The Fundamental Principle of Breach Prevention

Rui Biscaia

The fundamental principle of breach prevention

Rui Melo Biscaia

Watchful Software, Coimbra, Portugal
rui.biscaia@watchfulsoftware.com

1 Introduction

Information has evolved to become a crucial commodity, requiring just as much security as any other tangible asset. People take it, use it, and 'leak' it out and organizations are challenged to protect a growing quantity of valuable digital information against careless mishandling and malicious use. In addition, a growing list of legislative requirements adds to the ongoing task of protecting digital files and information.

For the past decades, vast amounts of money and countless hours have been invested in breach prevention. The order of the day has been to harden network and server access through the deployment and redeployment of an evolving series of firewalls, anti-spam/anti-virus applications and intrusion detection and prevention systems – all of them, in essence, attempts to 'reinforce the perimeter' to protect what lies within.

While this remains good and necessary IT practise, it takes no account of two very important and inescapable truths: a) users are always inside the perimeter, and b) even those authorised users can cause significant damage. By ignoring these, CI(S)Os fail to address possibly the most fundamental persistent threat, that of a breach orchestrated by one or more of their organisation's own users.

Information leaks are all too often caused by trusted insiders, people with the right and credentials to be behind the firewall, who leak information whether knowingly or unknowingly. The sheer numbers and types of external storage media available make it very easy for information to leak out. Moreover, corporations are increasingly being held legally liable for the safeguarding of information they hold on their own employees as well as on their customers.

2 What is a malicious insider?

According to Carnegie Mellon University's CERT Insider Threat Center, which offers comprehensive and authoritative research on insider threats, a definition of a malicious insider is a "current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems."

Also, according to the CERT Insider Threat Center, the employees that pose the greatest risk for insider threat/theft include:

1. Disgruntled employee – This is usually the employee who feels personally disrespected, possibly due to a missed pay raise that was expected or a negative encounter with supervisors over benefits, time off, demotions, transfers or other similar issues. In this instance, revenge is the employee's motive.
2. Profit-seeking employee – This is a simple motivation for many people. They work for a wage; however, by stealing information, they can make more money selling the stolen data to organized criminals or modifying the data to steal an identity. The information could be easy to access and steal for the employee, plus the theft can be rationalized because, as a malicious insider might say to himself, "The Company won't even miss it". Motivations in such circumstances could include large financial or drug-related debt.
3. An employee moving to a competitor or starting a business – For someone starting a business in the same field, the theft of customer lists, business plans, and even simple forms or templates can be tempting. Alternatively, imagine the employee leaving to work for a competitor. Perhaps the competitor has hinted that an exchange of information can be made for a better position when the employee comes on board.
4. Believe they own the code or product – In this case, employees feel a sense of ownership over code they wrote or a product they developed. Therefore, they take the code for their future use or even for their next job.

3 Data-centric Security

The way to effectively and efficiently address those concerns seems to be Data-centric Security, whose focus is to classify and encrypt sensitive or confidential information and ensure that only properly authorized people have the key to decrypt it. Thus, even if an intended or unintended breach occurs, whether the information is sent, left on a USB key or stored on a web drive, the data can't be seen or used by anyone beyond the authorized audience.

The first step to accomplish Data-centric Security is encrypt confidential and sensitive data. This can be done automatically, without the user being involved in the process. Enterprises should develop dynamic global data policies, so that when information is created (be it an email, document, spreadsheet, presentation, engineering drawing, etc.) it is automatically encrypted using a secure wrapper. This protection lasts throughout the lifecycle of the information, regardless of how many times it is sent, opened, stored, saved or edited. The information will always have this classification and encryption wrapper protecting it, even if it's sent, carried or stored beyond the enterprise's secure IT perimeter.

The next step is to ensure that the keys are centrally stored and managed. Each time an attempt is made to use that protected information (to open, print, forward, etc.) the wrapper 'reaches out' to the central server managing the keys (more accurately, a list of who has the rights to what levels of information). Effectively, the wrapper asks: 'has this person the right to use me?'. If the answer is 'yes', the action is allowed. If the answer is 'no', then the encryption stands firm and the object is useless.

Moreover, in effective Data-centric Security, all interactions with the rights management server (requests to open information, to print it, to forward it, to save it, etc.) will be saved for future forensic, auditing, and tracking purposes. The records of interactions will be useful in cases where the attempted breaches were not unintentional.

4 Information Security "Rules of Thumb"

As with most approaches to Information Security, layered defenses need to be implemented to reduce insider threats. As there's no silver bullet, a recipe for success starts with following some simple "rules of thumb":

1. Information should be classified. This can be done in one of two ways: either manually, by the author; or dynamically, according to content and context aware policies established by the company. Advanced data-centric security solutions allow information to be classified as it is created (in the case of documents, spreadsheets, presentations, etc.) or as it is sent (in the case of messages and emails);
2. Information should be protected. Quite simply, the best way to protect information is to have it encrypted. There are many different types of encryption, and people employ encryption at different parts of the equation (on the drive, in transit on the network, etc.). Experts today, however, are agreeing that instead of trying to encrypt the physical media where the information might be stored (the drive, the network, etc.) if you simply encrypt the information itself then it's protected regardless of where it is. If it's on a laptop drive, it's encrypted. If it's in transit across the network, it's encrypted. If it's in a cloud based drive, it's encrypted. If it's on a USB key hanging around someone's neck, it's encrypted. What that means is that this information is persistently secure... regardless of whether it in inside or outside of network boundaries;
3. Information should be accessed based the user's "need-to-know". Users should be assigned appropriate security clearances and access to data should be granted based on the user need-to-know according to his job description and the classification of the data itself. Hence, enterprises should enforce separation of duties and privilege, thus not allowing access to sensitive information that the employee has no reason to view, obtain or download.
   In a nutshell, Insider threats can (and probably have) happened to every enterprise. Those organizations that are knowledgeable of the risks and are well prepared for such eventualities will thrive reducing and/or preventing the insider threat.