CYBERDÉFENSE & CYBERGUERRE

LA SÉCURITÉ PRÉVENTIVE ET COLLABORATIVE

Arnaud Kopp

Créé en 2005 par Nir Zuk, **Palo Alto Networks** est l'un des grands spécialistes mondiaux des solutions de sécurité pour les réseaux et les ordinateurs. Éclairage sur la stratégie d'un groupe avec Arnaud Kopp, directeur technique pour l'Europe Sud.

Quelles sont les origines de votre entreprise ?
Nir Zuk, notre fondateur, a créé l'entreprise en 2005 à Palo Alto (États-Unis) avec l'aide de vétérans de la technologie des réseaux. Mais notre entreprise a vraiment démarré en 2006 lors du dépôt des statuts. Nous allons fêter cette année nos 10 ans d'existence.

Depuis votre premier produit issu de cette équipe fondatrice, quelle est votre politique de développement ?
La sécurité ne doit plus uniquement s'intéresser à la partie purement technologique. Elle doit prendre beaucoup plus de hauteur pour comprendre les attaques de cyberpirates. Elle doit enclencher un échange d'informations dans un écosystème de lutte contre les attaques.

La sécurité est-elle une affaire d'hommes ou de machines ?
Notre fondateur avait remarqué la croissance importante du nombre des terminaux et de leur exposition aux cybermenaces. Mais derrière les machines, il pointait le maillon faible : les utilisateurs. Dès 2005, il posait un constat. Les utilisateurs vont se connecter à des réseaux plus ou moins sécurisés dans le monde. De leurs comportements doit dépendre le niveau de sécurité des infrastructures.

La numérisation est partout. Quels en sont les effets pour la sécurité ?
Le cyberespace était ouvert il y a 20 ans aux entreprises et aux gouvernants. Il est ouvert aujourd'hui à tout le monde qui se connecte sans forcément se rendre compte des risques de cyberattaques. Il a étendu par la force des choses le risque de vol d'informations et d'atteintes à la réputation d'entreprise ou de gouvernement.

Formez-vous vos utilisateurs quand vous installez vos systèmes de protection ?
Notre académie de formation permet de mettre à disposition des écoles et des institutions partout dans le monde nos contenus et nos informations. Ces programmes-là sont nécessaires, mais c'est toujours très long pour en voir les effets. Entre eux, les attaquants se forment, s'échangent des infos et mettre à jour très rapidement leurs attaques.

La formation ne serait pas toujours efficace…
La transformation numérique est tellement rapide qu'on n'a pas le temps de se former dans les entreprises et de rattraper le retard. Nos solutions technologiques sont là pour faire face à chaque nouveau projet de transformation numérique. Nous avons été présents dès la virtualisation des réseaux, l'apparition du cloud, de la mobilité et big data.

Comment agissez-vous contre les attaques ?
« *Praestat cautela quam medela* » (lat.) : mieux vaut prévenir que guérir !
Nous pensons que la prévention d'attaques est primordiale. Par conséquent, vu que la vaste majorité des attaques sont exécutées par des machines, il faut des machines et des mécanismes automatisés pour se défendre. La cyber warfare est une guerre entre machines en non pas entres hommes. Évidemment, l'homme crée ces problèmes, mais la solution doit être fiable et prévisible et requière donc des machines.
Nos équipes de recherche et de développement sont toujours à la pointe des nouvelles attaques dans le monde. Elles travaillent au sein de notre centre de recherche de développement en cybersécurité appelé « Unité 42 », en référence au livre *Le guide du voyageur intergalactique* de Douglas Adams, pour assurer l'adéquation de la prévention par les machines par rapport à la transformation des menaces.

Quel est le rôle de l'Unité 42 ?
Ses membres participent dans le monde entier à toutes les conférences sur la cybersécurité. Ils analysent les nouvelles situations et mettent à disposition de la communauté internationale qui cherche à se défendre un ensemble de documents, d'analyses et des comparaisons historiques.

En quoi les comparaisons historiques sont-elles importantes ?
Il est essentiel de rapprocher des événements qui semblent déconnectés dans le temps ou dans l'espace. Des éléments en commun peuvent en effet exister entre deux campagnes d'attaque de malware. Ils peuvent nous aider à améliorer les connaissances sur les menaces pour encore mieux nous en prémunir automatiquement et contribuer à l'éducation des utilisateurs.

Comment agissez-vous contre la rapidité d'exécution des attaquants ?
Nous fonctionnons dans un écosystème d'analyses et de compréhension des attaques par des systèmes informatiques. Quand l'une d'elles se déroule à un endroit contre un de nos clients,

elle est immédiatement bloquée. Elle procure suffisamment d'informations pour qu'elle puisse être une protection additionnelle chez tous les autres clients ou sur les autres postes de l'entreprise. En fait ce que l'on recherche à éviter, c'est la propagation.

Les attaquants seront-ils vraiment gênés ?
Nous cherchons à entraîner l'attaquant dans une spirale d'investissements supplémentaires. Nous tentons de mettre à mal la rentabilité de ses attaques dans la mesure où ses logiciels malveillants n'auront qu'une durée de vie limitée et ne pourront être réutilisés massivement.

Quels sont les atouts de votre écosystème pour les clients ?
Dans ce système de protection collaborative, nos clients n'ont pas besoin d'être experts en cybersécurité. Ils bénéficient de ce qui a pu être analysé et détecté chez d'autres clients. Nous sommes dans un réseau social de sécurité où l'on s'échange des informations et où l'on s'auto améliore constamment.

Cet écosystème permet-il de hiérarchiser les mesures de défense ?
Notre plate-forme de supervision globale de toutes les menaces que l'on appelle AutoFocus nous remonte toutes les informations. Elle cible le niveau de la cyberattaque en fonction de différents critères intelligents, et permet ainsi à l'entreprise de connaître son exposition au risque.

Les entreprises ont-elles toujours le temps de connaître leurs risques ?
Des prestataires habilités par l'Anssi (Agence nationale de la sécurité des systèmes d'informations) sont présents aux côtés des entreprises. Ils utilisent nos plates-formes pour contrôler techniquement et constamment leurs projets de transformation numérique au regard des attaques possibles.

Les entreprises courent-elles vraiment des risques ?
Certains services ne se rendent pas compte des risques qu'ils peuvent faire courir à leur entreprise aussi bien sur la fuite de données que sur l'entrée de menaces. Ils oublient que la transition numérique n'est plus un terrain d'amusement pour quelques fous d'informatiques ! Accessible à tout le monde, le monde numérique devient un endroit où un grain de sable peut avoir des impacts hallucinants…

Quels sont les risques ?
Dans le domaine de la propriété intellectuelle, la fuite des secrets est la pire chose qui puisse arriver à une entreprise. Qui sait quel concurrent pourra avoir accès à cela ? Si l'on ne regarde pas du bon côté, les entreprises et gouvernants sont à la merci d'organisation très bien établie qui savent tirer un avantage de ces données numériques.

Quel genre de contrôle peut-on prendre ?
Tout d'abord, il s'agit de s'assurer d'avoir une visibilité sur tous les mouvements de données numériques, et utilisation d'applications par les utilisateurs. Il est alors possible de gérer correctement le risque lié à ces usages, et de limiter l'exposition du système d'information et de ces utilisateurs. Nous parlons d'assainir les réseaux, les données numériques, et prévenir des attaques tout en maintenant les performances de ce monde numérique.

NOUS AVONS MIS EN PLACE UN SYSTÈME DE DISSUASION NUMÉRIQUE DE LA MÊME FAÇON QU'IL EXISTE UNE DISSUASION NUCLÉAIRE. C'ÉTAIT ESSENTIEL PARCE QUE LE NOUVEAU CYBERESPACE EST DEVENU UN TERRAIN D'ATTAQUE POUR TOUT LE MONDE.

Quel est le deuxième grand risque ?
Tout le monde peut avoir accès à ses données dans des aéroports, dans des gares et des cybercafés avec le risque de se les faire voler. La mobilité nécessite de sécuriser le système d'exploitation du terminal et de trouver des solutions.

Le cloud est aussi un danger…
Des entreprises ne se rendent pas compte que la sécurité qu'elles ont déjà mise en interne ne couvre pas toujours le nuage. Nous sommes là pour refaire le lien entre la sécurité interne et la sécurité externe.

Et pour terminer l'Internet des objets…
C'est la grosse difficulté actuellement. Nous ne pouvons pas toujours intégrer dans l'objet lui-même la sécurité. Elle doit être à un autre endroit…par exemple dans les relais 3 G ou 4 G.

Le risque est-il grand ?
Effectuer des recherches sur la vulnérabilité d'un « frigo » connecté, cela peut paraître idiot ! Mais il peut devenir le relais d'une attaque générale vers l'ensemble des réfrigérateurs d'une même marque. Cela peut entraîner un effet néfaste pour le fabricant et pour les denrées alimentaires d'un pays entier. Un frigidaire connecté est pratique, mais il peut ouvrir une surface d'attaque incroyable !

Comment en apprendre encore plus ?
En collaboration avec la Bourse de New York (NYSE), nous venons de publier un livre « Naviguez dans l'ère du numérique » que vous pouvez télécharger ici :
http://connect.paloaltonetworks.com/cyberhandbook
Nous serons heureux de l'envoyer aux anciens de l'X qui nous contacteront. ■

CHIFFRE CLÉ

28 000 clients entreprises
140 pays
55 % de croissance
928 millions de dollars de revenus
1 000 clients-entreprises nouvelles par trimestre

CONTACT

akopp@paloaltonetworks.com
www.paloaltonetworks.com