Greg Sim examines why law firms must require a new approach to prevent data theft

LOOKING BEYONI

The UK's most valuable and sensitive commercial information lies in the hands of the nation's law firms. This simple fact makes cyber security and data protection a top priority for these organisations. Despite this, many firms are relying on obsolete technology that is centred on perimeter security to protect their coveted documents, completely ignoring file-based threats. Worryingly, this is the weapon of choice for many successful cyber criminals, which make conventional security methods completely useless.

"Across the legal landscape there is little information about the huge growth in security threats carried in email attachments," says Janet Day, former IT director at a major UK law firm. "Open and free exchange of documents is the lifeblood of the legal profession, but there needs to be a recognition that email attachments are the most dangerous point of vulnerability."

While the reluctance to move forward with technology is not unprecedented, it carries with it an immense amount of risk. The databases of large, and even medium-sized firms, are home to a wealth of commercial information, such as data on trademarks, patents, mergers and acquisitions, corporate tax affairs and the activities of wealthy individuals. Needless to say, this data will likely pose a serious threat should it fall into the wrong hands.

Cyber criminals, business rivals, hacktivists and well-funded government organisations operating from the shadows are all looking to obtain this valuable information. The most successful style of attack these groups are currently utilising involves hiding sets of coded instructions within common file types sent out via email. Once these files find their way into an organisation, the results can be disastrous, with mass volumes of private information being pulled from databases.

Highly innovative and equipped with the latest methods and technology, these groups have the power to destroy the reputation of any law firm that has neglected its defences. Even facing a potential £500,000 penalty from the Information Commissioner's Office for breaching data protection legislation can seem miniscule when put up against the damage a firm can receive should it clients lose trust.

Cyber security is expected to become the number one priority for law firms, along with other organisations, as they prepare for the European General Data Protection Regulation to come into effect next year. The new law will enforce steeper fines on companies who fall victim to a data breach, who will also be publicly named, potentially spelling disaster for their reputations.

Though many law firms are taking the security of their data more seriously, the systems they have in place will always fail against new threats. Currently, many are utilising costly perimeter security solutions such as email scanning, firewalls and web controls, which only stand up to threats that are already widely known. With new forms of cyber attacks being developed every day, these types of solutions offer little solace.

©Getty Images

Law firms need a robust security system to ensure that only clean files get onto their computer system

The cold hard facts are that, across all businesses, roughly 94 percent of successful data breaches are the result of file-based attacks, and the figures continue to grow each year. This is leading to a lack of trust organisations have in their current security suppliers, as well as solutions billed as "new approaches" such as sandboxing, and a clear move towards embracing innovation.

Cyber criminals are walking the well-trodden route of emails and file attachments – which lawyers and their colleagues use hundreds of times each day – in order to reach the private information hidden in their databases. In order to prevent a data breach among the growing scale and complexity of cyber crime, it is crucial for law firms to acquire a solution that is 100 percent effective when dealing with currently existing and future file-based threats. This can be achieved by only allowing

O THE PERIMETER

clean versions of original files into the system, and the technology to do so is already available.

This technology has the ability to create replicas of the original files – whether they be PDFs, Word, PowerPoint or Excel files – free of any malicious lines of code that may be hidden by cyber criminals within the DNA of the file, and within mere seconds.

Perimeter security measures, even sandboxes, are unable to detect this malicious code. Sandboxes in particular are designed as quarantines in which files are analysed for mere minutes before being deemed safe. The tampered files used by cyber criminals, on the other hand, are programmed to set off weeks or even months after being embedded within a company's systems. One of the major flaws in sandbox technology is that it is backward looking, as it only searches for lines of code that have already been identified as malicious. Therefore, any cyber criminal using newly developed exploits will be able to sneak the code through any sandbox, as the technology won't recognise it as malicious.

In addition to offering little defence against file-based threats, sandboxes also produce high amounts of false positives – in some cases over 60 percent – which can take up mass amounts of time for IT teams to resolve them. With law firms emailing thousands of complex documents in many different formats to their clients and other third parties across different kinds of systems and devices, detecting malicious code within files is not an easy task. Furthermore, many of these corrupted documents originate outside of the usual orbit of the law firm.

Innovations in hackers' operations are making traditional perimeter security look even more obsolete. In many cases, these hackers are utilising social engineering in order to gain access to private data. In order to fuel their social engineering operations, cyber criminals use metadata acquired from a number of sources, such as files from a firm's website that have not been cleaned, data that has been leaked by unprotected partners or files intercepted during exchange in order to identify

LOOKING BEYOND THE PERIMETER

©Getty Images

Lawyers need to be confident that private and secretive data is protected from intrusion

information such as user IDs, server paths, software versions and even employee reference data.

By accessing this information, cyber criminals can then forge a convincing email to an employee, posing as a trusted regular contact and trick them into opening a link that sends a zero-day exploit into the firm's system to be set off at a later date. In order to prevent this, firms must ensure they prevent data leakage caused by poor internal processes and weak management protocols, keeping insider information away from cyber criminals.

Due to the innovative nature of hackers and the inadequacy of traditional perimeter security measures, law firms must turn towards a solution based on file-regeneration, one that boasts total security and full protection against macros and other malicious agents.

Some advanced security solutions are able to conduct thorough analysis of files and produce clean and perfect copies of legitimate documents free of any malicious code and in real time. They do this to protect organisations from the most complex and persistent file-based attacks by looking for the "known good" in the file after breaking it down to the byte-level and regenerating it in compliance with the manufacturer's standards. The solution keeps malicious exploits on the right side of the virtual glass wall, away from the firm's system. Additionally, it can also restore files that have been corrupted due to frequent use. Such a solution needs to be 100 percent effective in eliminating file-based threats, while also reducing the amount of money and time normally wasted on perimeter security measures, for example, by eliminating the need for IT staff to analyse the many positives produced by sandboxes.

The solution should also put control back in the hands of those at the corporate level, allowing them to make high-level decisions on security policy, as opposed to delegating it to employees. Essentially, this allows the board of a law firm to adjust the protocols regarding cyber security based on which file types individual users need.

While preventing file-based threats from carrying out their malicious tasks, the solution needs to be able to be action intelligence on the innovative nature of threats, comparing unknown file structures with known and established standards. This represents a huge advantage for law firms, many of whom encounter far more unstructured data than any other type of business on a daily basis. This level of intelligence allows boards to be frequently informed of the status of their cyber security, presenting this information in an intuitive and comprehensive way.

Law firms will also be able to prove their compliancy with best practice to both regulators and other third parties. Many banks have already adopted the practice of requiring their partners demonstrate compliancy with cyber security standards. This practice will only become more common as the European Union begins to implement new data protection regulations.

In conclusion, it is essential for law firms to keep in mind the modern reality of threats when considering a new approach to cyber security. In 2014, a Freedom of Information request to the ICO showed that it had investigated 173 law firms in relation to over 187 potential breaches of the Data Protection Act, 29 percent of which were related to security. The annual cost to the UK is estimated to be £36 billion. With the already huge level of risk growing each day, it is crucial for law firms to adopt a security solution that guarantees 100 percent protection from file-based threats.

Janet Day, former IT director at a major UK law firm, is insistent that adopting technology that enforces "Best practice" for all files entering or leaving a system is a necessary measure for all law firms, considering the potential damage that a data breach can have on the reputation of any organisation, not to mention the fines and penalties enforced. As she has said in the past, it will allow the free flow of information and permit fee-earners to continue with their work without risking the immensely valuable data stored in the database.

Greg Sim – Chief Executive Officer, Glasswall – is an entrepreneur and investor with a successful track record of fund raising and strategy realisation. Throughout his career he has also successfully founded and sold a number of businesses.