Protéger les administrations contre les cyber-attaques

Relever cinq défis en matière de sécurité pour les collectivités territoriales

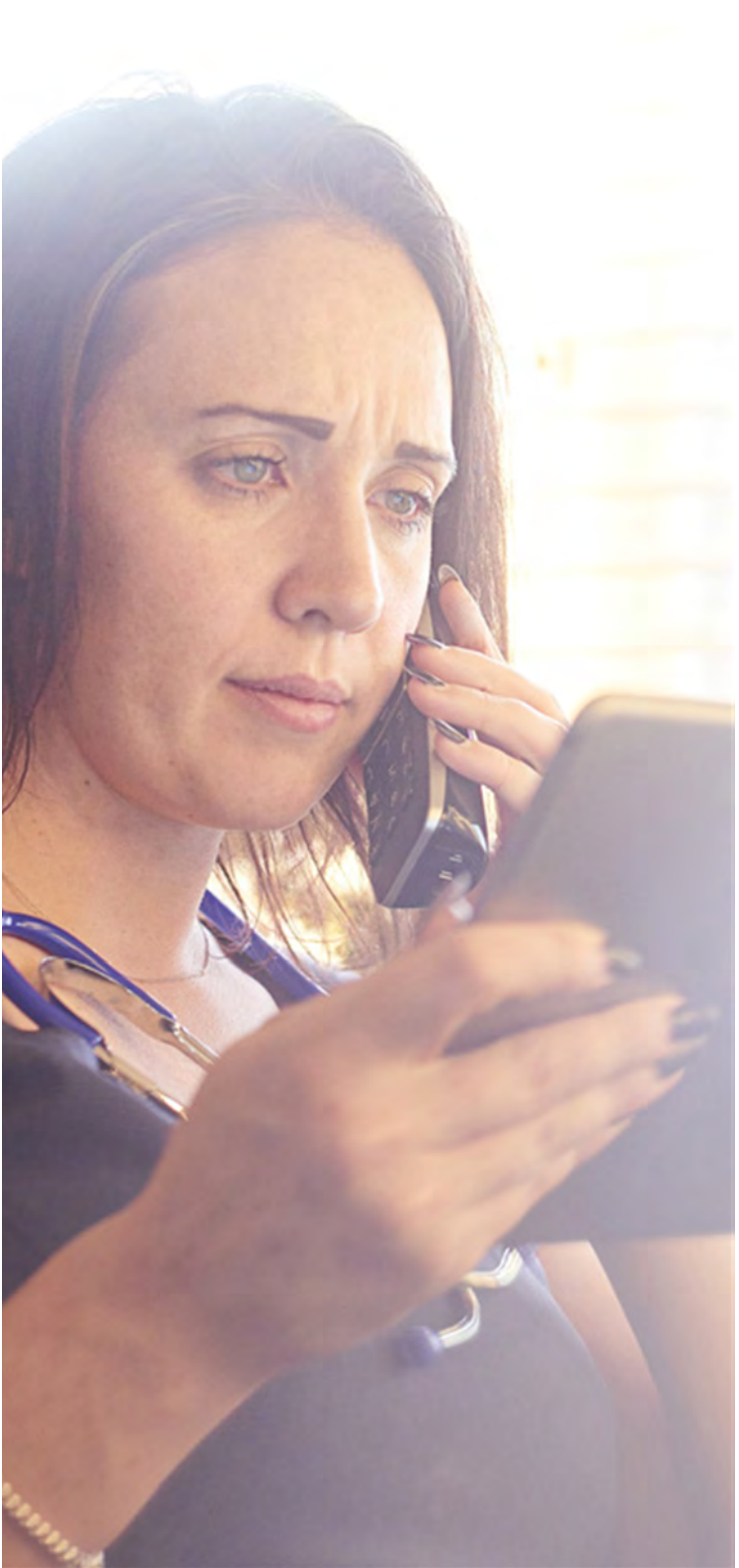
Introduction et objectif

Un monde connecté offre de nombreux bénéfices en matière de partage de l'information et de communication.

Cependant, le nombre important de connexions engendre par nature de nouvelles menaces, les frontières des entreprises devenant plus floues. En parallèle, les outils utilisés par les hackers deviennent plus sophistiqués et plus faciles d'accès.

Ces nouvelles menaces sont un défi permanent pour toutes les entreprises, particulièrement pour celles qui proposent des services au public. De plus, la propagation croissante de nouvelles menaces, telles que les ransomwares, montre que les hackers s'adaptent rapidement et que les entreprises ont du mal à contrer les attaques.

Dans ce document, nous abordons les cinq défis auxquels doivent faire face les collectivités. Pour y répondre, nous suggérons de traiter la sécurité comme un système et de l'intégrer dans une approche architecturale qui met en adéquation les besoins liés à l'activité et les technologies. Nous présentons ici des solutions qui aident à créer un système de sécurité efficace et robuste, pour offrir la meilleure protection possible.



Tandis que les collectivités territoriales cherchent à numériser leur offre de services publics, l'ouverture à un écosystème de plus en plus grand, combinée à un plus grand besoin de partage des systèmes et des informations, augmentent encore l'étendue des menaces. En outre, l'Internet des objets (IoT) prend de l'ampleur : il connectera bientôt des milliards d'objets, des voitures jusqu'aux bâtiments. Ce sont autant de nouvelles menaces en terme de sécurité. Ces objets connectés doivent être tout autant sécurisés que les autres systèmes IT.

Les contraintes budgétaires permanentes incitent les collectivités à modifier leurs prestations de services publics, cependant cette transformation s'accompagne de risques. Les pannes de systèmes doivent être évitées, car elles mettent en danger la vie même de l'organsiation. En effet, la moindre indisponibilité du système peut avoir un fort impact sur la réputation et le fonctionnement d'une administration et sur la confiance du public. En outre, le nouveau Règlement Général sur la Protection des Données (RGPD), obligatoire à partir du 25 mai 2018, sous peine de sanctions, donne les règles et instructions pour éviter les violations de données personnelles.

Il est essentiel de trouver l'équilibre et d'avoir une attitude proactrive, car les approches classiques pour protéger les données ne sont pas adaptées à un environnement dans lequel les menaces et les activités évoluent sans cesse.

Les modèles de sécurité qui ont pour unique objectif de protéger le périmètre du réseau et les terminaux ne sont plus fiables.

Cinq défis les plus courants en matière de sécurité pour les collectivités territoriales

L'évolution des menaces s'accompagne d'une augmentation du nombre d'attaques, avec la présence constante de menaces liées aux procédures ou aux comportements humains. Ce document couvre cinq grands types de menaces les plus couramment observés dans les collectivités territoriales.

1. Malwares

Les malwares représentent l'une des plus grandes cybermenaces pour toutes les entreprises ainsi que pour les collectivités territoriales. Face à l'augmentation exponentielle des nouvelles variantes de malwares et aux limites intrinsèques des défenses actuelles, les risques d'infection sont élevés.

Les ransomwares, par exemple, sont devenus très répandus et ont causé plusieurs crises de grande envergure. Cette tendance semble augmenter, dans la mesure où les ransomwares restent un moyen facile pour les hackers d'extorquer de fortes sommes d'argent à leurs victimes. En plus des risques financiers, une infection par ransomware peut avoir un impact lourd sur les collectivités territoriales, surtout si les systèmes sont infectés, car ils seront inutilisables jusqu'à leur restauration.

Un système de sauvegarde robuste et une procédure de reprise d'activité restent l'une des meilleures lignes de défense contre les ransomwares. Néanmoins, dans de nombreux cas, il est également possible de réduire le risque d'infection en sensibilisant mieux les utilisateurs et en déployant des contrôles réguliers qui ne dépendent pas uniquement des signatures.

2. Collaboration entre les différents acteurs

Les programmes de transformation numérique mis en place au sein des collectivités locales apportent des changements significatifs dans la conception et la prestation des services publics. Ils permettent de réduire les coûts et d'augmenter la productivité. Toutefois, ces programmes nécessitent également une meilleure collaboration au sein du secteur public et avec l'ensemble des partenaires du secteur privé.

Ce besoin croissant de collaboration s'accompagne d'un éventail de défis en matière de sécurité. Au niveau des politiques et de la gouvernance, il s'agit d'établir des contrats et des processus clairs pour garantir un échange d'informations sécurisé et de s'assurer que les données sont partagées d'un commun accord.

La mutualisation des bâtiments du secteur public est un aspect clé de cette collaboration. Cependant, il peut arriver que les espaces de travail partagés soient équipés d'une connectivité physique distincte pour chaque administration publique. Cela signifie que des collaborateurs en visite sur un site doivent pouvoir se connecter manuellement au bon réseau. Ce type de besoin augmente et cette approche est difficilement gérable. Elle doit être remplacée par la création de " bureaux flexibles" ou par un accès sans fil, afin de s'assurer que tous les utilisateurs disposent des accès appropriés et sécurisés basés sur leurs identifiants d'utilisateurs de l'organsiation.

3. Préparation de la gestion des incidents et attaques

Historiquement, les solutions de sécurité étaient conçues pour empêcher toute menace d'infiltrer le réseau. Cependant, la grande complexité des réseaux, combinée à la sophistication des malwares, rend cette approche obsolète.

Aujourd'hui, on ne se demande plus si un incident va se produire, mais quand il va se produire. En outre, le fait que les services publics s'appuient de plus en plus sur la technologie numérique signifie que les collectivités doivent mettre en œuvre de solides plans de gestion des incidents et attaques.

Étant donné le risque réel de faille, de tels plans ne peuvent pas se cantonner au département IT. En raison de l'impact potentiel des cyberattaques, les plans de gestion des incidents doivent s'aligner avec les plans de reprise de l'activité. Ils doivent également prendre en compte les processus requis pour faire appel à des services d'assistance externe et aux services de police. Ces plans doivent également prendre en compte les implications liées à l'obligation de notifier les failles de sécurité, mise en place par la réglementation RGPD, qui contraint les entreprises à déclarer les violations de données personnelles à l'autorité de surveillance appropriée dans les 72 heures. Enfin, pour rester efficace, il faut tester régulièrement le plan de gestion des incidents et l'améliorer sans cesse en fonction des résultats de chaque test.

4. Défis culturels

La culture reste un challenge permanent dans le domaine de la cybersécurité. On observe que la plupart des collaborateurs d'une entreprise privée ou publique, lorsqu'ils ont affaire à des systèmes IT peu ergonomiques qui freinent leurs activités professionnelles, trouvent des approches alternatives pour contourner et atteindre le résultat souhaité.

Ces solutions provisoires peuvent les amener à adopter des comportements non sécurisés, comme l'utilisation d'applications non prises en charge et non autorisées. Il existe de nombreux exemples de collaborateurs utilisant des messageries basées dans le cloud ou des applications de partage de documents non autorisés. Ces activités passent souvent inaperçues, ce qui entraîne des risques d'infection par malware et de perte de données, et potentiellement, des violations de la législation sur la protection des données. D'autres exemples comprennent l'utilisation d'applications de messagerie et de vidéoconférence grand public.

Plutôt que de réprimer ces comportements, il est important d'identifier et d'accompagner les besoins des collaborateurs et de développer des solutions sécurisées à ces besoins. En outre, il est important de favoriser une culture de la sécurité au sein de l'entreprise auprès des collaborateurs et de présenter les bonnes pratiques.

5. Direction

Tout comme le développement de la culture de la sécurité auprès des collabroateurs, l'implication de la direction représente également un défi pour les administrations cherchant à créer un programme de cybersécurité complet. L'ensemble de la direction doit s'impliquer entièrement pour parvenir à développer et à mettre en œuvre une stratégie de cybersécurité complète. Trop souvent, les problèmes de sécurité sont cantonnés au domaine technique et rapidement transférés au département informatique.

Lorsqu'elles délèguent cette responsabilité, les équipes dirigeantes fournissent généralement peu d'informations à l'équipe IT au sujet des applications les plus stratégiques. Cela empêche de bien identifier les risques à gérer et d'appliquer les contrôles appropriés. Cela augmente le niveau de risque à cause d'une protection inadaptée.

Il est donc essentiel que l'équipe dirigeante comprenne l'impact potentiel d'une faille de sécurité, sinon, cela peut nuire à la confidentialité, à l'intégrité ou à la disponibilité des systèmes publics
ou internes stratégiques, altérant la confiance du public et la réputation de l'administration, et réduisant la capacité d'un organisme à offrir des services au public. Pour aider l'équipe dirigeante à comprendre les enjeux, les équipes IT doivent parvenir à expliquer les risques d'une manière non technique et à demander des directives précises pour définir des priorités et budgets adéquats.

Adopter une approche architecturale

Nous avons identifié cinq défis en matière de sécurité pour le secteur public.

Si chacun d'eux peut être considéré de manière isolée, il est plus sûr et stratégique d'opter pour une approche globale pour contrer les attaques et protéger les systèmes d'information.

Adopter une approche architecturale implique de traiter la sécurité comme un système de bout en bout, plutôt que comme une mosaïque de composants distincts. Ce système global est plus facile à gérer et permet de partager des informations contextuelles essentielles concernant les menaces pour être plus réactif et efficace.

Une telle approche doit s'appuyer sur les grands principes suivants :

- Un changement de politique prenant en compte la sécurité comme un accélérateur d'activité.
- Les administrations doivent comprendre qu'il ne s'agit plus de savoir si une faille va se produire, mais quand elle va se produire.
- Les contrôles de sécurité doivent dépasser l'approche classique de « blocage », et tendre à améliorer les délais de détection et de correction.
- La sécurité doit être développée en tant que système. Les divers composants ne doivent pas fonctionner de manière isolée. Ils doivent être intégrés pour offrir une détection des menaces précises et simplifier la gestion.

Une approche architecturale se base sur les besoins liés à l'activité. En commençant par identifier les ressources d'informations et les systèmes sur lesquels l'activité s'appuie, il est possible d'évaluer l'impact d'un problème.

Les problèmes peuvent concerner trois aspects liés à la sécurité de l'information : la confidentialité, l'intégrité et la disponibilité. C'est un changement radical de perspective, car la confidentialité est trop souvent placée au premier plan, alors qu'une perte de disponibilité ou d'intégrité peut avoir aussi un impact beaucoup plus fort.

Une fois que vous avez identifié les ressources et étudié l'impact potentiel d'un incident, il est important de se pencher sur la menace. Dans ce document, nous avons identifié les cinq défis à prendre en compte, cependant ils ne sont pas exhaustifs. Il faut englober d'autres éléments comme les menaces internes et externes.

Comme pour toute approche architecturale, la compréhension du contexte global de l'activité aide l'administration à déterminer les fonctionnalités que la technologie offre afin d'améliorer l'expérience usager. La sécurité doit donc être prise en considération en tant que système plutôt que comme une solution temporaire qui résout les problèmes qui se présentent. Au fil de l'eau, avec une telle approche, les contrôles de sécurité deviennent transparents pour l'utilisateur. En outre, cette procédure évite le non-respect des contrôles.

En d'autres termes, la sécurité est un accélérateur d'activité.

Comment Cisco vous aide à vous protéger des menaces

Grâce à nos solutions de sécurité, nous sommes parfaitement positionnés pour répondre à vos besoins en matière de sécurité en tant au niveau du réseau, que des applications physiques ou virtuelles.

Lorsque vous développez votre architecture de sécurité, il est utile de considérer une cyberattaque comme un processus continu composé de trois phases. Cisco développe une protection avant, pendant et après l'attaque.

Avant

C'est la phase qui bénéficie des plus grands investissements en matière de sécurité, notamment le déploiement de fonctions de défense, telles que les pare-feu et les systèmes de protection contre les programmes malveillants. Il est essentiel de comprendre que vos défenses, bien qu'elles soient importantes, vont à un moment donné faire l'objet d'une faille. C'est pourquoi les investissements doivent être répartis de manière équilibrée.

Pendant

Les contrôles déployés lors de cette phase visent à améliorer la visibilité, pour qu'une attaque puisse être rapidement identifiée et maîtrisée. La segmentation du réseau permetde gérer les attaques lors de cette phase. Lorsqu'elle est correctement mise en œuvre, elle permet d'isoler une attaque sur un sous-ensemble du réseau et du parc IT.

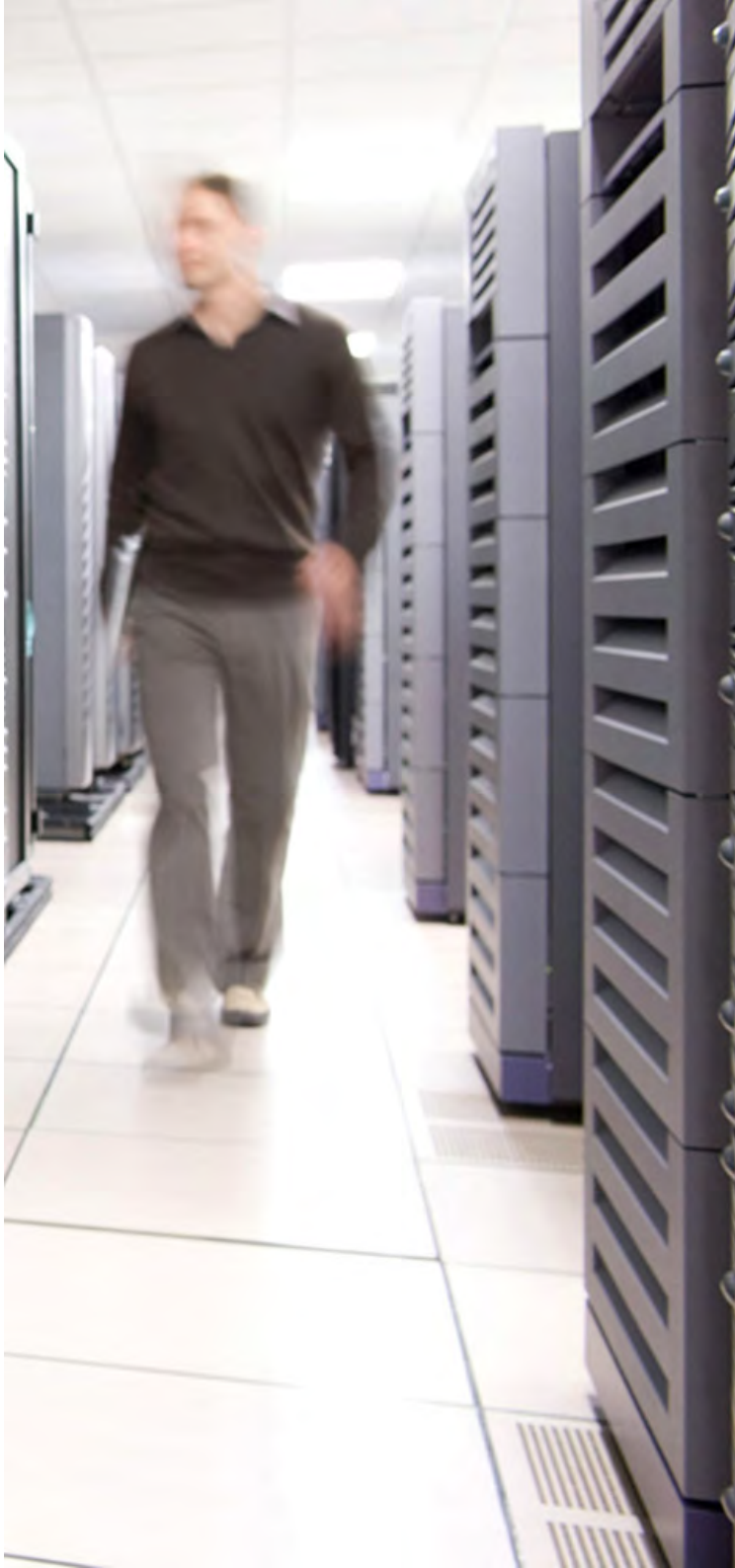
Après

La phase finale du processus correspond à l'élimination rapide de la menace. Elle comprend également des analyses qui contribuent à déterminer la manière dont une attaque a eu lieu et à identifier les systèmes qui peuvent avoir été affectés.

Lorsque vous suivez ce modèle, il est important de déployer des fonctionnalités qui couvrent l'ensemble du processus d'attaque, en vous concentrant non seulement sur les technologies de défense, mais également sur les éléments essentiels qui permettent d'identifier, d'isoler et de régler rapidement les incidents.

Le réseau représente le fondement de l'interconnectivité, c'est pourquoi il est particulièrement bien positionné pour offrir la visibilité et le contrôle dont vous avez besoin pour identifier et isoler rapidement les menaces. Des technologies telles que **Cisco Netflow** (intégré dans la plupart des matériels réseau de Cisco) offrent une télémétrie du réseau en temps réel, révélant qui parle à qui, avec quel protocole et pendant combien de temps. Grâce à ces données télémétriques détaillées, il est possible d'identifier et d'analyser rapidement les types d'activité inhabituels. Par exemple, un transfert de données unilatéral excessif, qui peut indiquer un vol de données, ou la transmission de données entre des systèmes internes et des machines basées sur Internet situées dans des endroits suspects.

La segmentation est une autre fonctionnalité essentielle basée sur le réseau. Elle occupe une place de plus en plus importante, notamment lorsque l'on considère le besoin de connecter une plus large gamme d'appareils et de communautés d'utilisateurs à une infrastructure de réseau commune. Toutefois, la segmentation reste complexe, car de nombreux environnements s'appuient toujours sur une segmentation statique basée uniquement sur l'emplacement physique. En outre, la segmentation en place n'est pas toujours optimum pour réaliser les contrôles de sécurité sur l'ensemble du trafic.



Cisco TrustSec englobe toute une gamme de fonctionnalités qui permettent la segmentation logicielle du réseau. Il s'agit de pouvoir appliquer dynamiquement une politique de segmentation lorsqu'un utilisateur ou un appareil se connecte au réseau, via un accès filaire ou sans fil.

TrustSec peut récupérer les données liées au terminal connecté. Ainsi, la prise de décision concernant la politique à appliquer se base sur des informations concrètes. Ces données peuvent inclure de simples identifiants d'utilisateur, le type d'appareil utilisé, le logiciel installé ou la conformité avec les politiques logicielles (c'est-à-dire si l'appareil possède les derniers correctifs). En recueillant ces informations, le système est à même de prendre des décisions plus abouties et d'appliquer une politique de sécurité prédéfinie, de sorte que l'appareil ne bénéficie que de l'accès dont il a besoin. Par exemple, cela peut être utile pour appliquer une segmentation dynamique entre les membres d'une administration, garantissant aux deux communautés qu'elles disposent bien des accès dont elles ont besoin pour réaliser leurs tâches et limitant leur accès aux autres systèmes.

Cisco Netflow et TrustSec ne sont que deux innovations parmi toutes celles que Cisco a développées pour intégrer la sécurité dans le réseau. Nous proposons également une suite complète de fonctionnalités, allant du contrôle d'accès du périmètre à la prévention des intrusions, en passant par des solutions avancées de protection du réseau et des terminaux contre les malwares.

Notez que chaque composant peut fonctionner avec les autres, formant un système de sécurité intégré à même de partager les données relatives aux menaces et au contexte.

Le résultat global est un système plus réactif aux menaces qui peut identifier rapidement les problèmes lorsqu'ils surviennent. La correction des problèmes et la reprise de l'activité sont rapides, et l'entreprise peut fonctionner sans entrave.

Pour relever les défis abordés dans ce document, il faut adopter une approche « de haut en bas » de la conception d'une stratégie de cybersécurité. Les services Cisco de conseil pour la sécurité peuvent aider les collectivités territoriales à atteindre cet objectif grâce à ces étapes :

- Identifier les risques auxquels s'expose l'administration en analysant l'impact potentiel d'une faille ou d'une perte de données sur l'activité
- Analyser les vulnérabilités pour identifier l'écart entre le niveau de contrôle requis et l'état actuel du système
- Déterminer les domaines stratégiques d'investissement en matière de sécurité au niveau de l'entreprise, des politiques et des technologies, afin d'assurer la prestation sécurisée des principaux services

La technologie numérique a un impact particulièrement bénéfique pour les collectivités territoriales lui permettant de proposer de plus en plus de services aux usagers. Cependant, devant la recrudescence des attaques, il est nécessaire de s'appuyer sur une architecture de sécurité conçue « de haut en bas ».

Nous sommes particulièrement bien positionnés pour aider nos clients à développer ces fonctionnalités. N'hésitez pas à nous contacter pour découvrir comment procéder.

Nous contacter

Cisco dispose d'une équipe dédiée pour répondre à toutes les questions. Grâce à ses connaissances sectorielles pointues, notre équipe peut identifier les solutions Cisco adaptées à vos besoins.

Reportez-vous au numéro ci-dessous pour démarrer une conversation avec votre conseiller Cisco le plus proche.

Auteurs

Contactez-nous	0800 770 400