Cert-Lexsi: comment empêcher fuites et vols de data sensibles?

Les fuites de données sensibles sur Internet doivent-elles être prises au sérieux ? La pire des situations pour une entreprise, je crois, c'est de ne pas savoir que des informations sensibles « fuitent », -s'achappent. Sur Internet, leur diffusion peut être rapide et causer des dommages considérables. Il faut donc pouvoir intervenir rapidement, à bon escient, ce qui exige une connaissance fine des mécanismes du web.

Ces fuites sont de deux sortes. Les fortuites, d'abord, les comptes-rendus de réunions, les documents comptables ou techniques devenus subitement accessibles en *peer-to-peer* ou sur un serveur mal sécurisé ; les informations confidentielles postées dans les CV, les forums techniques ou les blogs.

Puis il y a les fuites volontaires, dues à des salariés mécontents, des rivalités de managers. Des tribunes comme Boursorama ou Indymedia peuvent être des vecteurs de déstabilisation redoutables. Dans la chronologie d'un conflit, il y a presque toujours une phase de diffusion de documents sensibles.

Comment les neutraliser ?

En surveillant les nouveaux contenus sur internet bien sûr, mais les moyens techniques ne suffisent pas, car ils sortent beaucoup de faux positifs. Il faut aussi l'expertise humaine pour trier et jauger. Trouver comment l'information a fuité, puis envisager la bonne réaction. Et surtout ne pas sur-réagir la plupart du temps. Cela demande à comprendre la psychologie des bloggeurs et des individus. Mais l'entreprise doit aussi savoir qu'il ne suffit pas de protéger telle ou telle machine ou périmètre technique. Il faut protéger l'information elle-même. Il faut maîtriser son cycle de vie et sa dispersion. Pour traiter ces questions, nous avons donc également un département Lexsi Conseil.

Et les fraudes, la cybercriminalité organisée ?

La menace principale, ce sont les vols de codes d'accès et d'informations de cartes bancaires par usurpation d'identité (phishing) ou malware. Ils frappent non pas seulement les sites d'e-commerce, mais également les SI et les réseaux des opérateurs. Il s'agit le plus souvent de cybercriminalité organisée. Car les codes d'accès et numéros de CB volés sont blanchis et revendus à d'autres, qui ne les exploiteront pas forcément, en tout cas pas immédiatement. Ces menaces viennent aujourd'hui des pays de l'Est, de l'Afrique de l'ouest, des pays anglo-saxons et de la Chine principalement.

Comment les contrer ?

C'est l'essentiel de notre travail. Nous avons des 'pools d'analystes, pratiquant nativement une douzaine de langues des pays concernés. Ils scannent l'internet pour comprendre les modes opératoires, repérer les fraudes et constituer des preuves, que nous faisons au besoin constater par huissier. Il faut savoir agir rapidement, en liaison avec les services de police et les CERT locaux. Nous alertons l'opérateur et l'hébergeur des fraudeurs.

Nous obtenons la fermeture d'un site de *phishing* en 45 minutes en moyenne et cela dans une soixantaine de pays, et nous en faisons fermer une vingtaine par mois. Mais il faut rester vigilants. Ces sites renaissent, mais pour attaquer d'autres clients que les nôtres et nos missions de fermeture s'apparentent alors à une guérilla sans fin. Il faut donc parallèlement enquêter en profondeur pour que des procédures judiciaires soient lancées. L'été dernier, nous avons réussi à démanteler à temps une fraude qui aurait pu causer un préjudice de 80 millions d'euros. Cert-Lexsi traque également les filières de contrefaçons de médicaments et de produits de luxe.

Des millions de contenus analysés chaque jour

Lexsi (Laboratoire d'Expertise en Sécurité Informatique), créé en 1999 par Joël Rivière, ancien DSI de l'Institut de recherche criminelle de la Gendarmerie Nationale, ne cesse de grandir. Il emploie aujourd'hui 120 personnes pour quelque 600 clients, dont la plupart des banques du marché hexagonal. Et les recrutements continuent. Des 4 Cert (Computer Emergency Response Teams) français, c'est le seul de droit privé. Ses systèmes analysent plusieurs dizaines de millions de contenus chaque jour pour y détecter des fraudes et conduire des enquêtes.