Alinto

Livre blanc

Novembre 2021

Messagerie professionnelle : comment protéger votre entreprise des cyberattaques ?

Sommaire

Resserrer les mailles du filet

Seule une entreprise sur deux se dit équipée et préparée pour faire face à une cyberattaque[1]. C'est un triste constat qui amène les organisations à repenser la sécurité de leur réseau IT, et plus particulièrement de leur messagerie professionnelle.

En effet, la majorité des attaques informatiques provient d'emails frauduleux. Et les techniques et technologies utilisées par les hackers sont de plus en plus sophistiquées. Ils ciblent dorénavant toutes les entreprises : de la TPE à la multinationale, en profitant de la faible sensibilisation des collaborateurs quant aux emails malveillants.

Les entreprises les plus vigilantes instaurent des mesures de sécurité strictes : pare-feu, patch, antispam… Néanmoins, ces protections, souvent liées aux solutions de réseau, système et messagerie en place, montrent des limites. Un email peut passer à travers les mailles du filet.

Dans ce Livre Blanc, nous faisons le point sur les cyberattaques, passons en revue les bonnes pratiques pour renforcer la sécurité de votre messagerie, et vous livrons nos conseils pour mieux protéger votre organisation.

[1] 6ème édition du baromètre annuel du CESIN

Sécurité de l'email : état des lieux

On ne le répètera jamais assez, **l'email est le canal privilégié des cyberattaques**. Et cela s'intensifie année après année, malgré l'amélioration de la sécurité des messageries personnelles et professionnelles, la sensibilisation des utilisateurs et la diffusion d'alertes aux phishing et aux cyberattaques. De leur côté, les cybercriminels utilisent des logiciels malveillants de plus en plus sophistiqués et leurs techniques sont plus abouties, pouvant donc prêter à confusion.

Ransomware, phishing, malware… sont autant de menaces pour les entreprises, qui doivent alors **redoubler de vigilance et sensibiliser leurs collaborateurs**. D'autant plus que les cybercriminels surfent sur la pandémie de Coronavirus, usant de la peur pour inciter au clic.

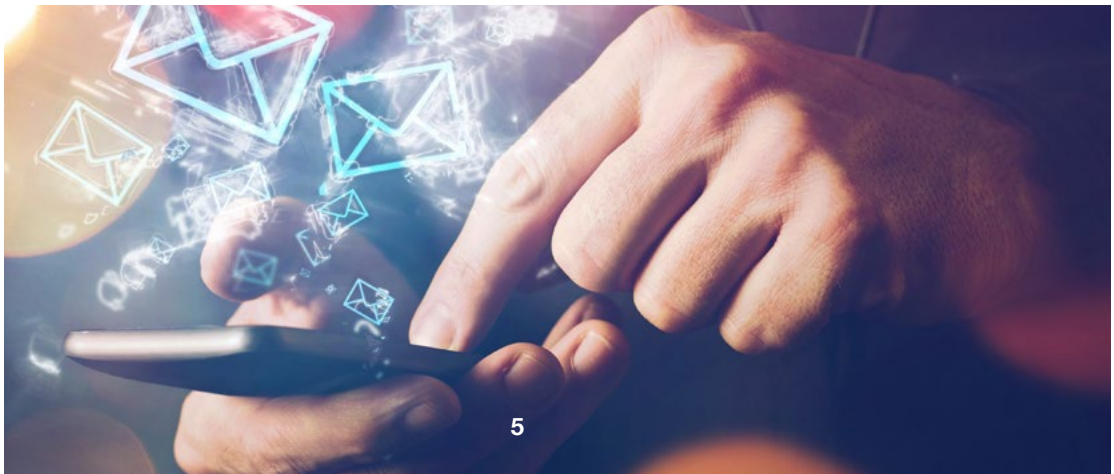
Pour y voir plus clair, nous vous proposons un état des lieux de la situation.

Cybersécurité : l'augmentation inquiétante des attaques par l'email

En 2020, les attaques informatiques ont quadruplé par rapport aux années précédentes[1]. Les cybercriminels sont aujourd'hui mieux organisés, envoient de nombreux emails frauduleux et ciblent les vulnérabilités dans les réseaux IT des entreprises. Les attaques sont industrialisées, planifiées. Nous sommes loin d'une personne qui agit seule derrière son ordinateur.

Voici quelques chiffres pour illustrer la situation actuelle et la vulnérabilité liée aux messageries en France :

- Les ransomwares représentent **11 % du volume total d'emails malveillants**[2].
- **80 % des entreprises françaises cyber-attaquées en 2020** l'ont été via des emails de phishing ou spear-phishing[3].
- En 2020, **une entreprise sur cinq déclare avoir subi au moins une attaque** par ransomware au cours de l'année.
- Seule **une entreprise sur deux est confiante** en sa capacité de faire face à une cyberattaque[5].
- La crise sanitaire apporte de nouveaux risques : **augmentation de 35 % des cyberattaques**[6].



- 57 % des entreprises prévoient d'augmenter leur budget dédié à la cybersécurité[7].

- **85 %** des entreprises souhaitent **acquérir de nouvelles solutions techniques** pour améliorer leur sécurité IT[8].

- **75 %** des emails reçus sont **indésirables**[9].

- Les **signalements au gouvernement** de cyberattaques de la part de professionnels ont augmenté de **30 %** par rapport en 2019[10].

Le développement du télétravail, la peur induite par la pandémie, le développement du cloud, la professionnalisation des attaques par email expliquent cette évolution. Rien n'indique un changement de tendance : le phénomène devrait se maintenir pour les années à venir et rester une véritable préoccupation pour les organisations.

Cyberattaques : des conséquences importantes pour les entreprises

Il est difficile d'estimer le coût d'une cyberattaque. Cela ne se traduit pas uniquement par des conséquences économiques, mais également par l'impact sur la réputation de l'entreprise, la fragilisation de l'infrastructure IT, ou encore des difficultés opérationnelles pour les différents métiers.

En 2020, **58 % des cyberattaques ont eu des conséquences avérées sur le business**, avec des perturbations directes sur la production dans 27 % des cas[11].

Les principales conséquences des attaques[12] se répartissent ainsi :

- Vol de données (**30 %**)
- Déni de service (**29 %**)
- Blocage de l'activité suite au chiffrage des données par un rançongiciel (**24 %**)
- Usurpation d'identité (**23 %**)

Une étude menée par le cabinet Bessé montre que le risque de défaillance d'une entreprise augmente de 50 % dans les trois mois qui suivent l'annonce de la cyberattaque. Ce risque atteint même parfois 80 %[13].

Une autre étude menée par IBM Ponemon Institute établit que 80 % des entreprises françaises n'ont pas de plan de réponse aux incidents. Autre chiffre significatif : il faut en moyenne **201 jours** à une entreprise pour découvrir qu'elle a été victime d'une cyberattaque. Les conséquences directes peuvent aussi toucher les clients si leurs données personnelles ont été volées.

Un simple clic anodin sur un lien dans un email peut donc fragiliser de façon irrémédiable l'ensemble de l'entreprise. C'est pourquoi il est important de continuer à sensibiliser les collaborateurs, mais aussi de renforcer la sécurité IT à travers différentes solutions dédiées **de protection** de la messagerie performantes.

---

[1] Cyberattaques : le nombre de piratages a quadruplé l'année dernière, selon un expert en cybersécurité - France TV info
[2] Intervention Devensys - Les méthodes pour améliorer votre sécurité mail 2018
[3] Les cyberattaques les plus courantes contre les entreprises françaises - Statista
[4 à 8] 6ème édition du baromètre annuel du CESIN
[9] Messagerie : chiffres et menaces - sécurité dsisionnel
[10] Cybersécurité : des signalements plus nombreux en 2020 - magazine vie-publique
[11] 6ème édition du baromètre annuel du CESIN
[12] Les cyberattaques les plus courantes contre les entreprises, CESIN et OpinionWay
[13] Sur un panel d'ETI

Quelques exemples de cyberattaques et de leurs conséquences :

- Un hôpital du New Jersey (USA) a payé une rançon de plus de **600 000 dollars** (2020).

- Verne Harnish, PDG de Gazelles inc. s'est fait voler **400 000 $** de son compte bancaire lorsque des pirates ont pu accéder à son ordinateur et intercepter des courriels entre lui et son adjoint (2019).

- EasyJet annonce avoir été victime d'une cyberattaque d'ampleur : plus de **9 millions de données de clients** (adresses email et information de voyage), dont 2 000 données de cartes bancaires ont été illégalement consultées (2020).

- L'Université de Californie à San Francisco (UCSF) a été touchée par un ransomware paralysant l'accès aux données de son réseau informatique. Finalement, l'Université s'est résolue à payer une rançon d'environ **un million d'euros** (2020).

Quatre bonnes pratiques pour éviter les cyberattaques liées au mail

La porte d'entrée privilégiée des hackers sur Internet est l'email. Et le développement massif du télétravail causé par la pandémie a accentué le nombre d'attaques, surtout par des ransomwares. En effet, le Club des experts de la sécurité de l'information et du numérique (Cesin) estime qu'en 2020, **57 % des entreprises ont été victimes d'une attaque informatique**. Un chiffre multiplié par quatre en un an.

Cependant, ce n'est pas une fatalité ! Il existe des solutions pour protéger votre entreprise. Cela passe par l'adoption de **plusieurs bonnes pratiques**, que nous vous livrons dans cet article.

Bonne pratique #1
Sensibiliser les collaborateurs

La première chose à faire est de communiquer auprès de vos équipes à propos des risques de cyberattaques et des conséquences qu'elles peuvent entraîner pour l'entreprise. Il s'agit donc d'expliquer comment reconnaître un email suspect et les différentes précautions à prendre pour sécuriser l'accès à leur messagerie. Vos collaborateurs seront ainsi incités à définir un mot de passe sécurisé, limiter l'envoi et l'ouverture de pièces jointes, ne pas cliquer sur des liens qui semblent suspects, ne pas divulguer d'informations confidentielles, contrôler l'identité de l'expéditeur...

Il est aussi important d'insister sur l'importance de **prévenir le service IT en cas de suspicion d'email frauduleux**. La réaction doit être rapide pour qu'il puisse déclencher la procédure adaptée, avant que le virus ne se propage et ne cause de dommages importants.

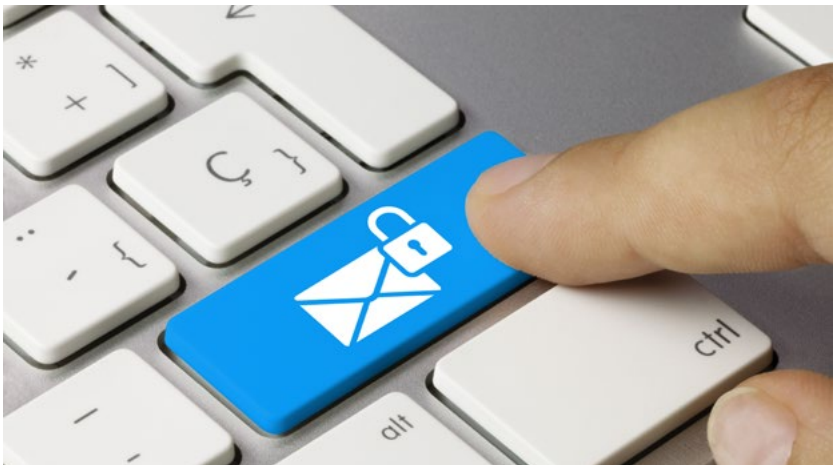
Bonne pratique #2
Sécuriser les données sensibles

Depuis l'entrée en vigueur du RGPD, les **enjeux liés à la cybersécurité** sont devenus encore plus stratégiques pour les entreprises. La sécurité d'accès au SI et aux informations personnelles doit être garantie.

Pour sécuriser les données, il est indispensable de mettre en place une **politique de gestion des mots de passe rigoureuse**. C'est le premier levier de sécurisation des postes de vos collaborateurs. Les mots de passe doivent être complexes, difficiles à deviner, confidentiels et renouvelés régulièrement.

Pour plus de sécurité, paramétrez les postes de vos collaborateurs de manière à ce qu'ils se verrouillent automatiquement au bout de quelques minutes d'inactivité. Il est aussi indispensable de protéger les fichiers qui comportent des données sensibles et de réserver leur accès aux personnes habilitées.

Toujours dans le but de sécuriser le SI, il est important de chiffrer les données sensibles telles que celles relatives à la santé, les informations de paiement… Toutes ces précautions sont indissociables d'une protection au niveau de l'infrastructure réseau avec l'installation de pares-feux, de routeurs filtrants, de sondes anti-intrusions, de système d'équilibre de charge et de détection d'attaques DDoS…

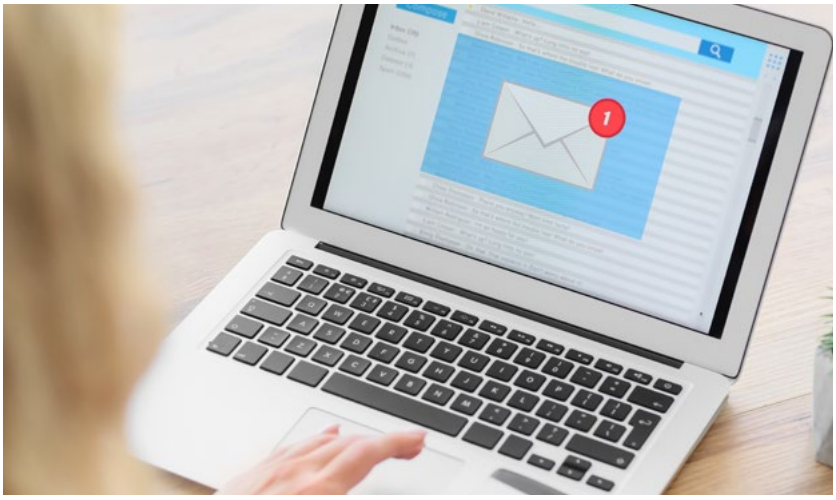


Bonne pratique #3
Garder le contrôle sur le trafic mail

L'email est toujours **le canal de communication le plus utilisé dans le monde**. Les utilisateurs en reçoivent des centaines par jour. C'est à la fois synonyme de stress, de perte d'efficacité, mais cela a aussi un impact non négligeable sur l'exposition à des risques de cyberattaques. Car, comme le montre notre état des lieux sur la sécurité de l'email, plus de **75 % des emails sont indésirables**.

C'est pourquoi le contrôle du trafic mail est primordial : il faut s'assurer que les mails frauduleux restent aux portes du SI de l'entreprise. Mais ce filtrage doit être fin et précis pour **ne pas éliminer des mails valides**, utiles aux collaborateurs.

C'est pourquoi il est important de mettre en place et **adapter en permanence les règles de filtrage**, de faire évoluer les listes blanches et noires, de placer les emails non frauduleux, mais soupçonnés d'être commerciaux dans une zone de quarantaine. Les utilisateurs pourront y avoir accès pour ne manquer aucune information importante.



Bonne pratique #4
Déployer une solution de sécurisation de l'email

Pour renforcer la sécurité de votre messagerie professionnelle, il est indispensable de déployer un logiciel de protection des emails (type antispam ou antivirus). Ces solutions sont mises à jour au fil de l'apparition de nouvelles cyberattaques. **Elles s'adaptent parfaitement aux différentes solutions de messagerie professionnelles** à commencer par Microsoft 365 Exchange. Ces outils filtrent les spams en vérifiant de multiples critères, mettent automatiquement certains expéditeurs en liste noire, protègent votre réputation (pour l'envoi massif d'emails…).

Les fournisseurs de solutions de messagerie proposent nativement des solutions antispam, mais elles ne suffisent pas toujours (voire rarement). Il est donc essentiel d'assurer **une protection renforcée grâce à des outils dédiés**, tels que Alinto Protect. Les avantages sont nombreux : protection de la messagerie, boîte de réception email plus propre, finesse de filtrage, gestion de quarantaine, gain de temps pour la gestion des emails…

Pour rappeler ces quatre recommandations essentielles, n'hésitez pas à **consigner l'ensemble des bonnes pratiques dans un document** à disposition de vos collaborateurs. La communication et la sensibilisation des équipes sont aussi essentielles pour une bonne protection de votre messagerie professionnelle.

Pourquoi les antispams intégrés des solutions de messagerie ne suffisent pas ?

De nombreuses entreprises utilisent les logiciels antispam proposés avec leurs solutions de messagerie. Elles ne voient pas l'intérêt d'opter pour une solution supplémentaire. Certaines n'en utilisent même pas ! C'est pourtant un réel enjeu pour les organisations. En effet, **l'email est la principale porte d'entrée des cyberattaques**.

Au-delà de la sensibilisation des salariés quant aux bonnes pratiques pour reconnaître un email frauduleux, il est important de renforcer la sécurité de votre messagerie professionnelle. Car bien souvent, l'antispam proposé par votre fournisseur n'est pas suffisant. Nous vous expliquons pourquoi.

Les antispams intégrés ne sont pas assez efficaces

Les antispams intégrés aux systèmes de messagerie filtrent les courriers indésirables grâce à des règles de filtrage générales et prédéfinies. Ces dernières sont difficilement administrables, peu adaptables aux besoins des utilisateurs et à l'apparition soudaine de nouvelles menaces. C'est donc une protection incomplète de la messagerie, qui bloque les emails venant des listes de spams, qui ont des objets ou des pièces jointes douteuses.

La preuve : en 2016, AV Comparatives a envoyé 127 800 spams à des comptes détenus auprès de fournisseurs de services de messagerie. Les taux de détection étaient très bas : **89,87 %** des spams sont arrivés à destination chez l'un des fournisseurs. Cela montre bien qu'il est important de ne pas se contenter des versions de base - en apparence gratuites, tout du moins sans coût additionnel - et de s'équiper d'une solution complémentaire plus performante.

Les versions plus puissantes sont très chères

Bien évidemment, les fournisseurs de messagerie proposent des versions renforcées et payantes de leurs logiciels antispam (comme Microsoft Advanced Threat Protection / Microsoft 365 Defender). Celles-ci proposent des fonctionnalités plus poussées. Par exemple, elles sont paramétrables par les administrateurs (affichage, modification, configuration). Il est également possible de **créer des règles personnalisées propres à chaque utilisateur**, qui primeront toujours sur les règles globales.

Ces versions proposent aussi des processus automatisés grâce à l'intelligence artificielle. Elles vont ainsi plus loin et identifient des campagnes commerciales qui échappent au filtrage de premier niveau. Des tableaux de bord sont également disponibles, pour analyser l'évolution du trafic mail et le nombre de spams, de courriers indésirables…

Cependant, ces solutions ont un prix assez conséquent et sont facturées sur la base du nombre d'utilisateurs. En moyenne, il faut compter **plusieurs dizaines d'Euros par mois et par utilisateur**. Faites le calcul selon vos effectifs : c'est un montant non négligeable pour les entreprises, qui préfèrent parfois s'en passer. C'est ainsi qu'elles laissent un champ plus libre aux cybercriminels.

Antispam : quel support vous offre votre fournisseur de messagerie ?

Les fournisseurs de messageries professionnelles populaires sont parfois victimes de leur succès. Revers de la médaille : leur support n'est pas facilement joignable ou disponible. Or, en cas d'incident, il est important d'avoir accès à un **support performant et réactif**. De plus, il est souvent nécessaire de passer par des intégrateurs pour déployer ces solutions, limitant les relations directes avec l'éditeur.

En faisant appel à un éditeur de solution antispam à taille humaine comme Alinto, vous mettez toutes les chances de votre côté pour bénéficier d'un partenaire réactif, accessible et conscient de vos problématiques. C'est un avantage non négligeable quand on connaît les conséquences d'une **indisponibilité de messagerie ou d'une cyberattaque**. Renseignez-vous bien avant de faire votre choix, car tous les prestataires ne proposent pas le même niveau d'accompagnement et de support.

Même si les grands fournisseurs de messagerie professionnelle proposent des antispams en standard, renforcer la sécurité des boîtes email de vos collaborateurs est indispensable. Et pour cela, un large éventail de solutions complémentaires s'offre à vous. Afin de faire le bon choix, définissez une liste de critères que vous jugez indispensables : accompagnement, fonctionnalité, ergonomie, proximité, bases tarifaires… N'oubliez pas : **c'est le logiciel qui s'adapte à vos enjeux et pas le contraire !**

Cinq fonctionnalités clés pour votre logiciel de sécurisation des e-mails

Vous en êtes convaincus : il vous faut une **protection supplémentaire de votre messagerie professionnelle**. Cependant, difficile de choisir dans le flot de solutions disponibles. Entre les antispams intégrés directement à la messagerie et les logiciels additionnels, votre cœur balance.

Selon nous, cinq fonctionnalités s'avèrent incontournables. Elles doivent absolument être proposées par votre futur fournisseur. Découvrez-les dans cet article.

Fonctionnalité #1
Le filtrage des emails entrants

Bien évidemment, votre futur logiciel de sécurisation de votre messagerie doit vous proposer un filtrage des emails entrants performants. Cela passe par plusieurs méthodes :

- **Filtrage des emails basé sur la réputation :** filtrage des spammeurs connus, interrogation des bases de données internationales de réputation...
- **Liste blanche (ou white list) :** choix des expéditeurs dont l'entreprise accepte les emails.
- **Liste noire (ou blacklist) :** liste des expéditeurs dont l'entreprise rejette les emails.
- **Analyse du contenu :** blocage d'un message en fonction du contenu (analyse des mots, de liens, d'images, de pièces jointes…).

Pour toujours plus d'agilité et d'adaptabilité, optez pour une solution qui permet de modifier, adapter, supprimer ou ajouter des filtres facilement, en quelques clics et selon les besoins de vos utilisateurs finaux.

Fonctionnalité #2
L'antispam et l'antivirus

En rapport avec la première fonctionnalité, il est bien sûr important de choisir une **solution de protection dotée d'un antispam et d'un antivirus performants**. En effet, si la première fonctionnalité permet de s'assurer de la légitimité de l'expéditeur, ce dernier peut à son insu envoyer un spam ou un virus. Dès lors, le message doit être analysé en profondeur. De nombreux emails indésirables réussissent à passer les antispams intégrés aux solutions de messagerie et se retrouvent dans les boîtes de réception de vos utilisateurs.

Optez pour une solution basée sur des technologies performantes, qui interroge les bases de données mutualisées internationales, profite également de ses propres bases de spam qui s'adapteront à la sémantique locale et soumet les emails à différents antivirus pour un **meilleur filtrage des cybermenaces**.

Plus précisément, pour que le logiciel définisse avec rigueur si l'email reçu est un spam, il analyse plusieurs éléments de l'email : liens, objet, pièce-jointe, images… selon des critères fixés.

Fonctionnalité #3
La protection de votre réputation

Il est important que votre nom de domaine ait une bonne réputation pour ne pas que les mails envoyés par vos utilisateurs, notamment commerciaux, soient considérés comme spam. Pour cela, un sender score est mis en place. Il prend en compte plusieurs éléments comme le taux de hard ou soft bounce, les taux d'ouverture, les plaintes pour spam, le nettoyage régulier de vos bases de données, l'utilisation de protocoles d'identification et la qualité de vos emails (éviter les pièces-jointes, les images ou les objets trop publicitaires).

Le but du sender score est d'éviter de vous retrouver dans des bases de blacklists et d'augmenter la délivrabilité des emails de vos collaborateurs.

Fonctionnalité #4
Le PCA (Plan de Continuité d'Activité)

L'impossibilité d'accéder à une boîte email peut avoir des conséquences désastreuses sur l'activité des entreprises. C'est pourtant ce qui peut se produire en cas de **défaillance système ou d'indisponibilité d'une infrastructure IT**.

C'est pourquoi nous vous conseillons d'opter pour une solution de messagerie dotée d'un Plan de continuité de l'activité (ou PCA). Ainsi, vos utilisateurs continuent d'utiliser leur boîte mail **via un webmail de secours**, en toute transparence, et ne seront pas impactés par une indisponibilité du serveur de messagerie même si ce dernier est dans le cloud d'un gros acteur. Aucun ne garantit, ni ne peut proposer une réelle disponibilité de 100%.

De plus, dès que l'accès au serveur est rétabli, les échanges mails effectués pendant la coupure sont re-synchronisés avec la messagerie de manière à ne perdre aucune information. **Un vrai plus**.

Fonctionnalité #5
L'intégration à l'environnement existant

Au-delà des fonctionnalités, la facilité de déploiement peut faire la différence. Optez pour une solution de protection qui **s'adapte à votre environnement de travail** : fournisseur de messagerie, hébergement, besoins de personnalisation des règles suivant les utilisateurs, autonomie d'utilisation de la solution, disponibilités d'APIs…

C'est indispensable pour renforcer la protection de votre messagerie et garder une autonomie de gestion. Qu'elle soit on-premise ou dans le cloud, sur site ou externalisée, votre future solution doit s'adapter à vos exigences, et non le contraire.

Bien évidemment, cette liste de **fonctionnalités "must have"** est non exhaustive. Cependant, ce sont à notre sens les critères indispensables à prendre en compte dans le choix d'une solution de protection pour votre messagerie professionnelle. Si vous souhaitez en savoir plus à ce sujet, n'hésitez pas à nous contacter.

Quel accompagnement pour déployer un antispam renforcé ?

Comme nous l'avons vu précédemment, les fonctionnalités de votre logiciel de sécurisation de la messagerie sont critiques. Mais un autre critère, non des moindres, est à prendre en considération : **l'accompagnement**. Que ce soit dans le cadrage de votre projet, pendant le déploiement de la solution ou en cas de nouveau questionnement en aval, optez pour un prestataire de proximité qui se comporte en véritable partenaire.

Et c'est ce que nous proposons chez Alinto ! Découvrez, dans cet article, comment nous assurons l'accompagnement de nos clients au cœur de notre solution.

Logiciel antispam : l'expertise et le support avant tout

Nul besoin de le répéter, la protection de votre messagerie professionnelle est stratégique pour votre entreprise. Il est donc important de faire appel à un partenaire qui l'a dans son ADN et qui possède une **vraie connaissance de la sécurité des emails**. Et c'est là le point fort de Alinto.

Depuis plus de 20 ans, les experts Alinto accompagnent les entreprises dans la gestion de leurs messageries professionnelles. Nous répondons à leurs attentes, suivons les évolutions et les tendances en matière de cyberattaques et proposons des fonctionnalités toujours plus pointues. Nous consacrons **30 % de notre CA à la recherche et au développement** pour offrir des solutions toujours plus performantes et sécuriser les messageries de nos clients. À travers plusieurs acquisitions d'entreprises spécialisées dans la sécurité des emails, nous possédons toutes les compétences et connaissances nécessaires pour assurer la protection de vos boîtes email, et au-delà de vos systèmes d'information.

Le service support est la clé de voûte de notre entreprise. Grâce à un système de ticketing, nos experts sont alertés en temps réel des situations rencontrées par leurs clients. Ils peuvent ainsi apporter une réponse ou prendre les décisions adaptées à la problématique dans des délais proportionnés aux risques.

Déploiement solution antispam : la réactivité comme maître mot

En lien avec le service support clients, les équipes de conseil Alinto se tiennent à votre disposition pendant toutes les étapes de votre projet. En amont, en vous aidant à cadrer votre projet. Lors du déploiement, en vous accompagnant pour installer le logiciel, et paramétrer les fonctionnalités nécessaires. Et en aval, avec la réponse à vos questions, la maintenance, le support…

La taille humaine et la stabilité de nos équipes nous permet de bien connaître nos clients et leurs enjeux. Nous répondons ainsi rapidement aux différents besoins, communiquons efficacement entre nos différents services afin d'apporter une solution adaptée et rapide. Notre logiciel, et donc votre protection, bénéficie de cette agilité. Nous savons à quel point l'interruption de votre service de messagerie peut être problématique, c'est pourquoi la proactivité est le maître mot de nos services.

Au-delà de l'antispam : l'optimisation de la gestion de la messagerie

Pour protéger votre messagerie professionnelle, il ne suffit pas de mettre en place un antispam, même si c'est indispensable. Il est important de voir plus loin pour **optimiser la gestion et la protection de vos emails**. Optez donc pour un logiciel qui propose des fonctionnalités additionnelles.

Chez Alinto, nous proposons, en plus de la protection antispam et antivirus :

- Une solution d'archivage, utile pour répondre aux exigences réglementaires. Vous choisissez ce que vous souhaitez garder ou non, vous pouvez faire évoluer les règles, la fréquence… et êtes alertés avant la destruction des emails.

- Un relais de messagerie SMTP pour garantir l'envoi d'emails "propres" et ne pas mettre en péril la réputation de votre domaine de messagerie.

- L'encryption qui sécurise les emails sortants grâce à un système de chiffrement, exigés dans les échanges de certaines industries. Seuls les administrateurs sont impactés par le chiffrement, qui reste totalement transparent pour les utilisateurs. Des services cloud de fax et SMS pour bénéficier d'une solution unique pour l'ensemble de vos canaux de communication. Grâce à des APIs ou directement via des emails, bénéficiez de toute l'expertise Alinto pour dématérialiser vos fax et SMS.

Alinto propose aussi d'autres services liés aux E-mail . Avec une constante : la proximité ! Vous avez un projet ou des questions ? N'hésitez pas à nous contacter !

Conclusion

Avec une menace de cyberattaques de plus en plus sournoises, **la protection de la messagerie professionnelle n'est plus une option pour les organisations !** Et se contenter des versions standards des antispam n'est plus suffisant.

C'est pourquoi, opter pour un logiciel de protection de la messagerie professionnelle s'avère la meilleure option pour mettre toutes les chances de votre côté. Il est également important de sensibiliser les collaborateurs, communiquer autour des bonnes pratiques du quotidien et veiller et anticiper **les tendances en matière de cybersécurité**.

À propos

Fondée en 2000, Alinto est une entreprise spécialisée dans les métiers de l'email : service de messagerie en mode SaaS, anti-spam, serveur email... à travers plusieurs produits :

- **Alinto Protect :** le relais de messagerie sécurisé qui immunise des risques d'Internet en assurant un accès permanent aux emails.
- **Alinto Gateway :** le relais de messagerie SMTP permet à des serveurs ou des applications d'envoyer des emails pour garantir un trafic dit « propre ».

Présent en France, Suisse et Espagne, Alinto compte plus de 30 personnes et assure un service de qualité à plus de trois millions d'utilisateurs. Plus de 15 millions d'emails sont envoyés chaque jour grâce à ses services de messagerie.

Le groupe Alinto rassemble plusieurs entités depuis 2016 pour se placer comme acteur majeur de la messagerie électronique. Il est composé des entreprises suivantes :

- **Cleanmail :** entreprise suisse spécialiste du filtrage antispam dans le cloud depuis 2002
- **SerenaMail :** spécialiste espagnol de la sécurité du courrier électronique (filtrage antispam).
- **Alinto :** services sécurisés de messagerie.

Cela permet au groupe d'affirmer sa position sur le marché et d'étendre son développement international.

Lyon (siège)
15 quai Tilsitt
69002 Lyon
+33 481 09 01 10

Barcelone
Avda. Diagonal, 434
08037 Barcelona
+34 91 005 29 64

Zurich
Gertrudstrasse 1
CH-8400 Winterthur
+41 52 208 99 66

Alinto

www.alinto.com