Compte-rendu ReSIST

Référence RÉSIST/2013-02

12 mars 2013

Les présentations faites lors de la réunion RÉSIST de mars 2013 sont :

Philippe Bourgeois, CERT/IST Bilan 2012 sur les attaques et les menaces

M^e^ Alexandrine Pantz, avocate Stratégies judiciaires d'une entreprise dans le cadre d'un incident ou attaque informatique : de l'obtention d'une indemnité à l'enquête pénale.

1 Bilan du CERT/IST des menaces sur 2012

Philippe Bourgeois, a présenté le bilan du CERT/IST quant à l'année 2012.

1.1 Veille sur les vulnérabilités et les menaces

Il y a eu environ 4000 « événements de sécurité » (grossièrement, de nouveaux CVE publiés) en 2012. Du fait de l'optique du CERT/IST, centré sur les entreprises, ces événements sont par la suite qualifiés et regroupés (peuvent-ils concerner des entreprises ?). Cela a donné lieu à 755 avis et alertes émis par le CERT/IST. Sur ces 755, il y a eu **une alerte** et **dix-sept dangers potentiels**.

Pour le CERT/IST, le nombre de vulnérabilités continue à croître. Indirectement, cela signifie qu'un système qui n'est pas tenu à jour voit mécaniquement sa sécurité se dégrader. Malgré cela, de très nombreux systèmes en production ne sont pas tenus à jour.

1.1.1 Vulnérabilités Java

En 2012, Java s'est révélé être **le** vecteur d'attaque privilégié, tout particulièrement lors de la navigation sur Internet. De nombreuses vulnérabilités dans Java permettent de contourner le bac-à-sable Java et d'atteindre la session de l'utilisateur.

Le CERT/IST a fait quelques préconisations ou suggestions, centrées sur les deux questions

– avez-vous besoin de Java ?
– avez-vous besoin de Java pour naviguer sur Internet ?

Il peut se révéler intéressant
– de filtrer Java sur le relais de navigation, ou
– d'utiliser deux navigateurs, l'un avec Java réservé à l'accès aux applications internes de l'entreprise, l'autre sans Java pour naviguer sur Internet.

1.1.2 Vulnérabilités Windows

Il semble de plus en plus difficile de trouver des vulnérabilités sur Windows. Toutefois, dès qu'une vulnérabilité est identifiée, elle est exploitée très rapidement. Cela sous-entend une très forte compétence Windows chez les développeurs d'outils d'exploitation. Il existe à l'évidence des développeurs dont le métier est de produire du code malveillant.

1.1.3 Autres

L'année 2012 a vu plusieurs incidents de vol de code source (PCAnywhere, VMWare...). Ces incidents ont très rapidement été suivis de publication de correctifs dans les outils concernés par les sociétés qui en ont été les victimes.

1.2 Evénements majeurs de 2012

Les « événements majeurs » évoqués s'entendent du point de vue des entreprises.

1.2.1 Les architectures SCADA

Le terme *SCADA* est ici utilisé pour désigner de manière générique les infrastructures informatiques industrielles.

En 2010, Stuxnet a confirmé que les architectures SCADA étaient des cibles potentielles. En 2011, de nombreux spécialistes de la sécurité informatique « classique » ont commencé à se pencher sur le SCADA. Cela a amené à l'identification de vulnérabilités dites *forever-day*, qui ne seront jamais corrigées par le fournisseur du fait d'architectures non-sécurisées dès leur conception.

2012 n'a pas vu d'incident majeur concernant le SCADA, à l'exception d'une intrusion chez Telvent (aujourd'hui Schneider Electric). La cible en était la famille de produits OASys, avec une possibilité de diffusion de l'incident sur chaque installation postérieure.

1.2.2 Advanced Persistent Threats

Les attaques de type APT (attaques par infiltration, sur des cibles choisies) se sont généralisées, sur une très grand échelle. Elles ne sont plus réservées à quelques secteurs précis.

Qui sont les attaquants ?

- des états (pour des objectifs stratégiques)
- des sociétés spécialisées, intervenant sur le marché « gris »
- des individus ou groupes isolés

L'un des grands problèmes lié aux attaques par infiltration vient de la collision de l'augmentation de la compétence et du nombre de développeurs offensifs, et des demandes d'ouverture tous azimuts de la part des utilisateurs.

1.2.3 Augmentation du risque lié aux zéro-days

On sait depuis longtemps que des *zéro-days* (vulnérabilité gardées secrètes par les découvreurs pour les utiliser dans des attaques) existent. Mais on se rend compte désormais que le nombre de 0-days circulant dans la nature est plus important que ce que l'on pensait jusque là.

L'augmentation de cette menace implique que les entreprises prennent en compte explicitement ce risque, en l'intégrant dans les architectures et les processus. Même si l'on dispose d'un système complètement à jour, la compromission arrivera. Ce n'est qu'une affaire de temps. Il est important de s'organiser pour y survivre.

1.2.4 Le paysage actuel

Que peut faire une entreprise ? Le *Guide de l'hygiène informatique*, diffusé par l'Anssi, est un bon point de départ. Même s'il ne présente rien de particulièrement novateur, il faut déjà commencer par appliquer les recommandations qu'il contient. La défense en profondeur reste pleinement à l'ordre du jour.

1.3 Sujets d'actualité

Philippe Bourgeois a ensuite abordé quelques sujets d'actualité, dont notamment

le cloud c'est un domaine aujourd'hui relativement bien cadré, tant juridiquement que techniquement.

le Big Data d'après M. Bourgeois, il s'agit d'un marché de niche, du fait de la rareté des entreprises réellement concernées (Amazon, Google, etc.). Les volumes et l'hétérogénéité des informations concernées sont tels que l'ensemble se révèle très difficile à sécuriser. Sur le plan sociétal, le *Big Data* soulève de réelles questions.

les smartphones relativement peu d'évolutions sur ce sujet. L'essentiel des incidents revient à une monétarisation directe (appels vers des numéros surtaxés). Il y a eu peu d'attaques sophistiquées spécifiques aux smartphones.

le BYOD phénomène émergent, avec des risques réels, même si peu d'incidents effectifs ont été observés.

le cybercrime essentiellement centré sur le vol de données personnelles.

1.4 En conclusion

La situation reste complexe, avec des risques qui augmentent et de nouvelles demandes de la part des utilisateurs et des projets. La veille en matière de sécurité doit demeurer un élément important de la sécurisation d'un système d'informations.

2 Stratégies judiciaires d'une entreprise

Maître Alexandrine Pantz, avocate au barreau de Toulouse, a abordé les stratégies judiciaires qu'une entreprise peut suivre en cas d'incident informatique.

2.1 L'indemnisation

Dans une procédure civile, l'indemnisation vise à réparer un préjudice subi. La plainte peut avoir été déposée par n'importe qui (la victime), sachant qu'un avocat ou une assurance peuvent poursuivre en votre nom.

Au pénal, seul le procureur peut poursuivre la plainte (et, éventuellement, choisir de ne pas aller jusqu'au procès).

Il est important de souligner que l'indemnisation répare le préjudice subi, ni plus, ni moins.

2.2 L'événement déclencheur et les responsabilités

Il faut identifier le type d'événement qui se situe à l'origine du dommage. Ce peut être une attaque, une défaillance, une panne... ou un cas de force majeure. Les responsabilités ne sont alors pas les mêmes.

En cas d'attaque ou de malveillance, il est possible de constituer un dossier pénal. En cas de défaillance contractuelle, ce sera un dossier civil ou commercial.

Me Pantz a souligné les notions de

responsabilité délictuelle Celle-ci signifie que chacun est responsable des dommages qu'il a causés, que ce soit de son fait, de sa négligence ou de son imprudence (article 1383 du Code civil).

responsabilité contractuelle Dans ce cadre, tout (ou presque) peut être envisagé. Le contrat peut même contenir des clauses léonines (qu'il faut faire annuler par un tribunal).

2.3 Apporter la preuve

L'une des principales difficultés dans tout dossier judiciaire est d'apporter la preuve de ce que l'on allègue. Cela ne s'improvise pas, même si la preuve simple reste toujours envisageable.

Preuve simple Il s'agit d'éléments de preuve apportés « comme ça ». La preuve simple peut être combattue, même si l'adversaire doit disposer d'éléments appropriés visant à affaiblir la dite preuve. Il faut donc bien « construire » cette preuve, d'autant plus soigneusement qu'elle est importante dans le dossier.

Intervention d'un huissier Pour un constat, une saisie, une mise sous séquestre, etc. Le constat sur Internet, tout particulièrement, doit être réalisé de manière soigneuse, même s'il n'est pas obligatoire de suivre la norme Afnor NFZ67 (Cour d'appel de Paris, pôle 5, chambre 1, arrêt du 27 février 2013).

Saisie douanière Les forces de polices et gendarmerie ont la possibilité de procéder à des saisies, dans le cadre d'actions dûment autorisées. La douane a des pouvoirs de saisie plus étendus que ceux de la police ou gendarmerie.

Saisie-contrefaçon La saisie-contrefaçon, qui peut être réalisée par un huissier (suite à une requête déposée devant un tribunal) permet de « mettre à l'abri » des éléments de preuve en cas de suspicion de contrefaçon. Il est impératif d'ouvrir une action au fond dans le mois qui suit la saisie, sous peine de la voir frappée de caducité. L'arbitrage entre les parties n'est plus possible.

Ordonnance sur requête Une ordonnance, produite par un tribunal, permet d'engager l'action d'un huissier (qui peut être accompagné d'un expert judiciaire dans le cas d'une saisie ou d'un constat requérant des compétences techniques spécifiques) ou d'ouvrir une expertise judiciaire.

2.4 Evaluation des préjudices

Celle-ci est souvent réalisée via une expertise judiciaire, elle-même diligentée suite à une requête auprès d'un tribunal. Un rapport d'expertise judiciaire étant toujours contradictoire [1], ses conclusions [2] ont un poids certain.

1. Sous peine de voir l'expertise annulée.
2. Qui peuvent être combattues devant la cour, et que les magistrats peuvent ne pas suivre.