



EDITORIAL

EDITORIAL	p1
AGENDA	p1
ACTUALITES	p2
ZOOM	p3
➤ Chrome, le nouveau bijou de Google	
L'ESSENTIEL	p6
➤ La mutualisation des RLI	

Instaurer la confiance dans la sécurité de l'information

Nous traversons une crise économique qui, pour la plupart des professionnels de la profession (pour plagier Jean-Luc Godard) est loin d'avoir révélé toute son ampleur. Ils considèrent pour la plupart, qu'un des facteurs de la relance économique sera la « confiance ».

La sécurité de l'information n'échappe pas à cette règle. Tous les RSSI savent que l'établissement de la confiance dans la sécurité du système d'information n'est pas toujours une sinécure. Elle passe par l'implication de tous les acteurs de l'organisation et en premier lieu, celle de la Direction Générale.

Bien que le positionnement du RSSI fasse encore l'objet d'un vaste débat, il reste déterminant pour atteindre cet objectif. Prendre en compte les exigences de sécurité et les contraintes exprimées par le métier participe à l'instauration de la confiance.

L'exposition des informations face aux différentes menaces issues des nombreuses vulnérabilités, conduit à des compromis de couvertures sans que les enjeux et risques associés aient été précisément étudiés.

L'amélioration du processus de sécurisation et, par là même, la confiance qui en découle, sont liées aux étapes décrites dans les normes et standards :

- ✓ Réaliser une analyse de risques qui passe par l'évaluation de l'impact des menaces en fonction des vulnérabilités, sur l'activité de l'organisation.
- ✓ Mettre en place un ensemble de mesures pour réduire les risques à un niveau de protection choisi.
- ✓ Surveiller de façon continue et contrôler de façon indépendante.
- ✓ Améliorer les règles définies, en tenant compte des résultats obtenus par le contrôle et réévaluer la cohérence d'ensemble en fonction des impacts sur l'activité.

C'est bien la bonne vieille roue de Deming que l'on retrouve et qui tend à prouver que le bon sens reste une valeur sûre par les temps qui courent.

Cette démarche, assez récente quant à son application dans le processus de sécurisation des systèmes d'information, est basée sur une approche méthodique, est mise en œuvre depuis de nombreuses années par les entreprises de production. Elle contribue à la bonne qualité du produit final et inspire la confiance.

AGENDA

Rappel : INFOSECURITY - 19 et 20 novembre 2008 - Paris Porte de Versailles

Le Salon Infosecurity se tient les 19 et 20 novembre 2008 au Parc des expositions de la Porte de Versailles - Hall 5. 130 exposants - 60 conférences solutions - 5 événements associés - 5 sessions de formation.

➤ Plus d'infos : <http://www.infosecurity.com.fr>

Conférence OWASP - mercredi 19 novembre 2008 - Paris Porte de Versailles

L'Open Web Application Security Project est un projet open source dédié à la sécurité des applications Web. Thème de la conférence : ce qu'il faut faire, tout comme ce qu'il ne faut pas faire en matière de sécurité des applications Web.

➤ Plus d'infos : <http://www.infosecurity.com.fr>

Conférence Gestion des risques - 20 novembre 2008 - Paris Porte de Versailles

Thème de la conférence : les options fondamentales des méthodes de gestion des risques vues par le CLUSIF. L'étude présentée met en évidence de grandes différences entre les diverses méthodes de gestion des risques.

➤ Plus d'infos : <http://clusif.asso.fr>



ACTUALITÉS

L e laboratoire de l'ESEC vainqueur

L'équipe du laboratoire sécurité de l'ESEC a participé à la conférence annuelle Hack.Lu 2008 qui s'est tenue du 22 au 24 octobre à Luxembourg ville. Notre département de R&D a brillamment remporté le challenge « Capture the flag ».

Cette quatrième édition, forum de discussion sur des sujets liés à la sécurité

informatique et de l'information, aura permis à une vingtaine d'experts (dont 4 de l'ESEC) de faire connaître les résultats de leurs recherches. Cet événement s'est achevé par un discours du ministre de l'économie et du commerce extérieur luxembourgeois, Jeannot Krecké qui soutient le projet depuis sa création.

Pour en savoir plus :

http://wiki.hack.lu/index.php/Main_Page

Le compte rendu jour par jour

<http://esec.fr.sogeti.com/blog/index.php>

C ompromission électromagnétique des claviers filaires

Deux étudiants membres du laboratoire « Sécurité et Cryptographie » de l'École polytechnique fédérale de Lausanne (EPFL) se sont penchés sur la sécurité des claviers filaires. Bien que nettement plus sécurisés par nature que leurs homologues sans fil, ces derniers ont également des limites qu'il est intéressant de mettre en évidence.

L'axe de recherche choisi est la potentielle compromission électromagnétique qui n'a jamais été pratiquement réalisée.

Les dénommés Sylvain Pasini et Martin Vuagnoux affirment ainsi être les

premiers à en démontrer la faisabilité. Ils ont publié sur le site de leur laboratoire une courte présentation de leurs expérimentations.

Selon leurs travaux, ils affirment avoir réussi la compromission de onze claviers à une distance allant jusqu'à 20 mètres.

Les preuves avancées, quelques vidéos, demandent vérification. S'il s'avère que la faisabilité est bien réelle, la généralisation de solutions visant à protéger la saisie des informations sensibles sera la seule protection.

Diverses solutions existent, comme la saisie de mots de passe par clic à la souris sur un clavier virtuel affiché à l'écran.

Pour en savoir plus :

<http://www.01net.com/editorial/393953/les-claviers-menaces-de-piratage-a-distance/>

F lash vous filme : dysfonctionnement du plug-in flash

Si votre ordinateur est équipé d'une webcam, vous êtes le possible héros d'un clip vidéo qui a déjà fait le tour du monde.

Cette vulnérabilité permet non seulement de faire activer la webcam, mais également le microphone lorsqu'un utilisateur navigue sur un site malveillant.

Le 7 octobre 2008, Adobe a publié l'avertissement de sécurité APSA08-08 «Flash Player workaround available for "Clickjacking" issue».

Il est inquiétant d'imaginer que l'on peut techniquement être exposé sans aucun contrôle. Heureusement, la faille a été corrigée par Adobe.

Pour en savoir plus :

<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-490/>

<http://www.01net.com/editorial/392683/une-faille-de-flash-player-permet-de-pirater-les-webcams/>

<http://www.adobe.com/support/security/advisories/apsa08-08.html>

L es données de 30 millions de clients d'un opérateur télécom allemand en accès libre

Un opérateur télécom allemand a rendu public samedi 11 octobre qu'un problème de sécurité de son système d'information permettait un accès libre à des données personnelles de ses clients, dont certaines données bancaires.

Ce type de problème n'est pas nouveau dans cette entreprise.

En effet, début octobre, la presse allemande, notamment *Der Spiegel*, révélait qu'une filiale de cet opérateur s'était fait voler les données personnelles de 17 millions de clients.

Cette fois le problème était plus grave puisque les données n'étaient pas que consultables : l'opérateur a reconnu qu'il était également possible de les modifier.

Pour en savoir plus :

<http://www.01net.com/editorial/393163/les-donnees-de-30-millions-de-clients-de-deutsche-telekom-en-acces-libre/>

ZOOM

Chrome, le nouveau bijou de Google

La rumeur filtrait déjà depuis un certain temps, mais le 1^{er} septembre, coup de théâtre : Google annonce officiellement le lancement de son navigateur baptisé « Chrome » (version bêta finale). Le géant de l'Internet garde son humour habituel : c'est par le biais d'un « comic book » (bande dessinée) qu'il communique la nouvelle et explique la raison d'être de ce nouvel outil. Les internautes sont habitués à la créativité débordante de Google puisque les sorties de nouvelles applications (Gmail, Picasa, Calendar, Google Desktop, Google Maps, Google Earth, etc.) sont régulières, mais le lancement d'un navigateur est tout de même un événement.

Il est légitime de se poser les questions suivantes : quelle valeur ajoutée ce navigateur pourrait-il bien apporter ? Quelle place reste-t-il à Google dans ce marché déjà fortement concurrentiel et quel est véritablement son objectif ? Dans une optique de sécurité, on en vient aussi à se poser deux questions supplémentaires : Chrome fera-t-il preuve d'une plus grande robustesse que ses semblables ? Quelle sera la réponse de son éditeur face aux inévitables « 0 days » ? Reste enfin, la question la plus sensible : avec une suite de logiciels constituée de Chrome, google.com, Gmail, GTalk, Google Desktop, Calendar et Picasa, n'est-il pas envisageable que Google soit en mesure de reconstituer le profil complet de ses utilisateurs ? En effet, il détiendrait les conversations, les photos, l'emploi du temps et même les recherches de chacun. Ainsi l'ombre de Big Brother n'est-elle pas en train de s'étendre à l'infini derrière le logo aux quatre couleurs ?

Après une analyse des raisons invoquées par Google pour le lancement de son navigateur, cet article dessine un panorama des fonctionnalités de Chrome et s'efforce de livrer les éléments nécessaires à l'évaluation du pouvoir et des intentions de Google.

Portrait d'un navigateur

Septembre 2008 : c'est au travers d'une bande dessinée humoristique de 39 pages que Google informe le monde de sa nouvelle création.

Dès la première page, la firme expose les raisons qui l'ont poussée à développer ce nouvel outil :

- Internet ayant énormément évolué, il est nécessaire de **repenser le navigateur** complètement
- Les navigateurs ont besoin de davantage de **stabilité** et de **sécurité**
- Ils ont également besoin d'être plus **rapides**
- L'interface doit être **épurée** pour rendre la navigation plus simple.

Afin de répondre à ces exigences, plusieurs nouveaux concepts ont été élaborés.

Rapidité

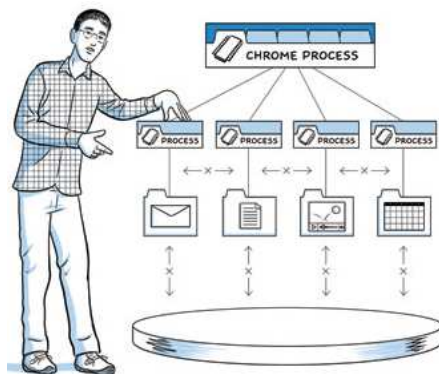
En premier lieu, afin de gagner en stabilité et en rapidité, chaque onglet de navigation est associé à un processus différent (une construction ayant son propre espace mémoire et sa propre copie des structures de données globales). Ainsi lors d'un problème sur une page, les autres onglets ne sont pas affectés.

Étant donné la place prépondérante du JavaScript dans les pages Web, une attention particulière doit être portée à celui-ci afin d'en accélérer le traitement. Pour cela, on intégrera une machine virtuelle JavaScript d'ores et déjà existante chez Google, la V8.

Sécurité

La structure « multithreadée » de Chrome permet d'appliquer des

permissions restrictives sur les processus, formant ainsi une « SandBox ». Les « processus onglet » ont interdiction formelle d'écrire sur le disque et ne peuvent absolument pas communiquer entre eux. C'est le processus principal qui se charge de toute écriture sur disque (ex. : cookies) et des connexions réseau. Cette architecture est illustrée par le dessin ci-dessous.



Sandbox Chrome – Chrome Google Book

Par ailleurs, pour lutter contre le *phishing* et les *malwares*, Chrome intègre un mécanisme intéressant. Il synchronise régulièrement des listes de sites dangereux et notifie l'utilisateur lorsque celui-ci tente d'accéder à l'un d'eux.

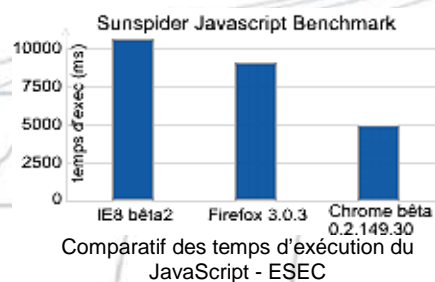
Interface

Deux idées sont à l'origine de la conception de l'interface utilisateur. Premièrement, chaque onglet représentant un processus différent, il est logique que chacun d'eux détienne sa propre barre d'adresse. Deuxièmement, la barre d'adresse doit évoluer et remplir davantage de fonctions. Elle doit permettre de saisir des URL, mais aussi servir de champ de recherche et

représenter un vecteur pratique pour l'affichage de l'historique.

Chrome a été développé pour répondre aux exigences énoncées précédemment. Mais finalement, qu'en est-il des performances obtenues ?

D'après nos constatations, Chrome est sans conteste l'un des navigateurs les plus rapides. Par exemple, son moteur JavaScript V8 est extrêmement performant comme le montre le graphique ci-dessous.



Cependant, l'architecture « multithreadée » de Chrome comporte un défaut notoire : une consommation élevée en mémoire vive. En effet, « à vide », Chrome consomme 32Mo de mémoire contre 27Mo pour Firefox3. Mais, c'est lorsque l'on ouvre de nombreux onglets que les choses se gâtent, puisque chacun d'eux crée un processus individuel avec son espace mémoire. Lors de l'ouverture de 10 onglets identiques sur Chrome, 260Mo de mémoire sont utilisés alors que pour le même nombre d'onglets, Firefox3 en consomme 120Mo. Par contre, Chrome gère mieux la libération et la réutilisation de la mémoire : en fermant les onglets, on revient à la consommation initiale (32Mo) alors que pour Firefox3, on redescend difficilement à 65Mo.

Côté sécurité, il est essentiel d'analyser la robustesse de la SandBox de Chrome. Gynvael Coldwind a posté sur son blog une analyse intéressante, dans laquelle il étudie les propriétés des processus créés : tokens, job objects, alternate desktops et integrity levels (voir encadré ci-contre « Sécurité des processus sous Windows »). Ceux-ci sont générés avec un jeton contenant seulement deux SIDs : le Logon SID et le NULL SID ; tous les autres sont positionnés à « deny » et l'ensemble des privilèges a été supprimé. En ce qui concerne les Job Objects, tout ce qu'il est possible de restreindre est restreint : Handles, Desktop, Clipboard, etc. Afin d'empêcher les processus associés aux onglets de communiquer avec d'autres processus, ils sont créés à l'intérieur d'un autre bureau nommé ChromeRendererDesktop. Pour les utilisateurs de Vista, le niveau d'intégrité des processus créés est positionné au minimum. Actuellement, cette architecture peut être considérée comme relativement efficace dans la lutte contre les malwares, qui était depuis le début un des objectifs visés par Google (voir illustration ci-dessous). Il s'agit, quoi qu'il en soit, d'une piste intéressante qui reprend les principes utilisés dans les machines virtuelles (cloisonnement).



Chrome et la sécurité – Chrome Google Book

Du côté des déceptions, on trouve l'interface utilisateur. À vouloir alléger celle-ci, nombre d'internautes ayant essayé l'application ont l'impression qu'elle a été trop dépouillée. Aussi, l'OmniBox (la barre d'adresse qui fait aussi office de barre de recherche et d'historique) n'a pas rencontré le succès escompté, les utilisateurs se plaignant de la confusion que cela apporte. Ajoutons aussi que le navigateur ne supporte que la version 6.10 beta de Java, et qu'il est lent lors du traitement des vidéos.

Depuis le 1^{er} septembre

Dès son lancement, Google Chrome a subi des tests de vulnérabilités poussés. Plusieurs failles de sécurité dont une grande partie de dénis de service

(« Remote DOS ») ainsi qu'un débordement de tampon et un transfert de fichier masqué ont été débusqués. Google n'a réagi que le 5 septembre (soit 4 jours après la sortie) en publiant la version 0.2.149.29 de son logiciel. Le changelog de cette version, repris ci-dessous, indique d'ailleurs la correction de trois failles de sécurité :

- Fix a buffer overflow vulnerability in handling long filenames that display in the Save As... dialog.
 - Fix a buffer overflow vulnerability in handling link targets displayed in the status area when the user hovers over a link. This is a critical risk that could lead to execution of arbitrary code.
 - Fix an out-of-bounds memory read when parsing URLs ending with :%. This is a low risk that can be used to crash the entire browser, possibly causing loss of data in the current session.

Le 17 septembre, c'est au tour de la version 0.2.149.30 de faire son apparition. Le changelog de celle-ci nous informe de la correction d'une seule et unique faille de sécurité :

- Fix a potential denial of service with very long title attributes on tags. The title attribute sets the tooltip text when you hover the mouse over an element.

Depuis, d'autres vulnérabilités ont été découvertes sans qu'aucun correctif n'ait été publié (cf. Chronologie des vulnérabilités ci-dessous).

Les « known issues » du support de Chrome livrent également des informations précieuses. Notamment, il est intéressant de constater que l'équipe de développement est incapable de fournir un correctif au problème de mauvaise gestion de l'authentification SSL.

Au final, il semble que le nouvel arrivant ne puisse pas encore jouer dans la cour des grands et que, pour l'instant, son éditeur ne soit pas prêt à porter une attention particulière à son développement. Par ailleurs, Le SGDN (Secrétariat Général à la Défense Nationale) a déconseillé son utilisation en entreprise, en attendant une version finalisée. Cependant, il serait injuste de condamner ce produit certes inachevé, mais très prometteur.

Quelle confiance peut-on avoir ?

La première question que l'on se pose porte bien évidemment sur le nombre et la précision des informations collectées par Google. Cependant, une autre atteinte à la vie privée et à la propriété

SECURITE DES PROCESSUS SOUS WINDOWS

Tokens

Un « token » (jeton) est un objet décrivant le contexte de sécurité d'un processus. Les informations contenues dans un jeton comprennent l'identité et les privilèges du compte utilisateur associé au processus. Lorsqu'un processus essaie d'accéder à un objet, le système vérifie ses permissions grâce aux jetons que ce processus possède.

Job Objects

Un « job object » est en quelque sorte une manière de grouper des processus afin de les gérer plus facilement. Notamment, il permet d'appliquer des restrictions sur les éléments suivants : Desktop, Display Settings, Exit Windows, Global Atmos, Handles, Read Clipboard, Write Clipboard, System Parameters.

Desktops

Un « desktop » (bureau) dispose d'une surface définie et contient des objets tels que des fenêtres, des menus, des « hooks », etc. Bien qu'un seul bureau ne soit visible à l'utilisateur (c'est le bureau Winsta0, ouvert lors de l'authentification à l'hôte), d'autres bureaux – invisibles ceux-là – peuvent exister parallèlement, c'est le cas du bureau Winlogon que l'on aperçoit lorsque l'on exécute la séquence CTRL-ALT-SUPPR. Ce mécanisme présente un intérêt autre que graphique : le cloisonnement des processus. En effet, les processus appartenant à des bureaux différents ne peuvent pas communiquer entre eux.

Integrity levels

Ce mécanisme n'existe actuellement que sous Windows Vista. Il permet d'affecter aux processus un niveau d'intégrité, sorte de note appliquée en fonction du niveau de confiance que l'on accorde à un processus. Plus le niveau d'intégrité d'un processus est bas, moins il a de droits.

intellectuelle s'est silencieusement glissée dans les conditions d'utilisation du navigateur.

En effet, la section 11 de ce document relative aux licences liées aux contenus générés avec Chrome stipule que Google s'octroie « une licence perpétuelle, irrévocable, mondiale, sans royalties et non exclusive pour reproduire, adapter, modifier, traduire, publier, présenter en public et distribuer n'importe quel contenu ». Dans le cadre d'un navigateur, cela semble absurde. C'est un peu comme si l'oculiste réclamait des droits sur tout ce qu'une personne pourrait lire grâce à ses lunettes. Cependant, arguant un oubli lié aux conditions d'utilisation génériques appliquées à l'ensemble de ses produits,

Septembre	
01	Annonce de lancement
02	Lancement de Google Chrome (bêta finale, version 0.2.149.27)
03	- Malicious link Dos 0.2.149.27 - SecurityFocus BID 30987 - Automatic File Download Part One 0.2.149.27 - SecurityFocus BID 31000 - Malformed 'title' tag Dos (Bad WebKit) 0.2.149.27 - SecurityFocus BID 30975. aviv.raffon.net
04	- Malformed Attachment Filename Dos 0.2.149.27 - SecurityFocus BID 31031
05	- SaveAs Remote BOF Exploit 0.2.149.27 - SecurityFocus BID 31029 - a href Dos (Bad Boundary Check) 0.2.149.27 - SecurityFocus BID 31034 - Inspect Element Remote Dos - SecurityFocus BID 31038 - Malformed 'view-source' HTTP Header Remote Dos 0.2.149.27 - SecurityFocus BID 31035
08	- Automatic File Download Part Two 0.2.149.27, 0.2.149.29 www.websecurity.com.ua/2423
23	- Carriage Return Remote Dos 0.2.149.29, 0.2.149.30 - SecurityFocus BID 31375
27	- Google Chrome Window Suppressing Remote Dos 0.2.149.27, 0.2.149.29, 0.2.149.30 - Milworm 6609
Octobre	
06	- Google Chrome XSS 0.2.149.30 www.websecurity.com.ua/2505

Chrome : chronologie des vulnérabilités

Google s'est empressé de modifier l'article dérangeant.

Comment s'assurer qu'aucune donnée personnelle, pas même les recherches, n'est transmise aux serveurs de Google ? La réponse d'un expert en sécurité de l'information est la suivante : il faut tout d'abord observer l'ensemble des données émises et reçues par le navigateur afin d'en vérifier la pertinence en utilisant des logiciels spécialisés. Ensuite, le code source du logiciel peut être analysé. Néanmoins, Chrome n'est pas réellement Open Source : c'est une version modifiée appelée Chromium qui est distribuée. Dans tous les cas, ces études prennent du temps et l'on n'est pas à l'abri d'une analyse incomplète.

En attendant, d'après le blog de Matt Cutts (chef de l'équipe « Webspam » chez Google), les seules informations échangées entre Chrome et les serveurs de Google sont les suivantes :

- Chrome vérifie la présence de mises à jour toutes les 24 heures
- Les listes de sites dangereux (malwares, phishing) sont synchronisées toutes les 25 heures
- Les serveurs sont informés de toute erreur 404 rencontrée par l'internaute
- Toute recherche effectuée au travers de l'omnibox est envoyée aux serveurs

Google afin de calculer les suggestions de recherche

Ce dernier point est litigieux. En effet, il existe donc une communication de la totalité des « déplacements » de l'internaute sur la toile vers Google. Un article écrit par Ina Fried sur le site CNET indique que Google conserve 2% de ces recherches et les associe à l'adresse IP de l'internaute. Il est bien entendu possible de désactiver cette fonctionnalité en décochant le service de suggestion dans le menu « options ». Pourtant, l'autorité allemande de sûreté de l'information (BSI) n'a pas hésité à déconseiller l'utilisation du navigateur en affirmant que l'accumulation de ce genre de données par un même fournisseur posait problème. Ce courant de pensée qui vise à protéger la vie privée semble tout de même déranger Google puisque Matt Cutts n'hésite pas à qualifier les personnes qui y adhèrent de « théoriciens de la conspiration ».

Un élément plutôt étrange vient encore ternir l'image bienfaitrice de Google : à chaque installation de Chrome est affecté un identifiant unique. Même si la méthode n'est pas nouvelle, car Google Desktop est aussi muni d'un tel dispositif, elle n'en reste pas moins inquiétante. Cela permettrait au géant de conserver

une « fiche » dans laquelle serait renseigné l'ensemble des recherches effectuées par l'internaute et éventuellement ses données Gmail, Picasa, Facebook et autres produits Google. La firme se défend d'utiliser de telles méthodes, mais il est important de prendre conscience que cela lui serait extrêmement facile. Toutefois, les forces de protection du droit à l'anonymat et à la vie privée ont vite trouvé une parade à ce problème : elle se nomme *UnChrome*. Cette version patchée de Chrome remplace l'identifiant gênant par une séquence de valeurs nulles.

Ajoutons que la désinstallation du navigateur n'est pas complète, car ni l'identifiant unique ni le Google Updater ne sont supprimés. Une entrée vers celui-ci se situe toujours dans la clé `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run` ce qui a pour effet de lancer ce programme à chaque démarrage. Que peut-il bien mettre à jour ?

Afin de réellement compléter la désinstallation, il faut exécuter le programme `GoogleUpdate.exe` avec l'option « `--uninstall` ». Mais toute cette procédure est étrangement bien cachée...

Sur le plan des performances, Chrome a certainement sa place aux côtés des navigateurs de renom. Il introduit de nouveaux concepts qui, bien que perfectibles, ont le mérite d'obliger les éditeurs traditionnels à innover. C'est plutôt du côté de l'atteinte à la vie privée qu'un problème se pose. Les erreurs avouées esquissent l'ombre d'un acteur omniscient sur la scène planétaire. Cependant, l'utilisateur a la possibilité de faire un choix dans une liste toujours croissante de navigateurs (Microsoft Internet Explorer, Mozilla Firefox, Opera Software Opera, Apple Safari, Google Chrome, et d'autres) et ainsi rester maître des informations qu'il diffuse.

Pour aller plus loin :

- <http://www.google.com/googlebooks/chrome/index.html> (le "comic book")
- <http://www.google.com/support/chrome>, <http://chromevoice.com>
- <http://chromekb.com>, <http://www.milworm.com>
- <http://gynvael.coldwind.pl/?id=49>, <http://www.mattcutts.com/blog>



ESSENTIEL

La mutualisation des réseaux industriel et bureautique

Au-delà de la possibilité d'interconnecter leurs différents réseaux locaux industriels (RLI) et bureautiques (Intranet), certaines entreprises s'interrogent sur l'opportunité de les mutualiser. Cette démarche entraîne une réflexion profonde dont le résultat peut avoir des impacts sur chaque infrastructure et aboutir à une confrontation entre des métiers jusqu'alors séparés par nature. D'un côté l'Intranet sous la responsabilité du directeur du système d'information (DSI), de l'autre le RLI sous la responsabilité du responsable de la production (RP). La gestion de la sécurité du RLI est, lorsqu'elle existe, fréquemment déléguée à l'équipe de supervision du processus industriel ou à l'automatisme. Les prérogatives sont donc différentes, mais complémentaires au sein de l'entreprise. Cet article propose une vision de la mutualisation sous l'angle de la sécurité de l'infrastructure informatique résultante, à savoir, le Système d'Information d'Entreprise (SIE).

Origine du besoin de mutualisation

Pourquoi mutualiser¹ les infrastructures des réseaux industriel et bureautique de l'entreprise ?

Les RLI sont indispensables dans tous les systèmes de production automatisés. Quant aux réseaux bureautiques, la question ne se pose plus depuis longtemps.

La question de la mutualisation naît naturellement avec la concomitance de métiers, usages ou fonctions qui sont ou deviennent similaires au sein de l'entreprise :

- **les services et métiers** associés aux réseaux de l'entreprise (exploitation, supervision, gestion de la sécurité et maintenance)
- **les technologies** pour transporter et échanger des données (Ethernet, TCP/IP...)
- **les moyens** pour réaliser l'activité (poste de travail commun : PC, outils bureautiques, navigateur...)
- **les obligations légales**, respect des lois, réglementations et normes.

La jointure, et donc l'émergence du besoin, s'effectue généralement lorsque tous les facteurs coût, délai et qualité peuvent, de façon cohérente, être remis en question et sources de profit.

La mutualisation peut représenter un axe d'optimisation de toutes les activités connexes aux infrastructures industrielles et bureautiques de l'entreprise et, *in fine*, source de réduction des coûts associés.

Par sa nature, cette démarche peut provoquer une révolution culturelle. Elle confronte deux univers (industriel et bureautique) jusqu'alors séparés ou connectés, avec les précautions d'usages et dont les contraintes (technique, fonctionnelle et organisationnelle) sont, *a priori*, intrinsèquement différentes.

La Figure 1, ci-contre, illustre les différences de priorité des deux types de réseau.

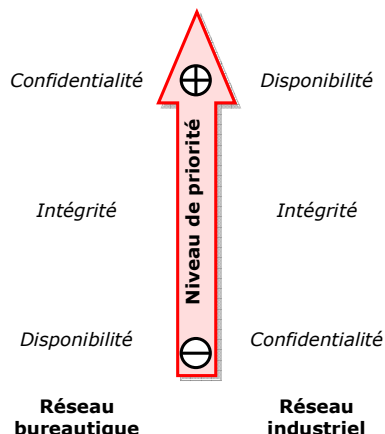


Figure 1 : Différence de priorité des réseaux industriel et bureautique

La réflexion qui aboutit à la mutualisation n'est pas univoque. Elle ne se cantonne pas à une comparaison technico-technique dont le but est de trouver des similitudes entre les réseaux.

Dans le monde des RLI les équipementiers sont traditionnellement enclins à opacifier leurs solutions. Ils sont toutefois amenés progressivement à les adapter aux exigences d'interopérabilités (réseaux ou applicatifs) des entreprises. Ce besoin accélère l'ouverture et la standardisation. L'adhésion des constructeurs provoque l'effet de masse nécessaire à la réduction des coûts de production.

De par leur conception, les RLI n'étaient pas sujets aux menaces connues dans les réseaux bureautiques. Mais leur interconnexion avec le reste de l'entreprise a occasionné une première évolution. La plupart s'appuyaient sur des protocoles propriétaires. Aujourd'hui ces protocoles (DNP3 : Distributed Network Protocol ; Modbus TCP ; ProfiNet ; HSE : High Speed Ethernet ; BACnet/IP) ont évolué et permettent des connexions directes avec l'Intranet de l'entreprise via TCP/IP.

L'illustration pragmatique du besoin de mutualisation apparaît notamment au sein des entreprises industrielles qui utilisent le système SCADA (Supervisory Control and Data Acquisition). Cette plate-forme rassemble de nombreux composants destinés à l'acquisition des données, la commande, le contrôle et la

supervision des organes impliqués dans les process industriels.

SCADA intervient notamment dans des environnements et des systèmes critiques tels que :

- la production, le traitement, le transport ou le stockage de matière (pétrole, gaz...)
- la fabrication (centrale nucléaire) et le transport de l'énergie électrique
- la gestion du transport, ferroviaire, aérien ou automobile
- les usines de traitement des eaux et autres matières plus ou moins dangereuses.

SCADA peut s'interconnecter au réseau de l'entreprise et donc, potentiellement, au réseau mondial Internet. Ce qui le rend potentiellement accessible depuis n'importe quel point de la planète. S'ajoutent à cela, les avantages que procurent les accès sans-fil (wi-fi) ou encore la mobilité (nomadisme) offerte aux utilisateurs. Cette capacité, utile au demeurant, introduit également son cortège de menaces conduisant à redéfinir complètement la sécurité de ce type de réseau jusqu'alors plus ou moins épargné.

Les risques, menaces, vulnérabilités et impacts

Les systèmes SCADA sont donc devenus vulnérables aux mêmes menaces et attaques que les réseaux sur lesquels ils s'appuient.

Ils peuvent, de surcroît, être la cible de malveillances dont les impacts directs ou collatéraux peuvent avoir de lourdes conséquences.

L'absence de sécurité, notamment sur d'anciens systèmes SCADA ou plus prosaïquement par négligence, peut se traduire par des conséquences pour les entreprises et les populations telles que :

- des coupures d'électricité dans des villes entières
- l'explosion d'une usine (raffinerie de pétrole par exemple)
- la pollution des eaux potables
- l'arrêt d'une chaîne de production critique.

Les enjeux d'une bonne sécurité sont donc importants et peuvent être de natures différentes en fonction des

¹ **Mutualiser** : action qui consiste à regrouper les moyens, les connaissances et les savoir-faire afin d'en tirer des avantages économiques...



entreprises concernées (juridiques, réglementaires, législatifs, financiers, écologiques ou morales (réputation, image de marque de l'entreprise)).

Le nombre d'attaques contre les RLI n'a cessé de croître depuis le début des années 2000. De nombreux incidents dus à des actes volontaires nous rappellent leur fragilité :

- 2005 - USA : Le ver Zotob provoque l'arrêt de 13 usines d'assemblage de véhicule aux USA.
- 2007 - USA : une erreur de commande provoque la contamination accidentelle par hydroxyde de sodium des eaux de ville. Conséquences, des dizaines de victimes et des blessés graves dans le Michigan.
- 2008 - Pologne : prise de contrôle du système de signalisation ferroviaire et déraillement de 4 wagons qui fait plusieurs blessés.

Les aspects légaux

Les États-Unis restent le pays le plus touché par ces attaques. À tel point que le problème a été traité au plus haut niveau de l'État qui a émis des directives :

- « PDD-63 : Presidential Decision Directives » publiée en mai 1998 sous l'égide du président Clinton.
- « HSPD-7 : Homeland Security Presidential Directive No. 7 », qui est une mise à jour de la PDD-63, publiée en 2003 par George W. Bush.

Le gouvernement français a également pris la mesure de ces menaces par l'application du décret n° 2006-212 du 23 février 2006 relatif à la Sécurité des Activités d'Importance Vitale (SAIV).

Ce décret s'adresse à toutes les organisations publiques ou privées exploitant des établissements ou utilisant des installations et ouvrages dont l'indisponibilité, la destruction ou l'avarie pourraient avoir des conséquences graves, telles que :

- la diminution importante du potentiel industriel militaire ou économique
- la réduction du niveau de sécurité ou de la capacité de survie de la Nation
- la mise en danger de la population.

Ces organisations sont tenues de coopérer à la protection de leurs établissements, installations ou ouvrages contre toute menace, notamment à caractère terroriste.

Le décret précise la notion d'opérateur d'importance vitale et identifie les SAIV. Une directive est définie par secteur d'activité nationale de sécurité et élaborée sous la responsabilité d'un ministre. La directive permet à chaque entité d'élaborer des plans de sécurité couvrant leurs activités, puis des plans particuliers de protection de chacun de leurs points d'importance vitale. La

Figure 2, ci-dessous, illustre cette déclinaison.

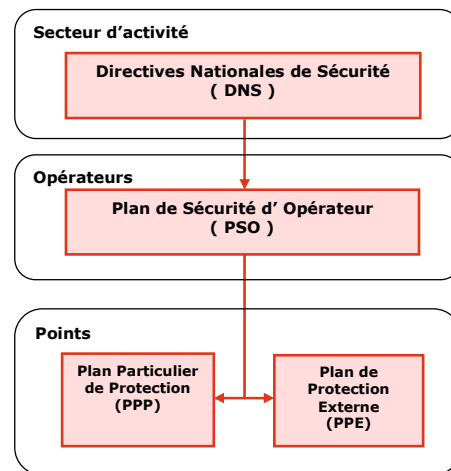


Figure 2 : Déclinaison du décret SAIV

Ce dispositif s'inscrit dans la logique du plan Vigipirate. Il permet à l'État de s'assurer que l'ensemble des opérateurs désignés d'importance vitale prendra des dispositions cohérentes avec celles que le gouvernement aura lui-même arrêtées ou recommandées.

Cependant, les entreprises ne disposent pas toujours des compétences nécessaires pour conduire ce type projet.

Mutualisation et sécurité

Tous projets industriels, de mutualisation ou non, comportent une composante sécurité qui répond à des objectifs destinés à réduire des risques identifiés par une analyse de risque. Analyse qui tient compte des caractéristiques intrinsèques de chaque contexte en plus de celui qui résultera de la cohabitation.

L'évaluation des risques s'effectue par une classification des impacts qui seront fonctions du domaine industriel et de la portée du service rendu (locale, régionale, nationale ou internationale).

L'autre étape intimement liée à la sécurité est la conception de l'architecture résultante.

Cette infrastructure tient compte des résultats de l'analyse. L'architecture résultante doit répondre à des objectifs précis afin de réduire les risques au niveau résiduel défini en amont. L'étanchéité des droits doit être garantie entre les différents acteurs et profils qui accèdent aux machines (administrateur, régulateur, superviseur, développeur ou mainteneur). Il est entendu que ces règles ne s'appliquent qu'avec des applications qui le permettent. Les accès distants au RLI doivent être contrôlés. C'est le cas par exemple de la télémaintenance qui doit faire l'objet d'une attention particulière. Le poste de travail du fournisseur qui se connecte au RLI doit faire l'objet d'un processus de validation strict. Les contraintes de

production impliquent souvent que le RLI soit physiquement isolable de tous les autres réseaux. La fonction d'isolation doit être validée par le DSI, le RP et faire l'objet d'une procédure validée.

Enfin, il faut informer, former et organiser la gestion et le suivi de la sécurité à l'aide d'indicateurs clés.

Les questions préliminaires

La mutualisation engendre naturellement de nombreuses questions.

Quels sont les gains potentiels ?

Bien entendu, la réponse sera différente en fonction de l'entreprise considérée. Toutefois, on peut citer quelques postes de réduction possible : parc d'équipement de l'infrastructure, coûts d'acquisition et de maintenance associés, optimisation des équipes d'exploitation et de supervision de l'infrastructure globale, coûts associés à la télémaintenance...

Quelles sont les menaces associées ?

Ce sont les mêmes menaces qui pèsent sur le réseau bureautique.

Comment assurer un niveau de sécurité acceptable pour le nouvel ensemble mutualisé ?

Le niveau de sécurité résultant sera issu d'une évaluation préalable des niveaux requis de part et d'autre (avant mutualisation) ainsi que des nouveaux besoins de sécurité engendrés par la mutualisation.

Quels investissements consentir ?

La réponse à cette question dépend évidemment du contexte de l'entreprise, de sa maturité sécuritaire et des objectifs y afférant.

Quelle démarche adopter pour mutualiser ?

La démarche de mutualisation s'effectue selon une méthodologie pensée et adaptée à cet objectif. Tous les vecteurs (techniques, fonctionnels, économiques ou organisationnels) doivent faire l'objet d'une étude préalable. L'étude, effectuée auprès des acteurs concernés, prendra en compte les contraintes et les spécificités des parties impliquées. Le but étant d'obtenir une grille de comparaison susceptible de révéler des compatibilités ou, inversement, des objections suffisamment fortes pour contrecarrer le scénario de mutualisation.

La Figure 3 décrit une étape de recherche de compatibilités techniques entre les réseaux.

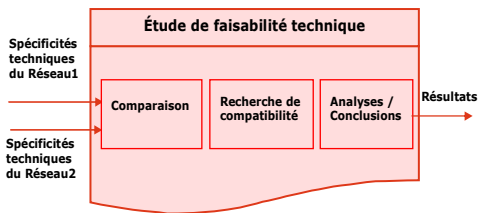


Figure 3 : Étude de faisabilité technique

L'audit sera suivi d'une analyse sous forme de scénario qui permettra d'établir la pertinence, étayée par des avantages et inconvénients spécifiques, ou le rejet pur et simple de la mutualisation envisagée.

Le principal vecteur de mutualisation auquel on pense instinctivement est l'infrastructure technique (câblage, hubs, switchs, routeurs, annuaire LDAP ou AD, DNS...).

Cependant, le vecteur technique n'est pas le seul axe de mutualisation. D'autres voies, souvent indirectes, peuvent être sources de gains. Un scénario de mutualisation financière peut s'appliquer à des postes de dépenses de licence logicielle d'application utilisées de part et d'autre.

La Figure 4, ci-dessous, illustre un scénario possible pour établir une mutualisation financière sur une fonction commune aux deux réseaux.

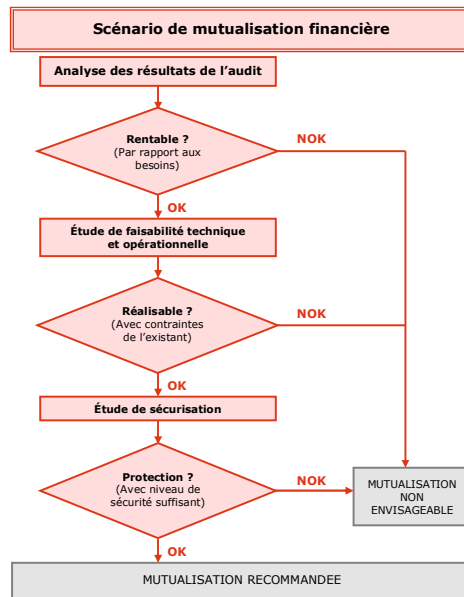


Figure 4: Exemple de scénario de mutualisation financière

Et après ...

Lorsque la recommandation est la conclusion d'un scénario de mutualisation, sa mise en œuvre peut engendrer des bouleversements organisationnels, fonctionnels et techniques au sein des services impactés. Il peut donc s'avérer indispensable de procéder à une phase d'accompagnement pour :

- mettre en place les éventuels nouveaux processus et procédures opérationnels
- s'assurer de la cohérence des différentes fonctions support
- former les personnels d'exploitation ;
- garantir le niveau de sécurité (au sens large) du nouvel ensemble
- mettre à jour ou adapter le référentiel documentaire de l'entreprise (procédure d'exploitation et de maintenance, Politique de Sécurité...).

Pour aller plus loin :

Un livre :

- « Réseaux Locaux Industriels » par Pascal VRIGNAT, édition Gaëtan MORIN (1999).

La méthode EBIOS :

- <http://www.ssi.gouv.fr/fr/confiance/ebiospresentation.html>

Le système SCADA :

- <http://ref.web.cern.ch/ref/CERN/CNL/2000/003/scada/>
- [http://www.itoc.usma.edu/Workshop/2005/Papers/Follow_ups/WP_IEEE_\(Jun_2005\)_-Next_Gen_SCADA_Security.pdf](http://www.itoc.usma.edu/Workshop/2005/Papers/Follow_ups/WP_IEEE_(Jun_2005)_-Next_Gen_SCADA_Security.pdf)
- http://www.isa.org/filestore/Division_TechPapers/GlassCeramics/TP04AUTOW_046.pdf

Décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale.

- <http://www.legifrance.gouv.fr>

La mutualisation n'est pas une fin en soi. Derrière ce concept, trop souvent associé à la technique, se cache une véritable démarche de recherche d'amélioration et de coopération entre les processus et les métiers de l'entreprise industrielle. In fine, cela permet dans le meilleur des cas, où des scénarii de mutualisation ont pu être trouvés, d'améliorer la productivité et donc atteindre l'objectif initial : trouver des avantages économiques. Si aucun scénario de mutualisation n'a pu aboutir, le travail de remise en question du modèle technique, fonctionnel, organisationnel ou économique des infrastructures industrielle et bureautique constitue indéniablement une démarche de progrès.



Réagissez aux articles de la newsletter sur le blog de l'ESEC :

<http://esec.fr.sogeti.com/blog>

Inscription à la Newsletter : newsletter-subscribe@esec.fr.sogeti.com

Désinscription : newsletter-unsubscribe@esec.fr.sogeti.com

Agence ESEC

Sogeti Infrastructures Services

6-8 rue Duret 75016 Paris - France

Tél. : +33 (0)1 58 44 26 79

Site : <http://esec.fr.sogeti.com>

Mail : esec@esec.fr.sogeti.com

Société par Actions Simplifiées au capital de 15 999 790 € - RCS Paris 479 942 583

Conformément à la loi « Informatique et libertés » du 6 janvier 1978, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez vous adresser au directeur de l'agence ESEC.

Sogeti ne peut être tenue pour responsable en cas avéré de détournement des liens communiqués à titre d'illustration dans ses propos.

Cette newsletter a été réalisée par des consultants sécurité de l'agence **ESEC**.

Responsable de la publication : Edouard **JEANSON**

Auteurs :

- Cyprien **CLERC**
- Claude **AMIENS**

Rédacteur en chef : Nicolas **VINCENT**

Relecteurs :

- Jean-Baptiste **BEDRUNE**
- Alexandre **GAZET**
- François-René **HAMELIN**
- Margaret **MONTANARO**
- Marie-Céline **MUSSARD**
- Anthony **ROBINSON**
- Eric **SAVIGNAC**

