Marriott data breach: 500 million times concerned

January 2 2019, by Bertrand Venard

On November 30, 2018, Marriott International announced an enormous data breach concerning 500 million clients, the second biggest ever. With new data breaches being announced almost daily, you have to ask yourself, how is this possible?

Given the number and the magnitude of all the data breaches, stealing data on the Internet seems easy. However, hackers' failures are not much reported, since as for any crime, their unsuccessful attempts are by nature hidden. Clearly, criminals keep trying to break information systems, at least because there are plenty of easy targets in cyberspace and because that's where the money is, as the saying goes. For example, in general, individuals are not really protected themselves. Many people buy connected devices and forget to change the default password – it's like leaving your house keys on the door. Every parent should fear having hackers talking to kids through their toys.

Also, many small businesses have very often have little or no cybersecurity. In some cases, the hackers could do whatever we want. Once, they stayed 10 years in the information system of one company. The only good news is the poor quality of the information in their databases. Like: "Mr Smith123 lives in New iork cityu, Thailand, Passeport number: ABCD. Credit Card: Expired five years ago". With so many errors, such databases are not worth anything.

Plenty of cases

Of course, major companies are clearly the targets of skilled hackers. In recent years, plenty of them or their subsidiaries were victims of piracy such as at Equifax, Yahoo, Facebook, Uber, eBay, Home Depot, FedEx, JP Morgan Chase. In the new Mariott Data Breach, the pirates stayed four years quietly sucking the Marriot information system dry. The criminals were able to getting out sensitive information about the 500 million guests. No problem at Marriot with their new golden rule: "travel brilliantly", protect strangely, hack splendidly.

Green flags for hackers

Looking at the different cases, hackers seem to be looking for Green Flags before acting. Thus, each time a firm launches a new product on a large scale in a very competitive market, and strive to beat competitors, the firm may forget about logistics and cyber security and therefore, this moment could be an opportunity for hackers. Also, the structure of organizations could give a "go" sign to pirates. When the Chief Information Officer reports only to the Chief Financial Officer, a cost reduction strategy may imply low cyber security budgets. When a new CEO screams to investors that it is time for austerity and drops in spending, cyber security programmes could suffer and hackers could be welcome. The Marriott case illustrates another green flag moment: a new merger or a great acquisition. Indeed, the hackers may invite themselves to the "wedding". In such situation, executives are occupied to fight to keep their positions and to influence the business, but at the same time, the difficult integration of different information systems create security issue. The hackers could take this opportunity to break in.

Facing so many cyber security issues, we could question governmental actions. The government defence is very difficult since hacking is more than often transnational and hackers hide their path. For example, the Marriott breach has been linked to Chinese Ministry of State Security. Pirates working for abroad and protected by their governments are

obviously hard to catch. Curiously, governments could also help pirates. For example, when the United States Computer Emergency Readiness Team (CERT) notified the world about the Apache Struts issue, hackers started to surf Internet to look for potential victims. However, the Equifax staff failed to apply patches to the flaw and after 76 days and 9000 queries (of course unnoticed) did Equifax staff start minding about a data breach that concerned over 150 million people.

No 100% safety on the Internet

With so much success, the question is: should we be worried? As the Marriot website stated: "We seek to use reasonable organizational, technical and administrative measures to protect Personal Data. Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure." Indeed, as the Marriott cyber experts: no safety is possible at 100%. So, all of us should be worried since there is no safe place in cyber space. In the end, whatever the technical layers of security, there is always a human mistake to be made. The hackers are just waiting for it.

Provided by The Conversation