John Chambers, Cisco : l'impact de l'Internet of Everything sur la sécurité

Toutes les entreprises ont été en proie à des attaques ou à des incidents de sécurité en 2014, même si seulement quelques attaques de grande envergure ont fait les gros titres de l'actualité. En 2014, nous avons constaté que 100% des systèmes d'information étaient infectés, attestant ainsi que la menace est désormais permanente pour les entreprises. Les tendances montrent que les attaques continuent d'évoluer dans leur sophistication et dans leur fréquence. Pour cette raison, la question que les entreprises doivent se poser aujourd'hui n'est plus : « est-ce que mon entreprise va être attaquée ? », mais plutôt : « quand les cybercriminels vont-ils attaquer mon réseau ou mon datacenter ? »

L'année dernière, lors du Forum Economique Mondial, j'avais décrit comment, à mon avis, l'Internet of Everything – l'évolution de l'Internet des Objets puisqu'il s'agit d'un réseau mondial connectant non plus seulement les objets mais aussi les personnes, les données, les processus – était en train de changer le monde. Un an plus tard, nous constatons de plus en plus l'impact de l'IoE sur nos vies. Aujourd'hui, les équipements de surveillance portables dans le domaine de la santé, les voitures intelligentes, les réseaux intelligents, les plates-formes pétrolières connectées ou encore la fabrication industrielle connectée révolutionnent notre manière de travailler, de vivre, de jouer ou d'apprendre.

Une nouvelle approche de la sécurité

L'Internet of Everything représente une opportunité économique estimée à près de 19 000 milliards de dollars au niveau mondial. Cependant, à l'ère de la connectivité omniprésente, la sécurité doit devenir une préoccupation bien plus importante. Étendre simplement les équipements et mesures de sécurité actuelles pour répondre à la prolifération de l'IoE ne sera pas suffisant. Une nouvelle approche de la sécurité, basée sur une réflexion en rupture avec ce qui se faisait jusqu'à présent, ainsi qu'une vraie approche innovante, apparaît aujourd'hui comme critique et indispensable.

J'invite les décideurs d'aujourd'hui à prendre en compte quelques considérations majeures :

De par leur conception, les menaces profitent de la confiance accordée aux systèmes, aux applications, aux personnes et aux entreprises. La réalité, c'est que bien souvent lorsqu'un système est infecté, le maillon faible est de source humaine et interne à l'entreprise. Même si cela peut paraître insurmontable, c'est en fait une opportunité pour les entreprises d'aborder la sécurité en tant que moteur de la croissance, en mettant en place des stratégies qui peuvent tirer parti de la technologie et de leur expertise en matière de sécurité. Nous devons examiner la sécurité dans tout le continuum d'attaque – avant, pendant et après une attaque.

Chaque entreprise est une entreprise de sécurité

Pour maintenir un important niveau de confiance avec leurs clients, leurs partenaires et leurs employés, les entreprises doivent se considérer elles-mêmes comme des entreprises de sécurité.

Puisqu'il n'existe pas aujourd'hui de réseaux ou de terminaux entièrement fiables, une stratégie qui se base sur les problèmes de sécurité clés – les menaces – va permettre aux responsables de la sécurité d'anticiper les attaques ciblant le réseau étendu de l'entreprise ou un environnement professionnel en constante évolution.

Ainsi les dirigeants se doivent d'être intransigeants dans l'auto-évaluation de leurs équipements de sécurité en place en se posant les bonnes questions : quels modes de contrôle avons-nous en place ? A quel point ont-ils été testés ? Avons-nous des processus de reporting en place ? Que devrions-nous savoir d'autre ?

La sécurité n'est plus seulement une problématique technologique, elle doit être l'affaire de tous au sein de l'entreprise. Il est absolument nécessaire pour les dirigeants et les responsables IT, de discuter et de s'aligner sur les risques potentiels et de travailler ensemble pour trouver les solutions adéquates qui vont protéger la propriété intellectuelle, industrielle et financière de l'entreprise.

Une vigilance à tous les niveaux

Être vigilant à tous les niveaux et partager les connaissances liées au réseau constituent deux des éléments majeurs pour une bonne sécurité. En l'absence de standards internationaux, le débat autour de la sécurité s'invite dans le monde entier. La cybercriminalité fleurit dans des zones où la cybergouvernance est faible, comme en Europe de l'Est. Cette variété dans l'approche de la sécurité en fonction des pays peut mener à des restrictions dans la circulation des données à travers les frontières. Un dialogue international entre les gouvernements, les entreprises et le secteur privé, peut aider à créer des accords pour mieux sécuriser l'économie numérique. Les progrès de l'Internet Engineering Task Force (IETF) et des autres groupes travaillant à l'élaboration de standards pour Internet laissent à penser que la collaboration sera de mise à l'avenir, mais finalement il est de la responsabilité des dirigeants d'aujourd'hui de se regrouper pour résoudre les problèmes de cybergouvernance.

L'Internet of Everything peut transformer notre monde, mais pour créer le changement de manière durable et intelligente, nous devons réfléchir aux moyens d'assurer que chacun puisse bénéficier des opportunités de l'IoE, en toute sécurité. Et cela doit être fait en positionnant la sécurité comme un moteur de croissance, non de manière individuelle pour sa personne ou son entreprise, mais dans une réflexion servant l'économie mondiale. Si chacun au sein de la communauté internationale voit la sécurité comme une cause commune, cela nous rassemblera sous le même objectif, et nous pourrons attaquer de front les grands défis technologiques et économiques de notre monde.

A lire aussi :

Cisco Live 2014 : cap sur l'Internet of Everything
Un routeur Cisco pour les milliards d'objets de l'Internet of Everything

Crédit photo : Severin Nowacki / World Economic Forum