SYMPOSIUM SSTIC 2-4 juin 2004 à Rennes
SUR LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION ET DES COMMUNICATIONS

- Gestion des Correctifs
- Patch Management -

Olivier CALEFF
olivier.caleff (at) apogee-com.fr - olivier.caleff (at) devoteam.com

APOGEE Communications - DEVOTEAM
Tél : +33.1.69.85.78.00
http://www.apogee-com.fr - http://www.devoteam.com

Agenda

- 1 – Contexte
  - Vulnérabilités, correctifs, niveaux de risques, le facteur temps, populations cibles
- 2 – En **amont** de la gestion des correctifs
  - L'organisation, la veille, l'identification, les tests, les éléments de prise de décision
- 3 – La **mise en œuvre** des correctifs
  - L'organisation, les principes et conditions de déploiement, les impacts
- 4 – En **aval** de la gestion des correctifs
  - Les suivis, la gestion de parc, la communication
- 5 – Éléments **complémentaires**
  - Le facteur temps, la gestion des exceptions, les outils
- 6 – Conclusions
- 7 – Bibliographie

1 – Contexte

- Comment s'appelle une fonctionnalité non prévue par les développeurs ?
  - Un bogue ou un *bug*
- Comment s'appelle une personne qui découvre un bug ?
  - Un chasseur de bug, un hacker, une personne mal-intentionnée, … un utilisateur
- Et si cette personne le fait savoir ?
  - On la remercie pour avoir prévenu du bug
  - On l'accuse de tous les maux si le bug est exploité de façon malveillante
- Comment s'appelle un programme qui corrige un bug
  - PTF, *fix*, *enhancement*, patch, correctif
- Les bugs existent depuis les débuts de l'informatique
  - Idem pour les patchs !

Un peu d'histoire : IBM et la gestion des correctifs

- Mainframes IBM
  - APAR : *Authorized Program Analysis Report*
    - "*a method of reporting a code problem or error to IBM, a tracking number for a possible problem*", avec des Codes
      - CAN Cancelled APAR
      - DOC Documentation error
      - PER Programming error
      - RET Returned to the user for more documentation
      - SUG Suggestion
      - USE User error
      - FIN Fixed if next release
  - PTF : *Program Temporary Fix*
    - "*provides corrective service or enhancements to a function, the actual code change that fixes the problem*"
  - Publication régulière et périodique des PTF et APAR
    - Une fois installé, un PTF reste …
      - Jusqu'à ce que le code fasse l'objet d'un APAR puis d'un nouveau PTF qui corrige le premier PTF … puis d'un autre …
      - … jusqu'à la prochaine version du logiciel/driver/noyau

Les "bugs" d'aujourd'hui

- Affectent un parc important de machines
  - Cible privilégiée (mais non exclusive) : Windows
  - Niveau moyen de protection des postes en entreprise : moyen à élevé
  - Niveau moyen de protection des postes personnels : nul à moyen, parfois élevé
  - Rapidité de mise à jour des correctifs : de nulle à élevée

- Synthèse
  - La plupart des postes personnels sur Internet est vulnérable bien après que les correctifs soient disponibles

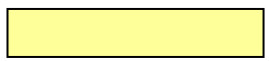
- Remarques
  - Toute vague d'attaque massive ou de propagation de vers qui infectent les postes de travail sera efficace sur Internet
  - Tout poste infecté pourra devenir un vecteur de propagation ou d'attaque

Description d'une vulnérabilité

- Avis typique
  - Niveau de gravité
  - Présentation de la vulnérabilité
  - Cibles vulnérables et versions impactées
  - Impact potentiels
  - Méthode de prévention et de protection
  - Correctifs
  - Historique
- En option
  - Conditions d'exploitation
  - Existence de code d'exploitation

- Bonne pratique
  - Lire les avis de vulnérabilités
  - Mieux : les comprendre
  - Encore mieux : mesurer la portée réelle

Qualification des niveaux de gravité

- Critique / Critical 
  - Mesures appropriées au plus vite impératives
    - Procédures d'interventions exceptionnelles
  - Exploitation de la vulnérabilité : conséquences grave
    - Compromission totale du système, propagation automatique d'une charge
- Élevé / High 
  - Mesures appropriées dans un délai "court", sans revêtir un caractère d'urgence
  - Exploitation de la vulnérabilité : conséquences importantes
    - Atteinte à la confidentialité, intégrité des données, qualité de service offerte
- Moyen / Moderate 
  - Opérations de correction et de réduction des risques à planifier
    - Opérations classiques et périodiques de remise à niveau
  - Exploitation de la vulnérabilité : pas d'impact majeur
- Faible / Low 
  - Opérations à réaliser lors de la prochaine campagne de mise à jour
  - Exploitation de la vulnérabilité : très complexe, faible probabilité d'occurrence

- niveau de risque = impact x probabilité / protection

Conséquences d'un "bug" ou d'une vulnérabilité

- "Un bug n'est pas un phénomène exceptionnel" … malheureusement

- En cas de bug, le comportement du logiciel ou du micro-code est déterminant
  - Redémarrage de l'application : perturbation
  - Arrêt de l'application : dysfonctionnement mineur
  - Arrêt du système : dysfonctionnement majeur
  - Arrêt d'une chaîne de traitement : dysfonctionnement majeur
  - Arrêt en chaîne des systèmes de traitement : dysfonctionnement critique
  - Rien ne se passe : dysfonctionnement critique
  - Passage de l'application dans un état inconnu : dysfonctionnement majeur à critique
  - Arrivée de l'application au niveau système : dysfonctionnement critique

- Critères
  - Avertissement du problème
  - Impacts : niveaux opérationnels et techniques
  - Confinement des risques

Les populations concernées

- 4 types de population sont concernés
  - Internautes non sensibilisés aux problématiques de la sécurité — critique
    - Pas d'anti-virus, pas d'outils de protection
    - Pas informés des avis de vulnérabilités et de la disponibilité de correctifs
  - Internautes sensibilisés aux problématiques de la sécurité — faible
    - Anti-virus, firewall personnel
    - Suivent les avis de vulnérabilité et appliquent les correctifs
  - Entreprises sans organisation informatique ou sécurité dédiée — élevé
    - Niveau d'équipement variable
    - Suivi négligé
  - Grandes entreprises avec équipe(s) sécurité — moyen
- Tous les composants sont concernés
  - Serveurs, postes de travail, équipements réseaux …
  - Système d'exploitation, application, base de données …

La course contre la montre

- 3 questions pour savoir qui est le plus rapide !
  - qui du correctif ou du code d'exploitation ?
  - qui des configurations sur les outils de détection ou du code d'exploitation ?
  - qui de l'application du correctif ou de la diffusion du code d'exploitation ?
- Anticiper est primordial ☺
  - Disposer d'un réseau de veille et d'alerte, déclencher des procédures pré-établies
- Décaler dans le temps l'application de correctifs ☹
  - Accroissement naturel du niveau global d'insécurité
- Délai d'apparition après diffusion de l'avis
  - 2001 : Nimda, 10 mois
  - 2003 : SQL Slammer, 6 mois – Welchia, 5 mois - Blaster : 3 semaines
  - 2004 : Sasser, 2 semaines
- Vitesse de propagation
  - Avant 2001 : par messagerie, plusieurs heures ou jours
  - 2001 : Code Red, quelques jours – Nimda, quelques heures
  - 2003 : SQL Slammer, quelques minutes

2 – En amont

- En amont, plusieurs procédures doivent donc être mises en place
  - Homogénéité : Suivi du parc informatique
  - Veille : Suivi des annonces et mises à disponibilité de correctifs
  - Identification des correctifs adaptés
  - Environnement de test ou de pré-production pour les tests
  - Estimation et analyse des risques et des impacts en cas de non-application des correctifs
  - Circuit de décision

- Être réactif par l'anticipation

Configuration de départ

- Les versions installées "par défaut" sont elles correctes et bien configurées ?
  - Ex : Linux

	Linux 3.0	Fedora Core 1	Debian 3.0r2	SuSE 9.1	Mandrake 10
kernel	2.4.21	2.4.22	2.2.20	2.6.4	2.6.3
apache 1.x			1.3.26		1.3.29
apache 2.x	2.0.46	2.0.47		2.0.49	2.0.48
bind	9.2.2	9.2.2p3	8.3.3	9.2.3	9.2.3
iptable	1.2.8	1.2.8	1.2.6a	1.2.9	1.2.9
mysql	3.23.58	3.23.58	3.23.29	4.0.18	4.0.17
openssh	3.6.1p1	3.6.1p2	3.4p1	3.8p1	3.6.1p2
openssl	0.9.7a	0.9.7a	0.9.6c	0.9.7d	0.9.7c
perl	5.8. 0	5.8.1	5.6.1	5.8.3	5.8.3
postfix	2.0.11	2.0.11	1.1.11	2.0.19	2.0.18
postgresql		7.3.4	7.2.1	7.4.2	7.4.1
rpm	4.2.1	4.2.1	4.0.3	4.1.1	4.2.2
samba	3.0.0	3.0.0	2.2.3a	3.0.2a	3.0.2
sendmail	8.12.10	8.12.10	8.12.3	8.12.10	8.12.11
Xfree-86	4.3.0	4.3.0	4.1.0	4.3.99.902	4.3.0
xinetd	2.3.12	2.3.12	2.3.4	2.3.13	2.3.12

Veille Sécurité

- Définition du périmètre de cette veille
- Sites officiels, des éditeurs, des grands forums et listes de discussion
- Récurrence et régularité
- Microsoft et la politique du "Super Tuesday"
  - Publication des avis de vulnérabilités tous les deuxièmes mardi de chaque mois
  - Planification de mises à jour possible
  - Chronologie du packaging des correctifs
    - Patch, Cumulative Patch, Security Rollout Package, Service Pack
      - Correction cachée dans un Service Pack !

- Disposer d'une information adaptée
  - Suivre les news est suffisant pour un individu
  - Nécessité de qualifier l'information et d'en déduire un niveau de risque réel et ne pas se contenter de celui de l'éditeur
  - Croiser avec les outils de gestion de parc
  - Transmettre une information utilisable et pratique aux personnes concernées

Tests de validation

- Récupération et vérification du correctif
- Vérification de ses pré-requis et dépendances théoriques
  - Portée réelle du correctif
- Vérification de l'adéquation du correctif
  - Efficacité : suppression ou contournement de la vulnérabilité qu'il adresse
    - Analyse de la "signature" de la plate-forme
    - Tests de **non-régression**
  - Complétude : réalisation des fonctions attendues sans besoins annexes
    - Pré-requis, **droits et privilèges**, **langue** … !
  - Indépendance : **absence d'effets de bord** ou de dysfonctionnement
    - Pas d'écrasement de configurations ou de paramétrages spécifiques
  - Intégrité : **retour arrière possible**
    - La suppression du correctif permet de retrouver le système tel qu'avant
- Test grandeur réel sur un site pilote
  - Journalisation et documentation des opérations réalisées
  - Préparation du déploiement, avec des outils ou des personnes

Dossier de prise de décision

- Analyser des risques couverts et des risques résiduels
- Estimation des coûts induits
  - Par le déploiement des correctifs
    - En manuel ou en automatique, en heures ouvrables ou non
  - Par le non-déploiement des correctifs
    - Mise en place de parades ou de solutions de contournement
  - Par une indisponibilité des plates-formes vulnérables en cas d'arrêt
  - Dans le cas d'une exploitation de la vulnérabilité concernée
- Estimation des coûts et impacts potentiels en cas de non-respect d'une directive métier ou d'une législation
- Les principaux éléments constitutifs d'un dossier d'aide à la prise de décision sont alors réunis.

- *GO/NO GO*

3 – Mise en Œuvre

- Dans le respect des procédures existantes et des contraintes d'exploitation
  - Déploiement maîtrisé avec des outils de télé-distribution qui transmettent des paquetages logiciels
  - Déploiement semi-maîtrisé par l'entreprise avec les plates-formes cibles qui viennent chercher leurs paquetages logiciels de façon asynchrone et indépendante
  - Déploiement non maîtrisé par l'entreprise car c'est l'utilisateur qui va chercher les correctifs
  - Suivi de l'avancement du déploiement
  - Suivi des rejets ou des échecs
  - Suivi des effets de bord
- Les outils !
  - Plusieurs offres, mais attention au domaine de couverture
    - système d'exploitation, application, Windows, Unix, Linux …
    - Microsoft : MSUS, MBSA, HFNetCheck
- Traiter le cas des postes nomades !

4 – En Aval

- En aval aussi, plusieurs procédures doivent être mises en place
  - Le suivi immédiat après application du correctif
    - Suivi de projet, effets de bord
  - Le suivi des mises à jour pour les correctifs
    - Suivi des évolutions du correctif lui-même
  - La mise à jour de l'inventaire du parc informatique
    - Pour le prochain correctif à appliquer
  - La communication des résultats obtenus
    - Le dire quand le travail avance bien

- Les tableaux de bord
  - Direction Informatique
    - Mesure du suivi et du niveau du parc
  - Direction des Risques Opérationnels
    - Mesure du niveau de sécurité et mise à jour des analyses de risques

5 – Compléments

- Pourquoi les utilisateurs n'appliquent pas les correctifs
  - Pas au courant
  - Utilité ?
  - Est-on vraiment concerné ? Est-on vraiment susceptible d'intéresser quelqu'un ?
  - Trop long à récupérer !
  - À peine installé, il faut en installer d'autres, c'est une histoire sans fin
  - J'ai déjà un anti-virus

- Pourquoi les entreprises n'appliquent pas les correctifs
  - Elles le font, mais cela représente une grosse charge de travail
  - Elles le font, mais avec du retard
  - Elles le font, mais ils y a des effets de bord non négligeable
  - Elles le font, mais certains postes sont réservé à des applications métiers non maîtrisées
  - Elles le font au travers d'un master remis à jour tous les 6 mois et qui est installé sur tous les postes
  - On a un problème avec les portables et les PDA

Ce qui ne peut pas être mis à jour

- Certains systèmes ne peuvent pas être pris en compte, ceux de type "clé en main"
  - Plates-formes dédiées au pilotage de processus industriels
    - Production industrielle
  - Plates-formes dédiées pour des applications métiers
    - Gestion "complète" par l'éditeur
  - Applications ou module réutilisé en "OEM" par d'autres applications
    - Encore faut-il savoir quel sont les "embedded run-time"
      - SQL Server, Apache, IE, IIS …
- Approches
  - Appliquer directement les correctifs ?
    - Effets de bord presque certains
    - Perte de la maintenance ou de la garantie constructeur
  - Déterminer qui maîtrise vraiment les applications "clé en main"
- Faire remonter les vulnérabilités à l'éditeur/concepteur
  - Puis attendre !

6 – Conclusions

- Pour les particuliers
  - …
- Pour les entreprises
  - Mettre en place une organisation spécifique
    - information en amont, qualification, applicabilité, tests, déploiement, vérification et suivi
  - Sensibiliser et de convaincre le management de l'entreprise
- Le nombre de logiciels de "patch management" augmente en ce moment
  - Surtout la partie de récupération et de déploiement

Quelques évidences … quoi que …

- Il faut patcher !
- Patcher 1 machine, ça va
  - Patcher 20 machines, ça va
    - Patcher 300 machines, bonjour les dégâts !
- Au lieu de patcher *a posteriori* …
  - il vaudrait mieux installer correctement dès le départ
- Plutôt que de conserver des vieux Windows ou des vieux IE, autant upgrader

L'avis de William Shakespeare ;-)

- "To patch, or not to patch, - that is the question: -
- Whether 'tis nobler in the mind to suffer
- The slings and arrows of outrageous script kiddies,
- Or to take up patches against a sea of troubles,
- And by opposing, end them?"

7 – Bibliographie

- NIST: SP800-40 "Procedures for Handling Security Patches"
  - http://csrc.nist.gov/publications/nistpubs/800-40/sp800-40.pdf
- GAO: GAO-03-1138T - "Effective Patch Management is Critical to Mitigating Software Vulnerabilities"
  - http://www.gao.gov/new.items/d031138t.pdf
- SANS: "Security Essentials: Patch Management as a Necessary Part of Defense In Depth, A Case Study" par Kay A. Cornwell
  - http://www.giac.org/practical/GSAE/Kay_Cornwell.pdf

APOGÉE Communications - Groupe DEVOTEAM
Olivier Caleff
Consultant et Auditeur Sécurité Senior
Tel + 33 1 69857800
15, Avenue du Cap Horn - ZA de Courtaboeuf
91940 Les Ulis - France
www.apogee-com.fr - www.devoteam.com

Auteur Adresse Email #1 Adresse Email #2	Olivier Caleff Olivier.Caleff(at)Apogee-Com.Fr Olivier.Caleff(at)Devoteam.Com
Date de la présentation	Jeudi 3 juin 2004
Nom du fichier Version du fichier	SSTIC-2004-Caleff-PatchManagement.ppt 2.3

Implantations du Groupe DEVOTEAM

France
Danemark
Royaume-Uni
Pays-Bas
Belgique
Espagne
Autriche