SÉCURITÉ de l'information
Sécurité Informatique / Numéro 6 ////// Novembre 2009

Éditorial

Du bon usage de la veille pour la gestion des vulnérabilités

PAR YVON KLEIN
Directeur Technique du Cert-IST

Le Cert-IST **(Computer Emergency Response Team – Industrie Services et Tertiaire)** est une association de loi 1901 qui a pour vocation d'assurer, pour ses adhérents, des **services de veille et d'alerte, de prévention des risques et d'assistance aux traitements d'incidents** destinés aux entreprises et organismes français.

Les membres partenaires, responsables de la stratégie des services, sont le CNES, France Telecom Orange, Sanofi Aventis et le groupe Alcatel-Lucent.

L'activité de prévention du CERT-IST s'appuie sur une analyse quotidienne des nouvelles vulnérabilités, de leurs criticités et des moyens de protection pour y répondre. Les avis et alertes de sécurité, que le Cert-IST diffuse auprès de ses adhérents, permettent à ceux-ci d'être informés sur les menaces sur leur Système d'Information et sur les parades.

Le système d'information d'une entreprise ou d'un organisme est un organe vital pour son fonctionnement, et toute dégradation du service rendu par le S.I. se traduit par des dommages tant sur son image, dans la réalisation de ses activités et missions, que sur le plan financier. L'objectif de l'entreprise sera de se protéger le plus efficacement possible contre toutes menaces sur son S.I.

L'expérience du Cert-IST en matière de veille permet de faire un constat sur l'évolution des menaces pesant sur les organismes ou les entreprises et sur l'évolution des moyens de protection que ceux-ci doivent mettre en œuvre pour contrer les vulnérabilités toujours plus nombreuses touchant les composants de leur S.I.

Jusqu'à présent la menace sur le S.I. d'un organisme, quel qu'il soit, portait en priorité sur son architecture et sur la cohérence et la complétude des moyens de protection. Aujourd'hui, la menace est indissociable des vulnérabilités découvertes et suivies au fil des jours et qui peuvent altérer la robustesse propre aux composants mêmes du S.I.

L'objectif de ce numéro est d'analyser les actions que les entités doivent mettre en œuvre pour disposer du meilleur niveau de protection et de la réactivité la plus efficace face à cette évolution de la menace.

directeur-technique@cert-ist.com

Évolution de la menace

Philippe Bougeois
(Expert sécurité au Cert-IST),

Thierry Maronier
(Expert Sécurité Alcatel-Lucent)

L'analyse des bilans annuels du Cert-IST sur les menaces et les vulnérabilités permet de suivre l'évolution du risque sur le système d'information d'un organisme.
Il y a quelques années, le principal risque pouvant affecter les systèmes d'information était constitué par le manque de protection du système contre le risque d'attaques massives via de nombreux virus informatiques et autres chevaux de Troie.

Des attaques de plus en plus rapides

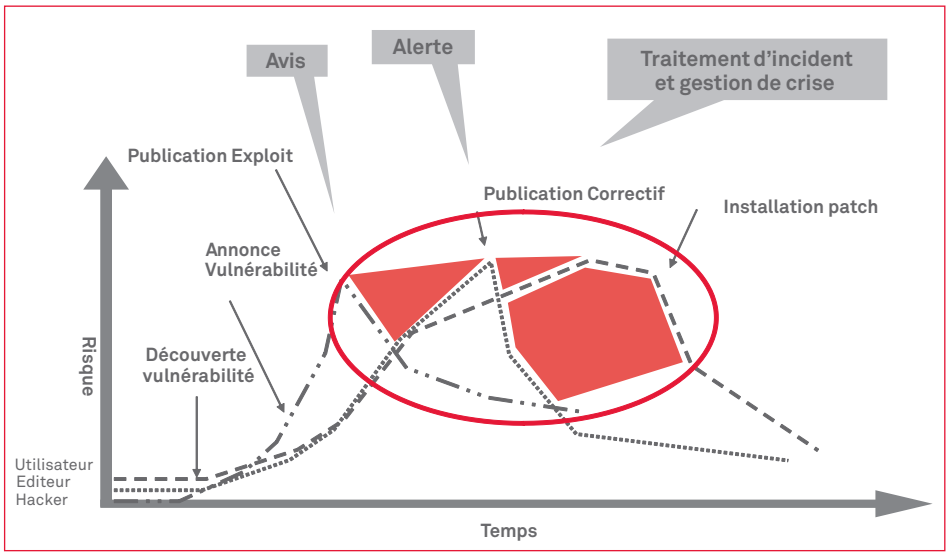
Ces dernières années, la menace virale reste toujours aussi importante, mais elle a sensiblement évolué, devenant plus pernicieuse et nécessitant la prise en compte d'un certain nombre de paramètres :

- La modification de l'enchaînement des événements qui suivent la découverte d'une vulnérabilité et la réduction des intervalles de temps dans cette chaine,
- Des attaques de plus en plus ciblées, notamment sur les vulnérabilités des systèmes d'exploitation et des applications,
- Des agresseurs mieux outillés et plus « professionnels »,
- Des méthodes d"attaques plus structurées.

Dans un cas idéal, la chronologie des événements pour une vulnérabilité devrait suivre les étapes suivantes : la découverte d'une vulnérabilité, la publication du correctif approprié pour cette vulnérabilité, puis éventuellement la publication d'un code d'attaque qui permet la mise en œuvre de cette vulnérabilité (exploit). Malheureusement, comme le montre le schéma temporel ci-dessous, le cycle réel des événements n'est souvent pas dans cet ordre idéal, ce qui expose le S.I. à un risque d'attaque, avant d'avoir mis en place une protection.
Pour prendre en compte cette chronologie, une cellule de veille sera amenée à traduire ces événements successifs suite à l'émission par le Cert-IST de différentes publications :

- un Avis est publié quand une vulnérabilité est annoncée, et qu'il existe soit un correctif, soit une mesure de contournement,
- un Danger est publié lorsqu'un exploit est identifié pour cette vulnérabilité,
- une Alerte est publiée quand l'exploit est utilisé pour réaliser des attaques ciblées ou massives.

>>>> *suite page 2*



Evolution du risque dans le temps

Le fuzzing est une technique initialement utilisée pour tester des logiciels et pour automatiser l'identification de bugs ou de failles dans des applications, avec pour principe d'injecter des données aléatoires dans les entrées d'un programme. Lorsque le programme (fuzzer) échoue (par exemple en s'arrêtant brutalement ou en générant une erreur), alors il y a des défauts [à corriger]. Les fichiers, les périphériques (clavier, souris, etc.), les variables d'environnement, les données reçues du réseau peuvent constituer des points d'entrée pour un programme de fuzzing.
Initialement destinés à améliorer les développements, les pirates en font aussi usage car ils leur permettent de découvrir rapidement des vulnérabilités et de concevoir des codes d'exploitation avant la mise à disposition de correctifs.

Durant les dernières années, le temps de réaction entre la découverte d'une vulnérabilité et son exploitation en vue d'une attaque s'est considérablement réduit.
En 2003, le temps moyen de réaction pour la réalisation d'une attaque de masse était de 25 j environ (e.g. Blaster ou Sasser). En 2005, ce temps de réaction moyen est passé à 4 j (e.g. Zotob).
Ce changement induit une transformation indispensable des processus de veille, afin d'anticiper les crises potentielles et de couvrir au mieux la période de risque maximal qui suit l'alerte sur une faille et ne commencera à décroître qu'avec l'application du correctif approprié.
Ceci entraîne une évolution dans le cycle de veille des vulnérabilités. Il est, par exemple, possible dans le cas d'attaques utilisant des vulnérabilités encore inconnues (attaques appelées « 0-day »- vulnérabilité exploitée sans préavis de découverte et publication) de voir apparaître l'émission d'une alerte avant même l'émission de l'avis qui décrit la vulnérabilité exploitée.

Des attaques de plus en plus ciblées

Pour saisir les différents aspects de cette évolution, il est important de tenir compte des motivations mêmes des agresseurs. Les objectifs poursuivis par ceux-ci sont maintenant principalement d'ordre économique, guidés par la recherche de gains financiers considérables, mais peuvent aussi relever d'intérêts d'ordre idéologique (politique, religieux, terrorisme par exemple).
Ainsi, la menace pour les organismes a changé. Les années 2001 à 2005 ont été celles des attaques virales massives qui paralysent les réseaux d'entreprises (avec par exemple : Nimda et CodeRed en 2001, Slammer en 2003, Sasser en 2004, et Zotob en 2005).
La menace est devenue plus pernicieuse : beaucoup plus discrète, et beaucoup plus puissante. Cela signifie pour l'entreprise un renforcement du risque de type « atteinte à l'image » ou « perte de données ». Ainsi, à partir de mars 2006, les nombreuses vulnérabilités identifiables dans les navigateurs génèrent une nouvelle vague d'attaques en phishing notamment dirigées vers de grandes banques françaises.
Certes, dans le même temps le niveau de défense des entreprises s'est accru, mais aujourd'hui s'il reste le moindre point faible dans la cuirasse, il y a fort à parier qu'il y aura quelqu'un capable de l'identifier et de l'exploiter. En effet, ces faiblesses seront maintenant majoritairement ciblées pour voler (discrètement) de l'information ou de l'argent à l'entreprise ou à des utilisateurs finaux.
Du fait de l'importance de ces enjeux, la cybercriminalité passe forcément par une phase de « professionnalisation » accrue. Au cours de ces années, l'expertise des attaquants (et le nombre de personnes capables de devenir attaquants) s'est fortement développée, la recherche de faille s'est automatisée et systématisée (au moyen d'outils tel que les « fuzzers » [voir l'encadré]) et le risque d'une fraude financière ou d'une compromission de données devient de plus en plus important.

Des attaquants de plus en plus professionnels

En 2007, cette tendance s'est largement confirmée et la professionnalisation a franchi une étape supplémentaire par le biais de :

- la professionnalisation des outils (comme « metasploit », « mpack », etc.) et codes malveillants qui se traduit par une sophistication de plus en plus grande des codes malveillants (Stormworm/zhelatin, Conficker, ...) ;
- la professionnalisation des agresseurs, avec au-delà de la criminalisation de l'escroquerie électronique (phishing et autres « xxx-ing »), les premières attaques massives de caractère cyber terroriste.

Par exemple, le ver Storm Worm (apparu en 2007) consacre la fusion des techniques d'attaques : association de la propagation d'un spam et/ou d'un cheval de Troie avec infection par la navigation web, puis utilisation sur le poste infecté de techniques de furtivité, de rootkit, de défense active, et enfin mise en réseau des différentes machines infectées au travers d'un botnet P2P.
Ce botnet est aussi l'un des premiers botnets conçus pour être difficiles à détecter et éradiquer, en particulier sur une infrastructure opérateur/grand public, car il utilise (au lieu d'un classique serveur IRC) un modèle de communication P2P totalement décentralisé (utilisation du protocole « Overnet » qui est la forme la plus aboutie de système P2P décentralisé). D'une part, il se fond dans le trafic P2P habituel (typiquement eMule) d'autre part, il est très difficile de lui associer une signature réseau (pas de ports fixes, trafic UDP, etc.) sans recourir à des solutions complémentaires telles que le DPI (Deep Packet Inspection).
Plus récemment, le ver Conficker (apparu fin 2008) a été un autre exemple de la sophistication permanente des codes d'attaques. Il pallie ainsi à une des faiblesses identifiées dans Storm Worm (sa faible résistance à l'infiltration par de faux agents) et implémente pour la première fois au monde le protocole cryptographique MD6 pour renforcer le

Maîtriser son Système d'Information

L'évolution de la menace conduit les entités à devoir adapter leur réactivité aux nouvelles formes d'attaques. Pour pouvoir garantir cette réactivité, il est nécessaire de s'appuyer sur une parfaite maîtrise du Système d'Information. Ceci demande de réaliser une « cartographie » du S.I. basée sur les risques.

Gestion du risque du Système d'Information

Cette cartographie fait partie des mesures que l'entité met en œuvre dans le cadre d'une gestion du risque complète et efficace. On distingue généralement plusieurs types de risques, les risques financiers, opérationnels, de conformité ou d'atteinte à l'image. Les risques liés à l'usage du Système d'Information sont vus comme des risques opérationnels. La cartographie sera réalisée à partir de l'analyse des différentes fonctions du S.I. dans la vie de l'entité, que ce soit d'un point de vue métier ou d'un point de vue technique.

Cartographie du Système d'Information

Elle va permettre d'identifier chaque composant du S.I et, pour chaque composant, sa fonction, ses interfaces et les acteurs responsables de ce composant, que ce soit les acteurs pour les fonctions métiers (en général, la Maitrise d'ouvrage) ou que ce soit ceux pour les fonctions techniques (en général les administrateurs). A partir de sa cartographie, il est possible de comprendre les enjeux du S.I. et d'en maîtriser le risque, qu'il soit fonctionnel ou technique, en particulier en identifiant dans les chaînes de traitement de l'information les « maillons faibles » sur lesquels devra se porter l'attention pour contrer les menaces.
Cartographier son S.I. ne signifie pas nécessairement être capable de le représenter sur une série de diagrammes, ce qui n'apporterait rien à la problématique du maintien en condition de sécurité, mais bien d'identifier les responsabilités de chaque acteur et de mesurer avec eux les différents risques pesant sur ce composant, et leurs impacts sur l'entreprise.
Les risques propres au S.I. peuvent concerner les serveurs ou les postes de travail, les infrastructures et les réseaux, les O.S. ou les applications. La mesure de la criticité des composants du S.I. devra se faire en prenant en compte les différents aspects des fonctions mises en œuvre, comme la disponibilité ou la continuité du service, mais aussi l'intégrité ou la confidentialité des informations et des fonctions, et leur auditabilité.

Maintien du niveau de sécurité du Système d'Information

A partir de la cartographie du S.I., il est donc possible de définir la criticité de chaque composant et de maîtriser les processus d'évolution et de mise à jour de ces composants, en permettant aux acteurs responsables de conduire une analyse de risque, prenant en compte la finalité des fonctions offertes par le composant dans le fonctionnement de l'entreprise et le poids effectif de la menace sur ces fonctions.

Au-delà du risque sur les composants du S.I., le risque existe aussi sur les acteurs qui auront à gérer et exploiter ce S.I. Cela nécessite des efforts importants de formation et de sensibilisation, et la cartographie sera un outil indispensable au maintien des compétences des équipes concernées.

L'application des correctifs de sécurité ou des mesures de contournement d'une menace nécessite d'établir une coordination entre les différents acteurs qu'ils soient métiers, exploitants ou sécurité. La cartographie sert alors de support de communication et d'échange. Elle doit pouvoir être facilement appréhendée par chaque acteur pour être un outil d'aide à la décision par la vision globale du S.I. qu'elle fournit.

La cartographie du S.I. sert aussi de base pour le contrôle de l'application des correctifs et la définition de la stratégie d'audit du S.I. pour cibler en priorité les systèmes critiques. Cette approche conduit l'entreprise à mettre en place une politique d'application des correctifs de sécurité sur son S.I.

contrôle d'intégrité sur les codes malicieux téléchargés.
Le marché informatique est caractérisé par un rythme élevé d'innovations et de possibilités d'interconnexions toujours plus nombreuses, dont la technologie est toujours plus complexe. Ces innovations ont également entraîné une augmentation du nombre des vulnérabilités et accentué les conséquences de celles-ci. C'est souvent la sécurité qui en souffre le plus. En particulier, la conjonction de certains facteurs, tels que la complexité, l'interconnexion, l'interdépendance de ces nouvelles fonctions, mais aussi l'urgence de la mise en œuvre et la valeur marchande des fonctions qu'elles offrent à l'entreprise, augmentent le risque pour ces fonctions de devenir la cible de cybercriminels. Dernier exemple en date : avec la mode des réseaux sociaux, les dernières générations de Botnets s'appuient désormais sur Twitter.
La professionnalisation des attaques a considérablement progressé : le niveau de technicité des codes malveillants, la multiplicité des aspects maitrisés et la coordination globale au niveau des attaques ne peuvent en effet qu'être le résultat d'une activité très structurée. Ceci a conduit à une évolution très forte dans le mode d'attaque.

Évolution radicale dans les motivations et les modes d'attaque

Avant 2005, les attaques étaient plutôt gratuites (sans but mercantile) :

- Prise de contrôle de machines pour y installer des serveurs d'échanges de données (serveurs Warez).
- Attaques entre « clans pirates » rivaux (guerres IRC, attaques DDOS).
- Démonstration de savoir-faire ou lancement de vers sans but précis sur Internet (CodeRed, Slammer, etc.).

En 2005 et 2006, les attaques sont clairement devenues motivées par le gain d'argent :

- Vol de données confidentielles (Cartes bleues, comptes bancaires) au travers de phishing ou de « keylogger ».
- Chantage à la destruction des données. L'attaque consiste à chiffrer les données de l'utilisateur et à demander une rançon en échange de la clé de déchiffrement.
- Chantage vers certains sites marchands (menaces d'attaques en DDOS).
- Attaques ciblées entre concurrents (espionnages industriels).

Et depuis 2007, la recherche des gains financiers s'est accentuée en s'appuyant sur des outils de plus en plus professionnels (cf. par exemple les techniques décrites au paragraphe précédent pour Storm Worm ou Conficker).
Les modes d'attaques évoluent à présent vers des attaques dirigées, rarement massives, souvent ciblées et en tout cas de plus en plus sophistiquées.
Par exemple les internautes se font désormais attaquer lorsqu'ils visitent des sites web anodins qui ont été eux-mêmes compromis et qui propagent, sans le savoir, ces attaques. On assiste aussi de la part des attaquants à l'utilisation systématique des vulnérabilités dans un déploiement rapide et sur une grande échelle, ce qui provoque des vagues d'attaques. Ainsi, les vagues d'attaques par « Injection SQL » vues début 2008 ont permis à des attaquants de déposer des codes malicieux silencieusement en quelques heures sur des milliers de sites web, permettant ensuite d'infecter les ordinateurs de victimes visitant ces sites.

Conclusions

Les attaquants semblent de plus en plus forts. Les techniques d'attaques, la vitesse des cycles de vie et l'action coordonnée ont progressé.
L'évolution des menaces nécessite que les entreprises renforcent l'efficacité de leurs moyens de protection.
Même si le niveau de défense dans les entreprises a progressé, en termes techniques grâce aux outils notamment, ou en terme organisationnel, cette protection requiert de leur part une réactivité plus importante et très rigoureuse.

Elles doivent désormais disposer d'un processus industrialisé d'application de correctifs qui doit intégrer :

- un système de veille de sécurité,
- la maîtrise du parc par une gestion des moyens exhaustive et à jour en permanence,
- une gestion de configuration des correctifs de sécurité maîtrisée,
- un processus de déploiement des correctifs rigoureux, tenant compte des aspects opérationnels et techniques de disponibilité, non régression, ... (voir l'encadré, page 3)

L'évolution de la menace a conduit le Cert-IST à adapter ses livrables aux besoins de l'entreprise et à fournir les informations adaptées aux processus de traitement des vulnérabilités. ■

Philippe.Bourgeois[à]cert-ist. com,
Thierry.Maronier[à]alcatel-lucent. fr

Mettre en place une politique d'application des correctifs

Yvon Klein
Directeur Technique du Cert-IST

David TRESGOTS
Chef de projet Cert-IST

L'activité de veille du Cert-IST produit deux types de publications :

- **Les avis de sécurité** : un avis de sécurité est publié pour **décrire une vulnérabilité** et son correctif associé. Le Cert-IST publie annuellement plus de 600 avis de sécurité, et suit plus de 750 produits. Le suivi des avis de sécurité permet aux organisations de maintenir à jour (en termes de correctifs de sécurité) leurs parcs informatiques.
- **Les alertes de sécurité** : une alerte est publiée pour **prévenir d'une menace** particulière. Cela se produit typiquement lorsqu'il y a un risque important qu'une vulnérabilité donnée (pour laquelle il existe par ailleurs un avis de sécurité) soit utilisée pour réaliser des attaques. Le Cert-IST publie annuellement une dizaine d'alertes. Le suivi des alertes de sécurité permet aux organisations de se protéger contre les attaques en cours.

La réception de ces deux types de publication déclenche au sein des organisations deux processus de traitement différents que nous examinons maintenant.

Gestion des avis de sécurité

Processus

Le tableau ci-contre décrit les étapes types du processus déclenché par l'arrivée d'un avis de sécurité.

■ *Qualification interne*

Cette phase a pour objectif de déterminer si l'avis reçu doit **déclencher un processus** de traitement au sein de l'organisation (ou bien s'il va être simplement écarté car considéré comme non applicable à l'organisation) et le **niveau de priorité** de ce traitement.
Le processus de qualification peut être plus ou moins élaboré. Il peut par exemple inclure des règles de fonctionnement telles que :

- prendre en compte uniquement les avis ayant un niveau de risque « Elevé » et « Très élevé » (les autres avis sont alors pris en compte à intervalle de temps régulier, par exemple mensuellement dans le processus de maintien opérationnel du S.I.) ;
- transmettre chaque avis à un expert du domaine technique pour une analyse détaillée de l'impact dans l'environnement concerné ;
- s'appuyer sur les outils d'inventaires pour déterminer les composants du S.I. impactés et s'appuyer sur la cartographie du S.I. pour identifier les systèmes critiques impactés ;
- etc.

■ *Diffusion*

A l'issue de la qualification, les avis de sécurité sont transmis aux entités qui ont à charge le maintien opérationnel des plates-formes, accompagné d'un niveau de priorité. Typiquement le niveau de priorité demandera :

- une prise en compte immédiate ;
- ou une prise en compte lors de la prochaine phase de maintenance ;
- ou ne demande pas de prise en compte explicite, auquel cas l'avis est envoyé au destinataire « pour information » plutôt que « pour action ».

Phases	Description
Qualification interne	Analyse de la vulnérabilité. Détermination des S.I. impactés.
Diffusion	Transmission des avis pour mise à niveau des S.I. impactés.
Mise à niveau des plates-formes	Les correctifs pour la vulnérabilité sont déployés sur les plates-formes impactées.
Suivi	Mesure de la prise en compte effective des avis diffusés.

Le destinataire acquitte la réception de l'avis puis transmet à intervalle régulier l'état de traitement de la demande, ce qui permet un suivi (cf. le paragraphe consacré au suivi ci-dessous).

■ *Mise à niveau des plates-formes*

La mise à niveau des plates-formes correspond généralement à un processus déjà existant dans l'entreprise. Mais il devra pouvoir être adapté aux besoins de réactivité et de suivi qu'exige le processus de gestion des avis de sécurité. Ce processus peut typiquement inclure les phases séquentielles suivantes :

- test : la modification à apporter aux configurations est en cours de test ;
- déploiement pilote : la modification a été appliquée sur des configurations pilotes ;
- déploiement généralisé : la modification a été qualifiée et est déployée sur l'ensemble des configurations concernées.

■ *Suivi*

Le suivi formel de la prise en compte des avis est généralement fait uniquement pour les avis ayant un niveau de priorité élevé. Dans ce cas, l'avancement est tracé en associant un statut à chaque avis suivi :

- **Rejeté** : l'entité destinataire a bien reçu l'avis mais estime que dans son contexte opérationnel la vulnérabilité n'est pas applicable ;
- **Planifié** : l'entité destinataire a prévu d'appliquer le correctif mais cette application est différée ;
- **En cours** : le processus de mise à niveau des plates-formes est en cours de réalisation. Cette mise à niveau suit typiquement les étapes identifiées au paragraphe précédent (test puis déploiement pilote et enfin déploiement généralisé) ;
- **Effectué** : le processus de mise à jour est terminé.

Le suivi donne un moyen au responsable sécurité :

- d'avoir un indicateur du niveau de sécurité des S.I. ;
- d'établir un tableau de bord sur le processus de déploiement des correctifs de sécurité et sur son efficacité :
  - nombre d'avis traités par an ;
  - délai moyen de prise en compte ;
  - nombre de rejets ;
  - etc.

Outillage du processus

Dans sa forme la plus simple, la mise en œuvre du processus présenté peut être réalisée avec les outils de bureautique simple : tableur pour le suivi et e-mail pour la diffusion. Cette solution n'est cependant applicable que si le nombre de composants du S.I. contrôlés et le nombre d'avis traités restent de tailles modestes. Sa simplicité de mise en œuvre constitue son atout majeur. Il est souvent une première étape avant une progression vers une solution plus industrielle.

Certaines organisations ont choisi pour implémenter ce processus de s'appuyer sur les outils déjà existants dans l'entreprise, tels que :

- les outils de « ticketing ». Les avis de sécurité à appliquer au sein de l'organisation sont alors transmis et suivis en créant des « tickets de traitement ». L'intérêt majeur est alors de disposer ainsi de toutes les facilités proposées par l'outil de « ticketing » pour suivre l'évolution du traitement des avis.
- les outils de travail collaboratif (type « LotusNotes », etc.). Il est en effet souvent facile dans ces environnements de décrire un processus de traitement et de suivre ensuite l'évolution de chaque avis.

Lorsque le nombre d'avis à traiter ou la taille du S.I. augmente, il peut alors être intéressant de recourir à un outillage plus spécifique tel que, par exemple :

- une base de données locale contenant les informations de suivi de chaque avis de sécurité ;
- un couplage des avis avec les outils d'inventaire du parc ;
- une aide à la mesure d'impact et à l'identification des priorités.

▸ Gestion des alertes de sécurité

Processus

Le tableau ci-dessous décrit les étapes types du processus déclenché par l'arrivée d'une alerte.

■ *Qualification interne*

Cette phase a pour objet d'analyser si la menace signalée par la cellule de veille s'applique au contexte de l'organisation. Typiquement cette analyse inclut les éléments suivants :

- Le produit menacé existe-t-il dans l'organisation ?
- Existe-t-il des mécanismes de protection propres à l'organisation (ou plus généralement une politique de sécurité) qui rend la menace caduque ? Par exemple, si certains types d'attachements e-mails sont interdits dans l'entreprise, une attaque basée sur ces attachements n'induit pas de menace réelle dans l'organisation.
- Quels sont les composants du S.I. de l'organisation qui sont exposés à cette menace ? Quelle est l'importance (en nombre ou en criticité) de ces composants du S.I. ?

■ *Création d'une cellule de traitement*

Si la phase de qualification confirme que l'organisation est exposée à une menace significative alors un incident est ouvert, et une procédure de traitement de l'incident est engagée, pouvant conduire par exemple à la mise en place d'une cellule de traitement de cette menace. L'objectif de cette procédure est d'établir un plan d'action permettant de :

- diminuer le degré d'exposition à la menace (mise en place de mesures particulières de protection et suivi de ces mesures) ;
- détecter les attaques qui touchent effectivement l'organisation.

Suivant le contexte opérationnel, la mise en place de mesures de protection ponctuelles (par exemple le blocage d'un port réseau) peut nécessiter un processus plus ou moins strict. Ce processus inclut d'une part la chaîne de décision (qui a autorité pour décider de la mise en place de cette mesure ? quel est le circuit de validation de cette demande ?) mais également des aspects techniques (quel est le processus de qualification de la mesure technique ?). Dans les environnements ayant un fort besoin de disponibilité, la mise en place de telles mesures nécessite généralement une description formelle de :

- l'impact induit sur le service nominal,
- la procédure de déploiement, de surveillance et de retrait de la mesure technique.

■ *Suivi*

Cette dernière phase a pour objectif la surveillance de l'infrastructure IT pendant la période critique (période pendant laquelle la menace existe). Elle se termine lorsqu'une mesure de protection définitive a été déployée (typiquement un correctif de sécu-

Phases	Description
Qualification interne	Analyse de l'exposition. Détermination des SI impactés.
Création d'une cellule de traitement	Assignation à un responsable « incident». Définition d'un plan de protection et de détection. Qualification et déploiement du plan d'action.
Suivi	Suivi de l'évolution de la menace. Retrait du plan de protection.

rité) sur l'ensemble des composants du S.I. concernés au sein de l'organisation.

De façon générale, les outils les plus couramment employés pour détecter l'évolution de la menace au sein de l'organisation sont les IDS ou IPS réseaux. En effet ces outils permettent de surveiller des points stratégiques du S.I. pour voir si des tentatives d'attaques y transitent. Mais de nombreuses autres approches sont également possibles, comme par exemple :

- placer des machines pot-de-miel et observer les tentatives d'accès qu'elles subissent ;
- analyser certains journaux systèmes (par exemple les journaux http des proxys web ou les journaux des services DNS) pour voir si des machines internes ont un comportement anormal (cas où une machine infectée cherche à contacter un « bot-master » sur Internet par exemple) ;
- ou même utiliser un scanner des vulnérabilités afin de mesurer à intervalle régulier la vulnérabilité de son S.I. et suivre ainsi le déploiement effectif des correctifs.

Outillage du processus

En général, l'ensemble du processus de gestion des alertes est pris en charge par la structure « sécurité » de l'organisation. Il s'agit donc d'un processus interne (par opposition au processus de gestion des avis qui implique, lui, plus d'acteurs hors de la structure sécurité). Le besoin d'outillage « process » est donc ici moins important.

La plupart du temps, l'alerte est traitée avec le même type d'outils « process » que ceux utilisés pour les incidents. Il s'agit le plus souvent d'un espace partagé accessible à l'ensemble des intervenants appartenant à la cellule de traitement.

Même si ce n'est pas aujourd'hui systématiquement fait, le Cert-IST recommande qu'une trace formelle de chaque « incident » soit conservée afin de permettre un suivi et une analyse de cette activité :

- nombre d'incidents traités par mois,
- durée de traitement
- etc.

Conclusion

Depuis plus de 10 ans le Cert-IST offre à ses membres un service de veille et d'alerte sur les menaces et les vulnérabilités, s'appuyant sur les principes de mutualisation et de coopération entre les membres pour pouvoir adapter ses fournitures aux besoins des entreprises.

La menace a évolué et elle est devenue plus ciblée et plus rapide, ce qui nécessite de la part de l'entreprise une mise en œuvre très rigoureuse de son processus de veille, d'alerte et de maintien en sécurité de son système d'information.

Les vulnérabilités sont de plus en plus nombreuses, et concernent l'ensemble des composants du S.I. L'entreprise doit donc être en mesure d'appliquer les correctifs de sécurité avec une très grande réactivité.

Pour protéger au mieux son système d'information, le principe d'application systématique et immédiate des correctifs à la totalité de son S.I. n'est plus viable.

Dans son rapport de 2008, « Protection de l'information : Enjeux, gouvernance et bonnes pratiques » le CIGREF indique :

« Il est nécessaire d'avoir une démarche consciente et explicite d'évaluation et de traitement des risques. Il faut ensuite inscrire cette démarche dans une politique de protection de l'information. Aujourd'hui c'est l'expression de besoin qui est difficile : que protéger et à quel niveau ?

Une démarche pragmatique, et progressive de cartographie des risques est un pré requis à la fois à une démarche de gestion des risques mais aussi à une démarche performante de protection de l'information. »

Il est donc nécessaire, comme le recommande le CIGREF, de réaliser une cartographie des risques sur l'information, celle-ci permettant ensuite d'établir une cartographie des risques sur le système d'information. C'est à partir de cette cartographie, qui permet d'identifier les systèmes critiques, que seront construites les procédures d'application des correctifs et des mesures de protection ponctuelles particulières pour certaines menaces.

Ces procédures seront alimentées par le système de veille et d'alerte qui permet d'identifier les menaces et les vulnérabilités sur les systèmes critiques. Ces procédures seront complétées par des procédures de suivi et de mesure du déploiement des correctifs.

Afin de suivre les menaces et les attaques avec toute la réactivité nécessaire le Cert-IST a fait évoluer ses méthodes et ses productions pour répondre aux nouveaux objectifs et aux besoins de l'entreprise qui souhaite mettre en place un processus de traitement des vulnérabilités.

L'objectif de ce dossier était de mettre en évidence les éléments clés de la protection du Système d'Information et de proposer des solutions concrètes, comme par exemple des éléments de procédures types.

Aujourd'hui, on ne peut pas envisager qu'une entreprise responsable exploite des systèmes critiques sans avoir mis en place un système de maintien en sécurité de son S.I s'appuyant sur une veille appropriée. ■

directeur-technique[à]cert-ist. com,
david.tresgots[à]cert-ist. com

Bibliographie

NIST: SP800-40 « Creating a Patch and Vulnerability Management Program »
http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf

SANS: "Security Essentials: Patch Management as a Necessary Part of Defence In Depth, A Case Study" par Kay A. Cornwell
http://www.giac.org/practical/GSAE/Kay_Cornwell.pdf

CIGREF 2007- Analyse et gestion des risques dans les grandes entreprises
http://cigref.typepad.fr/cigref_publications/RapportsContainer/Parus2007/gestion_des_risques/Analyse_et_gestion_des_risques_dans_les_grandes_entreprises_-_impacts_pour_la_DSI-rapport_2007_web.pdf

CIGREF 2008 - Protection de l'information : Enjeux, gouvernance et bonnes pratiques
http://cigref.typepad.fr/cigref_publications/2008/10/2008---protecti.html

Cert-IST : Bilan 2005
http://www.cert-ist.com/documents/Document_Cert-IST_000202.pdf

Cert-IST : Bilan 2006
http://www.cert-ist.com/documents/Document_Cert-IST_000230.pdf

Cert-IST : Bilan 2007
http://www.cert-ist.com/documents/Document_Cert-IST_000272.pdf

Cert-IST : Bilan 2008
http://www.cert-ist.com/documents/Document_Cert-IST_000312.pdf

SÉCURITÉ DE L'INFORMATION
Sujets traités : tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité : 4 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :
Joseph Illand
Fonctionnaire de Sécurité de Défense
Centre national de la recherche scientifique
3, rue Michel-Ange, 75794 Paris cedex 16
Tél. : 01 44 96 41 88
Courriel : joseph.illand[à]cnrs-dir. fr
http://www.sg.cnrs.fr/fsd

Rédacteur en chef :
Robert Longeon
Chargé de mission SSI du CNRS
Courriel : robert.longeon[à]cnrs-dir. fr

Impression : Bialec, Nancy (France) - D.L. n° 72633
ISSN 1257-8819