How to stop intruders
Diego Sacristán

The presence of undesired persons on the internal nets of companies is one of the biggest problems at the moment.

As organisations reduce the actual physical presence of their operations, they find themselves moving towards a world of virtual activity where external agents are becoming users of company information systems. For example, companies increasingly have available extranets from which customers can check on the state of their orders or from which suppliers can find out the company’s inventory level. However, as the consultancy firm Gartner Group points out, when a large number of external users are managed via electronic media the costs associated with this management rise exponentially. Furthermore, the access of multiple users, company members or not, raises numerous challenges not only from the security point of view, but also for the management and organisation of companies. Intruders must be stopped from accessing the system but, above all, the roles and functions of each individual user within the hierarchy of the organisation must be established. In order to resolve these questions identity management services have recently appeared.

These are an assembly of technologies that allow the centralised administration of personal access to corporate systems with regard to the identity of the user and not simply on the representation of users at the system (user identification). This simple process allows companies to break out of the traditional technological straightjacket: the customer, supplier or internal user is no longer simply a name and password but is now an individual acting in his own name or representing an organisation and, as such, has an identity with a series of attributes that have to be managed.

The first step in bringing about adequate management of identity is the assigning of technological and business requirements to distinct identities as well as establishing their correspondence with internal and external units of the organisation. The same functions will not be able to be granted to a secretary as to a financial director, and neither will it be possible that certain identities, whatever their status, will have access to certain applications of the system. In a similar way, not all suppliers will have access to the company net to the same extent and it will be necessary to delimit the applications (Enterprise Resource Planning and Supply Chain Management), the rights and the access routes (intranet and point to point nets) for each of them.

Tools

Once the conceptual aspects have been defined, the centralised identity management tools come into play. These applications include, amongst other functions, the setting up of, cancellation and assignation of access rights with regard to the hierarchy of human resources and functional roles, in such a way that users can register themselves on the
applications and manage all the information concerning their access (change of password, consultation on the state of a request and variations in their localisation or functions).

However, identity management is not carried out in a completely automatic way. The crucial processes, like those related to human resources or company finances, require, in many cases, that the owners of the applications (system administrators) approve access. In this sense, the definition of work flows is also applied to the advanced management of identities. All these functions are being translated into an improvement in security and a reduction in costs, that can be attributed to three factors: the centralisation of management, the semi-automation of processes and the execution of decisions at source. Whilst the first two are starting to become habitual in information systems, the capacity of managers to execute decisions for themselves from the system is breaking the old segregation between systems departments and business personnel.

"Are companies ready to manage a large volume of identities?"

What is needed is efficiency
Manuel Cortés, Manager of consulting, PwC
The change of scenario that has been produced in the last few years has meant that the number of users does not only depend on the size of the company, but also on the level of openness that it shows to customers, suppliers and members. Traditional businesses that have started to adapt themselves to this new scenario have found themselves faced with the problem of making their infrastructures adequate to the requirements of the efficient management of large volumes of users compared to companies set up in the new scenario that have adapted new ways of managing their users. That is why companies, as well as having accommodated the reengineering of their business processes, must undertake the redesign of their user management. For that there are technologies and good practices that can be integrated with both existing and new applications to achieve an efficient management of this large volume of users.

A model replete with doubts
Brian Subirana, IESE Professor
The management of identities in information systems carries relative risks to security, access control, the model of identity data, the regulatory environment, mistakes in associated processes, viruses and the methodology of programming and management of versions. Companies are not prepared for all of that. Moreover, it is not clear what is wanted. Should users have access to all the information related to their identity? Should all transactions related to identity disappear without trace? Will a unique methodology of programming have to be imposed? Often in the introduction of new technologies there exists a period in which a dominant design is defined that allows economies of scale and that satisfies the needs of all users. Are we prepared to accept a standard model that does not adapt perfectly to the needs of our personal and professional virtual identity?