Sécurité Informatique et Réseau :
Des réponses pour mieux agir et se protéger

Hub One
Une connexion d'avance

SOMMAIRE

ÉDITO

VOUS ACCOMPAGNER DANS UNE MEILLEURE COMPRÉHENSION DES MENACES INFORMATIQUES QUI PÈSENT SUR LES ENTREPRISES, QUELLE QUE SOIT LEUR TAILLE.

« Un livre blanc pour mieux comprendre, prendre des décisions et améliorer la sécurité des réseaux et des systèmes d'information. »

Tous les indicateurs le révèlent, le nombre d'attaques informatiques ne cesse de croître à la fois dans leur volume et dans leur diversité. Et il ne faut pas s'y tromper : aucune organisation ne peut prétendre se trouver à l'abri de cette menace. Une situation qui découle de la valeur et l'omniprésence, dans les activités professionnelles mais aussi dans nos vies personnelles, de la donnée. Cet actif immatériel, revêt la même importance stratégique que l'on soit une PME ou une multinationale.

Si la menace est chaque jour plus forte, la conscience que nous avons tous de cette menace a grandi elle aussi. Pourtant, les utilisateurs demeurent des failles à leur insu, les protections sont souvent mal déployées, les outils mal paramétrés et les cyberattaques se détectent par définition trop tard... Au final, le préjudice se révèle colossal tant sur le plan financier que sur l'image que l'on renvoie à ses clients et à son écosystème.

Multiplication des terminaux, maladresse des collaborateurs, malveillance mais aussi appât du gain pour les cybercriminels, la protection absolue et définitive n'existe pas. Néanmoins, une entreprise démontrant qu'elle prend le problème au sérieux et déploie un arsenal convaincant, saura détourner l'attention des pirates qui s'orienteront vers des proies plus faciles. Volontarisme, rigueur, exigence... après avoir dressé l'état des lieux de votre système d'information, vous pourrez définir la meilleure stratégie de sécurité.

Autant de questions centrales, auxquelles Hub One, par son vaste socle d'expériences et sa maîtrise technologique, saura vous apporter des éléments de réponses indispensables.

Bien à vous,

Patrice Bélie,
Directeur Général Hub One

SÉCURITÉ INFORMATIQUE : POURQUOI DOIT-ELLE ÊTRE AUJOURD'HUI UNE PRIORITÉ ABSOLUE ?

Plus qu'une tendance, un enjeu majeur

Alors que les enjeux de sécurité devraient être au cœur des préoccupations de tout un chacun, nous assistons malheureusement à une banalisation certaine de cette problématique. Les mauvaises pratiques des collaborateurs, les protections installées mais mal configurées, exposent les entreprises à une insécurité latente.

De nos jours, la question n'est plus de savoir si votre entreprise fera un jour l'objet d'une cyberattaque, mais quand celle-ci interviendra. Car elle interviendra ! Selon une étude OpinionWay[1], plus de 8 entreprises sur 10, ont été victimes d'une attaque informatique en 2015. Il est donc temps d'agir car les conséquences peuvent être dramatiques ! Données clients piratées, attaques sur l'outil de production... le préjudice financier peut être considérable et la désorganisation qui découle de l'attaque peut générer une perte d'exploitation sur plusieurs semaines.

5 facteurs

qui rendent la sécurisation des réseaux locaux d'entreprises indispensable

- **De plus en plus d'applications métiers sont utilisées en mode SaaS[2] et rendent la sécurité des connexions réseaux incontournable.**
- **Les collaborateurs nomades sont connectés à distance sur le système d'information de l'entreprise.**
- **Smartphone, tablette tactile, ordinateur portable, la multiplication des périphériques complique la mise en place d'une politique de sécurité homogène.**
- **Le décloisonnement des différents services de l'entreprise, les importants volumes d'informations mutualisés entre ces services, multiplient les risques de propagation des attaques.**
- **Les collaborateurs sont insuffisamment sensibilisés aux bonnes pratiques et aux enjeux de sécurité informatique.**

(1) Club des Experts de la Sécurité de l'Information et du Numérique - Baromètre de la cyber-sécurité des entreprises - Janvier 2016
(2) Software as a Service (Logiciel en tant que service)

L'INSÉCURITÉ EN QUELQUES CHIFFRES

57 %

des entreprises ont déjà connu un incident en matière de cybersécurité.[3]

9 000

c'est le nombre de fichiers malveillants détectés chaque jour sur l'environnement Android au second semestre 2016. Au total, 3 246 284 nouvelles applications malveillantes pour Android ont été recensées en 2016.[4]

N°3

c'est le classement de la notion de cyber-risques au Top 10 des risques encourus par les entreprises en 2017.[5]

52 %

des entreprises utilisent le Cloud. Pour 68 % d'entre elles, les questions relatives à la sécurité des données externalisées sont les plus importantes.[6]

20 % d'après l'institut Gartner, le coût de la sécurité représente à ce jour 1 % des budgets annuels mais augmentera à 20 % à l'horizon 2020.[7]

469

c'est le nombre de jours nécessaires en Europe pour détecter une infection du système d'information d'une entreprise.[8]

2 100 milliards de dollars

c'est le coût estimé du vol de données pour l'année 2019, soit 2,2 % du PIB mondial.[9]

100 %

des victimes disposent d'un antivirus qui est à jour en termes de signatures.[10]

Sources : (3) Etude EY 2016 (Global Information Security Survey) - (4) G Data Software - (5) Allianz Risk Barometer 2017 (Baromètre des risques Allianz)
(6) NetMedical Europe en 2016 - (7) Conférence Gartner Symposium/ITxpo - (8) Rapport M-Trends 2016 de FireEye - (9) Juniper Research
(10) Verizon 2015 data breach investigation report

DES MENACES VARIÉES, DES CONSÉQUENCES GRAVES

Perte d'exploitation, désorganisation, interruption de la production ou perte de crédibilité auprès des clients, toute agression informatique non maîtrisée constitue un préjudice grave !

La menace virale comme moyen de pénétrer votre système d'information

Virus, vers informatiques, chevaux de Troie, ces programmes malveillants (ou malwares) s'installent sur les machines et se répandent progressivement sur l'ensemble du système d'information.

Les conséquences : lorsque ces malwares ont pris place sur les machines de votre réseau local, ils peuvent laisser libre accès à l'ensemble des données (fichiers clients, documents stratégiques...) et compromettre gravement l'activité à court, moyen et long terme !

Le déni de service pour saturer votre système d'information

Une attaque par déni de service (DDOS)[11] repose sur le principe de la saturation de vos serveurs par la multiplication de requêtes simultanées. Pour ce faire, les pirates prennent insidieusement le contrôle de milliers d'ordinateurs de par le monde et font en sorte qu'ils se connectent tous, au même moment, sur vos serveurs qui ne peuvent résister à la charge et ne répondent plus.

Les conséquences : sur un site de vente en ligne, le préjudice est évident. Chaque seconde d'indisponibilité conduit à une perte de chiffre d'affaires. Mais toutes les activités sont concernées. En cas d'attaque par déni de service, les collaborateurs ne peuvent plus exploiter le système d'information saturé et sont réduits à l'impuissance.

Les ransomwares paralysent l'activité

Des logiciels malveillants bloquent les ordinateurs infectés et exigent le paiement d'une rançon (le plus souvent en bitcoins) pour vous en rendre le contrôle. Les plus évolués chiffrent le contenu du disque dur, empêchant toute tentative pour vous en débarrasser.

Les conséquences : si les machines infectées gèrent un processus de fabrication industrielle, ce dernier est interrompu et même en cas de paiement de la rançon, vous n'êtes jamais assuré d'une reprise de contrôle réelle de la machine.

(11) Distributed Denial of Service (Déni de service)

Les Bots & PC Zombies : la menace silencieuse

Ces réseaux d'ordinateurs corrompus contrôlés par un ou plusieurs cybercriminels peuvent être utilisés à différentes fins : attaques DDOS, campagne de spam, de phishing ou diffusion de malwares (logiciels malveillants). Plus ces réseaux sont vastes, plus leur impact peut être important.

Les conséquences : le détournement de l'ensemble du parc informatique d'une entreprise par un pirate informatique, entame les performances de chaque machine infectée, mais aussi la bande passante disponible. L'activité est ralentie et la brèche ouverte par les Bots, reste une vulnérabilité qui peut être exploitée à d'autres fins...

Le défacement de site Web : un préjudice d'image sévère

Les pirates peuvent s'introduire sur les serveurs hébergeant le site Web de l'entreprise et substituer la page d'accueil habituelle par des contenus inappropriés (sites pornographiques par exemple), ou par une page revendiquant leur prise de contrôle de votre site et votre incapacité à le sécuriser.

Les conséquences : cette menace peut sembler anodine sur le fond car le défacement n'implique pas nécessairement une compromission de la sécurité globale de vos données. Toutefois, elle adresse un message à tous les visiteurs de votre site : votre protection est imparfaite !

Les exploits démontrent la faiblesse de votre protection

Les exploits sont des programmes informatiques qui mettent en œuvre l'« exploitation » d'une vulnérabilité, d'une faille, publiée ou non. Chaque exploit est spécifique à une version d'une application car il permet d'en exploiter les failles. Les exploits sont généralement écrits en langage Perl ou C.

Les conséquences : lorsqu'un exploit met au jour une vulnérabilité, le pirate peut menacer l'entreprise de divulguer la faille détectée. Une fois l'exploit compilé, il peut être commercialisé sur le Blackmarket (marché noir) pour que les cybercriminels puissent utiliser la faille contre leurs victimes.

Le phishing usurpe l'apparence de sites connus

Le principe du Phishing (ou Hameçonnage), consiste à adresser un e-mail demandant à son destinataire de saisir des données personnelles pour accéder à un service familier. Sites bancaires, sites marchands, les cybercriminels créent des clones de sites familiers pour duper les destinataires.

Les conséquences : le détournement d'informations par le phishing permet aux criminels d'accéder à de nombreuses données.

Le phishing en chiffres[12]

66 % des attaques de cyber-espionnage sont initiées par un e-mail de phishing.

50 % des e-mails de phishing sont ouverts dans l'heure qui suit leur expédition.

23 % des destinataires ouvrent ces messages.

11 % exécutent les fichiers joints aux e-mails de phishing.

Des conséquences financières indirectes

- Frais associés à la gestion de crise (communication),
- Investigations pénales et frais de justice éventuels,
- Investissements liés à la remise à niveau du système d'information,
- Enquête pour identifier les causes de vulnérabilité...

(12) Source: Verizon 2015 data breach investigation report (Rapport d'investigation sur les brèches de données)

COMPARTIMENTER, SEGMENTER, CONTENIR LES MENACES

Assurer une sécurisation efficace du réseau local de l'entreprise, c'est, au-delà des moyens déployés, un état d'esprit ! Accepter que la menace soit permanente, qu'elle vienne de l'extérieur avant d'être propagée souvent par la maladresse des collaborateurs à l'intérieur du système d'information, c'est déjà comprendre le problème.

Avec le développement du BYOD[13] et de l'IoT[14], le réseau est exposé à de nouvelles menaces. Contrôler ces nouveaux équipements, qui échappent de fait au DSI[15] et RSSI[16], est complexe.

Reste à définir les pratiques qui contribueront à limiter votre exposition aux dangers extérieurs et à contenir la propagation des menaces qui peuvent vous affecter.

En segmentant les activités informatiques, en créant des profils d'utilisateurs ciblés en fonction de leurs missions, il est possible de réagir vite et bien !

(13) BYOD : Bring Your Own Device (Amenez vos propres équipements) - (14) IoT : Internet of Things (Internet des objets)
(15) Directeur des Systèmes d'Information - (16) Responsable de la Sécurité des Systèmes d'Information

5 phases

1 Réaliser un audit du système d'information

Il n'existe pas de solution de sécurisation globale applicable à toutes les entreprises. En fonction de l'activité, du nombre de collaborateurs, des usages, de la sensibilité des données échangées, la définition de la politique de sécurité est un travail sur mesure.

2 Sécuriser l'accès à Internet

Le premier levier à actionner consiste à limiter l'exposition aux risques venus de l'extérieur. Il convient de déployer un arsenal indispensable pour s'en préserver. Anti spam, Antivirus, un pare-feu parfaitement configuré pour filtrer les données entrantes et sortantes.

3 Créer des profils d'utilisateurs

En définissant des politiques de sécurité adaptées à chaque type d'utilisateur dans l'entreprise, vous parviendrez à limiter votre exposition aux menaces. Le filtrage d'URL, mais aussi la fermeture de certains ports pour éviter le téléchargement de logiciels ou encore la limitation du débit de données pour des activités non essentielles à la mission du collaborateur, sont autant de moyens de préserver l'intégrité du système d'information.

4 Tunneliser pour contenir les menaces

Éviter la propagation d'une menace informatique, c'est comme éviter la contagion par la grippe. L'essentiel consiste à confiner les organismes sains pour éviter qu'ils ne soient infectés. La compartimentation des données, et des activités informatiques répond à ce principe et permet de définir des stratégies de protection périmétrique. Des collaborateurs accédant à distance au système d'information via leurs équipements personnels (BYOD) devront passer par un VPN[17] parfaitement étanche.

5 Étanchéifier et limiter la contagion via une détection précoce

PC, imprimante, caméra de sécurité... tout périphérique connecté au réseau local constitue de facto un risque. Chaque élément, chaque utilisateur accédant au système d'information doit faire l'objet d'un contrôle bienveillant mais sérieux des flux de données qu'il génère. En analysant les flux de données, les anomalies peuvent être détectées et traitées rapidement en isolant les éléments suspects du reste du parc informatique.

(17) VPN : Virtual Private Network (Réseau privé virtuel)

DES MENACES QUI PÈSENT SUR TOUT TYPE D'ORGANISATION

Selon une étude menée par PwC[18], le nombre d'attaques informatiques dans les entreprises en 2016 a augmenté de 68 % par rapport à 2015.

Dans ce contexte, tous les systèmes d'information sont bel et bien exposés. Loin des images d'Épinal, il n'est pas nécessaire de manipuler des données extrêmement sensibles, de compter de larges effectifs ou de générer d'importants chiffres d'affaires, pour attirer à soi les cybercriminels.

Tout système d'information est exposé aux risques informatiques. Les données d'ordre financier ou relatives aux clients, l'image de marque, la propriété intellectuelle, ou les informations relatives aux employés, sont parmi les éléments critiques à protéger des failles de sécurité.

PUBLIC / PRIVÉ : UNE EXPOSITION COMPARABLE

En 2015, la Gazette des communes dressait la cartographie des degrés de sécurisation de plus de 14 000 sites de communes[19]. Près de 6 500 d'entre eux n'étaient pas à jour, et pourtant ! Suite aux attentats de 2015, de nombreux sites de communes étaient victimes de défacements.

Et ce n'est rien par rapport aux soupçons qui pèsent sur la fraude potentielle au vote électronique qui a peut-être influencé les dernières élections américaines.

Ce constat est d'autant plus inquiétant que la volonté politique de faire de la France une « République Numérique » implique la création d'un réel climat de confiance entre les usagers et l'e-administration.

(18) PWC - La fraude explose en France : La cybercriminalité au cœur de toutes les préoccupations
(19) Cartographie de la sécurisation des sites de communes - Gazette des communes Mars 2015

LES GRANDS COMPTES FORTEMENT EXPOSÉS

D'après l'enquête réalisée à l'automne 2016 par Forbes Insights[20] auprès de 308 cadres exerçant dans divers secteurs d'activités en Amérique du Nord et en Europe, 64 % des répondants placent la protection contre les menaces de sécurité connues et leur traitement au sommet de leurs priorités au cours des 12 prochains mois.

82 % des responsables informatiques déclarent par ailleurs que les investissements augmenteront à nouveau en 2017. Des tendances qui illustrent parfaitement l'augmentation exponentielle du risque en matière de sécurité informatique.

LES PME, CIBLES D'ATTAQUES MASSIVES

D'après l'étude réalisée par PwC, il apparaît que parmi les sociétés de moins de 100 personnes, plus de 2 entreprises françaises sur 5, déclarent avoir été victimes de fraudes ou de programmes malveillants. Un chiffre deux fois plus élevé que la moyenne mondiale ! 53 % des entreprises auraient ainsi été confrontées à un problème de sécurité de données en 2016, contre seulement 28 % en 2014.

Si les PME sont globalement conscientes des risques, elles demeurent mal équipées ! Ainsi d'après une étude Ipsos sur la conscience des PME sur les risques informatiques encourus, il apparaît que plus de la moitié des PME ne prend aucune autre sorte de disposition pour se protéger des actes de malveillance[21].

L'étude révèle ainsi que 26 % des petites et moyennes entreprises ne possèdent pas d'antivirus, qu'elles ne sont que 36 % à utiliser un anti-phishing et 52 % un pare-feu !

LES TPE NE SONT PAS ÉPARGNÉES

Contrairement aux idées reçues, être une TPE ne met pas à l'abri des menaces informatiques. En effet, l'absence de fonctions dédiées à la sécurité informatique ou un système informatique géré par une personne dénuée de formation appropriée, facilite la tâche des cybercriminels.

Ces derniers sont par ailleurs confrontés au rehaussement du niveau de sécurité dans les grandes entreprises. Ils s'orientent alors vers des cibles plus vulnérables.

(20) Étude BMC & Forbes Insights - Enquête annuelle sur la sécurité
(21) Sécurité informatique des PME françaises - Baromètre Ipsos-Navista

PAROLES D'EXPERTS

Christophe AUBERGER,
Directeur Systems Engineering France, Fortinet

Si vous deviez résumer les principales problématiques auxquelles les DSSI[22] sont confrontées, quelles seraient-elles ?

Lorsque je parle à des DSSI des problématiques qui les occupent, quels que soient les environnements qu'ils gèrent, elles peuvent être résumées en 5 points clés :

- **La sécurité des applications Cloud**
  Les collaborateurs utilisent les applications issues de Cloud publics, de Gmail à Dropbox et aux logiciels mobiles comme WhatsApp. La gestion et la maîtrise des risques associés constituent ainsi une priorité pour les DSSI.

- **Les menaces avancées**
  Souvent dénommées APT[23], ces menaces que je qualifie de ciblées, sont présentes sous de nombreuses variantes. Elles savent contourner les lignes de défense traditionnelles et ciblent généralement les informations confidentielles et les données personnelles. La valorisation de l'information en tant qu'actif à part entière de l'entreprise, devient donc monnayable aisément et attise l'intérêt des organisations criminelles.

- **La gestion des événements**
  La collecte des journaux, le reporting et la gestion des événements sont des tâches inhérentes à la mission des administrateurs informatiques. Pour les DSSI, l'abondance et l'hétérogénéité des informations sont tout aussi préjudiciables que l'absence d'informations sur une attaque. Les dispositifs de type SOC (Security Operations Center), qui se développent, soit directement au sein des entreprises ou sous forme de service externalisé, constituent une réponse...

- **La conformité**
  PCI DSS (Payment Card Industry Data Security Standard)[24], Sarbanes-Oxley (SOX) ou la réglementation française européenne (Loi de Programmation Militaire) en matière de confidentialité des données (GDPR)[25]... J'entends souvent les DSSI se plaindre des difficultés à assurer et pérenniser la mise en conformité réglementaire.

- **La pérennité des investissements de sécurité**
  C'est une préoccupation des DSSI : disposer d'une vision technologique pertinente répondant à cette préoccupation est un atout majeur pour leur organisation. En plus de tous ces points, il en existe un autre, sous-jacent et transverse à tous les autres. Il s'agit de la définition d'une stratégie de sécurité.

En quoi les stratégies de sécurité sont-elles si essentielles ?

Elles sont essentielles pour réduire le profil de risque des entreprises et repousser les menaces, surtout si elles sont ciblées. Mais très peu d'organisations prennent le temps d'en élaborer. Elles préfèrent la facilité en se basant sur des exemples génériques. Une approche intégrée et non segmentée est en accord avec ces stratégies de sécurité, mais cette dernière doit être globale et intégrer toutes les dimensions de la sécurité. Cette approche holistique doit incorporer les dimensions techniques, humaines, communication, gestion de crise, formation a minima.

Quel est, à vos yeux, le meilleur moyen de répondre à ces différents enjeux ?

Chacune de ces préoccupations plaide en faveur d'une architecture de sécurité intégrant les composantes matérielles, logicielles et de protocole de communication, tout en privilégiant une segmentation interne du réseau. Ainsi consolidée, l'architecture déploiera une protection transparente et intégrale sur une surface d'attaque qui s'élargit, intégrant désormais le Cloud et l'IoT. Le Cloud doit être perçu comme une extension du réseau d'entreprise, et les entreprises sont tenues de déployer une stratégie de sécurité capable d'identifier et de gouverner des volumes importants de données qui transitent sur un réseau décloisonné, filaire ou sans fil, privé ou public, traditionnel ou Cloud. Les entreprises doivent regarder au-delà des pare-feux traditionnels. Pour le DSSI, il est essentiel de connaître tous les équipements qui se connectent au réseau à tout moment et en tout point, pour comprendre le niveau de sécurité de son organisation et l'efficacité de ses règles et processus de sécurité.

(22) DSSI : Directeur de la Sécurité des Systèmes Informatiques - (23) APT : Advanced Persistent Threat (Menace persistante avancée) - (24) PCI DSS : normes de sécurité sur les données de l'industrie des cartes de paiement - (25) GDPR : General Data Protection Regulation (Règlement général sur la protection des données)

CAS CLIENTS

CAS • 1 Industrie médicale

Un acteur international qui conçoit, produit et commercialise des dispositifs médicaux divers, souhaite doter son centre de décision et de production en France, d'un accès Internet sécurisé.

Les objectifs
- Disposer d'un accès Internet sécurisé
- Contrôler le trafic d'accès Internet
- Améliorer la qualité de service

Le point clé de la réponse
La solution préconisée comprend l'accompagnement du client dans la migration de son accès Internet. Cet accès Internet est dorénavant sécurisé par la mise en place de firewall. Cette solution permet une visibilité des usages qui sont faits de la bande passante par les utilisateurs, afin de prioriser les applications métiers et améliorer la qualité de service.

CAS • 2 Start-up et robotique

Une start-up de moins de 20 collaborateurs souhaite sécuriser son réseau et pouvoir communiquer avec un site distant. Un réel besoin d'étanchéifier le réseau de toutes menaces extérieures.

Les objectifs
- Sécuriser l'accès Internet
- Communiquer vers un site distant de manière sécurisée et chiffrée
- Donner accès au réseau en toute sécurité aux collaborateurs nomades

Le point clé de la réponse
La solution déployée comprend un tunnel IPSEC[26] site à site sécurisé permettant la communication avec le site distant. Plusieurs comptes clients nomades (VPN SSL)[27] ont été créés pour répondre au besoin de mobilité. La solution offre à cette start-up la flexibilité indispensable à son organisation, en toute sécurité.

CAS • 3 Business Center innovant

Une plateforme logistique d'import-export de plus de 200 000 m², destinée à accueillir bureaux, entrepôts et commerces, souhaite s'équiper d'un réseau LAN[28] complet et sécurisé.

Les objectifs
- Apporter à chaque local un pack de services complets (Internet, voix, Wi-Fi, etc.)
- Sécuriser et étanchéifier les flux entre ces différents services

Le point clé de la réponse
Un service de télécommunication a été déployé au travers de la mise en place d'une infrastructure de réseaux LAN multiservices. Une véritable autoroute digitale desservant les besoins en télécommunications. La solution déployée est destinée à assurer une sécurité périmétrique vis-à-vis des menaces extérieures. Elle est également destinée à étanchéifier les services déployés sur le réseau local, ce qui évite les risques d'effet « domino ».

(26) IPSEC : Internet Protocol Security (Protocole de sécurité Internet)
(27) VPN SSL : Virtual Private Network (Réseau privé virtuel) Secure Sockets Layer (couche des "sockets" sécurisés)
(28) LAN : Local Area Network (Réseau Local)

LE COMPORTEMENT HUMAIN : PREMIÈRE MENACE EN MATIÈRE DE SÉCURITÉ

35 % des incidents de sécurité rencontrés par les entreprises sont causés par une imprudence d'un collaborateur(29). Maladresse, inconscience, empressement, le facteur humain se révèle être, bien souvent, le maillon le plus faible de la chaîne de sécurisation des systèmes d'information. Malgré les garde-fous, les verrous, les restrictions, les précautions... sans une prise de conscience profonde et sincère de l'utilisateur final des enjeux liés à la sécurité informatique, la protection n'atteindra pas un niveau optimal.

Quelques pratiques ayant fait leurs preuves...

(29) Étude PWC - La fraude explose en France : La cybercriminalité au cœur de toutes les préoccupations

Formez le management

En impliquant le management, en le sensibilisant lui-même à l'ensemble des bonnes pratiques liées à la sécurisation du système d'information, le message sécuritaire sera plus facilement distillé au quotidien à l'ensemble des collaborateurs. Les managers doivent être en mesure de relayer ces préceptes pour maintenir une pression saine sur les enjeux.

Fixez un cadre précis

Pour responsabiliser les collaborateurs, établissez une charte informatique claire. En une dizaine de points, définissez les règles de base. En couchant sur le papier les pratiques interdites (utilisation d'une clé USB non vérifiée, connexion d'un périphérique personnel sur le réseau Wi-Fi de l'entreprise, obligation de renouvellement mensuel du mot de passe, téléchargement d'applications...), chacun sait à quoi s'en tenir en cas de non-respect des règles.

Touchez vos cibles

Les collaborateurs n'ont pas tous la même maturité technologique. Certains peuvent peiner à s'approprier les discours et préceptes trop théoriques. Chaque point de votre charte informatique devra être accompagné d'exemples précis, reflets de pratiques quotidiennes.

Démontrez pour sensibiliser

L'utilisateur a rarement conscience des risques qu'il prend. Pour le sensibiliser plus efficacement, des ateliers peuvent être organisés en vue de démontrer les conséquences réelles d'une clé USB insérée de manière hasardeuse sur un poste de travail ou en démontrant la faiblesse de certains mots de passe.

Communiquez à intervalles réguliers

Marteler le message est une nécessité. La vigilance de chacun est de nature à s'affaiblir avec le temps. La sensibilisation aux enjeux de sécurité est un processus itératif. A intervalles réguliers, via le réseau social de l'entreprise, ou en diffusant des documents sur l'intranet, effectuez des rappels des enjeux et précautions à prendre au quotidien.

10 QUESTIONS POUR CHOISIR SON PARTENAIRE SÉCURITÉ

La sécurité des réseaux est une affaire trop sérieuse pour laisser une place aux incertitudes. Avant d'accorder votre confiance à un prestataire ou d'opter pour une solution, tentez de répondre aux questions suivantes, afin de mieux cerner vos besoins !

1 Quel est le périmètre d'action du prestataire ?

Dans quelle mesure votre partenaire peut-il vous accompagner au quotidien pour faire vivre le projet ? Conseil, études, ingénierie, déploiement, assistance, maintenance et infogérance... Le périmètre d'action et de responsabilité doit être clairement posé pour assurer un bon niveau de service.

2 Le prestataire est-il force de proposition ?

Préconisation et justification du matériel, normes et technologies à déployer ou encore suggestions de paramétrage et évolution de l'arsenal de protection... Le projet doit être animé et faire l'objet d'ajustements réguliers. Le prestataire doit par conséquent adopter une démarche proactive.

3 Quelles solutions utilisez-vous pour vous protéger des dangers d'Internet ?

Souhaitez-vous maîtriser la navigation sur Internet de vos collaborateurs (filtrage d'URL, contrôle des applications et contrôle des accès) ? Anti-intrusion, Antivirus, Anti spam, filtrage Web et contrôle applicatif, comment ces modules interagissent-ils entre eux et quels peuvent être les leviers d'amélioration ?

4 Savez-vous estimer l'impact qu'aurait une cyberattaque (indisponibilité du système d'information, fuite de données...) envers votre entreprise ?

Avant d'accorder votre confiance à un prestataire, comparez les moyens mis en œuvre pour assurer la garantie du niveau de service (SLA)(30) : garantie de temps de résolution, d'intervention...

(30) SLA : Service Level Agreement (Niveau de qualité de service)

5 Souhaitez-vous administrer, en partie, la configuration de la solution de sécurité ou comptez-vous la déléguer au prestataire ?

Pour accompagner l'évolution de vos usages et de vos besoins, le prestataire doit être en mesure de vous proposer une solution managée à 100 % ou à la carte en vous laissant le contrôle de certains paramètres tels que la gestion des règles de firewall, l'administration des profils de sécurité ou la gestion des comptes utilisateurs.

6 De quelle visibilité en temps réel pourrez-vous disposer sur votre réseau et votre lien Internet ?

Pour assurer la détection la plus efficace des menaces, disposer de tableaux de bord intégrés est un atout majeur. Ils permettent d'identifier les anomalies sur l'utilisation de la bande passante Internet, savoir à quel type d'attaque ou de virus vous êtes confronté. Ils sont une garantie de réaction rapide et appropriée.

7 La solution vous permettra-t-elle de prioriser les flux de données sur votre bande passante ?

À mesure qu'évoluent vos usages, votre organisation, vos effectifs, mais aussi en fonction de la saisonnalité de votre activité, il peut être utile de gérer la bande passante en allouant des pourcentages par application.

8 La solution envisagée permet-elle l'interconnexion de différents sites distants ?

Les entreprises multi-sites sont confrontées à un enjeu d'accessibilité des données lorsque les sites sont éloignés. L'interconnexion doit être effectuée de manière sécurisée via des tunnels IPSEC.

9 Comment la solution vous permet-elle de faciliter l'accès aux données de l'entreprise pour les collaborateurs nomades ?

Une connexion sécurisée (VPN IPSEC ou SSL) doit être établie entre le terminal de l'utilisateur et la solution de sécurité. Cela lui permettant de se connecter de manière sécurisée au réseau et aux applications de l'entreprise via tout type d'accès (Wi-Fi, réseau mobile...).

10 Comment le prestataire peut-il accompagner et anticiper les évolutions, qu'elles soient technologiques ou liées à l'évolution de votre (vos) site(s) et du nombre d'utilisateurs ?

Flexibilité, réactivité, modularité sont autant de qualités que le prestataire devra réunir pour s'engager dans une relation de confiance durable.

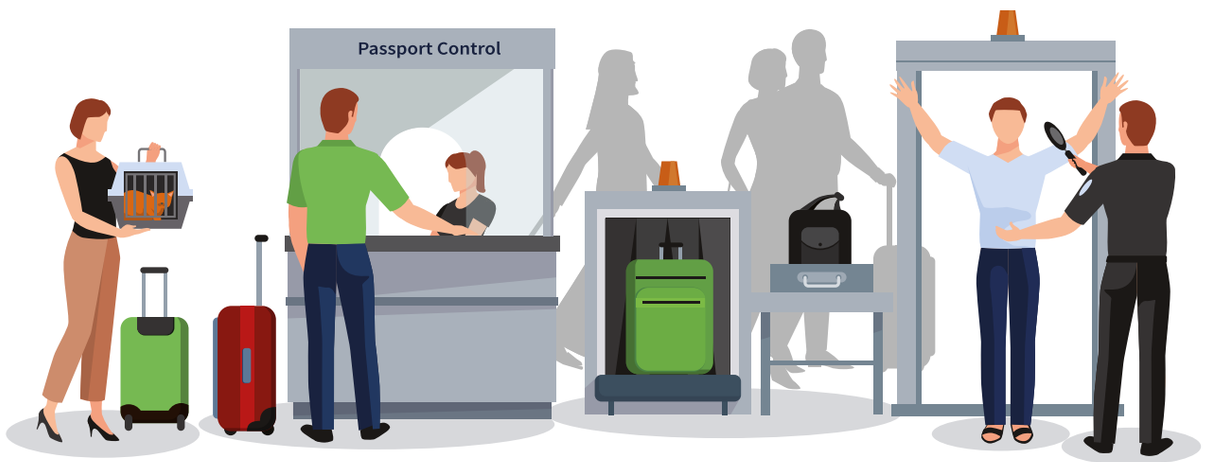
LA RÉPONSE HUB ONE

Hub One a pour mission au quotidien d'assurer une sécurité optimale des réseaux en milieu aéroportuaire.

De cette expertise et de cette expérience, Hub One est parvenu à développer des méthodes, des processus, et des moyens qui constituent autant de réponses opérationnelles aux exigences d'un secteur où la sécurité est une problématique critique et un enjeu de chaque seconde.

Aujourd'hui, Hub One met ce savoir-faire à la disposition des grands comptes et des PME de tout secteur d'activité.

Hub One vous propose des services de LAN Managé et Sécurisé.



Poser un diagnostic

Mieux comprendre pour mieux agir. Avant de déployer des moyens techniques, il faut cerner les usages de votre entreprise, réaliser un audit de la situation (matérielle, technique et humaine) en vue de définir les briques fonctionnelles indispensables à une sécurisation optimale. La qualification de vos besoins est déterminante en amont du projet.

Décrypter les usages

Quand la grille des usages des collaborateurs est établie, il est possible de définir les fonctionnalités nécessaires à une sécurité optimale des infrastructures informatiques et réseau. Antivirus, antipub, filtrage d'URL... l'activation des fonctionnalités s'accompagne d'une analyse permanente du rapport débit/sécurité. L'objectif étant d'assurer une protection optimale sans impact préjudiciable sur la bande passante disponible.

Se préserver des menaces de l'extérieur

L'hostilité ambiante sur Internet, l'insécurité latente vous obligent à mettre en place filtres et garde-fous pour éviter les intrusions dans votre système d'information. Priorisez les flux de données en vous recentrant sur les opérations indispensables à votre activité.

Déployer une sécurité périmétrique

Le risque Zéro est un leurre. En acceptant cette réalité, vous faites le premier pas vers l'efficacité. L'essentiel, en cas d'infection ou d'attaque, consiste à limiter la propagation en déployant des barrières virtuelles entre chaque service. Une sécurité périmétrique qui contribue à endiguer une attaque et à une reprise d'activité plus rapide.

Un accompagnement permanent

Grâce à un maillage resserré du territoire, le réseau d'agences et de partenaires Hub One permet le déplacement rapide d'un technicien pour l'installation ou le remplacement du boîtier physique de sécurité.

Surveiller et analyser à distance

Protéger efficacement un système d'information, c'est être en mesure d'anticiper les menaces en détectant, au plus tôt, les comportements inappropriés ou les vulnérabilités. Avec son outil de surveillance à distance assurée 24H/24 et 7j/7, Hub One peut intervenir avant la manifestation du problème de sécurité en faisant évoluer les règles de sécurité à distance.

Repenser sans cesse la protection

Les modules d'analyses générant des rapports d'activités généraux permettent de détecter les nouveaux usages au sein de l'entreprise. Mesure volumétrique du trafic, détection de pics de bande passante, des données à analyser pour, sans cesse, adapter la protection.

Hub One est un Groupe de services en technologies de l'information et de communication en environnements professionnels.

Hub One conçoit et concrétise la digitalisation des métiers, lieux et usages.

Hub One s'appuie sur son expérience en milieu aéroportuaire pour apporter des réponses sur mesure aux besoins opérationnels critiques et temps réel, aux Grands Comptes et aux PME.

Nos collaborateurs assurent un service de bout en bout, du cœur de réseau au terminal, du déploiement en mode projet jusqu'au maintien en conditions opérationnelles.

Nos solutions et expertises agrègent les métiers d'opérateur télécom, fixe, radio et mobile, d'intégrateur en mobilité et traçabilité, et l'ensemble des services associés.

Filiale du Groupe ADP
500 collaborateurs
4 500 entreprises clientes

Chiffres Groupe Hub One 2016

NOTRE DÉMARCHE RESPONSABLE ET ENGAGÉE

Hub One adopte une démarche volontaire en matière de développement durable et de Responsabilité Sociétale d'Entreprise. Notre stratégie, nos activités et nos solutions sont en phase avec les enjeux environnementaux, sociaux et sociétaux d'aujourd'hui afin de proposer des solutions innovantes qui aident nos clients à être plus vertueux.

Hub One S.A. • Bâtiment Mercure • Continental Square 1 •
2, Place de Londres • 93290 Tremblay en France • France

Hub One Mobility S.A.S. • 5, route de Paisy • 69570 • Dardilly • France

hubone.fr

Une filiale du **Groupe ADP**

Hub One
Une connexion d'avance