

«Il y a déjà trop d'agents et il est difficile de les faire cohabiter»

Agent installé sur le poste client ou appliance sur le réseau? Afin de mieux comprendre les avantages et inconvénients de ces deux approches, nous nous sommes entretenus avec Jacques Medina et Patrick Zwahlen de la société spécialisée Navixia, qui proposent une démarche plus pragmatique. *Interview: Rodolphe Koller*

Constatez-vous un changement en termes d'adoption du concept NAC chez vos clients?

Patrick Zwahlen: On assiste à une seconde vague d'adoption ou tout au moins de pilotes. Les clients sont plus au fait des solutions NAC et donc plus spécifiques quant au problème qu'ils cherchent à résoudre. Ce qui les intéresse c'est surtout d'obtenir davantage d'informations sur les machines qui se connectent, plutôt que de simplement leur ouvrir ou leur fermer l'accès. Dans la plupart des cas, les administrateurs ne peuvent pas définir un type restreint de machines conformes ou non-conformes: ils ont le top management avec des machines spécifiques ou encore des utilisateurs qui veulent absolument utiliser des Mac.

Jacques Medina: On constate que les départements IT sont souvent prêts à accepter des machines momentanément sur le réseau, mais veulent un contrôle beaucoup plus complet et en temps réel de ce que font ces appareils pour décider le cas échéant de les bloquer manuellement après quelques minutes. Le gros problème avec NAC c'est



Les deux experts de Navixia Jacques Medina (à gauche) et Patrick Zwahlen (à droite) considèrent que les solutions NAC bloquant automatiquement les accès à des machines négligent la complexité de l'environnement réel des entreprises.

emploie son ordinateur à la maison et revient avec une machine infectée, un collaborateur IT qui crée une machine virtuelle à des fins de test sans s'assurer qu'elle a tous les derniers patches et antivirus.

mier rôle de NAC c'est de faire la différence entre ces divers types de machines. En outre, ces solutions donnent à l'équipe sécurité des informations qui étaient en fait déjà disponibles à d'autres groupes IT, par exemple quels patches sont installés sur les machines qui se connectent.

Que pensez-vous des solutions basées sur un agent installé sur le poste client?

JM: Nous nous sommes éloignés de la solution qui nécessite de déployer du code sur le poste de travail, car pour nous il y en a déjà trop: antivirus, pare-feu personnel, cryptage, etc. et il est difficile de les faire cohabiter.

PZ: De plus, dans le cas des solutions intégrées qui sont proposées maintenant par la majorité des éditeurs on se retrouve avec le problème des machines qui ne sont pas gérées par l'entreprise. Or c'est justement un des problèmes que les entreprises souhaitent résoudre.

JM: Typiquement, une machine qui n'est pas sécurisée avec le logiciel préconisé par l'entreprise peut s'avérer parfaitement sûre, mais ne sera pas considérée comme telle. Bien sûr les partisans des logiciels clients argumenteront que c'est la meilleure façon d'avoir des

«Ce qui intéresse les entreprises, c'est surtout d'obtenir davantage d'informations sur les machines qui se connectent, plutôt que de simplement leur ouvrir ou leur fermer l'accès.»

qu'une machine propre qui se connecte à un moment donné peut devenir une menace, en particulier si l'utilisateur dispose des droits d'administrateur.

Quels sont les usages qui réclament ces solutions?

JM: Il y en a de toutes sortes: un consultant externe qui se connecte avec son laptop depuis la salle de conférence, un utilisateur qui

PZ: La majorité des entreprises qui déploient des technologies NAC commencent d'ailleurs par catégoriser leur parc (ordinateurs, téléphones, imprimantes), puis elles font rapidement la différence entre ce qui est géré par l'entreprise et ce qui ne l'est pas. Parfois aussi elles différencient les *guests* véritables de contractants tiers qui doivent avoir accès à certains systèmes, par exemple SAP. Le pre-

informations précises sur la machine, mais il est possible d'aller interroger la machine si l'on a les droits correspondants.

Et les approches hardware basées sur une appliance NAC?

PZ: C'est clair que Cisco et Microsoft sont les mieux positionnés, mais leurs solutions sont loin d'être idéales. En gros, avec Cisco j'ai l'avantage que le switch est au plus près de ma machine, mais, à part le contrôle du certificat 802.1.X, c'est des solutions externes qui ont été rajoutées et pas vraiment bien intégrées. Quant à Microsoft, tout va bien si vous avez Vista dernier cri et Windows 2008 au niveau du domaine, ce qui est loin d'être le cas dans la plupart des entreprises. Les autres solutions reposant sur une appliance ont le désavantage de remettre en cause le design de l'ensemble du réseau.

JM: Si l'on place un boîtier basé sur une architecture Intel au cœur du réseau, on va souffrir de problèmes de performance, de redondance et de stabilité. Nous avons eu de très mauvaises expériences avec ce type de solutions.

Quelle approche recommandez-vous à vos clients?

PZ: Nous avons une approche un peu alternative. On n'a pas de logiciel qui tourne sur le poste client et on n'est pas non plus dans le réseau.

JM: On évite les deux contraintes qui étaient dangereuses pour l'entreprise. Notre solution repose sur un boîtier *out-of-band* auquel nous donnons la vision du trafic. Il ne se situe pas entre deux segments et ne risque pas de faire tout tomber. C'est un câble intelligent en quelque sorte, mais il n'y a aucun risque de perte de fonctionnalité. La priorité pour les entreprises, c'est la productivité et pas la sécurité. C'est pour cela qu'on privilégie des solutions où le blocage n'est pas automatique mais décidé par un administrateur. Au début d'un projet, il arrive que nos clients veuillent tout couper automatiquement mais, quand ils voient le nombre d'anomalies auxquelles ils ont à faire, ils préfèrent une solution moins extrême. Ils disent oui à l'amélioration de la sécurité mais pas au détriment de la productivité des utilisateurs.

Cette architecture vous permet-elle de prendre des mesures de remédiation?

JM: Oui, au moment où une machine se connecte, on va procéder à des vérifications basées sur une *policy* et c'est en fonction du degré de conformité que l'on va agir, soit en laissant la machine continuer à travailler sur le réseau, soit en lui coupant l'accès car elle représente un risque. Ce contrôle prend plus ou moins une minute. Si la machine est

connue, je vais pouvoir tester son état (antivirus, pare-feu, etc.) grâce aux droits d'administrateur que j'ai sur elle. Si elle n'a pu se connecter à aucun système, je la considère comme étrangère.

PZ: En ce qui concerne les *guests* qui veulent accéder à internet, on peut les rediriger sur une page web (comme sur un hotspot Swisscom) où ils auront un mini-agent (ActiveX ou Java) à activer qui nous permettra de récolter de l'information sur l'état de la machine.

«En utilisant uniquement des postes virtualisés, on réduirait considérablement les risques et on éliminerait en quelque sorte le besoin du NAC.»

JM: L'avantage avec l'architecture que nous recommandons c'est que ces divers checks n'ont pas seulement lieu au moment où la machine se connecte sur le réseau, mais en permanence.

Et les approches hybrides basées à la fois sur un agent et une appliance?

JM: On n'y coupe pas, les éditeurs d'agents clients vont tous se mettre à offrir des appliances, que ce soit *in-line* ou *out-of-band*,

car la gestion des machines *guests* est trop importante. De plus, on ne va pouvoir continuer à rajouter une couche sur le poste de travail chaque fois qu'on rencontre un problème. Les éditeurs sont déjà contraints de réduire la taille des bases et d'enlever des vieilles signatures parce qu'ils n'arrivent plus à suivre

Concrètement, quels types de déploiement réalisez-vous pour vos clients?

PZ: Jusqu'à présent, nous n'avons pas de client qui souhaite un déploiement généralisé pour un vaste parc de 5000 utilisateurs. Les projets concernent des entités spécifiques de l'entreprise qui requièrent un niveau de sécurité spécial. Après les premiers tests, les entreprises se concentrent sur des usages particuliers: savoir si les gens qui se connectent au VPN sont conformes ou non; connaître l'état des machines sur le réseau *guest wifi*; limiter les accès dans un bâtiment précis.

Comment voyez-vous les solutions NAC évoluer?

PZ: Parallèlement à leur réflexion sur NAC, les entreprises s'intéressent de plus en plus à la virtualisation des postes de travail. En utilisant uniquement des postes virtualisés on réduirait considérablement les risques et on éliminerait en quelque sorte le besoin du NAC. On n'en entend pas encore parler en Suisse, mais on va peut-être voir des entreprises laisser leurs employés acheter leurs propres laptops. La société ne gère plus de hardware mais uniquement l'environnement virtuel utilisé par les employés.

JM: On voit aussi se développer des solutions basées sur la virtualisation d'applicatifs sécurisés. C'est ce que font certaines banques en donnant à leur client une clé USB sur laquelle se trouve un browser.



Pour les experts de Navixia, les entreprises ne sont pas prêtes à ce que le contrôle des accès se fasse au détriment de leur productivité.

Source: Fotolia