EXPERTS-COMPTABLES ET
COMMISSAIRES AUX COMPTES DE FRANCE

LES ÉTATS GÉNÉRAUX
DE LA CYBERSÉCURITÉ DE LA PROFESSION

28 FÉVRIER 2024

GUIDE D'HYGIÈNE EN SECURITÉ
DES SYSTEMES D'INFORMATION POUR LES CABINETS D'EXPERTISE COMPTABLE

1 - PILOTAGE DU PROJET

La sécurisation des systèmes d'information est un process qui englobe toute la sphère d'un cabinet d'expertise comptable et concerne tout son personnel, de l'expert-comptable associé au stagiaire d'été. Sa réussite passe incontestablement par un engagement fort de la direction. Se fixer des objectifs, mesurer et impliquer sont des jalons indispensables.

Ayez à l'esprit que la cybersécurité relève autant du matériel que de l'humain et des process.

2 - GEREZ VOS MOTS DE PASSE

Top 10 des mots de passe les plus utilisés en 2019-2022
Source : Etude NordPass 2023)

CLASSEMENT	MOT DE PASSE	TEMPS NÉCESSAIRE POUR LE DÉCHIFFRER	DÉCOMPTE
1	123456	< 1 Seconde	4 524 867
2	admin	< 1 Seconde	4 008 850
3	12345678	< 1 Seconde	1 371 152
4	123456789	< 1 Seconde	1 213 047
5	1234	< 1 Seconde	969 811
6	12345	< 1 Seconde	728 414
7	password	< 1 Seconde	710 321
8	123	< 1 Seconde	528 086
9	Aa123456	< 1 Seconde	319 725
10	1234567890	< 1 Seconde	302 709

LES STOCKER

Utilisez un gestionnaire de mots de passe, type Lockself, NordPass, KeePass, Dashlane.

Cet outil permet de ne retenir qu'un seul mot de passe fort et sécurisé (appelé le « mot de passe Maître ») pour chaque utilisateur. Au sein des cabinets d'expertise comptable, il offre l'avantage de combiner deux types d'usage :

- La gestion des mots de passe internes : Centralisez tous les accès et mots de passe du cabinet. Mettez à jour les identifiants de connexion et les mots de passe associés en utilisant ceux générés par le gestionnaire. Enfin, accordez les droits aux seuls collaborateurs habilités à se connecter au service concerné.
- La gestion des mots de passe clients : Répertorier les mots de passe transmis par les clients, au sein de « Notes sécurisées ». Veillez à en limiter l'accès aux seuls collaborateurs en charge du dossier.

A chaque mouvement de personnel, accordez les accès nécessaires aux nouveaux arrivants et supprimez les utilisateurs partants afin qu'ils ne gardent aucun des accès du cabinet ou des clients.

Enfin, en cas de compromission, changez votre mot de passe immédiatement !

Activez la double authentification (MFA) chaque fois que cela est possible.

COMBIEN DE TEMPS FAUT-IL À UN PIRATE POUR TROUVER VOTRE MOT DE PASSE EN 2023 ?

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
5	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
6	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
7	Immédiat	Immédiat	1 seconde	2 secondes	4 secondes
8	Immédiat	Immédiat	28 secondes	2 minutes	5 minutes
9	Immédiat	3 secondes	24 minutes	2 heures	6 heures
10	Immédiat	1 minute	21 heures	5 jours	2 semaines
11	Immédiat	32 minutes	1 mois	10 mois	3 ans
12	1 seconde	14 heures	6 ans	53 ans	226 ans
13	5 secondes	2 semaines	332 années	3 000 années	15 000 ans
14	52 secondes	1 an	17 000 ans	202 000 ans	1 million d'années
15	9 minutes	27 ans	898 000 ans	12 millions d'années	77 millions d'années
16	1 heure	713 ans	46 millions d'années	779 millions d'années	5 milliards d'années
17	14 heures	18 000 ans	2 milliards d'années	48 milliards d'années	380 milliards d'années
18	6 jours	481 000 ans	126 milliards d'années	1 trillion d'années	26 trillions d'années

Infographie FRANCENUM.GOUV.FR Source : Hive Systems

3 - SECURISEZ VOTRE MATERIEL ET VOS INSTALLATIONS

- Utilisez un cache web cam si celui-ci n'est pas intégré dans votre ordinateur
- En cas de déplacements fréquents ou de travail chez un client, recouvrez votre écran d'un filtre de confidentialité.
- Evitez au maximum de vous connecter aux Wi-fi publics ou inconnus (y compris ceux des clients). Privilégier le partage de connexion avec votre téléphone (sécurisez le partage de connexion avec un mot de passe). Si vous devez vous connecter malgré tout à un réseau externe, utilisez un VPN pour sécuriser votre connexion. Ne réalisez aucune opération impliquant des informations sensibles (paiement par carte bancaire, renseignement d'informations confidentielles, etc) lors de votre connexion.
- Utilisez un anti-virus et réalisez les mises à jour dès que celles-ci vous sont proposées.
- Paramétrez votre pare-feu afin de limiter les connexions non désirées.
- Bannissez l'usage de clés USB

La sensibilisation s'applique à tous, même aux experts-comptables eux-mêmes !

La première cause de réussite d'une attaque informatique est l'erreur humaine. Elle en représente même 80%, bien loin devant un matériel technique défaillant. Or la sécurité informatique doit s'ajuster sur son maillon le plus faible.

Par ailleurs, une année calendaire représente 7 années technologiques.

Ainsi, face à des techniques en constante évolution, qui se professionnalisent, il est indispensable de former régulièrement les utilisateurs. Une actualisation des connaissances est recommandée au moins annuellement.

Formez également votre personnel aux attaques les plus ciblées dans le domaine de l'expertise comptable :

- L'hameçonnage (« Phishing »)
- Le FOVI (Faux Ordre de Virement International)
- La fraude au faux fournisseur

Consultez les formations proposées par ECF en la matière.

4 - SENSIBILISEZ REGULIEREMENT

5 - LISTEZ ET CLASSIFIEZ VOS ACTIFS...

En matière de sécurité des systèmes d'information, tout n'est pas à traiter de la même manière.

Identifiez vos actifs : FEC, données figurant dans votre gestionnaire de mot de passe, matériel informatique, etc

Et classez-les selon le niveau d'importance que vous leur accordez: Elevé, Moyen, Faible

6 - ...ET SAUVEGARDEZ-LES

L'heure est aujourd'hui à la résilience: la question n'est plus de savoir si cela arrivera, ni quand cela arrivera, mais plutôt de savoir comment continuer à travailler lorsque cela arrivera.

Définissez une politique de sauvegarde : adaptez le support de sauvegarde et la fréquence de celles-ci selon le niveau de classification précédemment établi. Veillez à la retranscrire dans votre manuel de procédures, et à former les collaborateurs concernés aux manipulations nécessaires si celles-ci ne sont pas automatiques.

- Sauvegarde mensuelle, hebdomadaire, journalière
- Sauvegarde en ligne, déconnectée, redondance ou non

En matière de sauvegarde, la règle d'usage est celle du 3, 2, 1: 3 sauvegardes, sur 2 supports différents, dont 1 hors site (c'est-à-dire déconnecté: celui-ci doit en outre être chiffré). Cette règle vaut en particulier pour les actifs d'importance élevée et peut être adaptée pour les autres actifs.

Veillez à ne pas oublier de tester la restauration des sauvegardes. A défaut, toutes les dispositions prises précédemment pourraient n'être d'aucune utilité.

7 - CHOISISSEZ VOS PRESTATAIRES AVEC SOIN

Autant que possible, privilégiez des prestataires français, hébergés en France.

Analysez scrupuleusement leurs engagements en matière de sauvegarde des données, et de réversibilité. N'oubliez pas que face au client, c'est le cabinet d'expertise comptable qui sera tenu pour responsable en cas de perte de données ou d'indisponibilité de service qui empêche la bonne réalisation des prestations mentionnées dans la lettre de mission (notamment déclaratives).

Le label «SecNumCloud» de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) qualifie les prestataires de services d'informatique en cloud, que ce soit pour des offres SaaS (Software as a Service), PaaS (Plateform as a Service) ou encore IaaS (Infrastructure as a Service). Cette qualification atteste de la qualité et de la robustesse de la prestation, de la compétence du prestataire ainsi que de la confiance pouvant lui être accordée notamment en matière de sécurité face aux lois extra-européennes.

8 - ANTICIPEZ LA GESTION DE CRISE

Le risque 0 n'existe pas, et la sécurité à 100% non plus. Aussi, il est primordial d'anticiper la crise afin de préparer en amont tout ce qui peut l'être. La rédaction d'un Plan de Continuité d'Activité, « PCA », assure une poursuite de l'activité en mode dégradé.

Le Plan de Reprise d'Activité, « PRA », permet la remédiation une fois la crise passée.

Ces deux éléments doivent prévoir des scénarii plausibles (ex: Perte d'accès au logiciel de production, indisponibilité de la connexion Internet, etc) qui conduiront à prendre les décisions adéquates pour minimiser au maximum l'impact de leur survenance (redondance sur les actifs utiles, redondance de la connexion Internet).

Ces plans nécessitent d'être consignés par écrit et surtout testés en amont de leur utilisation. La mise en situation est primordiale car elle permet d'atténuer fortement l'effet de surprise et l'inconnu.

9 - SÉCURISEZ VOS ÉCHANGES AVEC LES CLIENTS

Distinguez les données confidentielles des données personnelles qui rentrent elles dans la règlementation du RGPD. A cet égard, toutes les informations relatives aux éléments de paie sont concernées, et celles-ci doivent transiter autant que possible via des messageries sécurisées et des coffres-forts électroniques.

Concernant les éléments financiers, l'envoi par un lien ayant une durée de vie limitée est toujours préférable au mail contenant une pièce-jointe. Privilégiez également les espaces de dépôts sécurisés proposés par vos outils.

10 - COMMUNIQUEZ SUR VOTRE ENGAGEMENT CYBER

Faîtes valoir votre cybersécurité! Communiquez auprès de votre personnel et auprès de vos clients sur vos avancées, l'obtention de labels etc.

Le niveau de sécurité des partenaires est aujourd'hui une exigence client de plus en plus présente. C'est un outil marketing à ne pas négliger.