Audit d'un système d'information : principales vulnérabilités

Céline Estieux and Laurent Estieux

Secrétariat Général de la Défense Nationale
Direction Centrale de la Sécurité des Systèmes d'Information
celine.estieux@sgdn.pm.gouv.fr
laurent.estieux@sgdn.pm.gouv.fr

Résumé Cet article a pour objectif de présenter plusieurs vulnérabilités relevées lors des audits menés par le bureau audits de la DCSSI. Il ne prétend donc pas être exhaustif, mais synthétise les résultats rencontrés lors d'audits menés durant quatre années auprès de plusieurs administrations. Ce constat semble d'ailleurs être le même dans tous les secteurs, de l'avis de sociétés auditées comme de sociétés auditrices. Cet article décrira donc rapidement le bureau audits et ses prestations réalisées pour ensuite couvrir de manière un peu plus approfondie les vulnérabilités rencontrées, en les regroupant en trois catégories principales : vulnérabilités liées aux problèmes organisationnels, techniques et humains.

1 Brève présentation du bureau audits

Le bureau audits a réalisé ses premières prestations en 2001, année de sa création au sein de la DCSSI. Il se compose actuellement de six personnes, et va, d'ici à la fin de l'année, voir son effectif passer à 8 personnes.

Il peut intervenir sur l'ensemble des administrations françaises. Il n'agit cependant que sur saisine officielle de l'entité requérant un audit de son système d'information (SI).

Les interventions du bureau couvrent trois domaines distincts : la sécurité logique (passerelles, réseau interne, SI dans son ensemble, ...), la sécurité physique des locaux (avec le SI pour objectif) et la sécurité des autocommutateurs téléphoniques (PABX).

Les prestations du bureau sont essentiellement liées à l'audit, même si parfois elles peuvent également être plus larges (conseils lors d'applications de recommandations par exemple). Les prestations d'audits sont également au nombre de trois :

- tests d'intrusion : externes en boîte blanche (avec connaissance préalable de la cible) ou noire (sans aucune connaissance de la cible) et internes en boîte blanche uniquement[1] ;

[1] Les tests d'intrusion internes sont destinés à simuler une attaque interne et il est donc plus réaliste de considérer qu'une personne interne a déjà une bonne idée du réseau sur lequel elle se trouve.

- audit dit « de premier niveau » : cette prestation a un champ d'application très large, mais elle est moins profonde techniquement que d'autres types de prestations. Elle est destinée à donner une image cohérente des mesures de sécurité appliquées afin de ne pas focaliser sur des points particuliers et avoir une sécurité homogène ;
- expertise technique approfondie : à l'opposé de la prestation précédente, l'expertise approfondie couvre un point très particulier et l'analyse en profondeur. Les systèmes audités pourront par exemple être des pare-feu, des serveurs web, ...

2 Problèmes organisationnels

Les vulnérabilités liées à l'organisation peuvent à première vue, tout du moins pour une personne très technique, être considérées comme secondaires face à l'étendue des problèmes techniques voire humains. Il n'en est rien cependant. C'est tout au contraire le premier problème à régler, dont toute la sécurité du SI dépendra.

Pour comprendre ce problème, on peut par exemple imaginer un cas concret très simple. Prenons le cas hypothétique d'une petite entité composée d'une équipe informatique restreinte avec peu de moyens. Ils gèrent donc tout le SI, administration et sécurité incluses. Cette entité a, de plus, de fortes contraintes de disponibilité. Si un serveur ne fonctionne plus à cause d'un problème logiciel, la première réaction de l'administrateur sera de réinstaller le serveur, même s'il suspecte une compromission de celui-ci. La cause du problème n'aura pas été traitée, le problème est ainsi susceptible de réapparaître par la suite. De plus si une compromission a réellement eu lieu, il est utile et nécessaire de laisser la machine en l'état afin de faire des constations plus avancées sur les causes de la compromission et ses conséquences.

2.1 Organisation de la SSI inefficace

Le premier problème lié à l'organisation sera donc une organisation de la SSI inefficace voire inexistante dans le pire des cas. Si personne n'est chargé spécifiquement de la sécurité, aucune décision concernant la SSI ne pourra être prise de manière indépendante. On ne sait pas en particulier qui va trancher lorsqu'une décision devra être prise ni quelles vont être ces décisions, et donc si elles seront prises pour garantir une sécurité optimale ou pour un besoin de fonctionnement. Il ne faut donc pas qu'il y ait des conflits d'intérêts pour les postes liés à la SSI. Il est pourtant extrêmement fréquent de rencontrer des équipes où le responsable de l'équipe d'administration du SI est également celui qui est chargé de la sécurité, ce qui ne permet pas de prendre des décisions indépendantes pour la sécurité du système.

Il faut également que les responsabilités liées aux personnes gérant la SSI soient réelles et correctement appliquées. Lors de certains audits, nous avons parfois réalisé une analyse complète du site sans que la personne censée gérer la sécurité (le RSSI local) ne soit impliquée...

2.2 Absence de prise en compte de la SSI dans les grands projets

Un deuxième problème concerne l'intervention inexistante ou trop tardive de la SSI dans le processus de décision. Lorsque de gros projets sont gérés, qu'ils concernent l'informatique ou non, la SSI est souvent oubliée ou perçue comme une contrainte tellement lourde qu'elle sera gérée *a posteriori* dans le meilleur des cas. Un exemple simple est le déménagement d'une entité dans un bâtiment distant. La salle serveur va donc être relocalisée dans un nouvel emplacement, et si la sécurité n'a pas été prise en compte, on peut se retrouver, dans un cas extrême, avec un projet de déménagement de la salle serveur dans une salle en rez-de-chaussée avec des ouvertures donnant sur un parking public.

2.3 Gestion de la sous-traitance

On peut enfin aborder la sous-traitance qui n'est pas toujours maîtrisée comme elle devrait l'être, et ceci à deux titres. Le premier concerne le recours à la sous-traitance via des appels d'offres et le second concerne le suivi des prestataires externes.

Dans le premier cas, le recours à la sous-traitance se fait généralement parce qu'il n'y a pas de temps ou de compétences suffisantes afin de mener le projet à son terme. Il ne faut toutefois pas oublier que ces éléments sont absolument nécessaires lors de la définition, du suivi et de la recette du projet afin de profiter pleinement de celui-ci et de s'assurer qu'il correspond aux attentes du client. Les ressources en interne peuvent ne pas être suffisantes ou n'avoir pas le recul, les connaissances ou la formation nécessaires pour la réalisation de ce projet. Si cela se produit, les équipes internes ne maîtriseront pas ce projet et pourront ne pas le comprendre, le maintenir et surtout se l'approprier.

Le suivi des prestataires externes est également un problème lourd et difficile à gérer si la sécurité n'a pas été prise en compte dès le début de la prestation. À titre d'exemple, si les serveurs d'une entité sont hébergés chez un prestataire externe, et qu'aucune clause d'audit n'a été prévue dans le contrat liant l'entité à ce prestataire, le niveau de sécurité ne pourra être évalué de manière efficace.

2.4 Regard global

Enfin il ne faut pas oublier tous les problèmes d'organisation qui pourront paraître anecdotiques mais qui sont pourtant essentiels pour avoir une sécurité appropriée. L'exemple le plus frappant est peut-être celui de la sécurité des postes informatiques des secrétaires. Sur ces postes transite généralement un grand nombre de documents avec des niveaux de sensibilité différents. Pourtant, la sécurité n'y est quasiment jamais renforcée, car ce n'est pas un dispositif dont le besoin de sécurité apparaît comme primordial. On peut voir ici qu'un auditeur efficace se doit de garder son esprit ouvert et surtout curieux afin de n'écarter aucun domaine *a priori*.

3 Problèmes techniques

3.1 Installation par défaut

De manière à rendre opérationnels leur produits dans le plus grand nombre de configurations possible, les éditeurs ont tendance à fournir des installations par défaut pourvues de nombreuses fonctionnalités. Ces fonctions souvent inutiles sont rarement désinstallées ou configurées correctement par les administrateurs. Ceux-ci ayant bien souvent une maîtrise imparfaite du produit, redoutent que ces modifications perturbent le bon fonctionnement du système. Tout ceci va bien entendu à l'encontre du moindre privilège qui préconise d'enlever toute fonctionnalité inutile.

Lors d'analyses de systèmes de type GNU/Linux, il n'est pas rare de voir des serveurs installés avec des noyaux standards fournis par les éditeurs comportant de nombreux modules dont l'utilité pour un serveur est loin d'être évidente : modules DRM, support cartes sons, support de systèmes de fichiers ésotériques. Ces modules sont d'ailleurs bien souvent chargés sans que l'administrateur ne le sache. Les installateurs graphiques, très conviviaux pour les administrateurs, conduisent à la mise en place de systèmes pourvus d'applications totalement inutiles. Les interfaces graphiques en sont le meilleur exemple du fait que pour rendre un service bien minime à l'administrateur (se rapprocher d'une interface semblable à un poste de travail), ces dernières introduisent tout un ensemble d'applications qu'il n'utilisera pas mais qui sont cependant susceptibles de comporter des bogues de sécurité.

Les systèmes Microsoft, largement déployés, sont eux aussi bien souvent installés sans tenir compte du moindre privilège. Il n'est pas rare de trouver des serveurs équipés de toutes les applications multimédia(WMP), de communications (MSN Messenger) alors qu'elles ne sont d'aucune utilité. Plusieurs de ces fonctions sont également configurées de manière à pouvoir interopérer avec des systèmes désormais obsolètes (Windows NT4.0 par exemple) et ne font que trop rarement l'objet de corrections. On peut citer le stockage des mots de passe sous forme de condensat LanManager (LM), l'autorisation de véhiculer des authentifications avec les protocoles LM, NTLMv1 alors que depuis le système Windows 2000 est utilisé Kerberos (et NTLMv2), la modification des droits d'énumération de l'utilisateur anonyme. Pourtant ces paramétrages sont recommandés par l'éditeur dans ses guides de sécurisation, qui ne sont que trop rarement consultés par les administrateurs.

Globalement, ce schéma se retrouve pour toutes les applications : les systèmes d'exploitations, les applications serveurs mais aussi les applications clientes. Les administrateurs devraient toujours garder à l'esprit que l'éditeur n'a pas défini les paramètres par défaut pour leurs cas particuliers, qu'il ne les a pas délibérément introduit –bien qu'ils en connaissent les défauts en terme de sécurité – mais qu'ils visent uniquement à maximiser les chances de fonctionnement sur un grand nombre d'environnements.

3.2 Gestion des correctifs de sécurité

La gestion de correctifs de sécurité comporte des problématiques connexes qui contribuent généralement aux défauts relevés lors des audits.

Méconnaissance des durées de vies des logiciels La plupart des éditeurs de logiciels ont généralement une politique de maintenance de leurs produits (Lifecycle policy, end-of life, etc.) souvent ignorée des administrateurs. Les produits Microsoft bénéficient d'un support fonctionnel et de sécurité sur une période de 5 ans puis un support gratuit restreint à la sécurité pour une autre durée de 5 ans.

En tenant compte du fait que rares sont les administrateurs à se précipiter sur les technologies nouvelles (au vu des proportions de systèmes Windows 2003, 2000 et NT4) et qu'il est toujours bon d'anticiper l'obsolescence des produits, on peut estimer la durée de vie d'un système donné à environ 5 ans. Pour certaines applications ou autres systèmes d'exploitation, ces durées peuvent varier mais elles sont généralement toujours surestimées dans les projets d'équipement. Un SI est donc nécessairement en perpétuelle évolution et la sécurité d'un produit n'est assurée que durant un temps finalement court. Les administrateurs ne devraient donc pas se laisser rattraper par les « dates limites de consommation » des produits informatiques.

Les audits montrent malheureusement que ce problème n'est généralement pas anticipé et il n'est donc pas rare de voir des systèmes Windows NT4 encore présents (non maintenu depuis Décembre 2004), des distributions GNU/Linux non maintenues et des applications dont on ne sait plus si l'éditeur assure encore la fourniture de correctifs.

Méconnaissance des solutions de déploiement de correctifs Les administrateurs connaissent généralement mal les outils disponibles afin de maintenir à jour leur système d'information. Même si ces outils sont imparfaits, ils apportent une réelle plus-value et doivent donc à ce titre être utilisés.

Il est effectivement trop rare de rencontrer des systèmes d'informations pourvus de « SUS Server » ou de miroirs des distributions GNU/Linux. Ces produits, même s'ils ne permettent pas de gérer l'ensemble des applications d'un système d'information, permettent, à peu de coûts, de maintenir à jour un parc important. Il existe aussi une offre commerciale qui couvre certainement certains points omis par ces outils « gratuits ».

Par contre les administrateurs devraient être conscients des limitations de ces outils afin de gérer eux-mêmes ces points non traités. Sur les systèmes Microsoft, les serveurs SUS ne gèrent qu'un nombre finalement restreint d'applications du seul éditeur Microsoft. Pour les autres applications, qu'elles soient du même éditeur ou d'un autre, l'administrateur doit s'arranger pour que les mises à jour puissent être distribuées par le réseau car sinon il est certain que le SI ne sera pas homogène en terme de correctifs. Sur les systèmes GNU/Linux, il est trop fréquent de constater que les administrateurs, quand ils gèrent de manière

centralisée le déploiement des correctifs, ignorent par exemple, que la mise à jour d'un noyau nécessite un redémarrage du serveur. La durée d'activité d'un serveur (« uptime ») est nécessairement majorée par la durée entre deux publications de correctifs de sécurité sur le noyau.

3.3 Le niveau applicatif

Désormais, quasiment tout le flux applicatif est une application web, c'est-à-dire se repose sur les protocoles HTTP et autres technologies connexes (HTML, PHP, JSP, ASP, etc.). Les avantages sont certains car une seule application, le navigateur, permet de réaliser ce qu'un nombre important d'applications dédiées faisaient auparavant.

Malheureusement, un grand nombre de problèmes se pose car cette nouvelle technologie a amené ses vulnérabilités associées : injection SQL, vol de session, de cookies par failles XSS, etc... Comme les problèmes organisationnels l'ont abordé, il est rare de voir un développement d'applications de ce type accompagné d'un volet sécurité. Sont alors mis en place des outils tels que les sondes de détection d'intrusion, les reverses-proxies qui, comme la plupart des mécanismes à base de signatures, sont pleinement fonctionnels en terme de sécurité lorsqu'ils protègent des technologies largement diffusées (dont on connaît les signatures).

Or les applications web marquent aussi le retour des développements « maison » dont la diffusion se limite à l'usage interne, ce qui ne garantit d'ailleurs pas l'absence de vulnérabilités, et leur éventuelle connaissance par un attaquant. Les dispositifs de protection nécessitent donc d'être personnalisés en fonction des applications à protéger ce qui est rarement le cas.

Les données deviennent donc un flux privilégié d'attaques que la compartimentation réseau, le filtrage de flux et les notions de rupture de protocoles de communication ne peuvent contenir seuls si les données ne sont pas analysées finement.

3.4 Machines de tests oubliées

Lors de la réalisation de tests d'intrusion, il n'est malheureusement pas rare de trouver, directement accessibles à l'attaquant, des machines de tests ou de validation oubliées par les administrateurs. Ces machines ont généralement pour propriété d'être pourvues de mots de passes triviaux et d'être configurées en violation complète du principe de moindre privilège.

En effet ces machines servent à expérimenter des paramétrages, des installations d'applications et de systèmes d'exploitation ; l'administrateur y fait souvent ses armes par tâtonnement. En résulte donc une configuration souvent instable et de nombreuses fonctions installées permettant à un attaquant d'en tirer facilement partie. Parfois même, dans le cas d'applications « web », ces serveurs de tests interagissent avec les mêmes données que les serveurs de production ce qui revêt un intérêt important pour les attaquants.

3.5 Gestion des comptes et mots de passe

Un administrateur consciencieux en terme de sécurité veillera donc à utiliser un système bien configuré, maintenu à jour, mais au final, la clé d'accès au système est généralement un mot de passe choisi librement par l'utilisateur. Et malheureusement, l'utilisateur est rarement consciencieux en terme de sécurité et choisit donc un mot de passe trop facile à découvrir.

L'administrateur est ici partiellement pris en défaut car la plupart des systèmes permettent d'imposer des règles de complexité à l'utilisateur. Malheureusement, les applications utilisent elles aussi des mots de passe et les véhiculent souvent de manière non sécurisée : en clair sur le réseau. Les utilisateurs, comme les administrateurs, recherchent souvent la facilité, construisent un mot de passe complexe mais l'utilisent systématiquement pour l'accès au système, aux applications locales ou distantes et ce mot de passe finit par transiter en clair sur le réseau.

Mais les audits ont tendance à montrer que les administrateurs créent également des comptes de secours avec des mots de passe triviaux. Plus un système d'information est important, en termes de services, utilisateurs ou machines, plus les chances de trouver un mot de passe trivial, tel qu'un mot de passe blanc, sont élevées parfois même sur des comptes importants comme des administrateurs de domaine. Ces défauts peuvent facilement être relevés en utilisant des outils largement diffusés tels que MBSA pour l'éditeur Microsoft.

4 Problèmes humains

Enfin, les problématiques liées au facteur humain sont essentielles dans le traitement de la sécurité. Elles le sont d'autant plus qu'elles sont généralement difficiles à traiter de manière efficace, car chaque personne présente dans le processus introduit un élément différent à traiter. De plus chacune des actions menées dans ce cadre nécessite l'acception complète des personnes impliquées pour que les actions soient traitées efficacement.

4.1 Manque de moyens et de formation

Le premier problème auquel on peut penser est tout simplement le manque de moyens humains ou la réalisation de SSI par des personnels non qualifiés. Le manque de moyens est un problème important qui ne peut pas être résolu par une solution technique miraculeuse, malgré ce que pourraient laisser croire de nombreux revendeurs. Il faut nécessairement avoir des personnes chargées de la SSI en nombre suffisant, et ces personnes devront être formées à tout niveau : administrateurs, responsables, utilisateurs et sur de multiples domaines : produits particuliers, sécurité de manière générale. Le manque de formation amène malheureusement parfois les exploitants à adopter des comportements inadaptés ou à laisser des configurations par défaut sans sécurisation adaptée, comme cela a été détaillé ci-dessus.

4.2 Manque de motivation

La sécurité d'un système repose sur les personnes qui le gèrent et l'utilisent, ces personnes doivent donc être sensibilisées aux problèmes de sécurité afin de pouvoir les appréhender. Le premier niveau consistant simplement à avoir conscience du risque est déjà un premier pas sur le chemin d'une sécurisation efficace.

Le travail de l'équipe chargée de la sécurité est un long travail ingrat. En effet, si la sécurité mise en place est faite de manière efficace, il n'y aura aucun retour quant à l'efficacité des moyens de protection. Au mieux l'équipe de sécurité pourra se targuer d'avoir bloqué des attaques. Les responsables pourront toujours douter et se demander si l'absence de problèmes n'est pas due à une absence d'attaques plutôt qu'à une sécurisation efficace.

Il y a ensuite, comme dans toute équipe, les problèmes interne de gestion d'équipe et la difficulté à réussir à garder une équipe motivée et volontaire même sur des tâches longues et ennuyeuses, comme la lecture des fichiers journaux, ou nécessitant une discipline rigoureuse (stockage des sauvegardes, voire des mots de passe, etc.).

4.3 Excès de confiance envers les produits

Le problème de la confiance intrinsèque dans les produits vient certainement à la fois d'une démarche marketing de fournisseurs de produits désirant vendre ceux-ci et également d'une volonté de régler les problèmes de sécurité d'une manière rapide. Il est en effet plus facile pour un responsable de demander un budget conséquent et d'acheter des produits coûteux, donc efficaces, que de motiver, de former et d'organiser une équipe pour obtenir une prise en compte réelle de la sécurité. Il est tout autant facile pour la personne ayant accordé le budget d'arguer de son montant pour justifier son investissement sur le domaine de la sécurité. Mais il ne faut pas se leurrer et croire au mythe du produit sécurisant la totalité du réseau ou de l'analyseur de journaux intelligent prenant des décisions de manière autonome.

4.4 Besoin de preuves

L'auditeur est également confronté directement à la problématique de l'« humain ». Il est par exemple extrêmement fréquent, lors de la réalisation d'un audit, de voir des membres de l'équipe auditée ne pas accorder foi aux dires de l'auditeur en l'absence de démonstration concrète. Par exemple, si l'auditeur indique qu'une machine n'est pas à jour et comprend une faille permettant de prendre la main dessus à distance, on peut se douter que l'équipe auditée va demander à voir l'exploitation de cette vulnérabilité réalisée, sans quoi l'attaque ne sera pour lui qu'une hypothèse hasardeuse.

Les administrateurs réagissant de cette façon ne seront pas enclins à appliquer les correctifs de sécurité des produits dès leur sortie car ils sont persuadés que l'attaque n'est pas réelle, ou nécessite des moyens trop importants.

4.5 Pas de prise en compte du réel niveau de menaces

Parfois, l'attaque a beau être réalisée et la mise en évidence de la faille établie, l'équipe auditée n'est toujours pas convaincue. L'auditeur apparaît ici comme une personne douée de compétences rares, qui ne pourront pas être mises en œuvre directement sur son réseau, à moins d'un déploiement de moyens absolument démesurés.

Les entités auditées ne réalisent généralement pas le niveau de menace auquel ils peuvent être confrontés et également l'imagination et la persévérance d'un attaquant éventuel. Sans adopter cependant un comportement paranoïaque bloquant et inefficace, il faut rester vigilant quant aux données qu'on veut protéger et réaliser que chaque entité dispose de données sensibles qu'elle n'aimerait pas voir divulguées. On pourra ainsi par exemple trouver sur des réseaux des bases complètes de comptes et de mots de passe protégés par des dispositifs inadaptés, comme des mots de passe de fichiers de bureautique qu'il est possible de casser en quelques secondes avec des ordinateurs classiques, tels les portables grand public.

4.6 Manque de bon sens

On peut enfin parfois s'étonner du manque de bon sens des personnes gérant la sécurité des systèmes d'information. C'est tout particulièrement apparent en ce qui concerne la sécurité physique. Il est parfois tout à fait surprenant de trouver des salles serveur protégées avec des digicodes, des portes blindées et un mur très fragile avec une fenêtre non protégée jouxtant cette porte blindée. On peut également douter de l'opportunité de mettre des tableaux électriques sous des tuyau d'évacuation d'eau.

5 Conclusion

Cet article détaille plusieurs vulnérabilités relevées au cours d'audits, mais il est bien entendu évident qu'elles ne se rencontrent pas toutes au sein de la même entité. En fonction des différentes perceptions de sécurité, de risque et de la technicité des entités auditées, on retrouvera des manques de sécurité dans des domaines différents. Cependant le domaine essentiel qui doit être renforcé quoi qu'il arrive est celui de l'humain. Sans une motivation forte des équipes dédiées, le niveau de sécurité ne pourra pas être élevé.