

Prestations & méthodes

Les bonnes pratiques

En sécurité, l'organisation prime souvent sur la technique. Et cela est vrai chez HSC comme chez ses clients. C'est pourquoi l'agence respecte un cadre strict lors de ses audits comme lors de ses tests d'intrusion. Ces derniers suivent ainsi une série de phases très codifiées, qui commence par la collecte d'informations publiques concernant les systèmes à tester (bases whois, forums de discussions techniques, serveurs DNS, archives diverses...), puis une phase « plus active et pas vraiment discrète », précise Thomas Seyrat, d'identification des cibles potentielles : quelles machines sont accessibles ? À l'aide de différents scanners et d'outils développés en interne, les consultants tentent alors de « cartographier » le réseau, ses services et éventuellement ses règles de filtrage. Enfin, ils exploitent les informations collectées précédemment afin d'identifier le chemin le plus court vers le cœur du réseau

de l'entreprise. Mais qui dit « *chemin le plus court* » dit aussi absence d'exhaustivité : les consultants iront à la faille la plus simple à exploiter et ne chercheront pas au-delà.

Le standard BS7799

Pour prendre de la hauteur et être capable de gérer la sécurité, HSC intègre l'audit dans une démarche globale et s'appuie pour cela, sur la norme BS7799 (ou ISO 17799), véritable garante de bonnes pratiques de sécurité. Objectif : « *rétablir le lien parfois rompu entre la direction et sa vision à long terme, d'une part, et l'opérationnel qui fait ce qu'il peut à un instant donné, d'autre part* », explique Alexandre Fernandez. La norme BS7799 permet ainsi la mise en place d'un système de gestion de la sécurité dans la durée et basé sur le modèle itératif PDCA (Plan, Do, Check, Act). La sécurité est un processus et c'est ainsi que la conçoit la méthode BS7799.



HSC offre des prestations d'audit et de tests d'intrusions dans un cadre contractuel et déontologique strict.

Elle permet d'appréhender la sécurité de manière globale, en incluant les hommes, les systèmes et, surtout, les processus par lesquels les premiers exploitent les seconds. HSC met en œuvre aussi bien la première partie de ce standard (un guide des bonnes pratiques) que la seconde, plus concrète, baptisée BS7799-2:2002. Elle décrit les mesures terrain à prendre pour créer une ISMS (Information Security Management System). L'avantage d'une telle démarche est une meilleure gestion et un meilleur contrôle de la sécurité du système d'information, ainsi que l'assurance d'une reconnaissance internationale. ■

L'ÉDITORIAL



par Hervé Schauer

Célébrer aujourd'hui les 15 ans d'expertise d'HSC nous offre l'occasion de mener une réflexion de fond sur le métier de la sécurité des systèmes d'information. Quels seront les enjeux auxquels devront faire face, demain, les RSSI ?

Leur métier – notre métier – a profondément évolué ces quinze dernières années. La profession reste, bien sûr, technique et l'excellence dans ce domaine demeure essentielle. Mais ce n'est plus la seule exigence : la sécurité des systèmes d'information passe plus encore aujourd'hui qu'auparavant par une meilleure organisation de l'entreprise, voire, bien souvent, une réorganisation...

Le rôle des services centraux, par exemple, illustre parfaitement ce besoin. À l'heure où la téléphonie converge vers le monde IP, où mes consultants découvrent régulièrement des incidents liés aux PABX, pourquoi ces derniers sont-ils parfois gérés par le service en charge des tables et des chaises et non par le service informatique ? Et quid des assistants personnels et des téléphones mobiles GPRS ou UMTS qui déportent des informations confidentielles de l'entreprise ? Des copieurs équipés de disques durs et branchés sur le téléphone dénués de toute protection ?

Voici finalement ce qui pourrait être le premier conseil sécurité pour cette décennie à venir : pour maîtriser le parc informatique, sachez d'abord vous (ré)organiser ! ■

1989-2004

15 ans au service de votre sécurité

Où étiez-vous il y a quinze ans ? Souvenez-vous, c'était l'époque du minitel, des réseaux pas encore vraiment IP et du règne d'Unix. HSC est né précisément au carrefour de toutes ces tendances : venu à la sécurité parce qu'il fallait bien protéger ses serveurs minitel des assauts de la concurrence dans la jungle qu'était le 3615, déjà créateur d'un groupe de travail sur la sécurité Unix, Hervé Schauer a fondé HSC avec deux objectifs en tête : assurer des formations sur la sécurité des systèmes Unix et TCP/IP et auditer cette dernière.

Un contributeur reconnu

Quinze ans plus tard, la sécurité a évolué comme peu d'entre nous ne pouvions l'imaginer alors, et HSC aussi : le cabinet a travaillé, via ses formations ou ses prestations d'audits, pour la quasi-totalité des grands comptes français et des établissements financiers, pour tous les opérateurs téléphoniques et de nombreux ministères. Mieux : il est devenu un contributeur reconnu parmi le petit monde de la sécurité internationale grâce au déve-

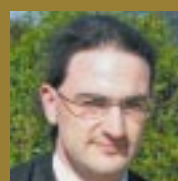


Consultants, ingénieurs commerciaux ou assistants : l'équipe de HSC accompagne vos projets sécurité depuis quinze ans.

loppement de nombreux outils gratuits, téléchargés à plusieurs milliers d'exemplaires à travers le monde (dont wifiscanner ou ssltunnel pour les connaisseurs). Son site web, qui offre aussi en téléchargement libre les supports de plus de 200 présentations très techniques, compte parmi les sites spécialisés les plus fréquentés en France. Ainsi, avec quinze formations au catalogue, la participation active à plusieurs groupes de travail spécialisés ainsi qu'à de nombreuses conférences dans le monde entier et un effectif composé à plus de 80 % de consultants opérationnels, HSC est devenu une référence en matière de conseil sécurité. De quoi célébrer sereinement ses quinze ans ! ■

HSC, aussi à Toulouse

Toulouse, capitale high-tech du grand sud, portail vers l'industrie aéronautique... et seconde implantation de HSC après Paris. Le choix de la Ville Rose est avant tout pragmatique : « *La région a toujours représenté le plus gros volume d'affaire après l'Île-de-France. Nous y avons réalisé nos premiers grands projets innovants, pour le Cnes de*



Denis Ducamp, responsable de l'agence HSC de Toulouse.

Toulouse, puis y avons conquis notre premier grand client industriel, Elf », se souvient Hervé Schauer. En ouvrant son agence toulousaine, HSC a non seulement voulu retrouver ses clients du sud, mais aussi se rapprocher

des nombreux centres de décisions qui s'y trouvent. « On rencontre à Toulouse les centres de sécurité d'entités nationales », poursuit Hervé Schauer, avant d'ajouter que le tissu des entreprises locales est aussi très demandeur de compétences sécurité pointues. « Nous avons beaucoup travaillé en formation pour les SSII de la région. L'avantage d'avoir un bureau sur place est que cela nous permet de créer une relation d'ingénieur à ingénieur, plus humaine », conclut Denis Ducamp, responsable de l'agence Toulousaine. Une agence d'ailleurs de moins en moins Toulousaine, tant ses consultants rayonnent désormais sur le grand sud-ouest, Rennes ou même l'Afrique du Nord ! ■

Une journée d'exception pour 15 ans de collaboration

Des massifs fleuris, une belle pelouse, du soleil et un ciel bien dégagé : cette fête d'anniversaire avait comme un petit air champêtre. Et pour cause, c'est à deux pas du quartier d'affaire de la Défense, au Jardin d'acclimation, que HSC a choisi d'inviter ceux sans qui rien n'aurait été possible : les RSSI des grands groupes, pour qui ses consultants travaillent régulièrement.

Au programme : un accueil chaleureux, un petit déjeuner de bienvenue et largement le temps de parler « *boutique* » entre deux verres, au soleil de cette



première journée de printemps. Dix sessions d'informations animées par des consultants HSC ont ensuite permis de faire le point sur les menaces, techniques et méthodes du moment et, parfois même, d'apprendre une astuce ou deux grâce aux démonstrations pratiques. Ponctuée d'un repas particulièrement

convivial et conclue par un cocktail informel afin de profiter des derniers rayons de soleil, la journée aura permis à la soixantaine de RSSI conviés de se rencontrer, d'échanger, d'apprendre et, aussi, de mettre un visage sur toute l'équipe HSC, pour la première fois réunie ! ■

» Les perles de la sécurité

Pour de nombreux RSSI présents lors de cette conférence, ce fut une révélation : oui, votre réseau sera probablement compromis à la faveur d'une erreur de configuration, d'un oubli ou d'une négligence, plutôt que d'une attaque complexe. Par exemple via les ACL (Access Control Lists) de rou-

terrain. Tout comme l'oubli de règles temporaires dans les pare-feu (pourtant bien pratiques pour tester un applicatif), ou les erreurs d'écriture de ces dernières. Ainsi les règles symétriques (on autorise tous les flux à sortir) sont certes plus simples à concevoir mais elles facilitent aussi de nombreux détournements. Un

fait un relais anonyme utilisable par le tout Internet ! Au cœur de l'entreprise, les consultants HSC découvrent aussi régulièrement des serveurs Unix ou Linux trop rapidement déployés. Un exemple typique : les utilisateurs limités au service FTP doivent, quand on veut les passer en SFTP (FTP sécu-

nier leur offre alors aussi un accès en ligne de commande et l'opportunité d'exploiter à loisir les failles locales du système. Configurations, scripts maison et autres projets réalisés en interne doivent ainsi être observés de près... Leur simplicité de mise en œuvre peut cacher de vraies chausse-trappes. ■

“ J'ai choisi HSC pour son indépendance. Ils savent prendre des positions fortes et argumentées face à n'importe quel acteur du marché ! ”

Éric Wiatrowski, directeur délégué à la sécurité chez Transpac.



» Le piratage des réseaux WLAN

Les WLAN ont le vent en poupe. En se promenant autour du Jardin d'acclimatation, les consultants ont identifié 57 bornes wi-fi, dont 20 disposaient encore de leur identifiant de réseau (SSID) par défaut et 31 n'utilisaient pas de chiffrement. Et tout cela en moins de 30 minutes sur un parcours de 1 500 m. Qu'est-ce que cela signifie du point de vue de la sécurité ? Jérôme Poggi, auteur

du logiciel *wifiscanner* et consultant HSC, en a fait la démonstration aux invités : en rejouant le trafic capturé lors de sa balade ou à l'aide d'une borne installée dans la salle de conférence, il a pu découvrir les SSID des derniers réseaux fréquentés par les machines sous Windows XP (un bug de ce système), démontrer une association « accidentelle » du client à une borne pirate, écouter certains trafics et,

même, tuer net tout trafic wi-fi dans la salle à l'aide d'un simple outil acheté 400 euros sur Internet. Il démontrait ainsi que les meilleures mesures de sécurité logique n'empêcheront jamais un réseau WLAN d'être plus vulnérable que son homologue filaire : il convient alors d'aborder le projet wi-fi de manière globale, en intégrant ces risques particuliers lors de la conception de l'architecture réseau. ■

Une journée sécurité avec HSC

teurs Cisco, qui doivent non seulement être déclarées mais aussi appliquées ! L'oubli semble stupide ? Il est pourtant rencontré sur le

serveur web a-t-il par exemple besoin d'initier des connexions vers l'extérieur ? Sans doute pas... Sauf si sa (mauvaise) configuration en

risé via SSH), tout de même disposer d'un compte sur le système pour que cela fonctionne. S'il n'est pas volontairement bridé, ce der-

» Les failles de type cross-site scripting

Elles sont le fléau des sites web mal développés. Les failles de type *cross-site scripting* (XSS) permettent à l'internaute malicieux de se servir d'un site web vulnérable afin de mener son attaque contre les autres internautes du site... tout en lui en faisant endosser la responsabilité ! Les démonstrations

menées lors de cette conférence par les consultants HSC ont surpris l'assemblée par leur simplicité et leur efficacité : ils ont détourné à loisir des sessions authentifiées sur un site web, provoqué l'exécution de code actif sur l'ordinateur d'un internaute et inséré du code HTML pendant l'affichage d'une page web exist-

tante. Dans ce cas, l'entreprise n'a même aucun moyen de savoir que le contenu qu'elle publie n'est pas celui qui est vu en réalité. Toutes ces attaques exploitent une erreur très courante dans les développements web actuels : le manque de validation des entrées utilisateurs (via des messages soumis à un forum de discussion, les pages HTML générées en dynamique à partir

d'informations collectées dans une URL...). Les solutions existent pourtant : il faut filtrer toutes les entrées en provenance des internautes pour en supprimer les balises et les commandes permettant l'exécution de code dynamique à travers HTML. Une tâche ardue à réaliser après coup mais particulièrement indolore si la sécurité a été pensée dès la conception. ■

» Vulnérabilités et correctifs

C'est le cauchemar des RSSI : comment conserver ses systèmes à jour alors que le temps entre la publication d'un correctif de sécurité et l'exploitation malicieuse de la faille en question se réduit à vue d'oeil (26 jours pour Blaster à l'été 2003 contre un jour seulement pour Witty, au printemps 2004) ? Premier conseil, presque du bon sens celui-là : il faut assurer une veille active en

matière de sécurité, en s'abonnant par exemple à des listes publiques et privées ou à des services d'alerte. Plus tôt le responsable informatique sera prévenu de la disponibilité d'un correctif, mieux il pourra le tester. Et, surtout, prendre les mesures nécessaires à la protection de ses systèmes en attendant son application (telles que l'isolement des ordinateurs mobiles, véritables vecteurs d'épidé-

mies sur le réseau local !). Il faut enfin établir des processus formels de test et de déploiement des correctifs : déterminer les systèmes affectés par la vulnérabilité, puis ceux à patcher en priorité et, enfin contrôler le bon déploiement du correctif. Par exemple, en appliquant un scanner de vulnérabilités. Là encore, la tranquillité est avant tout le fruit d'une bonne organisation interne. ■

» ROSI, quel ROSI ?

Quel retour sur investissement attendre de la sécurité ? Et surtout, comment le mesurer ? Pour Hervé Schauer, il s'agit désormais d'une composante essentielle que les RSSI ne peuvent plus se permettre d'ignorer : « *Puisque les entreprises sont gérées sur la base de justifications chiffrées,*

la sécurité n'a pas le choix : elle doit rentrer dans le moule », explique le fondateur d'HSC. Et fort heureusement, elle peut le faire : il est souvent possible de mesurer l'apport d'une composante de sécurité (un audit, une fonction spécifique, la mise en place d'un processus...) à un projet ou à l'entreprise.

Ces gains peuvent s'évaluer sur plusieurs fronts : diminution des incidents, bien sûr, mais aussi l'amélioration de la productivité, maîtrise des risques (d'où une meilleure allocation des ressources destinées à les couvrir) ou des performances métiers accrues (la sécurité devient alors un avan-

tage concurrentiel). Enfin, la sécurité peut également être vendue comme un outil de « *benchmarking* » servant, justement, à mesurer les gains, en comparant par exemple les incidents de sécurité survenus dans les filiales qui ont entamées une démarche BS7799 et celles qui ne l'ont pas fait. ■

“ La validation de nos choix et de nos procédures sécurité par un cabinet d'experts objectif et indépendant est un atout crucial. ”



Gilles Berthelot, OSSSI de la Brigade de Sapeurs Pompiers de Paris.



“ Pourquoi HSC ? Pour le professionnalisme d'Hervé Schauer. Il est, à mon sens, le meilleur spécialiste sur la place de Paris. ”

Jean-Pierre Belingard, responsable Coordination Sécurité Logique chez PSA Peugeot Citroën.

