



Thursday, July 27, 2006

Nine Tips on IT Security

By Adam Bosnian

If we're honest, every one of us can imagine what we'd do with a few million in the bank. The yacht in Cannes, the private jet in Nice, possibly our own football team, and maybe a few other high maintenance accessories top our list of must-haves. But of course the question is how to get there. Working till I'm too old to enjoy it is one option but of course there is an alternative; the lottery, online poker, a rich widow, stocks and shares -- increasingly risky these days -- or why not simply help myself to something very valuable.

After all, if I'm working in IT I probably have access to the corporate crown jewels. And that could be anything; source code for the next money spinning application that will be released, credit card details for thousands of customers, even the recipe for Coca Cola! Recently, a Coca-Cola employee and two accomplices were arrested in Atlanta for allegedly stealing confidential information from the Coca-Cola and trying to sell it to PepsiCo.

In fact, it's actually quite easy because if I'm working in IT, I have access to systems with all kinds of privileged information. Here is my employer thinking that his M&A data is safe and I'm allowed free access to the servers storing the data. I can help myself to whatever I want and no one will ever know. And of course it's much easier now than it was when I first started this job. Then I somehow had to get out of the building with everything under my arm, but now I have dozens of ways to get it out. Just make my choice -- mobile, USB stick, email attachments, VPN access from home and no one will ever know. And of course it may not even be my employer, just some company that we provide outsourcing services for -- it's never been easier!

The problem often lies in the fact that we are constantly tempted because the corporate jewels are literally just lying around where anyone can find them. The problem for today's enterprise is that the transfer of information is increasingly time-critical and the traditional approaches such as FTP and secure email are awkward to manage, and often lack the security mechanisms that sensitive data demands, thus making the risk of leakage very possible. And where it becomes really challenging is when you need to share information with business partners. So here are a few suggestions

1. Do not expose your internal network

The process of transferring files in and out of the enterprise must be carried out without exposing and risking the internal network. No type of direct or indirect communication should be allowed between the partner and the enterprise.

2. Make sure that intermediate storage is secure

While information is waiting to be retrieved by the enterprise or sent to the business partner, it must reside in a secure location. This is especially critical when the intermediary storage is located on an insecure network, such as the enterprise's DMZ, outsourced site, or even the internet.

But encryption and other security mechanisms are not helpful if the security layers where the data is being stored can be circumvented, for example by a systems administrator. Encryption is good for confidentiality, but does not protect data from intentional deletion or accidental modifications. It is important to have a single data access channel to the storage location and ensuring that only a strict protocol, that prohibits code from entering, is available for remote users. In September 2004, an unauthorized party placed a script on the CardSystems system that caused records to be extracted, zipped into a file, and exported to an FTP site. The result was the exposure of millions of credit card details and the eventual demise of CardSystems.

3. Ensure that Data at Rest is protected

The cornerstone of protecting storage while at rest is encryption. Encryption ensures that the data is not readable and thus maintains its confidentiality. But encryption that places high demands on managing is ineffective. By using transparent key management there is absolutely no need for user level or administrator level encryption key management or awareness, and the use of advanced cryptographic protocols, such as AES 256bit for both storage and session encryption and signing, guarantees the protection of the data :

4. Protection from data deletion, data loss

The protection of data by encryption is simply one part of the problem. Files may be accidentally or intentionally deleted or changed. Always keep older versions, ensuring an easy way to revert to the correct file content or recover from data deletion.

5. Protection from data tampering

Data inside protected storage must be tamper proof by integrating authentication and access control that ensures that only authorized users can change the data. In addition, to ensure that data manipulation that somehow bypasses the access control doesn't go unnoticed, digital signatures must be employed to detect unauthorized changes in the files.

6. Auditing and monitoring

Comprehensive auditing and monitoring capabilities are essential for security for several reasons. First, it allows the enterprise to ensure that its policy is being carried out. Secondly, it provides the owner of the information with the ability to track the usage of its data. Thirdly, it is a major deterrent for potential abusers, knowing that tamper-proof auditing and monitoring can help in identification. Finally, it provides the security administrator with tools to examine the security infrastructure, verify its correct implementation and expose inadequate or unauthorized usage.

7. End-to-End network protection

Security must also be maintained while the data is being transported over the network. The process of transferring data must be in itself secure. Users that store or retrieve data must be authenticated, sometimes using strong authentication mechanisms. In addition access control

must ensure that users only take appropriate action, and that only authorized actions are carried out.

8. Auditing is required to ensure that a detailed history of activities can be reviewed and validated.

A sophisticated user management scheme along with strong authentication capabilities is essential. Access control must allow the ability to departmentalize the data and the access to it, and detailed logs auditing and tracking of every activity must be available.

9. Process integrity

As data transfer is an essential part of a larger business process, it is critical to be able to validate that this step in the process was executed correctly. This requires the solution to provide auditing features, data integrity verification and guaranteed delivery options.

It's always comforting to know that there is still some honesty in the business world when we hear about Pepsi's action in alerting their main competitor. But I guess we have to accept that this is the exception rather than the rule; so who's deciding today whether to alert you to the fact that your corporate jewels are being hawked around, or are they just accepting that fate has dealt them a favorable hand. After all I'm sure there are quite a few out there who wouldn't say no to the south of France!

For further information about Cyber-Ark please visit www.cyber-ark.com or contact Adam Bosnian on 781-251-0670 or email adam.bosnian@cyber-ark.com.