2 Essential Strategies to Protect Against Data Breaches (Industry Perspective)

For a good defense, organizations must cover all vulnerabilities, external and internal.

BY ROMAN FOECKL / OCTOBER 28, 2015

Organizations and businesses must have a strong front line defense to protect themselves against data security threats. Organizations today, in both the public and private sectors, are facing daily threats on multiple fronts, including disgruntled employees, human error and external threats.

Let’s stop for a moment and think on the topic of chaos. Highly critical institutions like the Office of Personnel Managment and the Internal Revenue Service hold a massive quantity of personal data —data like Social Security numbers, birth dates and home addresses. And if breached, all hell can break loose, since these pieces of information can be used to obtain confidential data from other sources, like banks, insurance companies and health-care institutions. What may initiatlly seem like an isolated incident can become a serial ocurrence — and many times they're not connected.

For a good defense, organizations must cover all vulnerabilities, external and internal. And lately, internal vulnerabilities are surfacing more and more.

1. BUILD A FENCE AROUND YOUR INSTITUTION

External threats are the most targeted by data security professionals charged with keeping an organization secure and out of news headlines.

Since the first versions of antivirus software appeared in the 1990s, this has pretty much been the strategy. And it is not wrong; malicious people apply a multitude of schemes to penetrate companies’ networks and get ahold of sensitive data. Just in the last few years, many methods of attack have emerged: phishing, social engineering, BadUSB and Denial of Service, to name a few.

Possible entrances also have increased in number: mobile devices, wearables, portable storage devices, mobile apps and others. Most of these attacks are prevented by antivirus software, firewalls and IPS software, which serve as a fence around the institutions and block external attacks. This solution can be likened to ancient times, when people built defense walls to protect their wealth and their rulers.

2. UNCOVER THE "MOLE"

Also in ancient times, there was always a mole ù an insider who disclosed the defense strategy to the enemy. By the time they discovered the mole, the soldiers were already on the battlefield, waiting for the enemy, which eventually surprised them and won the battle.

In companies, most "moles" are actualy non-malicious employees who disclose confidential information, such as marketing strategy, private health-care records and personal identifiable information by mistake. Usually they lose thumb drives containing that data; they publish pictures on social media with their monitor behind them; they write passwords on the whiteboard (http://www.endpointprotector.com /blog/sysadmin-day-2015-contest-infosec-bloomers/). Although their intentions are not malicious, their actions should not be overlooked. Insider threats represent the cause of data breaches in more than 50 percent of the cases, so it's a major threat that all organizations, no matter the size or sector, should take into consideration.

There are several methods to tackle this type of threat. To prevent navigating to malicious websites or publishing confidential information, many organizations control what applications employees can use and what websites they can visit. Although when it comes to collaboration tools like Google Drive, Dropbox and Skype, which increase productivity, denying access is typically not the best strategy. On the other hand, not monitoring what information is being published on cloud storage and file sharing services is not an option either.

Being able to see exactly what files are being uploaded, what data is copied, what print screens are made and through what means is key in uncovering a "mole." It all depends on the flagged confidential data by the IT security specialist and the monitored points of exit. This is possible through data loss prevention (DLP) solutions, which have been popular on the IT security market since 2007/2008.

DLP solutions help detect unusual activity, like the transfer of a big number of internal documents to a non-trusted recipient or application. This essentially prevents a potential attack on another organization that makes use of the same data, such as banks, that save their customers' home addresses.

In the end, no matter the chosen solutions or methods, it is important to follow the two objectives above: Build a fence around the institution and uncover the "mole," meaning

to cover both external and internal threats. It all comes down to defeating your foe with the right weapons.

Roman Foeckl is the CEO and founder of CoSoSys, a cross-platform data loss prevention, device control and mobile device management solution. Before founding the company in 2004, he worked for Goldman Sachs in Frankfurt, Germany, and Paris.