LES DOSSIERS TECHNIQUES

Gestion des vulnérabilités informatiques : vers une meilleure gestion des risques opérationnels

[Valeur et caractère indispensable de la gestion des vulnérabilités]

Mai 2014

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11 rue de Mogador - 75009 Paris
Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88
clusif@clusif.fr – www.clusif.fr

Table des matières

I. Introduction 5
I.1. Objet 5
I.2. Description du sujet 5
II. La gestion des risques, un concept managérial connu 8
II.1. La prise de risques inhérente au fonctionnement d'une organisation 8
II.2. De l'importance de la gestion des risques des systèmes d'information 8
III. Les vulnérabilités informatiques 10
III.1. Définition 10
III.2. Cycle de vie de la vulnérabilité 10
III.3. Exemples concrets 11
III.3.1. Vulnérabilité des logiciels bureautiques sur un poste de travail 11
III.3.2. Vulnérabilité d'une application Web 11
IV. Valeur de la gestion des vulnérabilités 13
IV.1. Caractère indispensable dans une stratégie de sécurité 13
IV.2. Bénéfices et principaux usages 14
IV.3. Stratégies de mise en oeuvre 15
V. Conclusion 16

Remerciements

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Le responsable du groupe de travail :

François	**GRATIOLET**	*Qualys*

Les contributeurs :

Jean-François	**AUDENARD**	*Orange*
Alexis	**CAURETTE**	*Bull*
Sébastien	**GIORIA**	*Advens*
Astrid	**LANG**	*APHP*
Sébastien	**MAUPTIT**	*Systalians*
Vincent	**MAURY**	*DenyAll*
Hervé	**SCHAUER**	*HSC*
Arnaud	**TARRAGO**	*EDF*
Alain	**VIDAL**	*Agence Nationale pour les Chèques-Vacances*

Le **CLUSIF** remercie également les adhérents ayant participé à la relecture.

I. Introduction

I.1. Objet

Le présent document fournit aux RSSI des éléments d'accompagnement et de sensibilisation à la gestion des vulnérabilités auprès des DSI, Risk Managers et Dirigeants de leur organisation. On entend par organisation aussi bien les grands groupes, les administrations publiques que les PME.

Ce document adresse spécifiquement les vulnérabilités informatiques (logicielles[1] ou de configuration[2]) – que nous nommerons simplement vulnérabilités par la suite – et non les vulnérabilités organisationnelles, de processus, comportementales, etc., ni les vulnérabilités matérielles (pouvant compromettre la sécurité physique).

I.2. Description du sujet

Grandes organisations, TPE, PME : même combat devant les cyber menaces et intentions malveillantes des réseaux criminels, de compétiteurs peu scrupuleux, d'hacktivistes, voire de gouvernements !

Les systèmes d'information restent vulnérables et peuvent impacter les organisations pour lesquelles nous travaillons ainsi que nos vies privées. Tous les secteurs d'activités sont concernés ! De par leur taille et ressources, les TPE/PME sont d'autant plus vulnérables.

Les vulnérabilités concernent l'ensemble des équipements et réseaux, par exemple les systèmes de téléphonie, les systèmes d'information d'entreprise, les systèmes d'information industriels ou les systèmes d'information alternatifs[3].

Selon l'organisme OWASP (Open Web Application Security Project), en 2013, 97% des applications Web restent exposées à des vulnérabilités connues, et les principaux risques liés aux applications Web demeurent identiques, notamment les injections SQL qui permettent à un tiers malveillant de récupérer, voler, modifier ou détruire des informations sensibles par exemple dans une base de données.

L'étude DBIR (Data Breach Investigations Report) réalisée en 2012 par Verizon a révélé suite à « l'autopsie » de 855 incidents que 92% des attaques étaient peu complexes, 79% étaient des cibles opportunistes et que 97% des infractions réussies auraient pu être évitées si la victime avait déployé entre autres des correctifs de sécurité et des mots de passe robustes.

Le Gartner Group estime qu'en 2015, 80% des attaques réussies exploiteront des vulnérabilités connues.

[1] Voir la base CVE (*Common Vulnerability Enumeratio*n)
[2] Voir la base CCE (*Common Configuration Enumeration*)
[3] cf. les définitions du livrable « Cybersécurité des systèmes industriels : Par où commencer ? » http://www.clusif.fr/fr/production/ouvrages/pdf/CLUSIF-2014-SCADA-Panorama-des-referentiels.pdf

Un retour aux basiques sécuritaires est plus qu'urgent ! L'ANSSI a publié en 2013 un guide d'hygiène informatique[4] qui reprend les mesures de sécurité requises dans toute organisation.

Ainsi, la gestion des vulnérabilités est une mesure de sécurité mise en oeuvre dans tous les grands référentiels, standards, régulations sectorielles ou bonnes pratiques du marché, par exemple, la famille des normes ISO 27000, les accords de Bâle, le standard PCI-DSS[5], les standards ETSI ISI[6], ou encore les « 20 Critical Controls » du SANS Institute et du Conseil de la Cybersécurité[7]. Il existe désormais plusieurs exemples publics d'organisations ayant adopté avec succès et efficacité ce référentiel des « 20 Critical Controls » aussi bien aux Etats-Unis (exemple du US Department of State[8]), en Australie, en Angleterre qu'au Canada.

La gestion des vulnérabilités devient réglementaire par exemple pour les Opérateurs d'Importance Vitale (OIV) et leurs prestataires. A ce titre, la Loi relative à la Programmation Militaire (LPM)[9] leur impose la mise en place de systèmes de détection d'évènements pouvant affecter la sécurité de leurs systèmes d'information, et de manière implicite la détection et le traitement des vulnérabilités.

Les organisations s'accordent ainsi sur le caractère fondamental et désormais règlementaire de la détection d'évènements susceptibles d'affecter la sécurité de leurs systèmes d'information. La correction des vulnérabilités limitera d'autant les événements susceptibles d'affecter la sécurité de leurs systèmes d'information.

La mise en place d'un processus de gestion des vulnérabilités apparaît essentielle afin d'évaluer en continu et « en temps réel » le niveau de sécurité de l'organisation et de décider des actions prioritaires à conduire.

Force est de constater que malgré ces nombreuses références et la pression réglementaire croissante, un grand nombre d'organisations gère leurs vulnérabilités informatiques au rythme de l'évolution de leur système d'information, souvent sur un cycle de plusieurs années !

Quelles sont les raisons de cet échec et les obstacles rencontrés par les organisations ?

- Les Dirigeants soutiennent de manière insuffisante les initiatives visant à leur déploiement au sein de leur organisation, se retrouvant confrontés à une maturité insuffisante de leur organisation, un manque de moyens, et disposant probablement d'une connaissance partielle de la valeur apportée par la gestion des vulnérabilités. Ils craignent également que la correction ait un effet négatif sur la stabilité du service.
- Bien que des solutions technologiques et opérationnelles matures existent, celles-ci restent peu déployées. Leur taux de couverture est rarement proche de 100% du périmètre du système d'information propre à l'organisation.

[4] http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf
[5] https://www.pcisecuritystandards.org
[6] http://www.etsi.org/deliver/etsi_gs/ISI/001_099/002/01.01.01_60/gs_isi002v010101p.pdf
[7] http://www.counciloncybersecurity.org/practice-areas/technology/
[8] http://www.sans.org/press/department-state-wins-ncia.php
[9]http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=4511A3DD931A64F4DD5C139AE65FE70A.tpdjo07v_2?cidTexte=JORFTEXT000028338825&categorieLien=id

- Lorsqu'il y a lieu, le déploiement de ces solutions est souvent confronté à un manque d'organisation et de processus pourtant indispensables à l'utilisation efficiente de ces outils. Il est difficile pour les RSSI d'avoir un retour sur le nombre d'actifs vulnérables qui ont fait réellement l'objet d'une correction.
- Enfin, les administrateurs informatiques sont peu incités à déployer les correctifs de sécurité ou à modifier les configurations sur les machines informatiques lorsque des vulnérabilités sont découvertes.

Contrairement aux menaces qui sont difficiles à contrôler, et aux incidents pour lesquels seules les conséquences peuvent être limitées, il est important de garder à l'esprit qu'il est possible d'agir sur les vulnérabilités car elles sont intrinsèques à une organisation.

Ces éléments ont motivé la rédaction du présent document qui a pour objet de rappeler la valeur et le caractère stratégique de la gestion des vulnérabilités au sein d'une organisation afin d'obtenir une adhésion et un support au plus haut niveau, et de donner les moyens au RSSI de lancer un tel programme et de mettre en place une structure opérationnelle.

II. La gestion des risques, un concept managérial connu

II.1. La prise de risques inhérente au fonctionnement d'une organisation

Quelle que soit l'organisation, publique ou privée et sa taille, sa finalité est de générer de la valeur : de la valeur financière et un rendement pour les actionnaires d'une entreprise, de la valeur d'usage perçue par les clients ou usagers dans le cas d'un organisme public.

La capacité d'une organisation à créer de la valeur, obtenir ainsi que maintenir un avantage concurrentiel est déterminée par sa chaîne de valeur constituée de ses actifs.

La famille de normes ISO 27000 définit un actif comme « tout élément représentant de la valeur pour l'organisation ». Un actif se caractérise par sa nature (activités, processus et informations). Les actifs de production (logistique amont, fabrication, logistique aval, marketing & vente, services, etc.) concourent directement à la vente des produits, et reposent sur des actifs de soutien (achats, R&D, gestion RH, finances, informatiques, etc.).

Gérer une organisation pour ses mandataires sociaux et ses Dirigeants consiste à identifier de manière proactive des options stratégiques et des actions (par exemple, lancement d'un nouveau produit, pénétration d'un marché, etc.), et à faire un choix éclairé du risque pris selon l'option retenue, c'est-à-dire mettre en rapport un bénéfice espéré face à un risque redouté.

Ces arbitrages coûts/bénéfices/risques sont applicables à l'ensemble des fonctions de l'organisation et des ressources utilisées par ces fonctions, notamment les systèmes d'information.

Afin d'identifier ces options stratégiques, les Dirigeants sont amenés à connaître les menaces et opportunités de l'environnement concurrentiel, ainsi que les forces et faiblesses de leur entreprise, et pour cela, à conduire une analyse SWOT (Strengths Weaknesses Opportunities Threats).

II.2. De l'importance de la gestion des risques des systèmes d'information

Longtemps associés à des activités de soutien comme par exemple la comptabilité, les systèmes d'information et l'informatique sont aujourd'hui présents au cœur de la plupart des processus de l'organisation, y compris les activités de production, et dans l'ensemble des secteurs d'activité. L'automatisation des tâches ainsi réalisées permet des gains importants en termes de qualité, de fiabilité et de rapidité de traitement. Le système d'information devient un facteur de différenciation concurrentielle et d'innovation.

La contrepartie des bénéfices ainsi apportés par les technologies de l'information est une dépendance accrue des activités de l'organisation aux systèmes d'information (matériels, logiciels, personnels, sites, etc.), que ces activités soient liées aux actifs de production ou de soutien. Ainsi, cartographier ses actifs Métiers et informatiques sous-jacents devient essentiel pour une organisation.

De par la nature et la diversité de leurs composants logiciels (réseaux, systèmes, bases de données, messagerie électronique, serveurs Web, etc.) et surtout leur nombre, les systèmes

d'information sont vulnérables. Un logiciel ou une application développé avec un code informatique de mauvaise qualité, mal paramétré ou insuffisamment testé peut ainsi introduire des failles dans les systèmes.

Ces vulnérabilités exploitées par des personnes malveillantes (concurrents, hacktivistes, salariés, partenaires, fournisseurs, gouvernements, etc.) peuvent porter préjudice au bon fonctionnement des systèmes d'information (indisponibilité, intrusion dans les systèmes, vol d'informations, etc.) et de l'organisation (image détériorée, perte de confiance des clients, non-respect de règlementations, baisse des revenus, réduction de la marge opérationnelle, etc.).

Les cyber attaques et incidents de sécurité ne sont plus des phénomènes isolés mais une vraie réalité relayée par les médias comme l'attestent les nombreux articles publiés dans les journaux économiques[10].

Il est urgent que les Dirigeants intègrent dans l'analyse de leur environnement les faiblesses liées aux systèmes d'information.

La gestion des vulnérabilités informatiques en tant que telle ne crée pas directement de la valeur. Par contre, une absence de gestion des vulnérabilités limite indirectement la création de valeur pour l'organisation.

Les vulnérabilités d'une infrastructure informatique constituent un risque opérationnel majeur et nécessitent d'être adressées au plus haut niveau.

[10] http://www.lecho.be/actualite/marche_placements_marches/Les_Bourses_vulnerables_aux_cyberattaques.9431496-3458.art?ckc=1
http://www.latribune.fr/entreprises-finance/20140215trib000815524/le-secteur-aeronautique-francais-cible-d-une-cyberattaque.html

III. Les vulnérabilités informatiques

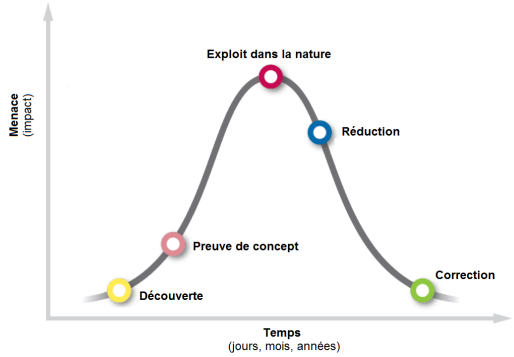
III.1. Définition

La famille des standards ISO 27000[11], adoptée par de nombreuses organisations dans le monde, et reprise par de multiples standards fonctionnels et techniques[12], définit une vulnérabilité comme une faiblesse - au sein d'un actif ou groupe d'actifs - dont l'exploitation potentielle (par une menace) peut porter préjudice à l'organisation : fuite d'informations confidentielles, image détériorée, perte de confiance des clients, non-respect de règlementations, baisse des revenus, réduction de la marge opérationnelle, etc.

III.2. Cycle de vie de la vulnérabilité

Le cycle de vie d'une vulnérabilité débute par sa découverte. Dans le cas où une personne malveillante la découvre, elle va tenter de l'exploiter en développant un code spécifique appelé exploit (*zero-day*[13]) en attendant que cette vulnérabilité devienne publique (remontée par des sociétés spécialisées en sécurité informatique, des éditeurs de logiciels, des cellules de veille, etc), soit qualifiée puis enfin corrigée. A ce titre, l'ANSSI a publié un guide sur les vulnérabilités 0-day de « Prévention et bonnes pratiques »[14]. Dans le cas d'une vulnérabilité logicielle, l'éditeur devra fournir soit un correctif (*patch*) qui sera installé sur les systèmes vulnérables soit une nouvelle version du logiciel qui corrige la vulnérabilité.

La mesure de la demi-vie d'une vulnérabilité (intervalle de temps nécessaire à la réduction de l'occurrence d'une vulnérabilité de moitié sur l'ensemble du système d'information) peut fournir un indicateur sur la complexité de résolution d'une vulnérabilité. Pour des organisations matures ayant automatisé le processus de gestion des vulnérabilités, cette demi-vie oscille entre 30 et 60 jours pour une vulnérabilité critique selon les secteurs d'activité.



Le diagramme ci-contre illustre le cycle de vie d'une vulnérabilité au regard du degré d'importance de la menace. L'organisation reste exposée durant tout le cycle de vie, rendant nécessaires l'identification de la vulnérabilité au plus tôt et sa prise en compte rapide. Le traitement d'une vulnérabilité ne consiste pas systématiquement à la corriger directement, pour des considérations de temps et de coût, voire d'impossibilité (les éditeurs ou constructeurs ne corrigent pas systématiquement toutes les

[11] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
[12] ETSI ISI-002, IETF RFC 2828, ENISA, ISACA, etc
[13] Une vulnérabilité zero-day est communément définie comme une vulnérabilité pour laquelle un code d'exploitation existe mais pour laquelle aucun correctif n'est encore disponible.
[14] http://www.ssi.gouv.fr/IMG/pdf/guide_vulnerabilites_0day.pdf

failles de sécurité). Dès lors que la vulnérabilité est connue, un contournement doit, si possible, être mis en place.

Ces décisions dépendent également de la nature de la vulnérabilité. Dans l'exemple d'une faiblesse de configuration sur une application dont l'organisation est propriétaire, celle-ci sera autonome dans sa résolution. En revanche, si la vulnérabilité touche un logiciel commercial, l'organisation se retournera vers l'éditeur tant qu'il est engagé contractuellement à livrer un correctif (avec un délai et des éventuelles pénalités de retard).

III.3. Exemples concrets

Prenons deux exemples réels de vulnérabilités et examinons les possibles remédiations.

III.3.1. Vulnérabilité des logiciels bureautiques sur un poste de travail

Les logiciels couramment installés sur un poste de travail – Microsoft Office, navigateurs Web (Google Chrome, IE, Firefox, etc.) et plug-ins, Acrobat Reader, Java, Flash, etc.- font l'objet de nombreuses vulnérabilités dont l'impact touche autant les postes de travail de l'organisation que les ordinateurs personnels utilisés par les employés à leur domicile.

Le nombre de vulnérabilités potentielles impactant les postes de travail d'une organisation est non seulement lié à leur nombre mais également à la variété des logiciels utilisés. Les éditeurs de ces logiciels fournissent régulièrement des correctifs corrigeant des lots de vulnérabilités[15].

L'installation de ces correctifs étant parfois non automatisée, non automatisable ou mal contrôlée, le cycle de vie de ces vulnérabilités peut durer plusieurs mois à plusieurs années.

Durant cette période d'exposition, plusieurs mesures permettent de réduire l'impact de l'exploitation de ces vulnérabilités: par exemple, diminution des droits de l'utilisateur, utilisation d'une solution d'antivirus à jour, activation d'un pare-feu, maîtrise du parc logiciel et suppression simple des logiciels faisant l'objet de trop nombreuses vulnérabilités.

III.3.2. Vulnérabilité d'une application Web

Une vulnérabilité de développement Web (par exemple, une injection SQL utilise une vulnérabilité de sécurité d'une application interagissant avec une base de données, en injectant une requête SQL non prévue par le système et pouvant compromettre sa sécurité) risque typiquement de compromettre les données sous-jacentes au site Web (moyens de paiement, données à caractère personnel, etc).

Sa correction nécessite de modifier le code source du site Web, de le tester puis de le déployer. Ce processus peut se révéler complexe, surtout si l'auteur du développement n'est pas réactif (ou injoignable) ou si l'organisation ne dispose pas d'un contrat de maintenance avec des clauses exigeant de traiter ces vulnérabilités dans des délais acceptables.

Dans l'attente de la correction effective de la vulnérabilité, l'organisation peut mettre en œuvre des règles de filtrage spécifiques sur un pare-feu applicatif Web (WAF ou Web

[15] Exemples publics non exhaustifs : http://helpx.adobe.com/security/products/flash-player/apsb14-07.html; http://technet.microsoft.com/fr-fr/security/bulletin/ms14-001

Application Firewall) analysant les requêtes du site Web et bloquant les attaques visant à exploiter l'injection SQL. Ce mécanisme de « patching virtuel » permet de protéger l'application Web avant que la vulnérabilité de l'application Web ne soit effectivement corrigée.

Ces exemples illustrent le fait que les vulnérabilités touchent tous types d'organisations, tous types d'utilisateurs et tous types de logiciels tant les logiciels commerciaux que propriétaires. Leur remédiation peut être complexe selon le contexte. Elle doit être gérée par priorité, suivant une réflexion découlant de la stratégie de l'organisation.

IV. Valeur de la gestion des vulnérabilités

IV.1. Caractère indispensable dans une stratégie de sécurité

La Politique de Sécurité des Systèmes d'Information d'une organisation doit comporter un chapitre traitant de la gestion des vulnérabilités. La gestion des vulnérabilités est un pilier essentiel de tout programme de sécurité. La Direction doit s'assurer que des mesures sont effectivement mises en œuvre et maintenir en condition opérationnelle de sécurité les composants du système d'information, en mettant l'accent sur les actifs les plus exposés ou les plus critiques pour les activités de l'organisation.

Les organisations doivent intégrer la gestion des vulnérabilités et des risques au cœur de leur stratégie de sécurité de façon à ce que les moyens alloués et activités soient coordonnés avec les autres activités opérationnelles. La gestion des vulnérabilités renforce la sécurité intrinsèque des systèmes tout en venant compléter d'autres types de mesures de sécurité (gestion des accès, filtrage des flux, détection et blocage des attaques, etc.) pour former un ensemble cohérent.

La gestion des vulnérabilités se traduit par une activité opérationnelle au sein d'une organisation, et s'inscrit dans une logique d'amélioration continue, comme schématisé ci-dessous :

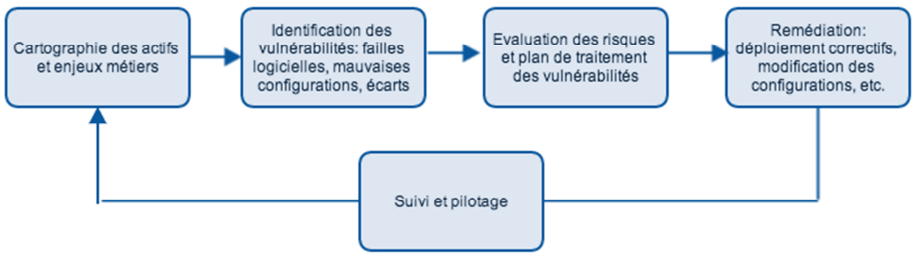


Figure 1: Activité de gestion des vulnérabilités et contrôle permanent

Cette activité collecte à fréquence régulière des informations de sécurité (actifs, vulnérabilités logicielles, vulnérabilités de configuration) et permet d'ajuster si besoin les politiques et standards de sécurité de l'organisation au regard de l'exposition aux risques.

Les mesures doivent être effectuées de manière fiable et indépendante.

IV.2. Bénéfices et principaux usages

A titre d'illustration, prenons la récente faille médiatisée Heartbleed[16] qui a touché entre les sites Internet de banques, d'e-commerce et de réseaux sociaux. La gestion des vulnérabilités permet de répondre aux questions suivantes :

- quel est le nombre d'applications Web exposées sur Internet ?
- où et comment sont hébergés les applications (Intranet, Extranet, cloud, SaaS, etc.) ?
- quelles sont les applications vulnérables à Heartbleed ?
- quel est l'état d'avancement du plan de remédiation ?
- les anciens certificats SSL des sites Web ont-ils été révoqués ?
- peut-on garantir que les applications Web vulnérables ne le sont plus ?

La valeur apportée est d'identifier rapidement et de corriger les vulnérabilités qui représentent un risque opérationnel réel et majeur pour l'organisation, avant qu'elles ne soient exploitées.

Les Dirigeants et Responsables Sécurité des Systèmes d'Information d'une organisation disposent ainsi d'une vision globale et consolidée de l'exposition aux risques de l'infrastructure informatique (qu'elle soit exposée sur Internet, interne, ou externalisée par exemple auprès d'un hébergeur ou d'un fournisseur de cloud), leur permettant de prendre les décisions (déploiement de correctifs, modification des configurations, etc.) pour réduire le risque à un niveau acceptable.

La gestion des vulnérabilités peut être à la fois considérée comme un processus de sécurité au sens des normes de la famille ISO 27000 mais également comme un moyen de contrôle permanent, en particulier pour les entreprises côtées et des organismes dans le monde bancaire et assurantiel.

Le vocable « Contrôle permanent » ou « Continuous monitoring » relatif à la gestion des risques d'une entreprise provient du référentiel de contrôle interne COSO[17], reconnu internationalement, utilisé notamment par les lois Sarbanes-Oxley (SOX) aux Etats-Unis et Loi sur la Sécurité Financière (LSF) en France. Ce terme s'applique également au contrôle interne de l'activité informatique d'une organisation[18].

Un DSI doit pouvoir démontrer aux actionnaires de l'entreprise que l'infrastructure informatique fournie est sécurisée et que les risques associés sont maîtrisés. En général, le RSSI dispose d'une délégation de la part du contrôle interne, et met en place un tel dispositif de contrôle interne pour l'informatique et sa sécurité. Les mesures suivantes peuvent par exemple contribuer au dispositif de contrôle interne d'une organisation:

- 1er niveau: les utilisateurs doivent utiliser des mots de passe à XX caractères sur leur poste informatique (mise en place d'une mesure de sécurité pour réduire le risque d'accès aux applications métiers par exemple).

[16] http://www.lefigaro.fr/secteur/high-tech/2014/04/11/01007-20140411ARTFIG00496-heartbleed-la-faille-qui-frappe-le-coeur-de-la-securite-sur-internet.php
[17] http://www.coso.org/
[18] http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf

- 2ième niveau: l'organisation s'assure par une solution automatisée de gestion des vulnérabilités et de conformité que tous les mots de passe des postes informatiques font bien XX caractères (mise en place d'un contrôle permanent d'une mesure de sécurité).

IV.3. Stratégies de mise en oeuvre

Au sein des organisations, la mise en œuvre d'une activité de gestion des vulnérabilités peut rencontrer de nombreux freins organisationnels ou opérationnels. La stratégie de mise en œuvre doit donc être souple, progressive et adaptée aux moyens disponibles et au niveau de maturité de l'organisation. Une stratégie de défense en profondeur[19] est à privilégier.

L'ensemble des systèmes, applications et équipements en production doit être régulièrement analysé et intégré au processus et faire l'objet d'un traitement des vulnérabilités détectées. La remédiation ou correction des vulnérabilités ne se concentrera que sur les actifs les plus critiques pour les activités de l'organisation et ceux qui sont les plus exposés aux risques.

La gestion des vulnérabilités doit être intégrée dans le cycle de vie des systèmes et des applications en se rapprochant des équipes en charge du développement et de la maintenance, afin de détecter au plus tôt une vulnérabilité via des tests réalisés par les équipes en charge du développement ou de celles en charge de valider les systèmes avant leur passage en production. Cette approche dès la conception permet de « diffuser » une culture de la gestion des vulnérabilités au-delà des équipes en charge de l'exploitation et de l'administration des systèmes.

Il est à noter qu'une vulnérabilité ne « disparaît » jamais complètement à cause de réinstallation, de déploiement de nouveaux systèmes avec des anciennes configurations, de restauration de sauvegardes, etc. d'où la nécessité de continuer à les surveiller même après le déploiement d'un correctif.

Pour les vulnérabilités ne pouvant être corrigées pour diverses raisons (ressources humaines ou financières insuffisantes, correctifs non disponibles, freins organisationnels, contraintes techniques spécifiques, etc.), l'organisation devra s'attacher à mettre en place des mesures de sécurité palliatives. Ces mesures peuvent être par exemple des mesures de prévention (règle plus stricte sur un pare-feu situé en amont, etc.) ou des mesures de réaction (renforcement du niveau de supervision des traces, etc.).

Dans tous les cas, les risques résiduels (subsistant après traitement) devront être identifiés, formalisés et acceptés de façon explicite et formelle par le Management.

[19] http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/outils-methodologiques/la-defense-en-profondeur-appliquee-aux-systemes-d-information.html

V. Conclusion

L’exploitation d’une seule vulnérabilité informatique basique peut porter préjudice aux activités opérationnelles d'une organisation, également détériorer son image, entraîner une perte de confiance de ses clients, faire chuter sa valeur et à terme entraîner sa disparition.

La gestion des vulnérabilités en tant que telle ne crée pas directement de la valeur. Par contre, une absence de gestion des vulnérabilités limite indirectement la création de valeur pour l’organisation.

Les vulnérabilités d’une infrastructure informatique constituent un risque majeur opérationnel. Le plus haut niveau de l’organisation doit non seulement apporter toute la considération nécessaire à leur traitement par un suivi régulier, mais surtout apporter son soutien aux équipes en charge du traitement.

Ainsi, disposer d’une activité ou d’un processus de gestion des vulnérabilités informatiques au sein d’une organisation est essentiel.

Au préalable, un programme de gestion des vulnérabilités doit être lancé et visible de la Direction Générale ainsi que des Directions Métiers afin que celles-ci en comprennent la valeur et l’intérêt pour leurs activités et allouent les ressources en conséquence. On s’attachera à mettre l’accent sur les impacts opérationnels et les coûts associés, en conservant en second plan les aspects techniques moins directement compréhensibles pour des non techniciens.

Les facteurs clefs de succès de mise en œuvre d’un tel programme seront :

- Adopter une approche raisonnée et structurée
- Impliquer la Direction Générale et l’ensemble des parties prenantes concernées
- Nommer un responsable du programme de gestion des vulnérabilités
- Identifier et allouer un budget spécifique à la fois d’investissement et de fonctionnement
- Organiser, automatiser et industrialiser la gestion des vulnérabilités
- Communiquer de manière transparente et adaptée aux parties prenantes impliquées
- Créer des éléments de motivation pour les administrateurs informatiques
- Définir des indicateurs clefs

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11 rue de Mogador
75009 Paris
France
✆ +33 1 53 25 08 80
clusif@clusif.fr

Téléchargez toutes les productions du CLUSIF sur
www.clusif.fr