PCR

Reportage

Le CHU de Strasbourg sécurise avec la carte santé

La sécurité des accès au système d'information de ce centre hospitalier a recours à un couplage entre la carte de santé et un logiciel d'authentification.

L'ouverture du Réseau santé social (RSS) à l'ensemble du secteur médical va exercer un impact direct sur la stratégie de sécurité des établissements hospitaliers. C'est déjà le cas aux hôpitaux universitaires de Strasbourg, qui regroupent 8 900 personnes et 2 800 lits sur cinq établissements. Profitant de sa position de site pilote pour la carte des professionnels de la santé, qui sécurisera l'accès au RSS, cet établissement l'a adoptée sur son campus pour l'accès à son système d'information. Son informatique est duale, composée d'applications à vocation à la fois administrative et médicale. Près de 1 500 PC connectés en réseau accèdent à différentes bases de données : Oracle, Business Objects. *«La sécurité de notre système d'information hospitalier s'inscrit dans la durée»*, expliquait Germain Zimmerlé, directeur informatique des hôpitaux universitaires de Strasbourg. Son intervention a eu pour théâtre le 9e forum Eurosec, qui s'est tenu au Cnit de la Défense (92) du 16 au 18 mars dernier. Et Germain Zimmerlé de rappeler que, dès 1993, était établie une charte de communication de l'information médicale. En 1994, un serveur gère toutes les habilitations, c'est-à-dire les accès individuels des personnes aux réseaux.

Depuis l'automne dernier a commencé la dernière étape : le déploiement de la carte professionnelle de santé sur le campus des hôpitaux de Strasbourg.

Les postes de travail seront équipés progressivement de lecteurs de cartes.

Site pilote pour la carte de professionnel de la santé, le CHU de Strasbourg l'a aussi adoptée pour l'accès à son système d'information.

Cette carte est couplée avec une solution logicielle d'authentification unique de type Single sign on. C'est le noyau Autosecure SSO de Platinum qui a été retenu à cette fin. Le terme «unique» signifie que l'utilisateur accédant au système d'information et à ses applications, depuis son PC, est identifié et authentifié une fois pour toutes lors de la première connexion (voir encadré page 56). Cela permet de centraliser sur un seul serveur ces services de sécurité. Ce couplage entre un système d'authentification via un serveur et la carte des professionnels de la santé se justifie par les contraintes propres à la sécurité du système d'information hospitalier. Les postes de travail installés dans les unités de soins sont partagés par des professionnels aux métiers et aux profils différents. *«Dans les hôpitaux universitaires, les internes de médecine changent tous les six mois d'affectation sur le campus.»* C'est pourquoi la direction des ressources est associée au projet de sécurité. C'est elle qui renseigne le serveur informatique de sécurité sur les changements d'affectation du personnel. Deux éléments importants ont donc été mis en place au CHU de Strasbourg :

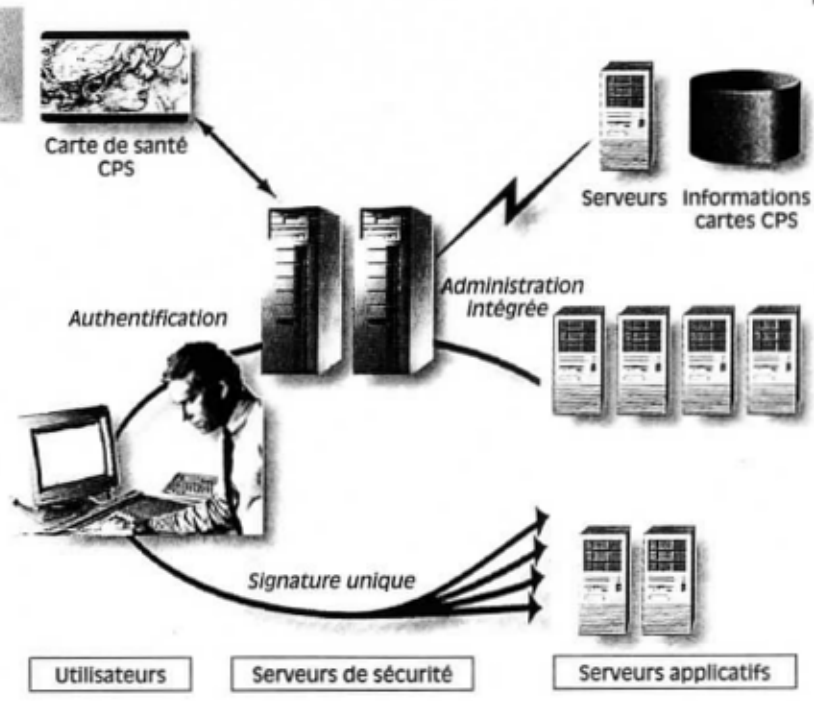
L'application en résumé

Les hôpitaux universitaires de Strasbourg, répartis sur cinq sites, disposent de 2 800 lits, comptabilisent 120 000 hospitalisations par an et emploient 8 900 personnes. Le service informatique occupe 60 personnes. Voici le contexte informatique de l'application de sécurité :

- **Système d'information administratif et hospitalier :** Unix, Oracle pour les bases de données et Business Objects.
- **Serveur de sécurité :** Logiciel Autosecure SSO de Platinum.
- **Intégration de la carte professionnelle de santé :** Carte d'identification à microprocesseur.
- **Administration centralisée** avec utilisation d'un annuaire normalisé X500.
- **1 500 PC connectés en réseau**, à équiper progressivement de lecteurs de cartes.

m°124

Architecture de sécurité des hôpitaux universitaires de Strasbourg



- **Le poste de travail.** Il est sécurisé par l'emploi de la carte des professionnels de santé. Elle propose une identification du porteur à la fois en tant que personne et tant que professionnel de la santé. Dans sa version 2, elle offrira des possibilités de chiffrement et la signature électronique. *«Cette carte devra aussi servir au comptage du temps de présence des personnels. Elle n'est pas encore mise en œuvre sur le campus.»* Chaque PC doit être équipé d'un lecteur de cartes. La carte dispose, notamment, d'un code porteur qui identifie la personne et qui est modifiable.
- **Le serveur de sécurité.** Bâti sur le logiciel Autosecure SSO de Platinum et développé sur cette base par ICL France, il a été retenu pour plusieurs raisons. Son paramétrage en fonction des choix effectués par l'établissement – gel du poste, sauvegarde du contexte, etc. – a semblé intéressant. Ce logiciel a été considéré comme une solution industrielle pouvant s'intégrer dans une architecture client-serveur. Enfin, il fallait que le logiciel soit portable, car les hôpitaux universitaires de Strasbourg sont des sites de qualification au plan national. *«Il fallait que d'autres hôpitaux puissent reprendre les développements faits pour notre compte»*, explique le directeur informatique.

La réalisation du prototype de cette architecture de sécurité a exigé une phase d'assemblage qualifiée d'«opération complexe». Il a fallu, en particulier, intégrer les procédures d'authentification au système d'information de l'hôpital et effectuer des développements à partir d'interfaces de programmation fournies avec le logiciel Platinum. Germain Zimmerlé a souligné, lors de la présentation faite à Eurosec, *«l'ampleur du chantier, la multiplicité des acteurs et le manque de maturité de certains composants»*.

Les premiers essais du nouveau système de sécurité ont porté, en septembre 1997, sur un nombre limité de postes de travail : 60, utilisé par 180 personnes, réparties sur 5 services. Au début de 1998, 8 services représentant 80 postes et 400 utilisateurs étaient desservis. *«La montée en charge est plus longue que prévu.»* Quoi qu'il en soit, les fondations d'une nouvelle approche de la sécurité en milieu hospitalier sont jetées. Parmi les perspectives offertes à terme figurent la dématérialisation du dossier de soins, l'interfaçage avec la carte Vitale (carte personnelle du patient) et l'ouverture du système d'information vers les partenaires de l'hôpital dans le cadre du Réseau santé social.

Frédéric Bergé

Qu'est-ce qu'un système d'authentification unique

Les spécialistes de la sécurité parlent de Single sign on (SSO), ce qu'on pourrait traduit par système d'identification/authentification unique. Le principe consiste à permettre à l'utilisateur qui souhaite accéder au système d'information de le faire à partir d'une seule authentification. Cela lui évite d'avoir à entrer une succession de mots de passe ou d'identifiants pour avoir accès aux applications du système d'information : messagerie électronique, applications bureautiques. Après avoir authentifié l'utilisateur, le serveur de sécurité, sur lequel est hébergé la fonction SSO, met en œuvre l'automatisation des connexions vers les applications auxquelles l'utilisateur a droit d'accéder. Plusieurs logiciels du marché assurent ces fonctions d'authentification unique qui sont, en général, fournies via des interfaces de programmation ou via des extensions spécifiques (voir tableau ci-dessous).

Quelques produits d'authentification

Produit	Authentification unique	Administration centralisée	Support de produits tiers
Mynet de CKS	Scripts agents	non intégrée	Sécurité PC, calculettes, pare-feu
Autosecure SSO de Platinum	Scipts, Sesame, GSS-API	Module ESA	Sécurité PC, calculettes, pare-feu
Access Master de Bull-ISM	Scipts, DCE , GSS-API	ISM (modèle X 512)	Sécurité PC, cartes, pare-feu
Unicenter/SSO de CA	Sripts, agents	Unicenter TNG	Sécurité PC, calculettes, pare-feu
Secure Way d'IBM	DCE, Open Horizon	Tivoli	Cartes
Praesidium de Hewlett-Packard	DCE, Open Horizon	DCE	Cartes

Source : Isabelle Petit (XP-Conseil)