Guide de la cybersécurité

Sommaire

L'état des lieux

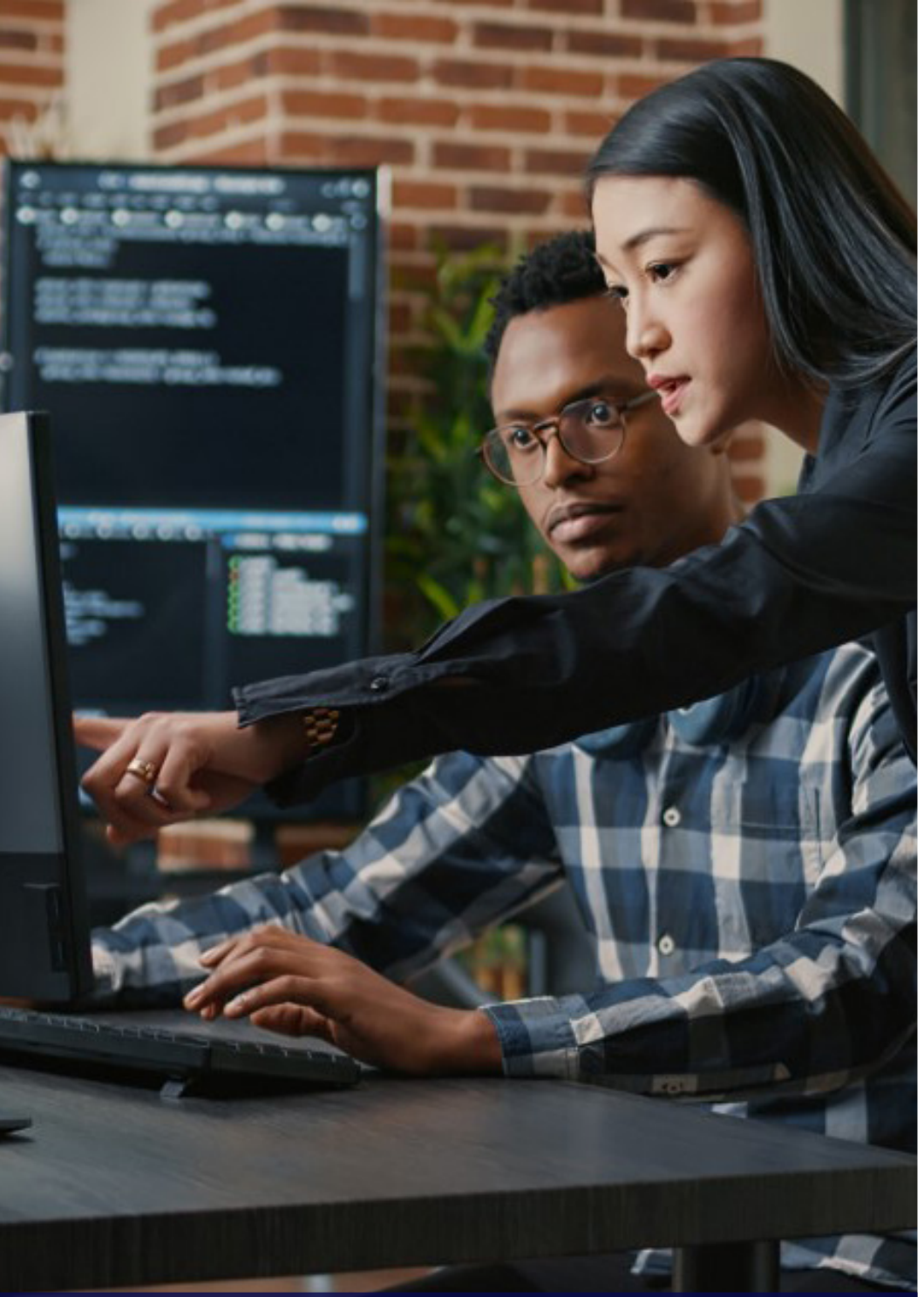
Le secteur de la cybersécurité

SUP DE VINCI
INGÉNIERIE DES SYSTÈMES D'INFORMATION

esli esti
CAMPUS E.S.P.R.I.T. Industries

GROUPEADSN

L’état des lieux



Pourquoi se lancer ou se reconvertir dans la cybersécurité en 2022 ? Découvrez nos 5 bonnes raisons. © DC Studio - stock.adobe.com

5 bonnes raisons de s'orienter dans les métiers de la cybersécurité

Tour d'horizon des principaux avantages qu'offre le secteur de la cybersécurité pour les futurs professionnels.

Les métiers de la cybersécurité vous intéressent, mais vous hésitez encore à vous orienter ou vous reconvertir dans ce domaine ? De belles opportunités s'offrent à vous, avec des professions et des missions variées, des salaires compétitifs, ainsi que de nombreux postes à pourvoir ! Voici 5 bonnes raisons de vous lancer dans la cybersécurité en 2022.

1. La cybersécurité est un secteur en pénurie de talents et qui recrute

Le constat est sans appel : en 2022, les entreprises sont confrontées au quotidien aux risques cyber. Les menaces sont multiples : des ransomwares au phishing et smishing (hameçonnage par SMS), en passant par les nombreux malwares sur mobile et sur desktop, les différentes failles de sécurité détectées (Apple, Windows, WordPress...), le sabotage et l'espionnage informatique par des organisations malveillantes, ou encore des attaques ciblant des infrastructures critiques...

Les entreprises, les associations, ainsi que les structures publiques ont plus que jamais besoin de talents pour les

aider à identifier les vulnérabilités dans leurs systèmes d'information, mettre en place une politique et des outils de cybersécurité efficaces pour contrer les cyberattaques, tout en évangélisant les bonnes pratiques auprès de leurs collaborateurs. Au total, ce sont plus de 15 000 postes qui sont actuellement à pourvoir dans la cybersécurité en France !

Face à la pénurie de talents, les possibilités dans ce domaine sont légion. En vous formant ou en suivant un projet de reconversion dans ce secteur qui recrute, vous serez assuré de trouver un emploi stable, bien rémunéré, avec des perspectives d'évolution et dans une discipline en pleine croissance.

Cybersécurité : bilan des menaces, nature des attaques et recommandations de l'ANSSI

2. Une diversité de métiers pour faire carrière dans la cybersécurité

Il existe une multitude de professions si vous souhaitez évoluer ou vous reconvertir dans la cybersécurité. Du consultant cyber au responsable sécurité des systèmes d'information (aussi désigné par le sigle RSSI), en passant par le poste de cryptologue, de pentester ou de hackeur éthique, les métiers de la cybersécurité sont variés et souvent méconnus, mais ils offrent des missions passionnantes afin de garantir la sécurité informatique des entreprises.

En 2021, l'ANSSI (l'Agence Nationale de la Sécurité des Systèmes d'Information) a lancé son Observatoire des métiers de la cybersécurité et a mené des travaux sur *Les Profils de la cybersécurité*, à partir d'une enquête interrogeant 2 381 professionnels. D'après l'analyse de 15 665 offres d'emploi (dont 46 % en IDF), les 5 postes les plus recherchés par les employeurs sont :

1. **Ingénieur cybersécurité :** il définit des règles pour assurer la sécurité des systèmes d'information (SI) et met en place un plan d'action en cas de cyberattaque, il analyse et traite les menaces d'intrusion.
2. **Consultant cybersécurité :** il aide les organisations (entreprises, startups, administrations…) à sécuriser leurs systèmes et réseaux informatiques en repérant les failles, en proposant des solutions adéquates pour répondre aux besoins de ses clients.
3. **Architecte en cybersécurité :** il conçoit et supervise des systèmes visant à limiter les cyberattaques.
4. **Analyste cybersécurité :** il détecte les incidents liés à la cybersécurité des entreprises en temps réel, les analyse, remonte à la source pour mieux les comprendre, et ainsi anticipe les futures attaques.
5. **Expert cybersécurité :** il gère la sécurité informatique des entreprises, en identifiant les failles, en configurant les systèmes d'information pour éviter les piratages, et il est amené à former les collaborateurs des différents départements aux bonnes pratiques cyber.

Et aussi : auditeur cybersécurité, RSSI, DPO (délégué à la protection des données), administrateur système informatique réseaux et sécurité, cryptologue… Pour 54 % des offres d'emploi analysées, les entreprises qui recrutent le plus des profils en cybersécurité sont issues des domaines suivants :

- l'informatique et les télécommunications,
- l'industrie et la technique,

- les services aux entreprises,
- la finance et l'assurance,
- la sécurité, les pompiers, la police et les armées.

En majorité, les profils les plus recherchés par les employeurs disposent d'un niveau bac+5 (46 %). Les contrats proposés sont le CDI (72 %), devant le CDD (9 %) et des missions en freelance (9 %).

Cybersécurité : l'ANSSI dévoile les 10 vulnérabilités les plus critiques de 2021

3. Des salaires attractifs dans les métiers de la cybersécurité

Selon l'étude de rémunérations nationale 2022 publiée par le cabinet de recrutement Hays, le poste d'ingénieur cybersécurité fait partie des métiers les plus en tension. L'enquête révèle également que la cybersécurité représente l'une des compétences parmi celles qui sont les plus recherchées sur le marché de l'emploi actuellement.

À titre d'exemple, voici les fourchettes de salaires annuels bruts pour la profession d'ingénieur cybersécurité, selon le niveau d'expérience :

- **De 0 à 3 ans d'expérience :** de 40 000 € à 45 000 €
- **De 3 à 5 ans d'expérience :** de 45 000 € à 50 000 €
- **De 5 à 8 ans d'expérience :** de 50 000 € à 65 000 €
- **Plus de 8 ans d'expérience :** de 65 000 € à 80 000 €

Du côté du poste de RSSI, la rémunération démarre entre 45 000 € et 50 000 € pour un profil junior, pour atteindre entre 85 000 € et 130 000 € pour un candidat senior (plus de 8 ans d'expérience). À noter qu'une différence de l'ordre de +10 % est à prendre en compte pour les salaires des postes à pourvoir en régions.

Si le marché du consulting vous intéresse, voici les taux journaliers moyens (hors taxes) en vigueur dans les métiers de la cybersécurité, pour les profils juniors et seniors, selon l'étude menée par Hays :

- **Ingénieur sécurité :** de 530 € (0-3 ans) à 805 € (plus de 8 ans d'expérience)
- **SecOps :** de 530 € (0-3 ans) à 805 € (plus de 8 ans d'expérience)
- **Architecte sécurité :** de 700 € (0-3 ans) à 935 € (plus de 8 ans d'expérience)
- **Ethical Hacker-Pentester :** de 680 € (0-3 ans) à 1 095 € (plus de 8 ans d'expérience)
- **RSSI :** de 795 € (0-3 ans) à 1 100 € (plus de 8 ans d'expérience)

Bon à savoir : pour obtenir la rémunération journalière moyenne de ces métiers en régions, le cabinet conseille de soustraire 10 % de ces taux.

4. Un statut qui correspondra à vos besoins et vos attentes

Parmi les avantages qu'offrent les métiers de la cybersécurité, et par extension le domaine de la tech, vous avez la possibilité d'exercer votre profession selon le statut de votre choix :

- en tant que salarié dans une structure publique ou privée, pour assurer la sécurité informatique de ses infrastructures,
- comme consultant dans une agence ou une ESN, où vous réaliserez des missions pour un ou plusieurs clients,
- ou bien en étant à votre propre compte, en freelance.

Selon l'enquête réalisée par l'ANSSI (mentionnée précédemment), les professionnels non-salariés représentent 14,5 % des répondants (sur un total de 2 381). Ainsi, pour le métier de consultant cybersécurité, 40 % des contrats correspondent à des missions de freelance. Que vous soyez à la recherche de stabilité ou que vous préfériez la liberté de vous organiser comme bon vous semble, les métiers de la cybersécurité satisferont toutes vos envies.

5. Les métiers de la cybersécurité sont ouverts à tous les profils

Quel que soit votre profil ou votre niveau, il est possible de s'orienter, de se reconvertir, ou encore d'ajouter cette brique technique à votre parcours professionnel, si vous désirez vous spécialiser dans la cybersécurité. L'essentiel est d'identifier le métier qui vous conviendra le mieux. Préférez-vous évoluer dans une posture de prévention, pour concevoir, sensibiliser et administrer la sécurité informatique d'une organisation, ou plutôt de protection, afin de réagir, mais aussi mener l'enquête, améliorer les infrastructures ou encore participer à la reconstruction d'un système d'information ?

Une fois que vous avez fait votre choix, vous devez acquérir les compétences nécessaires pour faire carrière dans cette voie. La cybersécurité étant un secteur pluridisciplinaire, elle exige de disposer de connaissances dans plusieurs domaines, comme par exemple (liste non exhaustive) :

- le droit, pour maîtriser les réglementations en vigueur (RGPD, ...),
- les mathématiques, si vous souhaitez travailler plus particulièrement vers la cryptologie,
- l'informatique, et notamment l'architecture de sécurité des SI,
- le hardware...

Les fondamentaux du langage de programmation Python ainsi que des systèmes d'exploitation, notamment ceux basés sur le noyau Linux, vous ouvriront les portes des métiers liés à l'open source et la cybersécurité, par exemple. Avec des notions en intelligence artificielle ou en machine learning, vous pourrez aussi évoluer dans ce secteur, avec l'essor des nouvelles technologies et du traitement exponentiel des données à protéger.

Du côté des soft skills, l'esprit d'analyse, la gestion du stress pour faire face à n'importe quelle situation, et une bonne communication, afin de sensibiliser les collaborateurs de votre entreprise ou de vos clients aux bons usages à adopter en matière de cybersécurité, sont indispensables. Le plus : des qualités de management, en vue de gérer une équipe, de la réactivité et un bon relationnel vous permettront de vous démarquer face à d'autres candidats.

De la déstabilisation à l'espionnage, découvrez les différentes menaces informatiques identifiées par l'ANSSI. © blackboard / stock.adobe.com

Cybersécurité : panorama des menaces informatiques

Tour d'horizon des menaces cyber en 2021, présenté par l'ANSSI.

À travers son panorama de la menace informatique, l'Agence Nationale de la Sécurité des Systèmes d'information (ANSSI) dévoile les grandes tendances qui ont marqué l'année 2021 en termes de menaces cyber. L'étude met en lumière l'amélioration constante des capacités des acteurs malveillants. Le chiffre marquant : une augmentation de 37 % des intrusions avérées dans les systèmes d'information entre 2020 et 2021.

Des cybercriminels aux méthodes toujours plus développées

D'après le dictionnaire Le Robert, la cybercriminalité constitue « *l'ensemble des activités illégales effectuées par l'intermédiaire d'Internet* ». Dans un monde de plus en plus digitalisé où les menaces de cyberattaques se multiplient, les cybercriminels qui se cachent derrière sont désormais très méthodiques. L'étude indique que ces derniers « *se spécialisent ainsi en fournisseurs de services proposant des codes malveillants, des infrastructures d'anonymisation, des accès à des réseaux compromis (Access Broker), des réseaux de machines zombies botnet, des services d'envoi de pourriels ou encore de blanchiment d'argent* ». Ils utilisent plusieurs types de cyberattaques, selon les infrastructures et les objectifs poursuivis. L'ANSSI constate que « *de plus en plus d'actions de déstabilisation débutent par des compromissions*

informatiques », qui permettent de récupérer des documents pouvant être divulgués en l'état, voire même parfois modifiés pour impacter leurs victimes.

Pour être de moins en moins identifiables, les attaquants utilisent de manière plus courante des outils déjà présents sur le réseau de la cible (comme PowerShell, par exemple), pour arriver à leurs fins. Ils sont alors plus difficiles à détecter, puisqu'ils n'utilisent désormais plus (ou peu) d'outils caractéristiques des activités malveillantes.

L'espionnage en tête des finalités poursuivies

En 2021, l'ANSSI a identifié 3 types de menaces informatiques majeures, qui ont fortement impacté les entreprises et les organisations. Le rapport précise que « *si les attaques à finalité lucrative ont occupé le devant de la scène au cours des derniers mois, il est important de rappeler que l'espionnage reste la première finalité poursuivie avec les tentatives de déstabilisation et les actions de sabotage informatique* ». Les différentes menaces identifiées par l'ANSSI en 2021 sont les suivantes :

- **L'espionnage et le sabotage informatique :** il s'agit du principal objectif affiché par les attaquants réputés étatiques. L'ANSSI qualifie ces menaces de « *particulièrement préoccupantes* », car elles sont à l'origine de la majorité des opérations de cyberdéfense menées par l'agence.
- **Le ciblage d'infrastructure critique :** moins répandu car plus risqué pour les cybercriminels, ce type de menace intervient généralement dans des contextes de fortes tensions géopolitiques.
- **Les actions de déstabilisation :** l'objectif de ce type d'attaque est de déstabiliser une organisation, une personne ou un État, à partir de données confidentielles récupérées via des compromissions informatiques. La divulgation des données est de plus en plus fréquente. En 2021, 39 actions de ce type ont eu lieu, selon l'ANSSI.

De nombreuses failles exploitées

Pour arriver à leurs fins, et réussir à dérober des données confidentielles, les acteurs malveillants n'hésitent pas à exploiter les moindres vulnérabilités qu'ils détectent. À l'inverse, trop d'organisations restent imprudentes, et tardent à appliquer les correctifs de sécurité fournis par les éditeurs de logiciels. L'ANSSI explique que « *dès la mise à disposition d'une méthode d'exploitation, en l'espace de quelques jours voire de quelques heures, l'exploitation de vulnérabilités peut être industrialisée notamment grâce à l'identification d'instances vulnérables par le biais de scans massifs et servir des finalités diverses, depuis l'espionnage informatique jusqu'à des attaques à finalité lucrative* ».

L'agence pointe également du doigt l'utilisation de clouds non sécurisés pour y stocker des données hautement confidentielles. En effet, ces dernières années, le recours aux services de cloud s'est particulièrement accéléré, et les cybercriminels l'ont bien compris. L'étude souligne qu'entre octobre 2020 et février 2021, plus de 2 100 instances cloud non sécurisées et facilement accessibles ont notamment été détectées.

Pour conclure son rapport, l'ANSSI ajoute que de nouvelles opportunités se présentent régulièrement aux attaquants. Les intentions associées ne devraient pas changer, et resteront hétérogènes, allant de la déstabilisation à l'influence, en passant par le gain financier et l'espionnage. L'agence « *appelle à une vigilance particulière de l'ensemble des parties prenantes* ».

Retrouvez les salaires moyens annuels bruts et journaliers pour les métiers de la cybersécurité. © RomanR - stock.adobe.com

Les salaires des métiers de la cybersécurité en 2022

Combien gagnent les professionnels de la sécurité digitale en 2022 ?

Les salaires annuels bruts des métiers de la cybersécurité

Les données partagées ci-dessous sont issues de l'étude des rémunérations 2022 de PageGroup. Elle s'appuie sur les résultats d'une enquête annuelle réalisée auprès des candidats et des clients du cabinet de recrutement. La rémunération indiquée correspond à un salaire brut annuel en euros, selon le niveau d'expérience. Il n'y pas de distinction de salaire entre Paris et les régions.

Pentester

- Junior (de 0 à 2 ans) : entre 35 000 € et 40 000 €
- Confirmé (de 2 à 5 ans) : entre 40 000 € et 50 000 €
- Senior (de 5 à 15 ans) : entre 50 000 € et plus de 70 000 €

Auditeur sécurité IT

- Junior (de 0 à 2 ans) : entre 38 000 € et 45 000 €
- Confirmé (de 2 à 5 ans) : entre 45 000 € et 60 000 €
- Senior (de 5 à 15 ans) : entre 60 000 € et 85 000 €

Analyste sécurité / SOC

- Junior (de 0 à 2 ans) : entre 40 000 € et 55 000 €
- Confirmé (de 2 à 5 ans) : entre 55 000 € et 70 000 €
- Senior (de 5 à 15 ans) : plus de 70 000 €

Ingénieur cybersécurité

- Junior (de 0 à 2 ans) : entre 40 000 € et 50 000 €
- Confirmé (de 2 à 5 ans) : entre 45 000 € et 70 000 €
- Senior (de 5 à 15 ans) : entre 70 000 € et plus de 90 000 €

Architecte cybersécurité

- Junior (de 0 à 2 ans) : entre 65 000 € et 75 000 €
- Confirmé (de 2 à 5 ans) : entre 75 000 € et 85 000 €
- Senior (de 5 à 15 ans) : entre 85 000 € et plus de 100 000 €

Responsable de la sécurité et des systèmes d'information (RSSI)

- Junior (de 0 à 2 ans) : entre 65 000 € et 80 000 €
- Confirmé (de 2 à 5 ans) : entre 80 000 € et 95 000 €
- Senior (de 5 à 15 ans) : entre 95 000 € et plus de 120 000 €

Responsable de la gouvernance sécurité

- Junior (de 0 à 2 ans) : entre 70 000 € et 90 000 €
- Confirmé (de 2 à 5 ans) : entre 90 000 € et 110 000 €
- Senior (de 5 à 15 ans) : entre 110 000 € et 150 000 €

À noter qu'une autre étude menée cette fois par Hays dévoile d'autres chiffres plus détaillés et liés à la rémunération pour le métier d'ingénieur cybersécurité. Il s'agit de l'une des professions les plus en tension dans ce secteur, selon le cabinet de recrutement. Les chiffres indiqués correspondent au salaire proposé en brut annuel en euros et en Île-de-France. La différence est de l'ordre de 10 % avec celui obtenu en régions.

- Junior (de 0 à 3 ans) : entre 40 000 € et 45 000 €
- Confirmé (de 3 à 5 ans) : entre 45 000 € et 50 000 €
- Expérimenté (de 5 à 8 ans) : entre 50 000 € et 65 000 €
- Senior (plus de 8 ans d'expérience) : entre 65 000 € et 80 000 €

Les taux journaliers moyens pour les métiers de la cybersécurité

Toujours d'après l'étude publiée par Hays, voici les taux journaliers moyens, exprimés en euros et hors taxes, pour les professionnels de la cybersécurité exerçant leur métier en tant que consultant, dans une ESN, en agence ou via des missions de freelance par exemple. Il faut ici soustraire 10 % de la rémunération indiquée pour obtenir le salaire en régions.

Ingénieur cybersécurité

- Junior (de 0 à 3 ans) : 530 €
- Confirmé (de 3 à 5 ans) : 595 €
- Expérimenté (de 5 à 8 ans) : 675 €
- Senior (plus de 8 ans d'expérience) : 805 €

SecOps

- Junior (de 0 à 3 ans) : 530 €
- Confirmé (de 3 à 5 ans) : 595 €
- Expérimenté (de 5 à 8 ans) : 675 €
- Senior (plus de 8 ans d'expérience) : 805 €

Architecte cybersécurité

- Junior (de 0 à 3 ans) : 700 €
- Confirmé (de 3 à 5 ans) : 780 €
- Expérimenté (de 5 à 8 ans) : 855 €
- Senior (plus de 8 ans d'expérience) : 935 €

Auditeur en sécurité informatique

- Junior (de 0 à 3 ans) : 625 €
- Confirmé (de 3 à 5 ans) : 705 €
- Expérimenté (de 5 à 8 ans) : 785 €
- Senior (plus de 8 ans d'expérience) : 865 €

Ethical Hacker / Pentester

- Junior (de 0 à 3 ans) : 680 €
- Confirmé (de 3 à 5 ans) : 805 €
- Expérimenté (de 5 à 8 ans) : 915 €
- Senior (plus de 8 ans d'expérience) : 1 095 €

Responsable de la sécurité et des systèmes d'information (RSSI)

- Junior (de 0 à 3 ans) : 795 €
- Confirmé (de 3 à 5 ans) : 875 €
- Expérimenté (de 5 à 8 ans) : 940 €
- Senior (plus de 8 ans d'expérience) : 1 100 €

Anticipez les éventuelles attaques informatiques, et protégez vos données. © Michael Traitov - stock.adobe.com

8 conseils pour assurer sa cybersécurité

Tour d'horizon des bonnes pratiques à appliquer pour assurer sa sécurité en ligne.

D'après une étude menée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) sur la menace informatique en 2021, le nombre d'intrusions avérées a augmenté de 37 % sur les 12 précédents mois. Pour se prémunir contre d'éventuelles cyberattaques, et protéger ses données en ligne, découvrez 8 bonnes pratiques à mettre en place facilement.

1. Utiliser un antivirus

Ce conseil peut sembler évident, et la majorité des appareils sont protégés par un antivirus dès l'achat, mais il arrive parfois que les licences expirent, ou que l'antivirus soit inactif. Pensez à bien vérifier que votre poste est équipé d'un antivirus, et installez-en un si besoin. Attention, si vous souhaitez en changer, pensez bien à désinstaller le précédent. En effet, il est fortement déconseillé d'utiliser 2 antivirus sur le même appareil, cela risque de générer des conflits entre les ressources du système, et donc de ralentir l'ordinateur.

2. Faire régulièrement les mises à jour de sécurité

Pour rendre les logiciels plus sûrs, les développeurs proposent régulièrement des correctifs de sécurité. Il est important de les installer rapidement, car ils corrigent

parfois des failles de sécurité majeures, exploitables par les cybercriminels. Assurez-vous dans la mesure du possible de toujours disposer de la version la plus récente de vos logiciels (antivirus, système d'exploitation…).

3. Activer l'authentification à double facteur

La double authentification est une méthode sécurisée, qui permet de renforcer la sécurité de vos comptes en ligne. Elle permet de réduire le risque de piratage, puisqu'en plus de l'identifiant et du mot de passe, un code supplémentaire est exigé. Vous pouvez généralement recevoir ce code par email, par SMS ou par téléphone. De plus en plus de plateformes proposent d'activer l'authentification à double facteur, afin d'ajouter une couche de sécurité.

4. Éviter les téléchargements suspects

De nombreux virus circulent sur Internet, et si vous n'êtes pas vigilants, vous pourriez en télécharger un par mégarde. En effet, ne téléchargez que les fichiers dont vous connaissez la source. Si votre ordinateur ou votre antivirus vous indique que votre téléchargement n'est pas recommandé, ne prenez pas de risque, et annulez l'opération. Pour toute installation qui concerne une application ou un logiciel populaire, il est conseillé de passer par le site officiel si possible. En cas de doute, évitez les téléchargements suspects.

5. Faire des sauvegardes régulières de vos données

Il est recommandé d'effectuer des sauvegardes régulières de vos données en ligne, pour être en mesure de tout récupérer en cas de perte ou de vol. Attention, il est important de bien protéger vos sauvegardes, au même titre que les données initiales. Vous pouvez par exemple opter pour une sauvegarde externe, sur un disque dur ou sur une clé USB.

À lire également

> 5 bonnes pratiques à adopter pour ne plus perdre ses données

6. Apprendre à repérer le phishing

Le phishing est l'une des méthodes de piratage les plus répandues. Elle permet aux attaquants de tromper les internautes, et ainsi de récupérer diverses informations confidentielles, comme des mots de passe ou des coordonnées bancaires. Pour éviter de se faire avoir, pensez à bien vérifier les URL sur lesquelles vous cliquez (n'entrez pas vos informations sur les pages web dont l'adresse est en HTTP et non en HTTPS). Faites aussi attention aux mails frauduleux ou aux messages privés suspects sur les réseaux sociaux. Vous ne devez surtout pas cliquer sur les liens ou les pièces jointes contenues dans ces messages, car vous risqueriez de vous faire pirater.

7. Utiliser un gestionnaire de mots de passe

Les gestionnaires de mots de passe sont des logiciels qui permettent de conserver vos identifiants et d'autres informations confidentielles en toute sécurité. Ils vous permettent à la fois de faciliter vos connexions, mais assurent également votre cybersécurité, puisque vous seul y avez accès. Il vous faudra ainsi définir et retenir un mot de passe maître, qui permet de garder en sécurité le reste de vos données. Ces logiciels sont fortement recommandés par des organismes, comme la CNIL par exemple.

8. Utiliser un VPN

Pour naviguer sur Internet sans risque, et de manière anonyme, vous pouvez utiliser un logiciel VPN. Ce réseau privé virtuel permet de se protéger des réseaux publics, en garantissant aux appareils la sécurité d'une connexion à un réseau privé. Lorsque vous utilisez un VPN, votre connexion est cryptée, votre IP est masquée, les données et les transferts sont protégés. Pensez à utiliser ce type d'outil lorsque vous vous connectez à un réseau public.

Le secteur de la cybersécurité

Des solutions open source peuvent être intégrées par les entreprises dans le cadre d'une stratégie de cybersécurité. © Gorodenkoff - stock.adobe.com

Cybersécurité : les avantages de l'open source pour protéger les entreprises

La protection des données et des systèmes d'information est essentielle pour faire face à l'explosion des cybermenaces. Parmi les solutions qui existent, l'open source présente de nombreux atouts pour aider les entreprises à renforcer leur sécurité informatique.

L'open source, une solution avantageuse pour la cybersécurité des entreprises

En facilitant le partage des connaissances et des outils, l'open source offre la possibilité aux organisations de développer des compétences nécessaires pour augmenter leur maîtrise des technologies liées à la cybersécurité, tout en bénéficiant des contributions de la communauté et des acteurs du numérique. « *L'open source est une bonne approche à la cybersécurité car les systèmes d'exploitation de cyberattaques les plus utilisés sont basés sur le noyau Linux*, explique Laurent Biagiotti, responsable du cycle mastère à l'école Sup de Vinci. *Beaucoup de personnes gardent encore en tête la faille Heartbleed d'OpenSSL ou celle de log4j, qui est considérée comme l'une des attaques les plus graves. Elles ont été résolues grâce la communauté open source.* »

En plus de proposer un apprentissage rapide, le logiciel

libre offre de nombreux avantages. À travers les projets réalisés dans le cadre de la spécialisation en cybersécurité, les étudiants de Sup de Vinci doivent respecter 4 règles fondamentales de l'open source, qu'ils pourront ensuite appliquer dans le cadre de l'entreprise à l'issue de leur formation :

- La liberté d'exécution des programmes,
- La liberté de modification via un fork (projet parallèle),
- La liberté de redistribution, c'est-à-dire l'amélioration d'un projet dans un but commercial, car le logiciel open source n'est pas gratuit,
- La liberté d'amélioration du code de n'importe quel projet.

Grâce à la transparence du code source, le logiciel libre allie à la fois liberté et éthique pour permettre aux entreprises de garantir la protection de leurs infrastructures. Autre atout : la possibilité que des vulnérabilités soient plus rapidement décelées et qu'un correctif soit apporté au plus vite afin d'y remédier. Si l'open source ne constitue pas en soi une finalité pour les multinationales, Laurent Biagiotti rappelle que ces dernières ont également besoin de services plus complexes, qui offrent notamment une meilleure traçabilité des logs et des services.

Les bonnes pratiques de l'open source pour une stratégie de cybersécurité efficace

Pour répondre aux besoins des entreprises, qui doivent renforcer la sécurité de leurs données ainsi que celle de leurs systèmes d'information face aux menaces de plus en plus croissantes, des solutions open source peuvent être intégrées dans le cadre d'une stratégie de cybersécurité. « *Je recommande de pentester* (procéder à des tests d'intrusion, ndlr) *toutes vos infrastructures de manière journalière car il y a de nombreuses attaques zero-day. Ce sont des failles de sécurité informatique dont le propriétaire n'a pas encore connaissance. L'expert en intrusion pourra s'appuyer sur des outils de cybersécurité, dont un certain nombre de solutions proviennent de labs open source de grands groupes* », ajoute le responsable pédagogique.

Parmi les bonnes pratiques à mettre en place, il est recommandé de « *ne plus chercher à repousser les assauts des pirates mais plutôt de les attirer vers un espace dédié afin de les berner et les démasquer* ». Cette méthode est désignée sous le nom de « pot de miel » ou « honeypot ». Le principe consiste, pour les cyberdéfenseurs, à créer de faux services de production et d'analyser les schémas d'intrusion suivis par les cyberattaquants. « *Cela permet de mieux connaître son ennemi et, ainsi, d'anticiper de futures attaques. Cet environnement est volontairement perméable et est déployé à côté d'un système réel en production, qui sera minutieusement supervisé.* »

À noter que la méthode de l'honeypot est enseignée grâce à l'utilisation de la plateforme open source T-Pot, développée par la Deutsch Telecom, ce qui permet aux étudiants à la fois de se familiariser avec cette technique et d'en maîtriser l'outil. L'objectif : être capable de la mettre en pratique dans le cadre d'un projet de cybersécurité à l'école, puis en entreprise.

Les compétences requises pour assurer la sécurité informatique des entreprises

Vous souhaitez vous orienter ou vous reconvertir dans ce secteur en pleine expansion et qui recrute ? L'école Sup de Vinci propose un mastère spécialisation cybersécurité en alternance, en vue de devenir un expert dans ce domaine,

avec également des compétences en management et en gestion de projet pour rester agile tout au long de sa carrière. Le programme de la formation est riche et complet avec l'apprentissage du langage de programmation Python, et la maîtrise des systèmes d'exploitation basés sur le noyau Linux, qui représentent 90 % des projets open source. Les soft skills tiennent également une place importante au sein de ce cursus avec, en particulier, le développement du quotient émotionnel. « *Cet aspect est vraiment très important en cybersécurité car la faille humaine est inhérente à toutes les attaques informatiques* », souligne Laurent Biagiotti.

La formation permet de devenir rapidement opérationnel en travaillant à partir de situations réelles, avec des cas existants et en suivant des labs, en partenariat avec des entreprises du marché. Les apprenants ont aussi des défis à réaliser sur des simulateurs d'attaques connues et référencées. « *Ce cocktail permet une montée en compétences sur les domaines liés à la cybersécurité, avec des approches différentes du métier (attaque, défense), du management, de la gestion de crises, et bien d'autres sujets encore… On est autant formé sur le plan technique que sur les soft skills, dans une dynamique portée par des challenges, des notations et des mises à l'épreuve sur plusieurs plateformes* », raconte Khaireddine Cherif, étudiant en mastère 2 Expert des systèmes d'information spécialité cybersécurité. Le parcours donne aussi l'opportunité aux étudiants de passer un minimum de 5 certifications, qui sont incluses et financées par l'école : CEH, CHFI, Palo Alto 114, Stormshield et AWS. Les résultats sont là : en 2020, le mastère spécialisé en cybersécurité comptait 96,5 % de taux d'insertion professionnelle au bout de 6 mois.

Inscrivez-vous pour devenir un expert en cybersécurité avec Sup de Vinci

Présentation de Sup de Vinci

Sup de Vinci est une école d'informatique, qui propose des formations de niveau bac à bac+5, en initial et en alternance, à destination des futurs cadres IT. Les parcours permettent d'acquérir des compétences techniques, managériales et transverses, afin de devenir rapidement opérationnel sur le marché de l'emploi. En mastère, vous avez le choix entre 5 spécialisations : big data & IA, devOps & cloud, développement, product owner et cybersécurité. Les cours sont actuellement dispensés sur 2 campus, à Paris La Défense et à Rennes, et sur un 3e à la rentrée 2022, à Bordeaux. Le plus : les étudiants bénéficient d'un suivi et d'un accompagnement personnalisés tout au long de leur cursus.

La cybersécurité est essentielle pour tous les professionnels impliqués dans la supply chain. © weerapat1003 - stock.adobe.com

La cybersécurité, un enjeu majeur pour la supply chain

Entre transformation digitale et recrudescence des cyberattaques, la supply chain est confrontée à la nécessité de renforcer la sécurité de ses processus.

La digitalisation de la supply chain entraîne de nouvelles cybermenaces et de multiples vulnérabilités pouvant affecter chaque maillon de la chaîne logistique. C'est pourquoi la cybersécurité devient un impératif pour tous les professionnels impliqués dans la supply chain, et pas uniquement pour les Responsables de la Sécurité des Systèmes d'Information (RSSI). Patrick Erard, délégué général adjoint du Pôle d'Excellence Cyber et responsable du mastère 2 cybersécurité de la supply chain du Campus E.S.P.R.I.T. Industries, nous éclaire sur les problématiques de la supply chain, les actions clés et les compétences nécessaires pour assurer sa sécurité.

Le rôle de la cybersécurité dans la supply chain

Les principales problématiques de la supply chain

La supply chain englobe toutes les parties tierces avec lesquelles une entreprise collabore, des fournisseurs aux prestataires, en passant par les partenaires et sous-traitants. Ainsi, la digitalisation accrue de la chaîne d'approvisionnement crée un environnement interconnecté, et donc à risque sur le plan de la sécurité. « *Si la supply chain est particulièrement exposée, c'est parce que de nombreux composants communiquent les uns avec les autres. Si un de*

ces maillons ne fonctionne plus, c'est l'ensemble de la chaîne qui est impactée », explique Patrick Erard.

Autre point qui vulnérabilise la supply chain : le manque d'interopérabilité. En effet, les matériels et logiciels utilisés par les différents acteurs impliqués possèdent souvent leurs propres protocoles, donc de nouvelles failles de sécurité. L'enjeu pour les entreprises est d'accéder à une vue d'ensemble du niveau de sécurité de leur écosystème.

La supply chain au cœur des risques cyber

Les risques cyber qui pèsent sur la supply chain sont multiples et concernent l'ensemble du cycle de vie d'un produit, de sa conception à sa maintenance. Les cyberattaques peuvent ainsi entraîner l'inaccessibilité des systèmes et des données, la corruption des données et des produits ou encore le vol de données. Les principales menaces auxquelles est confrontée la supply chain concernent :

- la sécurité du code ou de composants des matériels et logiciels,
- l'authentification et la gestion d'identité,
- le bon paramétrage des outils de sécurité,
- les chartes et politiques de sécurité organisationnelle,
- les normes juridiques qui diffèrent d'un pays à l'autre.

Les actions clés et les compétences essentielles pour assurer la sécurité de la supply chain

La nécessité de sensibiliser et d'informer

Il est indispensable d'informer les acteurs impliqués dans la supply chain, en les sensibilisant aux menaces, mais aussi à l'importance que le digital a pris dans leurs métiers. Selon le responsable pédagogique, une formation des managers et des dirigeants est primordiale, afin d'influer sur la Direction des Systèmes d'Information (DSI). L'objectif : faciliter l'intégration des mesures de sécurité, adapter les solutions aux besoins métiers et incorporer la cybersécurité dès la conception d'un produit.

Cette sensibilisation doit s'accompagner d'une formation aux outils numériques sécurisés, afin d'appréhender la manière de les paramétrer et de les implémenter. « *Il est indispensable d'apprendre la gestion de crise, réaliser des plans de continuité d'activité pour se prémunir des attaques, ou de reprise d'activité si l'attaque a réussi à arrêter le système* », estime le délégué général adjoint du Pôle d'Excellence Cyber.

Des compétences techniques et humaines

Pour allier supply chain et cybersécurité, il est primordial d'acquérir une bonne connaissance des matériels, des logiciels, de l'architecture, de l'implémentation. Appréhender les notions essentielles permettant d'élaborer et mettre en œuvre une politique de sécurité informatique est également indispensable. Les aspirants défenseurs devront accepter de se former tout au long de leur vie professionnelle.
« *L'informatique est un milieu où il faut toujours se remettre en question. Si on ne se tient pas au courant des évolutions du secteur, on n'est rapidement plus crédible* », souligne Patrick Erard.

Parmi les soft skills, le savoir-être est une qualité attendue dans les métiers de la cybersécurité. « *Nous avons besoin de gens avec la tête sur les épaules, investis et prêts à faire bénéficier leur structure de compétences techniques pour assurer la sécurité de son système d'information, car il est beaucoup plus difficile d'être un défenseur que de devenir hacker* », affirme le responsable pédagogique.

Une formation lancée pour répondre aux besoins de la supply chain en cybersécurité

Un parcours alliant fondamentaux de la supply chain et de la cybersécurité

Pour répondre aux besoins croissants en termes de sécurisation et d'anticipation des menaces informatiques qui pèsent sur l'ensemble des acteurs impliqués dans les chaînes d'approvisionnement, Campus E.S.P.R.I.T. Industries lance un parcours spécialisé en cybersécurité de la supply chain. Cette formation de niveau 7 (bac+5) vise à former des spécialistes capables d'intégrer au sein de leurs structures les enjeux de sécurité liés à la transformation digitale des entreprises.

Le parcours est intégré au sein du mastère Manager Logistique Achats Industriels (M.L.A.I.), et présente un programme qui s'articule autour des fondamentaux de la supply chain, complétés par des notions essentielles en cybersécurité. Le cursus vise à acquérir les connaissances suivantes :

- Fondamentaux des achats et les approches cyber de leurs processus,
- Gestion de la supply chain et son pilotage cyber,
- Organisation des transports et mobilités, et leur cybersécurisation,
- Digitalisation et innovation de la supply chain,
- Cybersécurisation de la dimension environnementale de la performance.

Les compétences acquises en cours peuvent ensuite être appliquées en entreprise. © Campus E.S.P.R.I.T. Industries

Former des défenseurs opérationnels

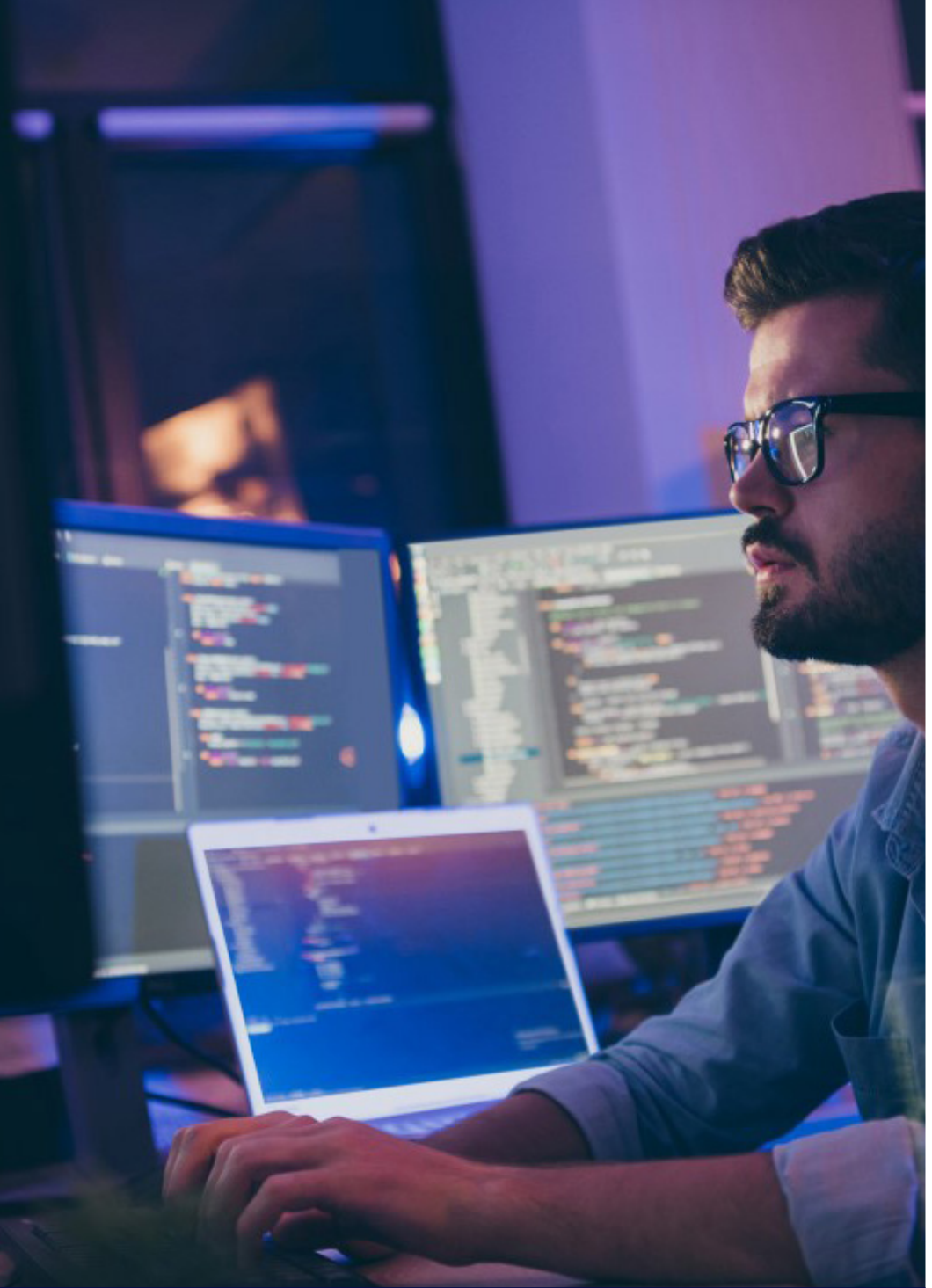
Campus E.S.P.R.I.T. Industries repose sur l'expertise d'industriels, issus de grands groupes, de PME et de PMI. Certains de ces experts interviennent à l'ESLI, leur enseignement reflétant les réalités et les problématiques de la supply chain. De plus, la formation propose un rythme en alternance de 2 semaines en présentiel à l'ESLI, situé à Redon (35), et 4 à 6 semaines en entreprise. « *L'atout de cette formation est que les apprenants sont en immersion au sein des entreprises. Ils peuvent appliquer ce qu'ils apprennent en cours au sein des systèmes d'information de leurs structures, mais en plus ils maîtrisent ce dont l'entreprise a besoin concrètement* », souligne Patrick Erard. À l'issue du cursus, les apprenants sont aptes à sécuriser la supply chain et à mettre en place des stratégies pour assurer la pérennité de SI complexes.

Le parcours cybersécurité de la supply chain proposé par Campus E.S.P.R.I.T. Industries s'adresse aux étudiants, mais aussi aux personnes en reconversion. Une session de recrutement est en cours jusqu'au 24 juin pour une rentrée prévue en octobre 2022.

Découvrir le parcours cybersécurité de la supply chain de Campus E.S.P.R.I.T. Industries

Présentation de Campus E.S.P.R.I.T. Industries

Le Campus E.S.P.R.I.T. Industries – Enseignement Supérieur Professionnalisation Recherche Innovation Technologies – basé à Redon (35) et à Paris, propose des formations en alternance de niveau bac+2 à bac+5. Les filières du Campus E.S.P.R.I.T. Industries sont axées vers l'industrie, notamment dans les domaines des achats, de la logistique, de la supply chain, et dans les métiers technologiques en électronique, mécatronique, robotique, mais aussi en maîtrise de l'énergie, électricité et développement durable. Les formations sont professionnalisantes et certifiantes, visant des métiers à forte employabilité.



Avec l'évolution des usages, le Groupe ADSN est passé d'une sécurité réglementaire et périmétrique à une sécurité dynamique et élargie. © deagreez - stock.adobe.com

Cybersécurité : comment garantir la protection des données personnelles les plus sensibles dans les professions réglementées

Nous avons interrogé Christian Revelli, vice-président du directoire du Groupe ADSN, et François Drouillot, directeur de la sécurité opérationnelle de l'ADSN, qui nous présentent les enjeux de la cybersécurité dans le domaine du notariat.

Quels sont les types de données que vous traitez et pourquoi sont-elles particulièrement sensibles ?

Christian Revelli : Nous traitons les données des notaires, dont le métier est de gérer les données personnelles et privées des Français, qui doivent de plus être conservées pendant 75 ans. À ce titre, nous traitons des données particulièrement sensibles.

François Drouillot : Nous gérons une très grande partie du patrimoine informationnel du notariat français. En ce sens, nous administrons un type particulier de données sensibles, ce qui fait de l'ADSN un acteur unique.

Quels sont les secteurs d'activité que vous accompagnez au quotidien ?

François Drouillot : Au quotidien, nous accompagnons la profession de notaires, qui sont nos principaux clients. L'ADSN imagine, conçoit, sécurise et maintient en condition opérationnelle leurs services numériques.

Christian Revelli : Notre client principal est le notariat, mais notre stratégie consiste à développer des services et outils pour d'autres professions réglementées. Il s'agit de venir consolider les offres, qui sont aujourd'hui destinées au notariat. Par exemple, notre offre de service de Délégué à la Protection des Données peut être proposée à d'autres professionnels, car sur le plan du process et de l'offre, elle n'est pas si différente d'une entreprise à l'autre.

En quoi la digitalisation des professions réglementées a-t-elle nécessité de renforcer la sécurité des données sensibles ?

Christian Revelli : Le taux de digitalisation représente plus de 90 % sur les actes. À partir du moment où nous numérisons et où nous concentrons les informations de toute la profession, et donc de tous les Français, sur une infrastructure unique, le risque associé à une perte ou à une intrusion est extrêmement important. Il est donc nécessaire d'adapter la sécurité et la protection vis-à-vis de ces menaces.

François Drouillot : Nous avons connu un changement de paradigme face à l'évolution des usages, où nous sommes passés d'une sécurité réglementaire et périmétrique à une sécurité dynamique et élargie, du fait justement de ces besoins de centralisation, qui ont ensuite découlé sur des besoins d'interconnexion. Pour imager : nous sommes passés d'un château fort avec de grosses murailles à une place forte avec de nombreuses portes ouvertes laissant passer des flux entre intérieur et extérieur. Il a donc fallu adapter la cybersécurité du Groupe en mettant en place de nouveaux outils. C'est ainsi qu'une nouvelle Direction de la Sécurité Opérationnelle (DSO) a été créée au sein de l'ADSN au printemps 2021.

Christian Revelli : D'ailleurs, 7 % des effectifs du Groupe ADSN sont dédiés à la cybersécurité.

À quelles menaces cyber devez-vous faire face ?

François Drouillot : Les menaces ciblent nos systèmes d'information : rançongiciel, vol de données, détournement d'actif financier, atteinte à la résilience des services du notariat… Ces tentatives pourraient porter atteinte à nos systèmes d'information et, par extension, aux services de l'État et du notariat, donc à la vie privée de millions de Français.

Christian Revelli : Nous devons également faire face à un type de menace sévère, à savoir l'usurpation d'identité, notamment lorsqu'il s'agit de dévier des flux financiers opérés entre les notaires et leurs clients vers des organisations criminelles.

Quelles sont les réponses technologiques mises en place par le Groupe ADSN pour répondre à ces menaces ?

François Drouillot : Au sein de l'ADSN, un pilotage à 2 niveaux a été mis en place pour la sécurité informatique :

- au niveau stratégique : le Responsable de la Sécurité des Systèmes d'Information (RSSI) est rattaché directement au directoire pour piloter les risques et le contrôle interne,

- au sein de l'ADSN : la DSO a été créée au plus près des actions liées à la sécurité des données.

Aujourd'hui, la DSO est basée sur 2 services : la sécurité opérationnelle et technique, avec les services SOC (surveillance et détection) et CSIRT (cybermenace, vulnérabilités, investigations et audits), ainsi que la gestion des services de sécurité (pilotage et contrôles opérationnels). Il est important de noter qu'au sein de l'ADSN, nous créons, développons et sécurisons des applications, au profit du notariat, afin de répondre aux besoins spécifiques de la profession.

Quelles sont les compétences humaines et techniques requises pour garantir la sécurité des données et des échanges au sein de ces professions ?

François Drouillot : La DSO du Groupe ADSN possède de nombreux métiers identifiés dans le panorama des métiers de la cybersécurité de l'ANSSI. Grâce à nos 25 experts, nous adressons un large panel de compétences, comme des investigations numériques poussées au DevSecOps (sécurité dans les projets). Des partenariats avec des centres de services et des grands acteurs du marché nous permettent d'être intégrés au sein de l'écosystème de la cybersécurité, et de pouvoir ainsi répondre aux enjeux de la connaissance et du maintien de la compétence.

Christian Revelli : Nous faisons aussi partie des acteurs qui ont créé le « *club des prestataires des services de confiance* ». Notre objectif : assurer la sécurité, avec la bienveillance de l'ANSSI, qui a cherché à travers ce groupement à obtenir un interlocuteur unique pour faire évoluer les mesures, les décrets et les règlements en matière de cybersécurité. Le Groupe ADSN et le notariat dans sa globalité, à travers les représentants et les compétences dont ils font preuve, ont été parmi les fondateurs de ce club. Nous restons les interlocuteurs privilégiés, avec l'ANSSI, pour faire évoluer les règlements, qui régissent les activités autour de la cybersécurité en France.

François Drouillot : Seulement 11 organismes en France sont certifiés eIDAS, et l'ADSN en fait partie.

Vous recrutez des profils experts en cybersécurité. Sur quels postes précisément ?

François Drouillot et Christian Revelli : Nous recherchons des experts en cybersécurité, sur des profils de type CSIRT (*Computer Security Incident Response Team*), pour venir agrandir nos équipes au sein de la DSO. Nous proposons de nombreux avantages en termes d'équilibre entre vie professionnelle et personnelle, à l'image du soleil provençal qu'on ne retrouve nulle part ailleurs !

Consulter toutes les offres d'emploi du Groupe ADSN

Présentation du Groupe ADSN

GROUPEADSN

Le Groupe ADSN est un acteur majeur de la sécurité des données sensibles des Français. Il assure le stockage et garantit la protection des données, ainsi que les échanges des professions réglementées entre elles, avec leurs clients et avec les autorités publiques. Il propose un éventail de solutions innovantes pour faciliter le développement et la croissance de ces activités (fichier central des dernières volontés, signature électronique, archivage numérique...).