KCS Group Europe

Is your data secure? Mossack Fonseca, a lesson learnt

27 March 2018

The closing down of the law firm Mossack Fonseca is only few days away. The firm has in fact announced that it will terminate its operations at the end of the month, after more than 40 years of service. The decision came after irreparable damage was inflicted on the firm as a result of the Panama Papers leak two years ago.

Established in 1986, Mossack Fonseca was one of the biggest law firms, boasting offices in more than 40 countries all around the world and innumerable collaborators. However, it mostly remained hidden until it was hacked in 2016.

The breach led to the divulging of 11.5 million documents, 2.6 terabytes of data, obtained from the Mossack Fonseca database. The hack is recognised as the biggest leak ever, even surpassing the famous WikiLeaks and Snowden's revelations. The documents contained emails, files, bank records, and PDFs related to some of the world's most powerful people. In fact, from the documents it emerged that twelve heads of state and 140 politicians were Mossack Fonseca's clients; they were avoiding taxes by setting up offshore entities. Multiple investigations have started. Amongst those there were Pakistan's Prime Minister, who had to resign from office in July because of the leaks, as well as some of Putin's close friends.

Mossack Fonseca is closing down as a consequence of a cyberattack. Today the cyber threat represents the greatest danger we face, and this particular case clearly proves it. The Mossack Fonseca case should be taken as a lesson to be learnt quickly as the time left to comply with the new provisions, GDPR and NIS directive, is running short.

The law firm was negligent on various cyber security aspects. First, the hacker that penetrated the system exploited various vulnerabilities. In fact, the access was gained through WordPress's Revolution Slider vulnerability as Mossack Fonseca's version was not updated and therefore easily exploitable. At the same time an SQL injection flaw was also detected on the system. That was the first mistake the company made. It is fundamental to have always updated software versions, as that is the most common point of access utilized by hackers. Especially when dealing with customers/client's data, the company is responsible for ensuring that their information is efficiently protected.

Secondly, Mossack Fonseca was storing all its data on the same server. Segmentation is a simple requirement that would help limit damage in case of a breach. Clearly Mossack Fonseca did not see the benefit of good practices. Given that nowadays everybody is vulnerable to cyberattacks, solutions to buffer the damages should be in place; decentralisation and division of critical data should be the first step, along with avoiding storing old unnecessary information.

KCS Group Europe

Is your data secure? Mossack Fonseca, a lesson learnt

Thirdly, businesses should always encrypt their data. Mossack Fonseca failed to do that. Obviously, the more layers of protection applied to the data there are, the safer those will be. Fourthly, proper monitoring of data flow would have spotted Mossack Fonseca's breach in live time. Finally, Mossack Fonseca did not have any risk management plan ready and therefore what came after the breach was unexpected and inevitably led to the dissolution of the firm. An incident response strategy would ensure the correct handling of a crisis situation and the restructuring of the business reputation.

Mossack Fonseca was negligent in taking the appropriate security and protection measures to ensure confidentiality of its clients' data. Had it applied the required actions, the hack would have been prevented or at least the consequences buffered. With spring, new cyber security requirements will come into force and companies will be expected to fully comply with the laws. The GDPR especially prospects heavy fines in the eventuality of a failure of compliance. The new regulations are aimed not only at safeguarding client's data but also at protecting a business's reputation and preventing their dissolution as a result of any breach, as it was for Mossack Fonseca. The law firm committed various mistakes and it is paying the price of those. The Mossack Fonseca case should be taken as a lesson. In a time where nothing can be secured anymore businesses should do their best to have in place efficient protections and to comply with the requirements; accepting that we are all vulnerable we can now only hope to contain the damages – rather than taking the arrogant assumption that hacks and breaches will only happen to other firms.