



> EXPLOITATION

L'INFOGÉRANCE DE LA SÉCURITÉ N'EST PLUS TABOU

Hier encore impensable pour les grands comptes, l'externalisation de la sécurité commence à convaincre. Mais les entreprises cantonnent toujours les prestataires à un rôle d'alerte.

CHIFFRE CLÉ

3,2 milliards de dollars

Le poids du marché de l'info-gérance de la sécurité dans le monde en 2006, selon Gartner. Ce secteur croît d'environ 20 % par an.

« **L'**évolution des mentalités est nette. » Pour Hervé Morizot, directeur de

XP Conseil, société de conseil appartenant à Devoteam, le souci du RSSI consiste aujourd'hui : industrialiser le maintien opérationnel de la sécurité, afin de se concentrer sur des sujets à valeur ajoutée. Une évolution qui, peu à peu, a gommé les réticences des entreprises à l'égard de l'info-gérance de la sécurité, vue, il y a encore peu, comme une perte de contrôle sur un domaine sensible.

Pour Gérard Souyri, directeur marketing et partenariats de Thales Security System, un prestataire spécialisé, plusieurs effets expliquent l'intérêt des entreprises, notamment des grands comptes : « La volonté de se concentrer sur les métiers, tout en contrôlant les coûts. Le besoin de tracer les événements de



Le centre opérationnel (SOC) de Thales Security System à Meudon (92) assure une supervision permanente des équipements.

sécurité pour faire face aux contraintes réglementaires. La complexité du sujet du fait de la multiplication des technologies. » Car si les équipes internes de sécurité ont gagné en maturité, elles peinent à se tenir à jour face aux perpétuelles évolutions technologiques ou aux sorties de nouveaux produits.

« C'est la gestion dans la durée des compétences qui pose problème, car avec le temps se creuse un écart entre la politique de sécurité définie par l'entreprise et les pratiques réellement constatées », avance Philippe

Launay, responsable des offres infrastructures de Sodifrance, un prestataire qui compte 40 à 45 clients pour son offre d'info-gérance parmi les comptes intermédiaires. « Avec l'externalisation, les entreprises achètent une garantie de bon fonctionnement, grâce à des experts qui ont connu de multiples cas de figure. » Autre bénéfice : les entreprises peuvent ainsi récupérer une surveillance 24 heures sur 24 et 7 jours sur 7, sans avoir à gérer les astreintes des salariés.

Définir un périmètre

Les compétences en interne restent cependant nécessaires pour piloter le projet et assurer l'interface avec le prestataire, notamment au moment de la mise en place du service. « Le prestataire a besoin d'interlocuteurs techniques, mais aussi fonctionnels », abonde Yann Fareau, responsable de l'activité technologies de la sécurité de XP Conseil. Le cabinet spécialisé Hervé Schauer Consultants recommande d'ailleurs de ne franchir le pas que si on dispose déjà d'une expérience de l'info-gérance.

Parallèlement à cette évolution des mentalités, l'offre s'est étoffée. A l'administration d'équipements, comme les antivirus et les pare-feu, sont venus se greffer les audits de vulnérabilité, qui permettent de dresser un état des lieux périodique du périmètre de sécurité de l'entreprise, et la supervision des équipements, qui consiste à corriger les alertes des différents équipements et, éventuellement, à intervenir pour parer une attaque. Autour de ces briques fondamentales gravitent d'autres services comme la validation des procédures dans un environnement de test, l'administration à distance des

QUELQUES OFFRES D'EXTERNALISATION DE LA SÉCURITÉ

Prestataire	Offre	Commentaires
Cyber Networks (www.cyber-networks.fr) ISS (www.iss.net)	Management à distance des composants, reporting (y compris propositions d'action et veille), maintenance matérielle et logicielle. Gestion à distance de la sécurité des serveurs, réseaux et postes de travail (y compris mobiles), supervision de pare-feu, détection d'intrusion et audits de vulnérabilité.	Avant tout intégrateur, Cyber Networks dispose d'une bonne expérience de l'info-gérance. SOC situé à Paris. Editeur de logiciels de sécurité et concepteur de serveurs spécialisés, Internet Security Systems a élargi son offre à l'info-gérance.
Securalis (www.securalis.com) Sodifrance (www.sodifrance.com)	Supervision de pare-feu, de RPV, d'antivirus, d'outils de filtrage de contenus, de serveurs d'authentification, de sondes de détection d'intrusion. Gestion de la sécurité des accès (pare-feu, sondes...), des contenus (filtrage, antivirus), des données et des infrastructures (jusqu'au site de secours). Télé-administration et supervision.	Société de services spécialisée, Securalis propose une offre de supervision assez complète. Offre de conseil également. Venu de l'info-gérance, Sodifrance propose un ensemble de services dépassant la simple télé-administration d'équipements pour flirter avec la continuité de service.
Symantec (www.symantec.fr)	Gestion de pare-feu, de sondes de détection d'intrusion, d'antivirus, de boîtiers spécialisés. Surveillance du respect des politiques de sécurité. Audits de vulnérabilité.	L'offre vient du rachat d'un spécialiste (Riptech). Couverture mondiale avec plusieurs SOC répartis dans le monde entier.
Thales Security Systems (www.thales-security.com)	Corrélation des alertes (avec le logiciel NetForensics), gestion des vulnérabilités, hébergement sécurisé, validation des procédures et mises à jour, veille.	Spécialisée dans les grands comptes (banques, administration, services, industrie), la société dispose d'une solide expérience dans cette activité.
Ubizen (www.ubizen.com)	Gestion des équipements (pare-feu, sondes, RPV, routeurs...), corrélation d'alertes.	Présente sur ce créneau depuis 1995, la société est spécialisée dans l'info-gérance de sécurité.

A cette liste de « spécialistes » s'ajoutent d'autres catégories d'acteurs : des opérateurs télécoms (Equant, AT&T), des SSII généralistes (CSC, EDS...) ou des fournisseurs d'infrastructures (IBM, Unisys...)

SOURCE : LMI



LES IDÉES À RETENIR

> En choisissant l'infogérance, les entreprises allègent leur fardeau en ce qui concerne la mise à jour des compétences.

postes nomades, la validation des patches, la veille technologique, etc.

A partir de ce canevas de base, l'entreprise doit définir le périmètre de son infogérance. Tout est envisageable : d'une simple gestion des antivirus en mode hébergé à la supervision et intervention sur tous les équipements (pare-feu, sondes, antivirus, etc.). « La supervision en reste à ses balbutiements, tempère Yann Fareau. Certes, cinq ou six grands comptes français ont mis cette fonction en infogérance. Mais la relation entre le prestataire et l'interne est complexe. Les grands comptes n'externalisent souvent que la détection et le diagnostic. Pour les interventions, ils préfèrent encore repasser par un système d'astreinte en interne. Sinon, il leur faudrait accepter les interruptions de service effectuées par le prestataire. » Avec les conséquences

financières que cela comporte. Un mode difficile à gérer dans le cadre d'une relation contractuelle.

Risque d'atrophie des compétences internes

Autre caractéristique de l'offre : elle émane d'acteurs très différents : opérateurs télécoms, SSII ou prestataires spécialisés, éditeurs de logiciels désireux de muscler leur offre de services. Les premiers proposent à la fois l'hébergement et l'administration des équipements, dans le cadre d'offres de réseau privé virtuel. Tandis qu'avec SSII et éditeurs, le matériel reste dans l'enceinte de l'entreprise, puisque ces prestataires repartent de l'existant. Seule la supervision s'effectue depuis un site distant, le SOC.

Dans un document portant sur la manière de choisir un presta-

> A l'origine tournée vers les antivirus et les pare-feu, l'offre s'élargit aux audits de vulnérabilités et à la supervision des alertes.

taire d'infogérance de services de sécurité (MSSP), Gartner recommande notamment de veiller à la présence de compétences spécialisées dans le management des contrats d'externalisation au sein des équipes du prestataire. La maîtrise des techniques ne suffisant pas à asseoir une relation avec une entreprise. Ou encore de vérifier l'exhaustivité et la qualité de la documentation des processus de gestion de la sécurité fournie par le MSSP. Sans oublier d'évaluer la richesse du portail sécurisé que proposent les prestataires à leurs clients (gestion des modifications, reporting). Pour Gartner, en choisissant l'externalisation, une entreprise risque d'atrophier sa propre expertise en matière de sécurité. Le prestataire doit fournir suffisamment d'informations techniques et des outils d'analyse permettant à

Le prestataire doit fournir à l'entreprise des informations techniques et des outils d'analyse pour garder les équipes internes à niveau.

l'entreprise de conserver en interne la connaissance de ses défenses. Au minimum, ces rapports doivent renfermer les changements de règles de sécurité ou de configurations, une liste des alertes (par ordre de priorité) et des informations sur les nouvelles menaces pouvant nécessiter une adaptation des règles en vigueur.

Soigner le contrat

Comme dans toute relation avec un prestataire, le juge de paix n'est autre que le contrat. D'où l'importance de la négociation de ses termes. « Parmi les points clés figurent les engagements contractuels quant au temps de réaction sur incident ainsi que les processus mis en œuvre (par exemple lors de la correction d'un événement jugé sévère ou grave), explique Gérard Souyri. Il s'agit également de bien détailler la limite de responsabilité de chaque partie et le choix de la formule correspondante. » Par exemple : l'option supervision aboutit à prévenir les équipes internes d'un client lors d'une attaque alors que l'option administration conduit à intervenir. Les limites de l'intervention du prestataire doivent donc être clairement précisées, en balayant toutes les hypothèses.

Le montant de l'abonnement mensuel est calculé d'après plusieurs facteurs : nombre d'équipements concernés, typologie et puissance de ces équipements, nature du service attendu (supervision, administration...), durée du contrat, délai de réaction sur incident sur lequel s'engage le prestataire, etc.

Enfin, comme dans tout contrat d'infogérance, l'entreprise devra veiller à la réversibilité du contrat, afin d'anticiper le retour des services externalisés en interne, mais aussi aux clauses permettant le transfert du contrat à un autre prestataire. Une question élémentaire de gestion des risques qui ne devrait pas échapper aux RSSI. ■

REYNALD FLÉCHAUX
rfléchaux@idg.fr

MOTS-CLÉS MSSP

Managed Security Service Provider. Prestataire d'infogérance de services de sécurité.

RSSI

Responsable de la sécurité des systèmes d'information.

SOC

Security Operation Center.

Centre opérationnel à partir duquel les prestataires supervisent les équipements de leurs entreprises clientes. Un SOC est généralement ouvert 24 heures sur 24, 7 jours sur 7.

EN SAVOIR PLUS

www.hsc.fr/ressources/articles/infogérance/infogérance.pdf

Comment choisir son fournisseur de services d'infogérance en sécurité ? Une synthèse du cabinet Hervé Schauer Consultants abordant tous les points d'une démarche d'infogérance de la sécurité



MISE EN ŒUVRE

UN RÉSERVOIR DE COMPÉTENCES POUR LES POMPIERS



Les astreintes sont assurées par les techniciens du SDIS, plutôt que par Sodifrance. Ce qui abaisse le coût de la prestation.

Créé au début des années 2000, comme ses homologues des autres départements, le Service départemental d'incendie et de secours (SDIS) des Côtes-d'Armor (22) partait, sur le plan informatique, d'une feuille blanche. « En 2001, j'ai reçu comme objectif de créer le SI du SDIS », résume Hervé Guihard, le DSI. « En matière de sécurité, je me suis vite rendu compte que je n'arriverais pas recruter une personne couvrant toutes les compétences requises. » Le SDIS, qui affiche de fortes exigences opérationnelles (la structure regroupe le centre de traitement des alertes et la salle de gestion de crise du départe-

ment), décide alors d'externaliser une partie de sa sécurité chez Sodifrance. « Nous conservons en interne tous les services de proximité (maintenance de parc et d'applications, gestion des bases de données et du décliné). » Pour le reste (gestion des éléments actifs de réseau, des pare-feu, de l'antivirus, filtrage des flux, supervision de serveurs, etc.), quatre personnes travaillent chez le prestataire pour ce SDIS de 2 200 personnes. Une réunion de suivi du contrat a lieu chaque mois. Pour Hervé Guihard, la rapidité d'intervention ne constitue pas réellement un critère dans le choix d'un prestataire : « Il se montre rapide de toute façon. Mieux vaut s'attacher à vérifier qu'une documentation du site (paramétrages, configurations...) est tenue à jour chez le prestataire. Et affiner le reporting pour qu'il nous permette d'anticiper sur l'évolution de notre système. » Le DSI envisage désormais de demander à Sodifrance la prise en charge des alertes gérées par le SDIS jusqu'au pompier. ■ R. F.

> LA SOLUTION ADOPTÉE

Externalisation de la gestion des éléments actifs de réseau, des pare-feu, de l'antivirus, du filtrage des flux, de la supervision des serveurs, etc., chez Sodifrance. Coût annuel : entre 80 000 et 90 000 euros.