Sécurité des systèmes d'informations : quels seront les challenges des responsables européens ?

Nous le savons tous, le rÃ´le du RSSI (Responsable de la SÃ©curitÃ© des SystÃ¨mes dâ€™Information) Ã©volue. Il doit Ã la fois avoir les compÃ©tences professionnelles du chef dâ€™entreprise astucieux, Ãªtre un expert technique et maÃ®triser parfaitement PowerPoint.

Des challenges qui viennent sâ€™ajouter Ã dâ€™autres problÃ©matiques moins connues mais auxquelles les RSSI sont confrontÃ©s au quotidien, quel que soit le secteur dâ€™activitÃ©.

Challenge nÂ° 1 : la surcharge dâ€™informations

Ã€ lâ€™Ã©poque de lâ€™Internet des Objets, du Cloud, de la mobilitÃ© et du SaaS, le premier problÃ¨me est que nous gÃ©nÃ©rons beaucoup trop dâ€™informations. Actuellement, en matiÃ¨re de dÃ©tection et de rÃ©ponse aux menaces, nous consignons tout. Pour dÃ©tecter une menace et y rÃ©pondre, il faut savoir ce que nous recherchons. Les systÃ¨mes autonomes et les solutions ad hoc viennent aggraver la situation. Ã‰voquant lâ€™utilisation des informations sur les menaces dans le contexte du terrorisme, le spÃ©cialiste en sÃ©curitÃ© informatique, Bruce Schneier, a Ã©crit que le danger Ã©tait de devoir chercher la mÃªme aiguille dans une plus grosse botte de foin. Il en est de mÃªme pour la cybersÃ©curitÃ©. Les RSSI ont besoin dâ€™indicateurs de compromission et dâ€™informations sur les menaces fiables pour trouver lâ€™aiguille dans cette botte de foin toujours plus grosse.

Challenge nÂ° 2 : les attaques sont dramatisÃ©es et les rÃ©glementations obligent Ã divulguer des informations

Aujourdâ€™hui, il semble que chaque cyberattaque est immÃ©diatement attribuÃ©e Ã une campagne sophistiquÃ©e dirigÃ©e par un Ã‰tat. Cet argument est un moyen dâ€™apaiser les gens, lâ€™idÃ©e Ã©tant que la complexitÃ© de lâ€™attaque est telle quâ€™aucune entreprise ne peut se dÃ©fendre. Nous devons rÃ©flÃ©chir aux techniques, procÃ©dures et outils mis en Å“uvre, mais dans un monde de dissimulation et dâ€™anonymisation, pouvons-nous Ãªtre sÃ»rs de lâ€™identitÃ© de notre attaquant ? Le GDRP (RÃ¨glement gÃ©nÃ©ral sur la protection des donnÃ©es) est un autre aspect Ã prendre en compte. Les entreprises nâ€™auront que 72 heures pour signaler une violation, elles doivent donc mieux maÃ®triser leurs flux de donnÃ©es et avoir une vue plus complÃ¨te des menaces auxquelles elles sont exposÃ©es. Une rÃ©glementation si stricte, va trÃ¨s certainement obliger les entreprises Ã mettre en Å“uvre des plans structurÃ©s de rÃ©ponse aux cyberattaques en vue de reproduire les attaques, de comprendre les responsabilitÃ©s et de transmettre les informations rapidement et avec prÃ©cision.

Challenge nÂ° 3 : le ransomware

Le ransomware est devenu une activitÃ© rentable pour les criminels. Il existe de nombreux programmes dâ€™affiliation dans le cadre desquels des criminels louent lâ€™infrastructure utilisÃ©e pour le ransomware Ã dâ€™autres criminels et prennent un pourcentage sur les bÃ©nÃ©fices. Ce mode opÃ©ratoire repose sur le modÃ¨le de services utilisÃ© dans tous les secteurs dâ€™activitÃ©. Ã€ partir lÃ , les obstacles sont plus faciles Ã surmonter et les criminels sont sans cesse plus nombreux Ã se tourner vers le ransomware. La question qui se pose pour les entreprises est la suivante : faut-il payer ou non la ranÃ§on ? Le coÃ»t pour les entreprises peut Ãªtre Ã©levÃ©, mÃªme si par rapport aux coÃ»ts de la perte de donnÃ©es, elles sont prÃªtes Ã payer le prix. Les RSSI pourraient se poser en champions de la morale et prÃ©tendre que le paiement favorise lâ€™extorsion, mais en fin de compte, les interruptions de service sont coÃ»teuses. Les RSSI commencent Ã Ãªtre confrontÃ©s au ransomware 2.0, cette Ã©volution logique du ransomware consiste Ã cibler la multitude de machines ou objets connectÃ©s que nous appelons lâ€™Internet des objets.

Challenge nÂ° 4 : lâ€™Internet des Objets

La dÃ©finition de Â« lâ€™ordinateur Â» Ã©tant chaque jour plus opaque, il est devenu nÃ©cessaire de sÃ©curiser toutes les ressources connectÃ©es de lâ€™entreprise. La protection ne doit plus uniquement concerner que les Ã©quipements de bureau traditionnels tels que les imprimantes, elle doit Ã©galement couvrir des appareils tels que le rÃ©frigÃ©rateur et la cafetiÃ¨re ! Tous ces Ã©quipements sont des points dâ€™accÃ¨s potentiels permettant aux pirates dâ€™infiltrer le rÃ©seau dâ€™une entreprise et câ€™est aux RSSI quâ€™il revient de mettre en Å“uvre un ensemble cohÃ©rent de contrÃ´les de sÃ©curitÃ©. Cela Ã©tant dit, si nous nâ€™apportons pas une garantie quant Ã la sÃ©curitÃ© de tous les appareils quâ€™il nous incombe de contrÃ´ler, sommes-nous nÃ©gligents si ces appareils commencent Ã attaquer dâ€™autres machines ? Auparavant, la sÃ©curitÃ© visait Ã protÃ©ger la confidentialitÃ©, lâ€™intÃ©gritÃ© et la disponibilitÃ© de nos donnÃ©es, quâ€™en est-il aujourdâ€™hui ? Le RSSI doit-il dÃ©sormais se prÃ©occuper de la protection de lâ€™infrastructure Internet critique ? Si tel est le cas, il faut alors totalement repenser notre approche de la cybersÃ©curitÃ©.

Challenge nÂ° 5 : et si le RSSI Ã©tait lui-mÃªme Ã lâ€™origine dâ€™une attaque DDoS !

Tous les employÃ©s disposent dÃ©sormais de smartphones, de tablettes et dâ€™ordinateurs portables connectÃ©s au monde extÃ©rieur et aux applications SaaS. Une situation qui fait monter en flÃ¨che les besoins rÃ©seau des entreprises. Le problÃ¨me des RSSI est que leur infrastructure rÃ©seau pour le Web nâ€™a pas Ã©tÃ© conÃ§ue pour de tels volumes de trafic et ils craignent que sans technologies dâ€™optimisation de la bande passante et de mise en forme des paquets, lâ€™augmentation du trafic empÃªche dâ€™accÃ©der aux applications mÃ©tiers lÃ©gitimes. Concernant les contrÃ´les de sÃ©curitÃ©, ils sont confrontÃ©s Ã une contrainte supplÃ©mentaire. Les passerelles de sÃ©curitÃ© sont-elles en mesure de faire face Ã lâ€™augmentation du dÃ©bit ? Si oui, quâ€™en est-il face Ã la croissance exponentielle du trafic chiffrÃ© ? Souvent, des compromis sont nÃ©cessaires pour assurer le bon fonctionnement de lâ€™entreprise.

Challenge nÂ° 6 : le conseil dâ€™administration veut des indicateurs clairs et prÃ©cis

GÃ©rer les attentes des membres des conseils dâ€™administration, qui ne sont gÃ©nÃ©ralement pas composÃ©s de professionnels de la sÃ©curitÃ©, est au cÅ“ur des dÃ©fis Ã rÃ©soudre par les

RSSI. De plus en plus, ils financent de nouveaux programmes de cybersÃ©curitÃ© sans comprendre quâ€™ils rÃ©duisent les risques de violation, mais quâ€™aucune structure nâ€™est infaillible. TrÃ¨s souvent, ils ignorent tout des informations concernÃ©es. Il nâ€™est pas nÃ©cessaire quâ€™ils aient connaissance des 350 000 alertes portant sur des malwares qui dÃ©montrent lâ€™efficacitÃ© de lâ€™outil quâ€™ils ont payÃ©. Ils doivent simplement avoir lâ€™assurance que des rÃ¨gles de sÃ©curitÃ© sont en place, Ã©tudiÃ©es et comprises par toutes les parties prenantes. Pour convaincre le conseil dâ€™administration de la crÃ©dibilitÃ© de la stratÃ©gie de sÃ©curitÃ©, il faut Ãªtre en mesure dâ€™identifier les indicateurs de compromission, de rÃ©duire le dÃ©lai de dÃ©tection dâ€™une infection et de garantir une reprise rapide de lâ€™activitÃ© Ã la suite dâ€™une attaque.