Cybersécurité

Commission Numérique

09/12/2022

01

Le risque numérique

La cybercriminalité en quelques exemples récents

Après **les centres hospitaliers** de Corbeil-Essonnes, Dax, Vitry-le-François ou encore Saint-Gaudens, c'est celui de Versailles qui est, depuis le **samedi 3 décembre 2022** la victime d'une cyberattaque par rançongiciels.

Le **conseil départemental** de la Seine et Marne, le conseil départemental des Alpes Maritimes, et le conseil régional de Guadeloupe ont chacun également été au cours du mois de **novembre 2022** la cible d'une cyberattaque.

En **janvier dernier**, **un petit cabinet d'avocats** français est victime d'une cyberattaque par rançongiciel. Au total, 9.859 documents dérobés lors de cette attaque ont été publiés.

Tout le monde est concerné par le risque numérique : particuliers comme professionnels, et ce, quel que soit leur taille et leur secteur d'activité

L’industrie de la cybercriminalité

Il existe une véritable industrie de la cyberattaque

Chaine d’intervenants professionnels et spécialisés

Un individu crée le rançongiciel,
un autre identifie une faille de la sécurité,
un autre encore s’occupe de la diffusion du rançongiciel et **de la perception** de la rançon,
le tout sous les ordres d’un donneur d’ordre qui répartit les gains financiers entre chaque maillon de la chaîne

Attaques de masse et d’opportunité

Les attaques **visent** généralement **le plus grand nombre** et **n’atteignent que ceux qui ont un faible niveau ou une sécurité numérique inexistante**.

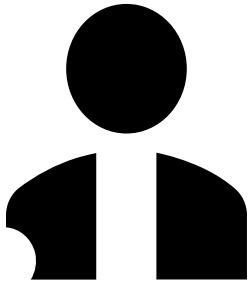
Leur objectif : **dérober le plus grand nombre de données possible qu’ils pourront revendre**.

Gains décuplés

+ d’1 milliard d’euros par an générés par la cybercriminalité

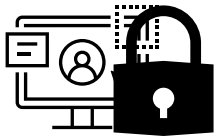
Le 25 novembre dernier, une opération menée par Interpol a permis d’intercepter **130 milliards de dollars**.

L’avocat, cible privilégiée des cybercriminels

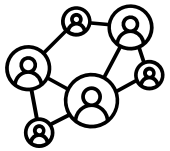


Les avocats sont **tous concernés** par le risque numérique, et ce, quel que soit la taille de leur cabinet et leur secteur d’activité

Les avocats sont **une cible très appréciés** des cybercriminels, car ils possèdent un grand nombre de données stratégiques et/ou personnelles



Les avocats **sont les maillons d’une chaine.**



Quelques exemples :

- Une sécurisation insuffisante d’une boite mail professionnelle peut conduire à transmettre aux CARPA de fausses instructions
- Le fait qu’un cabinet, composé d’avocats inscrits à la communication électronique, soit victime d’une attaque cyber pourrait compromettre toute la communication électronique avec les TJ et les CA.

L’accès digital aux tribunaux ne sera possible que si le système d’information de l’avocat est sécurisé

Les risques les plus fréquents

1. **Le rançongiciel (ou « ransomware »)** → L'attaque se matérialise par l'envoi d'un programme malveillant qui chiffre les données de la victime. Le cybercriminel lui propose de les déchiffrer en échange du paiement d'une rançon

2. **Le hameçonnage (ou « phishing »)** → L'attaquant se fait passer pour une personne ou un tiers de confiance.
La cible reçoit un courrier piégé qui l'invite à cliquer sur un pièce-jointe, un lien ou à communiquer des informations personnelles et/ou privées. Cela permet à l'attaquant de prendre le contrôle de votre système et/ou de faire usage de vos informations

3. **Le piratage de compte**

4. **L'attaque par déni de service (ou « DDoS »** → L'attaque vise à rendre indisponible un ou plusieurs serveurs afin de provoquer une indisponibilité ou un fonctionnement fortement dégradé

La cybercriminalité en quelques chiffres

L’hameçonnage (phishing)

Principal vecteur de cyber malveillance

+ 139%

Piratage de compte

Les messageries de plus en plus ciblées

+ 95 %

Rançongiciels

1ere menace

Chiffres 2021
Source : www.cybermalveillance.gouv.fr

Les impacts de la cybercriminalité

Quels sont les impacts ?

Directs

Vol de données, chiffrement des données, interruption de services sur une durée indéterminée, perte de confidentialité …

Indirects

Couts financiers de rétablissements des services, atteinte à l'image et à la réputation, conséquences juridiques …

La sécurité numérique, un risque d'entreprise qui nécessite une approche globale

1 VOLET PREVENTIF

Se préparer et prévenir le risque de cyberattaque

- Cartographie, analyse et hiérarchie des risques
- Mise en place de mesures de sécurité numérique et d'hygiène informatique adaptées à chaque risque identifié
- Sensibilisation aux incidents
- Mise en place d'un plan de gestion de crise, préparation de la stratégie de communication associée

2 VOLET CURATIF

Traiter le risque numérique réalisé

Une fois l'attaque détectée (1ère étape), il convient de traiter rapidement et efficacement en s'appuyant sur les dispositifs, procédures et outils construits et éprouvés préalablement

Le traitement doit être adapté aux spécificités de l'attaque survenue

02

Projet de feuille de route pour les avocats

L’accompagnement des avocats dans la gestion du risque numérique

Cette feuille de route devrait reposer sur les piliers suivants :

La sensibilisation à la protection des données qu’ils possèdent et à l’importance de mettre l’humain au cœur de cette stratégie

La nécessité de **sécuriser l’adresse email professionnelle**

L’organisation de formation pour appréhender le risque numérique, organiser son cabinet à la prévention et au traitement du risque

La vérification que les polices d’assurance souscrites par les ordres incluent la protection du risque cyber

La mise en place d’une checklist pour les guider dans leurs premiers pas

Le lancement de réflexions sur la sélection de partenaires aptes à accompagner les avocats

03

Projet de feuille de route pour le CNB

ORIENTATIONS

6 orientations pour le CNB afin de répondre aux enjeux stratégiques autour de la cybersécurité

Plan d'action sur 3 ans

Plan d’action

Connaitre et évaluer la dette technique

Enjeux	Plan d’action
Avoir une vision précise de l’existant et identifier là où des mesures de gestion de l’obsolescence seront nécessaires	**Etape 1** : Cartographie complète du système d’information **Etape 2** : Cartographier les risques **Etape 3** : Identifier les chantiers par priorité de remise à niveau en fonction des risques • Sur le système d’information interne : PC, réseaux … • Sur le système d’information avocat : obsolescence applicative (API, messagerie avocat …)

Se connecter

Enjeux	Plan d’action
Renforcer la sécurité de l’authentification	1. Mise à niveau du système d’authentification du CNB (e-Dentitas) 2. Généraliser l’authentification via e-Dentitas sur toutes les applications CNB et partenaires (ministère) 3. Ne plus autoriser en interne les authentifications en dehors de l’annuaire CNB 4. Renforcer et contrôler la politique de gestion des accès

Plan d’action

Superviser, auditer et réagir

Enjeux	Plan d’action
Connaitre l’état du système d’information à un instant précis et enclencher les actions de prévention si cela est nécessaire.	1. Activer et configurer les journaux des composants les plus critiques avec la mise en place d’un Security Operation Center (→2022 – 2023 Nouvel ebarreau) 2. Renforcer la politique de sauvegardes des composants critiques 3. Procéder à des contrôles et audits de sécurité réguliers et appliquer les actions correctives 4. Définir les procédure de gestion des incidents et la gestion de crise

Sécuriser

Enjeux	Plan d’action
Veiller à ce que le SI du CNB soit le plus étanche possible	1. Mise en place d’une politique Zero Trust : • Etanchéité des environnements • Anonymisation des données • Mise en place d’une solution de chiffrement des bases de données les plus critiques • Gérer le nomadisme

Plan d’action

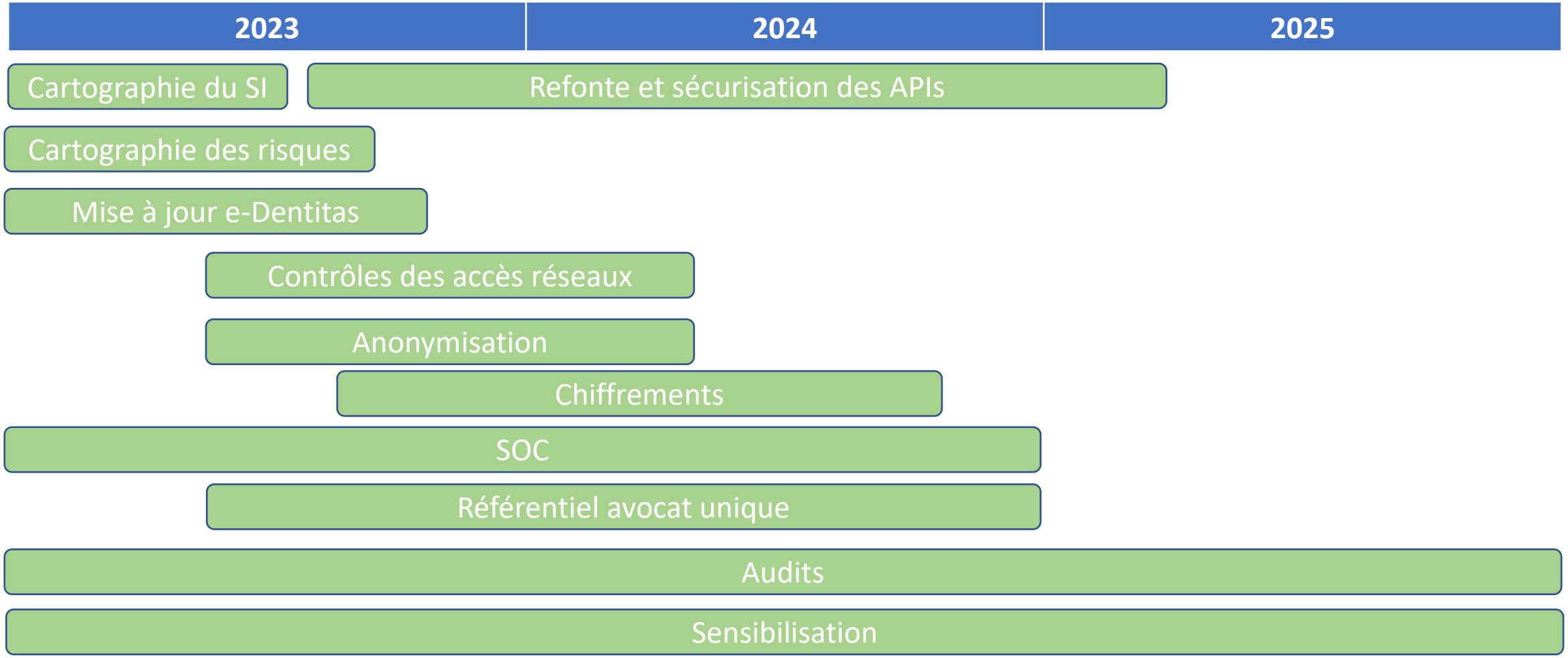
Echanger

Enjeux	Plan d’action
Sécuriser et fiabiliser la donnée et permettre sa transmission	1. Mise en place d’un référentiel unique des avocats 2. Plan de remise à niveau de la gestion des APIs avec la mise en place d’un API Management 3. Sécuriser les flux entrants et sortants

Sensibiliser

Enjeux	Plan d’action
Former les équipes aux reflexes du Security by Design pour toutes les technologies du CNB Sensibiliser les utilisateurs à l’usage des outils numériques et aux risques inhérents	1. Définition d’un plan de gestion des compétences 2. Politique de sensibilisation de la profession à monter en lien avec l’ANSSI 3. Animation d’ateliers à destination de la profession de sensibilisation et d’information à la cybersécurité 4. Mise à disposition d’un référentiel documentaire pour faciliter la transmission de l’information par la profession

MACRO PLANNING



BUDGET

Un plan d’investissement sur 3 ans

2023	2024	2025
700 K€	700 K€	700 K€