SÉCURITÉ INFORMATIQUE

numéro 28 février 2000

SÉCURITÉ DES SYSTÈMES D'INFORMATION

ARCHITECTURE DE RÉSEAUX

« Sécurité informatique » aborde tous les deux mois un thème différent. Chacun d'eux est un élément de notre conception de la sécurité sur lequel nous appelons à la vigilance. Celui de ce numéro, « Architecture de réseaux », mérite plus encore notre attention : il ne peut y avoir de sécurité sur des réseaux qui ne sont pas convenablement structurés. L'article de J.-L. Archimbaud ci-dessous résume notre conception en la matière et constitue des **recommandations fortes** du CNRS.

Développer une sécurité informatique active

éditorial

Nous constatons tous les jours des attaques de nos systèmes informatiques : ce sont souvent des tentatives d'intrusion par des *hackers* plus ou moins professionnels, mais, dans un certain nombre de cas, ce sont aussi des actes délibérés de pillage de données ou de logiciels. Trop souvent, nous devons constater que des *indélicats* se sont installés, subrepticement et parfois depuis longtemps, dans nos machines et poursuivent à partir de là leurs méfaits vers d'autres sites.

Lorsqu'une intrusion est constatée, les dégâts sont souvent importants et nécessitent un travail long et fastidieux pour remonter le système et supprimer les failles de sécurité. Tout cela affecte lourdement la continuité du service informatique dans le laboratoire.

Les méthodes et les outils qu'utilisent les pirates sont bien rodés et d'un accès malheureusement très facile ; des kits entiers de piratage circulent sur le réseau.

Nous l'avons souvent répété : nul n'est à l'abri de ce problème, même si certains pensent a priori que leurs données n'intéressent personne et qu'il n'y a rien à voler sur leurs machines.

En même temps qu'il développait l'utilisation du réseau dans les laboratoires, le CNRS a conduit une politique forte de sécurité informatique : il y consacre, à travers l'UREC, des moyens importants, il a augmenté le nombre d'ingénieurs en charge de la sécurité informatique ; délégation régionale après délégation régionale, il mobilise le réseau des administrateurs système pour conduire des opérations de sécurité sur chaque campus.

De son côté, le GIP Renater a gonflé la structure de surveillance et d'alerte (le CERT) en France en liaison avec ses homologues à l'étranger.

Il reste encore trop de vulnérabilités dans notre outil informatique et il faut y remédier : éliminer les fonctionnalités inutilisées qui peuvent constituer des faiblesses, revoir l'architecture de notre outil informatique pour séparer les serveurs d'accès public des ressources privées, mettre en place une protection adaptée à chaque niveau.

C'est à cela que vous invitent les articles qui suivent, c'est à cela que nous vous proposons de nous atteler ensemble dans les prochains mois.

Christian Michau
Directeur de l'UREC

Recommandations d'architecture de réseau pour améliorer la sécurité

Cet article n'essaie pas de résoudre tous les problèmes de sécurité, loin de là. Il se focalise sur les vulnérabilités liées aux réseaux, en particulier aux attaques provenant de l'Internet, et essaie de proposer un modèle d'architecture associé à des contrôles d'accès pour limiter ces vulnérabilités. Il ne demande pas d'investissements lourds et peut être facilement accepté par nos utilisateurs, voire transparent pour eux. Comme tout modèle il est à adapter à chaque environnement. Les recommandations ci-dessous ne sont pas nouvelles, depuis de nombreuses années nous les avons exprimées de très diverses manières. Mais maintenant, il s'agit de les généraliser à tous les sites car les risques et les attaques augmentent de jour en jour.

Le succès de l'Internet n'était pas prévu

Nos sites sont connectés à l'Internet depuis longtemps. Lors du choix de l'architecture, la sécurité était très loin d'être un critère important. Le but principal était alors que toutes les machines des sites, sans exception, puissent accéder et être accessibles de l'Internet avec le

suite page 2

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

suite de la page 1

meilleur débit possible. La connectivité totale *(full connectivity)* était l'objectif. L'Internet n'était qu'un ensemble de réseaux de recherche où « tout le monde se connaissait ». On n'avait pas d'attaque de spam, scan, smurf, flood, spoofing, sniffer, ... (se référer aux articles de la presse informatique grand public). Maintenant l'Internet est devenu un outil de communication mondial, utilisé par des bons et mauvais citoyens, et toutes les déviances courantes y sont présentes. Même le terme de village global, qui désignait l'Internet avec sa note de convivialité et de quiétude, semble avoir disparu. L'Internet n'est pas plus noir que le monde mais il n'est pas plus blanc non plus.

On a pu voir rapidement que cette connectivité totale était une aubaine pour les personnes mal intentionnées qui pouvaient ainsi essayer très facilement d'attaquer toutes les machines d'un site et découvrir rapidement un maillon faible. Des réactions extrêmes aux premières attaques, celles-là même qui aujourd'hui font partie de notre quotidien, ont été de préconiser l'installation d'un garde-barrière en entrée de chaque site. Mot magique, assurance tous risques ! Cet équipement allait résoudre tous les problèmes. Mais les gardes-barrière de l'époque se sont avérés très contraignants. Ils n'acceptaient que certaines applications, demandaient (et demandent toujours) une administration lourde, étaient des goulets d'étranglements en terme de débit, ... Nous n'avons pas recommandé cette solution pour tous les sites. Une autre raison très pragmatique est que nous n'avons pas les moyens financiers et humains pour installer et administrer ce type d'équipement dans chaque laboratoire. Le garde-barrière n'est pas une solution à rejeter systématiquement ; dans certains environnements, elle peut se justifier, mais elle n'est pas à généraliser à tous les laboratoires.

Le choix du « tout ouvert », au moment où il a été fait, n'était pas une erreur. Mais rester maintenant dans la même logique en est une. Il faut absolument limiter les possibilités de communication entre l'intérieur et l'extérieur, non en restreignant les utilisateurs mais en ne laissant passer que ce qui est utile, ceci sur tous les sites. De la même manière que l'on ferme à clé son appartement ou sa voiture, que l'on contrôle l'accès à son bâtiment, il ne faut pas laisser complètement ouvert son accès Internet. Les sociétés commerciales qui se sont raccordées à l'Internet bien plus tard n'ont pas eu la même démarche que nous. Elles ont considéré l'Internet dès le départ comme un monde externe, hostile. Elles ont construit un réseau interne privé, Intranet, pour toutes leurs communications intra-entreprise (souvent confidentielles). Elles ne sont connectées avec l'Internet qu'en un ou deux points par lesquels circulent principalement des informations publiques. Ces portes sont contrôlées par un équipement de type garde-barrière. Nous, nous utilisons Renater comme un Intranet, alors que c'est l'Internet. Nous avons ainsi plusieurs centaines de points d'accès à l'Internet, d'où une situation totalement différente, beaucoup plus dangereuse.

En interne sur les sites, lorsque les réseaux locaux ou les réseaux de campus ont été mis en place, le but était le même que pour l'accès Internet. Il fallait raccorder le maximum de postes, tous les postes devant pouvoir communiquer avec tous les autres. Le réseau n'a donc pas été segmenté (découpage du réseau) avec une prise en compte de la sécurité. L'usage du réseau se généralisant, on a pris conscience que, sur un même site, certains groupes comme les étudiants avaient de grandes chances d'héberger au moins un pirate, que certains laboratoires (avec de nombreux contrats industriels, par exemple) avaient besoin de plus de sécurité que d'autres, que certaines machines de gestion contenaient des informations sensibles, ... et qu'Ethernet était un réseau à diffusion où, avec un simple logiciel d'écoute installé sur un PC utilisateur, on pouvait récupérer tous les mots de passe qui circulent sur le réseau quand celui-ci n'est pas segmenté.

Dans la seconde vague de mise en place des réseaux de grands sites, la segmentation a été mise en œuvre, de manière physique d'abord (« une fibre » pour l'enseignement, une pour la recherche, une pour l'administration), logique ensuite avec les VLANs (Virtual LAN, Local Area Network).

Il s'agit maintenant d'essayer de généraliser aux sites moyens cette segmentation qui était jusque-là réservée aux seuls grands sites.

Des systèmes informatiques imparfaits

Quel est le risque de la connectivité totale, c'est-à-dire de la liberté totale de communication entre les machines internes et l'Internet ?

Si tous les systèmes étaient parfaits et si toutes les machines étaient administrées avec un suivi quotidien, il n'y aurait aucun risque supplémentaire. Mais on est extrêmement loin de cette image d'Épinal. Presque quotidiennement, un avis d'un CERT (Computer Emergency Response Team) annonce un bug dans un logiciel avec le correctif approprié. Généralement cet avis fait suite à la diffusion sur l'Internet d'un outil d'attaque qui utilise ce bug pour acquérir les droits d'administrateur de la machine vulnérable. Pour manier cette arme logicielle gratuite et disponible pour tous, inutile d'être un génie, il suffit de lancer un programme. Heureusement pour nous, la grande majorité des internautes a d'autres objectifs que d'essayer de pirater les machines de recherche. Mais dans les dizaines de millions d'utilisateurs, il y a une poignée de petits psychopathes ou délinquants – et il y en aura toujours – qui pour montrer leurs capacités, par jeu, par vengeance, prennent plaisir à pénétrer les systèmes, les casser... On a aussi quelques concurrents scientifiques ou commerciaux qui n'hésitent pas à se servir de ces outils pour s'approprier le travail de certains laboratoires. Plusieurs attaques dans des unités étaient vraiment ciblées sur des résultats de recherche ou des développements intéressants. Ainsi au CNRS, en moyenne deux attaques violentes par semaine nous sont signalées.

L'autre talon d'Achille d'un système d'information distribué en réseau tel qu'on l'a aujourd'hui est le très lourd travail d'administration des multiples systèmes Unix et NT. Ces machines sont livrées avec de nombreux services réseau installés par défaut. Nous ne les utilisons pas tous, mais ils restent néanmoins actifs dans le système et augmentent inutilement sa vulnérabilité.

Avec ces logiciels bogués qu'il faut corriger régulièrement et des serveurs livrés ouverts qu'il faut reconfigurer, tâches qui se rajoutent à leur travail quotidien, les administrateurs n'ont matériellement pas le temps de maintenir l'ensemble des systèmes d'un site dans un état acceptable pour la sécurité. Le but de ces recommandations est de proposer une architecture qui permette de réduire à quelques-uns le nombre de systèmes sur lesquels portera l'essentiel de l'effort de configuration, de mise à jour et de surveillance sans que cela nuise trop à la sécurité de l'ensemble.

L'architecture

Principes

Dans le sens du flux sortant – du site vers l'Internet –, tous les postes doivent pouvoir atteindre les serveurs Web, échanger des messages, accéder à des services extérieurs,... Les communications seront donc rarement limitées. Néanmoins on peut estimer que pour certains groupes présentant des risques particuliers (les étudiants par exemple), il est nécessaire d'avoir une politique de sécurité plus restrictive.

Un document plus complet et plus technique, à usage des administrateurs informatiques et de réseaux, reprend toutes ces recommandations. Il est disponible en ligne : http://www.urec.cnrs.fr/securite/articles/archi.reseau.pdf.

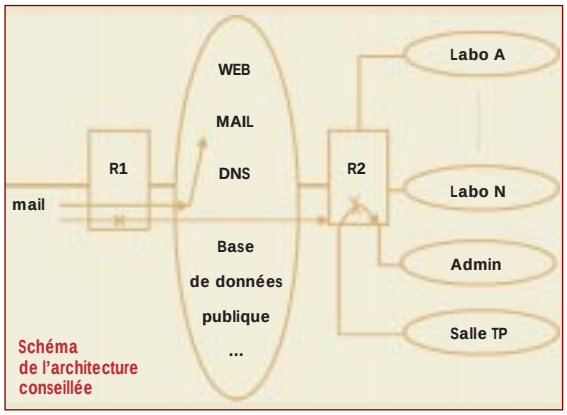


Schéma de l'architecture conseillée

Dans le sens du flux entrant – de l'Internet vers le site –, sens qui permet d'accéder aux services réseau sur les stations locales du site, le besoin de connexion est généralement très faible : évidemment le serveur WEB doit être accessible par tout l'Internet, mais un poste de travail utilisateur en a rarement besoin (il est uniquement client), de même un serveur local de calcul par exemple. Or c'est ce flux qui présente un danger et on va donc essayer de le limiter, autant que faire se peut.

Partant de ce constat, le principe de l'architecture est simple. Dans un premier temps, il faut séparer les machines qui ont besoin d'être accessibles de l'Internet (les serveurs réseaux) des autres (les machines utilisateurs clientes et les serveurs locaux) et disposer les premières dans une zone semi-ouverte entre l'Internet et le réseau purement local.

Dans un second temps, sur le réseau local, il faut tenir compte des différentes communautés sur le site et les identifier : unités, laboratoires, écoles, services généraux, ... classées selon leur rattachement administratif, leurs besoins réseau, leurs besoins de sécurité, leurs utilisateurs (plus ou moins « fiables »), ... Les machines de ces groupes seront réparties dans différents sous-réseaux physiques ou logiques. On arrive ainsi à une architecture segmentée où il est alors très simple d'installer des filtres dans les équipements de connexion (routeurs R1 et R2 sur le schéma) pour n'autoriser que les services utiles et contrôlés à circuler, et d'isoler certaines machines sensibles ou certains groupes à risque.

Services dans la zone semi-ouverte

Dans une zone semi-ouverte, en entrée de site, il faut installer toutes les machines qui assurent les services réseau avec l'extérieur : DNS, messagerie, Web, FTP anonyme, accès téléphoniques, news, bases de données publiques, ... Ces machines seront dédiées à ces fonctions, PC sous Linux ou NT par exemple (elles ne seront pas utilisées comme station de travail « classique »), et tous les services réseau inutiles seront inhibés.

Avec ces services en dehors du réseau local interne, il y aura très peu de communication directe de l'extérieur vers les réseaux derrière l'équipement R2. Il reste que certains utilisateurs peuvent avoir besoin d'accéder en telnet ou ftp sur leurs postes internes depuis l'Internet. On interdira cette connexion directe, mais on rendra le même service en installant dans la zone semi-ouverte une machine relais qui sera le passage obligé entre l'extérieur et l'intérieur. Ainsi un utilisateur qui depuis l'extérieur veut accéder en interactif sur sa machine de laboratoire devra d'abord se connecter sur ce relais, puis ensuite faire un autre telnet ou ftp. Sur ce relais, une trace de tous les accès sera conservée et un contrôle très fin des comptes utilisateurs (durée de vie des comptes, solidité des mots de passe, ...) sera effectué.

Sur toutes ces machines de service, un « ménage » complet des services inutiles sera effectué avant la mise en service. Les versions des systèmes et des applications seront régulièrement mises à niveau et les correctifs de sécurité seront installés dès qu'ils seront diffusés. Sur chacune sera installé un outil de contrôle et de trace des connexions, et tous les messages de journalisation (logs) seront redirigés vers un serveur interne. Elles constituent la poignée de machines qu'il faut parfaitement gérer.

Architecture interne

Sur le réseau interne (*cf.* schéma), un découpage du réseau par services et par niveaux de sécurité sera effectué. Chaque sous-réseau connecté à R2 pourra être soit physique (un câble dédié), soit logique (VLAN). La structuration à faire dépend entièrement du site. L'exemple montre un sous-réseau par laboratoire ou équipe de recherche, un sous-réseau administration pour les stations de gestion, un sous-réseau pour un salle de TP (travaux pratiques avec des utilisateurs à risque). On peut ainsi concevoir plusieurs sous-réseaux sur ce modèle, mais aussi sur d'autres : sous-réseau de stations non gérées par les administrateurs (portables de visiteurs, stations personnelles de chercheurs, ...), sous-réseau de machines rendant des services locaux à l'ensemble du site (serveur de sauvegardes, d'applications, de calcul, Web interne, ...).

Filtres sur R1 et R2

L'architecture mise en place ne devient vraiment utile pour la sécurité que si l'on installe des mécanismes qui limitent les trafics avec l'Internet et entre les différents sous-réseaux, concrètement des filtres dans les équipements R1 et R2. Les routeurs ou les commutateurs de niveau 3 ont maintenant tous de base ces mécanismes de filtrage.

La politique de R1 sera de tout interdire (dans le sens entrant) sauf certains services que l'on connaît et maîtrise, c'est-à-dire les services vers les machines de la zone semi-ouverte. Le schéma donne comme exemple un filtre qui n'autorise que les messages entrant vers le serveur de courrier électronique de la zone semi-ouverte. Tous les autres seront rejetés. Il faudra mettre le même type de filtre pour tous les autres services.

En interne, on pourra limiter les communications entre communautés en installant des filtres sur R2. Le schéma montre ainsi que l'on interdit toute connexion depuis une salle de TP vers le réseau administration.

Les possibilités offertes par les filtres sont très nombreuses mais leur compréhension demande une bonne connaissance technique en réseaux. On se reportera au document cité en introduction qui détaille un ensemble de filtres recommandés.

Attention, ne nous méprenons pas sur les objectifs de tout ceci. Le but de ces filtres n'est pas de brimer les utilisateurs, mais de ne laisser passer que ce qui est vraiment utile. Les besoins particuliers, par exemple, peuvent et doivent être pris en compte. Si une équipe de recherche a une station d'un réseau interne qui doit impérativement communiquer avec une autre station externe, on ouvrira les filtres pour permettre le dialogue uniquement entre ces deux stations (repérées par leur numéro IP) pour l'application utilisée (repérée par son numéro de port).

Quelle est l'utilité d'une telle architecture ?

La technique la plus courante d'attaque actuellement utilisée sur l'Internet est de découvrir toutes les machines d'un site (par « scan »), de détecter tous les services réseau installés sur ces machines, de tester les trous de sécurité connus de ces logiciels serveurs et de se servir de ces trous pour acquérir les privilèges d'administrateur sur les machines. Inutile d'être un expert pour arriver à ses fins, de nombreux outils sont disponibles sur des serveurs connus et sont utilisables par n'importe quel utilisateur. Si vous n'avez pas de filtre en entrée de votre site, ces outils détecteront sans effort des machines vulnérables chez vous et... Par contre, si vous avez les filtres recommandés, les attaques n'atteindront que la poignée de machines de la zone semi-ouverte, machines correctement administrées qui seront peu vulnérables. Toutes les autres attaques vers les machines internes seront arrêtées par les filtres. Donc, même si une station d'un réseau interne est mal administrée ou présente des vulnérabilités logicielles, le risque d'attaque réussie depuis l'extérieur sera faible.

Le problème des mots de passe sera aussi moins critique. Ainsi, si un utilisateur « prête » son mot de passe personnel à une connaissance, celle-ci

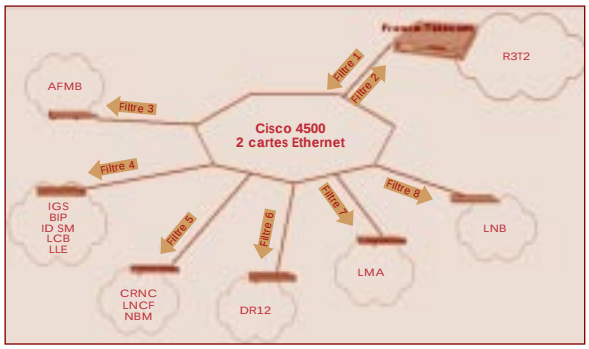
ne pourra pas accéder à cette station depuis l'extérieur. Dans le même registre, si un pirate installe un sniffeur (logiciel d'écoute sur un réseau) sur la zone semi-ouverte, il ne découvrira pas les mots de passe des stations de la zone interne. De même si un tel logiciel est installé dans cette zone (par exemple sur le sous-réseau « Salle de TP »), seules les autres stations du sous-réseau correspondant (la salle de TP) se trouvent compromises. De nombreux autres avantages existent qu'il serait fastidieux d'énumérer ici.

Mise en pratique

Le terme « site » peut désigner un laboratoire, un groupe de laboratoires, un campus, ... Mais le schéma est un modèle qu'il faut adapter. Ainsi, pour un campus, il ne faut pas obligatoirement pousser à une centralisation de chaque service réseau sur un serveur de la zone semi-ouverte. On peut vouloir maintenir un serveur de messagerie ou de Web par laboratoire. Ce n'est pas interdit. Par contre, il faut correctement les situer dans l'architecture, installer les filtres nécessaires et appliquer les recommandations d'administration décrites précédemment.
Pour mettre en place cette architecture, qui devrait être progressive, il faut une concertation et une adhésion complète de tous les administrateurs des entités du site. Cette coordination est obligatoire en phase de conception, mais aussi ensuite pour installer des filtres et surveiller. En effet, une fois cette architecture en place, il faudra assurer une surveillance étroite des serveurs, des journaux (logs) alimentés par les rejets des paquets filtrés, ... La lecture régulière des différents avis CERTs permettra de tenir correctement à jour les systèmes et applicatifs des serveurs de la zone semi-ouverte. Il faut rester vigilant.
En conclusion, cette architecture ne vous mettra pas complètement à l'abri, mais vous protégera – disons à 98 % – des attaques actuelles les plus courantes.

Les articles qui suivent décrivent les architectures et les démarches de deux campus CNRS.

Jean-Luc Archimbaud
Chargé de mission sécurité réseaux au CNRS
Directeur Technique de l'UREC (http://www.urec.fr/)



Le campus du Groupe des Laboratoires de Marseille (GLM)

Au sud de Marseille, ce campus regroupe 14 unités CNRS qui représentent 800 personnes, 1 100 machines, 6 classes C connectées au réseau régional R3T2.

L'architecture du réseau est en étoile basée autour du routeur d'accès du campus, un Cisco 4500, derrière lequel on trouve les commutateurs des laboratoires reliés aux différents bâtiments par fibre optique. Chaque entité, laboratoire ou groupe de laboratoires, a son réseau local connecté sur une interface du routeur. Ainsi les flux des entités du campus sont différenciés.

La sécurité du campus

La sécurité du campus est centralisée au niveau du routeur qui est contrôlé uniquement par l'administrateur du campus, moi-même. Avec une politique de *tout ce qui n'est pas permis est interdit.* Sur chaque interface du routeur est placée un filtre – deux pour l'interface reliant le campus à R3T2, le réseau régional. En entrée de campus, le filtre 1 *interdit tout ce qui est reconnu dangereux et permet tout le reste.* Ce qui est reconnu dangereux correspond aux différentes attaques référencées par l'UREC dans sa liste de contrôles de sécurité, les avis de sécurité du CERT-Renater et diverses littératures. Par exemple, sont interdits le SMURF, netbios, back orifice, netbus, les r-commandes, NFS, SNMP, etc. Ce filtre doit être maintenu à jour et ce pour **tout** le campus. En sortie du campus, le filtre 2 concerne également la totalité du campus, *tout est permis en sortie pour les classes C du campus sauf ...* netbios, le X, le SMURF. Ensuite, sur chaque interface des entités du campus, un filtre spécifique est placé avec comme politique *tout est interdit sauf ce qui est explicitement autorisé.* Par entité, l'on trouve un serveur SMTP, POP, Telnet, Web et FTP autorisés. Toutes les autorisations ou interdictions spécifiques à l'entité se trouvent dans ces filtres, ce qui permet de ne pas changer les filtres du campus en cas de modification pour une entité ; ouverture temporaire d'un port, d'une session X entre deux machines connues (dans ce cas, il est généralement nécessaire de modifier le filtre en sortie du campus). Les accès refusés par le routeur sont comptabilisés sur un serveur syslogd.

Quelques chiffres

Quotidiennement, le routeur envoie 1,2 Mo par jour de logs correspondant aux interdictions des filtres. Chaque fois que j'analyse ces chiffres, je suis inquiète. En effet, **tous les jours** les six classes C du campus sont sujettes à des attaques SMURF, ainsi qu'à des scans sur différents ports.
En décembre, j'ai constaté 30 scans effectués sur des ports supérieurs à 1023.
Au mois de novembre, le service IMAP a été largement scanné : j'ai trouvé 2080 lignes de logs envoyées par le routeur concernant le SMURF ; pour chaque ligne de log, le routeur a arrêté de 1 à 265 paquets ! Le record est détenu par le 9 novembre : si toutes les classes C avaient répondu, le réseau du campus tombait.
Je m'arrête là : ces attaques « ratées » me font penser qu'il y en a certainement qui aboutissent, mais nous ne les connaissons pas.

Conclusion

La sécurité commence par le routeur d'accès avec des filtres. Grâce à ces filtres, les administrateurs réseau et système du campus sont plus sereins, seules les machines serveur connues sont à surveiller. Le fait de centraliser la sécurité permet d'avoir une vue synthétique de l'ensemble du campus. Une seule personne a besoin de connaître les mécanismes de filtrage du routeur. Pour satisfaire pleinement les administrateurs réseau et système du campus, je traite immédiatement leur éventuelle demande de modification.

Sophie Nicoud
Ingénieur réseaux
nicoud@graal.dr12.cnrs.fr

Le campus de la Délégation Côte d'Azur

Les laboratoires CNRS situés dans les Alpes-Maritimes sont reliés pour la plupart par la plate-forme ATM CNRS/UNSA (Université de Nice Sophia-Antipolis). Ce réseau de campus virtuel est un véritable réseau métropolitain qui s'étend de Menton à Cannes avec deux pôles principaux situés à Nice et Sophia-Antipolis distants de 25 km.

Le campus relie la plupart des sites de recherche du CNRS sur les Alpes-Maritimes, l'Observatoire de la Côte d'Azur, l'Observatoire Océanologique de Villefranche, ainsi que tous les sites de l'UNSA.
Il est organisé autour d'un backbone ATM commun avec un seul point d'accès à Renater 2. L'accès des sites à la plate-forme ATM se fait *via* des commutateurs de niveau 3 disposant d'un Uplink ATM. L'accès à Renater 2 est réalisé par une connexion ATM en direct sur le NRD (Nœud Régional Distribué) de Sophia-Antipolis. L'administration de ce réseau est réalisée conjointement par le CNRS (service réseau de campus de la Délégation Côte d'Azur) et par le Centre de Ressources Informatique de l'UNSA.

La gestion de la sécurité ne peut pas être concentrée sur l'entrée du campus virtuel car :
– le réseau regroupe quelque 5 000 machines et 32 000 personnes,
– la gestion du réseau est partagée,
– les sites internes doivent aussi pouvoir être protégés les uns vis-à-vis des autres,
– les populations sont très diverses et ne permettent pas d'appliquer une seule et unique règle de sécurité pour tous les sites.

La gestion de la sécurité est donc déconcentrée en entrée des laboratoires.

Les techniques de mise en œuvre de la sécurité

La mise en œuvre de mécanismes de sécurisation passe par diverses solutions toutes nécessaires :
– application d'une vraie politique de sécurité au sein du laboratoire (charte, gestion des arrivées et des départs des utilisateurs, conseils pour le choix des mots de passe etc.) ;
– installation de Tcp Wrapper avec activation du filtrage des accès tcp en fonction des adresses IP des clients ;
– suivi des découvertes des trous de sécurité et application des patches de sécurité ;
– upgrade des systèmes d'exploitation dans la mesure du possible ;
– dépouillement quotidien des journaux d'activité des machines ;
– etc., etc.

Malheureusement toutes ces solutions ne suffisent pas car :
– elles demandent une attention constante et ne laissent pas le droit à l'administrateur système de s'absenter, ne serait-ce qu'une semaine... car si un trou de sécurité est découvert en son absence, il risque fort de découvrir à son retour qu'une de ses machines a été l'objet d'un piratage (cette situation est arrivée, je pense, à bon nombre d'entre nous) ;
– elles ne s'appliquent pas à tous les services ; par exemple, comment filtrer sur la machine les accès UDP ?
– elles ne s'appliquent pas non plus à tous les systèmes d'exploitation :
  • exemple 1 : comment appliquer des patchs ou faire évoluer le système d'exploitation d'une machine gérant un microscope électronique et dont l'outil principal risque fort de ne plus marcher à la moindre mise à niveau ?
  • exemple 2 : comment savoir quels services tournent sur certaines « boîtes noires » livrées avec des appareils de manips ?
– il existera toujours sur votre réseau un système d'exploitation que vous connaîtrez moins et par conséquent sur lequel la sécurité sera moindre.

Nécessité d'un filtrage des accès en amont des machines

Le filtrage des accès à la frontière entre le réseau local et le réseau de campus s'avère donc lui aussi nécessaire.
Pour cela, plusieurs solutions sont disponibles parmi lesquelles on trouve le firewall applicatif et les filtrages des accès IP sur les routeurs.
La mise en place d'un firewall n'est pas applicable à tous les sites car nous n'avons pas forcément les moyens humains pour administrer ce genre de solution.
Nous avons préféré conseiller la mise en place d'un filtrage des accès entrants sur chacun des laboratoires. Les commutateurs situés en entrée des laboratoires ont la possibilité de recevoir des filtres qui ont une syntaxe et une philosophie assez semblables à celles des ACL de CISCO.
Ces filtres sont mis en œuvre par le service réseau de campus qui a aussi pour mission d'aider les sites à sécuriser leur accès à la plate-forme ATM.

Deux politiques de filtrage : laquelle choisir ?

La première chose à faire est de choisir la politique de filtrage que l'on souhaite mettre en œuvre. Nous avons le choix entre :
– *tout est interdit sauf...* ce qui est autorisé ;
– *tout est autorisé sauf...* ce qui est interdit.
Dans la littérature, il est souvent conseillé aux sites ayant un nombre conséquent d'utilisateurs qui ont acquis une longue pratique des réseaux ouverts de choisir la deuxième solution et de faire ensuite évoluer petit à petit les filtres pour tendre vers la politique *tout est interdit sauf...*
Nous nous sommes aperçus que cette méthodologie n'était pas satisfaisante car :
– les filtres n'évoluent pas suffisamment vite : on applique, on vérifie que personne ne proteste, on applique un nouveau filtre, on se rend compte qu'on passe un temps infini à affiner pour un résultat peu satisfaisant..., trop de services restant ouverts.
– Si on désire protéger les nouveaux services émergeants, cela demande une mise à niveau constante des filtres.
– Cette solution ne permet pas de connaître les besoins des utilisateurs *a priori*. L'utilisateur ne se sent pas consulté et considère négativement les barrières imposées et les tâtonnements qui les y mènent.
Notre expérience nous a permis de constater que la première solution peut tout à fait être installée directement, même lorsque les utilisateurs ont acquis une longue pratique des réseaux ouverts.
Elle doit cependant être installée avec une certaine méthodologie en impliquant et en informant les utilisateurs (*cf.* encadré ci-contre).

Exemple d'architecture de réseau avec une politique de filtrage

Je voudrais présenter ici l'architecture de réseau qui était installée jusqu'à présent à la Délégation Côte d'Azur.

Méthodologie de mise en place des filtres en entrée des laboratoires

Enquête auprès des utilisateurs

Dans un premier temps, l'administrateur du site fait le point des us et coutumes de ses utilisateurs. Cette enquête permet de remarquer quels sont les services qui sont utilisés par la majorité d'entre eux. Au cours de ce sondage, il explique ce qui va être fait et, en particulier, que la mise en place des filtres a pour but de protéger le site des attaques de l'extérieur et en aucun cas d'empêcher les gens de travailler. Peut-être un changement des habitudes de certains utilisateurs sera-t-il nécessaire, mais ce n'est pas certain.

Réunion de travail pour lister les besoins

Dans un deuxième temps, une réunion de l'administrateur du site et de l'administrateur du réseau de campus est organisée pour mettre noir sur blanc les besoins des utilisateurs qui sont remontés du sondage. Les utilisateurs qui ont des desiderata spécifiques peuvent aussi être conviés à cette réunion. Ils expliquent leurs besoins et ensemble nous affinons ces demandes.

Exemple :

Utilisateur : " Il faut laisser l'accès FTP ouvert vers ma station de travail. "
Administrateur : " Pourquoi ? "
Utilisateur : " Parce qu'elle fait de l'acquisition de données et qu'elle les diffuse à trois sites avec lesquels l'équipe travaille. "
Administrateur : " Donc si on ouvre les accès FTP sur votre machine vers ces trois sites et si on ferme ces accès pour le reste d'Internet, ça ira ? "
Utilisateur : " Comme ça, c'est OK. "

En revanche, si un utilisateur souhaite simplement faire du transfert de fichiers épisodique sur sa machine, on pourra lui conseiller d'utiliser la machine qui aura été désignée comme serveur FTP pour le laboratoire, quitte à faire un transfert en deux temps.

Détermination des principaux serveurs / fermeture de certains serveurs

Cette réunion amène souvent à la fermeture de certains services sur la plupart des machines et à la spécialisation de certains serveurs. Nous essayons d'en profiter pour revoir l'architecture logique du réseau. Nous essayons, dans la mesure du possible, de ne garder visibles de l'extérieur qu'un ou deux serveurs DNS, un serveur Mail, un serveur WEB, un serveur FTP, un serveur telnet.
Mais cela est fait en accord avec les besoins des utilisateurs : dans le cas de l'exemple ci-dessus, on ferme les accès FTP de l'extérieur vers toutes les machines sauf le serveur officiel et le serveur de " manip ".

Mise en place des filtres

Dans un quatrième temps, les filtres sont rédigés et installés sur le routeur du laboratoire. Tous les besoins listés font l'objet d'un test. Peut-on joindre les serveurs depuis l'extérieur ? L'équipe peut-elle continuer à faire ses transferts ? etc. Lors de cette phase, nous éliminons la plupart des problèmes causés par des erreurs de rédaction des filtres.
La semaine qui suit cette mise en œuvre est consacrée à un affinage de ces filtres. En effet, il existe toujours des incompréhensions, ou des besoins qui n'ont pas été exprimés par les utilisateurs.

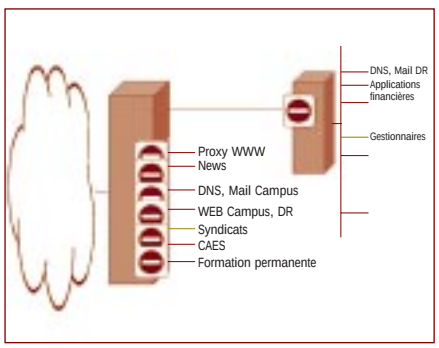
Avantages de cette méthode

Les filtres installés sont vite corrigés et le réseau est protégé très rapidement. Les nouveaux services sont protégés par défaut. Seuls les nouveaux besoins et les nouveaux services installés sur des ports non standard demandent une mise à jour des filtres.

La Délégation Côte d'Azur du CNRS est chargée de l'administration de la recherche des laboratoires CNRS situés sur les Alpes-Maritimes et le Var. Comme toutes les délégations, elle est chargée, entre autres, de la gestion financière et comptable des laboratoires ainsi que de la paye des agents. La sécurité de ses données est donc primordiale.

De plus la Délégation héberge :
- les machines gérant les services associés au réseau de campus de la DR20,
- les machines du CAES,
- les machines de la salle de formation permanente du CNRS,
- éventuellement les machines des syndicats.

Le schéma ci-dessous présente l'architecture du réseau de la DR20.



Architecture du campus de la Délégation Provence Côte d'Azur

Les machines n'ayant aucun rapport avec l'administration de la recherche sont installées sur un autre sous-réseau (formation permanente, CAES, syndicats, etc., ainsi que les machines de services dédiées).
Des *access lists* du style « Tout est interdit sauf... » sont installées sur les ports du commutateur. La commutation permet de garder un certaine sécurité aussi entre les machines de service du réseau de campus et les machines de la salle de formation permanente.
Des *access lists* du style « Tout est interdit sauf... » sont installées sur le routeur de la délégation.

Conclusion

Les *access lists* mises en œuvre améliorent grandement la sécurité des laboratoires, mais les décisions d'achat des matériels réseaux sont souvent basées sur des critères de performance, et les critères de sécurité étaient jusqu'à présent bien souvent oubliés. Les possibilités de filtrage des matériels réseau doivent être étudiées elles aussi en détail :
- permettent-elles des reports de tentatives d'intrusion sur les ports fermés vers un serveur syslog ?
- permettent-elles de faire des *access lists* dynamiques qui apportent le confort de n'ouvrir les ports clients que lors de la connexion à un serveur distant, évitant ainsi qu'un serveur installé sur cette gamme de ports ne soit utilisé comme cheval de Troie ?

Ces questions restent indispensables pour pouvoir assurer un minimum de sécurité, car bien sûr il n'existe pas de solution miracle... Car même si vous n'ouvrez les accès que vers un seul serveur DNS, si celui-ci est obsolète, vous serez quand même piraté... ;-)

Marie-Laure Miniussi
Ingénieur réseaux
Marie-Laure.Miniussi@sophia.cnrs.fr

SÉCURITÉ INFORMATIQUE
numéro 28 février 2000
SÉCURITÉ DES SYSTÈMES D'INFORMATION

Sujets traités : tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité : 5 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :
ROBERT LONGEON
Centre national de la recherche scientifique
Service du Fonctionnaire de Défense
c/o IDRIS - BP 167. 91403 Orsay Cedex
Tél. 01 69 35 84 87
Courriel : robert.longeon@cnrs-dir.fr
http://www.cnrs.fr/Infosecu

ISSN 1257-8819
Commission paritaire n° 3105 ADEP

Conseil et coordination : CNRS - DIST - Jacqueline Leclère • Conception et réalisation : La Souris 01 45 21 09 61