ISSN 2661-2666(Online) International Scientific Journal "Monte" DOI : 10.33807/monte.1.201904242
ISSN 2661-264X (Print)

THE ROLE OF SOFTWARE SECURITY IN MANAGING TAXATION TASKS

Mefail Tahiri
Professor at State University of Tetova
Ejup Rustemi
Dr.Sc. at State University of Tetova

Abstract

Everyone strives to work in a safe environment. This is especially true when we are dealing with something that is of high importance. Working with taxes definitely falls in the group of issues that are extremely delicate and require a precise approach. This certainly asks for high levels of security, in order to avoid any possible intrusion that will lead to major problems. By using IT tools to manage taxation tasks, we are directly dealing with issues of software security that should be closely monitored and evaluated. In this paper, we will explain the concerns related to this field of IT developments, and the ways we can improve tax security, for a safer operational environment.

Introduction

Data Security is a science that studies data protection methods. So data security means keeping data from abuses and accessing these data is under control. In this way, data security helps us maintain privacy. This also helps in maintaining personal data. Nowadays, computer systems connected to the network are often unprotected by codes generated by virtually unknown sources. When we add to this the tax-related issues, the seriousness rises for some levels. We say this because taxation tasks are a network that involves all aspects of our society, be it our own expenses, the way we manage our business or our relation to the state related taxation. In other words, taxation tasks represent a complex web of interaction that requires secure methods in order to manage it effectively. The final decade has been extremely sensitive concerning data security, especially if we mention the vast expansion of mobile technologies, which although they facilitate our everyday dealings, yet, at the same time, they put us at the forefront of the cybersecurity war.

What is a secure software?

Someone would say that secure software is a stable application with very strict access methods in order to avoid data breaches. In a way this is true, but things get tricky when we acknowledge the fact that most of the time data management software are tools of interaction between two or more sides, all with the purpose of getting things done fast and accurately. Interaction means that a certain database needs to be accessed by different parties, some of which do not have the proper training to deal with security issues concerning the data stored there. In other words, if one

sector of a certain institution has a high level of security, some other institution that needs to access the data with weak security will put the data at risk. The solution? Using the same level of security on all levels that will access the data, and continuously emphasize its importance, especially towards the client side of the communication chain.

Cloud computing strives to settle a lot of these issues by putting everything on the cloud, on more secure servers that are constantly maintained and updated in order to avoid unwanted access. Companies such as Oracle, Microsoft, Google, etc, are continuously emphasizing their cloud technologies that are affecting all branches of making business, where taxation tasks are not an exception.

Do IT security measures provide the needed safety?

After a seemingly endless amount of time, lawbreakers proceed to attempt and now and again prevail in their endeavours to submit assessment form extortion and data fraud. Since individuals are winding up increasingly mindful of a significant number of these plans, offenders have needed to depend on consistently evolving techniques.

For instance, the IRS as of late cautioned around one of the fresher tricks, a phishing trick that objectives assess bookkeeping firms and duty planning specialists. It is explicitly intended to gather touchy assessment data that will enable crooks to plan and document false government forms.

Norton Security website provides these forms of staying protected:

- Always use a robust security suite like Norton Security in your computer to keep all viruses and malware away.
- Never click on suspicious links in emails, even emails from friends and family.
- Back up all your data in safe external locations like the cloud or a portable device.
- Whenever possible, avoid using public Wi-Fi to file taxes. If public Wi-Fi is your only option, make sure you are encrypting the data and using two-factor authentication. Better yet, use a Secure VPN product like Norton Secure VPN

Companies such as Norton, Kaspersky or similar, always try to provide the best security software possible, while at the same time trying to educate their clients on how to stay protected. This e particularly important when accessing our tax information from our home through various applications.According to the head of BDO International Cybersecurity, the following are the main concerns of tax directors in the era of cybersecurity:

Fig. 1 Cybersecurity Concerns (BDO United States, 2017)

On the other hand, the IRS mentions some steps in order to stay secure when tax security is put at risk. These measures may not be applicable to every country in the world, especially when we consider the fact that in many of those, software tax management is still in an early phase, or not applicable at all, still, they are a good way to make things easier. Those measures are:

- Lock doors to restrict access to paper or electronic files;
- Require passwords and access controls for all computer files;
- Encrypt electronic data;
- Ensure disaster recovery includes backup of sensitive data;
- Schedule comprehensive destruction of electronic and paper data; and
- Encrypt emails when the content includes sensitive data. (Norton Security Website, 2018)

They go on and provide some other steps:

A lot of state-driven tax management software, deal with issues like this automatically with the support from IT companies that develop the software, by spending a considerable amount of their operating budget in that direction. The same thing applies to large companies when they manage their tax tasks. The issue becomes more vulnerable when things are on a personal level, when a given client access his or her tax data from their desktops or laptops, or nowadays from their smartphones. We are continuously hearing news about terrible passwords such as 123456 or "password", which put those who use them at huge risk. Tax tasks need to be taken seriously because they concern financial data, which are the main target of cybercriminals.

Developments in our region

Our region is a bit behind in applying IT solutions in tax administration, this makes talking about security even more out of place. But it should not be so. The fact that our countries are behind in IT developments, makes us more vulnerable, knowing that even if digital data systems are implemented we need extensive training for those workers who will need to manage tax databases. Some governments have put on their strategic planning these implementations. As an example we can mention the Albanian Task Administration Strategic Plan 2017-2022, where we can read things like:

- Improving quality in tax administration IT systems. Setting upa system to evaluate the accuracy of the data administered by the Tax Administration.
- Make the Transfer to Electronic Document Management in accordance with legal provisions.
- Development of a Central Tax Administration computer infrastructure andinformation system, in order to ensure access, reliability and data and information security.

If so risky, why use it?

It may not appear it so, but putting your taxes online is a standout ability and certainly one of the most difficult cybersecurity tasks that need to be managed.

Tax documents are loaded up with actual recognizable data and budgetary information – because that's what they must be. A bunch of profiteering cybercriminals know about this and are doing all that they can to acquire that information.

With this data, a programmer could imitate any of those people, opening records and taking out credits in their name, and atone point vanish with the money before any measures can be taken.

To ensure the security of our information against this kind of assault, we need to applyproper methods for affirming demands for tax records and distinguish those that can be a target in your organization by knowing who requests a particular tax record, and who provides the requested record.

To avoid these security issues, a lot of accountants do not send tax forms by email, but they prefer to obtain the data by actually calling the concerned party by phone.

As we mentioned before tax task administration requires the involvement of many parties, which in return makes way for an increasing number of errors. A survey by Raytheon-Websense, based in corporate environments in Germany and USA suggests that 70% of data security risks are as a result employee negligence. The following are some of the findings from the survey:

- Unintentional employee negligence severely diminishes the productivity of the IT function according to 73 per cent of U.S. respondents and 67 per cent of German respondents.
- Long hours and multitasking are red flags for risk. Multitaskers are more likely to be careless or negligent according to 79 per cent of U.S. respondents and 81 per cent of German respondents.
- German respondents are more likely to limit practices that can create unintentional risk (55 per cent), while their American counterparts prefer to monitor employees' behaviour (63 per cent).
- In both the U.S. and Germany, IT security practitioners spend an average of almost three hours each day dealing with the security risks caused by employee mistakes or negligence.
- Both German and U.S. respondents report ordinary users, contractors or third-parties pose the biggest threat to security. (Raython-Websense, 2015)

So, how to avoid these problems? Well, by leaving everything to the professionals who are constantly working in the direction of finding new ways to protect our tax data. They provide various schemes on how their software can protect us. According to the Swiss PWC, this is the cycle to protect our data:

Fig. 2Protection Scheme (PWC, 2018)

ISSN 2661-2666(Online) International Scientific Journal "Monte" DOI : 10.33807/monte.1.201904242
ISSN 2661-264X (Print)

Whereas the Federal Bank of Clevland provides us on this scheme of how cybercriminals make a DDoS attack financial systems in general, and tax system in particular:

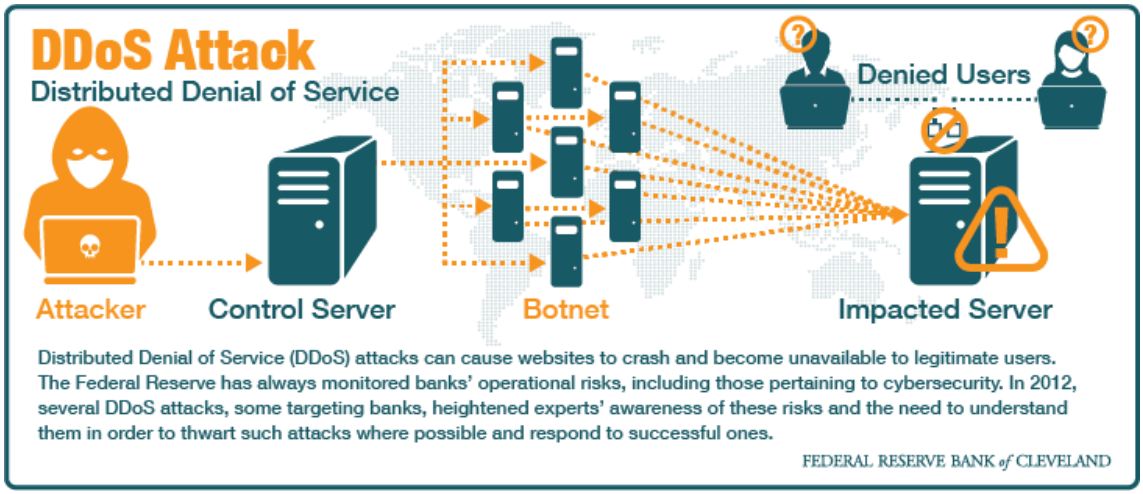

Fig. 3 Scheme of DDoS Attack (Federal Reserve Bank of Cleveland, 2018)

Conclusion

Managing taxation tasks is an extremely sensitive thing that needs to be dealt with high degree of caution. One misstep can lead to serious problems that will be hard to manage properly or fail to be managed at all. A company or institution that has its hands on taxation data, needs to direct a specific amount of financial expenses towards building a more secure information system, in order to keep tax data safe and cybercriminals at bay. It is true that those criminals are constantly changing their attack methods and it is in no way easy to construct a proper defence, but it is not undoable also. With proper skills and IT education, we can certainly find ways to make have a good night sleep.

References and Bibliography

1. AdministrataTatimore – PlaniStrategjik 2017- 2021, Drejtoria e Përgjithshme e Tatimeve
2. https://securityintelligence.com/irs-and-businesses-work-together-to-combat-tax-refund-fraud/
3. https://us.norton.com/internetsecurity-online-scams-is-your-tax-preparer-aware-of-cyber-security.html
4. https://www.bdo.com/insights/tax/federal-tax/2017-bdo-tax-outlook-survey-(1)/companies-look-inward-to-cybersecurity-liabilities

https://www.clevelandfed.org/en/newsroom-and-events/multimedia-storytelling/cybersecurity.aspx