SÃ©curiser la sÃ©curitÃ© : un enjeu majeur dans le cyber espace
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 12/12/2017 13:30:00

Comment faire naÃ®tre la confiance dans les technologies que nous proposons en tant que fournisseurs ? Ce sujet est incontestablement une question clÃ© qui mÃ©rite dâ□□Ãªtre soulevÃ©e et qui est rarement Ã©voquÃ©e par les Ã©diteurs et concepteurs de solutions de Cyber sÃ©curitÃ©. Il sâ□□agit donc de donner quelques pistes de lecture pour mieux comprendre ce point stratÃ©gique.

Bien comprendre le contexte gÃ©nÃ©ral

Lâ□□actualitÃ© rÃ©cente a montrÃ© que les solutions de sÃ©curitÃ© pouvaient se retrouver dans lâ□□Å□il du cyclone dÃ¨s que leur efficacitÃ© ou leur fiabilitÃ© suscitait le moindre doute.

Par exemple, lâ□□affaire Snowden a rÃ©vÃ©lÃ© aux yeux de tous lâ□□existence du catalogue ANT rÃ©pertoriant les Â« implants Â» et autres Â« portes dÃ©robÃ©es Â» utilisables dans les solutions de sÃ©curitÃ© rÃ©seau pour protÃ©ger et soutenir les intÃ©rÃªts des Ã□tats-Unis.

Cette information, sans Ãªtre vÃ©ritablement une surprise, Ã©tait dÃ©sormais dÃ©voilÃ©e publiquement.

Bien sÃ»r, ces portes dÃ©robÃ©es pouvaient avoir Ã©tÃ© mises en place maladroitement pour des raisons techniques ou Ãªtre liÃ©es Ã des vulnÃ©rabilitÃ©s 0-day. Nombre de fournisseurs impliquÃ©s prÃ©tendirent ne pas avoir dÃ©libÃ©rÃ©ment affaibli leur solution.

Je ne porterai aucun jugement sur ce point, car tel nâ□□est pas mon rÃ´le.

Cependant, au-delÃ de lâ□□impact potentiel sur la souverainetÃ© nationale, les portes dÃ©robÃ©es peuvent avoir dâ□□autres consÃ©quences dramatiques.

Nous avons Ã©tÃ© tÃ©moins des impacts dÃ©sastreux de la fuite rÃ©vÃ©lÃ©e par les Shadow Brokers concernant plusieurs failles de MS Windows utilisÃ©es par la NSA comme des portes dÃ©robÃ©es potentielles.

Les ransomwares Wannacry, NotPetya et mÃªme, plus rÃ©cemment, Bad Rabbit, ont pu se propager Ã grande vitesse grÃ¢ce Ã ces failles.

Je dirais que cette situation met en lumiÃ¨re un dÃ©fi majeur auquel sont confrontÃ©s les fournisseurs de solutions de cybersÃ©curitÃ©.

Nos technologies manipulent et inspectent des fichiers sensibles, traitent et stockent des donnÃ©es personnelles, cryptent des informations confidentielles, accÃ¨dent Ã des ressources dont lâ□□usage est rÃ©glementÃ©, gÃ¨rent des identitÃ©s numÃ©riques, analysent le trafic et les comportements, etc.

Comment garantir Ã nos clients et Ã notre Ã©cosystÃ¨me la fiabilitÃ© de ces opÃ©rations ?

Comment respecter la souverainetÃ© dans un contexte de tensions politiques internationales ? Nous le savons tous : lâ□□Ã©conomie numÃ©rique ne pourra sâ□□Ã©panouir que dans un climat de confiance. Ces questions attendent donc des rÃ©ponses.

Pour les fournisseurs de solutions de sÃ©curitÃ© rÃ©seau, cette question est dâ□□autant plus vitale que le cryptage du trafic est lâ□□un des piliers dâ□□un espace numÃ©rique fiable. Selon Gartner, 80 % du trafic des entreprises sur le web sera cryptÃ© dâ□□ici 2019, ce qui est une bonne chose.

Cela signifie Ã©galement quâ□□un nombre croissant dâ□□attaques par des programmes malveillants (y compris les ransomwares) passeront par HTTPS pour dissimuler lâ□□infection initiale et prendre le contrÃ´le des communications.

Face Ã cette situation, Gartner recommande aux entreprises et organisations de formaliser un plan pluriannuel autour de la mise en place de solutions de dÃ©chiffrement HTTPS et dâ□□un programme dâ□□inspection.

Cette technique dâ□□inspection SSL relÃ¨ve de la mÃ©thode du Man-In-The-Middle, ce qui signifie que nous crÃ©ons un point de vulnÃ©rabilitÃ© dans des communications et des Ã©changes sÃ©curisÃ©s. Une faiblesse dans les produits rÃ©alisant le dÃ©chiffrement et lâ□□inspection SSL pourrait alors entraÃ®ner lâ□□effondrement de toute la chaÃ®ne de confiance.

Quelques pistes envisageables

Tout dâ□□abord, nous pouvons nous fier aux tests effectuÃ©s par des entreprises externes spÃ©cialisÃ©es dans lâ□□Ã©valuation des technologies de sÃ©curitÃ©. Ils sont tout Ã fait Ã mÃªme dâ□□Ã©valuer lâ□□efficacitÃ© de mÃ©canismes de protection.

Cependant, ces tests â□□qui peuvent sâ□□avÃ©rer trÃ¨s onÃ©reux â□□ ne portent pas rÃ©ellement sur la conception en soi de la sÃ©curitÃ©.

Il est Ã©galement possible de sâ□□appuyer sur le cadre dÃ©fini par les critÃ¨res communs, adoptÃ©s par 26 pays. Toutefois, la portÃ©e de lâ□□Ã©valuation, appelÃ©e la cible de sÃ©curitÃ©, est dÃ©finie par le fournisseur lui-mÃªme et peut se limiter Ã une petite partie des logiciels auditÃ©s.

Malheureusement, seuls certains pays mesurent lâ□□importance et Ã©valuent la pertinence de cette cible de sÃ©curitÃ©. Enfin, la dÃ©multiplication des niveaux de garantie du cadre des critÃ¨res communs les rend difficilement comprÃ©hensibles pour les clients.

Nous pouvons Ã©galement Ã©voquer les programmes de Â« bug bounty Â», les logiciels dâ□□analyse statique de code ou les audits indÃ©pendants pour dÃ©tecter et corriger les failles. Ces initiatives sont efficaces pour amÃ©liorer la sÃ©curitÃ© des technologies, parfois dÃ¨s la phase de conception, mais il est difficile de les prÃ©senter comme garantie aux utilisateurs des solutions.

Enfin, les certifications officielles jouent un rÃ´le important. En France, par exemple, lâ□□ANSSI (Agence Nationale de la SÃ©curitÃ© des SystÃ¨mes dâ□□Information) Ã©value le niveau de fiabilitÃ© des produits de sÃ©curitÃ© Ã lâ□□aide dâ□□un cadre spÃ©cifique de qualification, qui est une extension des principes des critÃ¨res communs.

Ce cadre dÃ©finit trois niveaux de qualification basÃ©s sur des cibles de sÃ©curitÃ© prÃ©dÃ©finies. Leur comprÃ©hension sâ□□en trouve donc simplifiÃ©e. Selon le niveau de qualification, un audit de code indÃ©pendant est rÃ©alisÃ© sur des composant essentiels Ã la sÃ©curitÃ©, comme la cryptographie.

Les failles potentielles sont Ã©galement Ã©valuÃ©es, ainsi que lâ□□environnement physique de dÃ©veloppement. Cette mÃ©thode apporte une preuve de la soliditÃ© des produits et de lâ□□absence de vulnÃ©rabilitÃ©s pouvant servir de porte dÃ©robÃ©e.

La nÃ©cessitÃ© de concevoir un cadre global

Le fait que ce cadre de qualification ne soit reconnu quâ□□en France pose toutefois un problÃ¨me. A titre dâ□□exemple, lâ□□Allemagne et le Royaume-Uni disposent dâ□□un cadre propre, Ã©dictÃ© respectivement par le BSI (office fÃ©dÃ©ral de la sÃ©curitÃ© des technologies de lâ□□information) et le NCSC (Centre national de cybersÃ©curitÃ©).

La situation actuelle nâ□□est donc ni Ã©volutive, ni financiÃ¨rement acceptable pour la plupart des fournisseurs qui seraient amenÃ©s Ã passer les certifications dans chaque pays.

Pour crÃ©er un marchÃ© numÃ©rique unique en Europe, bÃ©nÃ©ficiant dâ□□un niveau de confiance appropriÃ© et assurant la souverainetÃ© europÃ©enne, nous devons mettre en Å□uvre des certifications reconnues par lâ□□ensemble des pays europÃ©ens.

Le message semble avoir Ã©tÃ© compris par la Commission EuropÃ©enne qui a prÃ©sentÃ© rÃ©cemment le lancement dâ□□une initiative pour crÃ©er un cadre global de certification en Europe.

Cette mesure constituera une avancÃ©e majeure, Ã la condition quâ□□elle sâ□□appuie sur lâ□□expÃ©rience et les critÃ¨res dâ□□Ã©valuation des pays matures en la matiÃ¨re et quâ□□elle ne constitue pas un nivellement des exigences par le bas.

Un cap et des perspectives nÃ©cessaires

Enfin, le dÃ©veloppement dâ□□un cadre de confiance dans les technologies de sÃ©curitÃ© passera forcÃ©ment par une meilleure collaboration et coopÃ©ration de lâ□□ensemble des parties prenantes de lâ□□Ã©cosystÃ¨me cyber.

Ainsi, les Ã©changes continus entre secteurs public et privÃ©, la crÃ©ation dâ□□alliances entre les fournisseurs de solutions de cybersÃ©curitÃ© et lâ□□implication des clients dans le processus de dÃ©veloppement, par le biais dâ□□une conception conjointe, permettront assurÃ©ment dâ□□Ã©lever le niveau de fiabilitÃ© et dâ□□efficacitÃ© des Ã©quipements de protections.

Matthieu BONENFANT, Directeur Marketing de Stormshield