© zothen - Fotolia.com

The CSO's Myopia

by Jordan M. Bonagura

Before reading this article, imagine what it would be like to be able to manage your own company without your customers' data, or, imagine what it would be like if your competitors got hold of these data...

Well, it has long been established that data are extremely valuable for companies. Your customers' databases and the experience they have acquired through the years are fundamental, and they represent a great competitive advantage in this new corporative era.
With this in mind, we can see the importance of implementing specific policies in order to build a base which will guarantee that these data are safe.

There has been a recent increase in incidents related to security issues in a way that IT management has become more and more complex, and automatically the need for a new kind of professional, the CSO, has emerged.

The CSO has become the responsible person for risk areas, data security, and also for the definition and implementation of the security strategies and policies that the company will implement.

Such policies are developed to reduce risks and their impacts, and limit exposure to liability in all areas.

Figure 1 (top right) shows the direct relation between security enhancement and risk reduction. It shows that the higher the security, the lower the risks.

However, the major questions it addresses do not consider the urge for good professionals in security or the development of good policies. Every company must go through these steps when it decides to implement or organize such policies.

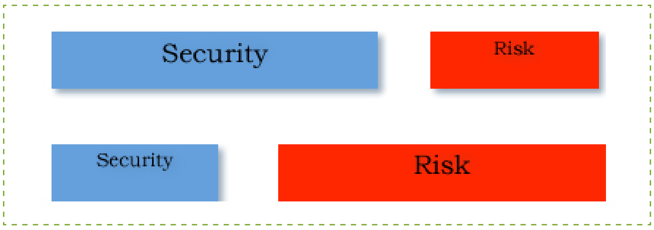
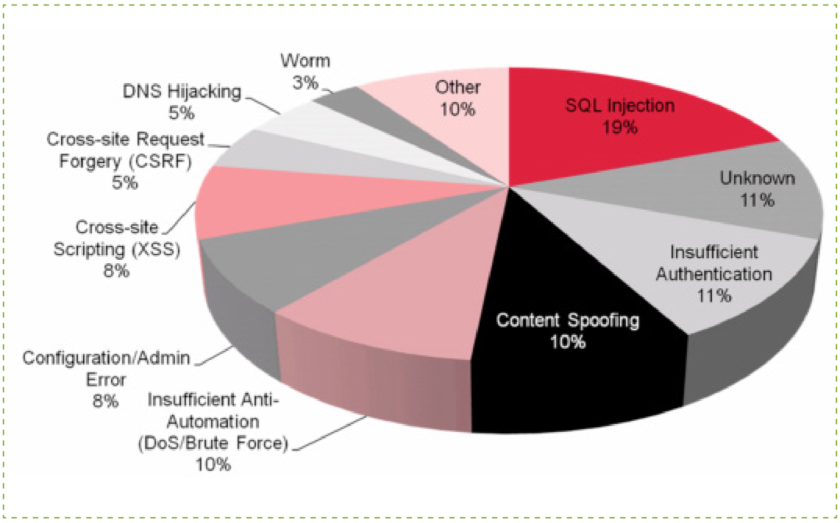


Figure 1

The "in-box" vision, commonly used at the time of creating these policies, is not enough to encompass all the company's existing range of vulnerabilities. When we analyze the graphic published by Breach Security Labs in August, 2009 on "The Web Hacking Incidents Database 2009", which demonstrates the vulnerabilities which were the hackers' most favorite during the first half of 2009, we obviously and automatically realize that a high percentage of them come from a particular breach in the SQL Injection (19%) – an opening for data theft. I say obviously, because, as previously mentioned, data is one of the company's most valuable assets.

What vulnerabilities do hackers use?



Source: Breach Security Labs

Such analyses are extremely relevant for a CSO, since they make it possible to enhance and update the logic control mechanisms (Firewalls, Anti Virus, IDS/IPS and, etc.) and thus reduce the risks relating to the well-known breaches that are addressed by the company's established policies. Furthermore, it becomes possible to take into account new ways to explore these breaches.

One specific risk I would like to briefly mention in this context is that there are people in charge of the administration and that people also make mistakes. Some might ponder that policies exist for this purpose and that they are there to be carried out precisely by the employees, yet it is worth emphasizing that policies require continuous review as much as physical and logical mechanisms require updating. And, also competent professionals involved in security matters require constant training.

Everything sounds perfect now, doesn't it?

Unfortunately not! Let's refer to the Bible where we find the line that says "the foolish man who built his castle on the sand ..."

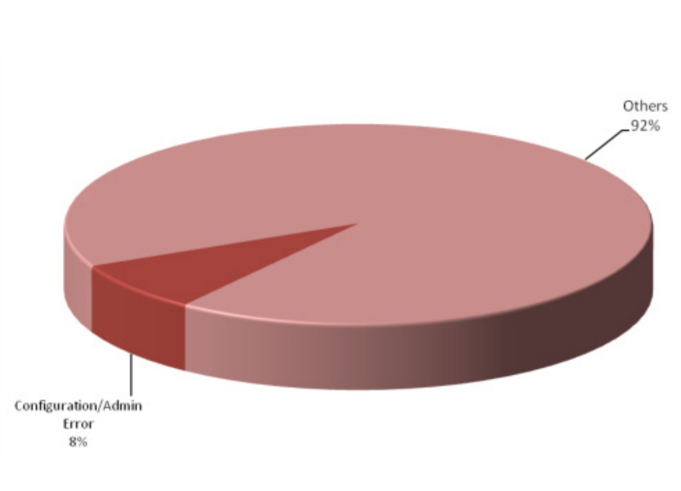
The major problem is that every security policy is developed with an "in box" vision, although a large range of well-known breaches are available "outside the box". In other words, the ones experiencing the problems are the ones who can't see them.

If the CSO simply relies on his own policy, he will not be able to see what it does not comprise and he will be deceived by his pseudo-security. That is what I call "CSO myopia". By believing in his defined policy, he thinks he can control the whole thing, when actually he is only controlling his whole policy.

I mean: **"Sometimes we hide the key under the doormat and forget to lock the door..."**

One of the main problems in this "myopia" is when we treat, for example, the risks concerning the errors of configuration and administration (Configuration/Admin Error (8%)) as in the graphic below.

What vulnerabilities do hackers use?



Source: Adapted from Breach Security Labs

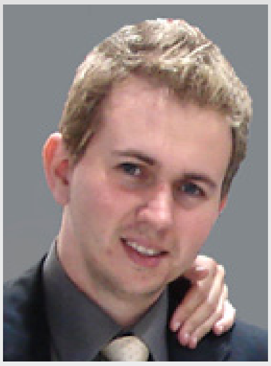
This sort of error, besides being considered a breach, may enhance the identification process and consequent exploration of other breaches. A practical example is the directory listing of a web server showing database configuration files.

Calm down! Not all is lost...

It is often difficult to have the "out box" 100% of the time when you are dedicated to the "in box" and mainly on the idea that everything is under control. A very important recommendation, in my opinion, is to resort to specialized consulting professionals (Pentest), who are experts at analyzing breaches, which are still not familiar to the company, and the different methods to explore the ones already considered by your present policy.
Attitudes like this might contribute to the decrease in the problems coming from the managerial myopia..

Keep alert, keep safe! □

> About the author



Jordan M. Bonagura
Jordan M. Bonagura is a computer scientist, post graduated in Business Strategic Management, Innovation and Teaching (teaching methodology and research). He works as a business consultant and researcher in information security with emphasis on new breaches.

He is lecturer in the area of information technology at various institutions, among them the Brazilian Institute of Advanced Technology (Veris/IBTA).

As a university professor he has conducted "in company" training at several nationally recognized organizations, among them the National Institute for Space Research (INPE).