HUISSIERS DE JUSTICE • COMMISSAIRES DE JUSTICE

LE JOURNAL

H.-S. N°1 • MAI 2021

Bimestriel d'information de la Chambre nationale des commissaires de justice et de la section professionnelle des huissiers de justice

Sécurité informatique

Le risque cyber & la profession

Hors-Série

LE MOT DE LA CNCJ

Cette période difficile, émaillée d'attaques répétées, nous a montré l'importance d'une réflexion élargie sur la sécurité numérique pour l'ensemble de notre écosystème. Architecturé autour des multiples facettes de nos métiers, celui-ci est d'ailleurs complexe, par la richesse et la diversité de ses acteurs, qu'il s'agisse des offices ou de la CNCJ et de ses filiales. De cette richesse naissent des enjeux numériques d'envergure pour lesquels la sécurité est un important pilier.

La CNCJ s'investit depuis 2016, sous l'impulsion de sa gouvernance et à travers sa direction informatique dans la mise en œuvre d'une démarche de gestion du risque et de la sécurité numérique au bénéfice de la profession, de son écosystème numérique et de ses partenaires. Nous avons entrepris un grand nombre d'actions de communication, de sensibilisation et nous continuons encore cette année principalement autour de la formation pour améliorer vos connaissances.

COMMISSAIRES DE JUSTICE
CHAMBRE NATIONALE
Section Huissiers de justice

La démarche de la CNCJ se traduit par des investissements humains, opérationnels et techniques significatifs afin de pouvoir assurer une veille active et continue dans ce domaine, associée à la mise en œuvre de différents programmes d'anticipation, de solutions, d'accompagnement, en relation étroite avec ses filiales et au bénéfice des offices.

Cet ensemble traduit une volonté forte de la CNCJ de soutenir et d'accompagner l'ensemble de la profession au plus près des enjeux de sécurité numérique. Étant moi-même un mauvais élève en matière de cybersécurité, le bureau m'a désigné, ainsi que Stephan Hubert, membre du bureau de section, et trois délégués, Élisabeth Fitoussi, Jean-Luc Bourdiec et Damien Tronel pour que nous nous assurions que les tutoriels et les formations (v. p. 10) qui seront prochainement proposés soient accessibles à toutes les consœurs et tous les confrères.

Je tiens à remercier le service informatique, dont le directeur est Bruno Le Nozer, notre partenaire Verspieren, notre consultant risques et sécurité, Jean Vinciguerra, et tous les autres acteurs autour de la sécurité numérique.

Pascal THUET
Trésorier de la CNCJ

LE MOT DE L'ANSSI

Comme tous les acteurs de la transformation digitale, les huissiers de justice bénéficient très largement des opportunités, à venir ou déjà apportées, par les services numériques mais en connaissent désormais les risques. Depuis maintenant plusieurs années, l'ANSSI, comme tous les services engagés dans la lutte contre la cybercriminalité, constate une augmentation des attaques informatiques, à la fois en volume et en sophistication. Cela fait longtemps que les courriels d'hameçonnage, qui cherchent à pousser le destinataire à cliquer sur un lien malveillant, ne contiennent plus de fautes grossières ou de logos mal imités. Ou que les modes de chiffrement des rançongiciels résistent aux méthodes classiques de déchiffrement, rendant ainsi plus complexe la réponse à apporter à un incident de cette nature.

S'il n'y a malheureusement que peu de raisons pour que cette tendance s'inverse, il est désormais acquis que la bonne application de certaines règles basiques de sécurité informatique permet de se prémunir d'une très large majorité des risques. Il est d'ailleurs probable que dans quelques années, on se souviendra avec étonnement du peu de prudence que nous avions vis-à-vis de la gestion de nos systèmes d'information.

La manière de s'authentifier et d'accéder à un réseau, la complexité de nos mots de passe, la séparation des usages numériques professionnels et privés, le chiffrement de données sensibles et plus généralement la fin d'une certaine naïveté face aux menaces informatiques seront devenus des principes compris et adoptés par tous les acteurs qui auront placés le numérique au cœur de leurs métiers.

La mise en application du RGPD est un accélérateur puissant dans la sécurisation de données personnelles. Mais la réflexion de chacun sur la protection de ses données ne doit pas s'arrêter à la conformité à ce règlement, il faut poursuivre l'effort en déployant une analyse plus globale qui intègre davantage de risques numériques. Nous savons aujourd'hui qu'une simple usurpation de compte de messagerie peut donner à un attaquant des moyens de dérober ou paralyser l'ensemble des données d'une administration, d'une entreprise, d'une profession libérale ou réglementée. L'action entreprise par la CNCJ de communiquer sur le risque cyber dans votre profession est donc tout à fait pertinente et concourt très significativement à mettre vos réseaux, vos données, hors de portée d'attaquants.

Des actions ont été menées ces derniers temps par votre Chambre nationale pour améliorer la défense de vos outils communs. Il est en revanche de votre responsabilité, en tant qu'huissier de justice, de prendre en compte ces enjeux au juste niveau et de décider la mise en œuvre des mesures de sécurité numérique nécessaires dans vos propres structures.

Le risque numérique ne doit ni être perçu comme une épée de Damoclès ni comme un enjeu purement technique, ne concernant que des experts informatiques. Sans anxiété mais avec lucidité et persévérance, il vous revient de hausser le niveau de vos défenses informatiques afin de pérenniser la poursuite de vos activités mais également de contribuer à la sécurité plus globale de l'écosystème dans lequel vous opérez. C'est dans ce sens que l'ANSSI soutient ce projet centré sur la formation aux risques numériques.

Patrice BIGEARD
Délégué sécurité du numérique Île-de-France
SGDSN Service du Premier ministre

QUELS RISQUES CYBER POUR L'ÉTUDE ?

L'agence nationale de sécurité des systèmes d'information recense un certain nombre de risques relatifs aux attaques numériques. On retiendra principalement pour l'étude des risques liés aux usages numériques de la profession :

- Le blocage de l'activité avec ou sans demande de rançon par l'introduction d'un logiciel malveillant qui va chiffrer les informations métiers.
- Le vol d'information métier pour la revente, la diffusion malveillante ou pour rançonner l'office.
- L'utilisation de l'identité et des moyens numériques de l'office pour propager des informations malveillantes ou attaquer d'autres organismes.

Les 12 bonnes pratiques à adopter pour les éviter

01

Choisissez vos mots de passe avec soin

12 caractères de type différent (1 majuscule, 1 minuscule, 1 chiffre, 1 caractère spécial) n'ayant aucun lien avec vous et ne figurant pas dans le dictionnaire.

02

Mettez à jour régulièrement vos logiciels

– Définissez et faites appliquer dans votre office une politique de mise à jour régulière ;

– Configurez vos logiciels pour que les mises à jour s'installent automatiquement, systématiquement pour les mises à jour de sécurité et chaque fois que cela est possible pour les autres ;

– Utilisez exclusivement les procédures de mise à jour recommandées par les éditeurs. N'utilisez que les sites internet officiels des éditeurs si vous devez télécharger les mises à jour par vous-même.

Bien connaître ses utilisateurs et ses prestataires

– Définissez des droits d'accès à votre informatique en fonction des usages ;

– Vous devez vous assurer que les droits de chacun de vos utilisateurs soient limités aux besoins de leur activité. Les droits d'administration de votre informatique doivent être strictement limités à des utilisateurs ou prestataires de confiance et disposant des connaissances nécessaires.

Effectuez des sauvegardes régulières

Assurez-vous que vos sauvegardes soient bien réalisées, et utilisables en cas de besoin. Gardez-les sur des supports numériques isolés du reste de votre informatique.

Sécurisez votre réseau informatique

– Chaque poste doit être équipé d'un anti-virus actif et à jour ;

– L'accès à internet doit être filtré et sécurisé par un équipement approprié (à définir avec votre prestataire informatique) ;

– Dans la mesure du possible, mettez en œuvre un réseau filaire pour les ordinateurs de votre office et réservez l'usage du WIFI à des activités non confidentielles ;

– Dans le cas de l'utilisation du WIFI pour vos activités métiers, assurez-vous de la mise en œuvre d'un niveau approprié de sécurisation de votre connexion.

Soyez aussi prudent avec votre smartphone ou votre tablette qu'avec votre ordinateur

Protégez vos données lors de vos déplacements

– Voyager avec des appareils professionnels nomades fait peser des menaces sur des informations sensibles dont le vol ou la perte auraient des conséquences importantes sur les activités de l'organisation ;

– Évitez d'utiliser les WIFI gratuits des restaurants et des hôtels ou utilisez une solution de sécurisation de votre connexion.

Soyez prudent lors de l'utilisation de la messagerie

Les courriels et leurs pièces jointes jouent souvent un rôle central dans la réalisation des attaques informatiques (courriels frauduleux, pièces jointes piégées, etc.). Il existe des outils et des process pour filtrer les courriels (ex. : solutions antispam).

09 **Téléchargez vos programmes sur les sites officiels des éditeurs uniquement**

10 **Soyez vigilant lors d'un paiement sur internet depuis vos outils informatiques**

– N'utilisez que des sites réputés et sécurisés (présence d'un petit cadenas à gauche du nom du site) ;
– N'enregistrez pas votre numéro de carte bancaire sur le site ;
– Ne transmettrez pas votre numéro de carte ou vos codes dans un message en clair ;
– Privilégiez le paiement vers un site bancaire avec une procédure de vérification.

11 **Séparez les usages personnels des usages professionnels**

– Utilisez des navigateurs ou des conteneurs de navigation différents ;
– Évitez d'utiliser votre client de messagerie professionnel pour consulter vos messages personnels ;
– Réduisez vos téléchargements aux seuls cas professionnels sur votre poste de travail.

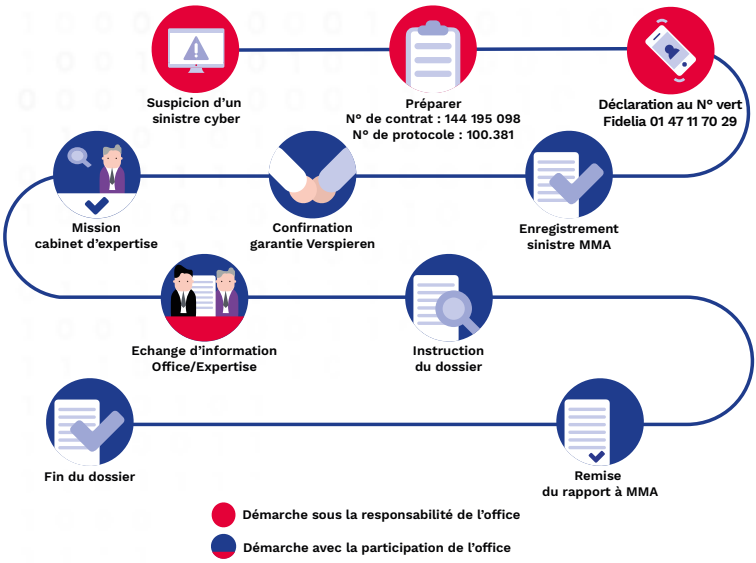
12 **Prenez soin de vos informations personnelles, professionnelles et de votre identité numérique. Soyez particulièrement circonspect sur les réseaux sociaux**

– Séparez vos comptes professionnels et personnels sur les réseaux sociaux ;
– Utilisez une identification différente (photo, présentation) pour chacun ;
– Prêtez une attention particulière aux messages personnels que vous pourriez diffuser à partir de votre compte professionnel. Votre communication professionnelle doit le rester strictement.

QUE DOIS-JE FAIRE ?

Si je suis victime d'une cyber attaque :

Appellez le numéro vert selon le processus ci-dessous
Signalez le problème à la CNCJ sur l'adresse : digitalalerte@huissier-justice.fr



Choisissez un Référent Sécurité Numérique !

Son rôle principal : Être le relais de la politique de sécurité numérique de la CNCJ, c'est-à-dire, sensibiliser et former au sein de l'office.
Le Référent Sécurité peut être le même que celui désigné pour le RGPD, il est tout de même préférable qu'il ait une sensibilité sur le sujet.

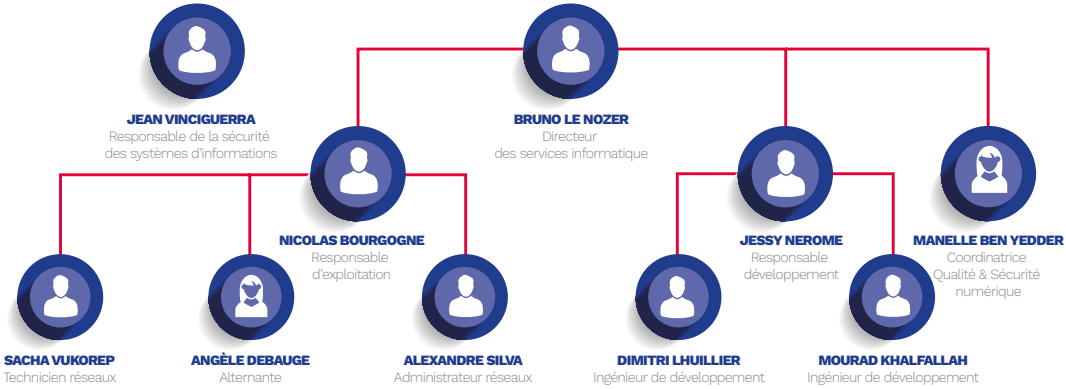
Formez-vous !

Des formations sur la sécurité numérique seront proposées au second semestre 2021 avec pour thèmes :
– Identification des éléments sensibles présents dans un office ;
– Votre environnement ;
– La contractualisation ;
– Types de menaces et canaux ciblés et bonnes pratiques ;
– Recueil des éléments.

Ces tutoriels de formation seront disponibles et consultables le moment venu, gratuitement, sur le RPSH.

Gardez ce livret à portée de main pour réagir au plus vite !

SERVICE INFORMATIQUE



Contact : support@huissier-justice.fr

Supplément Le Journal des commissaires de justice huissiers de justice

Bulletin d'information de la Chambre nationale des huissiers de justice Hors série. n°1 / Mai 2021
(Bon à tirer donné le xx/xx/2021)
Directeur de la publication : Thierry Bary
Rédactrice en chef : Clémentine Delzanno
Société d'édition - Réalisation : Editions juridiques et techniques
SARL au capital de 405 950 €
73, boulevard de Clichy - 75009 Paris
Tél. : 01 45 26 56 84 - **Fax :** 01 45 26 38 76
Mail : journal@editions-ejt.com
Gérant : Thierry Bary
Maquette et mise en page : Géraldine Delplanque
Impression : Corlet Imprimeur
Z.A. Maximilien Vox - 14110 CONDE-SUR-NOIREAU Dépôt légal : 1er semestre 2021
ISSN : 2275-1467

Imprimé sur papier labellisé PEFC.

COMMISSAIRES DE JUSTICE
CHAMBRE NATIONALE
Section
Huissiers de Justice

Chambre nationale des commissaires de Justice
Section professionnelle des huissiers de Justice
44, rue de Douai - 75009 Paris
Tél. +33 (0)1 49 70 12 90 • Fax +33 (0)1 40 16 99 35
www.commissaire-justice.fr • www.huissier-justice.fr