1

Cybercriminalité

La confidentialité tu garantiras

"Toute révélation d'un secret est la faute de celui qui l'a confié" Jean de la Bruyère

Anecdote

Dominique est comptable. Il consulte régulièrement les comptes de son entreprise sur le site mis en ligne par sa banque. Par facilité, il a choisi un mot de passe simple, car il le retient plus facilement. C'est la date de naissance de sa fille et le prénom de sa femme : 092014Marine. Ce mot de passe a été découvert facilement par un cybercriminel et l'entreprise s'est fait pirater son compte bancaire.

Essentiel

- **Sécurisez les échanges de données sensibles.**
- **Disposez de mots de passe robustes** : caractères diversifiés, renouvèlement régulier, pas de stockage, etc.
- **Ne divulguez pas d'informations sensibles** et soyez vigilant.
- **Maîtrisez votre e-réputation**.

Bonnes pratiques

Sécurisez les échanges de données sensibles

- Chiffrez les documents confidentiels : fichiers, mails, etc. y compris les clés USB.
- Appliquez les règles de bons sens recommandées par l'ANSSI dans son "passeport de conseils aux voyageurs" (site de l'ANSSI).
- Rappelez aux collaborateurs que les mêmes règles de sécurité doivent être appliquées au BYOD ("Bring Your Own Device" ou PAP en français "prenez vos appareils personnels") : mise à jour, antivirus, mots de passe, verrouillage systématique.

Disposez de mots de passe robustes

- Renforcez la politique de gestion des mots de passe : utilisez des mots de passe robustes (minimum 8 caractères, mots n'existant pas dans le dictionnaire, utilisation de caractères spéciaux et de chiffres), différents pour chaque accès et renouvelez-les tous les 3 ou 4 mois.
- Ne stockez jamais vos mots de passe de manière accessible.
- N'activez pas l'option "mémorisez vos mots de passe".
- Ne communiquez jamais vos mots de passe.
- N'utilisez pas d'autres comptes que le vôtre.
- Participez à la protection des informations de l'entreprise car vous êtes responsables des droits que vous pourriez donner à d'autres utilisateurs.
- Utilisez des coffres-forts virtuels.

Ne divulguez pas d'informations sensibles

- Ne parlez jamais des données personnelles de vos clients ou de procédures internes avec des tiers non autorisés.
- Ne diffusez aucune anecdote susceptible d'altérer l'image de marque de l'entreprise ni aucune pratique sensible propre à l'entreprise.
- Ne donnez jamais la possibilité à un tiers non autorisé de visualiser vos documents de travail. Vous pouvez utiliser des filtres de confidentialité.
- Verrouillez les ordinateurs.
- Mettez en place des procédures pour gérer le départ des collaborateurs (À quoi avaient-ils accès ? Pensez à changer leurs mots de passe et supprimer leurs accès).

Maîtrisez votre e-reputation

- Disposez d'une charte d'utilisation des réseaux sociaux afin de sensibiliser les collaborateurs aux risques liés à la divulgation de données confidentielles hors de l'entreprise (fraude aux présidents, fuite de données...). *Voir le 9e commandement.*
- Maîtrisez votre e-réputation (Google, Corporama, etc.) : vérifiez régulièrement votre identité numérique.

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

ORDRE DES EXPERTS-COMPTABLES
Conseil Supérieur

Un contrat de **cyber-assurance** tu souscriras

"On ne peut affirmer avec plus d'assurance que rien n'est assuré" Anatole France

Anecdote

Le Cabinet SIBERAUDIT est en infogérance. Il subit une panne à l'approche des fêtes et le contact technique est injoignable. Les membres du cabinet sont donc dans l'impossibilité de travailler pendant plus de 48h. Les frais engendrés pour récupérer les données auraient pu être couverts s'ils avaient mis en place un plan d'assurance sécurité adapté.

Essentiel

- **Définissez la typologie des risques assurables** : données personnelles, système d'information de l'assuré, données des tiers.
- **Analysez les offres disponibles** : couverture des dommages immatériels, préjudices, frais de communication de crise ; prise en charge de la gestion de crise et de la restauration des données ; responsabilité civile.
- **Répertoriez les propositions de valeur pour l'assuré** : évaluation, quantification, réduction et transfert des risques, expertise post-incident.

Bonnes pratiques

Définissez la typologie des risques assurables

- Données personnelles : frais de notification, d'expertise, de défense, frais en cas de contrôle ou d'enquête ; sanctions pécuniaires, atteinte à la propriété intellectuelle.
- Système d'information de l'assuré : vol, ajout, détérioration, destruction, interruption de service ; atteinte à l'image et à la réputation ; compromission du SI, perte d'exploitation et frais supplémentaires ; site internet non opérationnel.
- Données des tiers : interruption de services et réclamation des tiers, corruption des données, erreur, frais de défense.

Analysez les offres disponibles

- Couverture des dommages immateriels.
- Couverture des préjudices occasionnés aux tiers.
- Prise en charge de la gestion de crise et l'assistance.
- Prise en charge de la restauration des données.
- Couverture perte de revenus due aux cyberattaques.
- Responsabilité civile.
- Prise en charge des frais de communication de crise visant à protéger la réputation de l'entreprise, etc.

Répertoriez les propositions de valeur pour l'assuré

- Évaluation des risques : accompagnement dans l'identification des risques sur le SI, audit du SI et évaluation des mesures de sécurité.
- Quantification des risques encourus par le client en fonction des résultats des tests, valorisation des risques en fonction des impacts potentiels (financiers, image, temps, etc.).
- Réduction des risques : mise en œuvre d'un plan de traitement des risques permettant de réduire les risques à un niveau acceptable, accompagnement du client et expertise en cyber sécurité.
- Transfert des risques : identification des risques assurables, formalisation des garanties et primes d'assurances.
- Expertise post-incident : acompagnement du client pour limiter la propagation de l'incident, expertise permettant de revenir à un état stable.

Une **perte** ou un **vol** tu anticiperas

"Celui dont la pensée ne va pas loin verra ses ennuis de près" Confucius

Anecdote

Maryse a cliqué par inadvertance sur un lien d'une page infectée. Un programme malveillant s'est alors installé automatiquement sur son ordinateur. Malgré les sauvegardes régulières, elle n'a pas pu récupérer les fichiers car elle ne s'était pas assurée du bon fonctionnement des sauvegardes. Sauvegarder c'est essentiel, les tester c'est vital !

Essentiel

- **Ayez une stratégie rigoureuse de sauvegarde.**
- **Soyez conscients des avantages et inconvénients des supports.**
- **Prenez des précautions dans l'utilisation des supports.**

Bonnes pratiques

Ayez une stratégie rigoureuse de sauvegarde

- Raisonnez par priorité et protégez les informations les plus sensibles.
- Sauvegardez les données sur des serveurs distincts : elles peuvent être stockées en interne, mais aussi auprès d'un prestataire informatique ou d'un hébergeur de données dans le cloud.
- Isolez informatiquement et physiquement le lieu de stockage des fichiers de sauvegarde : cela évite, en cas d'attaque, que les fichiers de sauvegarde ne soient eux aussi contaminés par le virus.
- Démultipliez les sauvegardes sur plusieurs supports : il faut évaluer leur viabilité par des essais périodiques de restauration.
- Faites une sauvegarde "hors ligne" pour éviter qu'elle soit elle aussi cryptée au moment de l'attaque.
- Vérifiez régulièrement que les sauvegardes se sont bien déroulées en vérifiant le rapport de sauvegarde.
- Testez régulièrement les sauvegardes en restaurant quelques dossiers ou fichiers.

Soyez conscient des avantages et inconvénients des supports

Type de supports	Avantages	Inconvénients
Les supports physiques externes, (disque dur externe, CD, DVD, clé USB, carte mémoire, etc.)	Facile à déplacer, facile à utiliser, coût limité	Durée de vie des supports, capacité de stockage limitée, support pouvant être compromis par les hackers pour faire une cyberattaque, peut être facilement perdu/volé
Le serveur de fichiers et serveur NAS	Capacité de stockage, centralisation et partage des données avec plusieurs appareils, sauvegarde de l'ensemble des données à partir d'un endroit unique ; accès gratuit aux données, permet de rester propriétaire de ses données	Système d'administration complexe, intégrité des données en cas de défaillance du NAS : prévoir un système de sauvegarde de secours, attention à la sécurité des accès
Les espaces de stockage en ligne (cloud)	Disponibilité quasi immédiate, travail collaboratif, gestion du ATAWAD (AnyTime, AnyWhere, AnyDevice)	Sécurité limitée, risques spécifiques pour la confidentialité des données, risques juridiques liés à l'incertitude sur la localisation des données, risques pour la disponibilité et l'intégrité des données, risques liés à l'irréversibilité des contrats

Prenez des précautions dans l'utilisation des supports

- Vérifiez l'intégrité du support de sauvegarde.
- Veillez à la confidentialité des données sensibles en rendant leur lecture impossible à des personnes non autorisées (mot de passe) ou en les chiffrant.
- Soyez vigilant en prenant connaissance des conditions générales d'utilisation.

4

De boucliers tu te muniras

"Lorsque deux forces sont jointes, leur efficacité est double" Isaac Newton

Anecdote

Didier n'a pas mis à jour son antivirus. Après avoir téléchargé une application sur un site non sécurisé, un logiciel espion non détecté par l'antivirus a crypté l'ensemble de ses fichiers. Celui-ci vient de subir une attaque de type "ransomware" car il aurait dû mettre à jour son antivirus pour bloquer le logiciel espion. Ça lui a coûté 10 Bitcoins (soit environ 66 000 € à fin novembre 2017)...

Essentiel

- **Munissez-vous d'antivirus et d'antispam** : régulièrement à jour et actif, inspectez le contenu des clés USB et fichiers téléchargés.
- **Vérifiez que les systèmes sont régulièrement à jour** : évitez les systèmes obsolètes et les versions logicielles anciennes, révoquez les droits des collaborateurs en cas de départ, etc.
- **Disposez de pare-feux actifs.**

Bonnes pratiques

Munissez-vous d'antivirus et d'antispam

- Mettez en place un antivirus et un antispam.
- Vérifiez que l'antivirus et l'antispam sont actifs et à jour.
- Faites toujours inspecter le contenu des clés USB inconnues par l'antivirus.
- Avant d'ouvrir les documents téléchargés, lancez systématiquement une analyse antivirus en désactivant l'ouverture automatique de ces derniers.
- Ne désactivez pas l'antivirus et l'antispam.
- Faites régulièrement les mises à jour proposées de l'antivirus et antispam.
- Vérifiez que les mises à jour sont faites sur les sites officiels et sécurisés (https://).
- Configurez vos logiciels pour que les mises à jour de sécurité puissent s'installer automatiquement lorsque cela est possible.

Vérifiez que les systèmes sont à jour

- Faites régulièrement les mises à jour proposées des systèmes et logiciels : Windows, Adobe, Java, Office, Flash, etc.
- Vérifiez que ces mises à jour sont faites sur les sites officiels et sécurisés (https://).
- Évitez les systèmes d'exploitation obsolètes (Windows XP, Windows 2003), et les versions logicielles anciennes (Office, Adobe).
- Assurez-vous que les droits octroyés sur les systèmes d'information sont bien révoqués lors du départ d'un collaborateur.
- N'hésitez pas à utiliser les journaux d'évènements pour réagir aux évènements suspects.

Disposez de pare-feux actifs

- Vérifiez que vous disposez de pare-feux actifs sur les postes Windows et routeurs.
- Ne désactivez pas le pare-feu.
- Consultez régulièrement le pare-feu afin de vérifier les ports qui sont ouverts, vous pouvez également paramétrer votre pare-feu pour refuser toutes les connexions entrantes.

Aux **cyberattaques** tu réagiras

"Il n'y a pas de vent favorable pour celui qui ne sait où il va" Sénèque

Anecdote

Thierry, expert-comptable associé dans le Rhône a été victime au sein de son cabinet d'une cyberattaque en juin dernier. Par chance, un des collaborateurs n'ayant plus accès aux fichiers a donné l'alerte aussitôt. Des mesures efficaces ont été prises pour éviter que le virus ne se propage. Tous les collaborateurs ont fermé leur session et se sont déconnectés du réseau. Le prestataire informatique est intervenu dans la foulée et à l'aide des sauvegardes quotidiennes, les fichiers ont pu être restaurés.

Essentiel

- **Adoptez une méthodologie de traitement du risque au jour de l'attaque** : débranchez l'ordinateur du réseau, n'utilisez plus l'équipement corrompu, portez plainte, ne payez pas la rançon, procédez à une analyse complète par l'antivirus, lancez la récupération des données, prévoyez des plans de secours, etc.
- **Contactez les structures d'assistance aux victimes de cyberattaques** : ACYMA, CERT, Cybermalveillance, Stopransomware.

Bonnes pratiques

Adoptez une méthodologie de traitement du risque au jour de l'attaque

- Débranchez immédiatement votre ordinateur du réseau (cable éthernet) et coupez votre wifi, afin que le virus ne se propage pas sur tout le réseau informatique.
- Signalez l'attaque au service informatique ou au prestataire dans les plus brefs délais afin qu'il puisse intervenir pour évaluer les dommages et limiter les conséquences.
- Arrêtez d'utiliser l'équipement corrompu afin de ne pas effacer les preuves : en matière de préservation des traces et indices, il est nécessaire de figer "la scène de crime" en rassemblant le maximum d'éléments qui permettront de mener à bien une enquête.
- ⚠ **Portez plainte auprès de la gendarmerie ou de la police nationale.**
- En cas de ransomware : ne payez pas la rançon, cela ne garantit en rien le déchiffrement des données.
- Procédez à une analyse complète par l'antivirus afin qu'il essaie de repérer et supprimer le code malveillant => si cette étape n'est pas concluante, il faudra alors procéder au formatage (effacement de toutes les données) du disque dur mais le mieux étant d'en acheter un neuf.
- Lancez la restauration des données à partir d'une sauvegarde.
- Prévoyez des plans de secours, élaborés avec des spécialistes, permettant d'éviter la perte irrémédiable de données et de garantir la continuité d'exploitation.
- Établissez un plan de communication en cas de crise suite à une cyberattaque grave.

Contactez les structures d'assistance aux victimes de cyberattaques

- ACYMA : plateforme d'assitance aux victimes d'actes de cybermalveillance. Grâce à ses réponses au questionnaire, la victime est orientée vers les prestataires de proximité susceptibles de répondre à son besoin technique.
- CERT : centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques.
- Cybermalveillance.gouv.fr : plateforme d'assitance du risque numérique mise en place par l'ANSSI.
- Stopransomware (réseau Cecyf prévention).

6

Le RGPD tu respecteras

"Pour savoir où l'on va, il faut savoir d'où l'on vient" Proverbe africain

Anecdote

Le cabinet Hergé gère la paye de ses clients et dispose des données personnelles des salariés. Dès le 25 mai 2018 le cabinet Hergé sera concerné par le RGPD et encourt une amende administrative pouvant aller, pour les cas les plus graves, jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

Essentiel

Vous-êtes tous concernés par le RGPD, mais faites-vous partie des 9% d'entreprises qui se déclarent prêtes ?

- Désignez un responsable des questions personnelles.
- Cartographiez vos traitements de données personnelles existants dans le cabinet.
- Priorisez et hiérarchisez les actions à mener.
- Gérer les risques.
- Organisez les processus internes.
- Documentez pour prouver la conformité au RGPD en cas de contrôle.

Bonnes pratiques

Étape 1 — Désignez un responsable des questions personnelles

- La désignation d'une personne chargée de ces questions est :
  - **obligatoire** si vous réalisez un suivi régulier ou traitez à grande échelle des données dites "sensibles" ou relatives à des condamnations pénales et infractions ;
  - **facultative** pour la plupart des cabinets d'expertise-comptable mais la CNIL encourage cette désignation : possibilité de désigner un DPO mutualisé ou externe.
- En attendant 2018, vous pouvez désigner un CIL pour commencer à organiser les actions à mener.

Étape 2 — Cartographiez vos traitements de données personnelles existants dans le cabinet

- Faites un inventaire des traitements de données personnelles mis en œuvre pour évaluer les pratiques, identifier les risques et arrêter un plan d'action.
- Organisez la gouvernance de la donnée avec le registre des traitements (modèle disponible sur le site de la CNIL) : Qui ? Quoi ? Pourquoi ? Où ? Jusqu'à quand ? Comment ?
- Les modèles de déclaration CNIL peuvent vous aider pour déterminer les finalités des traitements.

Étape 3 — Priorisez et hiérarchisez les actions à mener

- Déterminez les actions à mettre en œuvre pour respecter les nouvelles règles du RGPD.
- Assurez-vous que seules les données strictement nécessaires à la poursuite de l'objectif du traitement sont collectées et traitées.
- Identifiez la base juridique sur laquelle se fonde votre traitement (intérêt légitime, contrat, obligation légale, consentement de la personne...).
- Révisez vos mentions d'information pour qu'elles soient conformes aux exigences du règlement.
- Vérifiez que vos sous-traitants connaissent leurs nouvelles obligations et leurs responsabilités, assurez-vous de l'existence de clauses contractuelles (modèles de clauses sur le site de la CNIL) telles que : sécurité, confidentialité, protection des données.
- Prévoyez les modalités d'exercice des droits des personnes concernées : droit d'accès, de rectification, droit à la portabilité, retrait du contentement...
- Vérifiez les mesures de sécurité.

• • •

Le RGPD tu respecteras

• • •

Étape 4 — Gérez les risques

- S'il existe des risques élevés pour les droits et libertés des personnes concernées (traitements de données sensibles, traitements reposant sur le profilage…) menez pour chacun de ces traitements une étude d'impact sur la protection des données ("Privacy Impact Assessment" ou "PIA").
- Une PIA doit contenir une description du traitement et de ses finalités, une évaluation de la nécessité et de la proportionnalité du traitement, une appréciation des risques sur les droits et libertés des personnes concernées, les mesures envisagées pour traiter ces risques et se conformer au RGPD.
- L'outil PIA de la CNIL vise à accompagner la conduite d'analyse d'impact et faciliter l'appropriation des guides PIA de la CNIL (disponible sur le site de la CNIL).

Étape 5 — Organisez les processus internes

- Mettez en place des procédures internes pour assurer la protection des données tout au long du traitement :
  - en cas de faille de sécurité, de demande de rectification ou d'accès, de demande de modification des données collectées, de changement de prestataire ;
  - anticipez les violations de données : notifiez à l'autorité de protection des données dans les 72h et aux personnes concernées dans les meilleurs délais ;
  - prévues dans le RGPD : audits, privacy by design, notification des violations de données, gestion des réclamations et des plaintes…
- Établissez une politique de protection des données personnelles dans le cabinet et sensibilisez vos collaborateurs par le biais de communications et formations.
- Traitez les réclamations et demandes des personnes concernées en définissant les acteurs et les modalités.

Étape 6 — Documentez pour prouver la conformité au RGPD en cas de contrôle

- La documentation réalisée à chaque étape doit être réexaminée et actualisée régulièrement pour assurer une protection des données en continu.
- Documentation de vos traitements de données personnelles : registre des traitements (responsables des traitements) ou des catégories d'activités de traitements (sous-traitants), analyses d'impact sur la protection des données (cf. étape 4), encadrement des transferts de données hors de l'UE.
- Information des personnes : mentions d'informations, recueil du consentement des personnes concernées, procédures mises en place pour l'exercice des droits.
- Contrats définissant les rôles et responsabilités des acteurs : contrats avec les sous-traitants, procédures internes en cas de violations de données, preuve que les personnes concernées ont donné leur consentement.
- Lien avec la norme professionnelle de maîtrise de la qualité (NPMQ) et le manuel existant dans les cabinets.

7

Cybercriminalité

Des clés USB (et tous supports physiques externes) tu te méfieras

"Un ordinateur en sécurité est un ordinateur éteint. Et encore..." Bill Gates

Anecdote

Marc a reçu une clé USB en "cadeau". Cette clé USB a en réalité été distribuée par un pirate dans la boîte aux lettres, comme un cadeau. Par curiosité, et c'est humain, Marc branche alors cette clé sur son ordinateur pour voir ce qu'elle contient... Et se retrouve avec un virus qui donne accès aux pirates à toutes les données qu'il contient, mais également à l'ensemble des données de l'ensemble des postes connectés au réseau.

Essentiel

- **Adoptez des mesures préventives** : n'utilisez jamais une clé USB "abandonnée", avant toute utilisation, scannez et nettoyez la clé USB, bloquez la fonction "Autorun", affectez une clé par usage, chiffrez le contenu de vos clés USB.
- **Préparez vos déplacements à l'étranger** : n'emportez que les données indispensables pour la mission, marquez vos clés et gardez-les sur vous, jetez-les après usage.

Bonnes pratiques

Adoptez des mesures préventives

- Bloquez la clé en écriture pour éviter qu'une application malveillante ajoute des malwares sur votre clé.
- Ne tentez jamais de connecter votre poste de travail à un support de stockage externe, sauf s'il fait partie des outils de travail qui vous ont été attribués officiellement.
- Utilisez exclusivemet des clés USB sécurisées, fournies par l'entreprise et, en votre absence, conservez-les dans un rangement sécurisé (coffre, armoire, sous clés).
- Nettoyez proprement le contenu de la clé en utilisant des logiciels adaptés et faites analyser les fichiers provenant de supports USB via un antivirus avant ouverture.
- Attribuez des comptes et droits utilisateurs adéquats (pas de connexion en mode administrateur).
- Bloquez la fonction Autorun.
- Verrouillez les postes de travail en cas d'absence pour prévenir des accès intrusifs.
- Chiffrez les données enregistrées sur la clé USB pour éviter le piratage.
- Affectez une clé par usage pour réduire les risques de contamination, cet outil doit être strictement personnel et non cessible.

Préparez vos déplacements à l'étranger

- N'emportez que les données dont vous avez besoin pour la mission.
- Évitez de partir avec des données sensibles.
- Marquez d'un signe distinctif vos clés (pour repérer tout échange...).
- Gardez vos clés USB sur vous.
- En cas de perte ou de vol, informez les personnes compétentes et/ou prenez les mesures de sauvegardes prévues.
- Emportez une clé destinée aux échanges commerciaux et jetez-la après usage et destruction.
- À votre retour, ne connectez pas les clés sans les avoir testées au préalable.

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

ORDRE DES EXPERTS-COMPTABLES
Conseil Supérieur

De **bonnes pratiques managériales** tu adopteras

"Celui qui déplace une montagne commence par déplacer de petites pierres" Confucius

Anecdote

L'entreprise AYMHACK, PME locale dans le secteur industriel, détient des données stratégiques telles que des brevets. Arthur est commercial et dispose d'informations sensibles... Il vient de se faire pirater lors d'un déplacement. Une classification des données sensibles de l'entreprise aurait permis de mieux les sécuriser afin de bloquer le "hacker" avant qu'il n'atteigne ces données.

Essentiel

- **Instaurez une classification des données de l'entreprise.**
- **Adoptez de bonnes habitudes de travail**
- **Renforcez vos procédures internes** : restrictions d'accès, gestion des départs des collaborateurs, procédure en cas de modification des RIB fournisseurs, etc.
- **Supervisez, auditez et corrigez** : tests d'intrusion, plan de reprise et de continuité d'activité.

Bonnes pratiques

Instaurez une classification des données de l'entreprise

- Identifiez les données stratégiques qui pourraient être particulièrement convoitées par les pirates.
- Évaluez les menaces et vulnérabilités sur ces données sensibles.
- Renforcez leur niveau de protection si besoin.

Adoptez de bonnes habitudes de travail

- Organisez des réunions d'information pour alerter les collaborateurs sur les nouveaux types de menaces.
- Sensibilisez, informez, avertissez les collaborateurs via des mesures de bons sens. Des vidéos, e-learning et sites permettent d'illustrer les dangers liés à la cybercriminalité de façon pédagogique et démontrent qu'il suffit parfois de simples mesures de bon sens pour se prémunir des attaques.
- Formez les collaborateurs les plus aguerris. Deux Mooc (Massive Open Online Course) certifiants sont disponibles sur le site de l'ANSSI pour vous initier à la cybersécurité, approfondir vos connaissances et ainsi vous prémunir des cyber-risques.

Renforcez vos procédures internes

- Mise en place de restrictions d'accès.
- Mise en place de procédures pour gérer le départ des collaborateurs (changez leurs mots de passe, supprimez leurs accès).
- Disposez d'une procédure en cas de demande de modification des RIB fournisseurs : prévoir une supervision ou un contre-appel vers un numéro déjà référencé.
- Renforcez les procédures de confirmation des banques.
- Soyez prudent dans les lieux publics : n'importe qui peut voir l'écran (disposez d'un filtre de confidentialité peut éviter certaines fuites) ou écouter une conversation / anecdote susceptible d'altérer l'image de marque de l'entreprise ; protégez les pratiques sensibles propres à l'entreprise.

Supervisez, auditez et corrigez

- Procédez à des tests d'intrusion pour tester la vigilance des collaborateurs et faciliter l'adhésion de l'ensemble des acteurs à la mise en place de mesures simples de prévention de cyberattaques.
- Rédigez un plan de reprise et de continuité d'activité qui permet de garantir les fonctions vitales de l'entreprise en cas d'attaque.

Les usages tu règlementeras

"Si vous pensez que la technologie peut résoudre tous vos problèmes de sécurité, alors vous ne comprenez ni les problèmes, ni les technologies..." Bruce Schneir

Anecdote

Lydie va quotidiennement sur les réseaux sociaux pour relater ses journées avec ses clients et ses collègues. Elle vient d'annoncer sur Twitter que son entreprise est en train de se faire racheter et a juste oublié qu'il s'agissait d'une information confidentielle à ne pas divulguer... L'existence d'une charte d'utilisation des réseaux sociaux, annexée à la charte informatique, aurait permis d'éviter ce type de risques.

Essentiel

- **Encadrez les pratiques par l'utilisation d'une charte informatique.**
- **Fixez les règles et consignes que les utilisateurs doivent respecter.**
- **Rendez-la opposable aux salariés** soit en l'annexant au contrat de travail des salariés, soit en formalisant l'acceptation individuelle par chacun des salariés ou en lui donnant une valeur de règlement intérieur.

Bonnes pratiques

Encadrez les pratiques par l'utilisation d'une charte informatique

- La mise en place d'une charte informatique est indispensable... voire obligatoire dès lors que le cabinet collecte des données à caractère personnel... Ce qui s'avère aujourd'hui omniprésent ! Un modèle est disponible sur le kit mission "accompagner ses clients dans la mise en place d'un règlement interieur".
- Responsabilisez les acteurs par une démarche d'explication et de sensibilisation des enjeux et risques associés à son utilisation.
- Pour faire adhérer tous les collaborateurs, disposez d'un charte claire, à la portée de tous et diffusée à l'ensemble du personnel.
- Informez les salariés des modalités de contrôle de leur employeur tout en veillant au respect de la vie privée.

Fixez les règles et consignes que les utilisateurs doivent respecter

- Définissez les principes généraux de sécurité : accès, habilitation, sécurité, matériels, programmes, logiciels...
- Formalisez les règles d'utilisation du système d'information : séparez les usages personnels et professionnels, mots de passe, sauvegarde, utilisation d'internet...
- Prévoyez d'y intégrer les modalités d'utilisation des réseaux sociaux et de l'ensemble des moyens technologiques mis à disposition des salariés (smartphones, supports nomades...).
- Prévoyez des mesures de contrôle par l'employeur : équilibre vie privée et protection du SI...
- Déterminez les politiques de sanctions prévues en cas de violations des obligations : les sanctions devront être proportionnelles à l'impact que l'infraction aurait sur le système d'information.
- Prenez acte de sa perfectibilité et révisez-la régulièrement pour qu'elle s'adapte à l'évolution des technologies.

Rendez-la opposable aux salariés

- Pour qu'elle soit opposable aux salariés, plusieurs options sont possibles :
  - option 1 : annexez la charte au contrat de travail des salariés ;
  - option 2 : formalisez l'acceptation individuelle par chacun des salariés ;
  - option 3 : donnez à la charte une valeur de règlement intérieur et respectez scrupuleusement le formalisme préalable à l'adoption d'un règlement intérieur => dépôt au greffe du Conseil des Prud'hommes et transmission à l'inspection du travail.

Les **collaborateurs** tu sensibiliseras

"Le maillon faible se situe entre la chaise et le clavier" Anonyme

Anecdote

L'entreprise PADEUBOL subit une attaque liée à une mauvaise pratique d'un collaborateur suite à la réception d'un email douteux. La continuité d'exploitation est compromise, elle doit mettre la clé sous la porte. La simple mise en place d'un test d'intrusion aurait permis d'anticiper et d'éviter cette attaque. En effet une prise de conscience générale et immédiate des collaborateurs aurait facilité l'adhésion des acteurs au sein de l'entreprise à la mise en place de mesures simples de prévention de cyberattaques.

Essentiel

- **Sensibilisez les collaborateurs.**
- **Nommez un responsable de la sécurité du Système d'Information pour piloter la démarche** et coordonner les différentes actions à mener.
- **Impliquez et responsabilisez les usages dans les mécanismes de cyberprévention** : informez, sensibilisez, formez, motivez.
- **Soyez interactif et passez d'une pédagogie "passive" à une pédagogie "active".**

Bonnes pratiques

Sensibilisez les collaborateurs

En 1982, Rich Skrenta, lycéen américain âgé de 15 ans, a créé le 1er virus référencé qui se propage automatiquement par échange de supports amovibles : "Elk Cloner". Le mécanisme viral associant les fragilités humaines à un code malveillant, déjà présent dans les années 80, est strictement identique aux mécanismes actifs aujourd'hui. Il faut donc l'accepter : depuis plus de 35 ans, l'Homme est le maillon faible de la défense numérique. Longtemps délaissé au profit de la technologie, le facteur humain doit désormais faire partie intégrante de la cybersécurité.

Nommez un responsable de la sécurité du SI pour piloter la démarche

- Sa mission est de garantir l'intégrité, la confidentialité, la disponibilité et la traçabilité des données de l'ensemble des systèmes d'information du cabinet.
- Véritable chef d'orchestre de la sécurité du SI, il définit les orientations, élabore et met en œuvre une politique de sécurité.

Impliquez et responsabilisez les usagers dans les mécanismes de cyberprévention

1/ **Informez > Quoi ?** L'utilisateur sait qu'un danger existe.
2/ **Sensibilisez > Pourquoi ?** L'utilisateur connaît les risques pour le cabinet et lui-même.
3/ **Formez > Comment ?** L'utilisateur sait ce qu'il faut faire.
4/ **Motivez > Quand ?** L'utilisateur sait qu'il doit être vigilant constamment.

Soyez interactif et passez d'une pédagogie "passive" à une pédagogie "active"

- Selon le "cône d'apprentissage" d'Edgar Dale, l'expérimentation et la simulation permettent de retenir 90 % des messages clés contre seulement 10 % de ce qui est lu : test d'intrusion...
- La sécurité est avant tout une question de jugement et de comportement. C'est donc en impliquant les utilisateurs que les consciences à la sécurité de l'information seront éveillées durablement.

Les objets connectés tu sécuriseras

"Tout artiste ou chercheur le sait, sans un espace protégé, et même sanctuarisé, où l'erreur est possible, l'innovation cesserait d'exister" Inconnu

Anecdote

Dans le cadre du télétravail, Madame Alexa SNIPS profite de la fonctionnalité « kit main libre » de son enceinte intelligente pour mener des réunions en téléconférence avec ses équipes.
Or, cette dernière a été piratée et le fraudeur a enregistré ces réunions de travail dont certaines abordent des sujets stratégiques / confidentiels.

Essentiel

- **Sécurisez les échanges de données.**
- **Protégez** votre profil utilisateur.
- **Maîtrisez les enjeux** autour de votre vie professionnelle et privée.

Bonnes pratiques

Sécurisez les échanges de données

- Vérifiez que l'appairage ainsi que la connexion de l'objet depuis Internet nécessitent un bouton d'accès physique ou l'usage d'un mot de passe.
- Modifiez le paramétrage par défaut (mot de passe, code PIN, etc.).
- Vérifiez l'accès aux données et la possibilité de les supprimer.
- Éteignez l'objet non utilisé afin d'éviter qu'il ne capte les données sensibles.
- Privilégiez l'utilisation d'un VPN (Virtual Private Network, afin de sécuriser les flux d'informations entre l'objet et le réseau de l'entreprise) en l'absence de cloud.
- Assurez la protection du réseau wifi personnel à l'aide d'une clé de chiffrement robuste (clé WPA *a minima*).
- Réalisez les mises à jour de sécurité proposées par les fabricants d'objets connectés.

Protégez votre profil utilisateur pour les objets nécessitant l'ouverture d'un compte en ligne

- En cas de télétravail, ne connectez pas vos outils professionnels aux objets à reconnaissance vocale personnels.
- Utilisez des pseudonymes (et non vos données personnelles).
- Ne communiquez pas d'informations superflues (donnez une date de naissance au 1er janvier si le système a besoin de déterminer un âge).
- Créez une adresse secondaire de l'adresse principale et qui soit différente de l'adresse professionnelle.
- Pour aller plus loin : https://www.cnil.fr/fr/objets-connectes-noubliez-pas-de-les-securiser.

Maîtrisez les enjeux autour de votre vie professionnelle et privée dans le cas des assistants vocaux

- Éteignez l'appareil lorsqu'il est inutilisé ou que l'on ne souhaite pas être écouté.
- Informez les tiers du possible enregistrement des conversations (à défaut, coupez le micro).
- Connectez uniquement les services présentant une réelle utilité ; attention aux risques à partager des données confidentielles ou des fonctionnalités sensibles.
- Gardez en mémoire que les propos tenus peuvent enrichir votre profil publicitaire.
- Supprimez régulièrement l'historique des conversations.
- N'hésitez pas à contacter les services supports en cas de questions et, le cas échéant, la CNIL. https://www.cnil.fr/fr/enceintes-intelligentes-des-assistants-vocaux-connectes-votre-vie-privee

Scannez le QR code pour accéder aux fiches

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

ORDRE DES EXPERTS-COMPTABLES
Conseil Supérieur