

Managed hosting – enterprise server base management – is fast growing in popularity. Belgacom NSI also operates in this field. To provide your enterprise with maximum security for its server base, early this year the company implemented a new password protection system from the specialist Cyber-Ark.

Belgacom NSI Highly secure managed hosting

Frans godden
A growing number of companies are choosing to subcontract all or part of their IT hardware infrastructure to a specialised partner. The reason is generally simple: they want to get rid of all of the technical worries and entrust them all to a specialist that can offer a 'one-stop-shop' solution, so that they can concentrate on their core business. Some prefer to place their own servers in the partner's data centre, whilst others make use of the servers provided and managed by their partner.

Even more security

Belgacom Network & System Integration has more than one hundred clients, mainly large enterprises that have opted for one of these two formulas, running on more than 300 servers in Belgacom data centres. Each of these enterprises has some critical information on these servers, which therefore has to be protected as effectively as possible. It goes without saying that Belgacom uses all of the traditional security tools (firewalls, antivirus, anti-spam, etc.), including password authentication.

"However, in the latter case, we thought that we could go a step further", states Bernard Philippe, Server Product Manager at Belgacom NSI. "Naturally, our passwords were already encrypted and stored in files only accessible using very complex keys. Nevertheless, this system was open to im-

provement, if only because the passwords that people had chosen themselves were not always particularly original."

A rare bird

It was for this reason that in May 2005 Belgacom set out to find a more professional approach to password security. "Unfortunately, although the market is full of programmes adapted to 'self management', enabling end users to modify their passwords", continues Bernard Philippe, "we could not find what we were looking for, that is to say a product with which we could manage passwords from the standpoint of a system administrator or a host provider that needs to store passwords securely, with encryption, error tolerance and passwords that can be generated in a completely random manner." Finally, Belgacom tracked down this rare bird: Network Vault and CPM (Central Password Manager) from Cyber-Ark, an American company originally from Israel that is devoted entirely to the security of networks and critical information. "There was no real alternative", claims Bernard Philippe, "no other product was capable of managing passwords at administrative level in a secure environment with security policies."

Change of attitude

The decision was taken quickly: the platform was tested for two months, went into pre-production

in July, and was fully operational at the end of the year. The fact that the whole operation lasted this long, according to Bernard Philippe, is due less to the technical aspects than to the change of attitude required by the application. "You have to persuade people that it is a good programme, that it may be a little more difficult to obtain a password, but that the level of security is significantly higher and also that, in the end, it is the only correct and professional way to work. And that was no easy matter, involving initiation, training, coaching and migration support. But now that we are in production, everyone is very satisfied with the choice", enthuses Bernard Philippe.

The roll-out, which was completed without a hitch, was carried out entirely by our own technicians, with excellent support from the English subsidiary of Cyber-Ark. There were no problems of integration with other software because, in the words of Bernard Philippe, Network Vault is easy to install and acts as a totally independent system that only manages passwords, both for the database and for end users.

Undeniable benefits

The benefits of the Cyber-Ark system are legion, according to him. "With this application, we now have the possibility, for the administrator, the helpdesk and persons that have to intervene in the event of a breakdown, of viewing

■ Bernard Philippe, Server Product Manager at Belgacom NSI: "Previously we had no log, but now that anyone who wants access must first be identified, we know for sure what it is about, why he or she wants access and when the request took place."



the password required using a completely secure process. One advantage of the product is that we can link different policies to the process. For example, you can make Cyber-Ark change the password automatically after two hours if you estimate that the person handling the intervention needs only two hours. Someone who happens to pass in front of the technician's screen cannot use it two hours later. The same applies to staff who leave the company, or when a computer remains without a user for a certain time. You can also define password access in two phases. When someone requests access to the passwords, a request is sent to the administrator, who verifies the identity of the requester and precisely what that person wants, before granting or refusing authorisation, in full knowledge of the facts."

No more disputes

When a request for access comes directly from an enterprise with

a server hosted at Belgacom, a VPN is created with the network of the company concerned, with all the necessary identification procedures. Access is then granted to certain passwords, depending on the profile of the requester. "The advantage of this product is that it also has a control function," explains Bernard Philippe. "Previously we had no log, but now that anyone who wants access must first be identified, we know for sure what it is about, why he or she wants access and when the request took place. In other words, we have a fully logged overview that excludes any form of dispute – and this is very important because we often have sensitive information on the site for several clients."

This possibility of precisely tracing who did what becomes even more useful if security problems arise for one reason or another, or if a person has to intervene for someone else and therefore has to have the necessary passwords. "Our clients often ask us to create

a management opening for a limited period; using this system we can create temporary management passwords entirely automatically," continues Bernard Philippe. A control mechanism is

protecting other sensitive information stored on the file servers of an organisation. "This is because the product is so multi-faceted that it can also be used in the future to secure Word or PDF docu-

No other product was capable of managing passwords at administrative level in a secure environment with security policies

also built into Network Vault, which ensures that the system still retains complete access control after the successful authentication of a user. To achieve this, Network Vault is subdivided into 'vaults' in which users only see the data to which they have access.

Many more applications

Bernard Philippe is aware that a product such as Network Vault, with its Central Password Manager, is also perfectly suited to pro-

ments, for example, such as confidential management reports. It will certainly be extremely useful if we are asked to manage servers at client sites, because we will then be able to ensure that everything that occurs is completely secure via our password management system. As you know, Network Vault is a relatively costly product and represents a major investment for us, but it provides real added value for our clients and therefore a real commercial advantage." ■