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°69

Pôle Défense et Sécurité des Systèmes d'Information

Notes d'information technique

Edition ► Mai 2021

I – Cybercriminalité et attaques informatiques

Dans le MONDE

- ***Un club famille Nestlé piraté, des données volées.***
  Un pirate informatique vient de diffuser les données volées à un club « famille » de la marque Nestlé.
  Source Zataz

- ***En Belgique, des attaques DDoS de grande ampleur visent les institutions.***
  Le réseau Belnet a été victime d'une campagne d'attaques DDoS massives dans la journée d'hier, perturbant le fonctionnement de plus de 200 institutions belges. Une enquête a été ouverte par les services de police.
  Source ZDNet – UD

- ***Le ministère fédéral de l'Intérieur belge est victime d'un piratage informatique depuis deux ans.***
  Cette attaque a pour la première fois été classée dans la catégorie « crise nationale ». Selon plusieurs experts en cybersécurité, la Chine est très probablement derrière cette cyberattaque. Source Siècle Digital – ZDNet

- ***Le principal opérateur américain de pipelines est paralysé par un ransomware.***
  Le plus grand opérateur d'oléoducs pour produits raffinés aux États-Unis, le groupe Colonial Pipeline, a été frappé par un ransomware. Cet incident de sécurité a suspendu le fonctionnement d'un oléoduc de 8800 kilomètres transportant du diesel et de l'essence depuis Houston jusqu'à New York, approvisionnant 45 % de la côte Est. Depuis, le service n'a été réouvert que partiellement. Ce qui fait craindre des pénuries et donc une hausse des prix. Source UD – ZDNet – SN – Siècle Digital – Siècle Digital – ZDNet – UD

- ***Le cambriolage numérique totalement fou de la Police de Washington.***
  Le groupe de pirates informatiques caché derrière le ransomware Babuk vient de diffuser 250Go de données appartenant à la police de Washington. Les autorités ont voulu payer, mais pas assez pour les pirates !
  Source Zataz

- ***Canada : piratage d'une boutique de vente de cannabis.***
  Pièces d'identité, photographies … un pirate informatique diffuse des centaines de documents de clients et clientes d'une boutique canadienne de vente de cannabis. Source Zataz

- ***Une attaque au ransomware bloque les services de santé irlandais.***
  Les systèmes informatiques du service de santé irlandais ont été mis hors ligne par « précaution » et certains rendez-vous de consultation externe ont été annulés. Source ZDNet – ZDNet – UD

- ***Les données médicales de 270 millions d'Indonésiens seraient impliquées dans une fuite.***
  L'Indonésie est potentiellement victime d'une fuite de données de taille. Le ministère des communications a indiqué aux médias que les données du système de santé indonésien pourraient avoir été dérobées, mettant en péril les informations personnelles de 270 millions d'habitants. Une enquête est en cours.
  Source UD – Numerama

- ***Des millions de données d'Air India compromises.***
  Deux mois après la cyberattaque du fournisseur de systèmes de service SITA, la compagnie d'aviation indienne a annoncé être une victime collatérale. Air India a ainsi annoncé que plusieurs millions de données ont été compromises. Source LMI – ZDNet

  Un ransomware compromet les données de Bose.
  Le spécialiste du son Bose a été victime d'un ransomware début mars. La firme a alerté sur une violation de données. Source LMI

- ***Le réseau d'eau en Floride visé par un autre incident avant la tentative d'empoisonnement.***
  La société de cybersécurité Dragos a publié un rapport montrant qu'un navigateur de la ville d'Oldsmar a visité un site web contenant un code malveillant le même jour qu'une autre attaque. Source ZDNet

En FRANCE

Cybersécurité

Des failles par injection SQL ciblant des entreprises françaises aux enchères.
Un opérateur malveillant a annoncé la mise aux enchères de 168 failles par injection SQL relatives à des entreprises françaises dont Auchan, Axa, Banques Populaires ou encore Alinea et Agnès b. Faille logicielle ou attaque par rebond d'un fournisseur de services IT pourraient en être à l'origine. Source LMI

Le CAC 40 se mobilise contre la fraude par email.
94 % des cyberattaques sont aujourd'hui initiées via la boîte email, faisant de ce canal le principal vecteur de fraude en ligne. La plupart du temps, les pirates informatiques créent des leurres liés à l'actualité (COVID-19, impôts…) et usurpent les noms de domaines d'entreprises reconnues ou d'organisations légitimes pour piéger leurs victimes. Source GlobalSecurityMag – UnderNews

Attaque du CINOV
La Fédération des métiers de la prestation intellectuelle du Conseil, de l'Ingénierie et du Numérique victime des pirates d'Avaddon. Les pirates ont commencé à diffuser des données internes. Source Zataz

Piratées en décembre 2020, des données de l'Agglomération d'Annecy diffusées dans le darkweb
Dans la nuit du 27 au 28 décembre 2020, des pirates prennent d'assaut l'informatique de l'agglomération du Grand Annecy. Six mois plus tard, les voleurs diffusent des données dans le darkweb. Source Zataz

Veja, spécialiste des baskets éco-responsables, a été victime d'une cyberattaque
Les adresses emails des clients de la marque Veja ont été dérobées lors d'une cyberattaque. Les coordonnées bancaires et les mots de passe ont été épargnés, précise l'entreprise spécialisée dans la conception de baskets éco-responsables. Une plainte a été déposée. Source UD

Des bureaux asiatiques d'Axa ciblés par le ransomware Avaddon
L'assureur français a du mal avec les gangs de ransomware. Avaddon a revendiqué une attaque sur plusieurs succursales d'Axa en Asie et plus de 3 To de données auraient été subtilisées.
Source LMI – ZDNet – UD – Siècle Digital

DarkSide s'attaque maintenant à une filiale de Toshiba
Après Colonial Pipeline, c'est au tour de Toshiba Tec Corp de subir une cyberattaque au ransomware par le groupe DarkSide. La filiale française de l'entreprise semble avoir été visée. Source ZDNet – UD

La gestion des menaces internes préoccupante dans les entreprises françaises
Une récente enquête réalisée par l'éditeur Proofpoint en partenariat avec le CESIN révèle que les entreprises françaises s'améliorent sur la gestion des menaces internes, mais que des progrès restent à faire. Source LMI

Les données personnelles de 8 000 employés de Decathlon exposées (MAJ)
Une enquête menée par VPNmentor montre que des données incluant noms, mails, photos et jetons d'authentification de près de 8 000 employés de Decathlon ont été exposées. Une mauvaise configuration de bucket S3 relatif à un serveur utilisé par un partenaire du groupe en est à l'origine.
Source LMI – Siècle Digital – ZDNet

60 % des établissements d'enseignement victimes d'attaques de phishing
Selon une enquête de Netwrix, 60 % des établissements d'enseignement ont été victimes d'attaques de phishing ciblant les données du cloud. Il s'agit du taux le plus élevé parmi tous les secteurs analysés. L'étude révèle également que 27 % des établissements d'enseignement ont subi une attaque par ransomware et que 49 % d'entre eux ont mis plusieurs jours à la détecter. Source Alliancy

Ciseaux à bois, Team Viewer, et ATM Desk: les coulisses d'une filière de jackpotting
Un procès vient de dévoiler les méthodes d'une filière de jackpotting, ces piratages de distributeurs de billets, qui a visé des automates dans l'Est de la France à l'hiver 2018. Source ZDNet

Cyberdéfense

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

Le gouvernement réoriente sa stratégie sur le cloud de confiance
Label cloud de confiance, accord de licences avec les fournisseurs étrangers, renforcement juridique contre l'extra-territorialité de certaines lois étrangères, rationalisation des clouds pour l'administration, voici la feuille de route du Gouvernement pour sa stratégie nationale autour du cloud. Source LMI – IT Social

Atos, Sopra Steria, Idemia et Idakto ont été choisis pour le chantier de l'identité numérique
Atos, Sopra Steria, Idemia et Idakto ont été sélectionnés par le ministère de l'Intérieur pour développer le système de gestion de l'identité numérique du gouvernement. Atos remporte le lot le plus important, car il sera chargé de la maintenance des applications permettant aux Français de s'identifier aux services publics via FranceConnect. En revanche, le lot sur la reconnaissance faciale n'a pas encore été attribué. Source UD

Le SI de la Sécurité Civile confié à Scalian
Scalian, cabinet français de conseil en technologies, vient de se voir confier par le ministère de l'Intérieur la refonte du système d'information de l'ORSEC, un dispositif critique dans la préparation et la gestion des crises.
Source L'1FO

Les conseils de Bpifrance et Cybermalveillance aux PME-ETI
Moins médiatique que les attaques contre les grands groupes, les PME et PMI ne sont pas épargnées. Pour renforcer la sensibilisation, BPI France et la plateforme Cybermalveillance publient un guide avec différentes mesures afin de se protéger des menaces. Source LMI

La cyber-hygiène devient un impératif pour s'adapter à un univers de menaces post-pandémie
[par Derek Manky, Chief, Security Insights & Global Threat Alliances chez FortiGuard Labs]
Une menace qui existe bel et bien au sein des entreprises. D'autant qu'elle s'accentue, au fur et à mesure que les entreprises développent leurs réseaux et étendent leur surface d'attaque sans pour autant déployer d'architecture holistique ou de système de gestion dédiés à la sécurité. Source Alliancy

La task-force nationale de lutte contre les arnaques publie une version enrichie de son guide de prévention
En avril 2020, à l'initiative du ministère de l'Economie et des Finances, les services de l'État et les autorités de contrôle se sont associés au sein d'une « task-force de lutte contre les arnaques » afin de mutualiser leurs compétences et d'optimiser l'action publique dans le contexte de la crise sanitaire. La task-force publie une version enrichie de ce guide de prévention afin de protéger les consommateurs et les entreprises contre les fraudes et escroqueries. Source DGCCRF – DGCCRF

II – Actualités

Brèves

Cybersécurité

10 attaques couramment observées sur les réseaux Windows
Quelles sont les techniques préférées des cybepirates pour accéder aux réseaux Windows ? C'est ce qu'a voulu savoir Red Canary, le fournisseur de solutions d'opérations de sécurité en mode SaaS, dont le rapport comporte des conseils sur la surveillance des logs et le repérage des techniques d'intrusion. Source LMI – Reseaux&Telecoms

Les utilisateurs réticents à signaler des incidents de sécurité
Malgré une perception accrue des risques cyber avec la pandémie, les utilisateurs restent réticents à signaler les incidents de sécurité, comme le montre une récente étude de Fujitsu. Source LMI

Une réponse internationale pour combattre les ransomwares
Face aux déferlements des ransomwares, plusieurs experts ont créé un groupe de travail pour essayer d'endiguer cette menace. Plusieurs recommandations ont été émises autour de la coordination internationale et la régulation des crypto-monnaies. Source LMI

Une nouvelle étude menée par Enterprise Strategy Group (ESG) et HUMAN révèle les principales attaques de Bots, le niveau de préparation et les préoccupations des responsables de la sécurité dans les entreprises
HUMAN (anciennement White Ops) publie une nouvelle étude sur les perceptions et les réponses des responsables de la sécurité face aux attaques sophistiquées de bots. Source GlobalSecurityMag

La géographie des courriels d'hameçonnage révèle une toile d'araignée mondiale
Les pays d'où proviennent les courriels d'hameçonnage et le nombre de pays par lesquels ils sont acheminés jusqu'à leur destination constituent des signes précurseurs importants d'hameçonnage. Hélas, ils sont rarement pris en compte Source IT Social

Rançongiciels : seules 8 % des entreprises ayant versé une rançon ont pu restaurer l'ensemble de leurs données
En matière de rançongiciels, verser une rançon n'est pas une garantie de récupération des données chiffrées. Cela pourrait être en partie dû à la complexité liée à l'utilisation de clés de déchiffrement, d'un code de mauvaise qualité ou compilé à la hâte. Source IT Social

Que faire et ne pas faire en cas d'attaque de ransomware
[par Florian Malecki – Arcserve.]
Les décideurs IT se retrouvent coincés entre le marteau et l'enclume lorsqu'il s'agit de faire face à des attaques de ransomware. Payer et céder aux exigences des cybercriminels ? Utiliser les sauvegardes ? Certains optent pour une troisième option, et c'est là que la négociation entre en jeu. Source ZDNet

E-mails frauduleux : comment se protéger des hackers ?
L'e-mail est l'un des services de communication les plus utilisés au monde. Il cumule des millions d'envois et de réceptions par jour. Sa simplicité et sa rapidité dans la communication sont les raisons de son usage tant par les entreprises que par les particuliers. Source Data Security Breach

L'attaque des bots : augmentation de l'activité malveillante des bots et inquiétude des responsables sécurité
Les attaques de bots sont de plus en plus sophistiquées, allant de l'imitation des interactions numériques humaines à la récupération de données sensibles et au remplissage de formulaires web. Le niveau d'impréparation des entreprises inquiète les responsables de la sécurité. Source IT Social

Plus de 10 millions de dollars par mois sont perdus dans des arnaques aux cryptomonnaies
Les arnaques aux cryptomonnaies, nouvel Eldorado ? Les malfaiteurs surfent sur les espoirs de gains faciles alimentés par l'impressionnante croissance des cryptomonnaies pour mieux piéger leurs victimes. Source Numerama

Aperçu des cybermenaces mondiales au T1 2021 (janvier / février / mars)
Tous les trimestres, Kaspersky dresse un bilan des faits marquants et évolutions en matière de cybermenaces. Les rapports sont fondés sur l'analyse des menaces bloquées par les solutions technologiques Kaspersky ou identifiées par son équipe d'experts dans le monde entier.
Source GlobalSecurityMag – UnderNews

Plus de 290 entreprises touchées par six groupes de ransomware en 2021
Selon un rapport d'eSentire, les six groupes ont déjà récolté plus de 45 millions de dollars cette année auprès de dizaines de collectivités locales, d'hôpitaux, d'universités et de conglomérats multinationaux.
Source ZDNet

4,2 millions de dollars perdus par cyberattaque dans le secteur financier en Europe
Plus d'un an après le début de la pandémie, les banques, les assureurs et d'autres institutions financières font état de conséquences coûteuses dues à des cyberattaques venues du cloud et à des pannes de réseau. Source Globb Security – Globb Security

L'Europe doit penser communauté et besoin marché pour réussir !
[par David Bizeul – Sekoia.]
Face à l'explosion des cyberattaques, la Commission européenne a lancé une nouvelle stratégie de cybersécurité. L'enjeu ? Que la cybersécurité européenne ait une orientation commune tout en préservant ses souverainetés nationales. Source ZDNet

Cybersécurité de l'industrie

Verizon et Honda améliorent la sécurité des voitures autonomes avec la 5G
Honda a signé un partenariat avec le géant américain des télécommunications Verizon. En effet, cette coopération vise à explorer la manière dont la 5G et l'informatique mobile embarquée (MEC) peuvent accroître la fiabilité des véhicules connectés. Source OBJETCONNECTE

Les 5 tendances du secteur de la santé selon Zebra Technologies
Malgré les nombreux défis de 2020, les organisations de santé ont considérablement gagné en visibilité et expérience. Aujourd'hui, les hôpitaux sont en train d'adopter des technologies qui les aident à réaliser des économies essentielles mais aussi à être plus productifs. Ces avancées promettent d'être plus répandues dès lors que la pandémie ne sera plus qu'un lointain souvenir. Source GlobalSecurityMag

Cybersécurité industrielle – vers la fin (enfin) de l'empilement des solutions de sécurité ?
Cela fait plus de 20 ans que nous parlons des besoins en plateformes de sécurité entièrement intégrées. Et pourtant, à chaque fois qu'un nouveau défi de sécurité surgit, des centaines de fournisseurs se précipitent pour apporter une solution ciblée à cette menace spécifique. Résultat : un ensemble disparate de technologies et d'outils que les RSSI et leurs équipes de sécurité peinent à utiliser de manière efficace. Un rapport récent de l'institut Ponemon et d'IBM confirme cette tendance et révèle que les entreprises utilisent plus de 45 outils de sécurité différents en moyenne, et chaque incident traité nécessite un effort de coordination sur environ 19 outils. Source GlobalSecurityMag

IoT Industriel : comment surmonter les principaux défis liés à son intégration ?
L'intégration de l'IoT se diversifie, passant des applications grand public aux applications critiques dans le secteur industriel. Cette solution joue également un rôle clé dans la prochaine phase d'automatisation des usines, appelée Industrie 4.0. Source Objetconnecte

Sécurité numérique

La mauvaise collaboration entre les équipes sécurité et réseaux freine les projets de transformation numérique en Europe
Netskope dévoile une nouvelle étude surprenante montrant une rupture majeure dans la collaboration entre deux des principaux composants de l'équipe informatique – le réseau et la sécurité.
Source GlobalSecurityMag

22 % des PC dans le monde fonctionnent encore sous Windows 7, un système d'exploitation obsolète
Kaspersky s'est intéressé aux systèmes d'exploitation utilisés dans le monde et a réalisé une étude basée sur les métadonnées anonymisées des OS fournis par les utilisateurs consentants de son réseau Kaspersky Security Network. Au niveau mondial, près d'un quart (22 %) des utilisateurs de PC sont encore équipés de Windows 7, un système d'exploitation qui n'est plus pris en charge par Microsoft depuis janvier 2020. En France, ce chiffre tombe à 13,4 %. Lorsqu'un système d'exploitation arrive à la fin de son cycle de vie, aucune mise à jour supplémentaire n'est délivrée par le fournisseur, y compris les correctifs de sécurité. Source GlobalSecurityMag

Journée Internationale du Mot de passe – Les Français et leurs mots de passe : une étude exclusive Onfido dresse l'état des lieux
A l'occasion de la Journée Internationale du Mot de passe, Onfido, spécialiste de la vérification d'identité et de l'authentification en ligne, dévoile les résultats d'une étude internationale exclusive portant sur les relations, parfois compliquées, entre les internautes et leurs mots de passe.
Source GlobalSecurityMag – Data Security Breach

Passer de la conscience du risque à sa maîtrise
[par Pierre Oger, Directeur Général et Fondateur d'EGERIE]
Le 5e pilier stratégique pour l'amélioration de la cyber-résilience des collectivités ou de toute organisation requière la mise en œuvre d'un plan d'actions et d'amélioration continue. Source GlobalSecurityMag

Contre quoi protège vraiment le HTTPS ?
Si le HTTPS apporte une certaine confidentialité des échanges avec un site web, il ne garantira pas que ce site web est fiable et bienveillant. Source Numerarma

Quelles bonnes pratiques pour surveiller et gérer son réseau à distance ?
[par André Schindler – Directeur général EMEA chez NinjaRMM]
La crise sanitaire liée à la CoVid-19 a un impact considérable sur l'IT des entreprises. En effet, les équipes informatiques doivent s'adapter à une nouvelle normalité mixant des modes de travail hybride (présentiel et distanciel), réduisant comme peau de chagrin la frontière entre vie professionnelle et vie personnelle (la vie de bureau, mais à la maison) mettant à rude épreuve les réseaux/infrastructures informatiques et les « objets » qu'il compte en son sein. Source Globb Security

Auditer en continu son parc : un élément clé d'une gouvernance sécurité efficace
[par Thierry Balian, Directeur Business Unit Cybersécurité]
L'usage du numérique connaît chaque année une croissance exponentielle au sein des entreprises de toutes tailles. Dans ce contexte, les parcs informatiques ne cessent de se développer et de nouveaux équipements sont déployés à la hâte pour leur permettre de rester compétitives et de mener à bien leurs opérations. Source UnderNews

Pour 97 % des responsables IT, l'expérience utilisateur est une priorité
Une enquête mondiale effectuée par Citrix-Pulse révèle que les entreprises du secteur IT s'orientent vers de nouvelles approches de sécurité pour s'adapter à l'évolution des modalités du travail. Source IT Social

Tests phishings pour la sensibilisation : une réelle efficacité ?
En matière de sensibilisation des utilisateurs, la simulation d'attaques de phishing est à la mode. Si ce type de tests présente un réel intérêt, il faut faire attention à ne pas en faire le dispositif central de sa stratégie de sensibilisation. Parlons tout d'abord des points forts de ce type d'opérations. Le principe de ce type de tests est relativement simple. Il s'agit d'envoyer à une population cible un e-mail similaire à ceux qui sont utilisés pour de réelles opérations de phishing. Source UnderNews

FragAttacks : un cocktail de failles WiFi menace des millions de terminaux
Une compilation de failles affectant les protocoles WiFi a été mise à jour par un chercheur en sécurité. Avec à la clé des millions de terminaux potentiellement à risque. Source LMI

Le coût de reprise d'activité après attaque par ransomware flambe
Une enquête Sophos/Vanson Bourne sur les attaques par rançongiciel révèle que si le nombre d'entreprises victimes a diminué, en revanche le coût moyen de reprise d'activité a plus que doublé en l'espace d'un an. Les entreprises qui acceptent de payer une rançon ont très peu de chances de récupérer leurs données. Source LMI

4 conseils pour protéger vos données des éventuels sinistres
En matière de protection des données, les entreprises doivent s'équiper du meilleur et se préparer au pire. La mise en place d'un plan solide vous permettra de retomber sur vos pieds, quelle que soit l'ampleur de votre chute. Source Silicon

5 tactiques des pirates pour cacher leurs traces
Des outils de test de confiance aux LOLBINs (fichiers légitimes transformés), les attaquants abusent des plateformes et des protocoles de confiance pour échapper aux contrôles de sécurité. Voici quelques tactiques utilisées par les cybercriminels. Source LMI

Baromètre du premier trimestre 2021
Le premier trimestre de l'année 2021 est logiquement marqué par du « spam covid-19 », tandis que sur le front du phishing, la technique dite des « replay campaigns » (qui consiste à reprendre in extenso une campagne d'e-mailing légitime dans la foulée de son envoi à des fins d'escroquerie) a une nouvelle fois souligné le caractère évolutif et adaptatif des méthodes utilisées par les cyber-criminels.
Source Signal Spam – Signal Spam

Recommandations relatives à l'administration sécurisée des systèmes d'information
L'administration d'un SI se traduit par un ensemble de mesures techniques et non techniques visant entre autres à maintenir le SI en condition opérationnelle et de sécurité et à gérer des changements mineurs ou des évolutions majeures. Source ANSSI – ANSSI – ANSSI

Sécuriser un site web
Les recommandations de ce guide concernent la sécurité des contenus présentés par un navigateur web aux utilisateurs. Les sujets abordés se concentrent autour des standards du Web, dont les implémentations côté navigateur requièrent des paramètres à spécifier lors du développement et de l'intégration d'un site ou d'une application web, de façon à en garantir la sécurité. Source ANSSI – ANSSI

Sûreté

Les métiers IT des data centres
Les graves conséquences de l'incendie qui a frappé OHV ont rappelé le rôle clé que jouent les data centers dans l'écosystème IT. Ces sites emploient des câbleurs, des électriciens, des techniciens du froid et de la climatisation… mais aussi des informaticiens. Dédiés à des fonctions support, ils assurent l'exploitation de ressources informatiques pour des clients comme les acteurs du Cloud, les opérateurs télécom, mais aussi des banques ou des industriels. Tour d'horizon d'une profession méconnue, mais qui ne connaît pas la crise. Source L'1FO

Contrôle d'accès et serrures connectées : savoir anticiper la cybermenace
[par Stevenson Olibrice, SimonsVoss Technologie]
Maisons, hôtels et smart buildings regorgent de plus en plus d'appareils IoT interconnectés, pilotables via la voix ou une application mobile. Mais qui dit objets connectés dit aussi sécurité, et la vulnérabilité liée à un cryptage de données qui n'est pas suffisamment évoluée. De ce fait, les serrures connectées et les systèmes de contrôle d'accès, qui ont le vent en poupe, n'échappent pas à la règle. Est-ce suffisant pour éveiller la vigilance des utilisateurs ? Source ZDNet

IoT (objets connectés) / IA

Un hacker peut prendre le contrôle de ce babyphone mis en avant sur Amazon
L'équipe de recherche de Bitdefender a découvert comment pirater les babyphones de la marque Victure. Source Numerama

Des chercheurs alertent sur une nouvelle forme de hack visant les IA
Des chercheurs du centre de cybersécurité du Maryland, État de l'est des États-Unis, ont publié une étude dans laquelle ils alertent sur un nouveau type de cyberattaque visant spécifiquement les intelligences artificielles. L'attaque force le réseau neuronal à utiliser beaucoup plus d'énergie, entraînant un ralentissement de son efficacité. Source Siècle Digital

LOGICIELS MALVEILLANTS

Malware – Ransomwares

Une backdoor dans le malware Royal Road vise les sous-marins nucléaires russes
Une backdoor dans le malware RTF RoyalRoad délivrée par hameçonnage ciblé a été découverte dans une attaque visant un centre de conception russe spécialisée dans les sous-marins nucléaires.
Source LMI

Trois nouvelles familles de malwares découvertes
Doubledrag, Doubledrop et Doubleback sont l'œuvre de cyberattaquants « expérimentés » et dont les motivations pourraient être d'ordre financier, si on se réfère à leur modus operandi. Source ZDNet

Apple s'inquiète de la quantité de malwares sur les Mac
La cybersécurité s'impose comme la raison principale pour laquelle Apple doit garder l'iPhone, l'iPad et ses autres produits mobiles derrière le jardin clos de l'App Store, explique un cadre supérieur d'Apple.
Source ZDNet

Pour se préserver, le milieu cybercriminel fait mine de découvrir que les rançongiciels, c'est mal
Les représailles du pouvoir américain après la cyberattaque contre Colonial Pipeline a laissé des traces. Deux forums très utilisés par les gangs de cybercriminels pour recruter des hackers ont banni les rançongiciels des discussions. Source Numerama

Malwares brésiliens en augmentation : Kaspersky découvre qu'un nouveau cheval de Troie bancaire se propage à l'échelle mondiale
Les chercheurs Kaspersky ont découvert Bizarro, un nouveau malware bancaire en provenance du Brésil ayant ciblé 70 banques sud-américaines et européennes, dont 8 françaises.
Source GlobalSecurityMag – ZDNet

Qui se cache derrière les ransomwares ?
Derrière les ransomwares se trouve une myriade d'acteurs qui interagissent via des forums hébergés sur le darknet, d'après un rapport publié ce mercredi par Kaspersky. Dans la majorité des cas, ils choisissent leurs victimes par opportunisme. Les moins bien protégées sont des cibles faciles, d'où l'importance de renforcer sa sécurité informatique. Source UD

ACTUALITES JURIDIQUES - Législation et jurisprudences

CNIL

Clôture de l'injonction prononcée à l'encontre de GOOGLE
Par décision du 30 avril 2021, la formation restreinte de la CNIL a clôturé l'injonction prononcée à l'encontre des sociétés GOOGLE LLC et GOOGLE IRELAND LIMITED le 7 décembre 2020.
Source CNIL – Legifrance

Compteurs communicants LINKY : clôture de la mise en demeure à l'encontre d'ENGIE
Par décision du 4 mai 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 ENGIE le 10 février 2020. Source CNIL – Legifrance

COVID-19 : les questions-réponses de la CNIL sur les tests salivaires de dépistage des élèves dans les établissements scolaires
Le ministre de l'Éducation nationale a déployé des campagnes de tests salivaires de dépistages massifs des élèves dans les établissements scolaires. La CNIL répond aux questions que les jeunes et leurs parents se posent sur la protection de leurs données dans ce cadre. Source CNIL

Entrepôt de données santé IQVIA : la CNIL rappelle les conditions et le cadre légal ayant permis son autorisation en 2018
Dans son prochain épisode « Nos données personnelles valent de l'or ! » diffusé le 20 mai 2021, Cash Investigation s'intéresse à la société IQVIA et à sa collecte de données de santé à travers les pharmacies. La CNIL étant citée pour avoir autorisé en 2018 la constitution de cet entrepôt de données, elle rappelle les règles applicables et les garanties exigées d'IQVIA. Source CNIL

La CNIL publie son rapport d'activité 2020
Impact de la crise sanitaire, nouvelles règles sur les cookies, cybersécurité et souveraineté numérique : dans son 41e rapport d'activité, la CNIL revient sur les temps forts de l'année et son bilan, marqué par un nombre de plaintes toujours élevé et une augmentation considérable des violations de données, trois ans après l'entrée en application du RGPD. Source CNIL – CNIL – CNIL – CNIL – LMI

COVID-19 : la CNIL accompagne l'AP-HP dans le cadre d'un concert expérimental à Paris
Dans le cadre de la politique de déconfinement mise en place par le Gouvernement, la CNIL a accompagné et autorisé un projet de recherche visant à évaluer la transmission de la COVID-19 lors d'un concert expérimental organisé le 29 mai prochain. Source CNIL

Refuser les cookies doit être aussi simple que de les accepter : une vingtaine d'organismes mis en demeure
La Présidente de la CNIL a adressé le 18 mai 2021 une vingtaine de mises en demeure à des organismes ne permettant pas aux internautes de refuser les cookies aussi facilement que de les accepter. Parmi eux figurent des acteurs internationaux de l'économie numérique et plusieurs organismes publics. Ils ont un mois pour se mettre en conformité. Source CNIL – LMI – HAAS Avocats

RGPD – (Règlement général sur la protection des données)

Données personnelles de santé : la CNIL a-t-elle fait son travail sur Iqvia ?
Le géant américain de l'exploitation des données personnelles de santé Iqvia va faire l'objet de contrôles par la CNIL après un reportage sur cette société. Finalité d'usage au titre de l'intérêt public, droit d'opposition des personnes et risques de ré-identification vont être passés au peigne fin. Source LMI

Conformité, cybersécurité, formation… Quel bilan peut-on faire trois ans après la sortie du RGPD ?
47 % des entreprises et des organismes publics estiment avoir atteint « un niveau de complétude » supérieur à 70 % concernant le RGPD, rapporte une enquête menée par Data Legal Drive en partenariat avec Lefebvre Dalloz et l'Association française des juristes d'entreprise. Les niveaux de cybersécurité et de formation des salariés sont également en augmentation. Cependant, des efforts restent encore à faire, notamment dans les secteurs de la santé et de l'éducation. Source UD – IT Social

La protection des données de santé aux Etats Unis : qu'est-ce que l'HIPAA ?
[Par Stéphane Grynwajc, Avocat]
Depuis sa mise à jour par l'HITECH Act de 2009, HIPAA, la réglementation fédérale américaine en matière de données de santé, s'applique aux prestataires de soins mais aussi à leurs sous-traitants qui gèrent des informations médicales protégées. S'ajoute à la réglementation fédérale une myriade d'autres lois sectorielles et étatiques, qui peuvent s'appliquer à vos activités, en complément ou remplacement de ces lois fédérales. Source Village de la justice

Droit des TIC

Votre employeur a-t-il le droit de lire vos mails personnels ?
C'est une question qui revient régulièrement : un employeur a-t-il le droit de consulter les mails de ses salariés ? Tout dépend de quelle façon vous y accédez et de quelle manière ils sont identifiés.
Source Numerama – CNIL

La Cybersécurité au cœur des enjeux de l'entreprise moderne [par Shems Osmani, Juriste]
La protection des données numériques est devenue l'un des défis majeurs de notre époque. Nouvelle source d'enjeux politiques et économiques, dans un monde interconnecté où la collecte d'informations et les échanges numériques explosent, l'exposition aux cyber-attaques ne cesse d'augmenter.
Source Village de la justice

Le droit des chercheurs sur leurs créations scientifiques [Par Dalila Madjid, Avocat]
« *La connaissance s'acquiert par l'expérience, tout le reste n'est que de l'information* » Albert Einstein.
Les chercheurs, terme générique qui renvoie aux personnes qui se consacrent à la recherche scientifique, œuvrant dans la majorité des cas dans le cadre d'une mission de service public, peuvent s'interroger sur leurs droits et obligations qu'ils ont lorsqu'ils créent dans le cadre de leur activité scientifique.
Source Village de la justice

Juridique

Réaliser une recette de développement est un impératif
Une jurisprudence vient rappeler le caractère indispensable de la recette par le client et donc du test des développements livrés par un prestataire. Source LMI

Le Conseil constitutionnel dit non à l'utilisation des drones de surveillance
Saisi par 60 parlementaires et le Premier ministre, le Conseil constitutionnel a invalidé l'article encadrant l'utilisation des drones par certains services de l'État et la police municipale. Il juge que ce texte n'assure pas une conciliation équilibrée entre la protection de la vie privée et la prévention des atteintes à l'ordre public et de recherche des auteurs d'infraction. Source UD – Conseil constitutionnel

L'accès aux données de communications électroniques à des fins pénales
[Par Kate Jarrard et Noa Setti]
Par un arrêt du 2 mars 2021, la CJUE s'est prononcée sur les conditions d'accès par les autorités nationales, à des fins de lutte contre la criminalité et dans le cadre d'une procédure pénale, aux données de trafic et de localisation conservées par les fournisseurs de services de communications électroniques.
Source HAAS Avocats

Livraison d'un site : vérification préalable de son bon fonctionnement
Dans un jugement du 22 avril 2021, le tribunal judiciaire de Marseille a rappelé l'obligation du client, qui commande à un prestataire le développement d'un site, de vérifier son bon fonctionnement en procédant à son recettage. Source Legalis – Legalis

Législation

La communication politique par courriel à partir de la liste électorale consulaire
Les Français installés à l'étranger peuvent recevoir des messages électroniques de prospection politique. Dans la majorité des cas, les adresses de messagerie utilisées par les partis politiques ou les candidats proviennent des listes électorales consulaires. Cette pratique est légale. Source CNIL

Le Parlement pousse pour la création d'un parquet dédié à la cybercriminalité
Un document contenant 27 propositions pour lutter contre la cybercriminalité en France a été remis à Emmanuel Macron pour compléter le plan national présenté le 18 février 2021. Source Siècle Digital

Projet de loi relatif à la prévention d'actes de terrorisme et au renseignement : la CNIL publie ses avis
La CNIL s'est prononcée sur les dispositions du projet de loi qui intéressent la protection des données personnelles. Dans ses avis, elle rappelle notamment que les moyens mis en œuvre en matière de renseignement doivent être assortis de garanties fortes pour limiter les atteintes à la vie privée des personnes. Source CNIL – CNIL – CNIL – CNIL

La CNIL rend son avis sur le projet de passe sanitaire pour l'accès aux grands rassemblements de personnes
La CNIL s'est prononcée, le 12 mai 2021, sur le projet du Gouvernement relatif à la mise en place d'un passe sanitaire conditionnant l'accès à certains lieux publics recevant de grands rassemblements de personnes. La CNIL demande que la loi soit précisée et des garanties supplémentaires apportées.
Source CNIL – CNIL – vie-publique

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

Référence	Titre	Date
CERTFR-2021-AVI-416	[SCADA] Vulnérabilité dans les produits Siemens	(31 mai 2021)
CERTFR-2021-AVI-415	Multiples vulnérabilités dans les produits Stormshield	(28 mai 2021)
CERTFR-2021-AVI-414	Multiples vulnérabilités dans Microsoft Edge	(28 mai 2021)
CERTFR-2021-AVI-413	Vulnérabilité dans SonicWall NSM On-Prem	(28 mai 2021)
CERTFR-2021-AVI-412	Multiples vulnérabilités dans MOXA NPort	(27 mai 2021)
CERTFR-2021-AVI-411	Vulnérabilité dans Juniper Junos OS	(27 mai 2021)
CERTFR-2021-AVI-410	Vulnérabilité dans ISC Bind	(27 mai 2021)
CERTFR-2021-AVI-409	Vulnérabilité dans Drupal core	(27 mai 2021)
CERTFR-2021-AVI-408	Vulnérabilité dans IBM Spectrum Protect Snapshot	(27 mai 2021)
CERTFR-2021-AVI-407	Multiples vulnérabilités dans le noyau Linux de RedHat	(27 mai 2021)
CERTFR-2021-AVI-406	Multiples vulnérabilités dans le noyau Linux de SUSE	(27 mai 2021)
CERTFR-2021-AVI-405	Multiples vulnérabilités dans le protocole Bluetooth	(26 mai 2021)
CERTFR-2021-AVI-404	Multiples vulnérabilités dans Google Chrome	(26 mai 2021)
CERTFR-2021-AVI-403	Multiples vulnérabilités dans les produits VMware	(26 mai 2021)
CERTFR-2021-AVI-402	[SCADA] Multiples vulnérabilités dans Siemens Solid Edge	(26 mai 2021)
CERTFR-2021-AVI-401	Vulnérabilité dans IBM Db2	(26 mai 2021)
CERTFR-2021-AVI-400	Multiples vulnérabilités dans Joomla!	(26 mai 2021)
CERTFR-2021-AVI-399	Vulnérabilité dans Nginx	(26 mai 2021)
CERTFR-2021-AVI-398	Multiples vulnérabilités dans les produits Apple	(25 mai 2021)
CERTFR-2021-AVI-397	Vulnérabilité dans les produits QNAP	(21 mai 2021)

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

Référence	Titre	Date
CERTFR-2021-ALE-010	Vulnérabilité dans Adobe Acrobat et Acrobat Reader	Alerte en cours le 12/05/2021
CERTFR-2021-ALE-009	Vulnérabilité dans Microsoft Windows	Alerte en cours le 12/05/2021
CERTFR-2021-ALE-008	Multiples vulnérabilités dans Exim	Alerte en cours le 05/05/2021
CERTFR-2021-ALE-007	Vulnérabilité dans Pulse Connect Secure	Alerte en cours le 20/04/2021
CERTFR-2021-ALE-004	Multiples vulnérabilités dans Microsoft Exchange Server	Alerte en cours le 03/03/2021

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

Référence	Date
CERTFR-2021-ACT-023	(31 mai 2021)
CERTFR-2021-ACT-022	(28 mai 2021)
CERTFR-2021-ACT-021	(25 mai 2021)
CERTFR-2021-ACT-020	(18 mai 2021)
CERTFR-2021-ACT-019	(17 mai 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	78.10.1 ESR			
	Antérieures	CERTFR-2021-AVI-340	Mfsa2021-16	2021_04_23
Client officiel Pablo *	3.1.20	Multiples vulnérabilités		
Adobe Reader	Reader DC			
	Antérieures	CERTFR-2021-AVI-360	APSB21-29	2021_05_12
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-2021-AVI-353	Bulletin de sécurité Foxit du 06 mai 2021	
VLC	3.0.14			
	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***

♦♦♦♦