Bilan Cert-IST 2013 des failles et attaques

1) Introduction

Comme chaque année, le Cert-IST fait un bilan de l'année écoulée.
L'objectif de ce document est de retracer les événements marquants de l'année 2013 de façon à mettre en évidence les tendances sur l'évolution des attaques et d'aider les acteurs à mieux se protéger.

Nous présentons tout d'abord les évolutions les plus marquantes de 2013 (cf. chapitre 2) en parlant de l'affaire Snowden, des attaques matérielles (de bas niveau) et la sécurité offensive. Ces événements inter-dépendants sont pour nous les plus importants, en termes d'évolution de la menace pour les entreprises.

Nous passons ensuite en revue les principales failles et attaques de 2013 (cf. chapitre 3) en faisant un récapitulatif issu du suivi quotidien par le Cert-IST des vulnérabilités et des menaces. Cela inclut un bilan général de la production du Cert-IST (nombre d'Avis, de Danger Potentiels et d'Alertes), puis un examen rapide des Alertes et Dangers Potentiels, et enfin un zoom sur quelques failles et attaques.

Nous analysons ensuite comment l'entreprise peut se protéger (cf. chapitre 4) contre les principales classes de menaces (cyber-espionnage, attaques opportunistes) en prenant en compte les cibles types qu'elles visent (les utilisateurs, le poste de travail, les sites web, les systèmes Scada).

La conclusion (cf. chapitre 5) effectue une synthèse du paysage actuel de la cyber-menace et des challenges auxquels l'entreprise doit faire face.

➢ A propos du Cert-IST

Le Cert-IST (**C**omputer **E**mergency **R**esponse **T**eam - **I**ndustrie, **S**ervices et **T**ertiaire) est un centre d'alerte et de réaction aux attaques informatiques destiné aux entreprises. Créé en 1999, il aide ses adhérents à identifier les menaces en analysant quotidiennement les nouvelles vulnérabilités, leurs criticités et les moyens de protection pour y répondre. En cas d'incident de sécurité touchant l'un de ses adhérents, le Cert-IST peut apporter son aide dans l'investigation de cet incident et permettre une remise en service opérationnelle et sécurisée.

2) Les évolutions marquantes de 2013

2.1 L'affaire Snowden change la perception du risque « cyber-espionnage »

Les révélations d'Edward Snowden à propos des programmes de surveillance de la NSA constituent l'événement le plus marquant de l'année 2013. Voici les aspects qui nous paraissent les plus importants :

- **Juin** : première révélation de Snowden. Elle concerne l'existence du programme **PRISM** qui permet à la NSA d'avoir accès à des données d'abonnés chez les principaux hébergeurs américains (Google, Facebook, Yahoo!, etc…) et des opérateurs télécom (Verizon).
- **Août** : révélation à propos du programme **Xkeyscore**. La NSA (et d'autres états : UK, etc..) effectue des écoutes de masse sur les réseaux IP depuis un ensemble de sites répartis sur le globe. A partir du trafic réseau capturé, elle peut reconstituer des conversations de tout un chacun (échanges Facebook, emails, etc.)
- **Septembre** : révélations à propos de programmes pour **casser ou contourner le chiffrement** des données et des communications. Il s'agit par exemple du programme "Bullrun" ou de l'affaiblissement volontaire de l'algorithme cryptographique Dual_EC_DRBG.
- **Décembre** : publication du **catalogue ANT** de la NSA. Ce catalogue qui semble dater de 2008, liste une cinquantaine d'outils mis à la disposition des différents services secrets américains pour réaliser des missions offensives. Il propose par exemple des backdoors pour des équipements réseaux Cisco, Huawei ou Juniper.

Globalement, ces différentes révélations mettent en évidence le fait que la NSA (et probablement aussi les services équivalents des autres pays) utilisent abondamment l'arme informatique depuis plusieurs années et que, le savoir faire dans ce domaine est plus avancé qu'on ne pouvait l'estimer jusqu'à présent.

Aucun des éléments amenés par Snowden n'est réellement totalement nouveau, mais la menace correspondante était jusqu'à présent plutôt considérée comme théorique ou hypothétique. Ce que montre l'affaire Snowden, c'est que depuis une dizaine d'années, les gouvernements travaillent activement à développer un arsenal offensif, que cet arsenal existe (depuis au moins 2008), qu'il est utilisé pour certaines attaques, et que ces attaques sont de plus en plus largement utilisées. Il y a toutes les raisons de penser que ces techniques offensives sont développées par tous les pays (et pas seulement par les Etats-Unis).

L'événement « Snowden » est comparable à la découverte de « Stuxnet » en 2010 : il transforme un risque théorique en un événement certain et démontré.

Les conséquences sont de plusieurs natures :

- Pour les organismes qui doivent se protéger contre des attaques gouvernementales (par exemple des attaques de la NSA), il est nécessaire de réévaluer l'efficacité des mesures en place. Et la tâche est ardue car les moyens d'attaques de la NSA mis en évidence par l'affaire Snowden sont très avancés. L'isolation physique des projets sensibles, semble ici une obligation, mais elle a clairement un coût et des limites (l'isolation complète étant impossible).
- Les autres organismes doivent également se poser les mêmes questions, mais avec un degré d'exigence inférieur. Ils devraient par exemple vérifier que toutes les communications sortant de l'entreprise sont chiffrées ou que la compromission d'un poste de travail ne donne pas accès à l'ensemble des systèmes informatiques de l'entreprise. Il faut être conscient également que les attaques sophistiquées aujourd'hui réservées à un attaquant très aguerri (par exemple un état) vont se démocratiser et être reproduites par d'autres.

De façon plus anecdotique, la NSA devra aussi revoir son organisation interne pour comprendre comment une fuite d'une telle ampleur a pu se produire. Mais ce chantier a apparemment déjà été largement entamé.

2.2 Les attaques matérielles deviennent une menace réelle

Depuis plusieurs années, les publications concernant des attaques de bas niveau se sont multipliées. On peut citer par exemple :

- Les attaques visant le mode SMM (System Management Mode) des processeurs Intel et leurs applications pour des attaques de niveau BIOS (voir par exemple cette présentation SSTIC 2009).
- Les attaques des firmware de cartes réseaux (voir par exemple cette présentation CanSecWest 2010).
- Attaque DMA (Direct Memory Access) permettant depuis un périphérique d'accéder directement à la mémoire centrale (voir par exemple cette présentation SSTIC 2011)
- Etc.

En 2013, plusieurs nouvelles publications viennent compléter ce panorama :

- L'expérience d'implémentation d'une backdoor dans les firmware de disques durs (voir cette publication Eurecom de décembre 2013).
- Les vulnérabilités IPMI et BMC (voir cet article Cert-IST de septembre 2013).
- Le malware BadBIOS (voir cet article de ErrataSec d'octobre 2013). Même si ce malware n'existe pas vraiment (jusqu'à présent), il regroupe un ensemble de fonctionnalités avancées qui sont toutes théoriquement possibles.

L'ensemble de ces publications correspondent à des travaux de recherches ou à des prototypes. Par contre le catalogue secret ANT de la NSA (que nous avons déjà évoqué au chapitre précédent) découvert fin 2013, montre que la NSA dispose déjà de backdoors matérielles opérationnelles depuis 2008 :

- Backdoors embarquées sur disque dur,
- Backdoors de niveau BIOS,
- Backdoors embarquées sur une carte PCI.

Si ce catalogue ANT est authentique (mais il n'y a pas d'élément permettant de penser qu'il ne l'est pas), la possibilité de réaliser des attaques matérielles n'est donc plus un risque théorique.

L'évolution de la recherche montre depuis plusieurs années que les attaques de niveau hardware sont possibles (backdoor BIOS, attaques PCI, …). En 2013 cette menace a franchi un seuil significatif. En particulier le catalogue secret de la NSA, qui a été révélé fin 2013, montre que depuis 2008 la NSA dispose de ce type d'outil d'attaques. Il en est probablement de même pour d'autres gouvernements.

2.3 La sécurité offensive est de plus en plus présente

Depuis quelques années, la sécurité offensive s'est progressivement installée dans le paysage de la sécurité informatique. Et l'année 2013 marque une étape importante dans cette progression avec les événements suivants :

- Au niveau de l'état français, la sécurité offensive a été reconnue comme une composante à part entière de la Défense Nationale (cf. Le livre blanc publié en avril et la Loi de Programmation Militaire en novembre). Des initiatives équivalentes existent également dans les autres pays.
- La recherche et la commercialisation de vulnérabilités 0-day (et des codes d'exploitation associés), telles que pratiquées par exemple par la société française Vupen, sont désormais admises.

Cette évolution est compréhensible. Elle résulte des multiples cas d'attaques, contre des intérêts nationaux ou privés, constatés au cours de ces dernières années. Au niveau d'un état, il est devenu inconcevable de ne pas maîtriser la cyber-sécurité, d'un point de vue défensif aussi bien qu'offensif.

Par contre, il est clair que la sécurité offensive doit rester une prérogative des états et n'a pas sa place au niveau d'une entreprise. La montée en puissance de ces aspects suscitera cependant probablement des vocations, et on risque de voir se multiplier des sociétés qui proposent des services offensifs. Bien que cela ne semble pas une priorité actuelle pour les gouvernements, il paraitrait assez logique qu'une législation stricte et précise soit mise en place pour contrôler ce type d'activité. On pourra noter dans ce domaine, que fin 2013, le gouvernement français a mis en place des restrictions sur l'exportation de systèmes d'écoutes pour les réseaux IP (voir cet article de Numerama).

3) Revue des failles et attaques de 2013

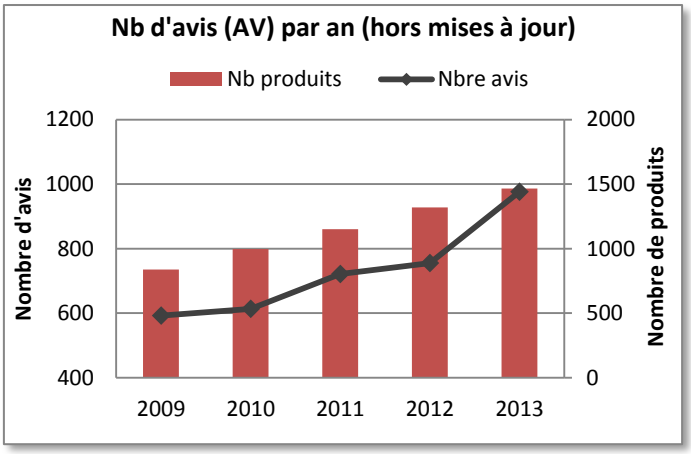
3.1 La production du Cert-IST en 2013

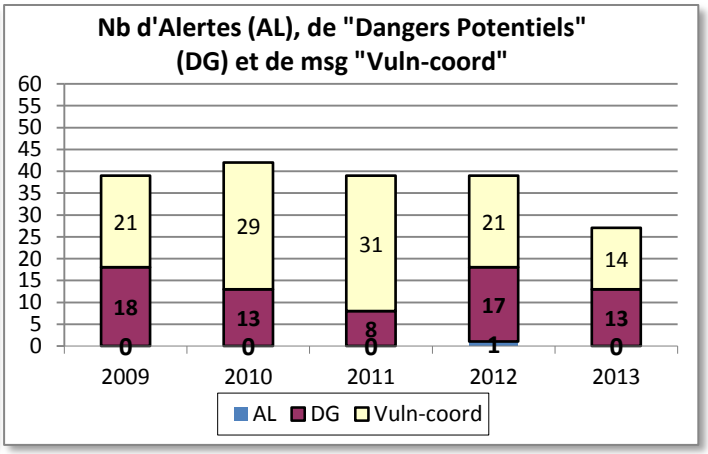
3.1.1 Veille sur les vulnérabilités et des menaces

Dans le cadre de son activité de veille sur les vulnérabilités et les menaces, le Cert-IST suit de façon continue, différentes sources d'informations (annonces constructeurs, blogs sécurité, mailing-lists, échanges privés entre CERT, etc.) afin d'être informé des nouvelles vulnérabilités. Ces informations sont analysées quotidiennement pour fournir à nos adhérents des informations triées, qualifiées et priorisées. Le Cert-IST émet ainsi plusieurs types de publications :

- Les **Avis de sécurité** : ils décrivent les nouvelles vulnérabilités découvertes dans les produits suivis par le Cert-IST. Ces avis sont enrichis de façon continue avec des mises à jour mineures ou majeures. Ces dernières correspondent typiquement au cas où des programmes d'attaques – des "exploits" – sont publiés.
- Des **Alertes**, des **Dangers Potentiels** et des **messages "Vuln-coord"**. Les Alertes du Cert-IST sont utilisées pour les menaces majeures nécessitant un traitement prioritaire. L'émission d'une alerte est un événement rare : par exemple le Cert-IST a émis en 2012 une alerte sur les vulnérabilités du JRE Java et les attaques associées. Les Dangers Potentiels décrivent des menaces significatives mais non encore imminentes (ou d'une gravité modérée) pour lesquelles le Cert-IST recommande des mesures de protection spécifiques. Les messages "Vuln-coord" enfin, sont des informations de coordination qui attirent l'attention sur des vulnérabilités particulières mais d'une dangerosité immédiate plus faible. Ces 3 catégories complémentaires sont axées sur les risques d'attaques alors que les avis de sécurité répertorient eux de façon systématique toutes les vulnérabilités (quelque soit leurs probabilités d'être utilisées dans des attaques).

Les graphiques ci-dessous montrent la production du Cert-IST au cours des dernières années.





Ainsi, en 2013, le Cert-IST a publié :

- **976 avis de sécurité**, suivis de façon continue au cours de l'année avec 2580 mises à jour mineures et 94 mises à jour majeures. Le nombre d'avis est en augmentation constante depuis plusieurs années (cf. la courbe ci-dessus), et ce phénomène s'est fortement accentué en 2013 (+29% par rapport à 2012). Cette augmentation continue montre que la découverte de vulnérabilités est un phénomène qui ne se tarit pas : invariablement, d'année en année, des vulnérabilités sont trouvées dans les produits qui constituent le S.I. de l'entreprise. Le maintien du niveau de sécurité passe donc forcement par une application régulière des

correctifs de sécurité sur ces produits. Au 31/12/2013 le Cert-IST suivait les vulnérabilités concernant 1 466 produits et 11 778 versions de produits.

- **Pas d'Alerte, 13 Dangers Potentiels et 14 messages "Vuln-coord"**. Nous analysons ces publications 2013 au chapitre 3.2 ci-dessous.

3.1.2 Veille technologique

En plus de la veille sur les vulnérabilités, le Cert-IST publie également des bulletins de veille technologique :

- Un bulletin quotidien de veille média recense les articles les plus intéressants parus sur Internet sur un échantillon de sites francophones et anglophones traitant de sécurité.
- Un bulletin mensuel de veille SCADA présente une synthèse de l'actualité sur la sécurité des systèmes de contrôle industriel.
- Un bulletin mensuel généraliste donne une synthèse de l'actualité du mois (en termes d'avis et d'attaques) et traite de sujets d'actualité au travers d'articles rédigés par le Cert-IST.

3.2 Les Alertes et Dangers Potentiels émis par le Cert-IST

En 2013, le Cert-IST n'a pas émis d'alerte. Ce type de publication est en effet réservé aux menaces les plus graves et la dernière alerte du Cert-IST reste donc celle que nous avons émise en 2012 à propos des attaques visant le JRE Java.

Nous avons par contre, émis 13 Dangers Potentiels (DG), qui correspondent à des menaces moins graves que les Alertes. Ces DG de 2013 se répartissent de la façon suivante :

- 6 DG concernent **Windows**, dont 4 pour **Internet Explorer,**
- 4 DG sur le JRE de **Java,**
- 1 DG sur **Adobe Reader,**
- 1 DG sur le malware **CryptoLocker,**
- 1 DG sur un système de video-conférence **Cisco TelePresence System.**

12 de ces 13 DG concernent des attaques visant le poste de travail. Cette année encore, le poste de travail reste donc la cible la plus exposée aux attaques. Le poste de l'utilisateur est en effet à la fois la cible des cyber-criminels (qui tentent d'infecter les postes des particuliers) et des cyber-espions (qui tentent de s'infiltrer dans les entreprises).

Windows (et Internet Explorer) restent des cibles de choix. Un grand nombre des attaques vues en 2013 visaient Internet Explorer 8 et Windows XP. Cet environnement était encore très présent dans les entreprises en 2013 et les attaques ciblées (qui visaient explicitement certaines entreprises) ont donc particulièrement concerné ces environnements.

Nous présentons plus largement les menaces **Java** et **CryptoLocker** dans le chapitre « Zoom » ci-dessous.

Pour le DG **Cisco TelePresence System,** il s'agit d'un mot de passe par défaut qui permet de prendre le contrôle complet d'un système vulnérable.

3.3 Zoom sur quelques failles et attaques

Nous décrivons ici les vulnérabilités et les attaques qui nous paraissent les plus importantes. Celles qui concernaient directement les entreprises et nécessitaient des réactions immédiates ont fait l'objet de Dangers Potentiels. Les autres ont généralement été traitées au niveau du bulletin mensuel du Cert-IST.

- **Vulnérabilités dans Java (de janvier à avril 2013)**

Nous avions identifié Java comme le composant le plus vulnérable (et donc le plus dangereux) dans notre bilan 2012, et les vulnérabilités de Java sont restées très présentes en 2013, en particulier au premier semestre. De janvier à avril 2013 :

- Oracle a publié coup sur coup 5 mises à jour (alors que son calendrier nominal n'en prévoyait que 2) pour corriger de nouvelles vulnérabilités découvertes.
- Nous avons publié 4 Dangers Potentiels pour avertir nos membres d'attaques utilisant des vulnérabilités Java.

De janvier à avril, Oracle a été pris dans une course qui semblait sans fin puisque de nouvelles vulnérabilités étaient découvertes quelques jours à peine après la publication d'un correctif pour les vulnérabilités précédentes. La situation s'est calmée à partir de fin avril, et Oracle n'a publié ensuite que des correctifs trimestriels. Il est difficile de dire si cette amélioration veut dire que Java est désormais un composant sûr. Il est possible en effet que ce soient les chercheurs de failles (et en particulier la société Security Exploration qui s'est beaucoup investi sur ce sujet) qui aient changé de cible et aient délaissé (provisoirement ?) la recherche de vulnérabilités Java.

Java reste un composant très sensible, et il est la cause principale des infections lors de la navigation web. Ce composant doit impérativement être maintenu à jour pour éviter ces attaques.

- **Vulnérabilités du protocole UPnP (janvier 2013)**

En janvier 2013, la société Rapid7 (éditeur du produit MetaSploit) a publié une étude à propos des dangers liés au protocole UPnP :

- De nombreux équipements sont mal configurés (17,5 millions !) et autorisent l'accès aux services UPnP depuis internet, alors que ces services ne devraient être accessibles qu'en interne.
- Des vulnérabilités majeures existent dans les implémentations les plus courantes de ce protocole (**libupnp** et **MiniUPNP**).

UPnP est connu depuis longtemps comme posant des problèmes de sécurité. Il s'agit d'un protocole plutôt destiné aux équipements résidentiels (de type « box » ADSL, ou serveurs multimédia) et devrait être peu présent en entreprise. Mais beaucoup de petits équipements, par exemple les caméras IP, intègrent UPnP. Il est donc très répandu : Rapid7 a identifié dans son étude environ 6900 produits embarquant un service UPnP vulnérable. Et la correction des vulnérabilités de ce type d'équipement est très souvent impossible car non prévue par le fournisseur.

Nota : Ces vulnérabilités ont fait l'objet d'un article dans notre bulletin de février 2013.

- **Attaque DDOS record contre Spamhaus (mars 2013)**

Spamhaus (organisme qui lutte contre le Spam) a subi en mars 2013 une attaque en déni de service d'une puissance record, avec des pics de trafic à 300 Gbits/s. L'attaque a été réalisée en utilisant la technique appelée "amplification DNS" : l'attaquant envoie du trafic vers des serveurs DNS mal configurés qui submergent alors involontairement la cible visée par l'attaquant avec des messages de

réponses. Au moins 2 personnes ont été par la suite arrêtées (en Espagne et en Angleterre) dans le cadre de l'enquête qui a suivi.

Nota : Cette attaque a fait l'objet d'un article dans notre bulletin d'avril 2013.

- **Vulnérabilités dans IPMI/BMC (août 2013)**

Des vulnérabilités graves dans IPMI (Intelligent Platform Management Interface) et BMC (Baseboard Management Controller) ont été révélées en 2013 : d'abord par Dan Farmer (début 2013), puis par Rapid7 et une université du Michigan à la conférence Usenix-Woot'13 (lors de l'été 2013).

IPMI est un protocole de bas niveau qui permet d'administrer à distance des serveurs. Il est très répandu en entreprise et est connu sous différents noms commerciaux : HP **iLo**, Dell **iDrac**, Oracle/SUN **iLOM**, Lenovo/IBM **IMM**, etc.

A notre connaissance il n'avait jamais été fait auparavant d'études de sécurité sur cette technologie et (comme on pouvait s'y attendre dans un tel cas) des défauts graves ont été trouvés, qui permettent de prendre le contrôle à distance des équipements.

Nota : Ces vulnérabilités ont fait l'objet d'un article dans notre bulletin de septembre 2013.

- **Attaques CryptoLocker (octobre 2013)**

CryptoLocker est un "ransomware" qui chiffre des fichiers (documents, photos, etc.) sur le poste infecté, puis réclame une rançon pour les déchiffrer. Les virus "ransomware" ne sont pas nouveaux, mais "CryptoLocker" s'est diffusé largement à partir d'octobre 2013 (via des campagnes d'envoi de mails piégés) et il cause une perte de données importante sur les postes infectés (le chiffrement est robuste et seul le paiement de la rançon permet de récupérer les fichiers chiffrés).

Nota : Le Cert-IST a émis un Danger Potentiel pour prévenir notre communauté de la menace induite par le virus « CryptoLocker ».

- **Attaque Adobe et vol de code source (octobre 2013)**

En octobre 2013, l'éditeur Adobe a annoncé avoir subi une attaque sévère, avec le vol de 40 Go de codes sources de ses produits, et d'un très grand nombre de comptes clients (données telles des numéros de cartes bancaires et des identifiants de connexion) Bien que stockées sous forme d'empreintes (hash), ces données clientes ont été diffusées sur Internet et des personnes malveillantes peuvent donc tenter de les décrypter. Initialement 2,9 millions d'identifiants étaient supposés être dans la nature, mais au final il s'agirait de plus de 150 millions de comptes.

4) Comment l'entreprise peut se protéger

Il existe aujourd'hui 4 grandes catégories d'attaquants : les amateurs, les hacktivistes, les cyber-criminels et les cyber-espions. Et pour l'entreprise les principales attaques qui en résultent sont de 3 types :

- Les attaques par infiltration (APT), qui sont principalement réalisées par les cyber-espions,
- Les attaques opportunistes, qui sont le plus souvent le fait d'hacktivistes,
- Les attaques visant les systèmes industriels (les SCADA).

Dans ce chapitre nous examinons ces différentes classes d'attaques et les moyens de s'en protéger.

4.1 Les attaques par infiltration (APT)

Le scénario de ces attaques est bien connu et nous l'avions détaillé dans notre bilan 2011 :

- Infecter un premier poste de travail au sein de l'entreprise et y installer une backdoor permettant d'agir à distance sur le poste.
- Rester invisible et survivre le plus longtemps possible sur le système infecté.
- Explorer son environnement et progresser au sein de l'entreprise en infectant de nouveaux systèmes jusqu'à atteindre sa cible.
- Collecter des données sensibles et les exfiltrer, ou saboter le système visé.

Dans ce scénario, l'attaquant doit tout d'abord prendre pied dans l'entreprise en compromettant un premier poste interne. Pour ce faire il essayera successivement 3 méthodes :

- **L'ingénierie sociale** pour convaincre l'utilisateur d'ouvrir une pièce jointe ou de visiter un site web piégé,
- **La vulnérabilité du poste de travail** : par exemple une faille PDF, Java ou Internet Explorer,
- **L'attaque au moyen d'un 0-day** si l'attaquant attache beaucoup d'importance à sa cible.

Les entreprises exposées à la concurrence internationale ne doivent plus se demander si un jour elles seront touchées ou non par une attaque par infiltration (APT), mais quand cela se produira. Elles doivent surtout se préparer à cet événement en limitant son impact potentiel et en développant leur capacité de détection et de réaction face à ce type d'incident.

Pour améliorer ses défenses l'entreprise doit prendre en compte ces 3 méthodes :

- **Informer les utilisateurs** du risque d'attaques par ingénierie sociale, leurs apprendre à les déjouer et à informer au plus vite lorsqu'une attaque de ce type a réussi.
- **Maintenir à jour les postes de travail** d'un point de vue sécurité. Cela s'applique aux systèmes d'exploitation, mais aussi aux logiciels applicatifs comme Adobe Reader ou Java.
- **Intégrer le risque d'attaque 0-day** dans le processus de gestion de la menace de l'entreprise.

Comme nous l'expliquions dans notre bilan 2012, le risque d'attaque 0-day ne doit pas être négligé. Les attaquants aguerris disposent assez facilement de 0-day. Ils peuvent par exemple les acheter à des sociétés spécialisées dans la recherche de telles failles. Il est donc nécessaire d'intégrer le risque 0-day dans le processus de gestion de la menace de l'entreprise. Cela implique en particulier de considérer comme un fait certain qu'un jour un poste de travail ou un serveur de l'entreprise sera victime d'une attaque réussie.

Au delà de la protection du poste de travail, la lutte contre les APT implique des actions plus larges, au niveau du système d'information :

- Adapter son architecture pour limiter l'impact d'une attaque réussie.
- Mettre en place une surveillance active au sein de l'entreprise, au travers d'une structure responsable de la supervision de la sécurité.
- Définir une procédure de réaction en cas d'incident définissant le comportement à adopter et les personnes à impliquer.

4.2 Les attaques opportunistes

Les attaques opportunistes, telles que celles réalisées par les hacktivistes, visent des proies faciles (on utilise souvent pour ces proies le terme de "low-hanging fruits"). Traditionnellement, il s'agit de sites web mal protégés. En 2013, nous avons vu également des attaques plus originales, qui visaient par exemple les comptes Twitter d'entreprises.

- **Les sites web mal protégés**

Les sites web des entreprises sont les cibles numéro un des attaques hacktivistes, et leur résistance aux attaques en déni de service, et la recherche de failles triviales sont deux éléments systématiquement testées dès qu'une campagne d'attaques est envisagée.

Le plus souvent les failles triviales n'existent pas lors de la mise en production initiale des sites web. Mais elles apparaissent avec le temps parce que ces sites web ne sont pas mis à jour en appliquant les patches de sécurité. Et au bout de trois ans sans mise à jour, l'état de sécurité du site web s'est considérablement dégradé car des vulnérabilités ont été découvertes dans le framework utilisé (par exemple Joomla, WordPress, etc…). Il est alors trivial pour un attaquant d'en prendre le contrôle.

Tout comme pour les postes de travail (cf. § 4.1) la mise à jour régulière des sites web en appliquant les correctifs de sécurité est indispensable.

- **Attaques de comptes Twitter mal protégés**

En 2013, les hacktivistes ont trouvé de nouveaux vecteurs d'attaques en s'attaquant une fois de plus au maillon humain. Par exemple le groupe SEA (Syrian Electronic Army – groupe hacktiviste qui prend parti pour Bachar el-Assad) est parvenu, grâce à des attaques de phishing à voler les mots de passe :

- de **comptes Twitter d'entreprises**. En avril, un compte Twitter du journal Associated Press a été détourné et les attaquants l'ont utilisé pour diffuser de fausses nouvelles (explosions à la Maison Blanche) ce qui a provoqué une courte chute de cours boursiers. Le même type d'incident a également touché les journaux The Guardian et New York Post.
- de **comptes de gestion des infrastructures DNS** . En août, le SEA a réussi à voler le compte d'un vendeur de noms de domaines australien (le registrar "MelbourneIT"). Cela a permis à SEA de modifier les enregistrements DNS associés pour plusieurs noms de domaines réputés, dont **Twitter**, et le **New York Times**, et de perturber le fonctionnement de ces sites.

Il s'agit d'attaques peu sophistiquées, basées sur l'ingénierie sociale, mais on voit que des cibles de renom peuvent en être victime. Il est difficile de se protéger a priori contre tous les types d'attaques. Par contre il est important de se tenir au courant de ces nouvelles attaques pour prendre au plus tôt les mesures pour s'en protéger :

- Informez les responsables de la communication des attaques possibles contre les comptes Twitter ou Facebook de l'entreprise, et aidez à définir des règles de protection pour éviter ces attaques élémentaires.
- Vérifiez que vos fournisseurs de noms de domaines ont connaissance des attaques qui ont touchés leurs confrères et vérifiez que des mesures de protection adéquates ont été prises.

Les conséquences de ces compromissions sont souvent spectaculaires (même si les détournements sont rapidement découverts et les incidents rapidement résolus) et sont comparables en termes d'impacts au défacement de la page d'accueil d'un site web institutionnel.

Ces attaques exploitent pour l'essentiel le maillon humain : l'attaquant envoie des mails de phishing vers un ensemble de cibles (par exemple des responsables de communication, ou des services d'enregistrement de noms de domaines) et parvient ainsi à voler le mot de passe de certains comptes. S'il a de la chance, il peut ainsi avoir accès à des comptes prestigieux.

4.3 Les attaques visant les systèmes industriels (SCADA)

Depuis 2010 et la découverte du malware Stuxnet qui visait les centrifugeuses d'enrichissement nucléaire de l'Iran, le risque d'attaque visant les systèmes industriels est devenu une préoccupation majeure.

Depuis cette date des indicateurs montrent que la menace progresse :

- En 2011, le nombre de failles publiées à propos des systèmes SCADA explose et atteint une progression de 500%. Des kits de vulnérabilité SCADA apparaissent. Il s'agit le plus souvent de failles triviales découvertes par des spécialistes de la faille IT qui n'ont pas de compétence particulière en SCADA
- En 2012, la recherche de failles devient plus pointue parce des spécialistes du monde SCADA se mettent eux aussi à chercher activement des vulnérabilités.
- En 2013, le nombre de vulnérabilités publiées a diminué, mais les vulnérabilités publiées sont souvent graves. Par exemple, des failles "génériques" sont découvertes (c'est le cas en particulier pour le protocole DNP3).

De même, Trend-Micro a publié en 2013 une étude qui montre que lorsqu'un système SCADA est connecté sur Internet, alors ce système est attaqué par des pirates qui recherchent spécifiquement ce type d'équipements : pour plus de précisions sur ce Honeypot SCADA, reportez vous à cet article qui résume la présentation de Trend-Micro à Blackhat 2013.

Comme nous le disions dans notre bilan 2012 : la sécurité industrielle est un domaine où la menace progresse et où le niveau de sécurité de certaines installations parait encore très insuffisant. Cette situation est préoccupante.

Les gouvernements sont bien conscients de cette situation et travaillent de façon active sur ces sujets. En France, l'année 2013 a été le témoin de progrès majeurs avec la constitution d'un groupe de travail et la publication en janvier 2014 de plusieurs guides de sécurisation.

La sécurisation des systèmes SCADA reste une priorité majeure et un enjeu stratégique.

5) Conclusions

Au cours de ces dernières années, les menaces visant les systèmes d'information de l'entreprise ont augmenté de manière significative et se sont durcies :

- 2010 : L'attaque Stuxnet a montré que **les systèmes SCADA** sont des cibles de choix et qu'il est impératif de les protéger activement
- 2011 : **Les attaques par infiltration** visant les entreprises (principalement dans un but de cyber-espionnage) se sont multipliées et sont devenues une préoccupation majeure. **L'hacktivismes** a aussi fait son apparition et démontré que des attaques opportunistes et relativement peu sophistiquées peuvent avoir un impact significatif en termes d'image.
- 2012 : La **multiplication des attaques 0-day** a montré qu'aucun système n'est à l'abri d'une attaque réussie et que les systèmes d'information doivent être conçus en prenant en compte le fait qu'ils seront compromis.
- 2013 : L'affaire Snowden montre que certains groupes (des groupes étatiques ou spécialisés dans les attaques de niveau étatiques) ont développé **un arsenal d'attaques bien plus poussé que ce que l'on pouvait imaginer** jusque là.

En parallèle, l'évolution de la société a augmenté la dépendance de chacun à l'outil informatique et à l'interconnexion des systèmes. Et il y a une demande croissante au sein des entreprises pour une plus grande ouverture à ces nouvelles technologies (Cloud, BYOD, etc..).

Le RSSI doit donc composer avec une situation complexe. Et pour informer les projets ou décider des actions à entreprendre, il a besoin de connaitre précisément les risques. Le Cert-IST, au travers de son activité de veille technologique et de ses bilans, lui donne une vision argumentée de la menace. Et celle-ci est clairement en augmentation. Il est de notre rôle aussi de rappeler que les modèles de sécurité éprouvés sont ceux qui appliquent les principes traditionnels d'une sécurité en profondeur (sécurisation des plates-formes, application des correctifs de sécurité, segmentation des réseaux, limitation des privilèges, etc.). Le guide « 20 Critical Security Controls For Effective Cyber-Defense » publié aux USA ou le « Guide de l'hygiène informatique » publié en France par l'ANSSI en janvier 2013 vont clairement dans ce sens.

Nous pensons que les actions de sécurisation doivent s'intéresser tous particulièrement aux aspects suivants :

- Sécuriser des infrastructures industrielles (le Scada).
- Informer les utilisateurs sur les techniques d'attaques (en particulier l'ingénierie sociale) et sur la conduite à tenir face aux tentatives d'attaques.
- Maintenir le niveau de sécurité des installations en appliquant les patches de sécurité, en particulier pour les installations directement exposées aux attaques (ex : le poste de travail et les serveurs web).
- Considérer que la compromission d'un poste de travail ou d'un serveur est un événement possible, en particulier du fait des attaques 0-day.

Pour traiter ce dernier point, les actions suivantes nous paraissent souhaitables :

- Adapter son architecture pour limiter l'impact d'une attaque réussie.
- Mettre en place une surveillance active au sein de l'entreprise, au travers d'une structure responsable de la supervision de la sécurité.
- Développer les procédures de réaction en cas d'intrusion et faire traiter les attaques par une équipe spécialisée.

Fin du document