I WILL REMEMBER LATER... BUT NOT WHEN IT IS TOO LATE!!!

By Marcelo Rito

Many people leave their house at certain times, they frequent vulnerable places and never imagine that sitting on the couch in their living room with their laptop, watching Internet TV, shopping or even playing a harmless game like Candy Crush, for example, can put them in harm's way.

It is a bad habit of many technology users; we put off updates until later, but, at the beginning of May, it was discovered that not only regular people, but also large corporations omit to perform such updates.

More than 70 countries were infected by a major data kidnapping event which was recently reported. Thousands of computers were infected and important services such as banks, operators and hospitals, among other, stopped functioning. In an extremely invasive offense, the person responsible for the attack, until now unidentified, requested a specific ransom in Bitcoins, a digital currency that is impossible to track.

This is not new, not only because we tend to suffer from "digital laziness", but also because we have failed to learn from previous cases of digital kidnapping.

Because of this, Ransomware is attracting widespread attention, and for good reason.
Ransomware, a type of program that infects a device (malware), silently encrypts the data and renders the archives inaccessible. To free the system, the software requires a ransom to be paid. Two options exist: paying the ransom, or attempting to recover the lost data by other means, such as backups. Meanwhile, the Ransomware could be spreading throughout the network and as well as all devices that connect to it.

These attacks do not generally have a focus, they can affect anyone.

Imagine yourself during the holidays, and the hotel where you are a guest has its data kidnapped, preventing you from enjoying yourself as you had planned. A luxurious European hotel, The Romantic Seehotel Jägerwirt, located more specifically in the Austrian Alps, admitted to paying thousands of dollars in Bitcoins to recover, from the hands of cybercriminals, its electronic door system (IoT) for the guest rooms. The hackers attacked the system with Ransomware and only when a sum had been paid in Bitcoins did they open the doors and "free their clients". The manager of the establishment, Christoph Brandstaetter, informed us that on a perfect day with maximum occupancy, there would be no other way but to pay, because neither the police nor security could help with the guests being held hostage.

Only after having been attacked three times and having paid thousands of euros did hotel administration make the decision to invest in a completely new security system so the hackers would not succeed in a fourth attack in the future. Because of this, the next time, the system was not compromised.

No institution is immune from cyber criminals. A major attack occurred in May 2017 and in China alone more than 29 thousand institutions were affected. The majority of them, more than 4 thousand, were educational institutions, such as schools and universities. Imagine a hacker kidnapping all the report cards and the data of hundreds of alumni. The cruelty of this specific attack does not spare anyone, not even hospitals and public services, both in the United Kingdom.

What to do?

It is estimated that the practice of cybercrimes using Ransomware programs has collected 1 billion US dollars in ransom in 2017. In fact, with only the use of one type of Ransomware, the Cryptowall, it is estimated that 325 million US dollars were generated in the last year alone. Small habits can minimize our risks, among these are:

- Constantly back up all critical data, in order not to become a digital hostage and to lose information relevant to your business;
- Keep the systems operational, always update your mobile devices;
- Be cautious; never click unknown links or open messages from unknown contacts;
- Remove unnecessary archives from the network;
- Always change your passwords. Be smart about this and avoid birthdays, names of loved ones or information that is obvious or personal;
- Integrate security

Hackers are constantly perfecting their strategies, in such a way that proper security comprising of several layers is essential. As we start to build or improve our defenses against Ransomware, a key question comes up: on what are we currently focusing our security reinforcements? A multi-layered defense is essential to protect critical business systems, especially from Ransomware and Malware in general and a variety of other threats that are always evolving.

Be like the hackers! Perfect your strategies! Constantly gather information on everything that is new in order to protect your personal digital life and your corporation's data. Remember to update your protection before it is too late.

Author:

Marcelo Rito

He holds a post-graduate degree in Cyber Security and is a specialist in Security Solutions. He works in the field of security and infrastructure since 1998.

He has worked in large organizations such as Embratel, Brasil Telecom, Marista and Santa Casa de Misericórdia.

He has worked on large scale security projects , such as Telefônica/VIVO, CEF - Caixa Econômica Federal, Supermercado SONDA, SEE-PE Secretaria da Educação do Estado de Pernambuco, PRODEB - Cia de Processamento de Dados do Estado da Bahia, MINICOM - Ministério das Comunicações - DF, among others.