Des RSSI réunis autour d'un défi de cybersécurité au Forum international de la cybersécurité à Lille.

Morgane Remy

Profession : pare-feu « anti-hackers »

Très recherchés par les banques, les « responsables de la sécurité des systèmes d'information » sont au cœur de la lutte contre les cyberattaques.

http://www.agefi.fr/emploi

PAR MORGANE REMY

Au 9e Forum international de la cybersécurité qui s'est tenu à Lille les 24 et 25 janvier, les « *hacking trucks* » ont dû beaucoup intéresser les responsables informatiques de banques… Et pour cause, au sein de ces véhicules mobiles, des étudiants d'écoles spécialisées ont réalisé des démonstrations de cyberattaques : le clone d'empreinte digitale qui permet notamment de déverrouiller un *smartphone*, le « *ransomware* » (logiciel de rançon) dont la spécialité est de prendre en otage des informations personnelles, ou encore le « *poison tap* », un équipement peu coûteux qui permet de siphonner toutes les données d'un ordinateur. Les banques étant des cibles de choix pour les cybercriminels, les professionnels de la finance ont tout intérêt à bien connaître ces pirates du numérique dont les agissements sont facilités par l'explosion des connexions bancaires à distance. C'est l'un des revers de la « digitalisation » : l'essor, ces dernières années, des canaux de contact non physiques a rendu les systèmes informatiques bancaires vulnérables face à des « *hackers* » de plus en plus sophistiqués. « *Nous observons une hausse sensible du volume de cyberattaques*, témoigne David Mingot, 44 ans, directeur de la sécurité chez Natixis, où ce mathématicien de formation travaille depuis une dizaine d'années. *Les hackers les plus avancés sont capables d'être très patients pour collecter de l'information via les réseaux sociaux, en se mettant en contact avec des*

employés, en prenant le temps d'observer une fois qu'ils sont entrés dans le système. » Face à ce phénomène, le législateur s'en est aussi mêlé : en plus des normes bancaires contraignantes, la loi de programmation militaire classe les grandes banques comme des « *opérateurs d'importances vitale* » (OIV) et leur impose de sécuriser encore davantage leur informatique.

Double compétence

Au cœur des dispositifs bancaires de lutte contre la cybercriminalité, les responsables de la sécurité des systèmes d'information (RSSI) jouent un rôle central. Une de leurs principales missions : détecter les attaques informatiques. « *Nous étudions et développons par exemple de nouvelles techniques comme le 'data mining' pour nous permettre, sur la base de journaux d'événements, de détecter des comportements anormaux non détectables par les outils traditionnels de surveillance*, raconte Joseph Schwartz, 55 ans, directeur sécurité chez BPCE Infogérance et Technologies, formé à Télécom Paris. *Il est aussi important d'investir dans une démarche complémentaire de veille pour comprendre l'évolution des cyberattaques et les anticiper.* » Pour mener cette bataille, les banques étoffent leurs effectifs. « *J'ai recruté six personnes en 2016, deux seniors et quatre profils plus juniors, tous très pointus grâce à leur formation de base et/ou leur retour d'expérience opérationnelle* », ajoute Joseph Schwartz. Les recruteurs prennent le parti d'employer de jeunes ingénieurs qui, fraîchement diplômés, sont au fait des technologies innovantes. D'autant que, depuis janvier 2017, plus d'une vingtaine de formations supérieures dédiées à la sécurité du numérique peuvent se targuer du label « SecNumedu » (*lire aussi l'encadré page 40*) de l'Agence nationale de la sécurité des systèmes d'information (Anssi). Créée l'an dernier, cette labellisation vise à renforcer ce type d'enseignement en France mais aussi à faciliter les recrutements pour les entreprises. Justement, de nombreux postes sont à pourvoir dans les banques de la place parisienne. « *Rien que dans le réseau de la banque de détail France, notre équipe a été multipliée par cinq en cinq ans* », illustre Yann Girard, 42 ans, directeur de l'audit informatique de la Société Générale (*lire le témoignage ci-dessus*). La double compétence informatique-banque est souvent un impératif. « *Depuis quelques années, nous renforçons notre équipe de RSSI*, déclare David Mingot. *Si tous doivent avoir un parcours très technique, nous veillons à ce qu'ils connaissent très bien le métier de la banque auquel ils sont dédiés : affacturage, moyens de paiement, activité de marchés, de crédits…* »

Les jeunes ingénieurs, plus au fait des technologies innovantes, sont très prisés

Dans ce contexte, la promotion interne est privilégiée afin d'accroître les compétences de ces experts tant sur le plan informatique que bancaire. Tous les professionnels à des postes de responsabilité ont un point commun : des parcours dynamiques au sein de l'établissement financier qu'ils ont rejoint. Chez Natixis, des postes de « *security and continuity manager* » ont été créés, en binôme avec les RSSI. Ils permettent de recruter des profils plus juniors qui, après un apprentissage de quatre ou cinq ans, deviendront eux-mêmes RSSI. « *Nous privilégions les collaborateurs qui ont grandi chez nous car ce métier est vraiment à la croisée des chemins entre le technique et l'opérationnel* », explique David Mingot. Même avant la création de ce vivier, les parcours internes étaient favorisés. C'est ainsi qu'Olivier Baranek est devenu RSSI de la banque de finance et d'investissement de BPCE, après un début de carrière dans des sociétés de conseil en sécurité informatique. « *Cela fait dix ans que je travaille chez Natixis, dans le domaine de la sécurité et que je m'améliore au contact du terrain*, dit-il, enthousiaste de toujours progresser chez son employeur. *J'ai eu la chance de pouvoir évoluer dans différents postes et métiers, afin de construire ma carrière et d'élargir en permanence le champ de mes responsabilités.* » Sa trajectoire est loin d'être atypique dans le secteur bancaire, a fortiori dans les métiers de la sécurité informatique ▶

TÉMOIGNAGE


DR

Yann Girard, 42 ans, responsable de la sécurité des systèmes d'information des réseaux France de la Société Générale

« Les sponsors de nos projets se situent à des niveaux très élevés »

« Ingénieur, j'ai commencé ma carrière de façon classique dans le développement informatique, puis je l'ai poursuivie dans l'ingénierie système, et enfin dans l'intégration de solution de sécurité au sein d'une petite société de conseil. Lassé de passer d'un sujet à un autre sans pouvoir les suivre sur la durée, j'ai rejoint Axa en 2001. Au sein du groupe d'assurance, j'ai rapidement pu progresser, en prenant en charge un projet de mise en conformité avec la loi américaine. Fort de cette expérience, j'ai pu rejoindre la Société Générale en 2008. Intégrer l'univers de la banque, très mature sur les questions de sécurité, a été une chance. Je peux approfondir les dossiers que je traite, augmenter mon champ d'action au fur et à mesure que je progresse, tisser des liens avec les opérationnels de la banque. J'apprécie de devoir comprendre leurs besoins, de travailler avec eux à la mise en place de solutions favorisant le développement de la banque tout en maintenant des conditions de sécurité optimales. Enfin, les sponsors de nos projets se situent à des niveaux très élevés. Celui sur lequel je travaille actuellement est ainsi porté directement par le responsable de la banque de détail en France de la Société Générale. »

Capitaliser sur le savoir-faire des RSSI, un impératif

où former et promouvoir les talents est désormais un enjeu crucial. « *Le 'digital' est porteur de nouveaux concepts – Blockchain, 'big data', méthode agile… –, les banques ont tout intérêt à capitaliser sur le savoir-faire de leurs RSSI* », souligne Alain Bouillé, président du Club des experts de la sécurité de l'information et du numérique (Cesin).

Salaires en progression

Non seulement les banques veillent à ce que leurs informaticiens évoluent en interne mais elles cherchent également à leur offrir des salaires attractifs… qu'elles préfèrent ne pas communiquer dans un contexte de concurrence exacerbée sur le marché du travail. Alain Bouillé, très souvent consulté pour dénicher la « perle rare » dans la sécurité informatique, a une bonne connaissance des rémunérations : « *Un RSSI avec quelques années d'expérience en cabinet percevra entre 50.000 et 60.000 euros brut par an, la grande majorité des postes se situant entre 60.000 et 100.000 euros brut par an. Les RSSI de grandes banques, de plus de cinq ans d'ancienneté, touchent en moyenne 100.000 euros et les RSSI groupe sont au moins à 150.000 euros.* » Les salaires continuent à progresser, portés par le phénomène de rareté. Il y a beaucoup moins de candidats que de postes, et encore moins de professionnels expérimentés à la fois techniquement et sur les métiers bancaires. « *Le rapport de force est très favorable aux salariés*, poursuit Alain Bouillé. *Toutes les entreprises, les cabinets de conseil et même la prestigieuse Anssi recrutent actuellement, créant une vive concurrence pour les banques historiquement présentes sur ce marché.* » En effet, en changeant d'employeur, ces informaticiens spécialisés peuvent obtenir sans peine une augmentation de salaire d'au moins 10 %.

Néanmoins, un paradoxe apparaît : tandis que les ressources humaines s'emploient à proposer des parcours variés et évolutifs, avec un changement de poste en moyenne tous les cinq ans, certains spécialistes fiers de leur niche ne souhaitent pas forcément changer de métier. « *Ils cherchent alors à changer de banque pour obtenir plus de responsabilités sans devoir changer de secteur ou de spécialité*, observe un responsable. *Comme ils ne peuvent pas le faire en interne, ils deviennent très sensibles aux tentatives de débauchage.* » Si le parcours de mobilité interne a parfois du mal à s'imposer dans ce métier, certains professionnels le voient comme un mouvement sain. « *Le turnover interbancaire est plutôt positif en termes d'échanges de bonnes pratiques*, note David Mingot. *Cette circulation permet de partager les meilleures méthodes.* » Et de pouvoir affronter des pirates informatiques dont les « compétences » sont, elles aussi, en constante progression… ■

TÉMOIGNAGE

DR

Marc Zanoni, 53 ans, directeur sécurité des systèmes d'information du groupe BPCE

« Le métier nécessite de travailler avec toutes les directions du groupe »

« Nous avons des équipes spécialisées dans la lutte contre la cybercriminalité. Les profils sont diversifiés, allant de l'opérateur bac+2 à l'expert de niveau bac+5, car les compétences requises ne sont pas les mêmes selon la nature et la complexité des incidents. Le métier est très transversal. Il nécessite de travailler avec toutes les directions du groupe, de réagir vite et de bien comprendre les enjeux afin d'apporter une réponse adaptée. Mais la pierre angulaire de notre protection reste la vigilance des collaborateurs. Nous avons ainsi largement déployé des modules d''e-learning', des 'serious games', et relayé la Hack Academy, une campagne de sensibilisation à la protection des données sur internet, conduite par le Club informatique des grandes entreprises françaises (Cigref). Le partage d'information entre les acteurs constitue un enjeu crucial. Au niveau interbancaire, un pas important a été franchi avec la loi de programmation militaire 2014-2019. Elle a favorisé une plus forte coopération entre les principales banques de la Place en matière de cybersécurité. La communauté des RSSI (responsables de la sécurité des systèmes d'information, NDLR) *des banques s'est renforcée. »*

Un label pour les formations dédiées à la cybersécurité

Afin de pallier la pénurie de compétences dans la sécurité informatique en France, le monde académique et celui de l'entreprise s'activent. Au Forum international de la cybersécurité, 26 formations de l'enseignement supérieur dédiées à la sécurité numérique se sont vu remettre, par l'Agence nationale de la sécurité des systèmes d'information (Anssi), les certificats (*photo*) qui attestent leur labellisation « SecNumedu » (attribuée pour trois ans renouvelables). Pour décrocher ce label, ces universités, instituts universitaires de technologies, écoles d'ingénieurs, etc., ont dû se conformer à une charte et des critères précis. Par ailleurs, Orange a inauguré le 24 janvier un nouveau centre de cyberdéfense à Lesquin, dans le nord de la France, qui sera notamment consacré à la formation des collaborateurs et aux étudiants de la région. Le groupe de télécoms lance aussi sa propre formation à travers l'Orange Cyberdefense Academy. De quoi donner peut-être des idées à la Société Générale dont le campus informatique de Seclin, dédié à la DSI des réseaux en France, n'est situé qu'à une petite dizaine de kilomètres du nouveau site d'Orange…

Anssi