AÉRONAUTIQUE

L'équipementier aéronautique a été victime de deux cyberattaques en 2009 et 2010. Leur similitude a poussé la direction à porter plainte auprès de la DCRI, même si aucune information sensible n'a été dérobée.

Espionnage présumé : plus de peur que de mal, assure Safran

Au moment où Renault espère en finir avec sa fausse histoire d'espionnage, une deuxième affaire vient de surgir qui vise un autre fleuron technologique français, Safran en l'occurrence (« Les Echos » d'hier). Mais avec, là encore, le risque de décevoir les amateurs de John le Carré, le premier équipementier aéronautique français démentant que des secrets industriels aient été dérobés.

Contrairement à la marque au losange, Safran a bien été victime d'une tentative de vol de données sensibles : une première fois en 2009 via sa filiale Turbomeca, qui fabrique des turbines d'hélicoptères, puis au niveau de l'informatique centrale, six mois plus tard. Dans les deux cas, la même méthode puisque les commanditaires ont voulu dresser la cartographie des réseaux informatiques, relate Michel Pagès, le directeur de la protection industrielle du groupe (lire ci-dessous).

C'est cette similitude qui a amené la direction à faire appel aux services spécialisés de l'Etat. La DCRI a ouvert une enquête préliminaire le 25 janvier 2010. Le tribunal de Nanterre a pris la suite.

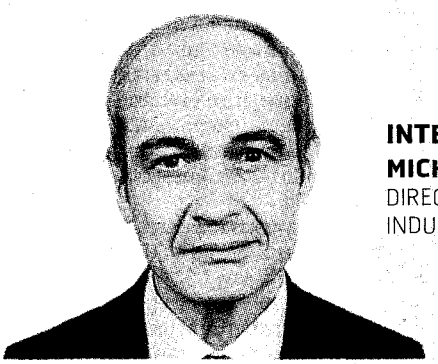
Sécurité informatique renforcée

En réagissant rapidement, Safran assure que ses bases de données industrielles sont restées inviolées. A ce stade, l'enquête judiciaire n'établit pas le contraire, assure Michel Pagès. A toute chose malheur est bon, le groupe en a profité pour muscler sa sécurité informatique, ce qui lui a coûté quelques dizaines de milliers d'euros au passage.

Reste à savoir qui sont les auteurs de ces attaques : organisations criminelles, hackers professionnels, ou organismes paravents d'un concurrent ou d'un pays ? Autre question : que visaient-ils ? Par leur sophistication, les tentatives de cartographier l'informatique de Safran font penser à une équipe de braqueurs qui commencent par une reconnaissance des lieux avant de commettre leur délit.

ALAIN RUELLO

« Aucune donnée à caractère industriel n'a été dérobée »



INTERVIEW
MICHEL PAGÈS
DIRECTEUR DE LA PROTECTION INDUSTRIELLE DE SAFRAN

Une enquête est en cours au tribunal de Nanterre pour introduction frauduleuse dans l'informatique de Safran. Qu'elle en est l'origine exacte ?
Il y a eu deux cyberattaques. La première a démarré le 18 juin 2009 et a visé Turbomeca. La société s'est rendu compte rapidement qu'un de ses serveurs était indisponible. Nos experts ont détecté un logiciel malveillant qui cherchait à cartographier le système d'information de Turbomeca. Après analyse, nous avons pris un ensemble de mesures correctives et préventives qui ont duré jusqu'en août, le temps de vérifier tout le parc informatique du groupe Safran. Nous avons averti la DCRI, mais sans porter plainte car l'attaque a été neutralisée très rapidement.

Et la deuxième ?
Elle est intervenue le 18 janvier 2010 et a visé l'informatique centrale de Safran cette fois. Les responsables de la sécurité ont été alertés par le fonctionnement anormal d'un serveur de supervision. Là encore, on tentait de dresser la cartographie du système d'information du groupe. L'alerte est remontée très rapidement à la direction générale. Comme l'attaque, qui pouvait toucher d'autres filiales, présentait des similitudes avec celle de Turbomeca, nous avons déposé immédiatement une plainte auprès de la DCRI pour essayer de savoir qui se cachait derrière.

« Dans son déroulé, l'attaque (de 2010) cherchait, comme dans le premier cas, à faire l'inventaire du système d'information. »

Quel est le préjudice ?
Il est faible. D'une part, il n'y a jamais eu d'exfiltration de données à caractère industriel. Dans son déroulé, l'attaque cherchait, comme dans le premier cas, à faire l'inventaire du système d'information. Or cet inventaire n'en était qu'à son début. Si des données ont été exfiltrées, ce ne sont donc que des données partielles sur notre système d'information.

Aucun secret de fabrication n'a donc été dérobé ?
Non.

On a évoqué des salariés en garde à vue ?
Aucunement. Nos serveurs ont été attaqués de l'extérieur, via des sites Web institutionnels de Safran. C'est pour cela que nous avons mené tout un travail en parallèle pour en durcir l'accès.

En savez-vous plus sur l'origine et les motivations de ces deux cyberattaques ?
L'enquête a montré que plusieurs serveurs devaient servir à remonter les informations. Ils sont situés à Singapour, à Taiwan, en Chine, en Suède et dans d'autres pays. Mais cela ne préjuge en rien de l'identité de ceux qui sont derrière.

Plusieurs commissions rogatoires ont été lancées et tout cela va prendre du temps. En aucune façon le nom d'Avic, notre partenaire chinois, n'apparaît dans l'enquête.

Les cyberattaques contre Safran sont-elles en augmentation ?
Comme toute société qui développe des technologies sensibles, Safran attire la curiosité. Mais là, il s'agit de la première attaque de cette ampleur contre le groupe.

PROPOS RECUEILLIS PAR
A. R.