le PARIS PHUKET

BANGKOK - CHIANG MAI - PATTAYA

© Jakkaphan Sanitprem

MENSUEL - AVRIL 2016

HACKER OUVERT

Christophe Chommeloux

SafeComs, le gardien de bits

Dans un monde de plus en plus techno-dépendant et face à une cyber-délinquance en plein essort, la sécurité informatique se révèle un enjeu décisif pour les entreprises. Installée en Thaïlande depuis 2005, SafeComs se consacre à leur protection. Nous avons rencontré Bernard Collin, son CEO.

La sécurité informatique et la protection des données englobent bien des aspects, tous couverts par **SafeComs**. De la mise en place de véritables politiques de protection au sein de l'entreprise à la récupération de données sur des disques durs endommagés, du back-up automatique encrypté et déporté dans un cloud basé en Thaïlande, crucial pour le transfert de gros volumes, à l'emploi de solutions de gestion sur mesures comme **Peppercan**.

Lauréate du prestigieux **Thailand ICT Award en 2009**, Peppercan est une suite professionnelle d'outils de management d'entreprises petites et moyennes, à la fois simple à implémenter et fonctionnant de manière sécurisée. 100% installée sur le web, elle intègre des modules de gestion des contacts, d'automatisation des ventes, de suivi collaboratif de projets, de e-marketing, de gestion de documents, de comptabilité et facturation, etc. Le tout étant sauvegardé en toute sécurité dans le nuage.

Bonjour Bernard, comment en arrive-t-on à monter une entreprise de sécurité informatique en Thaïlande ?
Je suis arrivé en Thaïlande il y a une douzaine d'années. À l'époque j'habitais en Australie où j'avais une société de sécurité informatique, nous faisions des outils de hacking, nous avions des ordinateurs qui simulaient des attaques pour tester la sécurité des entreprises.
À l'occasion de vacances à Bangkok, j'ai rencontré l'un des responsables du groupe thaïlandais Loxley. Il s'est énormément intéressé à notre système, au point de vouloir créer immédiatement une compagnie. Je suis donc venu pour monter une joint-venture avec eux. Mais nous avons tout de suite réalisé que c'était très difficile de s'adapter aux conditions de travail de nos partenaires thaïs. J'étais le seul Farang, je ne parlais pas la langue et je travaille dans un monde où la priorité va à l'éthique. Or la première chose que j'ai rencontrée ici c'est que les licences sont presque toutes piratées. Je me retrouvais face à des gens qui ne voulaient pas payer pour du software, qui ne voulaient pas payer pour du consulting et à qui on essayait de vendre des produits qui n'avaient pas de valeur marchande au kilo, puisque c'était de la propriété intellectuelle, dont ils ne voyaient pas vraiment l'intérêt. Et je passe sur les problèmes de corruption. J'ai alors rapidement repris mon indépendance, mais décidé de persévérer ici et en l'espace de deux mois, j'ai obtenu un agrément du Board Of Investment, en présentant un projet un peu différent.

C'est un statut très avantageux, notamment pour pouvoir employer des Farangs sans restriction, ainsi que sur le plan fiscal, mais quelles sont les contreparties ?
Nous avons démarré avec le soutien du BOI en 2005. En échange, nous devions investir dans le pays sous forme d'équipements, ce qui ne posait pas de problème puisque nous avions besoin de pas mal de matériel, des serveurs, etc. Nous avions ensuite comme impératif d'investir dans la formation de Thaïs, et chaque année nous devons présenter un plan de développement du personnel local que nous avons formé. Enfin, il voulaient qu'on transfère de la technologie. Qu'on donne la possibilité à des sociétés thaïes de développer de la technologie sur les bases de notre travail. C'étaient les trois critères et nous avons donc mis tout ça en place, nous avons formé énormément de Thaïs. C'est difficile, car très peu d'entre eux font montre de loyauté. On les forme et dès qu'ils sont opérationnels, la première chose qu'ils font est d'updater leurs CV et chercher un nouveau job.
Nous avons fait du monitoring de trafic et on s'est aperçu que les sites les plus visités dans les sociétés étaient les offres d'emploi.

SafeComs
Efficient Business

Si vous regardez un peu le trafic de vos employés thaïs sur le net, vous trouvez en premier les recherches d'emplois, ensuite des plateformes de chat, de messagerie, aujourd'hui c'est Facebook en priorité, puis énormément de partage illégal.

Au début, c'était une des principales demandes de nos clients : bloquer Facebook, les chats, et tout le transfert de fichiers Peer-to-peer.
Notre activité consiste aussi à protéger les organisations contre l'abus du réseau, ici il n'y a pas d'Hadopi, mais un trafic intense de ce type de données peut empêcher par exemple d'autres utilisateurs d'avoir le confort nécessaire pour tenir une conversation Skype avec un fournisseur dans un autre pays, c'est un vrai problème pour l'entreprise.

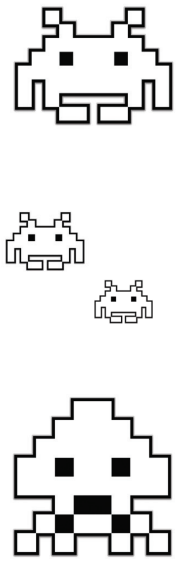
Quels sont vos clients, justement ?
Notre clientèle est essentiellement composée d'entreprises soit multinationales, soit locales, mais gérées par des étrangers. Nous avons tout de même quelques compagnies thaïes, comme ***sanuk.com*** qui fait des jeux en ligne et qui est très sensible aux problèmes de sécurité, nous avons travaillé pour la clinique ophtalmologique où le roi se fait soigner les yeux, ou avec Abhisit sur la sécurité de ses données quand il était Premier ministre, mais en dehors de ça, la plupart des boîtes que nous gérons sont étrangères, dont pas mal de françaises, nous avons d'ailleurs plusieurs Français dans l'équipe.

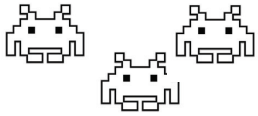
Pour qu'on s'occupe de la sécurité d'une société, il faut que les logiciels soient clairs, s'ils ne le sont pas c'est trop difficile à assurer.
La sécurité n'est pas un absolu, c'est une constante remise en question. Tous les jours on trouve de nouvelles possibilités d'effraction et il faut updater les systèmes en permanence. Si vous avez des licences qui ne sont pas clean, on ne peut pas faire proprement ces mises à jour et les clients ont de gros soucis. C'est un des gros problèmes en Asie du Sud-Est, cette attitude de laisser-faire, où les gens n'ont pas toujours conscience de la relation de cause à effet et planifient, organisent très peu.

Vous employez beaucoup d'étrangers également...
Dans la sécurité, quand on engage des employés, un certain nombre de critères sont importants et nous avons du mal à les trouver ici : l'esprit critique et la nécessité de poser des questions embarrassantes, en particulier. Quand on va faire un audit dans une entreprise, nous ne sommes pas le BSA qui vient vérifier les licences, mais nous sommes des amis, nous sommes là pour découvrir quels sont les problèmes potentiels afin d'y apporter des solutions avant qu'il ne se produise une catastrophe, c'est la définition même de ce que nous faisons comme business. Or, nous posons des questions et obtenons souvent des réponses alambiquées, car les gens ont peur de dire la vérité à leurs supérieurs et nos employés thaïs n'osent même pas poser les questions ou pointer les faiblesses...

Nous sommes donc obligés d'employer des Farangs, au moins aux postes d'encadrement. Nous avons un Allemand aux opérations, un Américain à la technique, des Japonais, Australiens, Français, Belges, nous sommes toute une équipe d'étrangers, ce qui ne pose pas de problème grâce au BOI, et nous encadrons l'équipe thaïe et gérons les moments embarrassants pour eux. Ils s'occupent ensuite des aspects techniques et le font très bien. Les Thaïs sont très procéduriers et quand un job est bien documenté, il n'y a aucun problème, il se réalise parfaitement.

Y a-t-il de bons hackers thaïs ?
Oui, en fait les Thaïs sont créatifs et c'est dans leur état d'esprit, on trouve ici des artisans exceptionnels et des hackers très doués. En plus, il n'y a pas cette notion du temps qui les dérange, le principe d'un hacker est d'essayer des choses jusqu'à ce que ça passe et donc ils peuvent y consacrer des semaines. On a des Thaïs très forts, ils ont étudié la technologie et ont pris goût à l'idée de chercher, mais le gros avantage de cette activité pour un Thaï est de ne pas être exposé, ça n'est pas public, ce que vous faites n'est pas critiqué, personne ne le sait et de temps en temps vous pouvez vous vanter d'une réussite auprès de vos copains, donc ça se passe bien. C'est de l'artisanat à tous les niveaux, que ça soit des objets ou du code informatique, c'est la même chose au niveau du processus de création et les Thaïs y sont très bons. En multimédia, par exemple, nous avons des Thaïs qui font des créations graphiques superbes.





“La sécurité n’est pas un absolu, c’est une constante remise en question. Tous les jours on trouve de nouvelles possibilités d’effraction et il faut updater les systèmes en permanence.”

Comment recrutez-vous vos troupes ?
Nous les recrutons dans les universités, avec l’inconvénient qu’ils sont encore jeunes et donc pas très matures et qu’ils n’ont pas forcément encore appris tout ce dont ils ont besoin. Mais nous voulons qu’ils soient encore ouverts, qu’ils aient envie d’apprendre et nous essayons de sélectionner ceux qui ont le plus de goût pour la découverte. Ce qu’ils ont appris à l’université nous intéresse très peu, mais ce qu’ils ont fait dans leur vie privée, les groupes de hackers auxquels ils participent, des choses comme ça, c’est là qu’on retrouve les caractéristiques qui correspondent à ce qu’on veut.

De toute manière, nous leur imposons une formation systématique, parce que les produits que nous utilisons ont été créés en interne, c’est une technologie qui n’est pas connue, nos langages de programmation non plus. Nous utilisons par exemple un langage inventé par un japonais il y a une vingtaine d’années, Ruby. C’est un langage tout nouveau qui a des avantages énormes, il est structuré et propre, portable, sécurisé, à l’opposé de ce que les gens utilisent en général, comme PHP, mais personne ne l’apprend à l’université...

Quelles sont les principales menaces auxquelles vous êtes confrontés ?
Il y a dix ou quinze ans, les virus étaient créés par des gens qui voulaient montrer leur expertise, on réussissait à infecter tant de milliers de machines et on en parlait le plus possible. Ensuite sont arrivés des gens créant des virus destructifs et qui en parlaient aussi beaucoup, mais de manière anonyme, à travers des avatars. Il y a 6 ou 7 ans, on avait des virus catastrophiques qui nettoyaient complètement vos disques durs, détruisaient vos données, etc. Et puis on est arrivé dans le domaine de la criminalité.
Il faut savoir qu’aujourd’hui les statistiques montrent que la cybercriminalité représente plus que la prostitution, la drogue et le grand banditisme combinés. Ça laisse moins de traces, c’est moins risqué et ça se fait dans des conditions de confort bien plus importantes. Le hacker est seul à l’abri dans sa cave, alors que les braqueurs prennent de gros risques. Le monde du hacking s’est énormément développé vers la criminalité et donc vers le secret. Il y a beaucoup de problèmes liés au hacking dont les gens n’ont pas conscience. Quand une banque se fait dévaliser par un hacker, elle ne va pas trop en faire la publicité.
Si une société retrouve le fichier de ses clients publié sur internet, elle va essayer de l’étouffer, surtout ici...

Je pense que le plus gros risque que courent désormais les gens est le vol d’identité. On a vu ces deux dernières années, surtout au Myanmar, mais aussi en Thaïlande des situations dans lesquelles on se retrouve avec un groupe de hackers ayant pénétré au sein d’une entreprise et qui font des déviations de paiements en usurpant l’identité d’un cadre.

Nous avons parfois été appelés en consulting pour des problèmes juridiques où le client et le fournisseur sont en opposition, avec une responsabilité difficile à localiser, l’un a payé une facture et l’autre a servi des prestations ou des produits, mais l’argent a disparu ! Dans certains cas les sommes sont colossales, plusieurs centaines de milliers de dollars. C’est le type de crime auquel les gens sont désormais confrontés.
Le deuxième type de menace, qu’on rencontre beaucoup en ce moment, est une recrudescence des cryptovirus, c’est un malware qui vient s’installer sur votre ordinateur et votre réseau et encrypter toutes vos informations, puis vous réclame un paiement en échange du mot de passe pour lever le cryptage. Le créateur du virus l’a ensuite mis en vente sur le net avant d’être arrêté. Problème : le virus est toujours en circulation, il y a un mois, un de nos clients a été infecté, il a versé l’argent sur le compte, mais le compte n’existe plus parce que le réseau a été démantelé... Dans certains cas on parvient à récupérer les données, mais les derniers chiffrements

utilisés sont tellement performants que ça prendrait des années pour y arriver.

La troisième menace n'est pas technologique. Pour moi, le plus important en matière de sécurité n'est pas la technologie, mais la connaissance, la formation du personnel. On peut mettre n'importe quelle infrastructure en place, on n'arrivera jamais à empêcher à 100 % les attaques parce que le maillon faible de la chaîne de sécurité est l'individu. Quand on effectue un audit dans une société, on fait des statistiques avec un outil qui craque les mots de passe de tous les comptes. Certains se craquent en une fraction de seconde, pour d'autres ça prend une semaine, quand le mot de passe est sérieux, ça peut prendre des mois. Mais on trouve énormément de mots de passe comme *1234* ou *12345*, *admin 123*, qu'on retrouve sur énormément de systèmes, *password* est très employé et on a beaucoup de code à quatre chiffres, souvent utilisés pour tous les sites où va la personne, le même que le code de la carte bancaire... Tout cela implique des risques importants.

Le phishing est actuellement très répandu et devient très sophistiqué. Vous recevez par exemple un document qui vous dit que votre compte, PayPal ou eBay ou votre compte en banque, a été compromis et vous demande de réactiver votre compte avec votre nom et votre mot de passe. Ceux-ci sont copiés et redirigés vers une base de données qui sera soit directement utilisée par les hackers, soit revendue sur internet. Aujourd'hui la revente de coordonnées de comptes et de cartes bancaires est devenue une vraie industrie.

Nous amenons nos clients à mettre en place une véritable politique de sécurité qui doit avoir un certain nombre de caractéristiques : elle doit être simple et courte, si on fait un bouquin de 20 pages, personne ne le lit, elle doit être adaptée à la personne à qui vous la donnez, enfin il faut qu'elle soit distribuée de façon à ce que tout le monde en prenne connaissance.

Ensuite, il faut faire du monitoring, vérifier qu'elle est bien appliquée.

Nous définissons des procédures, par exemple pour les comptes sensibles, on peut avoir un deuxième facteur d'authentification, comme un code reçu par SMS ou du biométrique, votre empreinte digitale ou une copie de votre iris. Nous mettons en place des systèmes qui vous donnent accès à des passwords avec votre compte, mais sans que vous les connaissiez. Si on vous retire ce compte, vous n'avez plus accès à rien. Un problème courant est la possibilité d'accès d'un ancien employé qui vous a quitté, car changer tous les mots de passe qu'il peut connaître est un processus tellement long et ardu que beaucoup d'entreprises ne le font pas. Alors que c'est une précaution élémentaire...

Nous sommes aujourd'hui confrontés également au fait que nombre d'employés d'une société utilisent leurs propres matériels, iPhone, tablettes et même laptops. L'environnement de l'entreprise s'est hypercomplexifié et engendre une perte de contrôle, là où il y a quelques années les accès et les serveurs pouvaient encore être très encadrés. Autant on gère facilement un réseau interne dans une société, le monitoring des serveurs et des ordinateurs in situ, autant c'est difficile avec des appareils qui sont connectés à tous les réseaux sans discrimination possible, y compris à travers la 3 ou 4G, en dehors du filtre du réseau de l'entreprise.

Désormais, nous commençons à mettre en place des systèmes pour différencier le professionnel du privé tout en acceptant la cohabitation sur une même machine. C'est un des tout nouveaux produits que nous lançons, l'**EMM, Enterprise Mobility Management**, avec l'installation d'un système de sécurité où on crée sur votre propre téléphone un container dédié à la société, au sein duquel on a un accès total et contrôlé. On peut accéder au container, l'effacer, le protéger avec des antivirus, surveiller et protéger son trafic web, ne donner que des accès provisoires ou limités à des documents, par exemple en interdire la copie ou le forward, et on peut l'encrypter. Si vous perdez votre téléphone, personne ne peut aller voir ce qu'il y a dans votre container société. Du côté privé, si vous avez omis de le bloquer avec un mot de passe, c'est votre problème. On peut même installer un système de tracking fonctionnant téléphone éteint...