perimetrix

FOCUS *on* Security

CHOOSING THE MOST VALUABLE OPTION TO PROTECT YOUR CONFIDENTIAL DATA

BEFORE WE DISCUSS the benefits of leak prevention tools, let's try to put ourselves in the position of an information asset owner and to understand what their essential requirements are. We can understand it quite easily by imagining a "valuable information asset" as a brand-new sports car that you left in a parking lot near a large shopping center. When you finally leave the shopping center with your bags, you look at the place where you had parked your car, and... What would you genuinely like to see happen in the above scenario? If you had to choose one of the following options, which would it be?

- I would like the shopping center CCTV cameras to quickly, and in great detail ***record everything that happened*** concerning the theft of my car.

- I would like to see the ***perpetrators found*** and punished for stealing my car.

- I would like to be fully ***reimbursed*** by the insurance company and provided with a taxi to get home.

What do you think of the above options? Are they encouraging? Anyone who owned such a car, out of all of the possible options, would actually prefer to have had their car **remain untouched**, exactly where it had been left. The same is absolutely true for owners of confidential data. The data must be protected to the extent that it simply cannot "leak". This is the most important requirement of the customer, to prevent a data leak from ever occurring in the first place.

Anatomy of data leak

Data or information, taken as objects to be protected, are at any given time, located in a certain "*container*" which is intended to be either temporary or permanent. This "container" can be paper, a file on a flash drive, a human brain, cloud storage, etc. From this perspective, a leak is defined as the movement of confidential data from a legitimate container to an illegitimate container, one that is not permitted by security policies to have access to the data. A leak also includes the use of an unauthorized transmission channel or the processing of data on an unauthorized computer or client device.

If we consider a data leak in this way, it becomes clear that it is technically possible to safeguard confidential data in a digital environment. However, data can only be protected if it is stored, moved or processed within a computer environment (e.g., in databases, complex multi-layer graphic objects, drawings, bulk text, audio or video files). Other, "simple" data that can be seen on a computer screen, eavesdropped, copied to a piece of paper or simply remembered cannot be protected by software. It is important not to have any illusions about this.

Do you need a means of offence or a means of defence?

DLP (*Data Leak Prevention*) solutions were created as an alternative to the rigid set of information security tools and policies often implemented for the protection of state secrets. Such rigid systems are not su itable for working with flexible and dynamic trade secrets.

The idea of monitoring data traffic through all possible communication channels, with dynamic detection of confidential data, is a beautiful idea in itself. Behavioral analysis, relationship mapping, and determining a user's degree of loyalty are a brilliant demonstration of the capabilities of DLP analytics. But what does this have to do with preventing data leaks?

Let's be honest: a system based on a **probabilistic approach** to determining the value of information **cannot serve** as a means of prevention. The system will either allow confidential information to leak, or it will needlessly prevent the movement of non-confidential information.

But if the purpose of a tool is to diagnose user loyalty, the aim of which is to identify possible leak scenarios as well as potential perpetrators, then DLP can certainly fulfill this role.

However, one shouldn't confuse the fight against data leaks with an investigation of incidents related to disloyal employee behavior. Nor should one confuse protection against leaks with the task of maintaining confidentiality. Both of which are quite useful and technically feasible in relation to a certain class of information asset as described above.

Defence of the security system

The principle of protecting confidential data should be both simple and without exception: *everything is prohibited except that which is explicitly allowed*. In other words, if you want to protect your confidential data from being leaked, there are several actions that must be performed.

First, clearly define what data you need to protect and assign this data a classification tag (a label that defines wich level of security is needed for access). Second, define the security perimeter for the classified data. This includes the allowed storage locations, transmission channels, permitted applications, and users with appropriate levels of authority. And third, use software and other technical tools to prohibit any actions that do not comply with the explicitly defined permissions. **That's when your confidential data will be protected.**

It is somewhat unfortunate that in this situation there will likely be very few incidents to investigate. And while incidents are the bread and butter of "leak control" tools, I would much rather prefer that my car wasn't stolen, and that it always remained untouched, where I had left it. ■

perimetrix

A Russian company founded in 2007, whose products have been trusted for more than 10 years to protect the confidential data of organizations such as AvtoVAZ, Gazprom Energoholding, the Federation Council of the Federal Assembly of the Russian Federation, TVEL and others. The company has a network of partners in Russia and abroad. The company's headquarters are located in Moscow.

www