Expert-Comptable : protégez votre cabinet des cyber-attaques

DBC

Assure votre **Indépendance**
Accélère votre **Digitalisation**

SOMMAIRE

Table des matières

1. Définition de la cyber-attaque

Une cyber-attaque est une attaque malveillante sur un Système informatique.

Elle cible différents dispositifs informatiques : ordinateurs ou serveurs, isolés ou en réseau, connectés ou non à Internet, des périphériques tels que des imprimantes, et même des dispositifs de communication tels que des téléphones portables, smartphones, ou tablettes.

Il existe quatre types de cyber-risques aux conséquences différentes qui touchent directement ou indirectement les individus, les gouvernements et les entreprises : la cybercriminalité, la corruption d'image, l'espionnage et le sabotage.

Quelques chiffres

60% des PME victimes d'une attaque informatique déposent le bilan dans les 3 ans

54% **des entreprises françaises** attaquées en 2021

50 % **des entreprises victimes** portent plainte, les statistiques sont donc sous estimées

50 000€ coût médian d'une cyberattaque

+255% **d'attaques** par ransomware (entre 2019 et 2020)

Sources : forbes, ANSI, CESIN, L'Usine Digitale, Stoik.io

- La cybercriminalité

Les attaques peuvent cibler des individus ainsi que des entreprises et des dirigeants. Leur but est d'obtenir des informations personnelles en vue de les exploiter ou de les revendre (données bancaires, identifiants de sites marchands, etc.). Le phishing et les ransomwares sont des exemples connus de comportements malveillants qui nuisent aux internautes. Mais quels sont les différents types d'attaques ?

Attaque par hameçonnage (« phishing »)

Le phishing est une technique malveillante qui consiste à usurper l'identité d'une personne physique ou morale. L'idée est d'obtenir des informations personnelles et des identifiants bancaires à des fins criminelles.

Les cybercriminels se « déguisent » en tiers de confiance (banques, autorités, fournisseurs d'accès, etc.) et diffusent des messages frauduleux ou contenant des pièces jointes piégées à un grand nombre de contacts. Le message invite les destinataires à mettre à jour leurs informations personnelles (généralement bancaires) sur un faux site internet vers lequel ils sont redirigés.

La liste comprend un grand nombre de contacts et augmente les chances qu'un des destinataires se sente ciblé par le message diffusé. Un clic le redirige vers un faux site qui prend généralement la même apparence visuelle que le site officiel, et qui collectera les informations saisies par l'utilisateur.

Ces informations sont alors mises à disposition du cybercriminel qui n'a plus qu'à faire usage des identifiants, mots de passe ou données bancaires récupérées.

Comment limiter les risques ?

- N'ayez pas une confiance spontanée dans le nom de l'expéditeur du message. Regardez systématiquement le format de l'adresse email en survolant le nom de l'expéditeur avec votre souris
- Interrogez-vous sur la pertinence de la sollicitation de ce contact : contexte, habitudes, contenu éditorial…
- Au moindre doute, n'hésitez pas à contacter l'expéditeur par un autre biais (téléphone, sms…)
- Méfiez-vous des pièces jointes, elles pourraient être contaminées. Au moindre doute, n'hésitez pas à contacter l'expéditeur pour en connaître la teneur.
- Ne répondez jamais à une demande d'informations confidentielles par messagerie.

Attaque par rançongiciel (« ransomware »)

Les rançongiciels sont des programmes informatiques malveillants de plus en plus répandus. L'objectif : crypter des données puis demander à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les décrypter.

Le cybercriminel diffuse un message qui contient des pièces jointes et / ou des liens piégés. Le corps du message contient un message correctement rédigé, parfois en français, qui demande de payer rapidement une facture par exemple.

En un clic, le logiciel est téléchargé sur l'ordinateur et commence à crypter les données personnelles : les documents bureautiques (.doc, .xls, .odf…etc), les photos, la musique, les vidéos…etc.

Les fichiers devenus inaccessibles, un message s'affiche pour réclamer le versement d'une rançon, payable en crypto-monnaies ou via une carte

prépayée, en échange de la clé de décryptage. Attention, rien n'indique que le décrypteur en question soit efficace !

Le cas d'In Extenso

Une cyber-attaque a paralysée une partie du système informatique d'In Extenso, un groupe spécialisé dans les services aux TPE et PME durant le week end du 10 avril 2021.

Cette cyber-attaque a été conduite avec un ransomware. Le groupe a précisé qu'aucune fuite de données n'a été détectée mais que, par mesure de sécurité, l'intégralité des systèmes d'information ont été arrêtés.

Comment limiter les risques ?

- Méfiez-vous des pièces jointes et des liens dans les messages dont la provenance est douteuse. Au moindre doute, n'hésitez pas à contacter l'expéditeur pour en connaître la teneur.
- Effectuez des sauvegardes de vos données régulièrement sur des périphériques externes.
- Mettez à jour régulièrement tous vos systèmes et principaux logiciels en privilégiant leur mise à jour automatique.
- Ne répondez jamais à une demande d'informations confidentielles par messagerie.

- L'attaque à l'image

Lancées à des fins de déstabilisation contre des administrations et des entreprises et régulièrement relayées par les réseaux sociaux, les attaques à l'image sont aujourd'hui fréquentes et généralement peu sophistiquées, faisant appel à des outils et des services disponibles en ligne. De l'exfiltration de données personnelles à l'exploitation de vulnérabilité, elles portent atteinte à l'image de la

victime en remplaçant le contenu par des revendications politiques, religieuses, etc.

Attaque par déni de service (DDoS)

Le déni de service peut porter atteinte à l'image de la victime et constitue une menace pour toute organisation disposant d'un système d'information en ligne.
L'objectif : rendre un site, et donc le service attendu, indisponible. Les motivations des attaquants sont diverses, allant des revendications idéologiques à la vengeance, en passant par les extorsions de fonds.

Le cybercriminel peut :

- exploiter une vulnérabilité logicielle ou matérielle (faille Windows)
- solliciter une ressource particulière du système d'information de la cible, jusqu'à « épuisement ». Cette ressource peut être la bande passante du réseau, la capacité de traitement globale d'une base de données, la puissance de calcul des processeurs, l'espace disque, etc.

Plusieurs indices révèlent une attaque DDoS : accroissement de la consommation de la bande passante sans explication légitime, allongement des files d'attente des serveurs de messagerie ou retards dans le temps de transit des messages, des ruptures de communications (« timeout », « host unreachable »), etc.

Plusieurs méthodes pour un résultat unique : dysfonctionnement ou paralysie complète d'un ou de plusieurs services de la victime.

Attaque par « défiguration » (« defacement »)

Généralement revendiqué par des hacktivistes, ce type d'attaque peut être réalisé à des fins politiques ou idéologiques, ou à des fins de défi technique (défis entre attaquants). L'objectif : modifier l'apparence ou le contenu d'un site, et donc altérer l'intégrité des pages.
Le cybercriminel exploite souvent des vulnérabilités connues (défaut de sécurité), mais non corrigées du site. Visible ou bien plus discrète pour le visiteur, l'atteinte réussie du site peut prendre différentes formes : ajout d'informations sur une page ou remplacement intégral d'une page par une revendication.

Comment limiter les risques ?

- Effectuez des sauvegardes régulières.
- Respectez toutes les étapes lors de la procédure d'installation de votre site afin de supprimer manuellement des éléments temporaires générés au moment de l'installation (exemple : mots de passe par défaut).
- Utilisez des mots de passe d'accès aux interfaces d'administration complexes et régulièrement renouvelés.
- Gérez les droits d'accès pour chaque répertoire de votre site.
- Appliquez les correctifs de sécurité régulièrement : mise à jour des éléments du site, ajouts limités de nouveaux modules non vitaux du site, etc.
- Assurez-vous de la mise en place d'une politique de sécurité efficace si votre site est hébergé chez un prestataire, surtout dans le cadre d'un hébergement mutualisé (plusieurs sites hébergés).

- L'espionnage

Très ciblées et sophistiquées, les attaques utilisées pour l'espionnage à des fins économiques ou scientifiques sont souvent le fait de groupes structurés et peuvent avoir de lourdes conséquences pour les intérêts nationaux. De fait, il faut parfois des années à une organisation pour s'apercevoir qu'elle a été victime d'espionnage, l'objectif de l'attaquant étant de maintenir discrètement son accès le plus longtemps possible afin de capter l'information stratégique en temps voulu.

Attaque par point d'eau (Watering Hole)

La technique du « point d'eau » consiste à piéger un site en ligne afin d'infecter les équipements des visiteurs du secteur d'activité visé par l'attaquant. Le site en question peut être :

- Un site légitime piégé de manière totalement invisible pour les internautes. Le cybercriminel exploite une vulnérabilité du site et y dépose un virus (« malware »).
- Un site créé de toute pièce pour piéger les utilisateurs ciblés, dans le cas d'attaques d'états par exemple.

Le site qui sert d'appât est choisi spécifiquement pour attirer la victime ciblée par l'attaque in fine.

Objectif : infiltrer discrètement les ordinateurs de personnels œuvrant dans un secteur d'activité ou dans une organisation ciblée afin de récupérer des données.

La victime ciblée est incitée à se rendre ou est redirigée automatiquement sur le site contaminé. Son navigateur exécute alors le malware et l'installe à son insu sur ses appareils (ordinateur, téléphone). Le cybercriminel dispose alors d'un accès total ou partiel à l'appareil infecté.

Le cybercriminel demeure discret afin de capter le plus longtemps possible des données.

Attaque par hameçonnage ciblé (Spearphishing)

Cette attaque repose généralement sur une usurpation de l'identité de l'expéditeur, et procède par ingénierie sociale forte afin d'obtenir un message très crédible : l'objet et/ou le corps du message contient des informations précises, en lien direct avec l'activité de la personne ou de l'organisation ciblée.
L'ingénierie sociale forte suppose que le ou les hackers aient échangés directement avec la victime ou aient collecté des informations précises sur elle, en particulier sur les réseaux sociaux.

Objectif : infiltrer le système d'information d'une organisation d'un secteur d'activité ciblé.

1. Le cybercriminel, via un email, usurpe l'identité d'une personne morale (établissement financier, service public, concurrent…) ou d'une personne physique (collègue de travail, famille, ami…).

2. Phase de contamination : le destinataire est invité à ouvrir une pièce jointe malveillante ou à suivre un lien vers un site malveillant (phishing). Une première machine est ainsi contaminée.

3. Phase d'infiltration : le cybercriminel en prend le contrôle pour naviguer dans le système d'information de l'organisation qui est la véritable cible.

4. « Escalade de privilège » : l'attaquant cherche à obtenir des droits « d'administrateur » pour pouvoir rebondir et s'implanter sur les postes de travail et les serveurs de l'organisation où sont stockées les informations visées (« propagation latérale »).

5. Phase d'exfiltration : l'attaquant vole le plus discrètement possible des données, soit en une seule fois, en profitant d'une période de moindre surveillance (la nuit, durant les vacances scolaires, lors d'un pont…), soit de manière progressive, plus insidieuse.

Il prend généralement soin de toujours effacer derrière lui toute trace de son activité malveillante.

Comment limiter les risques ?

- N'ayez pas une confiance spontanée dans le nom de l'expéditeur
- Soyez attentif à ce que vous publiez sur les réseaux sociaux et au périmètre de diffusion de ce que vous publiez
- Méfiez-vous des pièces jointes et des liens dans des messages dont la provenance est douteuse
- Mettez à jour régulièrement tous vos logiciels

- Le sabotage

Le sabotage informatique est le fait de rendre inopérant tout ou partie d'un système d'information d'une organisation via une attaque informatique.

Le sabotage s'apparente à une « panne organisée », frappant tout ou partie des systèmes, selon le type d'atteinte recherchée – désorganisation durable ou non, médiatisée ou non, plus ou moins coûteuse à réparer. Pour y parvenir, les moyens d'attaques sont d'autant plus nombreux que les organisations ne sont pas toujours préparées à faire face à des actes de malveillance.

Le sabotage et la destruction de systèmes informatiques peuvent avoir des conséquences dramatiques sur l'économie d'une organisation, sur la vie des personnes, voire sur le bon fonctionnement de la Nation s'ils touchent des secteurs d'activité clés.

2. Comment protéger son cabinet ?

Il existe à la fois des bonnes pratiques mais aussi des systèmes pour protéger son cabinet d'expertise comptable.

Nous vous proposons dans les paragraphes suivants une liste non-exhaustive et concrète vous permettant de limiter les risques, même si chacun sait que le risque zéro n'existe pas.

- Les bons réflexes et bonnes pratiques

Méfiez-vous des pièces jointes et des liens dans des messages dont la provenance est douteuse.

Dès le moindre doute sur l'authenticité d'un email, sur l'expéditeur ou sur l'adresse email de l'expéditeur, n'ouvrez pas celui-ci.

En cas d'ouverture du message, un phishing général ou ciblé (spearphishing) peut dans la grande majorité des cas être détecté grâce à des tournures de phrase, une orthographe, des formules de politesse, le tutoiement/vouvoiement, etc. ne correspond pas aux habitudes de l'expéditeur. Dans ce cas, vérifiez qu'il s'agit bien du bon expéditeur (en l'appelant au téléphone par exemple)

Si vous avez le moindre doute, n'ouvrez pas les pièces jointes et ne cliquez pas sur les liens qu'il peut contenir. **Rappelez-vous que la principale porte d'entrée d'une cyberattaque est un message piégé** (phishing ou spearphishing).

Effectuez régulièrement des sauvegardes

On ne le répète jamais assez mais il vaut mieux prévenir que guérir. Et pour cela, rien ne vaut la sauvegarde de vos données.

N'hésitez pas à innover en sauvegardant vos données sur le Cloud, après les avoir cryptées. A défaut, vous pouvez faire une sauvegarde sur un serveur ou un disque-dur externalisé. Attention, les sauvegardes sur des supports physiques comportent des risques d'altération ou perte de données en cas de dégradation ou vol de ce dernier, il est donc préférable de crypter toutes les sauvegardes,

même locales. De plus, si la sauvegarde est externalisée, le cryptage permet de respecter le RGPD sans équivoque.

Et n'oubliez pas qu'une sauvegarde ne vaut que si elle peut être remontée : vérifiez très régulièrement (tous les mois ou trimestre par exemple) que vous pouvez effectivement remonter vos sauvegardes internes, cloud ou externalisées physiquement.

Mettez à jour régulièrement tous vos logiciels

Les mises à jour de vos logiciels sont importantes pour la sécurité de votre cabinet. Que ce soit les logiciels métier, les logiciels bureautiques ou les petits logiciels annexes que nous avons tous sur nos ordinateurs (lecteur PDF, programme de compression/décompression de fichiers, …)

En effet, les éditeurs de logiciels identifient régulièrement des vulnérabilités dans le code de leur logiciel et y apportent des correctifs. Ces derniers permettent de vous protéger en limitant la vulnérabilité ou les portes d'entrée de certains hackeurs.

Utilisez des mots de passe complexes et régulièrement renouvelés pour l'accès aux interfaces d'administration. Activer idéalement la double authentification pour un degré de sécurité plus élevé.

La mise en place de mots de passe complexes et différents d'une utilisation à une autre est primordiale pour garantir un niveau de protection acceptable.

Gérez les droits d'accès pour chaque répertoire de votre site.

Pour limiter les risques, il est préférable de segmenter les droits d'accès des utilisateurs aux répertoires de votre serveur. Vous préserverez ce dernier d'intrusions pouvant mener à du sabotage ou de l'espionnage.

- Les pratiques techniques efficaces

Évitez les sauvegardes locales

Imaginez que le matériel de votre cabinet soit perdu, volé ou détruit lors d'un incendie. Comment ferez-vous ? Cette hypothèse banale est pourtant courante. Pour éviter les inconvénients, nous recommandons vivement toute sauvegarde sur le disque local de votre PC. Nous recommandons également d'éviter les sauvegardes sur les disques durs externes, pour les mêmes raisons. Si toutefois une sauvegarde sur disque dur externe est votre souhait, cryptez les données stockées et utilisez au moins deux disques en alternance pour vous prévenir ad minima de la panne d'un disque.

Sauvegardez vos données dans le Cloud

Optez pour une solution de sauvegarde cryptée de vos données dans le Cloud. Vous sécuriserez ainsi vos données même en cas de perte de vos matériels.

Privilégiez l'utilisation d'un bureau virtuel

Imaginez de pouvoir passer d'un ordinateur physique à un autre, voire à une tablette ou un smartphone, tout en retrouvant à chaque fois votre bureau et tout votre environnement de travail ! Ce n'est pas un rêve mais une réalité qui renforce votre mobilité. Nombreux sont les experts-comptables et les collaborateurs qui ont déjà recours à ce système qui permet de se déplacer en rendez-vous client ou de télétravailler sans contrainte et en toute sécurité.

Optez pour une gestion électronique des documents

Le nombre de cabinets d'expertise-comptable à utiliser une GED augmente de façon exponentielle car elle offre un nombre d'avantages considérable. En effet, une solution de GED en ligne permet de réduire les coûts (d'impression notamment) tout en maximisant la productivité : les documents sont disponibles à chaque instant, en tout lieu et par tous les collaborateurs concernés par tel ou tel type de document. Enfin, lorsque la GED est bien conçue, les documents sont accessibles sur tous les supports informatiques : tablettes, smartphones ou ordinateurs.

3. Découvrez comment DBC accompagne les cabinets

Pour sécuriser les cabinets d'expertise-comptable, DBC a développé deux solutions simples et performantes.

Extreme Mobility, une solution innovante et personnalisée d'hébergement dédié du système d'information du cabinet, basée sur la technologie de la virtualisation du poste de travail (VDI).

Quantum GED pour Expert-Comptable, une GED innovante de Gestion des flux entrants et sortants (workflow), de vos documents, pour votre relation client (Extranet Cabinet) et vos collaborateurs (Intranet).

EXTREME MOBILITY BY DBC

- L'hébergement infogéré pour expert-comptable

Votre poste de travail virtuel, accessible avec une simple connexion

Extreme Mobility, l'hébergement infogéré pour Expert-Comptable, apporte la mobilité complète aux collaborateurs du cabinet d'expertise comptable. Bénéficiez d'un poste de travail virtuel, disponible avec une simple connexion internet et connecté à tous vos outils.

Une gestion flexible des utilisateurs et de leurs droits

Bénéficiez d'une indépendance d'administration complète avec une gestion flexible des utilisateurs, de leurs droits, des plans d'archives et de sauvegardes. Avec Extreme Mobility, l'hébergement infogéré pour Expert-Comptable, le cabinet d'expertise comptable peut choisir les applications affectées à chaque collaborateur comptable. Le tout dans un strict respect du RGPD.

Sécurité et fiabilité de la plateforme DBC

DBC supervise la plateforme dédiée à chaque Cabinet-Comptable et en assure la sécurité et la pérennité. Chaque collaborateur comptable peut retrouver l'historique de ses documents individuels (versioning) afin de retrouver un fichier supprimé ou modifié par erreur. Extreme Mobility, l'hébergement infogéré pour Expert-Comptable, permet également la double authentification pour tout ou partie des collaborateurs.

QUANTUM DMS BY DBC

- GED pour expert-comptable

Avec Quantum GED pour Expert-Comptable, la récupération des documents est simplifiée

Quantum GED pour Expert-Comptable, vous offre la possibilité de simplifier la récupération des documents de vos clients et collaborateurs. Connectez vos outils et logiciels et récupérez ainsi tous vos documents, simplement.

Une gestion facilitée et un classement structuré des documents
Avec Quantum GED pour expert comptable, profitez d'une recherche intuitive et flexible par contenu et métadonnée. Bénéficiez de structures de dossiers flexibles, en personnalisant dynamiquement l'arborescence

Envie d'en savoir plus sur DBC ?

contact@digitalbc.fr

04 81 91 27 70

Assure votre **Indépendance**
Accélère votre **Digitalisation**