CYBERDÉFENSE & CYBERGUERRE

KASPERSKY LAB : LA SÉCURITÉ INFORMATIQUE PASSE PAR LA FORMATION

Tanguy de Coatpont

Le groupe **Kaspersky Lab** est le spécialiste de la sécurité informatique. Il développe et commercialise des solutions pour sécuriser à la fois le grand public et les entreprises. Éclairage avec Tanguy de Coatpont, Directeur général de Kaspersky Lab France et Afrique du Nord.

Vos solutions de sécurité ne sont-elles pas compliquées à comprendre ?
Technologiquement, la sécurisation des systèmes d'informations est complexe. En revanche depuis quelques années, un gros effort est entrepris sur l'ergonomie et la facilité d'utilisation de nos outils. Le problème n'est pas la complexité de nos systèmes, mais bel et bien la perception et la compréhension des risques informatiques par l'utilisateur lui-même.

D'où votre souci de militer en faveur de la formation à la sécurité...
Nous en sommes convaincus. Sans l'adhésion complète de l'utilisateur, à titre personnel et professionnel, la sécurité sera extrêmement difficile à assurer dans les entreprises.

Votre groupe mise-t-il sur la sécurité ?
Notre groupe exerce de nombreuses activités, mais nous mettons généralement en avant la sécurité. Nous cherchons à protéger le système d'information des entreprises contre les vols de données et la corruption. Notre cœur de métier est là, mais l'utilisateur reste central pour nous.

Pourquoi ciblez-vous l'utilisateur ?
L'utilisateur n'est plus cantonné dans les murs de sa société comme c'était le cas il y a quelques années. Il dispose aujourd'hui d'un Smartphone, d'une tablette et d'un ordinateur portable. Il est très mobile dans les murs et à l'extérieur de son entreprise,et doit accéder à l'information où qu'il soit. Dans ce contexte, la sécurité devient de plus en plus difficile à assurer sans l'aide concrète de l'utilisateur.

À quel niveau la sécurité doit-elle être prise en compte ?
La sécurité doit être intégrée dans tous les projets de digitalisation et de numérisation. Elle doit être prise en compte dès la phase de développement des systèmes industriels ou des logiciels.

Au sein de l'entreprise, qui est concerné par la politique de la sécurité ?
Il faut sensibiliser en permanence les salariés aux risques informatiques qui deviennent de plus en plus importants. La sécurité doit être prise en compte par les DRH dans tous les cursus de formation et doit être relayée dans toutes les divisions.

Les attaques concernent-elles tout le monde dans les entreprises ?
Dans la plupart des grandes attaques, les personnes ciblées étaient des comptables ou des chargés de marketing qui ont cliqué sur un mauvais lien. Nous le disons. Tous les employés sont désormais des cibles potentielles.

Prenez-vous en compte dans votre démarche vos distributeurs ?
Les distributeurs de nos solutions sont certifiés par nos soins. Ils doivent être bien formés dans l'installation, le paramétrage et le maintien en activité de nos logiciels. Nous estimons en effet que s'ils n'ont pas une bonne compréhension de nos logiciels, cela créera tôt ou tard des problèmes !

Comment familiarisez-vous les employés d'un groupe ?
Les « serious games » sont notre cheval de bataille. Cet ensemble de solutions ludique permet aux directions des ressources humaines de mettre en situation les salariés et de faire passer les messages clés.

En quoi ces jeux sont-ils essentiels ?
La formation sur la sécurité peut être rapidement rébarbative. Nous partons du principe que les messages ne passent pas si nous n'arrivons pas à impliquer des gens de manière ludique.

Comment jugez-vous les besoins en formation ?
Nos outils peuvent mesurer à un instant T le niveau de connaissances sécuritaires des employés. En fonction des besoins, nous pouvons déployer des modules de formation « on line » qui permettent à chaque employé de se perfectionner en permanence sur l'hameçonnage, sur la création et l'intérêt de mots de passé sécurisés...

Devant les attaques qui évoluent très vite, les formations sont-elles toujours utiles ?
La réponse est clairement oui. Nous sommes toujours ébahis, voire même choqués devant tant d'attaques aussi sophistiquées, ciblées et technologiquement avancées qui commencent par une simple erreur d'un employé. Sans un bon niveau de compréhension et de formation des utilisateurs, les pirates pourront faire ce qu'ils voudront !

Faut-il nommer un responsable de sécurité en systèmes d'informations dans chaque entreprise ?
Les responsables en SII existent depuis de nombreuses années. Ils se développent de plus en plus et sont présents dans les sociétés de taille importante. Ils commencent d'ailleurs à l'être dans des PME. Ces cadres-là sont très importants pour nous parce qu'ils sont des ambassadeurs de nos solutions.

Les réseaux sociaux sont parfois dangereux. Faut-il interdire leur accès ?
Entre l'interdiction totale et la permissivité, le curseur est difficile à placer. Interdire l'accès aux réseaux sociaux était une solution acceptable, il y a quelques années. Mais à l'heure où les générations Y et Z, ou générations connectées ,utilisent les réseaux sociaux en permanence à titre personnel et professionnel, il n'est pas réaliste de tout bloquer.

Quelle est donc la solution face aux réseaux sociaux ?
La responsabilisation. Il faut expliquer pourquoi on fait les choses ou comment on fait les choses si on les entreprend différemment. Les employés pourront mieux utiliser les outils sociaux importants pour les sociétés d'aujourd'hui s'ils comprennent les effets parfois dévastateurs de leurs actes.

Vous parlez beaucoup des utilisateurs. Êtes-vous en perpétuelle réflexion sur vos solutions ?
Nous évoluons au rythme de l'apparition de nouveaux usages, de nouveaux terminaux et des innovations. Kaspersky Lab dispose d'un des plus grands laboratoires mondiaux dans l'analyse des virus. Nous traitons de manière automatique un peu plus de 325 000 nouveaux fichiers malveillants par jour.

Qui traite ces fichiers ?
Nos robots et nos modèles mathématiques permettent de classifier et de traiter quasiment 99 % de nos fichiers. 1 % est directement géré par une équipe de 40 chercheurs, experts en sécurité, répartis sur les cinq continents. Ce 1 % est souvent le plus complexe.

Sur quoi travaillent-ils principalement ?
Ils travaillent sur les grandes attaques complexes telles que The Mask Careto, Dark Hotel, Equation... en lien notamment avec Interpol et Europol, les chercheurs publient le résultat de leurs recherches et de leurs investigations. Une partie de ces rapports est accessible sur notre site Internet. Une autre partie contient des informations non publiques vendues à des sociétés abonnées à nos services. Leur travail permet de développer des solutions technologiques mettant à l'abri le grand public et les entreprises des attaques.

Comment voyez-vous l'avenir ? La sécurité passe-t-elle par l'internet des objets ?
L'Internet des objets va démultiplier les risques informatiques comme le soutient notre fondateur Eugène Kaspersky. Notre crédo est de pousser les développeurs à penser à la « brique sécurité » dès la conception des objets connectés.

Vous êtes inquiet...
Si dès le départ la sécurité n'est pas intégrée dans les objets connectés, les conséquences peuvent être très graves. Récemment, des experts en sécurité ont réussi à pirater un Jeep en temps réel... Vous comprenez aisément que les briques sécurité sont fondamentales.

La sécurité a visiblement de l'avenir...
La sécurité informatique n'est pas prête de disparaître, car la notion d'objets connectés explose et que demain tout sera connecté. Notre groupe mène d'ailleurs un programme en interne avec l'aide d'une association pour étudier les piratages possibles de puces placées dans des corps humains.

Vous êtes sur tous les fronts...
Il faut comprendre que les hackers sont de vrais ingénieurs et capables d'investir plusieurs dizaines de millions d'euros pour leurs attaques ! Face aux menaces, nous essayons toujours d'avoir un coup d'avance. Mais notre mission est difficile dans la mesure où nous sommes là pour protéger et non pour attaquer. ■