Santé mentale des RSSI, agir avant qu'il ne soit trop tard

Selon une Ã©tude menÃ©e par le CESIN, 61% de ses membres ont un niveau de stress susceptible d'avoir des consÃ©quences nÃ©fastes sur leur santÃ©. La prochaine grande menace pour la sÃ©curitÃ© des entreprises ne rÃ©sidera donc peut-Ãªtre pas dans une nouvelle souche de logiciels malveillants ou dans les tactiques, techniques et processus innovants adoptÃ©s par les cybercriminels.

Elle pourrait en effet bien venir de la santÃ© mentale des responsables de la sÃ©curitÃ© des systÃ¨mes dâ€™information (RSSI), du fait de la pression Ã laquelle ils sont confrontÃ©s au quotidien.

Lâ€™Ã©quipe chargÃ©e de la sÃ©curitÃ© nâ€™est pas la seule sous pression au sein des entreprises. Des collaborateurs qui exercent des fonctions diffÃ©rentes doivent Ã©galement rÃ©pondre Ã des objectifs et des exigences trÃ¨s strictes, parfois mÃªme impossibles Ã atteindre. Mais ce qui rend le mÃ©tier du RSSI unique, câ€™est sa relative nouveautÃ© quand la plupart des autres fonctions dâ€™une organisation moderne existent depuis des dÃ©cennies et sont donc relativement bien dÃ©finies.

Un rÃ´le aux responsabilitÃ©s peu claires

Le responsable de la sÃ©curitÃ© IT se retrouve souvent responsable de toute dÃ©faillance liÃ©e Ã la prÃ©sence numÃ©rique dâ€™une organisation, soit des attributions dâ€™une trÃ¨s grande ampleur. Si les donnÃ©es des consommateurs sont compromises, le RSSI peut ainsi Ãªtre tenu responsable de toutes les implications qui en rÃ©sultent en termes de conformitÃ©, de service client et de marque. Si des paiements frauduleux sont effectuÃ©s, il peut Ã©galement Ãªtre tenu responsable des consÃ©quences financiÃ¨res qui en rÃ©sultent, ou bien dans le cas oÃ¹ des machines sont endommagÃ©es ou des processus sont perturbÃ©s Ã la suite dâ€™une attaque. De plus, si des employÃ©s transfÃ¨rent des donnÃ©es dans un systÃ¨me basÃ© sur le cloud, le RSSI en porte encore probablement la responsabilitÃ©, mÃªme si ses Ã©quipes ne sont pas au courant. Et si un nouveau type de menace, inconnu jusquâ€™alors, compromet les systÃ¨mes dâ€™une maniÃ¨re que personne nâ€™aurait pu prÃ©voir, une fois de plus : câ€™est de sa faute.

En rÃ©alitÃ©, tout ce qui a trait Ã la sÃ©curitÃ© des entreprises est plus nÃ©buleux en termes de responsabilitÃ©. Quel que soit le niveau hiÃ©rarchique dans lâ€™entreprise, les rÃ´les en matiÃ¨re de sÃ©curitÃ© sont rÃ©cents et ne bÃ©nÃ©ficient que rarement dâ€™une description de poste standard, par rapport aux autres fonctions dans lâ€™entreprise. Par exemple, la gestion des contrÃ´les dâ€™accÃ¨s peut relever de la compÃ©tence du RSSI dans une organisation, tandis que dans une autre, cela sera la responsabilitÃ© de lâ€™Ã©quipe rÃ©seau.

Les attentes extÃ©rieures

La pression est dâ€™autant plus forte que la direction nâ€™a pas forcÃ©ment des attentes rÃ©alistes quant Ã la capacitÃ© du RSSI, et de son Ã©quipe, Ã protÃ©ger les donnÃ©es et les applications de lâ€™entreprise. Les CEO, CFO, COO et directeurs juridiques considÃ¨rent souvent la sÃ©curitÃ© comme une Ã©quation mathÃ©matique. Ils pensent que le responsable de la

sÃ©curitÃ© est en mesure dâ€™identifier toutes les lacunes possibles, puis de les combler. La proposition semble simple mais, dans la rÃ©alitÃ©, la sÃ©curisation dâ€™une infrastructure dâ€™entreprise vaste et dynamique est tout sauf un exercice facile.

De plus, lâ€™Ã©quipe de direction et le conseil dâ€™administration attendent souvent du RSSI une rÃ©ponse immÃ©diate Ã toutes les questions quâ€™ils peuvent se poser. Si la personne est incapable de rÃ©pondre Ã lâ€™instant T, ses performances professionnelles sont susceptibles dâ€™Ãªtre remises en question, directement ou indirectement. Pourtant, lâ€™organisation peut utiliser plusieurs centaines dâ€™applications et dâ€™outils, qui se sont accumulÃ©s au fil des ans. Avoir besoin de temps pour se pencher sur une question, et enquÃªter en consÃ©quence, nâ€™est donc pas si surprenant.

Par ailleurs, les attentes des clients en termes dâ€™expÃ©rience dâ€™achat et de qualitÃ© de services, mais aussi de respect de la vie privÃ©e et la confidentialitÃ© des donnÃ©es, ajoutent une pression supplÃ©mentaire sur lâ€™Ã©quipe de sÃ©curitÃ©. En effet, des consommateurs insatisfaits ne vont pas hÃ©siter Ã abandonner leurs achats ou Ã se plaindre sur les rÃ©seaux sociaux ; ce qui impacte directement le chiffre dâ€™affaires et la rÃ©putation de lâ€™organisation. Enfin, lâ€™environnement rÃ©glementaire nâ€™est pas Ã nÃ©gliger dans les charges mentales qui sâ€™exercent au quotidien sur les RSSI : beaucoup dâ€™entre eux doivent dÃ©montrer Ã de nombreux organismes compÃ©tents que leur entreprise garantit la sÃ©curitÃ© dans des domaines spÃ©cifiques.

Pour certains RSSI, ces facteurs de stress sont aggravÃ©s lorsquâ€™un sentiment de responsabilitÃ© vis-Ã -vis de la communautÃ© ou de la nation vient sâ€™ajouter aux missions confiÃ©es. Des olÃ©oducs aux entitÃ©s gouvernementales, en passant par les Ã©tablissements de santÃ©, sont autant dâ€™infrastructures critiques qui ont rÃ©cemment Ã©tÃ© impactÃ©es par des ransomwares. La sÃ©curitÃ© nationale est dÃ©sormais Ã lâ€™ordre du jour des responsables de la sÃ©curitÃ©, un enjeu qui ne peut pas Ãªtre ignorÃ© mais pour lequel ils nâ€™ont pas forcÃ©ment reÃ§u de formation.

Les consÃ©quences sur la santÃ© mentale

Tous ces facteurs sâ€™accumulent et crÃ©ent une anxiÃ©tÃ© importante chez de nombreux RSSI et au sein des Ã©quipes de sÃ©curitÃ©. En parallÃ¨le, les hackers mettent continuellement les compÃ©tences de ces professionnels Ã lâ€™Ã©preuve, Ã la recherche de la moindre erreur quâ€™ils pourraient exploiter Ã leur avantage. Du point de vue de la santÃ© mentale, le bilan est donc lourd. Cependant - Ã lâ€™inverse des militaires, par exemple, qui sont soumis Ã des pressions similaires - les Ã©quipes de sÃ©curitÃ© manquent de lisibilitÃ© sur leur mission ainsi que dâ€™une structure de soutien ; obtenues au fil des siÃ¨cles par les forces armÃ©es.

De nombreux RSSI ont ainsi Ã©tÃ© touchÃ©s par des problÃ¨mes de santÃ© mentale ces derniÃ¨res annÃ©es. Pourtant, beaucoup dâ€™entre eux hÃ©sitent Ã en parler. En effet, sâ€™il est facile de demander Ã la direction des ressources ou des outils supplÃ©mentaires en argumentant chiffres Ã lâ€™appui une meilleure rentabilitÃ©, il est plus difficile de justifier un soutien psychologique. Des RSSI estiment Ã©galement que cela serait perÃ§u comme un manque de compÃ©tences et quâ€™une discussion sur le sujet indique quâ€™ils sont inaptes pour accomplir leur travail.

Cependant, laisser les problÃ¨mes de santÃ© mentale sâ€™envenimer peut avoir des consÃ©quences dÃ©sastreuses qui viendraient sâ€™ajouter Ã la pÃ©nurie de personnel de sÃ©curitÃ© :

Lâ€™Ã©puisement professionnel (burn-out) des RSSI, un phÃ©nomÃ¨ne que beaucoup connaissent dÃ©jÃ dans une certaine mesure ;

Le choix de certains jeunes diplÃ´mÃ©s de ne pas poursuivre une carriÃ¨re dans la sÃ©curitÃ©, parce quâ€™ils ne veulent pas en subir le stress.

Un turn-over Ã©levÃ©. En effet, une Ã©tude de ThreatConnect montre que les niveaux de stress Ã©levÃ©s figurent parmi les trois principales causes de dÃ©part des employÃ©s, citÃ©e par 27 % des personnes interrogÃ©es.

La gestion du stress par lâ€™automÃ©dication et lâ€™alcool ; un effet, trÃ¨s alarmant, du tabou autour de la santÃ© mentale. DÃ©but 2019, avant la pandÃ©mie, Forbes avait publiÃ© les rÃ©sultats dâ€™une enquÃªte dans laquelle 1 RSSI sur 6 admettait se tourner vers ces options pour faire face au stress liÃ© au travail. Mais ils Ã©taient probablement beaucoup plus nombreux Ã ne pas admettre Ãªtre dans une situation semblable Ã lâ€™Ã©poque.

Or, le niveau de stress des RSSI a augmentÃ© pendant la pandÃ©mie, en raison de la mise en place du tÃ©lÃ©travail et de la nÃ©cessitÃ© dâ€™accÃ©der aux ressources numÃ©riques Ã tout moment ; ce qui a multipliÃ© les risques de compromission et de perturbation. Tous ces bouleversements et le besoin dâ€™augmenter la productivitÃ© ont eu des rÃ©percussions sur la santÃ© mentale des responsables de la cybersÃ©curitÃ© et reprÃ©sentent une manne pour les cybercriminels. Un RSSI moins vigilant constitue en effet un risque majeur pour la sÃ©curitÃ©.

Que faire ?

Les entreprises doivent sâ€™attaquer Ã la crise de la santÃ© mentale, tant pour garantir une rÃ©ponse rationnelle lorsque la sÃ©curitÃ© de lâ€™organisation est en jeu, que pour former, attirer et fidÃ©liser les meilleurs talents pour faire face aux cybermenaces. Pour ce faire, les directions doivent prendre conscience du niveau de pression auquel les RSSI et leurs Ã©quipes sont soumis au quotidien. Lâ€™objectif est de promouvoir auprÃ¨s de ces Ã©quipes un Ã©quilibre sain entre vie professionnelle et privÃ©e, et de veiller Ã ce que lâ€™entreprise offre un environnement sÃ»r pour solliciter une aide en matiÃ¨re de santÃ© mentale. Il est Ã©galement nÃ©cessaire de mettre en place des outils simples pour gÃ©rer le stress, qui ne soient ni chronophages ni pÃ©nalisant pour les RSSI.

Au sein dâ€™une entreprise, chacun a son rÃ´le Ã jouer dans la sensibilisation des dirigeants Ã cette crise susceptible dâ€™Ã©merger Ã tout moment, afin quâ€™ils prennent conscience que ce travail est difficile et que de nombreux RSSI nourrissent des inquiÃ©tudes lÃ©gitimes quant Ã la possibilitÃ© dâ€™Ã©voquer des problÃ¨mes de santÃ© mentale. Il convient de rappeler aux dirigeants dâ€™entreprise quâ€™ils doivent tendre la main Ã leur responsable de la sÃ©curitÃ© IT de maniÃ¨re proactive et sans jugement. Car si les RSSI seront toujours sous pression du fait de leurs tÃ¢ches complexes et importantes, il existe des mÃ©thodes qui peuvent aider Ã attÃ©nuer ce stress.