Systèmes d'information organisationnels

2e édition

Coordination : Pascal Vidal et Vincent Petit

Avec François Lacroux, Marc Augier, Valéry Merminod, Marc de Gibon, Christophe Mangholz

ISBN : 978-2-7440-7296-3

Activités de la 1ere édition

Chapitre 10. Sécurité des systèmes d'information

Encadré 10.1 : Sodebo : la sécurité commence avec la gestion centralisée des mots de passe

Le traiteur Sodebo, basé à Montaigu (près de Nantes) et connu pour sa production de pizzas commercialisées dans les grandes surfaces, a décidé de sécuriser son système d'information. Cette entreprise n'a jamais subi de tentative d'intrusion informatique, mais par précaution, elle souhaite se protéger contre le risque de vol de secrets de fabrication ou simplement de sabotage industriel. Son chiffre d'affaires croît de 11 % par an depuis plusieurs années et la sécurité alimentaire constitue l'une des clés de sa réussite.

Quand il intègre la société en septembre 2001 en tant que directeur informatique, Fabrice Lacheref contribue à cette prise de conscience sécuritaire. Il participe à la mise en œuvre d'une politique globale de sécurité, avec la création d'un bâtiment dédié à l'informatique et doté d'un dispositif sophistiqué de contrôle d'accès par badge et lecture biométrique. Dans ce projet sécuritaire global, le contrôle d'accès au système d'information constitue l'une des parades essentielles, comme le souligne Fabrice Lacheref : « Le contrôle d'accès, c'est le b.a.-ba de la sécurité ! » Or, jusqu'en 2002, Sodebo n'utilise pas de véritable gestion des mots de passe.

L'hétérogénéité des systèmes (deux AS/400 partitionnés supportant l'ERP de production Movex, deux Risc 6000 sous Unix hébergeant une application Siebel, de multiples serveurs dont l'un de messagerie Lotus Notes et plus de 500 PC clients sous Windows) multiplie les codes d'accès (une gestion de mots de passe par système) et les rend ingérables pour les utilisateurs. Ainsi, des post-it traînent un peu partout, avec des mots de passe écrits lisiblement ! Le recours à un outil qui simplifie et centralise cette gestion des habilitations s'impose donc. Après une étude des solutions disponibles sur le marché, le Control-SA de l'éditeur BMC Software est choisi, pour plusieurs raisons techniques.

Premièrement, il existe peu de produits capables de prendre en compte le monde assez fermé de l'AS/400 : Control-SA sait le faire. Deuxièmement, le contrôle d'accès proposé par BMC n'est pas centralisé sur un serveur unique, dont l'arrêt imprévu aurait risqué de bloquer l'ensemble des applicatifs de production. De plus, le logiciel sait gérer l'accès à toutes les applications pour lesquelles l'utilisateur est habilité par un mot de passe unique et renouvelable une fois par mois : finis les mots de passe multiples ! Enfin, la gestion des habilitations est centralisée sur une console d'administration qui permet de créer des « comptes » par utilisateur et de visualiser leur état. Une interface activée avec un module de gestion des temps permet de verrouiller automatiquement le système à tout salarié quittant la société. Après une phase pilote, Control-SA est déployé à l'ensemble du système d'information, dès le printemps 2003.

Bien sûr, la mise en place des contrôles d'accès doit passer par un accompagnement et une sensibilisation à la problématique sécuritaire, comme le souligne Fabrice Lacheref. Pour changer les comportements des centaines d'utilisateurs, il faut inventer des astuces (diffusion de livrets, invention de jeux, etc.). Mais l'objectif est atteint : les utilisateurs ne laissent plus traîner de post-it avec leurs codes d'accès, changent régulièrement leur mot de passe et verrouillent leur session de travail. Centralisée, l'administration des habilitations et des accès est facilitée (quatre personnes à l'exploitation suffisent pour l'ensemble des machines et des applications). En 2004, la priorité concerne le renforcement de la sécurité du réseau, avec des outils d'analyse du réseau, de détection des flux anormaux et de tests d'intrusion. Des dispositifs sécuritaires doivent équiper les terminaux mobiles des commerciaux, pas encore connectés au système de production.

Questions

1. Dans quelle mesure la croissance constante du chiffre d'affaires de Sodebo imposet- elle une évolution de la politique de sécurité du système d'information ?

2. Quelles sont les grandes composantes de la nouvelle politique de sécurité mise en place ?

3. Quels ont été, selon vous, les promoteurs de cette nouvelle politique auprès de l'ensemble des utilisateurs ?

Source : « ExperIT.news », n° 6, mars 2004

Encadré 10.2 : La Sécurité au sein du Groupe Bosch

Michel Harouard est depuis plus de cinq ans responsable de la sécurité du groupe Bosch en France, poste stratégique au sein d'une entreprise qui a compris l'importance des enjeux de ce service. Il nous livre ici sa vision et nous fait partager sa problématique.

Pourriez-vous nous présenter l'activité du groupe Robert Bosch ?

Le groupe est présent dans de très nombreux domaines d'activité, de l'automobile (bougies, système de freinage) aux produits blancs (réfrigérateurs), en passant par les chaudières (Elm Leblanc) et l'outillage. Nous sommes également un acteur majeur de marchés industriels comme ceux des systèmes hydrauliques ou des machines-outils. En 2004, Bosch réalise un chiffre d'affaires de 40 milliards d'euros et emploie 242 000 personnes dans le monde. En France, l'effectif s'élève à près de 10 400 personnes réparties sur 21 sites.

Quelle place occupe le service sécurité au sein du groupe ?

Une place très importante. Le service sécurité est mis en place depuis plus de 15 ans et dispose d'une très forte autonomie. Il est directement rattaché à la direction générale et totalement indépendant du service informatique. En effet, la sécurité chez nous est une notion qui s'entend au sens large du terme. Elle recouvre notamment toutes les problématiques de protection des données, informatiques bien sûr, mais aussi d'espionnage industriel ou d'archivage légal.

Quels sont les objectifs prioritaires de la politique de sécurité mise en place chez Bosch ?

Notre priorité absolue est de tout faire pour éviter un arrêt de nos moyens de production. Nous connaissons l'impact que cela pourrait avoir sur notre activité. Conscients de la difficulté de tout protéger (nous disposons aujourd'hui de 107 sites informatiques qui constituent autant de points d'entrée), nous avons mis en place un plan de protection qui répond à un double objectif :

- réduire au maximum le temps de redémarrage d'un système qui aurait été victime d'une défaillance ou d'une intrusion ;
- agir là où les données sont les plus stratégiques et recenser les points d'entrée les plus vulnérables.

À quelles menaces êtes-vous principalement confronté aujourd'hui ?

Ce qui nous préoccupe vraiment est de nous retrouver confrontés à un « déni de service » suite à un piratage du réseau, qui nous empêcherait tout simplement de travailler. Les risques liés au piratage industriel sont également très présents dans nos esprits. Nous devons à tout prix préserver la confidentialité de nos propres secrets de fabrication ou ceux de nos clients (notamment lorsque nous travaillons avec des constructeurs automobiles sur le lancement de nouveaux modèles).

Face à ces menaces, à nous de définir les règles de sécurité (d'accès au réseau ou de protection des données) qui devront être appliquées par le service informatique. Pour cela, nous avons mis en place un système de classification des données qui permet de hiérarchiser leur importance et d'y affecter un process sécurité particulier. Plus on monte en niveau et plus les règles à respecter sont strictes.

Quelles difficultés majeures rencontrez-vous dans la mise en place de cette politique sécurité ?

Je dois préciser que le fait d'appartenir à un groupe d'origine allemande nous facilite la tâche. Quand une directive est fixée, elle est généralement bien appliquée. Ceci dit, nous sommes confrontés à trois grands types de difficultés. D'abord, il est difficile de maintenir un niveau de sécurité homogène sur l'ensemble des sites. Le risque du « maillon faible » sur un site mineur existe toujours.

La deuxième difficulté est liée à la stratégie d'acquisition du groupe. L'intégration de nouvelles sociétés aux cultures sécurité très différentes n'est pas toujours simple à gérer.

Enfin, le turnover du personnel impose un travail de formation très important. Dans chaque département, nous disposons d'un correspondant « sécurité » qu'il faut former à chaque changement.

Quelles sont les principales qualités d'un bon responsable sécurité ?

Pour moi, au-delà des compétences techniques, un responsable sécurité doit surtout faire preuve d'une véritable force de conviction et d'un grand sens de la communication. Ces qualités doivent s'exprimer à deux niveaux. Sur la direction générale, que l'on doit sensibiliser aux enjeux de la sécurité afin d'obtenir les moyens indispensables à sa poursuite. Sur les utilisateurs, qui doivent absolument suivre les règles mises en place.

En conclusion, trois mots pour résumer le message « sécurité » en entreprise ?

Communication, sensibilisation et information.

Questions :

1. En quoi la continuité des activités de Bosch est-elle liée à la sécurité de son système d'information ?

2. Quels problèmes particuliers pose le turnover du personnel, en matière de sécurité informatique ?

*Source : **www.symantec.fr**/. Symantec est une marque de Symantec Corporation.*

Encadré 10.3 : Sécurité : les atouts de l'externalisation

Les offres d'externalisation de la sécurité sont nombreuses et couvrent tous les besoins de chaque entreprise. Mais outre le coût de la prestation, l'engagement de résultat doit être un critère décisif dans la sélection du prestataire.S'il est maintenant admis que le système d'information doit s'aligner sur les objectifs stratégiques de l'entreprise, la sécurité informatique, quant à elle, reste un domaine à part. Les directions générales estiment qu'il est indispensable de la garantir avec un degré acceptable, mais elles rechignent souvent à admettre l'investissement significatif en temps et en ressources (humaines et technologiques) qu'elle requiert. « Avec la banalisation des accès nomades et de l'interconnexion de filiales, ainsi que l'ouverture aux clients et partenaires, les PME sont aujourd'hui tout aussi sensibilisées que les grands comptes. Mais elles parviennent rarement à maintenir un niveau de compétence suffisant », constate Philippe Launay, responsable marketing chez Sodifrance. Lorsqu'elles sont géographiquement dispersées, les grandes entreprises sont confrontées à la même difficulté. L'externalisation de la sécurité s'impose alors comme l'une des meilleures solutions et ce créneau est occupé par un nombre croissant d'acteurs qui s'adressent à toutes les catégories d'entreprises. Thales Secure Solutions, Ubizen et Symantec visent essentiellement les structures d'au moins trois à quatre mille employés. *Via* Net.Works, Netcelo et Sodifrance répondent plutôt à la demande des petites structures (dix à mille salariés), tandis que Cyber Networks, de son côté, compte des clients de toutes tailles.

De la supervision à la configuration des équipements

La palette des services proposés recouvre l'analyse de vulnérabilité, la supervision des équipements (avec alertes en cas de problème), leurs mises à jour logicielles, leur configuration, ainsi que la résolution des problèmes. Certains prestataires proposent – voire imposent – également la location des équipements, dont les plus connus sont le *firewall* et la passerelle VPN (souvent intégrée au *firewall*). Il faut y ajouter les passerelles antivirus, proxy et autres sondes de détection d'intrusions, voire les systèmes d'authentification forte. Même s'il est possible de se limiter à la supervision d'un seul *firewall*, la tendance est à la fourniture de services englobant tous les aspects de la sécurité informatique et tous les sites de l'entreprise. Dans la majorité des cas, les équipements restent chez le client. La démarche est donc différente de celle des opérateurs télécoms qui proposent, dans le cadre d'offres de VPN/IP, d'héberger et d'administrer *firewalls* et antivirus. Ces deux approches ne sont toutefois pas incompatibles. En effet, certains sites étrangers, hors de portée du VPN/IP, sont parfois contraints de posséder leurs propres équipements de sécurité, non pris en charge par l'opérateur. De plus, synonyme d'externalisation physique, l'hébergement d'un *firewall* peut effrayer certaines entreprises ou simplement introduire une certaine rigidité. « Le contrôle se réduit alors aux demandes de modifications des configurations auprès de l'opérateur », explique Michel Habert, directeur marketing stratégique de Netcelo.

Un tunnel chiffré entre client et centre de supervision

La majorité des prestataires n'impose pas l'origine des produits administrés. En effet, nombre d'entreprises ont un équipement existant dont elles souhaitent confier l'administration. En l'absence d'existant, chaque acteur préconise une ou plusieurs marques d'équipements. Un tunnel chiffré passant par Internet, ou une liaison louée, permet ensuite au centre de supervision de prendre le relais à distance. Certains prestataires possèdent plusieurs centres, ce qui leur permet de garantir le service en cas de problème sur l'un d'entre eux. Si le contrat le prévoit, ils peuvent assurer un service sept jours sur sept, vingt-quatre heures sur vingt-quatre. Très variables, les autres engagements concernent le délai d'intervention en cas d'attaque, de mise à jour des systèmes et des bases d'antivirus, de mise en œuvre de nouvelles règles de sécurité, ou encore le taux de disponibilité des équipements administrés. En revanche, personne ne s'avance sur le temps de résolution d'un problème, l'absence d'attaques réussies ou le taux d'indisponibilité du système d'information due à un problème de sécurité. « Nous sommes à la frontière entre engagements de moyens et de résultats », commente Franck Perrin, directeur de l'exploitation et des services chez Thales Secure Solutions.

Conserver un contrôle sur la sécurité

Externalisation ne signifie pas désengagement : l'entreprise conserve un accès distant à des tableaux de bord, voire à une console d'administration, mais uniquement en lecture. De plus, elle définit toujours sa politique de sécurité et transmet à son prestataire, *via* un extranet, les règles à appliquer. Il s'agira par exemple de contraindre les PC de se connecter à Internet grâce à un accès mutualisé, de bloquer les tentatives d'accès venant d'Internet, ou encore d'interdire le *streaming*.

Questions

1. L'externalisation constitue-t-elle la solution idéale en matière de sécurité ?

2. Doit-on considérer qu'il existe une problématique particulière concernant les PME en matière de sécurité informatique?

Source : ZDNet France (14/10/2004)
www.zdnet.fr

Encadré 10.4 : Entretien avec Samuel Barbaud, responsable réseau & sécurité du Groupe Richemont

(…) Le Groupe Richemont est d'abord une holding financière qui regroupe différentes marques dont Cartier, Lancel, Montblanc, Van Cleef & Arpels, Piaget, etc. Mais c'est aussi une entité opérationnelle. En effet, depuis juin 2001, le groupe affirme une volonté de rationalisation des services transversaux, dont les ressources informatiques. Le but est de rendre cohérents les choix et infrastructures informatiques.

Est-ce à dire qu'il s'agit plus d'un enjeu organisationnel que sectoriel ?

Tout à fait. La politique de sécurité informatique doit prendre en compte une donnée fondamentale : le Groupe Richemont est présent dans 150 pays, avec 15 000 collaborateurs. La multiplicité des marques renvoie donc à autant de sociétés historiquement indépendantes. L'idée est de mettre en oeuvre une stratégie informatique et de sécurité qui doit tenir compte des spécificités juridiques et culturelles nationales. Nous faisons des recommandations en termes de sécurité aux responsables informatiques locaux, en distinguant les choses qui doivent être faites des actions optionnelles recommandées.

Avez-vous une idée du degré de sensibilisation des différents collaborateurs par rapport aux enjeux de la sécurité informatique ?

Notre management est très sensibilisé aux enjeux de la sécurité informatique, mais ce n'est pas le cas des autres utilisateurs, qui n'ont pas toujours conscience de l'impact de leurs actions quotidiennes sur la sécurité du système d'information. On cherche donc à sensibiliser ces utilisateurs, et en particulier, les personnes qui gèrent le système d'information, ainsi que les assistantes de direction qui manipulent des données extrêmement confidentielles tout en constituant de bons relais pour la communication interne. Ces deux cibles représentent 500 personnes. L'implication des utilisateurs est en effet cruciale : dans le cas où je n'ai pas de solution technologique pour faire face à un problème de sécurité informatique, je dois faire confiance à la responsabilité des collaborateurs. C'est par exemple le cas face au « spam » : une des solutions les plus efficaces en la matière reste que les utilisateurs ne communiquent pas leur adresse mail à un tiers qu'ils ne connaissent pas.

Comment remédier à ces différences d'implication ?

La difficulté réside bien plus dans la mise en place des procédures que dans l'installation des solutions technologiques. C'est pourquoi la sensibilisation des utilisateurs est une étape obligatoire pour mettre en œuvre notre politique de sécurité.

Concrètement, pouvez-vous citer des exemples d'actions menées en ce sens ?

D'abord, nous avons bien sûr conçu une charte avec un volet sur la messagerie, un autre pour l'utilisation d'Internet et enfin un texte plus général sur le système informatique et la gestion des mots de passe. C'est un document de 28 pages, joint au contrat de travail, et qui doit normalement être lu par toute personne qui utilise un ordinateur dans le groupe. Mais surtout, on réalise des tests en interne pour vérifier le respect de tel ou tel dispositif. Le but n'est pas le « flicage », mais la sensibilisation des utilisateurs à qui l'on transmet ensuite les résultats, présentés de manière statistique donc anonyme. Enfin, on travaille à la réalisation d'un Intranet, appelé à devenir un véritable tableau de bord de la sécurité, qui permet de mesurer la sensibilisation des utilisateurs par rapport à cet enjeu, et d'agir en conséquence.

Quelles sont les équipes impliquées dans la réalisation de ces actions ?

Au sein du département informatique, quatre personnes sont responsables de la sécurité du système d'information, et elles travaillent en étroite collaboration avec l'équipe « email groupware ». Pour mener à bien ces différentes actions, on cherche également à impliquer d'autres services transversaux en interne : la communication et le marketing notamment, mais aussi les RH et le service juridique. Cela n'exclut pas pour autant le recours éventuel à des prestataires externes.

La gestion de la sécurité informationnelle prend-elle en compte des facteurs de risques internes ?

En effet, les risques ne viennent pas uniquement de l'extérieur. La sécurité informatique est spontanément associée aux attaques virales, au piratage d'informations stratégiques ou encore au problème du « spam ». Mais nous devons aussi prendre en compte d'autres enjeux comme le respect de la vie privée, en mettant en place des procédures qui définissent le cadre d'accès par un tiers à une boîte de messagerie. De plus, il s'agit aussi de contrôler la communication autour de ce thème : il faut savoir éviter les bruits qui s'amplifient et qui peuvent conduire à des prises de décision

disproportionnées par rapport à la nature du risque repéré. Dans ce domaine, la meilleure façon de contrôler la communication repose sur l'utilisation par les collaborateurs des outils de « reporting » des incidents.

Source : www.symantec.fr/

Questions

1. Commentez cette phrase de S.Barbaud : « La sensibilisation et l'implication des utilisateurs de notre système d'information sont essentielles pour la mise en oeuvre de notre politique de sécurité informatique. »

2. Pourquoi avoir joint un document sur les pratiques à respecter en matière de sécurité informatique, au contrat de travail des salariés du groupe ?

Cas pratique : Un nouveau partenaire commercial pour C2Alpha

Jessica Andover est ravie d'avoir trouvé un poste au sein de cette entreprise spécialisée dans la robotique. Bien sûr, il s'agit d'une start-up et son salaire n'est pas très élevé, mais l'entreprise est petite, ses collègues sont sympathiques, et elle a l'espoir de s'enrichir grâce aux stock-options qu'elle touche. Elle ne deviendra pas millionnaire comme les créateurs de la société, mais quand même suffisamment riche.

C'est pour toutes ces raisons que Rick Daggot est agréablement accueilli quand il franchit les portes de la société en ce matin d'août. Avec son costume Armani, sa montre Rolex Président et sa coupe de cheveux soignée, il a cette attitude virile et confiante qui faisait déjà tourner la tête des filles quand Jessica était au lycée.

« Bonjour, dit-il, je suis Rick Daggot et je viens pour mon rendez-vous avec Larry. »

Le sourire de Jessica s'évanouit : « Larry ? dit-elle. Il est en vacances pour la semaine.

– J'avais rendez-vous avec lui à treize heures. Je suis venu exprès de Louisville pour le rencontrer », répond Rick en allumant son PDA et le montrant à Jessica.

Elle regarde l'écran et secoue la tête : « C'est le 20, la semaine prochaine ». Il reprend son PDA et y jette un coup d'œil. « Oh non ! gémit-il. Je n'arrive pas à croire que j'aie pu faire une erreur aussi stupide.

– Je peux peut-être vous réserver un vol pour le retour ? », demande-t-elle, se sentant désolée pour lui.

Pendant qu'elle téléphone, Rick lui confie que Larry et lui étaient sur le point de mettre en place une alliance commerciale stratégique. La société de Rick fabrique des produits pour les chaînes d'assemblages, produits qui complètent parfaitement le prochain modèle de la société de Larry, le C2Alpha. Le C2Alpha et les produits de Rick formeraient une solution très compétitive qui ouvrirait des marchés importants pour les deux sociétés.

La réservation pour un vol en fin d'après-midi une fois effectuée, Rick déclare : « Bon, je pourrais au moins parler à Steve, s'il est là. » Mais Steve, le cofondateur et vice-président de l'entreprise est également absent.

Rick, dont l'amabilité vis-à-vis de Jessica frise la séduction, suggère alors que puisqu'il est là et qu'il doit attendre la fin d'après-midi pour son vol de retour, il pourrait emmener déjeuner quelques-uns des principaux collaborateurs de Larry. Et il ajoute : « Vous aussi, bien entendu. Y a-t-il quelqu'un qui puisse vous remplacer à l'heure du déjeuner ? »

Flattée à l'idée de déjeuner avec Rick, Jessica demande : « Qui d'autres souhaitez-vous voir ? » Il tapote sur son PDA et nomme quelques personnes : deux ingénieurs du service recherche et développement, le nouveau commercial et le responsable financier du projet. Rick demande à Jessica de contacter chacune de ces personnes pour leur signaler sa présence. Il mentionne ensuite le meilleur restaurant des environs, où Jessica a toujours voulu manger, dit qu'il réservera lui-même une table pour 12 h 30 et qu'il rappellera en fin de matinée pour s'assurer que tout se passe comme prévu.

Lorsque les quatre employés et Jessica arrivent au restaurant, leur table n'est pas encore prête, aussi s'installent-ils au bar, et Rick fait comprendre que l'addition sera pour lui. Rick a du style et met à l'aise. Il trouve le mot juste, a toujours une remarque à faire ou une anecdote intéressante à raconter quand la conversation faiblit. D'une manière générale, sa compagnie est très agréable.

Il mentionne juste assez de détails concernant les produits de son entreprise pour que ses interlocuteurs puissent se faire une bonne idée de l'offre commerciale conjointe qu'ils vont proposer. Il cite plusieurs très grosses sociétés clientes de son entreprise et, au bout d'un moment, tous ses interlocuteurs sont convaincus que leur produit sera un succès commercial dès son lancement.

Puis Rick se lance dans une discussion à part avec Brian, l'un des ingénieurs. Il partage en privé avec lui quelques idées, insistant sur les particularités du C2Alpha qui le distinguent de la concurrence. Il apprend ainsi que la société se montre volontairement discrète sur certaines de ces spécificités dont Brian est fier et qu'il qualifie de « Top ».

Rick bavarde ainsi discrètement avec chacun. Le commercial est content de pouvoir discuter de la date de sortie et du plan marketing. Le responsable financier tire une enveloppe de sa poche et note en détail les frais liés aux matières premières et à la fabrication, les prix de vente et la marge prévue, ainsi que les contrats qu'ils espèrent passer avec chacun des revendeurs, dont il n'oublie pas de préciser les noms.

Quand leur table est prête, Rick a échangé des idées avec tout le monde et gagné un cercle d'admirateurs. À la fin du repas, tout le monde lui serre la main et le remercie. Des cartes de visite s'échangent et chacun mentionne en passant à Brian, l'ingénieur, qu'il aimerait avoir une discussion plus approfondie avec lui dès que Larry sera de retour.

Le lendemain, Rick appelle Brian pour lui apprendre qu'il vient de s'entretenir avec Larry. « Je repasse lundi pour régler quelques détails avec lui, dit Rick, et en attendant, il voudrait que j'aie plus de détail sur votre produit. Il m'a dit que vous pourriez m'envoyer les derniers plans et les dernières spécifications. Il choisira les informations qui doivent m'être communiquées. »

L'ingénieur dit que cela ne posera pas de problème. « Bien », répond Rick. Et il poursuit : « Larry m'a dit de vous dire qu'il avait des problèmes pour récupérer son courrier électronique. Il s'est donc arrangé pour créer à partir de son hôtel un nouveau compte de courrier Yahoo. Il a dit que vous deviez envoyer les fichiers à l'adresse larryrobotics@yahoo.com.

» Le lundi matin suivant, quand un Larry bronzé et détendu arrive dans les locaux de son entreprise, Jessica ne peut s'empêcher de mentionner Rick. « C'est vraiment quelqu'un de sympa. Il nous a invités à déjeuner, moi et quelques autres. » Larry paraît déconcerté : « Rick ? Quel Rick ?

- Comment, quel Rick ? Ton nouveau partenaire commercial !
- Quoi ?
- Et tout le monde a été impressionné par les questions qu'il a posées.
- Je ne connais personne du nom de Rick.
- Qu'est-ce que tu racontes ? C'est une blague, Larry, tu me fais marcher !
- Convoque immédiatement tous les chefs de département. Et aussi tous ceux qui étaient présents à ce déjeuner, toi comprise. »

L'ambiance autour de la table de réunion est sombre : personne ne dit mot. Larry entre, s'assoit et prend la parole : « Je ne connais personne du nom de Rick. Je n'ai pas de partenaire commercial dont je vous aurais caché l'existence. Et je pensais que cela allait de soi. Si cette histoire est une plaisanterie, j'aimerais que la personne qui en est responsable se dénonce. »

Un silence pesant lui répond et l'atmosphère s'assombrit d'instant en instant.

Finalement, Brian prend la parole : « Pourquoi est-ce que tu n'as rien dit quand je t'ai envoyé l'email avec les spécifications du produit et le code source ?

– Quel email ? »

Brian se raidit : « Oh, bon sang ! »

Cliff, l'autre ingénieur, intervient : « il nous a donné des cartes de visite à tous. Il n'y a qu'à l'appeler pour exiger des réponses. »

Brian sort son PDA, y affiche une entrée, puis fait glisser l'appareil sur la table en direction de Larry. Contre toute vraisemblance, tous caressent encore un faible espoir, tandis que Larry compose le numéro. Après quelques instants, il appuie sur la touche du hautparleur du téléphone et tout le monde entend que la ligne est occupée. Après avoir essayé le même numéro pendant vingt minutes sans rien obtenir d'autre que ce même signal, Larry, excédé, appelle une opératrice pour obtenir des informations.

L'opératrice de la compagnie du téléphone lui demande sur un ton méfiant : « Où avez vous obtenu ce numéro, monsieur ? » Larry répond qu'il se trouve sur la carte de visite d'un homme qu'il doit contacter d'urgence. L'opératrice répond : « Je suis désolée. Il s'agit d'un numéro utilisé par nos techniciens pour effectuer des tests, et qui sonne toujours occupé. »

Larry liste toutes les informations qui ont été communiquées à Rick : le bilan n'est pas réjouissant.

Deux policiers viennent enregistrer les dépositions. Après avoir écouté l'histoire, ils font remarquer qu'aucun crime n'a été commis au niveau de l'État et qu'ils ne peuvent donc rien faire. Ils conseillent à Larry de contacter le FBI10, qui est compétent pour les litiges commerciaux impliquant plusieurs États. Quand Rick Daggot a employé une fausse identité pour se faire envoyer les caractéristiques du produit, il a peut-être commis un crime fédéral, mais il faudrait que Larry en parle avec le FBI pour en être sûr.

Trois mois plus tard, Larry prend son petit-déjeuner dans sa cuisine en lisant son journal lorsqu'il manque de renverser son café. Ce qu'il craignait depuis qu'il a entendu parler de Rick, son pire cauchemar, est arrivé. En première page de la section économie du journal, une société dont il n'a jamais entendu parler, annonce la sortie d'un produit qui ressemble point pour point au C2Alpha que sa propre entreprise développe depuis deux ans.

Des inconnus lui ont volé son produit et l'ont commercialisé avant lui. Son rêve est détruit. Les millions de dollars investis en recherche et en développement sont perdus. Et il ne pourra sans doute jamais rien prouver à leur encontre.

Questions

1. Quel est l'enseignement principal à tirer de cette histoire ?

2. Quelles sont les failles de sécurité qui sont identifiables ? Comment les corriger ?

3. Quels sont les enjeux organisationnels, managériaux et techniques auxquels Larry n'a pas su faire face efficacement, et qui ont conduit son entreprise à être aussi vulnérable ?

Source : L'Art de la supercherie, l'importance du facteur humain dans la sécurité informatique,
K. Mitnick, W. L. Simon, CampusPress, 2004