Gestion des Correctifs / Patch Management

Olivier Caleff

APOGEE Communications
olivier.caleff@apogee-com.fr

1 Introduction

À la suite de chaque vague d'attaque massive ou de propagation de vers qui infectent les postes de travail, on recherche des coupables : parfois ce sont des sociétés ou des individus, véritables chasseurs de vulnérabilités, qui ont révélé l'existence de failles, parfois ce sont les éditeurs qui ont mis du temps à publier les correctifs, souvent ce sont les entreprises ou les utilisateurs qui n'ont pas fait l'effort d'installer ces fameux correctifs. On notera surtout que dans la quasi-totalité des grandes vagues d'attaques médiatisées qui se sont produites ces dernières années, les correctifs étaient disponibles depuis au moins plusieurs semaines.

Il s'agit donc d'étudier le contexte dans lequel des correctifs peuvent et doivent être appliqués puis de formaliser cela afin de mettre en évidence les phases amont et aval afin d'être le plus efficace possible.

2 Contexte

Plusieurs milliers de vulnérabilités sont découvertes chaque année. Elles affectent la quasi-totalité des composants logiciels ou matériels du monde informatiques, des micro-codes et systèmes d'exploitation, aux progiciels et applications. Cela représente plus d'une centaine d'annonce de découvertes de vulnérabilités par mois et elles comportent généralement deux parties : la présentation de la vulnérabilité et une façon de s'en prémunir.

La présentation de la vulnérabilité détaille toujours de façon très précise les cibles vulnérables, avec le détail des versions vulnérables. Les conditions d'exploitation sont parfois indiquées mais généralement pas les détails permettant le développement d'un code d'exploitation spécifique. Si ce dernier existe déjà cela est indiqué et, avec les conséquences ou les impacts potentiels, cela fait partie des facteurs contribuant à la définition du niveau de gravité de la vulnérabilité.

Lorsque des éditeurs ou des constructeurs sont à l'origine des annonces de vulnérabilités, les correctifs ou le moyen d'y accéder sont indiqués. Dans le cas contraire, la date prévisible de disponibilité est indiquée ainsi que les méthodes de contournement.

La gestion des correctifs peut être abordée sous plusieurs angles d'analyse car 4 types de population sont concernés par cette problématique :

- celle des Internautes non sensibilisés aux problématiques de la sécurité, ne disposant même pas forcément d'anti-virus sur leur poste de travail et encore moins d'outils de protection. Il s'agit d'Internautes qui ne sont tout simplement pas informés des avis de vulnérabilités et de la disponibilité de correctifs ;
- celle des Internautes qui sont informés des questions de sécurité, suivent les avis de vulnérabilité et appliquent les correctifs ;
- celle des entreprises sans organisation informatique ou sécurité dédiée ;
- celle des grandes entreprises avec de nombreux systèmes informatiques et réseaux et une structure prenant en compte les problématiques de la sécurité.

Il existe au moins 2 types de correctifs : les correctifs systèmes qui résolvent des problèmes fonctionnels et les correctifs de sécurité.

Les correctifs de sécurité sont des modules logiciels qui corrigent des vulnérabilités ou viennent combler des failles de sécurité dont l'exploitation auraient des effets néfastes sur le bon fonctionnement, la disponibilité ou l'intégrité des systèmes informatiques, des applications ou même des données qu'elles gèrent.

La publication des correctifs par les éditeurs a pour objectif d'informer les utilisateurs et les administrateurs des systèmes concernés et vulnérables afin de réduire les risques de compromission.

Il existe aussi des vulnérabilités qui ne sont pas encore connues des éditeurs et qui font l'objet d'exploitation par des personnes malveillantes tant qu'elles ne sont pas détectées ou publiées.

Le niveau de risque peut être défini par une formule mathématique :

$$(\text{niveau de risque}) = \frac{(\text{impacts potentiels}) \times (\text{probabilite d'occurrence})}{(protectionoperationnelle)}$$

Le niveau de risque sera donc proportionnel aux conséquences liées à l'exploitation de la vulnérabilité, à la probabilité d'occurrence de l'exploitation de cette vulnérabilité. Bien que cette probabilité soit accrue par la diffusion de l'information, cette divulgation est nécessaire afin de pouvoir au mieux estimer les cibles vulnérables et la nature des risques. L'éditeur ou le constructeur doit donc être suffisamment explicite pour que le lecteur des avis de vulnérabilité puisse identifier rapidement si ses plates-formes sont ou non vulnérables... sans toutefois trop en dire afin de ne pas faciliter le travail de ceux qui seraient tentés de développer des outils d'exploitation.

En revanche, toute mise en place d'un mécanisme opérationnel de protection aura pour effet de diminuer le niveau de risque. Il en est ainsi de l'application des correctifs... Le facteur temps est aussi important : plus vite les correctifs sont mis en œuvre et protègent les plates-formes vulnérables, moins elles seront perturbées par des attaques visant à exploiter ces mêmes vulnérabilités.

Pour simplifier, les éditeurs et organismes officiels traitant de la sécurité (comme les " CERT " ou " CSIRT "), définissent trois ou quatre niveaux de gravité avec un niveau de prise en compte associé :

1. **Critique**.- Il est impératif de prendre des mesures appropriées au plus vite, pour supprimer la cause de la vulnérabilité ou tout au moins pour réduire

le niveau de risque, sans hésiter à déclencher des procédures d'interventions exceptionnelles. L'exploitation de la vulnérabilité pourrait avoir des conséquences aussi grave que la compromission totale du système ou la propagation automatique d'une charge virale ou maligne sans intervention de l'utilisateur.

2. **Élevé**.- Il est fortement recommandé de prendre des mesures appropriées dans un délai " court " mais de sans toutefois revêtir un caractère d'urgence, et sans nécessiter la mise en place de procédures exceptionnelles. L'exploitation de la vulnérabilité pourrait avoir des conséquences telles que la compromission de la confidentialité ou de l'intégrité des données de la plate-forme visée ou même perturber la qualité de service offerte et la disponibilité.
3. **Moyen**.- Les opérations de correction et de réduction des risques doivent être planifiées dans le cadre des opérations classiques et périodiques de remise à niveau, l'utilisation d'une plate-forme vulnérable n'étant pas rédhibitoire dans le cadre de l'activité. L'exploitation de la vulnérabilité n'aurait pas d'impact majeur sur le bon fonctionnement ou la cohérence globale de la plate-forme.
4. **Faible**.- Les opérations de correction et de réduction des risques pourront être reportées jusqu'à la prochaine campagne de mise à jour, les risques d'exploitation ou les impacts potentiels étant faibles. L'exploitation de la vulnérabilité est soit très complexe et requiert la combinaison de plusieurs facteurs ayant une faible probabilité d'occurrence.

Dans le contexte d'exploitation des plates-formes et en fonction des niveaux de gravité, il convient alors de déterminer s'il faut ou non appliquer les correctifs, et dans quel cadre, car cela ne se résume pas en la simple exécution d'un " *setup.exe* ", d'un " *update.pl* " ou d'un " *apt-get* " fournis par des éditeurs !

Le critère temps est de nouveau à prendre en compte :

1. Décaler dans le temps l'application de correctifs revient à voir s'accroître le niveau global d'insécurité et les conséquences en cas d'attaque, même interne, se mesurent vite en perte de productivité liée à des dysfonctionnements. Les correctifs – techniques, fonctionnels ou de sécurité – font partie du quotidien de l'informatique, et les intégrer dans les procédures d'exploitation et d'administration. Les conséquences financières directes liées à une panne ou à un virus sont loin d'être négligeables comme ont pu le constater au cours de l'été 2003 certaines entreprises.
2. Avant même cela, être averti au plus tôt est primordial. Il faut ainsi travailler en amont afin de pouvoir prendre les bonnes décisions et déclencher les procédures.

3 Gestion des correctifs

3.1 La phase amont

En amont, plusieurs procédures doivent donc être mises en place :

1. le suivi des annonces et des mises à disponibilité de ces correctifs,
2. l'identification des correctifs nécessaires dans le contexte de l'entreprise,
3. la mise en œuvre d'un environnement de test ou de pré-production permettant de faire une installation " *à blanc* " pour les vérifications de dépendances entre les différents environnements, les tests de non-régression et de retour arrière afin de déterminer s'il n'y a pas d'effets de bord, la vérification de l'efficacité des correctifs,
4. le suivi du parc informatique afin de déterminer toutes les plates-formes susceptibles d'être concernées,
5. l'estimation et l'analyse des risques et des impacts en cas de non-application des correctifs,
6. Le circuit de décision.

La veille sécurité La veille sécurité, qu'elle soit réalisée interne ou qu'elle soit externalisée auprès des sociétés spécialisées depuis de nombreuses années, est donc primordiale.

On se rend aussi vite compte que le périmètre de cette veille doit être bien défini au départ, faute de quoi on sera vite submergé par le flot d'information.

Dans un premier temps le veilleur souhaitant être autonome pourra se contenter des sites officiels et de ceux des éditeurs. Il se rendra cependant vite compte qu'il n'aura qu'une vision partielle des vulnérabilités découvertes.

Cette veille devra être régulière et même quotidienne, car il n'y a a priori pas de lien entre les découvertes de vulnérabilités et les périodes de l'année. Un seul éditeur se distingue pour le moment dans sa politique de diffusion : Microsoft a maintenant décidé de publier ses avis de vulnérabilités tous les deuxièmes mardi de chaque mois et non plus au fil des découvertes ou des disponibilités de correctifs. En revanche, certaines mises à jour d'avis et de correctifs continuent à être diffusés dès leur disponibilité.

Un premier élément d'organisation apparaît donc : la planification de mises à jour à certaines périodes du mois avec un premier éditeur.

L'identification des plates-formes concernées Une fois l'information disponible, il s'agit de déterminer son niveau de pertinence dans son propre contexte opérationnel. Le contenu de certains avis étant parfois d'une lecture complexe, cette étape est plus complexe qu'on ne le croit. Il faut en effet connaître les éventuels liens et imbrications des systèmes et des logiciels entre eux, et avoir une vision précise de tous les composants matériels et logiciels de l'environnement.

Une bonne connaissance de son parc informatique et un inventaire matériel et logiciel à jour permettra donc d'être plus efficace et d'extraire plus rapidement les plates-formes concernées.

Un élément vient cependant modifier l'exactitude des informations de l'inventaire : on assiste à l'inclusion de plus en plus fréquente de module de type

"run-time" ou de moteurs applicatifs " *embarqués* " dans des composants logiciels standards. Cela a été particulièrement mis en lumière lors de l'épisode du vers SQLSlammer fin janvier 2004 avec des run-time SQL Server, mais des versions minimalistes du serveur Web Apache se retrouvent aussi dans plusieurs logiciels ou serveurs applicatifs du commerce.

Il convient alors de mener une analyse de risque et de définir des priorités dans les plates-formes en fonction de différents critères objectifs tels que leur niveau de criticité ou leur emplacement dans l'architecture ou les chaînes de production de l'entreprise. On pourra alors dédier du planning et de l'allocation optimale de ses ressources lorsqu'une grande campagne d'application de correctifs sera nécessaire.

Les tests Il est alors temps d'aller rechercher les correctifs, d'en vérifier l'authenticité et l'intégrité, mais aussi de vérifier tous les pré-requis, tant en terme de plates-formes matérielles que logicielles, de système d'exploitation et de correctifs, mais aussi d'applicatifs ou de modules ou librairies.

Une fois le correctif obtenu et son intégrité vérifiée, il doit être validé techniquement avec plusieurs objectifs :

1. *vérification de son efficacité* : suppression ou contournement de la vulnérabilité qu'il adresse et analyse de la " *signature* " de la plate-forme mise à jour lorsqu'elle est testée par des outils de tests de vulnérabilités ;
2. *vérification de sa complétude* : réalisation des fonctions attendues sans besoin annexes, qu'il s'agisse de modules complémentaires ou de privilèges nécessaires à son installation ;
3. *vérification de son indépendance* : vérification de l'absence d'effets de bords ou de dysfonctionnement dans les autres modules logiciels ou applications mais aussi vérification du non-écrasement de configurations ou de paramétrages spécifiques liés à l'environnement de l'utilisateur ou de l'entreprise ;
4. *vérification de son autonomie* : vérification que la suppression du correctif laisse intègre l'environnement sur lequel il a été installé et qu'il permet de faire un retour arrière en cas de découverte de nouveaux dysfonctionnements *a posteriori*... comme cela se produit parfois.

Bien entendu, ces validations et vérifications doivent être effectuées dans un environnement similaire à ceux de production, mais décorrélé, afin de tester au plus près du réel sans risque de débordement incontrôlé. Dans le cas contraire d'un dysfonctionnement, la résolution de tout nouveau problème risque justement de devenir très problématique.

La documentation des opérations réalisées est impérative. Il faut en effet tracer toutes les opérations réaliser et les journaliser. Parfois, l'application d'un correctif est conditionnée à ce que d'autres correctifs antérieurs soient eux-mêmes installés, d'où l'importance de l'ordre dans lequel ils sont installés et la nécessité de tenir à jour un historique des opérations réalisées en complément de l'inventaire du parc logiciel. Il arrive parfois que l'on arrive à des situations de type

“ *Catch-22* ” ou “ *de la poule et de l'œuf* ” et l'appel au support technique de l'éditeur est alors nécessaire avec la fourniture du maximum de détails.

On pourra alors faire une dernière opération d'installation et de désinstallation, la valider et rédiger les procédures pour les personnes ayant en charge le déploiement. L'utilisation de logiciels de télé-distribution plus ou moins automatisés ne change en rien le principe de vérification.

Le site pilote optionnel Lorsque le temps et le contexte le permettent, un premier déploiement sur un site ou un environnement pilote peut être réalisé afin de mesurer les effets réels de l'application des correctifs sur des plates-formes opérationnelles.

L'analyse des risques et l'estimation des coûts La dernière étape avant la décision consiste à analyser les risques couverts et les risques résiduels, puis à estimer les coûts induits. Il s'agit à ce titre d'évaluer :

1. les coûts induits par le déploiement des correctifs, qu'il se passe de façon manuelle ou automatique, en heures ouvrables ou non,
2. les coûts induits par le non-déploiement des correctifs, en intégrant la mise en place de parades ou de solutions de contournement,
3. les coûts induits par une indisponibilité des plates-formes vulnérables en cas d'arrêt causé par l'exploitation de la vulnérabilité,
4. les coûts estimés en cas d'exploitation de la vulnérabilité concernée,
5. les coûts et impacts potentiels en cas de non-respect d'une directive métier ou d'une législation causés par la non-application du correctif.

Les principaux éléments constitutifs d'un dossier d'aide à la prise de décision sont alors réunis.

La prise de décision La prise de décision intervient lors d'une réunion de type “ *go/no-go* ” qui regroupe tous les décideurs, qu'ils soient informatiques ou métiers. Ce circuit peut être allégé et devenir purement formel lorsque les impacts sont maîtrisés ou que les actions à valider entre dans un cadre standard et déjà défini préalablement.

3.2 La mise en œuvre

Une fois les correctifs validés et la décision prise, le déploiement peut alors commencer, dans le respect des procédures existantes et des contraintes d'exploitation.

Plusieurs cas se présentent de nouveau :

1. le déploiement maîtrisé par l'entreprise avec des outils de télé-distribution qui envoient des paquetages logiciels aux plates-forme dans les conditions et contextes définis et planifiés par les responsables du déploiement,

2. le déploiement semi-maîtrisé par l'entreprise avec les plates-formes cibles qui viennent chercher leurs paquetages logiciels de façon asynchrone et indépendante, lors de l'allumage ou de la première connexion sur un serveur par exemple, ou tous les Lundi matin par exemple,
3. le déploiement non maîtrisé par l'entreprise avec les plates-formes qui vont chercher les correctifs lorsque l'utilisateur y pense (sic), valide la question qui lui est posé par sa plate-forme logicielle ou lance une application de vérification globale et de mise à jour.

Si les outils de télé-distribution ou de diffusion peuvent se révéler d'une grande efficacité, il faut aussi penser aux systèmes nomades des utilisateurs qui sont souvent à l'extérieur de l'entreprise mais qui communiquent souvent avec elle : il s'agit des postes nomades de type PC portables qui ne se connectent que de façon épisodique aux réseaux de l'entreprise, se raccordent sur des réseaux partenaires...

Même s'il existe des solutions techniques permettant la réalisation de l'opération d'application des correctifs, il faut donc vérifier que tout le parc est couvert et détecter ceux qui réussissent à passer entre les mailles du filet.

Outre les conséquences liées aux pertes de données dues à des vols ou à des destructions, une nouvelle problématique est apparue de façon particulièrement aiguë lors de l'été 2003 : la contamination de réseaux interne d'entreprises par la faute de PC nomades reconnectés : mal protégés et infectés en dehors du périmètre de l'entreprise lors de connexions directes à l'Internet, ils étaient porteurs de charges malignes qui se sont déclenchées une fois sur le réseau local. De nombreux mécanismes de protections d'infrastructure ont ainsi été contournés avec des conséquences parfois dramatiques.

3.3 La phase de suivi

En aval aussi, plusieurs procédures doivent être mises en place :

1. le suivi immédiat après applications pour lever les doutes au plus vite en cas d'apparition de dysfonctionnements,
2. le suivi des mises à jour pour les correctifs afin de pouvoir retirer ou redéployer les correctifs imparfaits déjà déployés,
3. la mise à jour de l'inventaire du parc informatique,
4. la communication des résultats obtenus auprès de la Direction Informatique et des responsables internes de la Sécurité.

Le suivi du déploiement Le déploiement doit être suivi pour des raisons habituelles de gestion de projets, mais aussi pour des raisons plus spécifiques :

1. il faut déterminer l'avancement dans le temps afin de mesure la couverture des plates-formes vulnérables et déterminer les environnements résiduels,
2. il faut détecter les éventuels dysfonctionnements, les qualifier et s'ils sont bloquants, envisager de faire un retour arrière et d'interrompre le déploiement,

3. il faut déterminer les éventuels effets de bord non détectés préalablement ou les vulnérabilités résiduelles non corrigées.

En cas de dysfonctionnement réel, la phase de levée de doute doit être lancée au plus vite.

Le suivi des mises à jour des correctifs Dans certains cas, des correctifs insuffisamment testés ou avec des effets de bords à retardement ont été observés. Les éditeurs ont alors du les retirer de la circulation ou diffuser des additifs. De même certaines listes de diffusions sur Internet se sont spécialisées dans le suivi des correctifs et dans le " *patch management* ". Il s'agit de sources d'informations particulièrement précieuses dans la mesure où l'on ne fait pas partie des premières entreprises à appliquer les correctifs.

Dans le cas de plates-formes fonctionnant sous un système d'exploitation francisé, un délai peut aussi apparaître quant à la date de disponibilité des correctifs.

La mise à jour de l'inventaire du parc Il s'agit d'une procédure qui peut souvent être automatisée et qui vise à disposer d'informations pertinentes lors de la prochaine campagne d'installation de correctifs.

La communication auprès des Directions Il s'agit d'intégrer la gestion des correctifs dans les tableaux de bords et dans le suivi global de l'informatique et de la sécurité. Les deux principales Directions concernées sont donc :

1. la Direction Informatique, pour la mesure du suivi et du niveau du parc,
2. la Direction Sécurité ou des Risques Opérationnels, pour la mesure du niveau de sécurité et la mise à jour des analyses de risques. i

Les responsables sécurité locaux ou les correspondants sécurité doivent aussi être avertis des campagnes de déploiement et des résultats, dont le pourcentage de couverture.

4 Éléments complémentaires ou spécifiques

4.1 Le facteur temps

Une fois qu'une vulnérabilité a été annoncée, de véritables courses contre la montre vont débuter :

1. qui du correctif ou du code d'exploitation sera publié le premier ?
2. qui des configurations et des paramètres à implémenter sur les outils de détection d'intrusion ou du code d'exploitation sera réalisé le premier ?
3. qui de l'application du correctif ou de la diffusion du code d'exploitation sera réalisée le premier ?

Depuis l'an 2000, de nombreux cas qui ont fait la une de l'actualité virale sont venus rappeler que les correctifs étaient publiés bien avant que les codes d'exploitations ne soient diffusés.

La réactivité des éditeurs et constructeurs est primordiale lorsqu'une vulnérabilité est dévoilée par un circuit non officiel.

La réactivité des entreprises, des utilisateurs et des responsables sécurité est primordiale lorsque administrateurs les correctifs sont diffusés officiellement par les éditeurs et les constructeurs. Les outils de déploiement de correctifs permettent alors de gagner un temps précieux.

L'organisation des entreprises est un facteur déterminant lorsque des éditeurs publient des découvertes de vulnérabilités et des correctifs à date fixe.

4.2 Les systèmes qui ne peuvent pas être pris en compte

Certaines plates-formes informatiques ont pour vocation le pilotage de processus industriels ou constituent le support technique d'applications métiers.

L'élément déterminant est alors le logiciel ou le matériel ainsi que le centre de pilotage. Les plates-formes ne sont alors plus gérées par les services informatiques ou tout du moins, ils ne maîtrisent pas leurs évolutions, car il s'agit plutôt de systèmes de type " *clé en main* ".

La connaissance de vulnérabilités affectant les composants systèmes, applicatifs ou même des couches logicielles fondamentales comme des vulnérabilités affectant la pile TCP/IP, doivent amener à une forte vigilance. L'application de correctifs n'est pas toujours possible, soit pour des raisons techniques soit pour des raisons contractuelles. Il faut alors faire cohabiter des plates-formes vulnérables et susceptibles d'être infectées ou compromises au sein d'un environnement que l'on s'applique à maîtriser.

Une difficulté supplémentaire vient s'ajouter lorsque ces plates-formes industrielles pilotent des processus vitaux pour la production de l'entreprise.

Il faut alors travailler au niveau des architectures réseaux et applicatives de façon à isoler autant que possible les environnements vulnérables de production tout en continuant à assurer les besoins de communication opérationnels et les suivis métiers.

5 Conclusion

Une organisation spécifique doit donc être mise en place et il s'agit finalement d'une chaîne complète de procédures qui doit être mise en place : l'information en amont, sa qualification, son applicabilité, les tests, l'application puis la vérification et le suivi. Cette organisation impose la mobilisation de ressources.

Il sera nécessaire de sensibiliser et de convaincre le management de l'entreprise du bien fondé de la mise en place d'une gestion des correctifs.

Une rapide étude du marché montre que le nombre de logiciels de " *patch management* " augmente en ce moment. Ils ne disposent cependant pas tous des fonctionnalités suffisantes pour s'intégrer dans les processus informatiques des

entreprises. Le " *patch management* " est toujours en phase de maturation mais devrait atteindre un niveau égal et satisfaisant pour les différents environnements phares de l'informatique répartie actuelle :

1. Microsoft Windows avec les produits initiaux qui montent en puissance, d'origine Microsoft ou tierce.
2. Unix avec des outils constructeurs ou d'éditeurs tiers rodés depuis plusieurs années.
3. Linux avec des outils parfois totalement intégrés dans le système d'exploitation mais qui peuvent être complétés par des outils tiers permettant d'avoir une vision homogène lorsque plusieurs environnement cohabitent au sein d'une entreprise.

Références

1. NIST (National institute of Standards and Technology) : Special Publication 800-40 - " *Procedures for Handling Security Patches - Recommendations of the National Institute of Standards and Technology* ", `http://csrc.nist.gov/publications/nistpubs/800-40/sp800-40.pdf`
2. GAO (United States General Accounting Office) : GAO-03-1138T - " *Effective Patch Management is Critical to Mitigating Software Vulnerabilities* ", `http://www.gao.gov/new.items/d031138t.pdf`
3. Kay A. Cornwell, (SysAdmin, Audit, Network, Security Institute) : " *Security Essentials : Patch Management as a Necessary Part of Defense In Depth, A Case Study* " , `http://www.giac.org/practical/GSAE/Kay_Cornwell.pdf`