Securing your remote work environment with domain name reputation lookups and more

Posted on April 14, 2020

The coronavirus infection is having a temporary but dramatic effect on the life of many people all around the world. Working from home has been gaining popularity anyway, especially in the IT sector. In spite of that, there are still many companies which insist on traditional offices and working hours. There can be a rationale behind that – for instance, confidential business is better done under more verified circumstances. However, many companies just insist on the conventional approach for lack of experience and trust.

The current situation is enforcing though: to keep their business running, enterprises must rely on remote work as much as possible. Needless to say, cybercriminals want to exploit this as well. And those who are not used to remote work otherwise can be ideal targets of various attacks. Here we give some advice on what an enterprise and an employee should take care of about remote work.

1. Separate private and corporate use of computers

At your home office it is a very bad idea to use the same machine with the same account for both your private purposes and your business. Some enterprises provide their remote workers with company-owned hardware that can be used for work only. But even if it is not the case, it is highly recommended for remote workers to have a virtual or physical machine dedicated to work, preferably with encrypted file systems, strong passwords, etc. Nobody wants to be accused of having company confidential data stolen from a lost laptop or pendrive, or collected by some malware installed along with a game the kids had installed on the computer.

2. Secure the channels for communication

When working remotely, a vast amount of communication is going on between the employee's computer and the company's IT infrastructure. If this communication is unencrypted, it can be sniffed anytime by a malicious third party. A good option is to use Virtual Private Networks, a solution for the very purpose. However, in many cases communication can be realized with encrypted web pages using https communication.

In any case, care should be taken when it comes to up-to-date versions of the chosen software solution, to minimize the risk of being hacked along some known security hole. An outdated piece of server software is a great opportunity for a cybercriminal. It is indeed striking that any publicly available server receives several attempts of attacks every minute. Hence, servers should run under proper supervision, and their log files have to be regularly analyzed for intrusion attempts. The log files contain IP addresses; a DNS lookup API helps to find the associated domain names, whereas the WHOIS API is capable of providing ownership information of the IP address. This helps a lot in identifying opponents.

It is also a good idea to restrict the access to the geographical locations where the employees reside. This can be implemented with the IP Geolocation API, which can tell the location of the machine that tries to connect to an IP address. This can be integrated into a firewall solution to implement the appropriate restriction.

As of web servers, they are secure if and only if the settings of their SSL encryption are rock solid. Running your own sites with the Domain Reputation API will result in a very detailed technical check of your site, which will draw your attention to all shortcomings in the settings, including those of the encryption. It will be detected if your certificates are about to expire, if you allow the communication through insecure versions of the protocol, etc. This can help a lot to achieve the desired level of security.

Also, do not forget that the good old e-mail is by default an unencrypted way of communicating.. It is possible to encrypt e-mails, but normally they just go through the network without any kind of encryption.

3. Beware of social engineering

Social engineering techniques are in the very basis of many cyberattacks, even though in many cases they could be avoided by at least a little bit more of awareness by the potential victims. It is known, for instance, that phishing has a significant share in cybercrime, and even very naive and amateur phishing campaigns can be very successful, unfortunately.

This is a general issue which is important to fight against anyway. In case of remote work, however, miscreants have even more opportunities for these kinds of attacks, and the consequences can be even more severe. For instance, especially in situations where personal communication is really limited, it is easier for a malicious actor to pretend that he is a colleague whom you hadn't met before.

So take some preventive steps before trusting any message. Prefer information coming from the company's dedicated secure channels, such as internal project management systems. Use these whenever possible to communicate with colleagues. Besides being encrypted (unlike e-mails, for instance), these also provide a trusted authentication and identification of the other party.

If you are still using e-mail, check the sender. It is better to look into the headers of the mail: the claimed "From:" address can be spoofed. If you find a domain name of the sending machine, or at least the IP address, you can take a quick look at the WHOIS data by using WhoisXML API's WHOIS service to make sure that it really comes from the claimed sender.

It is also a good idea to take a look at the involved addresses with an e-mail verification API. This will check the validity of the address, and the functionality of the server associated to the address. It will also reveal if it is a disposable address, or if it’s registered at a free provider. This information helps a lot in assessing the reliability of the e-mail in question.

Similarly, if you are invited to visit a web page in the e-mail body, always assess the related risks. Most importantly, read the message carefully, understand what it says and assess it in terms of common sense. Is it really plausible? If, for instance, it suggests that it comes from the company you work for, and specifically asks for credentials (saying e.g. that some password of yours has to be updated), double check the URL: is it in a domain used by or belonging to your organization? If unsure, WHOIS data will help you. The use of the Domain Reputation API can also yield important information: it will show if the domain you encounter is listed on a malware or phishing blacklist.

In many cases, maintaining IT security is not as complicated as is commonly believed. It is a matter of awareness, reason, discipline, and of course, that of appropriate tools. We hope that the above advice, and also the tools we provide will help people with carrying on their work on a remote basis - a crucial matter in these hard times.