Le RSSI : promoteur de la doctrine de sécurité de son entreprise

Par Hervé Schauer, Fondateur d'HSC

La SSI est une fonction transverse comme la qualité, le juridique, ou... la DSI. Le RSSI est responsable de la SSI, mais à quoi sert la SSI ? Que fait un RSSI ?
Sert-il à la continuité ? Le RSSI n'est pas nécessaire pour assurer la continuité des SI, il est rarement impliqué dans la redondance de liens, le RAID, ou les sauvegardes... Il n'est pas toujours impliqué dans les PRA/PCA, mais généralement consulté. Regardez qui gère les incidents de disponibilité des systèmes d'information, c'est généralement la DSI.
Sert-il à la confidentialité ? Oui, le RSSI est souvent impliqué.
Sert-il à l'intégrité ? Le RSSI sera souvent impliqué dans les cas de malveillance, mais plus rarement de simples bogues ou la corruption (usure physique...), qui ne relèvent pas de problèmes de sécurité.

Le RSSI est toujours moteur dans la réduction des risques en sécurité des systèmes d'information, parce qu'il est là pour y penser et personne d'autre ne le fera à sa place. C'est l'effet immédiat de son apparition, c'est son rôle opérationnel, avec une approche du bas vers le haut (bottom-up). Mais, le RSSI doit aussi être moteur dans la vision de son entreprise sur le long terme, il peut ne pas se placer dans les mêmes cycles courts que d'autres responsables, c'est son rôle plus orienté fonctionnel avec une approche du haut vers le bas (top-down). Cette double approche complémentaire est indispensable et aucun RSSI ne peut se défaire de l'une ou de l'autre.

Dans son approche opérationnelle, le RSSI doit faire en sorte de faire appliquer sans délai toutes les mesures de sécurité issues des bonnes pratiques qui manquent dans son périmètre (SANS Top 20, ISO 27002, etc.). Il va immédiatement mettre en oeuvre et formaliser une gestion des incidents liés à la sécurité de l'information. S'il ne le fait pas, il sera discrédité lors de l'arrivée du premier incident, qui ne sera pas forcément un incident lié à la sécurité, mais une patate chaude refilée aux bizuts. Sans processus de gestion des incidents de sécurité en place, il ne saura pas assez rapidement démontrer pourquoi cela ne relève pas des incidents de sécurité. Il va aussi faire connaître son existence et expliciter son rôle via une sensibilisation adaptée à chaque population démontrant l'utilité et l'importance de sa fonction. S'il a déjà du budget, il pourra mandater un diagnostic externe pour appuyer ses constats sur la situation. Pour cela, un RSSI doit avoir une parfaite maîtrise technique, il a besoin d'être techniquement compétent, afin de comprendre les dispositifs techniques. Ne serait-ce que comme conseil ou comme expert sécurité, auprès de

la DSI, de la bureautique ou du réseau; il doit savoir acheter des produits de sécurité sans se faire berner. Enfin, le RSSI doit, par lui-même, pouvoir contrôler les configurations des dispositifs techniques et savoir expliquer quelles corrections il faut apporter, auprès des opérationnels responsables, dans la configuration d'un firewall, comme dans la configuration d'Active Directory. Il doit savoir manipuler tout seul un logiciel de tests de vulnérabilités, comme Nessus, nul n'est besoin d'être encore expert technique pour cela.
Dans son approche fonctionnelle, le RSSI structure et formalise la vision de la SSI dans son entreprise. C'est moins urgent, mais indispensable, de savoir expliquer et démontrer à la hiérarchie qu'elle doit s'engager elle-même vis-à-vis de tout l'organisme dans la sécurité et que c'est une clé de la réussite. C'est ce qui est généralement appelé « politique de sécurité »; je préfère le terme de doctrine à la sécurité des systèmes d'information qui montre mieux l'engagement et évite la confusion avec politique au sens anglais « politics » et pas « policy ». L'engagement de la direction permet d'appliquer le PDCA (Plan-Do-Check-Act) de l'ISO 27001, et donc de formaliser et d'engager le métier du RSSI dans une activité continue qui perdurera. Là, le RSSI aura été moteur dans la vision de son entreprise et pourra décliner cette fois-ci du haut vers le bas la SSI, de la politique de sécurité il pourra faire une appréciation des risques, un plan de traitement des risques, démontrer le retour sur investissement des mesures de sécurité, lancer des audits pour vérifier la bonne mise en oeuvre des dispositifs de sécurité.
Sans compétence technique, le RSSI perd sa crédibilité dans son rôle fonctionnel, et il ne peut faire une appréciation des risques. Cependant, il ne doit pas avoir l'image d'un pur technique parce qu'il sait trouver les failles et demander les corrections. Il en sera d'autant plus crédible sur le plan opérationnel, parce qu'il est un RSSI fonctionnel qui a le soutien de sa direction.
L'approche de bas en haut est une gestion des risques au bon sens et à l'intuition, qui comme le dit Alexandre Fernandez-Toro, RSSI chez un industriel et formateur chez HSC, « permet de sortir de la zone d'humiliation » le plus rapidement possible. L'approche du haut vers le bas passe par une gestion des risques systématique qui permet le compromis entre les objectifs et les moyens. Cette gestion des risques, encore très peu répandue en dehors des grands pays européens, évite les tendances maximalistes de certaines influences : voyez les cycles trop longs, les projets trop coûteux, et les déploiements finalement plus limités que prévus pour réduire des coûts exponentiels. Elle oblige la direction à identifier ce qui compte le plus pour elle et à ordonnancer l'importance des actifs de l'organisme entre eux.

Un RSSI doit avoir envie de faire avancer le schmilblick de la SSI

Un RSSI doit avoir envie de faire avancer le schmilblick de la SSI, sans jamais être perçu comme un frein à l'innovation, à la productivité et au confort des utilisateurs. Pour chaque dispositif de sécurité en place, le RSSI doit savoir répondre à l'improviste quels risques ce dispositif permet de réduire. S'il ne sait pas, il y a un problème.
Le RSSI est concerné par tous les systèmes d'information : en premier lieu, les systèmes informatiques que la DSI connaît, mais aussi la téléphonie, les documents en format papier, maintenant les systèmes industriels, enfin les comportements humains... Comme on a l'habitude de le dire : « Quand on parle, c'est en clair, ce n'est pas chiffré » ! Mais la sécurité des systèmes d'information s'applique aussi aux infrastructures spontanées, dont tout le monde se sert et pour lesquelles « personne n'est au courant des risques car

Feature

CISO: promoter of the security doctrine in the enterprise

By Hervé Schauer, Founder of HSC

The Information Security System is a cross-functional operation like Quality Control, Legal offices, or ... the CIO. The CISO is responsible for ISS but what is the ISS for? And just what does a CISO do? Business continuity? The CISO is not necessarily involved in ensuring continuity of the information system, rarely concerned with link redundancy, RAID, or backups ... not always engaged in the DR / HA, but is nonetheless often called upon. Usually you find it's the CIO who ends up managing information system availability failure or downtime. Confidentiality? Yes, the CISO is often involved with this. Integrity? The CISO will often have to deal with malicious attacks, but more rarely with simple bugs or corruption (physical wear ...), which are not security issues.

ils demeurent invisibles… le Cloud, le big data. Derrière ces mots, il y a belle lurette que les utilisateurs ont fait d'Internet leur tuyau vers la liberté des applications achetées en un clic, et les RSSI ne doivent pas accepter que cette exportation de données appartenant à l'entreprise, soumises parfois à des législations, soient sorties sans l'application de la politique de sécurité. Le RSSI doit donc plus que quiconque anticiper les besoins, connaître les métiers, faire une appréciation des risques en amont pour accompagner chaque nouveauté afin qu'elle respecte les objectifs de la direction exprimés dans la politique de sécurité.

L'existence du RSSI est souvent plus importante que son rattachement hiérarchique proprement dit

Une question récurrente est la place du RSSI dans l'organisation… pas une conférence où la question « le RSSI doit-il être à la direction des risques ou à la DSI ? » ne soit posée. Dans une organisation avec peu de maturité SSI, où le poste de RSSI est nouvellement créé, il sera naturellement le plus souvent sous l'autorité du DSI, et portera ses premiers effets sur les projets de la DSI, tant que cela n'est pas trop coûteux. Dans une organisation avec une bonne maturité SSI, le RSSI aura un double rattachement, RSSI à la DSI en termes hiérarchiques, mais il rendra compte en dehors, à la DG, ou à la direction des risques opérationnels, ou à la direction de la conformité ou tout équivalent. Dans une organisation avec une très bonne maturité SSI, il y aura souvent une dualité du poste : un RSSI opérationnel, maîtrise d'oeuvre de la SSI, qui se trouve au sein de la DSI, et un RSSI stratégique, maîtrise d'ouvrage, nécessairement en dehors de la DSI, ou parfois en dehors de l'organisme lui-même dans une structure de groupe avec des filiales. Cela peut être aussi parfois un RSSI hybride à mi-temps dans chaque activité, ou un RSSI proche du métier mais placé dans un rôle fonctionnel SSI. Toutefois, l'important est souvent plus l'existence du RSSI, le fait qu'il soit là, motivé et compétent, que son rattachement hiérarchique proprement dit. Il convient de s'adapter au contexte politique et aux susceptibilités existantes, et faire progresser la maturité de la SSI. Grâce à celle-ci, le RSSI pourra progresser dans la hiérarchie.

Le RSSI en place depuis de nombreuses années est confronté à une explosion des coûts, liés à la maintenance des infrastructures de sécurité et du personnel nécessaire à leur exploitation. Il est confronté à l'évolution des systèmes vers toujours plus de complexité, ce qui permet de valider le fait que personne n'est capable de tout maîtriser. Et il est confronté à l'échec de la sécurité démontré à maintes reprises par un expert comme Nicolas Ruff, ou par l'actualité des organismes victimes de logiciels malfaisants. Il convient que le RSSI se pose ouvertement la question de l'adéquation des moyens mis en oeuvre pour réduire les risques à leurs besoins, à la pertinence de l'appréciation des risques qu'il n'a peut être pas mise à jour, comme l'imposent l'ISO 27001 et ISO 27005, qu'il reparte d'une analyse intrinsèque, c'est-à-dire comme s'il n'avait rien pour voir ce qui serait vraiment utile ici. L'engouement vers l'infogérance ou le Cloud permet en fait de déporter une complexité locale vers une complexité « lointaine » que l'on ne voit plus, mais qui est pourtant parfois pire, parole d'auditeur. Dans les grandes entreprises, ce sont les équipes de réponse aux incidents qui se développent, et elles nécessitent de plus en plus de personnels qualifiés. Cela a tendance à rendre l'expert sécurité expérimenté rare et courtisé, ce qui, à terme, ne peut qu'encore augmenter les coûts de la SSI. Chaque entreprise dispose de son équipe « CERT », et fait en plus appel à des sociétés privées. Il y aurait là matière à mutualiser pour réduire les coûts, si les RSSI le voulaient.

La SSI est une fonction qui devient importante; cependant, il n'existe aucune organisation idéale de celle-ci, il faut s'adapter, et réintroduire de l'humain dans les processus. ■■■

Retrouvez notre fil d'informations sur la sécurité et le stockage sur :
www.globalsecuritymag.fr
www.globalsecuritymag.com