Author: Jorge Orillac

The evolution of corporate cybersecurity in the digital age

Every day the threats and dangers from cyberattacks are more sophisticated and cybersecurity plays a crucial role.

Protecting your business is paramount. For this reason, around the world, hundreds of companies invest significant amounts of money each year in surveillance systems, as well as protection and prevention of possible risks to data security and business continuity.

However, what happens when these transgressions are invisible or unnoticeable? What can be done when such attacks have compromised the very roots of our business through a series of intricate digital networks capable of capturing critically important data? That's where cybersecurity comes in.

Perhaps ten to fifteen years ago, the issue of cybersecurity, although it was considered important, was not necessarily as much of a crucial area in business administration.

Today, the reality is different. Whether it is a company, a law firm or a retail business, cybersecurity has increasingly become an essential aspect, as business sustainability becomes increasingly dependent on digital systems, networks, and programs to be efficient and conduct business at the speed that is required today to be competitive.

Every day more data is captured including sales, customer billing, and in the case of law firms or banks; sensitive and confidential data requiring careful management and administration; which makes digital attacks a real threat to data protection and business continuity.

For example, law firms capture sensitive data required to conduct due diligence and that requires special care, including passports, bank reference letters, and the roles that different people have in companies and foundations.

This is why cybersecurity goes way beyond what you used to worry about.

In the past, attacks were primarily focused on denial of service (DoS) attacks, which saturated or bombarded servers with unsurmountable amounts of requests, causing them to collapse its services and interrupting the ability to do business.

Today the concern is more than anything about retaining and protecting data privately and securely.

According to an article on cybersecurity in Forbes magazine, 2020 broke all records with regards to the loss

of data due to data breaches as well as a huge number of cyber attacks on companies, governments and individuals.

In addition, it highlights the increase in threat sophistication due to the application of emerging technologies such as machine learning, artificial intelligence and 5G technology.

> TODAY THE MOST RELEVANT CONCERN IS ABOUT RETAINING AND PROTECTING DATA PRIVATELY AND SECURELY

Data protection in Panama

Given the importance of this issue, on May 28th, 2021, Panama regulated Law 81 on the Protection of Personal Data, which establishes the principles, rights, obligations and procedures to regulate the protection of personal data in Panama, which became effective on March 29th, 2021, two years after its sanction and promulgation in the Official Gazette.

With these regulations, companies that store personal or private data on companies or clients are required to go one step further. This means that you should not only worry about the data protection for your own company or the interruption of your services, but you should also worry about protecting your customers' data.

To achieve this, proactive and constant management is necessary, a trend that has changed over time.

In the past, the standard practice was for you to hire an external auditing company to review your systems annually or to carry out penetration tests to see if your security measures could withstand an attack.

However, that test returned results that indicated vulnerabilities to you at that specific point in time, something that today is not enough.

Today these tests have to be done constantly, as technology risks and threats change at unprecedented rates.

Hackers themselves develop new tools that learn from themselves to attack more intelligently; therefore, your defense tools must also use machine learning so that they learn at the same rate or faster about how to stop the attacks; so that your chances of defending yourself against those threats improve.

Protection tools and systems

It is healthy for a company to maintain annual evaluations of all its systems, but it is even more important to adopt a real-time internal security management that allows it to maintain the security of its systems for the rest of the year.

There are systems called SIEM (System Information Event Monitoring) which issue alerts to any system configuration or possible threats due to attacks. These tools are managed in a SOC (Security Operation Center), by a company dedicated to monitoring alerts that arise in real time.

Additionally, it is recommended that companies have a vulnerability scanning and patching system that carries out a review at least weekly.

Using this method, as its name suggests, the computers on the company network are scanned, and if a patch is found to be missing - from Windows, for example - that has been identified as a vulnerability, it is deployed and installed immediately.

The human factor

One of the greatest vulnerabilities that exists is the human factor. Users with access to a network or a system within the company can open a door to potential threats, such as the use of unsecure passwords.

The trend until recently had been to ask employees to use strong passwords, and to change them regularly every three months. However, what in practice ends up happening - in the face of repeated password change demands - is that users apply the same passwords with slight variations.

This makes them much more vulnerable than having a single strong and secure password combined with the application of a second authentication factor, such as a token that changes every 30 seconds or validated text message to the registered cell phone that includes a temporary code to log in at that time.

That is why the use of strong passwords combined with a second authentication factor, known as two-factor authentication, is the most recommended.

Cybersecurity training

It should be noted that, even if a company has all these surveillance systems, if a user is not able to recognize a phishing email and clicks on it, they can unknowingly open a malicious form, input their username and password, and immediately face a threat.

This is where constant user training becomes crucial. Doing social engineering exercises is highly recommended, in which users ability to recognize malicious threats is tested by sending a controlled phishing email to see if they believe it and open a vulnerability.

IT Policy

Every company must have an internal IT policy that indicates what the systems can be used for, what the password and token policies are, what can and cannot be installed on computers, etc.

This policy focuses on users and the technology department will use it as a manual to apply the system configurations in accordance with that policy.

In addition to this, doing social engineering exercises with users biweekly or monthly is recommended, so that they receive constant training and remain alert of potentially malicious emails.

The reality is that phishing emails and security threats change all the time, which is why all companies must keep up to date, comply with national and international cybersecurity standards to offer the secure environment for data protection that external clients seek.

Visit: www.focusalcogal.com