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

Lettre d'information SSI n°66

Pôle Défense et Sécurité des Systèmes d'Information

Notes d'information technique

Edition ► Février 2021

I – Cybercriminalité et attaques informatiques

Dans le MONDE

- **Le centre de gestion des paies des employés fédéraux américains également touché par l'attaque SolarWinds.**
  Un second groupe de hackers, chinois cette fois-ci, aurait exploité la faille dans la suite logicielle Orion de SolarWinds. Le National Finance Center, organisme de gestion des paies pour les employés fédéraux, serait l'une des victimes de cette attaque informatique attribuée à un État-nation. Cette agence stocke les données personnelles de plus de 600 000 salariés, ce qui fait craindre une fuite de données énorme. Source UD

- **Un hacker a tenté d'empoisonner l'eau potable d'une ville en Floride.**
  Grâce à une intrusion dans le circuit d'approvisionnement, un hacker a réussi à augmenter la teneur en soude caustique de l'eau postale de la ville d'Oldsmar en Floride. L'eau infectée n'a pas accédé au système de distribution évitant ainsi un empoisonnement massif car un technicien a rapidement réagi. Une enquête menée par le FBI a été ouverte. Source UD – LMI – ZDNet – Numerama – Globb Security – Siècle Digital

- **La Corée du Nord accusée de cyberattaque contre Pfizer.**
  Des hackers nord-coréens auraient tenté de pénétrer dans le système d'information du géant pharmaceutique Pfizer afin de voler des informations sur le vaccin contre le Covid-19, d'après un service de renseignement de la Corée du Sud. Cette campagne malveillante s'ajoute à des nombreuses accusations depuis le début de la pandémie. Source UD

- **Sur la messagerie Signal, un faux Amazon fait « gagner » des iPhone 12**
  Les phishings débarquent sur l'app Signal. Au menu : un faux jeu concours avec un iPhone 12 Pro à la clé. Source Numerama

- **Sequoia Capital victime de brèche et vol de données.**
  Le fonds d'investissement Sequoia Capital a subi une cyberattaque ayant débouché sur un vol de données incluant des informations financières. Le vecteur d'attaque utilisé pourrait bien être un hameçonnage par e-mail. Source LMI

- **L'avionneur Canadien Bombardier piraté, données volées.**
  Après Dassault Falcon, c'est au tour de l'avionneur Canadien Bombardier de se retrouver dans les mains de pirates informatiques. Source Zataz

En FRANCE

Cybersécurité

Incident de sécurité chez Stormshield.
L'ANSSI a été informée d'un incident de sécurité affectant la société Stormshield et travaille en étroite collaboration avec les équipes de la société. Source ANSSI – ZDNet – UD

Des pirates font chanter le loueur de véhicules UCAR.
Mi-janvier, le loueur de véhicules UCAR annonçait être victime d'un piratage informatique. Source Zataz

Un assureur et ses clients dans la ligne de mire d'Avaddon.
[SVI Assurances est dans de nombreux secteurs de l'assurance des risques spéciaux]
Depuis la disparition d'importants groupes de pirates tels que Maze, Egregor, Pysa, Netwalker, d'autres malveillants du web ont repris un flambeau bien encombrant qu'est le rançonnage des entreprises. Derniers cas : l'assureur français SVI et le professionnel du nettoyage Québécois Qualinet. Source Zataz – Zataz

Cyberattaque sur Centreon : une affaire SolarWinds à la française ?
L'ANSSI a publié un rapport sur une campagne menée sur Centreon, fournisseur de logiciels de supervision des systèmes d'information. Une offensive qui n'est pas sans rappeler l'affaire SolarWinds. Mais le rapport interroge sur plusieurs points. Qui sont les victimes ? Pourquoi autant de précautions sur l'attribution ? Source LMI – Silicon – UD – LMI – ZDNet – Siècle Digital

33 millions de données clients Cdiscount volées, un haut responsable mis en examen.
Cdiscount a été victime d'un vol de données clients. Au total, 33 millions de noms, prénoms, dates de naissance, numéros de téléphone, adresses e-mail sont concernés. Le directeur d'un site situé à Bordeaux vient d'être mis en examen et placé sous contrôle judiciaire. Il aurait mis ces données en vente sur le marché noir. Source UD – Siècle Digital

Des cyberattaques ont ciblé l'Institut Pasteur, qui vient d'abandonner son projet de vaccin contre le Covid-19.
L'Institut Pasteur a été victime d'une campagne malveillante via des attaques qui ont ciblé ses partenaires de recherche sur un vaccin contre le Covid-19, projet qui vient d'être abandonné faute de résultats convaincants. D'après les premiers éléments de l'enquête, aucune donnée sensible n'a pas été dérobée lors de ces intrusions. Source UD

Le Centre Hospitalier de Dax affecté par un ransomware.
Les systèmes informatiques et téléphoniques du Centre Hospitalier de Dax-Côte d'Argent ont été rendus indisponibles suite à une cyberattaque par rançongiciel. Des procédures de fonctionnement en mode dégradé ont été activées. Source LMI – ZDNet – UD – Numerama

Le ransomware Ryuk traumatise l'hôpital de Villefranche-sur-Saône.
Après Dax, c'est au tour du centre hospitalier de Villefranche-sur-Saône d'être la victime d'une cyberattaque. L'établissement a communiqué rapidement en nommant son agresseur : Ryuk.
Source LMI – UD – Siècle Digital – UnderNews

Plus de 400 000 données de patients français vendus dans le blackmarket.
ZATAZ découvre une vente de données personnelles et privées appartenant à plus de 400 000 patients français. Identités, téléphones, médecins, numéros de sécurité sociale et plus de 60 autres données sensibles.
Source Zataz – Zataz

Des données d'un laboratoire pharmaceutique français publiées par des pirates.
Le laboratoire pharmaceutique français Bailly-creat se retrouve confronté à la dernière phase malveillante orchestrée par les pirates informatique du groupe Doppel. Source Zataz

Le groupe BVA en prise avec des pirates informatiques.
La société française BVA Group, spécialiste des études comportementales, menacée par un groupe de pirates informatiques. Source Zataz

La Mutuelle Nationale des Hospitaliers au cœur d'une cyberattaque.
Un groupe de hackers a pour pris cible la Mutuelle Nationale des Hospitaliers, qui compte 600 000 adhérents. Touchés par un ransomware, son site internet et son standard téléphonique sont indisponibles depuis vendredi. C'est le groupe RansomEXX qui en serait aux commandes. Source UD

L'AFNor sous le feu du ransomware Ryuk (MAJ).
L'association française en charge de la normalisation a été victime d'une cyberattaque qui perturbe son fonctionnement. Le ransomware Ryuk déjà à l'œuvre dans les hôpitaux de Dax et Villefranche est également soupçonné dans le cas de l'Afnor. Source LMI – Zataz – ZDNet – SN – Numerama

Beneteau touché mais pas coulé.
Quelques mois après Fountaine-Pajot, c'est au tour d'un autre poids lourd de l'industrie nautique française, le groupe Beneteau, d'être victime d'une attaque informatique, probablement un ransomware. Redémarrage des systèmes informatiques en mode dégradé et enquêtes ont été lancées. Source LMI

Fuite de données pour Le Service Postal.
Le site Service Postal offre des solutions de services postaux pour les entreprises. Un pirate annonce le piratage de la société et commercialise la base de données volées forte de plus de 150 000 utilisateurs.
Source Zataz

La ville de Chalon-sur-Saône et l'agglomération du Grand Chalon sont victimes d'une cyberattaque.
Des cybercriminels ont réussi à pénétrer dans les systèmes informatiques de Chalon-sur-Saône et du Grand Chalon. Une cellule de crise a été ouverte pour gérer cet incident tandis que l'ANSSI accompagne les collectivités pour un retour à la normale le plus rapidement possible. À ce stade, aucune demande de rançon n'a été faite, d'après les victimes. Source UD – UnderNews

Cyberdéfense

6e édition du baromètre annuel du CESIN.
[CESIN (Club des Experts de la Sécurité de l'Information et du Numérique)]
Afin de mieux cerner l'état de l'art et la perception de la cybersécurité et de ses enjeux au sein des grandes entreprises françaises, le CESIN publie chaque année depuis 2015, son baromètre annuel avec OpinionWay. Le sondage OpinionWay pour le CESIN a ciblé 704 membres de l'association, les résultats de l'étude portent sur un échantillon de 228 répondants.
Source GlobalSecurityMag – CESIN – CESIN – LMI – Globb Security – SN

Des ransomwares plus nombreux et professionnels selon l'ANSSI.
Un rapport de l'ANSSI montre que les incidents de sécurité liés aux ransomwares ont progressé de 255 % entre 2019 et 2020, pour un total de 192 événements signalés. De plus en plus professionnalisés, les groupes de cybercriminels chassent leurs proies parfois plusieurs mois à l'avance.
Source LMI – ANSSI – Silicon – UD – Siècle Digital

Les RSSI des collectivités territoriales créent un réseau de partage.
Constatant un manque et avec le soutien de l'ANSSI, un réseau regroupant une centaine de RSSI de collectivités territoriales vient de voir le jour. Un lieu d'échanges et d'entraide particulièrement utile en cette période de vague de cyberattaques. Source LMI

OVHcloud et Capgemini s'allient pour un cloud souverain sécurisé.
Capgemini et OVHcloud accompagnent déjà depuis 2019 des organismes, notamment publics, autour d'offres souveraines sur-mesure. Source ZDNet

Faire face à la menace : la stratégie française.
Les récentes attaques sur les centres hospitaliers de Dax-Côte d'Argent et de Villefranche-sur-Saône, nous montrent la criticité de cette menace dans notre quotidien. Pour faire face à ces menaces, le président de la République a annoncé une stratégie nationale de cybersécurité, qui mobilise 1 milliard d'euros, dont 720 millions d'euros de financements publics.
Source ANSSI – ANSSI – ANSSI – ANSSI – ANSSI – LMI – ZDNet – UD – SN

Voici la stratégie gouvernementale pour lutter contre les cyberattaques visant les hôpitaux.
Le ministre de la Santé Olivier Véran et le secrétaire d'État au Numérique Cédric O viennent de présenter un nouveau plan pour renforcer la sécurité informatique des hôpitaux, quelques jours après les cyberattaques qui paralysent les établissements de Dax et de Villefranche-sur-Saône. L'accent est mis sur l'audit et la formation grâce à une enveloppe de 350 millions d'euros. En revanche, aucune mesure pour moderniser les infrastructures informations n'est prévue malgré l'urgence de la situation. Source UD – Numerama – Zataz

La nouvelle antenne de l'ANSSI se situera à Rennes.
L'Agence nationale de la sécurité des systèmes d'information continue de se développer et va s'implanter progressivement sur le territoire breton avec une antenne à Rennes. Source ANSSI

II – Actualités

Brèves

Cybersécurité

SolarWinds: la bombe à retardement des éditeurs de sécurité compromis.
La liste des victimes touchées par le hack mondial SolarWinds s'allonge. En ciblant les fournisseurs de solution de sécurité, les cyberpirates atteignent un vivier encore plus important encore d'entreprises à compromettre. Source LMI

L'Union européenne veut élaborer un système de certification des réseaux 5G.
L'Agence de l'Union européenne pour la cybersécurité est chargée de mettre au point un mécanisme de certification pour les réseaux 5G, dont l'objectif est de remédier aux vulnérabilités techniques de ces nouveaux réseaux. Des experts en sécurité informatique seront invités à participer à l'élaboration de ce label. Source UD

En une seule mise à jour, une app malveillante a détourné des millions d'appareils.
En une seule mise à jour, une application populaire de lecture de codes-barres sur Google Play s'est transformée en logiciel malveillant et a pu détourner jusqu'à 10 millions d'appareils. Source ZDNet

Attaques RDP : Les prochaines victimes seront des télétravailleurs.
Les chercheurs d'ESET ont détecté des milliards de cyberattaques visant à profiter des personnes qui travaillent à distance – et les cybercriminels ne relâchent pas encore leurs efforts. Source ZDNet

Kaspersky dresse le bilan de l'année 2020 et esquisse l'environnement pour 2021.
Bascule vers le télétravail, ciblage des hôpitaux, attaque Sunburst… La cybersécurité des systèmes d'information a été mise à rude épreuve en 2020. Source Industrie & Technologies

La flambée de la cybercriminalité en 2020 rapporte 350 millions de dollars aux pirates.
Après l'année de la COVID-19, 2020 aura aussi marqué l'histoire en étant l'année de la cybercriminalité. Source Siècle Digital

Comprendre les attaques rançongiciels en 6 points clés.
Rançongiciel, ransomware : vous avez sûrement déjà entendu parler de ce type d'attaque Pour mieux comprendre de quoi il s'agit et comprendre le principal enjeu des entreprises en matière de cybersécurité, voici quelques explications. Source Numerama

Cybersécurité : une majorité d'appareils d'occasion contient des données résiduelles exploitables.
La nouvelle économie circulaire a remis au goût du jour une pratique qui avait fini par être annihilée par la production de masse et l'obsolescence programmée : la revente des appareils d'occasion. Cependant, le réemploi de ces appareils, qui ont durant leur première vie contenu des informations à caractère personnel et privé, présente le risque de rendre ces données accessibles aux nouveaux propriétaires.
Source IT Social

Résolution des fuites de données : plusieurs mois sont nécessaires pour un quart des organismes publics.
Un quart des organismes publics ont déclaré une fuite accidentelle de leurs données stockées dans le cloud en 2020. Selon une étude de Netwrix, la détection et la résolution de ces fuites constituent l'incident le plus difficile à résoudre pour les organismes publics. Source IT Social

Pourquoi les attaques par compromission d'e-mails font plus de dégâts que les ransomwares
Les courriels de phishing qui dupent les utilisateurs pour envoyer des virements aux cybercriminels sont de loin la forme de cybercriminalité la plus lucrative. Voici ce que vous devez savoir à leur sujet.
Source ZDNet

Les attaques Ddos se sont multipliées en 2020.
Le dernier « DDoS Weapons Report » d'A10 Networks, confirme que les cybercriminels ont été très actifs tout au long de l'année et ont profité de la pandémie mondiale pour multiplier les attaques, petites et grandes. Source IT Social

Covid 19 : jamais le cyber-espionnage entre Etats n'a été si virulent.
[Par Nicolas Caproni, Directeur de recherche menaces et détection chez SEKOIA]
Le nombre de cyberattaques a explosé en 2020 avec notamment pour cibles les entreprises pharmaceutiques et établissements de recherche liés aux vaccins contre la Covid 19. Derrière ce cyber espionnage se cachent des groupements mandatés par des États. Jamais les hostilités dans le cyberespace n'ont été aussi nombreuses que depuis le début de la pandémie. Source IT Social

Cybersécurité de l'industrie

Tesla rappelle près de 135 000 voitures pour un problème de sécurité de l'ordinateur de bord.
Tesla va rappeler près de 135 000 voitures aux Etats-Unis, des Model S et Model X, pour un problème de sécurité lié à l'ordinateur de bord, après une alerte lancée mi-janvier par l'agence américaine de la sécurité routière, NHTSA. Source SN

Les préconisations de l'agence européenne de la cybersécurité sur les véhicules autonomes.
Qui dit véhicules autonomes, dit algorithmes et logiciels embarqués. Avec ces nouveaux systèmes, les risques en matière de cybersécurité sont décuplés et les conséquences peuvent être dramatiques. Conscient de ces enjeux, le Centre commun de recherche de la Commission et l'Agence de l'UE pour la cybersécurité (ENISA) a émis une liste de recommandations. Source UD

Réseau informatique industrielle : pourquoi il est dangereux de lui appliquer les recettes IT traditionnelles. [par Emmanuel Le Bohec, directeur des ventes de Claroty, un spécialiste de la sécurité des environnements OT]
Il peut être tentant de protéger les réseaux industriels (plus largement appelés OT pour technologies opérationnelles) en leur appliquant les recettes éprouvées des systèmes d'information bureautiques. Mais, il existe des différences fondamentales entre OT et IT, qui rendent cette approche inefficace. Source SN

70 % des failles ICS ont un score élevé, voire critique.
Selon une étude de Claroty, le nombre de vulnérabilités au sein des systèmes de contrôle industriels (ICS) a explosé au 2e semestre 2020 (+33 %). Principale raison : un élargissement de la surface d'attaque lié au télétravail. Source IT Social

« Il faut former beaucoup plus sur les risques de cyberattaques ».
[Par Marc-Oliver Pahl, chercheur à l'IMT Atlantique]
Les cyberattaques sont toujours en augmentation et ciblent hôpitaux comme industriels.
Source Industrie & Technologies

Sécurité numérique

Sécurité des systèmes d'information des entreprises : les recommandations de Kaspersky pour 2021.
Le passage accéléré et massif au travail à distance a bouleversé le fonctionnement des entreprises, et la sécurité informatique se retrouve au cœur de cette transformation. Parmi ces enjeux, la nécessité de considérer la sécurisation des postes de travail dans leur globalité (c'est-à-dire sur site et à distance) Source GlobalSecurityMag

5 cyber-escroqueries courantes : comment les éviter ?
[par Benoit Grunemwald Expert en Cyber sécurité, ESET France]
Les cyber-fraudeurs sont prompts à exploiter l'actualité à leur profit, mais de nombreux stratagèmes sont intemporels, indépendamment de ce qui fait l'actualité. Voici 5 escroqueries courantes auxquelles vous devez faire attention. Source GlobalSecurityMag

Comprendre la vérification d'identité et son importance pour les utilisateurs.
[par Nicolas Luneau de Auth0]
En juin 2021, la France doit se conformer au droit européen et doter ses citoyens d'une carte nationale d'identité électronique pour remplacer la Carte Nationale d'Identité (CNI) actuelle, mise en place en 1987. Ce projet s'inscrit dans la mission interministérielle, initiée en 2018, en faveur d'un parcours d'identification numérique sécurisé. Source ZDNet

Pourquoi tant de systèmes restent-ils sans correctif de sécurité et comment résoudre cette question ? [par Chris Goettl, Director of Security Product Management chez Ivanti]
Chris Goettl décrit ici les obstacles principaux qui empêchent l'application des correctifs et donne des pistes pour que cette dernière devienne un processus SecOps fluide. Source SN

L'App Store hébergerait de nombreuses applications frauduleuses.
Apple étant pourtant réputé pour être sévère dans le processus de publication des applications dans son App Store… Source Siècle Digital

Comment se protéger des programmes malveillants ?
Backdoors, rootkits, spywares, ransomwares…les entreprises sont confrontées à de nombreuses menaces. Source Siècle Digital

Technologies : de quoi 2021 sera fait ?
N'en doutez plus, 2021 marquera la confirmation de l'essor du travail à distance. Ce changement majeur dans le fonctionnement des entreprises va bouleverser le quotidien de toute la société. Source IT Social

Le cloud hybride plébiscité, mais les difficultés pour assurer la conformité et la sécurité rebutent les entreprises.
Malgré ses avantages évidents, le cloud hybride apporte des complexités en matière de sécurité et de conformité. C'est pourquoi de nombreuses entreprises font preuve de prudence dans la sélection des services et des fournisseurs de cloud hybride. Source IT Social

Comment vérifier si ses mots de passe ont été volés ?
[Par Mark Hachman, IDG (adapté par Jacques Cheminat)]
Face à la multiplication des vols de données, comment être sûr que ses identifiants ne font pas partie des listes vendues sur les forums underground ? Il existe des moyens pour surveiller cela et prendre le cas échéant des mesures. Source LMI

Le vol d'identifiants a connu une forte croissance en 2020.
L'étude « 2021 Credential Stuffing Report » de F5 Networks vient rappeler la place majeure du vol d'identifiants dans la cyber-criminalité. Source LMI

L'Identité Numérique La Poste labellisée « France Cybersecurity ».
L'Identité Numérique La Poste a obtenu, via Docaposte, filiale numérique de La Poste, le label « France Cybersecurity » valorisant les solutions françaises de souveraineté et de confiance numérique. Source SN

Sans sécurité pas de cloud.
Une étude de Sapio Research commandée par Trend Micro alerte sur les négligences en matière de sécurité lors d'une migration cloud. La pandémie de Covid-19 n'a rien arrangé à la situation.
Source Réseaux & Télécoms – LMI

Recrudescence de l'hameçonnage bancaire (DSP2).
Une recrudescence de messages d'hameçonnage sur le thème de la sécurité des comptes bancaires en ligne lié à la mise en place de la 2e Directive européenne sur les Services de Paiements (DSP2, voir notre encadré). Des cybercriminels exploitent ce sujet d'actualité afin de rendre plus crédibles leurs tentatives d'escroquerie. Source Cybermalveillance – UD

Pendant la crise, le ministère de l'Intérieur mise sur le VPN de TheGreenBow.
Avec la crise sanitaire, le ministère de l'Intérieur a dû rapidement déployer des solutions d'accès à distance sécurisée sur grande échelle. Pour cela, il s'est appuyé sur la solution VPN de TheGreenBow.
Source LMI

Baromètre de la perception du spam pour le dernier trimestre 2020.
Le baromètre Signal Spam permet d'apprécier les tendances d'après les signalements des internautes auprès de la plateforme Signal Spam. Les États-Unis et l'Espagne sont de manière préoccupante responsables de l'émission de beaucoup de communications signalées comme spam par les internautes français. Source Signal Spam – Signal Spam

Sûreté

Baser la sécurité sur une approche préventive : du mythe à la réalité.
[par Florent Embarek, Regional Sales Director Spark – Southern & Eastern Europe]
Il y a encore quelques années, la sécurité des infrastructures miser sur la prévention pour assurer la sécurité des infrastructures relevait du fantasme. Source Alliancy

Clubhouse : une faille met au jour de sérieux problèmes de sécurité.
Un utilisateur a été en mesure de diffuser les discussions de plusieurs salles sur un site internet. « Tous les utilisateurs doivent partir du principe que toutes les conversations sont enregistrées »
Source Siècle Digital – Numerama

IoT (objets connectés) / IA

Avast encourage les Français à renforcer la sécurité des objets connectés.
Les progrès accomplis dans le domaine de la technologie domestique intelligente sont en train de transformer les foyers français, mais ils offrent également des opportunités aux attaquants. Régulièrement, de nouveaux objets connectés destinés aux particuliers sont disponibles sur le marché hexagonal. Les experts en sécurité d'Avast encouragent donc les Français à s'assurer de la sécurité de leur foyer dès l'acquisition d'un appareil intelligent additionnel. Source GlobalSecurityMag

Beacon : tout savoir sur cette balise Bluetooth et son utilité pour l'IoT.
Sur le marché des appareils connectés, Beacon devient de plus en plus populaire. Pour les entreprises souhaitant déployer cette technologie, ce guide offre des détails sur tout ce qu'il faut savoir à son propos. Source Objetconnecte

LOGICIELS MALVEILLANTS

Malware – Ransomwares

Le botnet TrickBot se réactive en ciblant les avocats et les assureurs.
Le botnet Trickbot qui avait servi aux attaques Ryuk et d'autres ransomware a repris du service. Pour ce retour, les pirates ont remplacé les pièces jointes malveillantes des courriers électroniques par des liens malveillants. Il cible particulièrement les cabinets d'avocats et les compagnies d'assurance. Source LMI

Le malware Kobalos cible le HPC en dévoyant OpenSSH.
Les chercheurs d'Eset ont découvert un malware baptisé Kobalos qui cible les systèmes HPC. Pour cela, il se sert d'une version compromise d'OpenSSH pour voler des identifiants. Source LMI

Rançongiciels : un jackpot à 350 millions de dollars en 2020.
Sous la barre des 100 millions de dollars en 2019, les montants extorqués aux victimes de ransomware ont flirté avec les 350 millions de dollars en 2020. Ryuk, Maze et Doppelpaymer ont été les plus rémunérateurs. À noter que le 4e trimestre 2020 a connu une baisse des paiements de rançons.
Source LMI

Business des ransomwares : Netwalker en chiffre.
Après l'arrestation d'un opérateur présumé du ransomware Netwalker, le business se fait plus clair pour des voyous capables d'amasser des millions de dollars via leurs chantages numériques. Source Zataz

Un malware Linux s'attaque aux superordinateurs.
La base de code du malware Kobalos est réduite, mais son impact ne l'est pas. Ce malware, analysé par les équipes d'ESET, s'attaque notamment aux superordinateurs, mais l'objectif exact de ses créateurs n'est toujours pas déterminé. Source ZDNet

ACTUALITES JURIDIQUES - Législation et jurisprudences

CNIL

« Credential stuffing » : la CNIL sanctionne un responsable de traitement et son sous-traitant.
La formation restreinte de la CNIL a récemment sanctionné de 150 000 euros et 75 000 euros un responsable de traitement et son sous-traitant pour ne pas avoir pris de mesures satisfaisantes pour faire face à des attaques par bourrage d'identifiants (credential stuffing) sur le site web du responsable de traitement. Source CNIL – LMI – Cyberdroit – Haas Avocats

Cookies : la CNIL incite les organismes privés et publics à auditer leurs sites web et applications mobiles.
Le délai raisonnable pour mettre en conformité les sites web et applications mobiles aux nouvelles règles en matière de cookies ne saurait excéder le 31 mars 2021. La CNIL a souhaité sensibiliser à nouveau les organismes privés et publics par une campagne d'envoi de courriers et courriels, l'occasion de rappeler la présence d'outils et de conseils pratiques sur cnil.fr. Source CNIL – SN

Compteurs communicants LINKY : clôture de la mise en demeure à l'encontre d'EDF.
Par décision du 15 février 2021, la Présidente de la CNIL a décidé de procéder à la clôture de la mise en demeure du 31 décembre 2019 notifiée à la société EDF le 11 février 2020.
Source CNIL – Legifrance – CNIL – ZDNet

La CNIL rend son avis sur les évolutions de l'application TousAntiCovid.
La CNIL s'est prononcée le 17 décembre 2020 sur la modification du décret du 29 mai 2020 relatif au traitement de données « StopCovid ». Les évolutions visent principalement à alerter les utilisateurs de l'application « TousAntiCovid » lorsqu'elles ont été présentes dans un établissement recevant du public en même temps qu'une ou plusieurs personnes ultérieurement diagnostiquées ou dépistées positives à la COVID-19. Source CNIL

Reconnaissance faciale et interdiction commerciale de stade : la CNIL adresse un avertissement à un club sportif.
La Présidente de la CNIL a adressé un avertissement à un club sportif qui envisageait de recourir à un système de reconnaissance faciale afin d'identifier automatiquement les personnes faisant l'objet d'une interdiction commerciale de stade. Ce projet n'est en effet pas conforme au RGPD et à la loi Informatique et Libertés. Source CNIL

Violation de données de santé : la CNIL rappelle les obligations des organismes à la suite d'une fuite de données massive annoncée dans les médias.
À la suite de la publication dans la presse de plusieurs articles concernant une fuite de données de santé massive, la CNIL rappelle aux responsables de traitement leurs obligations en cas de violation.
Source CNIL – Zataz – ZDNet – UD

Fuite de données médicales de 500 000 Français : la CNIL n'a pas été alerté.
La CNIL annonce enquêter sur la fuite de données médicales de 500 000 Français sur le net. En particulier, l'autorité administrative s'interroge sur l'absence de notification qui lui a été adressée, alors que la loi l'exige. Source Numerama – Numerama

RGPD – (Règlement général sur la protection des données)

La CNIL et l'Inria décernent le prix « protection de la vie privée » 2020.
La CNIL et l'Inria ont remis le prix 2020 pour la protection de la vie privée à une équipe de recherche lors de la 14e conférence internationale Computers, Privacy and Data Protection (CPDP). Márcio Silva, Lucas Santos de Oliveira, Athanasios Andreou, Pedro Olmo Vaz de Melo, Oana Goga et Fabrício Benevenuto ont été récompensés pour leur article. Source CNIL

RGPD, la fête est finie ! Cookies, Consentement et Prospection Commerciale, nous sommes tous concernés. [par Philippe Gabillault, Expert en protection des données.]
Le 31 mars 2021 marquera la fin du délai de clémence accordé par la CNIL aux entreprises pour se mettre en conformité avec les lignes directrices modificatives en matière de cookies et autres traceurs du 17 septembre 2020. Source Village de la justice

Un « bac à sable » RGPD pour accompagner des projets innovants dans le domaine de la santé numérique.
Dans une logique de régulation agile et ouverte sur des problématiques innovantes, la CNIL lance un appel à projets « bac à sable » RGPD. Ce dispositif permettra aux trois lauréats de cette première édition de bénéficier d'un accompagnement renforcé pour aboutir à une solution technologique conforme à la réglementation et respectueuse de la vie privée. Source CNIL

Sanctions RGPD en 2020 : quel bilan pour la protection des données ?
Quelles données personnelles sont collectées et traitées à son sujet ? Pourquoi ? Et quels sont ses droits par rapport à ce traitement ? Source Alliancy – Alliancy

Droit des TIC

La cybersécurité et les « smarts building ». [Par Gérard Haas et Emilien Burel]
De plus en plus de « smart buildings » sont aujourd'hui construits. Ils offrent plus de confort et sont également plus économes et respectueux de l'environnement (gestion optimale de la température, de la ventilation, de l'éclairage…). Ces bâtiments promettent également d'être plus sûrs grâce à des systèmes d'alarmes, de détection d'intrusion, de vidéosurveillance, ou encore de contrôles d'accès. Mais cette promesse n'est-elle pas un leurre ? Source HAAS avocats

Les enjeux juridiques de deux décennies d'encyclopédie libre. [Par Gérard Haas et Elise Hausherr]
Lancée le 15 janvier 2001, Wikipédia est devenue la référence des encyclopédies en ligne. Son principe : permettre le partage universel de connaissances en permettant aux contributeurs d'écrire et de modifier des articles en ligne. Avec 500 millions de visiteurs uniques mensuels, une base de plus de 55 millions d'articles consultables dans 300 langues différentes, l'encyclopédie a su résister à ses détracteurs. Mais l'encyclopédie a aussi réussi à surmonter différents enjeux juridiques. Source HAAS Avocats

Jusqu'où peuvent aller les plateformes dans la censure des contenus ?
[Par Gérard Haas et Elise Hausherr]
Le 8 janvier dernier, Twitter, suivi par Facebook et Snapchat ont suspendu le compte de Donald Trump, alors toujours Président des États-Unis. Longtemps, les plateformes ont prétendu être de simples hébergeurs, les dédouanant de toute responsabilité sur les contenus diffusés. En suspendant les comptes de l'ancien président, elles ont admis la nécessité de fixer des limites à ces contenus. Mais dans quelles mesures un réseau social, entreprise privée, peut-il décider unilatéralement de censurer un contenu publié sur sa plateforme ? Source HAAS Avocats

Pourquoi avoir un guide juridique d'encadrement des réseaux sociaux ?
[Par Stéphane Astier et Anne-Charlotte Andrieux]
Les réseaux sociaux constituent une source de communication désormais largement plébiscitée par les entreprises. Ces outils constituent en effet un atout commercial majeur en permettant la diffusion rapide et facile de contenus à grande échelle. Toutefois, l'attractivité et la simplicité de leur utilisation peut faire oublier les risques de dérives liés à leur utilisation. Au regard de ces risques, fixer une stratégie de communication comportant un encadrement juridique précis et adapter apparaît essentiel.
Source HAAS Avocats

Garants de la conformité réglementaire des entreprises, les juristes s'emparent de la cybersécurité.
Cela fait quelques années que la fonction cybersécurité n'est plus exclusivement une affaire de réponse technologique à des menaces. Avec la transformation numérique, elle a appris à dialoguer avec les métiers. À présent, ce sont les conseils d'administration et les juristes qui se l'approprient.
Source IT Social

Un nouveau pas vers l'adoption du Règlement e-privacy.
[Par Gérard Haas, Jean Philippe Souyris et Théo Renaudie]
L'attente fut longue avant que le Conseil européen n'adopte une position commune, ce 10 février 2021 quant au Règlement e-privacy. Alors que la Commission avait publié son premier projet en janvier 2017 et que le Parlement avait fait une proposition en octobre 2017, le Conseil européen s'est fait attendre plus de 3 ans. Source HAAS Avocats

Juridique

La livraison conforme d'un logiciel personnalisé est une obligation de résultat.
Le 21 janvier 2021, le Tribunal de commerce de Vienne a jugé qu'en matière de logiciel spécifique, le prestataire est soumis à une obligation de résultat à l'égard de son client et que la livraison d'une version finale comportant des dysfonctionnements constitue un manquement à son obligation de délivrance d'un produit conforme de nature à engager sa responsabilité contractuelle, le règlement de la facture totale par le client ne valant pas recette tacite. En l'espèce, les manquements constatés n'étaient toutefois pas suffisamment graves pour justifier la résolution du contrat. Source Cyberdroit – Legalis

La case pré-cochée ne vaut (toujours) pas consentement.
[Par Jean-Philippe Souyris et Théo Renaudie]
La Cour de justice de l'Union européenne a à nouveau dû se prononcer sur la case précochée. Le 1er octobre 2019, déjà, la Cour avait exposé que la case précochée ne répondait pas à la nécessité d'un consentement actif de l'utilisateur au dépôt de cookies sur son terminal utilisateur.
Source HAAS avocats – CJUE – CJUE

La Cour de cassation à l'épreuve du numérique et de l'intelligence artificielle.
[Par Jean-Michel Sommer – Président de chambre à la Cour de cassation]
Il entre dans les missions de la Cour de se prononcer sur la conformité des jugements attaqués à la règle de droit. Il lui incombe ensuite de faire connaître ses décisions. Le numérique, y compris dans sa composante d'IA, s'implante progressivement dans ces deux tâches : le traitement des pourvois et la diffusion de la jurisprudence. Source Vie-publique

Législation

La CNIL rend son avis sur la proposition de loi « sécurité globale ».
Saisie par le président de la commission des lois du Sénat, la CNIL a rendu son avis sur la proposition de loi « sécurité globale » le 26 janvier 2021. Il sera présenté par la présidente de la CNIL au cours d'une audition publique le 3 février. Outre les implications éthiques, la CNIL constate qu'en l'état, le cadre juridique envisagé n'est pas suffisamment protecteur de la vie privée et des données personnelles.
Source CNIL – CNIL – SN – Cyberdroit – Siècle Digital

Le Conseil constitutionnel valide la loi dite « Anti Huawei ».
Le 5 février 2021, sur question prioritaire de constitutionnalité transmise par le Conseil d'État, le Conseil constitutionnel a validé différentes dispositions de la loi n° 2019-810 du 1er août 2019. Il a ainsi considéré que les dispositions soumettant l'exploitation de certains équipements de réseaux radioélectriques mobiles à autorisation du Premier ministre ne restreignaient pas de manière disproportionnée la liberté d'entreprendre, ne rompaient pas le principe d'égalité devant les charges publiques et ne portaient pas atteinte à la garantie des droits. Source Cyberdroit – Conseil Constitutionnel

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

Référence	Titre	Date
CERTFR-2021-AVI-149	Multiples vulnérabilités dans le noyau Linux d'Ubuntu	(26 février 2021)
CERTFR-2021-AVI-148	Multiples vulnérabilités dans Nagios XI	(26 février 2021)
CERTFR-2021-AVI-147	Multiples vulnérabilités dans les produits Cisco	(25 février 2021)
CERTFR-2021-AVI-146	Multiples vulnérabilités dans F5 BIG-IP	(25 février 2021)
CERTFR-2021-AVI-145	Multiples vulnérabilités dans les produits VMWare	(24 février 2021)
CERTFR-2021-AVI-144	Multiples vulnérabilités dans Mozilla Thunderbird	(24 février 2021)
CERTFR-2021-AVI-143	Multiples vulnérabilités dans Mozilla Firefox	(24 février 2021)
CERTFR-2021-AVI-142	Multiples vulnérabilités dans les produits Aruba	(24 février 2021)
CERTFR-2021-AVI-141	Vulnérabilité dans F5 BIG-IP	(24 février 2021)
CERTFR-2021-AVI-140	Vulnérabilité dans Python	(22 février 2021)
CERTFR-2021-AVI-139	Multiples vulnérabilités dans F5 BIG-IP	(22 février 2021)
CERTFR-2021-AVI-138	Multiples vulnérabilités dans le noyau Linux de SUSE	(22 février 2021)
CERTFR-2021-AVI-137	Vulnérabilité dans IBM WebSphere Cast Iron	(22 février 2021)
CERTFR-2021-AVI-136	Multiples vulnérabilités dans Asterisk	(19 février 2021)
CERTFR-2021-AVI-135	Vulnérabilité dans Xen	(19 février 2021)
CERTFR-2021-AVI-134	Multiples vulnérabilités dans Microsoft Edge	(18 février 2021)
CERTFR-2021-AVI-133	Multiples vulnérabilités dans Google Chrome OS	(18 février 2021)
CERTFR-2021-AVI-132	Vulnérabilité dans BIND	(18 février 2021)
CERTFR-2021-AVI-131	Vulnérabilité dans Cisco AnyConnect Secure Mobility Client	(18 février 2021)
CERTFR-2021-AVI-130	Multiples vulnérabilités dans Tenable Nessus Network Monitor	(18 février 2021)

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

Référence	Titre	Date
CERTFR-2021-ALE-003	Vulnérabilité dans VMWare vCenter Server	Alerte en cours le 25/02/2021
CERTFR-2021-ALE-002	Vulnérabilité dans Google Chrome	Alerte en cours le 05/02/2021
CERTFR-2021-ALE-001	Vulnérabilité dans SonicWall SMA100	Alerte en cours le 02/02/2021
CERTFR-2020-ALE-026	Présence de code malveillant dans SolarWinds Orion	Alerte en cours le 14/12/2020
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-2021-ACT-008	(15 février 2021)
CERTFR-2021-ACT-007	(15 février 2021)
CERTFR-2021-ACT-006	(08 février 2021)
CERTFR-2021-ACT-005	(01 février 2021)
CERTFR-2021-ACT-004	(25 janvier 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	78.7.1 ESR			
	Antérieures	CERTFR-2021-AVI-143	Mfsa2021-06	2021_02_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***

♦♦♦♦