

Décembre 2005

SOMMAIRE

EDITO

AGENDA - ACTUALITES

- VEILLE** : RFID, une nouvelle problématique de sécurité P. 3
- ZOOM** : Le *full-disclosure*, côté obscur de la Force ? P. 4
- L'ESSENTIEL** : Externalisation de la sécurité des SI (Outsourcing) P. 5

EDITORIAL

Le sapin de Noël à peine déployé, la galette des rois est déjà en vue ! Cette métaphore festive permet d'établir un bilan très positif de l'année 2005, qui a confirmé la solide reprise du marché de la sécurité, amorcée à la fin 2004.

Selon toute vraisemblance, 2006 devrait voir s'accélérer les investissements des entreprises dans la sécurité de leurs systèmes d'information, de nombreux chantiers structurants (Gestion des identités, mobilité, VoIP, etc.), lourds et complexes à mettre en œuvre, étant lancés ou sur le point de l'être. Les mois écoulés permettent de penser que le regard des décideurs sur la sécurité a favorablement évolué. Cette dernière commence à être réellement considérée non plus en terme de coût mais comme un investissement, chaque euro dépensé permettant potentiellement d'en économiser plusieurs !

Sachant que la part moyenne de la sécurité dans un budget informatique en 2005 ne représente finalement que 2,7%¹, il est facile d'imaginer que le marché de la sécurité a de beaux jours devant lui !

L'équipe ESEC

AGENDA – Sélection de fin d'année

- ⇒ **Panorama de la cybercriminalité 2005 – Cercle National des Armées, 12 janvier 2006, Paris, Place St Augustin**
 Comme chaque année, le CLUSIF présentera les faits marquants de la cybercriminalité pour l'année 2005.
Plus d'infos :<http://www.clusif.asso.fr/>
- ⇒ **Codexpo 2006 : Paris La Défense du mardi 24 janvier 2006 au jeudi 26 janvier 2006**
 Salon dédié à toutes les solutions d'identification automatique qui rejoint Traçabilité 2006.
Plus d'infos :<http://www.tracabilite2006.com/>
- ⇒ **Forum RFID 2006: Paris La Défense du mardi 24 janvier 2006 au jeudi 26 janvier 2006**
 Forum dédié à la technologie RFID. Il proposera un cycle de conférences à la fois pragmatique et novateur : Supply Chain, Gestion des actifs, Sécurité, Gestion des clients, ETC qui rejoint Traçabilité 2006.
Plus d'infos : http://www.tracabilite2006.com/fr/2006/A_salon/E_polerfid.htm
- ⇒ **Solutions Linux + Solutions OpenSource2006 – 31 janvier, 1^{er} et 2 février 2006, CNIT, Paris La Défense**
 Linux et les solutions Open Source ont désormais le vent en poupe et s'imposent de plus en plus dans les entreprises, les services publics et les administrations.
Plus d'infos :<http://www.solutionslinux.fr/fr/index.php>

¹ 2,1% en 2003, 2,4% en 2004. Source : <http://www.zdnet.fr/actualites/informatique/0,39040745,39291462,00.htm>

Décembre 2005

ACTUALITES

BlackBerry, un système parfaitement sécurisé ?

Alors que BlackBerry prône une sécurité parfaite, la BBC fait les frais d'un trou de sécurité... RIM, le fabricant canadien des BlackBerry affirme que le risque d'intrusion, de détournement des messages ou d'attaque est quasi nul. De plus, il dit offrir une solution sécurisée de bout en bout, grâce notamment au chiffage des mails (en 256 bits). Aussi, RIM annonce les atouts du NOC (centre d'opérations de RIM par où transitent les mails) car il sait que ce point est redouté des entreprises qui n'apprécient pas que leurs mails passent par l'Angleterre par exemple en ce qui concerne la zone Europe. Pour

rassurer au mieux le client, RIM rajoute qu'il a obtenu des certifications gouvernementales (Etats-Unis, Canada, Australie). Peu de temps après, la BBC doit suspendre son réseau BlackBerry suite à un bug massif. En effet, les utilisateurs se sont rendus compte que certains mails étaient mal routés. RIM a immédiatement réagi en dédramatisant la situation : pour le fabricant, seule une ancienne version est concernée par ce bug mystérieux et le patch existe déjà.

Pour en savoir plus : [Article Silicon.fr](#)



Sony ouvre les portes aux hackers

Deux chercheurs américains ont découvert que Sony BMG utiliserait un système pour protéger ses CD audio contre la copie. Il s'agit en fait d'un « rootkit », généralement utilisé par les hackers qui cherchent à pénétrer sur les ordinateurs de leur victime. Le but du rootkit de SONY est d'empêcher l'utilisateur de désinstaller le système de gestion des DRM (*Digital Right Management*) de sa machine. Mais ça ne s'arrête pas là. En effet, le code malicieux ouvre aussi des brèches qu'un hacker est capable d'exploiter pour pénétrer la machine : quelques programmes les utilisent déjà pour se rendre

invisible sur la machine infectée : Breplibot, Stinx. Sony a alors été obligé de réagir très rapidement pour limiter les dégâts causés sur son image de marque. Pour cela, la firme japonaise a proposé sur son site de télécharger un utilitaire permettant la désinstallation du rootkit... après avoir rempli un formulaire. Il semblerait cependant que plus de 500 000 PC soient déjà infectés.

Pour en savoir plus : [Article de l'Atelier](#)



Internet Explorer 7, toujours dans l'optique « secure »

Le protocole de communication paramétré par défaut ne sera plus SSL 2.0 (Secure Socket Layer) mais TLS 1.0 (Transport Layer Security Protocol). Ce choix de Microsoft a surtout pour but de sécuriser les communications en lignes et notamment les transactions pour le e-commerce. Il est cependant possible que certains sites ne reconnaissent pas le protocole TLS. Dans ce cas, c'est le SSL 3.0 qui sera utilisé. Ces changements vont impliquer un grand nombre de

sites marchands qui vont devoir modifier les pages concernées. Quant aux cybermarchands, ils n'ont donc pas d'autres choix que de s'adapter mais ne s'opposent pas pour autant. Du point de vue des intégrateurs, ils suivront l'évolution comme ils le font pour chaque amélioration du navigateur dans le but d'assurer aux clients la sécurité de leurs transactions.

Pour en savoir plus : [Article de Zdnet](#)



Première faille critique diffusée sur la Voix sur IP

Ce que les experts redoutaient depuis un moment semble être arrivé : des hackers auraient réussi à manipuler la trame IP utilisée dans les systèmes pour la Voix sur IP et auraient ainsi pu détourner des appels longue distance. Déjà, les PABX étaient la cible des attaquants mais ces derniers pouvaient facilement se faire tracer par la ligne téléphonique. Cette fois, le hacker a juste besoin d'un accès réseau à l'entreprise avec l'attaque « par rebond ». De plus, les attaquants auraient trouvé le moyen de manipuler les codes de

taxation utilisés par les sociétés de facturations. Les outils tels que le CallManager de CISCO et la solution open source Asterisk sont d'ailleurs vulnérables à ce type d'attaque. Les experts dans le domaine de la Voix sur IP mis au courant ont alors engagé des contrôles sur tous les commutateurs, même les vieux commutateurs type LUCENT 5ESS qui feraient partie des systèmes vulnérables.

Pour en savoir plus : [Article de vulnerabilite.com](#)

VEILLE TECHNOLOGIQUE

⇒ RFID : une nouvelle problématique de sécurité ?

📁 *La techno : rappels sur la RFID (Radio Frequency Identification)*

La puce RFID (appelée aussi « tag ») est composée de la puce elle-même pour contenir les informations et d'une antenne pour envoyer et recevoir des informations. Ensuite, une batterie peut être ajoutée, ce qui permet entre autre de rendre la puce RFID active et non plus passive. Elle envoie alors des informations en continu et non plus à la demande du lecteur. Ce dernier est composé de trois antennes UHF

différentes et disposées différemment. Cette technologie, vous la côtoyez déjà tous les jours avec votre pass Navigo, votre pass pour entrer dans un immeuble ou pour démarrer votre voiture. Nous pouvons utiliser la RFID partout et même sous la peau mais son usage doit être réglementé.

📁 *Les aspects sécurité*

☞ La sécurisation des échanges

Tout le monde connaît les problèmes de sécurité que pose une communication par ondes radio :

- L'authentification afin de s'assurer que le tag lu n'est pas un tag intrus,
- La confidentialité et l'intégrité des données,
- La disponibilité car les ondes peuvent être brouillées.

Pour la disponibilité, des recherches sont en cours afin que les puces RFID soient les moins sensibles à l'environnement. L'idée est de mettre la puce dans une petite boîte en plastique et d'écartier l'antenne du bord de 6 à 12mm, la distance nécessaire à la puce pour bien émettre même si le tout est contenu dans une boîte métallique par exemple. Pour les autres aspects de la sécurité, le lecteur va instaurer un défi. Tout d'abord, ce lecteur va demander à la puce : « Qui es tu ? ». La puce répond en chiffrant sa réponse (cryptage à clés symétriques). Enfin, le lecteur reçoit le message, le déchiffre et reconnaît ou non le tag.

☞ Les changements dans la sécurisation de l'entreprise :

- La modification du périmètre de sécurité,
- Le changement de règles au niveau de sa politique de sécurité et la création de nouvelles règles spécifiques.

📁 *Les attaques liées à la RFID*

Des attaques peuvent se produire à deux niveaux :

- ☞ L'écoute car un signal radio peut être capté relativement facilement et des personnes ont réussi à le faire à 23m voire 100m de distance selon le sens antenne-tag ou inversement.
- ☞ L'interrogation car on peut se faire passer pour quelqu'un d'autre, obtenir des informations, porter atteinte à la vie privée, localiser ou tracer un objet ou une personne, ...

☞ La normalisation : EPCGlobal

Afin de réguler les procédés, une norme en cours appelée EPCGlobal vise à se rapprocher de l'ISO et de l'AFNOR pour s'imposer et mettre sur le réseau les produits (qui peuvent être issus de tous les secteurs d'activité). C'est alors qu'entre en jeu la société Verisign connue pour la gestion du DNS et pour la certification dans les infrastructures PKI. Au lieu de DNS, nous parlons cette fois d'ONS (pour *Object Name Service*). Nous retrouverons alors des adresses URL comme celle-ci : <nom_produit>.<nom_fabricant>.ons.com. Aussi, l'idée est de mettre en place une certification pour l'authentification des tags. Concernant les technologies, certaines tentent de s'imposer mais il est encore trop tôt pour être sûr que celles-ci feront un jour l'unanimité. Pour le moment, il s'agit d'UDDI pour l'annuaire, SOAP pour les échanges et SAML pour la sécurité. La norme a aussi pour vocation de proposer des standards, de définir des principes et de construire un canevas d'interfaçage pour les webservices nécessaires. Pour arriver à cela, l'EPCGlobal a engagé un partenariat avec la Liberty Alliance. Restent encore des problèmes à résoudre. Par exemple, vu le nombre d'objets susceptibles de circuler sur le réseau, ces derniers nécessitant une adresse IP, il faudra certainement attendre l'IPv6 pour voir arriver concrètement cette normalisation.

De plus, nous sommes confrontés à toutes les failles d'une puce (nécessitant un matériel sophistiqué cependant) ainsi qu'à celles liées au matériel car le support empêche d'implémenter un cryptage fort. Le plus grand risque est de « tuer » la puce (via un équipement que l'on trouve sur le web) et de la rendre inactive : on peut alors sortir d'un magasin avec un objet de luxe sans être contrôlé ou passer un barrage quelconque.

Conclusion / En bref :

La RFID se développe dans la grande distribution (stockage, suivi et distribution de dizaines de milliers de références) mais montre ses limites dans les tentatives discutables d'identification biométrique et biologiques (tatouage sous-cutané d'animaux domestiques, d'êtres humains) liées d'une part à l'éthique, d'autre part à la faiblesse des éléments de sécurité de cette technologie.

ZOOM

⇒ Le *full-disclosure*, côté obscur de la Force ?

📁 *L'affaire Guillermito*

Le 8 mars 2005, Guillaume Tena alias Guillermito, est reconnu coupable de contrefaçon de logiciels et condamné à 5 000 euros d'amende par le TGI (Tribunal de Grande Instance) de Paris, dans l'affaire qui l'oppose à l'éditeur anti-virus Tegan depuis 2002.

Ayant fait appel, Guillermito nourrit l'espoir qu'enfin, une jurisprudence soit la conclusion de ce long épisode, afin de clarifier la trouble situation du « full-disclosure ».

📁 *Le vice et la vertu !*

Sous son appellation barbare, le *full-disclosure* est la démarche qui consiste à publier l'ensemble des éléments techniques relatifs à la découverte d'une vulnérabilité.

Par facilité, les éditeurs rejettent en général la responsabilité d'une éventuelle compromission du SI sur ces découvreurs de failles technologiques alors que ces mêmes éditeurs ont le devoir moral et commercial de remédier rapidement aux « trous de sécurité » de leurs produits.

Si la démarche est extrêmement louable et fortement appréciée par de (trop) rares éditeurs de logiciels, le pendant de cette activité est bien évidemment la possible utilisation d'une faille par des personnes mal intentionnées : les créateurs de codes malveillants (vers, virus, chevaux de Troie, etc.) et les pirates informatiques.

Pour mémoire, rappelons que le délai moyen entre la publication d'une faille et son exploitation par un ver est d'environ 10 jours !

📁 *Les failles de sécurité, nouvel Eldorado numérique*

Alors que la société *Red Database Security*, spécialisée dans la sécurité des bases de données Oracle, s'étonne avec une fausse naïveté que certaines failles classiques (CSS) ont plus de 720 jours (!), d'autres éditeurs tels que Sybase et même Microsoft ont décidé de travailler en étroite liaison avec les chercheurs de failles.

type « Code Red » ou « Nimda » témoignent de l'efficacité de ces attaques, reposant sur des vers qui ciblent une vulnérabilité non corrigée affectant un nombre très important de machines (on pense tout de suite à Microsoft qui a fait depuis de la sécurité la pierre angulaire de ses développements actuels et à venir).

Alors qu'Oracle n'a toujours pas fixé certains bugs critiques au bout de 650 jours, certaines sociétés commerciales (3Com avec son programme « Zero Day Initiative », iDefense avec « VCP ») ont initié de véritables programmes de rémunération visant à récompenser les chercheurs de failles. Deux approches radicalement opposées qui ont chacune leurs inconvénients. En censurant certains détails techniques relatifs à une vulnérabilité, l'éditeur prend le risque qu'un pirate peu scrupuleux s'engouffre dans la brèche. L'histoire encore récente des épidémies de

D'un autre côté, quelques pirates ont tout de suite vu l'opportunité financière en négociant (le terme « chantage » semble plus à propos) leurs talents, loin de l'esprit initial qui voudrait que l'éditeur soit averti avant la publication officielle afin qu'il ait le temps de développer un correctif. Et que penser de ces sociétés qui ne récompensent pas les chercheurs mais revendent chèrement (entre 50 000 et 100 000 dollars !) des listes de vulnérabilités non publiées à leurs clients ?

Conclusion / En bref :

Au tout début du mois de septembre 2005, un informaticien indépendant révélait les faiblesses de la carte Vitale. L'affaire a été fortement médiatisée (rappelez-vous également de l'affaire Humpisch, du nom de cet expert qui a été poursuivi pour avoir dénoncé et prouvé les faiblesses de la carte bancaire il y a quelques années) mais ces chercheurs ne doivent pas être confondus avec le monde trouble et sauvage de la piraterie numérique.

La solution aux poursuites² judiciaires de ces personnes consiste probablement à créer un processus légal d'échange collaboratif où les chercheurs seraient rétribués en fonction de la criticité des failles découvertes mais où également les éditeurs prendraient l'engagement de rapidement corriger ces failles. Marcus Ranum, expert et pionnier de la sécurité, propose dans ce cadre de créer un organisme indépendant qui agirait en tant que tiers de confiance chargé de gérer la divulgation des vulnérabilités entre chercheurs et éditeurs.

² Reportez-vous aux détails de l'affaire Guillermito sur <http://www.frstirt.com/actualite/08312004.Guillermito.php>

Décembre 2005

L'ESSENTIEL

⇒ Externalisation de la sécurité des Systèmes d'Information (Outsourcing)

Réflexion générale

La décision d'externaliser (*outsourcer*) la sécurité du réseau est une décision difficile. Les enjeux étant importants, il ne faut pas s'étonner des réactions de rejet lors de l'évocation du sujet.

Les promesses de l'externalisation sont attractives. La possibilité de renforcer la sécurité du réseau sans engager une demi-douzaine de spécialistes et dépenser une fortune ne peut être ignorée.

Les risques de l'externalisation sont réels. Les expériences de sociétés mettent en évidence qu'un mauvais choix de prestataire peut s'avérer catastrophique.

Critères de décision à la sous-traitance de la sécurité des SI :

Que faut-il externaliser ?

Les sociétés ne vont pas tout externaliser, simplement parce que certaines choses ne peuvent pas être correctement délocalisées vers une entité externe, soit parce qu'elles sont trop proches du cœur de métier, soit parce que le coût devient prohibitif, ou plus simplement à cause d'un problème d'échelle. Savoir quoi outsourcer est la clé.

Les soins médicaux offrent un exemple similaire particulièrement adapté à l'externalisation. Tout le monde utilise l'outsourcing pour sa santé, vous n'êtes pas votre propre médecin. Personne ne va non plus embaucher son propre médecin. Chacun apprécie d'ailleurs les services externalisés : l'ambulance qui arrive rapidement, les experts médicaux qui traitent le problème sans avoir à se préoccuper de leur coût ou de leur nombre et prêts à faire leur maximum pour vous soigner, sachant que le coût sera supporté (en majeure partie) par l'assurance. Il y a bien sûr les aspects que nous n'apprécions pas : les hôpitaux mal équipés, en sous effectif, qui ne fournissent pas les spécialistes requis à votre problème, les surcoûts éventuels.

Notre santé est de notre responsabilité, nous ne voulons pas qu'un tiers décide de vie et de mort pour nous. Pourtant, pour ces décisions ô combien importantes, nous faisons appel à des ressources externes.

La sécurité réseau n'est pas différente. L'expertise doit être externalisée : les recherches de vulnérabilités, le consulting, l'analyse après incident, ... Seul le management ne doit pas être externalisé.

Le critère différenciateur entre deux prestataires est la qualité du service rendu. Le consulting est un service rentable, y avoir recours pour des besoins précis en est le meilleur exemple. Certaines sociétés offrent ce genre de services : achat de certificats, études de vulnérabilités à distance, ...

Décider s'il faut externaliser ou non la sécurité est difficile. Décider de ce qui doit l'être et vers qui l'est encore plus. Ces dernières années de nombreuses sociétés offrant différents types services sont apparues sous le terme de MSSP (Managed Security Services Provider).

Les analystes se perdent à catégoriser les services offerts. Une société s'occupe des pare-feux, telle autre des vulnérabilités, une autre encore définit les politiques ou s'occupe des IDS.

La société qui achète le service devient propriétaire du management et du contrôle de l'information. Les services offerts sont utiles, performants, adaptés, acheteur et vendeurs sont gagnants.

Pourquoi externaliser la sécurité ?

L'argument majeur de l'externalisation est financier : une société peut disposer d'une expertise en sécurité bien moins cher en utilisant un prestataire externe qu'en embauchant une personne. Prenons le monitoring par exemple : un monitoring efficace est un monitoring constant : une attaque peut arriver à n'importe quel moment de la journée, n'importe quel jour.

Développer un service de détection et de réponse est évidemment possible, mais va coûter cher à mettre en place et à maintenir. Il faut prévoir un nombre conséquent de personnes pour pallier au problème de vacances, de temps de repos, un manager. Sans compter qu'il faut savoir retenir ce personnel au travail assez stressant et parfois ingrat : des temps de surveillance très calme, puis une crise soudaine, puis un retour au calme.

C'est pourquoi l'outsourcing est la solution. En reprenant l'exemple du médecin, il n'est pas nécessaire d'en disposer d'un de façon quotidienne par contre il se peut que l'on doive recourir au service d'un spécialiste. Mais comment choisir le bon spécialiste ? Externaliser la supervision de son système est la garantie d'avoir le bon spécialiste au bon moment, surtout si ce spécialiste se tient régulièrement au courant des dernières techniques, vulnérabilités, produits, outils... Les sociétés d'externalisations ont le budget nécessaire pour maintenir une équipe performante.

Décembre 2005

Comment choisir un prestataire ?

Il est difficile de définir ce qu'est une bonne et une mauvaise sécurité informatique, tout comme il est difficile de choisir entre un bon et un mauvais soin médical avant de l'avoir expérimenté, tout simplement parce que nous ne sommes pas nous-même des experts.

Choisir une société réputée est généralement une bonne pratique, aussi bien dans le domaine de la sécurité que dans le domaine médical. Certaines sociétés MSSP peuvent aussi avoir des conflits d'intérêt et doivent être évitées. Certaines offrent l'outsourcing aussi bien que de la sécurité et du monitoring. C'est un point délicat : si le prestataire découvre un problème (via monitoring), va-t-elle m'avertir ou corriger sans me le dire pour ne pas me déranger ? Les sociétés qui commercialisent et gèrent des produits de sécurité ont le même problème de conflit d'intérêt.

Il est capital de dissocier management de sécurité et monitoring.

La situation financière de la société choisie doit être prise en considération ; qui voudrait établir une relation de confiance durable avec un médecin qui va partir en retraite ?

 **Suite et fin ...**

Ce dernier point est crucial dans le choix que devra faire l'entreprise pour savoir si elle doit externaliser ou non sa sécurité des SI. : est-ce bien le cœur de métier de l'entreprise ?

Le sous-traitant dispose de consultants et d'ingénieurs compétents dans le domaine de la sécurité. Il s'engage par contrat à assurer le meilleur service possible.

Les sociétés ont tendance à pratiquer l'externalisation et préfèrent s'adresser à un spécialiste pour chaque besoin (prestataire pour la cantine, prestataire pour la santé, le nettoyage, ...). La société externalise également la sécurité physique (société spécialisée pour le gardiennage, l'accueil, ...). Les banques y ont elles-mêmes recours (sociétés spécialisées dans le transport de fonds).

En général, les éléments externalisés sont de trois ordres : complexes, importants ou peu intéressants. La sécurité informatique comporte ces trois aspects.

Son importance vient du fait que les sociétés sont aujourd'hui quasiment forcées de s'ouvrir sur le monde internet. Médecins et hôpitaux sont les seuls recours en cas de besoin médical. De même, l'externalisation est la seule manière de traiter les problèmes de sécurité des réseaux actuels.

Il s'agit pour l'entreprise de trancher entre la prise de risque qui consiste à laisser la sécurité informatique à un tiers et la prise de risque qui consiste à ne jamais avoir les compétences nécessaires en interne pour se protéger efficacement.

Décembre 2005

 **Questions à poser à un sous-traitant potentiel (en phase d'investigation) :****Demandez à visiter les locaux**

Commentaires : avant tout et pour vous rendre compte que vos exigences en matière de sécurité seront bien respectées, demandez à visiter les locaux. Si vous ne pouvez pas, méfiez vous des arguments marketing, rendez vous compte par vous même.

Assurez-vous que vos données seront bien protégées (contrôles physiques sur le site)

Commentaires : le prestataire devrait utiliser des badges d'accès, des formulaires à signer en entrée dans les bâtiments , des caméras de surveillance avec une restriction d'accès pour les data centers. Quelques prestataires de service sécurité, interdisent même à leurs employés, l'utilisation des téléphones portables avec caméras et appareil photos...

Assurez-vous que les employés du prestataire ont font l'objet d'un contrôle (profil, parcours, ...)

Commentaires : si le sous-traitant n'entreprend pas de telles démarches, surtout pour ceux qui administreront votre réseau, mieux vaut voir ailleurs. Demandez des exemples de CV.

Toutes les tâches sont elles menées chez le prestataire ou certaines sont elles externalisées ?

Commentaires : si c'est le cas, vous n'aurez en gros aucune visibilité sur qui accède à vos ressources, à votre réseau, à vos données... Si des tâches sont effectuées à l'étranger, que faire en cas de vol ou de pertes de données ? quels seront les recours internationaux ?...

Le prestataire emploie t'il des techniciens à plein temps ?

Commentaires : si ce sont des employés en CDD, demander combien de temps ils ont été présents en entreprise. En cas d'un haut turnover, votre réseau ne serait administré que par des débutants.

Le prestataire travaille t'il pour des concurrents directs ?

Commentaires : si c'est le cas, assurez vous que les mêmes ingénieurs et techniciens ne travailleraient pour les deux comptes. Ceci paraît en pratique difficilement envisageable.

Que propose le prestataire comme plan de secours en cas de sinistre survenant chez lui ?

Commentaires : le service pour lequel vous payez est il dans tous les cas assurés ?

Le prestataire est-il audité ?

Commentaires : le prestataire devrait l'être régulièrement, demandez des preuves.

Le support est-il adapté à vos besoins ?

Commentaires : si vos applications sont critiques, le prestataire met il en œuvre un support adapté 24/24, jours fériés, ...

Le prestataire fournit-il une assurance en cas de non respect des engagements ?

Commentaires : quelles sont les indemnités en cas de non respect des engagements de disponibilité de vos systèmes ?