Qontrol

2023

RAPPORT D'ENQUÊTE

La facture électronique : une porte vers la cybersécurité

EN PARTENARIAT AVEC : WELYB AG2R LA MONDIALE ACN Alliance pour la confiance numérique

Les coût des attaques Cyber en France a été estimé à 2 milliards d'euros (étude Astères 2022). 95% des attaques réussies concernent les PME. Les cabinets d'expertise comptable en particulier font face à des défis majeurs, comme la gestion de données sensibles et la transition vers la facturation électronique.

Face à cette montée des menaces, ce sont désormais les exigences accrues de vos clients qui deviennent le véritable moteur du changement. Ils attendent une protection optimale de leurs données, faisant de la cybersécurité une priorité incontournable pour les cabinets d'expertise comptable.

C'est pourquoi nous avons mené cette enquête dont nous vous présentons ici les résultats, accompagnés d'un guide des bonnes pratiques.

Nous espérons que vous trouverez ces informations utiles et pourrez les mettre en œuvre pour apporter des améliorations concrètes à votre pratique.

Nous avons adopté une approche multi-dimensionnelle, combinant une enquête auprès de 182 experts comptables, des données de sources gouvernementales comme le CERT-FR et l'ANSSI, des normes comme l'AICPA et ISO/IEC 27001, ainsi que nos propres modèles destinés aux petites structures, y compris celle du 'Passport Cybersécurité' Qontrol.

Charlotte Creachcadec
Expert-comptable
Référente Cyber TPE/PME

Mathieu Le Bihan
Spécialiste en cybersécurité
Qontrol

Enquête réalisée en partenariat avec :

WELYB

Welyb fournit aux experts-comptables un portail à l'image du cabinet ainsi qu'une GED interconnectée et collaborative pour simplifier les échanges clients.

ACN
Alliance pour la confiance numérique

L'Alliance pour la Confiance Numérique (ACN) représente les entreprises (leaders mondiaux, PME/ TPE, et ETI) du secteur de la Confiance Numérique, soit celles de l'identité numérique, de la cybersécurité et de l'IA de confiance.

AG2R LA MONDIALE

Spécialiste de la protection sociale et patrimoniale en France, AG2R LA MONDIALE assure les particuliers, les entreprises et les branches, pour protéger la santé, sécuriser le patrimoine et les revenus, prémunir contre les accidents de la vie et préparer la retraite.

Des menaces en pleine évolution

Les menaces cyber évoluent constamment : à mesure que de nouvelles vulnérabilités sont découvertes, les cybercriminels ajustent leurs tactiques. Il est donc essentiel de rester informé des risques, et des modes d'opération.

Il ne s'agit plus de sécuriser uniquement les systèmes internes de l'entreprise, mais bien de prendre en compte l'ensemble de la chaîne de prestataires que les experts-comptables utilisent, tout en reconnaissant qu'ils font également partie de cette chaîne vis-à-vis de leurs clients. En France, 24% des menaces proviennent de ces "supply-chain attacks".

À l'ère des deep fakes et de l'IA, les attaques sont désormais plus automatisées et apparaissent plus convaincantes. Avec les progrès fulgurants de ces technologies, le problème ne fera qu'empirer.

Attaques basées sur l'identité

Ces attaques exploitent des identités compromises pour accéder à des systèmes, rendant leur détection difficile. Mondialement, 80% de toutes les violations de données utilisent des identités compromises et peuvent prendre jusqu'à 250 jours à identifier.

Malware / Rançongiciels

Malware désigne tout logiciel conçu pour infiltrer ou endommager un système informatique. Les «Rançongiciels» sont des malwares qui chiffrent les fichiers et bloquent l'accès au système. Les cybercriminels exigent ensuite une rançon pour restaurer l'accès.

Menaces internes

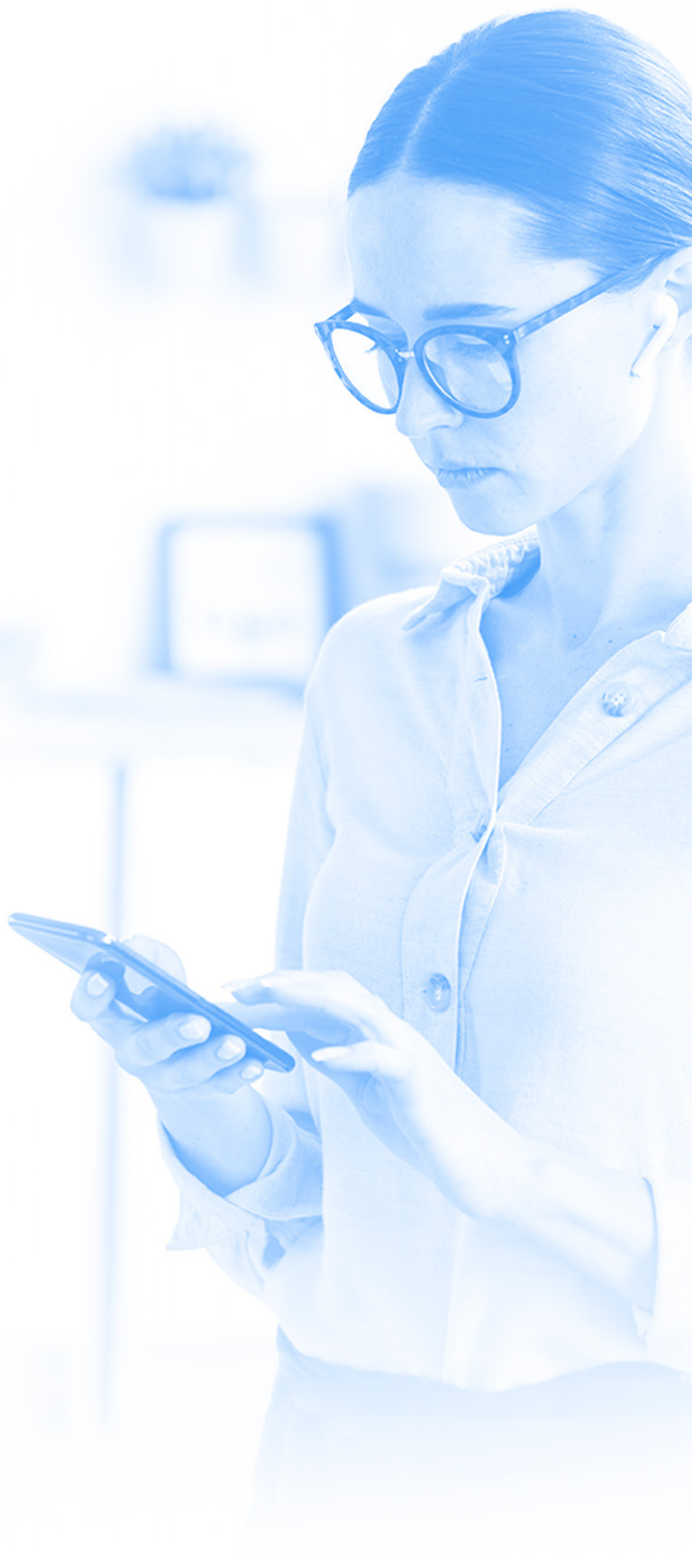
Risques posés par des employés ou partenaires qui abusent de leur accès aux systèmes. Les menaces peuvent être malveillantes ou simplement dues à de la négligence, souvent en raison d'un manque de formation.

Phishing & smishing

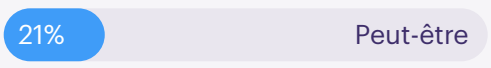
Une attaque par courrier électronique ("phishing"), et de plus en plus par SMS ("smsishing), visant à tromper l'utilisateur pour obtenir des informations sensibles, comme des mots de passe ou des données bancaires.

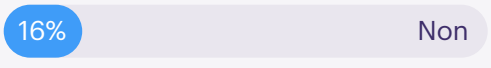
La facturation électronique au coeur de cette évolution

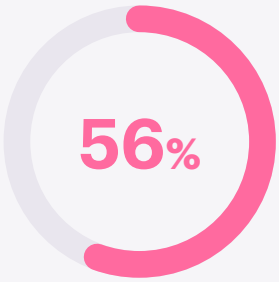
La transition vers la Facturation Electronique n'est pas seulement une évolution inévitable, mais elle représente également une opportunité en termes de cybersécurité pour les Experts Comptables : elle optimise la traçabilité et sécurise les échanges de données. Cependant, le virage numérique ouvre aussi la porte à de nouvelles cybermenaces, telles que le phishing et les rançongiciels. Par conséquent, vigilance et adaptation sont de mise. Il est intéressant de noter que les experts-comptables sont conscients de cette évolution, avec près de deux tiers des répondants à notre enquête estimant que la Facturation Electronique incitera les cabinets d'expertise comptable à renforcer leurs compétences en matière de cybersécurité.



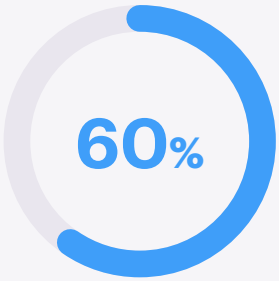
La facture électronique va-t-elle inciter les cabinets à améliorer leurs compétences en cybersécurité ?







des cabinets n'utilisent aucun gestionnaire de mots de passe



des cyberattaques ont un impact majeur sur les opérations commerciales des entreprises.

Mieux gérer les secrets

Alors qu'une seule faille de mot de passe peut causer de réels dégâts, la sécurisation de ces secrets s'impose comme une priorité.

Étonnamment, notre enquête révèle que seulement 27% utilisent systématiquement des outils de gestion des mots de passe. Plus inquiétant encore, la majorité (56%) des cabinets n'utilisent aucun outil de ce genre. Cela inclut donc la gestion des accès aux ERP ou outils comptables de leurs clients. C'est une négligence qui peut coûter cher et mettre en danger les clients des cabinets en cas de vol de mots de passe.

Selon un rapport de CESIN, 60% des cyberattaques ont un impact majeur sur les opérations commerciales des entreprises. Les types de dommages les plus fréquemment rencontrés incluent le vol de données (35%), l'usurpation d'identité (33%), et les données chiffrées par rançongiciel (22%).

Sans même parler de l'impact médiatique qui peut ternir irrémédiablement la réputation d'une entreprise sur le long terme.

Contrairement aux idées reçues, la cybersécurité n'exige pas forcément de gros moyens financiers.
Une sensibilisation annuelle de l'ensemble du personnel, un manuel des procédures à jour, une charte informatique et un gestionnaire de mots de passe constituent déjà un excellent point de départ, et ce, avec un budget très limité.

Charlotte Creachcadec
Expert-comptable
Référente Cyber TPE/PME

Sensibiliser et former

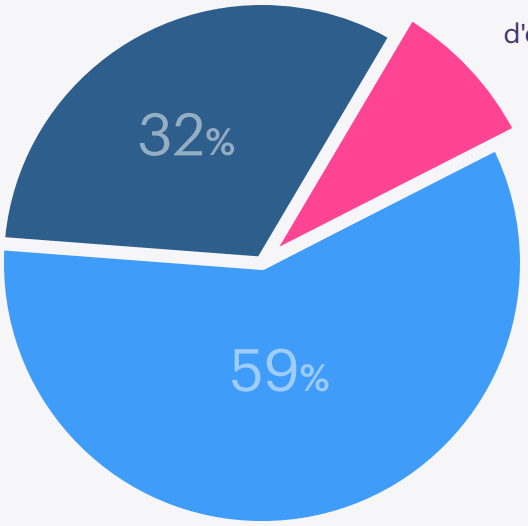
La première ligne de défense contre les cybermenaces, en particulier en ce qui concerne la gestion des mots de passe et des accès logiciels, est la formation des employés.

Selon notre enquête, 59% des cabinets d'experts comptables ont intégré des formations sur la gestion des accès et des mots de passe.

Toutefois, seuls 9% d'entre eux offrent une formation continue, et au-delà de la période d'intégration.

Ce manque de formation continue peut accroître significativement le risque de failles de sécurité en raison d'une négligence ou d'un défaut de mise à jour des compétences en matière de gestion des accès.

Est-ce que votre cabinet vous sensibilise à la gestion de vos accès en ligne ?



- Aucune sensibilisation
- Ont inclu une forme de sensibilisation
- Sensibilisations régulières

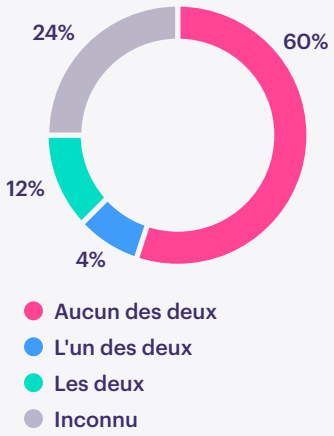
seuls **9%** d'entre eux offrent une formation continue

Plans de continuité et de reprise d'activité : Un maillon faible

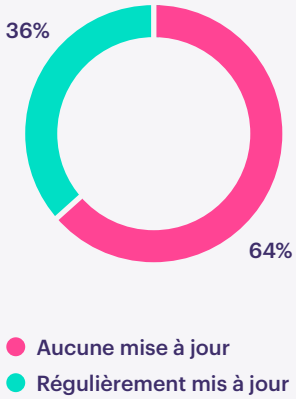
Lors d'incidents de sécurité, disposer d'un Plan de Continuité d'Activité (PCA) et d'un Plan de Reprise d'Activité (PRA) est crucial. Le PCA vise à assurer la continuité des opérations critiques en cas d'incident, tandis que le PRA est conçu pour récupérer les systèmes et les données après une catastrophe.

Nos résultats montrent que seulement 12% des cabinets d'expertise comptable interrogés déclarent avoir à la fois un PCA et un PRA en place. Plus surprenant encore, 60% des cabinets n'ont ni l'un ni l'autre.

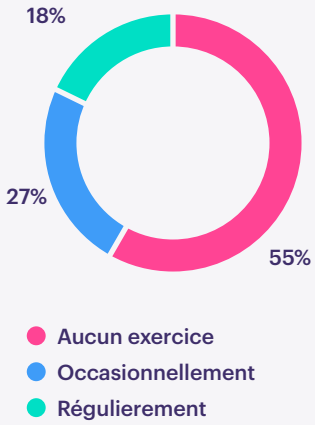
Votre cabinet a-t-il un PCA et un PRA en place ?



Si oui, ces plans sont-ils régulièrement mis à jour ?



Avez vous réalisé des exercises de mise en œuvre de ces plans ?



Soyons proactifs, et non réactifs. Un PCA/PRA robuste peut être la différence entre un petit contretemps et une crise majeure.

Mathieu Le Bihan
Spécialiste en cybersécurité Qontrol

Le nomadisme dans le collimateur

Le travail à distance ou en situation de nomadisme présente un ensemble de risques spécifiques.

Un danger souvent sous-estimé est le de vol d'appareil. Chiffrer les disques durs et utiliser un verrouillage de session sont des mesures essentielles pour sécuriser vos données en cas de perte ou de vol dans un espace public.

De plus, l'utilisation de Wi-Fi publics non sécurisés expose les travailleurs nomades à des risques de «man-in-the-middle» qui peuvent compromettre leurs données et leur vie privée.

Les cybercriminels sont très organisés et le marché du vol de données est lucratif, rendant ces formes d'attaques d'autant plus fréquentes et sophistiquées.

Notre enquête révèle que plus des trois quarts des experts comptable n'ont pas bénéficié d'une formation approfondie sur les bonnes pratiques en matière de travail à distance sécurisé. De plus, 69% n'utilisent pas de filtres de confidentialité pour protéger les écrans contre les regards indiscrets. En revanche, le fait qu'une majorité utilise un VPN pour sécuriser leur connexion montre une certaine prise de conscience des risques associés, bien que 44% ne prennent pas encore cette précaution.

Ce manque de mesures de sécurité peut considérablement augmenter la vulnérabilité aux cyberattaques dans des environnements de travail déjà risqués.

8 cabinets sur 10

ne proposent pas de formation sur les mesures de sécurité lors de nomadisme

7 collaborateurs sur 10

n'utilisent pas de filtre de confidentialité lors de travail réalisé dans un cadre de nomadisme

4 collaborateurs sur 10

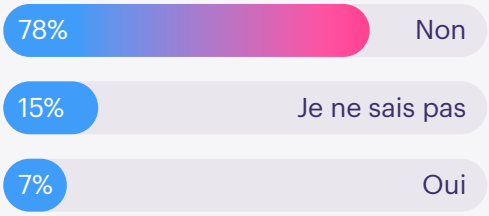
n'utilisent pas de VPN lors de déplacement professionnels

Conformité au RGPD et sécurité en facturation électronique

La facturation électronique, bien qu'efficace, pose des questions cruciales de sécurité et de conformité au RGPD. En effet, tout manque expose les entreprises à des risques accrus de cyberattaques et à des sanctions réglementaires. Il est donc vital d'intégrer des pratiques sécurisées et conformes aux standards.

Malgré ces enjeux, notre enquête révèle un manque de préparation au RGPD. Seuls 4% des cabinets d'expertise comptable interrogés ont affirmé avoir mis en place des procédures spécifiques pour garantir cette conformité dans le cadre de la facturation électronique.

Votre cabinet a-t-il mis en place des procédures spécifiques pour assurer la conformité avec le RGPD dans le cadre de la facturation électronique ?



> *Auparavant, la cybersécurité était souvent perçue comme une chasse gardée pour les techniciens informatiques.*
>
> *Mais soulignons le triptyque gagnant dans ce domaine : une alchimie entre la technique, les procédures et l'élément humain.*
>
> *Aujourd'hui, la prise de conscience de cette dimension plus globale la rend plus accessible. De plus en plus d'experts-comptables s'y intéressent, il faut poursuivre dans cette voie pour se l'approprier pleinement.*

Charlotte Creachcadec
Expert-comptable
Référente Cyber TPE/PME

Au terme de notre enquête, nous notons plusieurs domaines d'amélioration pour les cabinets d'expertise comptable.

Le mot d'ordre est l'adaptabilité, soutenue par une formation continue et une prise de conscience collective. La sécurité numérique n'est pas simplement une case à cocher ; c'est un processus continu qui demande une vigilance et une adaptation régulières.

C'est pourquoi nous avons inclus, dans la page suivante de ce rapport, un guide des bonnes pratiques à adopter pour protéger efficacement votre cabinet et vos clients.

Il s'agit de transformer la cybersécurité d'une préoccupation en un véritable atout pour votre cabinet.

Nous tenons à remercier sincèrement tous les participants à cette enquête ainsi que nos partenaires pour leurs contributions précieuses. Ces informations, nous l'espérons, serviront de catalyseur pour un changement positif dans votre métier, et contribueront à une meilleure protection contre les menaces cyber.

Guide des bonnes pratiques

Il est temps de passer à l'action ! Renforcez votre sécurité numérique en suivant le guide :

Gestion des Mots de Passe

Un bon gestionnaire de mots de passe, c'est comme un coffre-fort numérique. Vous y mettez tous vos trésors, et lui, il les garde en sécurité. Ça vaut le coup, vous ne trouvez pas ?

- **Mots de passe uniques pour chaque service.**
- **Utilisation de mots de passe forts et complexes avec la génération aléatoire.**
- **S'aider d'un gestionnaire de mots de passe reconnu (1password, Bitwarden, Lockpass, etc.)**
- **Mise en place d'une double authentification sur les outils (SaaS, outillage interne, etc.)**

Formation en Cybersécurité

Hey, vous savez quoi ? La cybersécurité évolue tout le temps ! Alors, que diriez-vous de pimenter un peu vos journées avec des formations continues ? C'est le moyen idéal de rester à la page et de ne pas se faire prendre au dépourvu.

- **Sessions trimestrielles de formation.**
- **Modules en ligne pour un apprentissage autonome.**
- **Campagne de faux-phishing.**

Conformité RGPD

Le RGPD, ça vous parle ? Si ça vous semble compliqué, pas de panique. C'est comme un "guide" un peu juridique de bonnes pratiques pour traiter les données personnelles comme il se doit.

- **Etablir un registre de traitement (RGPD).**
- **Politiques de rétention de données clairement définies (rédaction correcte de la politique de confidentialité).**
- **Formations spécifiques sur le RGPD.**

Sécurité en Nomadisme

Vous êtes souvent en déplacement ? Pas de souci, mais ne négligez pas la sécurité ! Un VPN et un peu de bon sens peuvent vous sauver la mise. Après tout, qui voudrait que ses données se promènent sur un Wi-Fi public ?

- **Chiffrement des ordinateurs portables.**
- **Filtre de confidentialité en déplacement.**
- **Formation sur les risques liés au Wi-Fi public.**
- **VPN obligatoire pour toutes les connexions externes.**

Confidentialité & sauvegardes

Chut... On a tous des secrets, n'est-ce pas ? Et dans le boulot, certains doivent vraiment le rester. Alors, pourquoi ne pas veiller à ce que les données restent là où elles doivent être : entre vous et votre écran.

- **Chiffrement des données en transit et au repos notamment des sauvegardes.**
- **Régularité des sauvegardes et tests de rejeu pour garantir leur fiabilité.**
- **Respect du principe du "moindre privilège" avec la mise en place d'une sécurité basée sur les rôles.**

Traitement des incidents

Oups, un petit incident de sécurité ? Pas de panique, ça arrive même aux meilleurs ! L'important, c'est d'avoir un plan en place pour y faire face. Pensez-y comme à un exercice d'évacuation incendie : c'est beaucoup moins stressant quand on sait quoi faire, où aller, et qui appeler. Donc, prenez le temps de rédiger une fiche pratique de traitement d'incident pour vous guider le jour J !

Qontrol

Qontrol est le premier assistant virtuel en cybersécurité pour les petites structures qui ne demande aucune connaissance technique, parfaitement adapté aux Cabinets d'Expertise Comptable.

Audit et roadmap sur mesure
Les mesures de sécurité qui vous conviennent

Accompagnement total
Prise en charge dès les premières mesures

Gain de temps
Aucun besoin de recherche, laissez vous guider en toute simplicité

2 minutes par jour par employe
Mise en place des mesures, sensibilisation et formation

Passport Sécurité Qontrol
Affichez fièrement votre conformité et vos engagements

PIERRE-HENRI TRANCART
VP Business development & Partner

ph@qontrol.io
+33 (0) 6 08 77 83 60