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°67

Pôle Défense et Sécurité des Systèmes d'Information

Notes d'information technique

Edition ► Mars 2021

I – Cybercriminalité et attaques informatiques

Dans le MONDE

Après une cyberattaque sur SITA, des données voyageurs compromises.
[SITA – acronyme de société internationale de télécommunication aéronautique]
Les informations de passagers de plusieurs compagnies aériennes ont été compromises après la cyberattaque de SITA. Cette dernière gère la fourniture de services à l'industrie aéronautique dont les centres de réservation. Source LMI – ZDNet – Globb Security

L'enseigne GUESS en prise avec des pirates. Les données du patron dans les mains des voyous 2.0.
[la société américaine Guess est une entreprise spécialisée dans la mode]
L'information est restée très discrète. Mi-février, l'entreprise de mode Guess tombait sous les coups d'une cyberattaque. Un mois plus tard, plusieurs dizaines de milliers de documents volés sont diffusés. Source Zataz

Le géant de l'informatique ACER aux prises avec des pirates informatiques.
Le groupe pirate d'opérateurs du ransomware Sodinokibi s'attaque au géant taiwanais Acer. Les premières données volées ont fuité. Source Zataz

Shell révèle une fuite de données touchant ses actionnaires.
Les informations concernant des actionnaires ont été compromises dans cette fuite de données, l'exploitation d'une faille de sécurité dans la solution Accellion FTA aurait été à l'origine de l'attaque. Source ZDNet

Une attaque par ransomware interrompt la production chez Sierra Wireless, fabricant d'objets. connectés. Les systèmes internes sont toujours hors service à la suite d'une attaque par ransomware, mais les produits des clients n'ont pas été affectés, selon la société. Source ZDNet

38 élus allemands sont victimes d'un piratage par des cyberespions russes.
L'opération Ghostwriter, orchestrée par une branche du renseignement russe, aurait fait de nouvelles victimes. Des parlementaires allemands sont victimes d'une campagne de cyberespionnage. Source Numerama

En FRANCE

Cybersécurité

L'ANSSI alerte sur un variant du ransomware Ryuk.
L'ANSSI a révélé l'existence d'un variant du rançongiciel Ryuk particulièrement dangereux. Il peut se copier automatiquement à d'autres terminaux reliés aux réseaux locaux auxquels le système cible est connecté. Source LMI – ANSSI

Découverte d'une fuite de près de 2 millions d'identifiants de connexion de Français.
Un pirate met à disposition une base de données de près de 2 millions d'identifiants de connexion. L'ensemble des mots de passe présents sont en clairs. Source Zataz

Réaction tardive, 28 laboratoires… On en sait plus sur la fuite de données d'un demi-million de patients. La fuite de données de santé d'un demi-million de patients concerne 28 laboratoires d'analyse biologique situés en Bretagne, Centre-Val-de-Loire et Normandie. Source UD

Le géant laitier Lactalis est victime d'une attaque informatique.
« Un tiers malveillant » a tenté de pénétrer dans les serveurs de Lactalis. Une enquête interne a été ouverte et les autorités compétentes ont été notifiées de cette attaque. Aucune donnée n'aurait été dérobée lors de cette intrusion, rassure le groupe français de produits laitiers. Source UD

L'hôpital d'Oloron Sainte-Marie victime d'un ransomware.
Après Dax, c'est au tour du centre hospitalier d'Oloron Sainte-Marie dans les Pyrénées Atlantique également en région Nouvelle Aquitaine, d'être la cible d'une cyberattaque. Un rançongiciel a paralysé les systèmes d'information et une rançon de 50 000 dollars demandée.
Source LMI – ZDNet – UD – Globb Security – UnderNews

Que peuvent faire les malfaiteurs avec votre numéro de sécurité sociale ?
Le numéro de sécurité sociale est une de vos données personnelles les plus précieuses, mais savez-exactement pourquoi ? Source Numerama

Le gouvernement promet de soutenir OVHcloud, après l'incendie de son centre de données.
Le gouvernement « continuera de soutenir » OVHcloud, le groupe français de cloud dont un centre de données a brûlé la semaine dernière avec des conséquences potentiellement lourdes pour certains clients, a-t-il indiqué. Source SN – Reseaux-Telecoms

Les pompiers du Calvados victimes d'une cyberattaque.
Le service départemental d'incendie et de secours (SDIS) du Calvados a été victime d'une cyberattaquela semaine dernière, sans conséquence sur le travail des sapeurs-pompiers. Source L'1FO

La France est dans le top 10 des pays qui ont connu le plus de cyberattaques en 2020, d'après le FBI. Le FBI dévoile son étude annuelle sur l'état de la cybersécurité aux Etats-Unis. Le nombre de plaintes déposées par des victimes de cybercrimes a presque doublé et le phishing est l'attaque la plus répertoriée. À l'échelle internationale, la France figure à la septième place dans le top 20 des pays par nombre total de victimes. Source UD

En France, environ 15 000 serveurs ont été exposés aux failles de Microsoft Exchange. D'après l'ANSSI, près de 15 000 serveurs informatiques exploités par des entreprises françaises ont été exposés aux failles de Microsoft Exchange, révélées il y a quelques semaines. Il y a cependant très peu de victimes avérées, précise l'autorité française, qui recommande très fortement de faire les mises à jour. Source UD – ZDNet – Siècle Digital

Une base de données d'enseignants de Télécoms Sud Paris revendue dans le black market. Un pirate commercialise, quelques euros, une base de données d'enseignants de Télécoms Sud Paris. Source Zataz

Découverte d'une base de données de plus de 360 000 français Identités, adresses, téléphones ! ZATAZ constate une base de données de plus de 360 000 français de la région de Toulouse. Ne vous étonnez plus d'être appelé par des malveillants ! Source Zataz – Zataz

Les données personnelles de 363 770 habitants de Haute-Garonne sont en libre accès sur Internet. Les noms, prénoms, adresses postales et numéros de téléphone de 363 770 habitants de Haute-Garonne sont en libre accès sur le dark net. Cette base est utilisée par Distrix, une entreprise spécialisée dans les campagnes de distribution de prospectus. Mais d'après son dirigeant, cette fuite est de la faute de son hébergeur, dont il n'a pas divulgué l'identité. L'ANSSI a été saisie du dossier. Source UD

Défiguration du site Internet de la Mairie d'Altkirch (68). Source Zone-H

Cyberdéfense

L'État accélère 3 chantiers numériques dont FranceConnect. Un point d'étape a été présenté sur la simplification des démarches administratives en ligne, l'équipement des agents publics et les objectifs d'ouverture et de souveraineté des données. La plateforme FranceConnect pour sécuriser la connexion aux services s'étend en mars à Pôle Emploi et en juillet à la CAF. La question du choix des technologies cloud est aussi posée. Source LMI

le Cigref et Kaspersky répondent à l'Appel de Paris. Le Cigref et Kaspersky co-président un groupe de travail de l'Appel de Paris consacré au renforcement de la sécurité et de la stabilité du cyberespace. L'Appel de Paris « pour la confiance et la sécurité dans le cyberespace » a été lancé le 12 novembre 2018 par le chef de l'Etat français, Emmanuel Macron. L'Appel est devenu depuis une initiative multipartite soutenue par 1 100 acteurs publics et entités privées. Source Silicon – Appel de Paris

Le ministère des Armées en renfort de cybermalveillance.gouv.fr. La plateforme Cybermalveillance.gouv.fr a annoncé la signature d'un partenariat avec le ministère des Armées. L'objectif est de renforcer les liens entre la plateforme et les entreprises du secteur de la défense, en comptant sur l'aide de la direction du renseignement et de la sécurité de la défense. Source ZDNet

La gendarmerie se dote d'un commandement dans le cyberespace. Au Journal Officiel, un arrêté intègre dans la liste des formations administratives de la gendarmerie nationale un commandement dans le cyberespace. Cette création vise à une meilleure coordination des missions de la gendarmerie dans ce domaine. Source LMI

Le gouvernement veut renforcer la sécurité informatique des collectivités, des hôpitaux et des ports. « Mieux prévenir, protéger et faire face ». Voici l'objectif fixé par le gouvernement pour lutter contre les intrusions malveillantes dans trois types de structures : les collectivités territoriales, les établissements de santé et les infrastructures portuaires. Un appel à manifestation d'intérêt vient d'être lancé pour trouver des solutions « innovantes ». Dans le cadre de ce dispositif, l'État prendra en charge jusqu'à 50 % des investissements engagés. Source UD

Quelle stratégie française pour faire face aux cyberattaques ? [par Christophe Corne, le PDG de Systancia] - L'éditeur d'une plateforme d'accès aux applications d'entreprises, de gestion des identités et des accès (IAM), etc., évoque le rôle de l'État pour optimiser la cybersécurité des entreprises privées et publiques. Source SN

L'ANSSI et la DGEFP, en collaboration avec l'AFPA, lancent une enquête sur les professionnels de la cybersécurité. Qui sont les professionnels de la cybersécurité ? Parcours, missions, secteur d'activité, vision du métier, accès à la formation, perspectives d'évolution, etc. autant d'éléments mal connus et pourtant essentiels pour accompagner le développement de l'écosystème cyber. L'objectif du questionnaire proposé par l'ANSSI, la Délégation générale à l'Emploi et à la Formation professionnelle (DGEFP) et l'Agence nationale pour la formation professionnelle des adultes (AFPA) est de recueillir ces informations directement auprès des premiers intéressés afin d'en restituer, in fine, une vision synthétique et globale, au bénéfice de tous. Source ANSSI – ANSSI

L'ANSSI renforce la responsabilité des acteurs privés aux côtés de l'OCDE.
Le groupe de travail sur la sécurité dans l'économie numérique (GTSEN), présidé par Yves Verhoeven, sous-directeur Stratégie au sein de l'ANSSI, vient de rendre publics deux rapports visant à mieux définir la responsabilité des acteurs privés dans le cyberespace (Appel de Paris), afin d'en renforcer sa stabilité. Source ANSSI – ANSSI

FRANCE RELANCE et cybersécurité – Protéger l'État et les collectivités territoriales.
Dans le cadre du plan France Relance, l'ANSSI bénéficie d'une enveloppe de 136 millions d'euros pour renforcer la cybersécurité de l'État et des territoires sur la période 2021-2022. L'objectif est d'élever durablement le niveau de cybersécurité de l'État, des collectivités et des organisations au service des citoyens, tout en développant le tissu industriel français de cybersécurité. Source ANSSI – ANSSI

II – Actualités

Brèves

Cybersécurité

Les hackers de SolarWinds ont au moins 5 malwares exclusifs dans leur arsenal.
FireEye a identifié un cinquième malware utilisé par le groupe de hackers qui a compromis SolarWinds. Nommé Sunshuttle, il sert à installer des portes dérobées chez les victimes. Source Numerama – Numerama

Comment l'agence européenne du médicament a-t-elle été piratée ?
En décembre, l'Agence européenne du médicament se déclarait victime d'une cyberattaque. Les hackers auraient réussi une campagne de phishing, avant d'abuser d'un défaut dans la protection des emails de l'entreprise. Source Numerama

Pourquoi vous devriez vraiment vous intéresser aux cyberattaques contre Microsoft. Exchange.L'affaire Microsoft Exchange est la nouvelle crise de cybersécurité mondiale. Cyberguerre vous donne 4 clés pour comprendre son ampleur. Source Numerama

Des violations de données provoqueraient jusqu'à 223 milliards de dollars de perte pour les 100 premières marques mondiales.
Infosys et Interbrand, une société mondiale de conseils en matière de marques, ont révélé les résultats d'un rapport commun portant sur l'impact de la cybersécurité et la valeur des marques. Les 100 marques les plus valorisées pourraient ainsi perdre, en termes de valeur, jusqu'à 223 milliards de dollars en cas de violation de données. Source GlobalSecurityMag

Les 12 règles d'or pour la gestion de projets en cybersécurité.
[par Kumar MSSRRM, Vice Président adjoint en charge de la Distribution Cybersécurité, Infosys]
La cybersécurité est un domaine avec de fortes composantes technologiques. La gestion des projets et des programmes est essentielle à la bonne réussite de ces dits projets. Cependant, les outils de gestion de projet habituels doivent être ajustés au domaine de la cybersécurité, qui comporte intrinsèquement des exigences différentes, complexe par nature et qui implique des processus systématiques.
Source GlobalSecurityMag

Pourquoi le ransomware a-t-il toujours autant de succès ?
[par Nicolas Casimir, Zscaler] - Les attaques de ransomware se multiplient, le nombre de victimes ne cesse de croître. Cependant, les entreprises ont les moyens d'éliminer efficacement cette menace une bonne fois pour toutes. Source ZDNet

La moitié 50 % des PME ont subi une intrusion sur leur site web.
Dans un rapport sur la sécurité et les menaces à destination des PME, Sectigo, spécialiste américain de la cybertech, dévoile son rapport sur l'état de la sécurité des sites web et des cybermenaces.
Source IT Social

Le web et l'e-mail représentent 65 % des vecteurs d'attaque d'une PME.
Internet reste la porte d'entrée n°1 des cybercriminels pour pirater les PME, d'après une étude réalisée auprès de 23 000 PME sur janvier et février 2021 par OZON en partenariat avec WALLIX, Docaposte Arkhineo, Visiativ, Swiss Re Corporate Solutions et Croissanceplus. Source IT Social

Attaques de phishing : ces émotions qui nous poussent à cliquer sur les liens malveillants.
Alors que les utilisateurs sont de plus en plus avertis de la fraude par mail, ce type d'arnaque ne faiblit pas, et les cybercriminels continuent inlassablement de tendre leurs pièges. Source UnderNews

Applications : 1 utilisateur sur 4 leur autorise automatiquement l'accès à son micro ou à sa webcam. Près d'un utilisateur sur quatre autorise automatiquement l'accès à son micro ou webcam à ses applications, selon une étude Kaspersky. Source UnderNews

Tout comprendre aux failles Microsoft Exchange.
Début mars 2020, Microsoft alertait sur des failles zero-day exploitées sur son outil Microsoft Exchange. Voici un dossier complet pour mieux comprendre les menaces qui pèsent sur les clients professionnels, et les conséquences de cette attaque majeure. Source ZDNet – ZDNet – ZDNet – ZDNet – Numerama

31 millions de patients ont été affectés par un piratage.
Le baromètre des violations de Protenus montre que le secteur des soins de santé a combattu deux ennemis silencieux en 2020 : la COVID-19 et les cybermenaces. Ces dernières sont un impact sur des millions de dossiers de patients et d'autres informations de santé. Protenus note que de nombreux piratages, en 2020, découlaient davantage d'erreurs que d'intentions malveillantes… Source IT Social

Cybersécurité de l'industrie

L'industrie fortement touchée en 2020 selon IBM Security.
Dans son dernier rapport annuel des menaces cyber, IBM Security pointe un doublement des attaques contre les industriels, notamment ceux en première ligne contre la pandémie. Les attaques par ransomware contre les réseaux de l'industrie manufacturière sont en nette progression.
Source Industrie & Technologies

Comment la supervision IT et OT unifiée améliore l'efficacité des usines.
[par Fabien Pereira Vaz, Technical Sales Manager France chez Paessler AG]
Les systèmes informatiques traditionnels (IT) ont longtemps été séparés des technologies opérationnelles (OT), mais cette situation est en train de changer avec la convergence IT/OT qui fait figure de révolution pour la connectivité de l'informatique industrielle. Source SN

La prochaine génération du sans-fil : WiFi 6, 5G ou 5G privée ?
Les technologies WiFi et 5G s'améliorent. Elles prennent en charge une bande passante plus élevée et un plus grand nombre d'utilisateurs par point d'accès. Mais laquelle répond le mieux à vos besoins ? Une réflexion approfondie s'impose. Source Reseaux-Telecoms

Des organisations du monde automobile développent des standards pour les véhicules autonomes.
L'Autonomous Vehicle Computing Consortium (AVCC) et le SAE International travaillent à l'établissement de normes communes pour les véhicules autonomes et les systèmes avancés d'aide à la conduite. Ces organisations regroupent beaucoup de constructeurs et de sociétés technologiques travaillent sur ces questions. Elles cherchent à accélérer le développement et la production en masse de ces technologies, et d'en assurer une certaine interopérabilité. Source UD

Sécurité numérique

Les nouvelles tendances en matière de souveraineté numérique et d'évolution des budgets IT.
Les deux premières restitutions de l'étude de l'Agora des DSI pour T-Systems avaient mis en lumière le déploiement des solutions pour affronter les confinements et la massification du télétravail ainsi que l'analyse des forces et points d'amélioration pour les DSI. Cette troisième et dernière restitution de l'étude met quant à elle en avant le sujet de la souveraineté numérique et de l'évolution des budgets IT.
Source GlobalSecurityMag

Méfiez-vous des arnaques et de la désinformation sur les vaccins contre la COVID 19.
[par Benoit Grunemwald Expert en Cyber sécurité, ESET France]
La campagne de vaccination est une arme essentielle dans la lutte mondiale contre la pandémie, mais c'est aussi un sujet qui risque d'être exploité par les fraudeurs et les fournisseurs de fausses informations.
Source GlobalSecurityMag

Les hausses d'humidité constituent un défi latent pour les centres de données.
[par Aggreko] - L'un des défis latents auxquels est confrontée le secteur mondial des centres de données est l'augmentation des taux d'humidité, selon un récent rapport lancé par Aggreko, spécialiste du contrôle temporaire d'humidité et de température. Source GlobalSecurityMag

Baser la sécurité sur une approche préventive : du mythe à la réalité.
[par Florent Embarek, Regional Sales Director SPARK – Southern]
Il y a encore quelques années, la sécurité des infrastructures miser sur la prévention pour assurer la sécurité des infrastructures relevait du fantasme. La protection des endpoints était essentiellement basée sur la correspondance entre la signature des programmes malveillants et les données détenues par les systèmes de sécurité. Ce type de méthodes, qui demandaient une analyse préalable du fichier suspect, laissaient l'opportunité au malware de se répandre avant même qu'il ne soit catégorisé de malveillant. D'autres approches consistaient à envoyer une quantité astronomique de données dans le cloud pour qu'elles puissent être analysées, générant ainsi d'importants délais de latence entre l'infection et sa détection. Si ces solutions assurent un premier niveau de défense, elles reposent principalement sur des approches purement réactives. Source GlobalSecurityMag

Fuite de données : quel est l'impact pour les entreprises ?
Malveillantes ou accidentelles, les fuites de données augmentent avec la généralisation du télétravail. Temps, ressources, réputation… Quel est l'impact ? Source Silicon

La pandémie de la Covid 19 accélère la modernisation IT du secteur public.
Nutanix présente les résultats dédiés au secteur public de son étude annuelle Enterprise Cloud Index. Cette étude mesure les progrès des entreprises en matière d'adoption du cloud. Pour ce qui est du secteur public, les tendances recueillies indiquent une concentration des efforts de modernisation IT au cours des derniers mois et soulignent que 70 % des personnes interrogées déclarent que la COVID-19 a permis d'adopter une vision plus stratégique de l'informatique dans leur organisation.
Source GlobalSecurityMag

Cyberassurance : Tout ce que vous devez savoir sur son fonctionnement.
La cyberassurance est de plus en plus populaire. Mais que couvre-t-elle, que ne couvre-t-elle pas et que devez-vous rechercher lorsque vous choisissez une police d'assurance ? Source ZDNet

Les causes de l'incendie OVH Strasbourg: des explications stupéfiantes.
Quelles sont les vraies causes du sinistre ? Pourquoi le départ de feu a-t-il été si rapide ? OVH n'a pas pu ou voulu nous répondre, mais les explications recueillies sont stupéfiantes. Source SN – SN

Comment concilier télétravail agile et cybersécurité ?
[Par Larkin Ryder, Chief Security Officer de Slack]
Alors que la pandémie continue d'avoir un impact sur nos vies à tous, le travail à distance et hybride devient la « nouvelle norme ». Cette évolution s'est accompagnée de changements majeurs dans la culture et les règles de sécurité de nombreuses entreprises. Source Alliancy

Directeur général, le « rôle modèle » de la cybersécurité.
[Par Anne Doré, fondatrice de ADHEL, cabinet de conseil dédié à la cybersécurité]
Pourquoi les directeurs généraux refusent-ils de parler (vraiment) de cybersécurité ? Pourquoi leur implication est-elle souvent limitée aux discussions budgétaires, ou au temps de la crise ? Source Alliancy

Dix trucs et astuces de RSSI à la tête de petites équipes pour renforcer leur posture de sécurité.
Le risque d'attaques est plus élevé que jamais, que ce soit sur les grandes ou les petites entreprises. Les RSSI des petites structures ont développé des stratégies pour renforcer la sécurité de leur entreprise.
Source IT Social

Les mesures possibles pour renforcer la maturité de votre organisation en matière de sécurité.
Toute organisation est confrontée à des risques. C'est la façon dont chaque organisation est préparée à atténuer ces risques qui fait la différence. Source IT Social

Pour tout savoir sur la sécurité de vos données dans les datacenters.
Au travers de l'incendie chez OVH Strasbourg, les utilisateurs médusés ont pu s'inquiéter sur la protection de leurs données hébergées, tant le sujet est méconnu et souvent opaque, ne serait-ce que par sa technicité. Source SN – SN

Pourquoi est-ce vraiment grave de réutiliser votre mot de passe sur plusieurs comptes.
Oui, avoir le même mot de passe pour plusieurs services facilite la vie. Mais malheureusement, cette pratique met vos comptes en danger. Source Numerama

Big data et santé : les géants du numérique à l'épreuve des épidémies.
[par Martin Biéri, Chargé d'études prospectives] [LINC (Laboratoire d'Innovation Numérique de la CNIL)]
La pandémie de Covid-19 a éprouvé nos limites, qu'elles soient d'anticipation, de suivi ou encore d'analyse sanitaire. Pourtant, les outils à notre disposition n'ont jamais été aussi puissants et la question du mariage du big data et des données de santé n'est clairement pas nouvelle. Les grandes plateformes du numérique ont toutes investi dans la recherche (intelligence artificielle, machine learning, ordinateur quantique, etc.), avec le champ de la santé comme application. Qu'ont donc apporté les géants du numérique à la lutte contre la pandémie ? Source LINC

Mécanismes cryptographiques.
[deux documents fournissent des moyens de choisir de tels mécanismes.]
La sécurité des systèmes d'information repose pour partie sur l'emploi de mécanismes cryptographiques permettant de remplir des objectifs de sécurité tels que la confidentialité, l'intégrité et l'authentification. Une question qui se pose aux développeurs qui intègrent des mécanismes cryptographiques à leurs produits et aux administrateurs qui configurent les mécanismes cryptographiques des produits qu'ils mettent en œuvre est la sélection de mécanismes cryptographiques robustes.
Source ANSSI – ANSSI – ANSSI

Publication du 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 (COVID-19). Aussi, l'ANSSI a élaboré un référentiel pour les prestataires de vérification d'identité à distance. Ce nouveau référentiel d'exigences, valorisé par un visa de sécurité ANSSI et qui a fait l'objet d'un appel à commentaires, permettra d'identifier les prestataires fournissant un service de vérification d'identité à distance attestant d'un niveau de garantie substantiel ou élevé. Source ANSSI – ANSSI

Sûreté

Clubhouse, le média social qui fait parler et inquiète.
Des salles de conversations ouvertes dans lesquelles on peut entrer à tout moment pour écouter ou intervenir. C'est ainsi que l'on peut décrire Clubhouse, le petit réseau social qui monte, et surfe sur le retour de la voix. Il attire célébrités et inconnus du monde entier. Mais sa sécurité et les règles de confidentialité inquiètent. Source LMI – LMI

Les 5 manquements de Clubhouse à ses débuts sur la confidentialité des données.
Clubhouse est un nouveau genre de média social basé uniquement sur la voix, qui a considérablement gagné en popularité ces derniers temps. Cette application est devenue très tendance, car elle donne aux utilisateurs la chance exceptionnelle – aussi virtuelle soit-elle – de pouvoir approcher des personnalités riches et célèbres, comme Elon Musk, Drake, Oprah Winfrey ou encore Kevin Hart. Malheureusement, la plateforme qui n'en est qu'à ses débuts, a déjà connu une violation de données. Mais elle n'est pas la seule dans ce cas. Clubhouse, comme de nombreuses autres applications, fournit une passerelle directe vers vos données et informations personnelles. Source GlobalSecurityMag

Piratage de caméra de vidéosurveillance … et si vous arrêtiez de vous mettre un doigt dans l'œil.
Un retour sur le piratage de 150 000 caméras de vidéosurveillance installées par la société Verkada. Un piratage de vidéo surveillance qui cache un business du voyeur bien plus large !
Source Zataz – UnderNews

Posture Vigipirate « Sécurité renforcée – RISQUE ATTENTAT ».
Le Premier ministre, en accord avec le président de la République, a décidé d'abaisser le niveau Vigipirate à « Sécurité renforcée – risque attentat » à compter du 5 mars 2021. Source SGDSN

IoT (objets connectés) / IA

Les entreprises françaises accélèrent les déploiements d'IA pour contrer les cybermenaces.
[Etude Juniper Networks et Vanson Bourne]
Alors que la menace cyber ne faiblit pas (+255 % de signalements d'attaque par rançongiciel selon l'ANSSI), le recours aux technologies basées sur l'intelligence artificielle apparaît plus que jamais stratégique. Source GlobalSecurityMag

Peut-on concilier IA et sécurité des données ?
[par Timothée Rebours, Seald] – [machine learning (ML) – appelé apprentissage automatique (AA) en français]
Pour proposer de nouveaux produits, services ou fonctionnalités, les entreprises ont besoin de recourir au ML et à l'IA, des technologies nécessitant d'utiliser des données lisibles. Pseudonymiser les données utiles à l'IA et chiffrer de bout-en-bout les autres est la solution. Source ZDNet

Objets connectés et maison intelligente : savoir se protéger contre les cyberattaques.
Selon une étude de Statista, le marché mondial de la maison intelligente devrait croître et atteindre les 157 milliards de dollars d'ici 2024. Ces équipements domotiques permettent à chacun de contrôler la consommation, la sécurité ou encore la gestion de leur maison sur place mais également à distance. Un nouveau mode de vie numérique qui a incité 66 % des Français interrogés à acheter un nouvel appareil connecté en 2020. Source Globb Security

LOGICIELS MALVEILLANTS

Malware – Ransomwares

Silver Sparrow : un malware découvert dans plus de 30 000 Macs, y compris ceux équipés de puces M1.
Un logiciel malveillant surnommé « Silver Sparrow » a été découvert dans près de 30 000 ordinateurs Apple. Chose surprenante, il visait à la fois les machines équipées de processeurs Intel et celles dotées des puces M1 signées Apple, qui viennent tout juste d'être commercialisées. Source UD

En France Qbot est le cheval de Troie bancaire qui aura été le plus diffusé en février.
Check Point Research (CPR), la branche de renseignement sur les menaces de Check Point® Software Technologies Ltd. a publié son Rapport de sécurité 2021. Les chercheurs ont découvert que le cheval de Troie Trickbot se classait en première position pour la première fois, après avoir occupé la troisième place en janvier. Source GlobalSecurityMag

Un dangereux dropper de logiciels malveillants découvert dans 10 applications utilitaires de Google Play Store.
Check Point Research (CPR) a découvert un nouveau dropper, un programme malveillant conçu pour diffuser d'autres logiciels malveillants sur le téléphone d'une victime, dans 10 applications utilitaires du Google Play Store. Source GlobalSecurityMag

Le malware Purple Fox évolue pour se propager sur les machines Windows.
Les nouvelles capacités du logiciel malveillant ont entraîné une augmentation rapide du taux d'infection. Source ZDNet

« Black Kingdom », le dangereux rançongiciel qui fait n'importe quoi.
Black Kingdom ne fonctionne pas comme prévu, et ça le rend encore plus dangereux. Source Numerama

ACTUALITES JURIDIQUES - Législation et jurisprudences

CNIL

Fuite massive de données de santé : comment savoir si elle vous concerne et que pouvez-vous faire ?
Récemment informée de la publication sur internet d'un fichier contenant des données médicales de près de 500 000 personnes, la CNIL répond aux questions des personnes potentiellement concernées.
Source CNIL

Cybersécurité, données de santé, cookies : les thématiques prioritaires de contrôle en 2021.
En complément des contrôles faisant suite à des plaintes ou en lien avec l'actualité dans le contexte de la crise sanitaire, la CNIL orientera ses actions de contrôles autour de trois thématiques prioritaires en 2021 : la cybersécurité des sites web, la sécurité des données de santé et l'utilisation des cookies.
Source CNIL – UD

Fuite de données de santé : le tribunal judiciaire de Paris demande le blocage d'un site web.
Suite à une saisine de la CNIL, le tribunal judiciaire de Paris a demandé aux fournisseurs d'accès à internet (FAI) de bloquer l'accès à un site hébergeant des données de santé de près de 500 000 personnes. La CNIL, qui a déjà mené trois contrôles sur cette fuite de données, poursuit ses investigations. Source CNIL – LMI – Zataz – ZDNet

Entrepôts de données de santé : la CNIL lance une consultation publique sur un projet de référentiel.
La création d'un entrepôt de données de santé nécessite le respect de certaines formalités. Afin de simplifier ces procédures en proposant un cadre adapté aux pratiques, la CNIL organise une consultation sur un projet de référentiel jusqu'au 02 avril 2021. Source CNIL

RGPD – (Règlement général sur la protection des données)

Doctolib, de nouveau chahuté sur la confidentialité des données.
Un article de France Inter a rallumé la mèche, affirmant que les données manipulées par Doctolib étaient accessibles à des entreprises américaines. Doctolib s'en défend, tant bien que mal. Source ZDNet

La CNIL ouvre une enquête sur l'application Clubhouse.
Saisie d'une plainte contre Clubhouse, la CNIL a lancé des investigations pour vérifier la conformité au RGPD de ce nouveau réseau social. Source CNIL – HAAS Avocats

OVHcloud Strasbourg : Après un nouvel incident, la CNIL rappelle le RGPD.
Un autre incident est survenu dans le site d'OVH à Strasbourg. De la fumée a été détectée dans un local de batteries du datacenter SBG 1 dans la soirée du vendredi 19 mars et les opérations de relance ont été suspendues. Dans le même temps, la CNIL rappelle les obligations en matière de RGPD en cas de destruction des données personnelles. Source LMI – SN

Les bons réflexes à adopter selon les clubs utilisateurs.
Après un guide, les quatre clubs d'utilisateurs USF, AUFO, GFU-JDE et CUP présentent des fiches pratiques pour mettre en œuvre le RGPD. Source LMI

Droit des TIC

Me Bensoussan nous explique les droits des entreprises victimes de l'incendie chez OVHCloud.
[Par Alain Bensoussan, avocat du cabinet Alain Bensoussan-Avocats, président du réseau Lexing]
L'incendie survenu en mars dans le datacentre strasbourgeois de l'hébergeur OVHCloud a jeté un froid chez ses clients et ceux des opérateurs Cloud. Me Bensoussan parle même de « sidération ». Cet expert reconnu du droit numérique nous explique les droits et responsabilités des différentes parties en cas de perte de leurs données, ainsi que les éventuels recours en justice pour les entreprises sinistrées.
Source SN

La CNIL lance un programme d'évaluation des solutions de mesure d'audience.
[Par Gérard Haas, Anne Charlotte Andrieux et Elise Hausherr]
Afin d'accompagner les responsables de traitement dans leur mise en conformité RGPD sur la gestion des cookies, la CNIL a lancé début mars un programme d'évaluation des solutions mises sur le marché. Ce programme permet aux fournisseurs de solutions de mesure d'audience exemptées de recueil du consentement de soumettre à la CNIL pour analyse leur documentation technique et notamment les éléments de configuration disponibles de leur solution, afin que la CNIL confirme si l'offre proposée remplit bien les caractéristiques d'exemption du consentement. Source HAAS Avocats

Comprendre la cybersécurité des objets connectés.
[Par Sabine Marcellin, Avocat.]
Les objets connectés sont vulnérables, dès lors qu'ils contiennent du code. Un rapport de l'OCDE de février 2021 analyse la sécurité des produits connectés, du gadget au smartphone. Cette publication recherche l'origine des défaillances et propose des politiques visant à renforcer la sécurité des objets.
Source Village de la justice

CNIL et Cookies des entreprises et administrations : mise en conformité au 31 mars 2021.
[Par Steve Outmezguine, Avocat]
Qui n'a pas encore constaté lors de sa navigation sur Internet l'apparition d'un bandeau invitant à « tout accepter » ou « tout refuser » quant à l'utilisation de cookies sur son ordinateur ? Peu de personnes répondraient à cette question par la négative… Source Village de la justice

Juridique

Prison ferme pour un administrateur système revanchard.
Aux États-Unis, un administrateur système a été condamné à une peine de prison pour avoir supprimé les comptes Microsoft de son ex-employeur. Source ZDNet

Une nouvelle pierre à l'édifice en matière d'hyperlien.
[Par Anne-Laure Caquet, Avocat.]
En jugeant que les titulaires de droit d'auteur peuvent mettre en place des mesures techniques pour interdire la transclusion et restreindre ainsi l'accès de leurs œuvres au seul site d'origine, la Cour de Justice de l'Union Européenne procède à un rééquilibrage en faveur des titulaires de droit auteur, dans sa construction jurisprudentielle en matière d'hyperlien. Source Village de la justice – CJUE

Le déréférencement des données relatives aux condamnations pénales.
[Par Gerard Haas, Avocat]
La Cour de cassation rappelle qu'une juridiction saisie d'une demande de déréférencement doit impérativement apprécier si « l'inclusion du lien litigieux dans la liste des résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, répond à un motif d'intérêt public important, tel que le droit à l'information du public, et si elle est strictement nécessaire pour assurer la préservation de cet intérêt ». Source Village de la justice

Législation

L'État autorise l'analyse vidéo du port du masque dans les transports.
Un décret a été publié pour autoriser les transporteurs à utiliser les caméras de surveillance pour réaliser des statistiques sur le port du masque. La RATP avait testé cette possibilité en juin dernier avant d'être recalée par la CNIL. Source LMI – Legifrance – CNIL – HAAS Avocat

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

Référence	Titre	Date
CERTFR-2021-AVI-230	Multiples vulnérabilités dans VMware vRealize Operations	(31 mars 2021)
CERTFR-2021-AVI-229	Multiples vulnérabilités dans Google Chrome	(31 mars 2021)
CERTFR-2021-AVI-228	Vulnérabilité dans Xen	(31 mars 2021)
CERTFR-2021-AVI-227	Multiples vulnérabilités dans Citrix Hypervisor	(31 mars 2021)
CERTFR-2021-AVI-226	Multiples vulnérabilités dans Zimbra	(31 mars 2021)
CERTFR-2021-AVI-225	Vulnérabilité dans Apache SpamAssassin	(30 mars 2021)
CERTFR-2021-AVI-224	Vulnérabilité dans les produits Apple	(29 mars 2021)
CERTFR-2021-AVI-223	Vulnérabilité dans F5 BIG-IP	(29 mars 2021)
CERTFR-2021-AVI-222	Multiples vulnérabilités dans SolarWinds Orion	(26 mars 2021)
CERTFR-2021-AVI-221	Multiples vulnérabilités dans OpenSSL	(26 mars 2021)
CERTFR-2021-AVI-220	Multiples vulnérabilités dans le noyau Linux d'Ubuntu	(26 mars 2021)
CERTFR-2021-AVI-219	Multiples vulnérabilités dans les produits Cisco	(25 mars 2021)
CERTFR-2021-AVI-218	Multiples vulnérabilités dans le serveur LDAP de Samba	(24 mars 2021)
CERTFR-2021-AVI-217	Multiples vulnérabilités dans le noyau Linux d'Ubuntu	(24 mars 2021)
CERTFR-2021-AVI-216	Multiples vulnérabilités dans Mozilla Thunderbird	(24 mars 2021)
CERTFR-2021-AVI-215	Multiples vulnérabilités dans Mozilla Firefox et Firefox ESR	(24 mars 2021)
CERTFR-2021-AVI-214	[SCADA] Multiples vulnérabilités dans Moxa EDR-810	(23 mars 2021)
CERTFR-2021-AVI-213	Vulnérabilité dans Adobe ColdFusion	(23 mars 2021)
CERTFR-2021-AVI-212	Vulnérabilité dans Foxit Reader et PhantomPDF	(23 mars 2021)
CERTFR-2021-AVI-211	Multiples vulnérabilités dans le noyau Linux d'Ubuntu	(22 mars 2021)

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

Référence	Titre	Date
CERTFR-2021-ALE-006	Vulnérabilité dans F5 BIG-IP	Alerte en cours le 20/03/2021
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
CERTFR-2020-ALE-026	[MaJ] Présence de code malveillant dans SolarWinds Orion	Alerte en cours le 14/12/2020

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

Référence	Date
CERTFR-2021-ACT-012	(29 mars 2021)
CERTFR-2021-ACT-011	(22 mars 2021)
CERTFR-2021-ACT-010	(15 mars 2021)
CERTFR-2021-ACT-009	(01 mars 2021)
CERTFR-2021-ACT-008	(15 février 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	78.9.0 ESR			
	Antérieures	CERTFR-2021-AVI-215	Mfsa2021-11	2021_03_26
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	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-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***