Cybersecurity Weaknesses and how to protect your organization

NEOCLEOUS

Introduction

What makes law firms different from any other organisations and attractive to cyber-attackers is the legal rules that require maximum confidentiality between attorney and client. Law firms hold a great deal of data which has huge potential value, particularly in the wrong hands. This could be commercially confidential information concerning deals or negotiations, companies' vital private data or simply sensitive information that clients prefer to keep out of the public domain. One of the examples we recently witnessed is the leak of 11.5 million files from the Panama-based law firm Mossack Fonseca. The leak uncovered secret offshore deals and vast loans exposing offshore companies and the involvement of 128 politicians and public officials around the world.

The reality is that no company or organisation can be completely immune to cyber-attacks. The best that can be done is to take every possible precaution against them. Cyber-attacks are a daily threat to organisations and individuals and are constantly increasing in sophistication. If an organisation is not vigilant and well-prepared it may fall victim to an attack, resulting in significant economic loss and reputational damage.

In law firms as in other organisations there are certain procedures and defence systems that could safeguard the infrastructure and sensitive information.

Identifying threats

There is a common misconception that hackers are near-magical beings endowed with an array of supernatural abilities holed up in a basement, their faces lit up by a screen of green-on-black blocks of code screen, aggressively typing away at the keyboard and intruding into remote systems or infrastructure. On the contrary, successful hackers are mainly people with highly developed communication skills, which allow them to psychologically manipulate users in order to trick them into giving away sensitive information or even direct access to data. This technique is known as social engineering.

"All the technical controls in the world are worthless if you share your password or hold the door open."

Employees have long been recognised as the weakest link in an organisation in terms of cyber-security. Statistics have shown that employees are the direct cause of more than 70% of data breaches. Some may be disgruntled individuals intentionally seeking to cause harm to the organisation by disseminating confidential data. Others may be inexperienced employees inadvertently giving access to confidential data by negligence, for example by accessing a harmful website, clicking on a link or downloading an attachment included in an email, which covertly

installs malicious software on the individual's computer. One form of malicious software, known as ransomware, can allow the attacker to encrypt all the organisation's data so as to demand a ransom payment to decrypt it. Another technique, known as phishing, tricks users into disclosing their username and password.

From a digital forensics perspective, it is more likely that the "Panama Papers leak was internal rather than the result of external hackers transferring data over the network. Given the immense volume of data involved (2.6 Terabytes), the transfer would either have had to be to carried out using a technique called "low and slow", in which case it would have taken several months or longer, or else it would have been immediately detected in a direct transfer of files.

The cybercriminals' arsenal is getting bolder and more sophisticated every day. Malicious software such as viruses, backdoors, botnets and ransomware, the latest type of malicious software, can penetrate the network and cause harm to the target in the form of damage to systems, unauthorised access to users' data and withholding of access to essential data. All that is needed for this malicious software to be deployed and cause harm is poor housekeeping such as holes in the network and system vulnerabilities such as unpatched computers and servers or out-of-date antivirus systems.

How to protect.

The main objective of cybersecurity is to protect the network and sensitive information of the organisation against unauthorised access or attack. IT departments and security professionals need to always stay one step ahead of the changing tactics and approaches used by hackers.

The first and most important approach to protect the organisation's network is to identify the possible threats and mitigate them according to cybersecurity best practices.

Employee Awareness

As previously noted, the weakest link in an organisation's cybersecurity is generally its employees. The best protection against an inadvertent security breach due to employee negligence is a combination of employee awareness programs and effective security policies and procedures. According to the US Department of Defense, "Employee awareness is a countermeasure against those vulnerabilities and a means to reduce human-related risks. To maximise the protection of systems and information, it is essential to maintain a federal workforce that is aware of, trained on, and educated about information security and assurance."

An effective awareness program will help users to understand their role in keeping the organisation's cyberspace secure. Users who have undertaken a successful awareness program will think twice before opening email attachments, following a link on an email or using a weak password. In addition, users will also be able to distinguish a legitimate email from a phishing mail and will know how to apply the relevant rules to avoid falling into the trap.

Patch Management and System Updates

Patch management is the term used to encompass software updates, not only to implement new features of the software but also, and most crucially, to fix a bug or a security vulnerability in the system. If system and software updates are systematically downloaded and installed as soon as they become available, the vulnerabilities that virus writers rely on to infect the computer are removed.

It is important to discard any old hardware on which operating system support has been discontinued by the manufacturer. For example, Windows XP and early versions of Apple OS X are no longer supported and updated, making them more dangerous to use and vulnerable to attack.

Email Gateway Security

Enforcing the human factor is of course a great benefit but technologies need to be implemented and upgraded in order to safeguard the infrastructure. As the human error factor can never be entirely eliminated it is essential to put in place effective security controls to minimise the possibility of a malicious email being received in the mail servers of the organisation and becoming available for an unsuspecting user to download.

An ideal email gateway security uses technology based defences such as antivirus and spam filters to analyse email attachments and malicious URLs and to successfully quarantine malicious emails used in advanced attacks.

Data Leakage Prevention (DLP) and Data Encryption

Controls such as DLP should have prevented data leakage on the scale of the Panama Papers leak. DLP is a solution whose purpose is to prevent data breaches by intruders. DLP solutions analyse and identify the confidentiality level of all the organisation’s data files and prevent transfers or create alerts in the case of unusual activity.

Data encryption provides an additional layer of protection by using keys to encrypt and decrypt the data in the network so that even if a malicious individual were to gain access to the data, it would not be readable and would be useless to the attacker.

UTM Firewall

Traditional firewalls have increased in sophistication and evolved into Unified Threat Management firewalls providing additional capabilities and functionality such as spam blocking, gateway antivirus, spyware prevention, intrusion prevention and URL filtering. A great advantage of UTM firewalls over traditional firewalls is application filtering which evaluates network packets for valid data at the application layer before allowing a connection instead of managing ports.

End User Antivirus

The advantage of having effective antivirus protection is directly related to the potential consequences of not having any protection. It is the most basic security solution, but it will at least protect computers from the most prevalent viruses by scanning the system against the known signatures of these viruses. It is essential to download and update the antivirus software systematically and be up to date with the latest virus signatures.

Conclusion

An inevitable consequence of our ever-increasing reliance on ever more-sophisticated digital information systems is the risk of loss, leakage or corruption of data. Organisations have become highly dependent on cyber infrastructure and measures to prevent and safeguard them from cyber-attacks are vital. Incidents such as the Panama Papers leak should be a wake-up call for all and cybersecurity should be regarded as a tier one threat to the organisation's security.

Michael Ioannou