perimetrix

BURSTS OF CYBER WARS

CONCERNING INTERNAL ATTACKS TO ENTERPRISE INFORMATION SECURITY

News about incidents in the field of information security from business giants such as **Apple, AT&T, British Airways, DreamWorks, Electronic Arts, Google,** etc. could certainly be used as the basis of a script for an action–packed blockbuster movie.

> The money involved can provoke full–fledged corporate cyber wars with insidious intrigues, real spies and professional hackers. But is it really necessary to be frightened of these *James Bond-like* scenarios, especially for the management of an "ordinary" company? A company that works with personal data "like everyone else"? Or a company where there is no data containing "state secrets"? Or where competitors are not high–tech monsters, but other similar organizations such as manufacturers, design institutes, trade and production enterprises? One definitely shouldn't be afraid. However, it is absolutely necessary to think about to evaluate one's own company from the perspective of possible cyberattacks.

Secrets – simple and complex

Almost every company has trade secrets. However, before you can begin to deal with their possible leakage, you need to first carefully analyze what exactly are your company's secrets.

Do you even have secrets? What corporate information delivers added value to your business that should be kept hidden from outsiders? Are your secrets "simple"? Is it possible to merely write them down on a piece of paper or memorize them so that you can reproduce them in their entirety to an interested party? Or are your secrets, on the contrary, fairly "complex" and exist in exclusive or hard-to-reproduce formats? Or are they created through the efforts of a significant number of people and therefore are even more valuable?

If the secret is "simple" and can be stolen in a relatively easy way (viewing, retelling, rewriting, photographing), then it is not worth wasting time and effort on very complex, technical measures. They likely won't help anyway. It would be more effective to monitor the actions of employees since they are the main "communication channel" between the company and the outside world. Safeguarding "simple" secrets will largely depend on employee discipline and loyalty.

However, if your secrets are contained in fairly complex formats (drawings, projects, research materials, databases, etc.), then they can only be leaked through "technical communication channels". This means that the protection of such information can be achieved with the help of specialized security tools. And, as strange as it may appear, the complex nature of your trade secret can actually simplify the very process of protecting it.

Everything is prohibited

except that which is explicitly allowed

The most important thing that the owner of confidential information (such as *the owner* of the company, a top manager, a developer, etc.) can do is to define and implement the “correct” process for working with confidential data.

However, you should not entrust this to IT specialists. Often, IT specialists don’t have a clear understanding of which business processes and workflows allow employees to access confidential information. They often adhere to the principle of “do no harm” (or even “it’s not within my scope”) and give employees the right to determine what can be done with confidential data. This, of course, does not in any way contribute to information security.

The situation does not change, even when access to confidential data is granted to only a limited number of employees. Remaining free to do whatever they want with confidential information, they will inevitably distribute it everywhere, because “it is more convenient for them”. But just as one can't be “a little pregnant”, one can’t keep a secret “a little bit”. It should be clearly understood that in relation to confidential data, only one principle is appropriate: *everything is forbidden except that which is explicitly allowed*.

The “10 MOST COMMON EMPLOYEE MISTAKES THAT LEAD TO DATA LEAKS” essentially all have one root cause: *disorder*. Disorder in terms of business processes and documentation within an organization and disorder regarding the lifecycle of confidential data. Despite all the modern DLP security solutions, employees still make mistakes that may lead to data breaches. Human error caused **90% of cyber data breaches in 2019**[1], marking yet another year-on-year increase.

To address this issue,

the following steps should be taken

— **Identify and classify confidential data** in order to separate it from “ordinary” information that will not cause damage if leaked.
— **Define how confidential data should be used** (e.g. created, stored, copied, and generally utilized in workflows).
— **Identify and standardize**, to the largest extent possible, **the main business processes** that are sensitive to information security issues.
— **Reduce** to the minimum degree possible **the ability of employees** to interact with confidential data.
— **Train and require employees** to be disciplined in adhering to the established security policies.

As a result of organizing and maintaining proper procedures when working with confidential data, the likelihood of the latests cyberattacks impacting your organization will be significantly reduced. ■

[1] SOURCE ↴ **Infosecurity Magazine, 2019**

perimetrix © 2021 Perimetrix LLC

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.