR-2021-ACT-016	(26 avril 2021)
CERTFR-2021-ACT-015	(19 avril 2021)
CERTFR-2021-ACT-014	(12 avril 2021)
CERTFR-2021-ACT-013	(06 avril 2021)
CERTFR-2021-ACT-012	(29 mars 2021)

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

Référence	Titre	Date
CERTFR-2021-IOC-002	Campagne d'attaque du mode opératoire Sandworm ciblant des serveurs Centreon	(15 février 2020)
CERTFR-2021-IOC-001	Infrastructure d'attaque du groupe cybercriminel TA505	(10 février 2020)
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)

- **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-2021-CTI-004	Campagne d'attaque du mode opératoire Sandworm ciblant des serveurs Centreon	(15 février 2020)
CERTFR-2021-CTI-002	Infrastructure d'attaque du groupe cybercriminel TA505	(10 février 2020)
CERTFR-2021-CTI-001	État de la menace rançongiciels à l'encontre des entreprises et institutions	(05 février 2020)
CERTFR-2020-CTI-012	Le rançongiciel Egregor	(18 décembre 2020)
CERTFR-2020-CTI-011	Le rançongiciel Ryuk	(30 novembre 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	78.10.0 ESR			
	Antérieures	CERTFR-2021-AVI-287	Mfsa2021-16	2021_04_23
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	5.6.3			
McAfee ViruScan	8.8.0.P7			
7-zip	19.00			
	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-2021-AVI-055	sb-vlc3012	

	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***

♦♦♦♦