Government Exposure due Freemium Tools

December, 2019

Alexandre Vasconcelos

SIKUR

Abstract

This document's purpose is to show how vulnerable government agencies are due to the usage of freemium tools. Technology is crucial these days, but the misuse of its tools and resources might be even more harmful than not having them.

It seems that governmental entities have no accurate planning to implement the appropriate tools for developing their job and use to go in the supposedly easiest way: freemium tools, widely available, and with no direct costs.

The Motivation

In the current digital economy, it is easy to find tools on the Internet to achieve something to do some task. Some are free, some partially free and others paid. The point is: when there is no planning in place, the shortest path is seductive.

It is easy creating a new e-mail account in the most popular sites, downloading and using that instant communication tool that everybody has, and many others to get the job done. It is fast, with no charge, and ready to use! Why should governments not use them? Let’s save money, let’s do it fast, let’s do the same than others, it is easier.

Separating personal from corporative is a perception that is not embedded in everyone’s mindset, but it should. That would start solving a lot of issues in the government and corporation's workspace, existing, and the ones to come.

Shadow IT in the Government

Shadow IT is a quite known concept in the technology management: it is the use of information technology software or hardware by a department or individual user without the knowledge of the IT security group or management in the organization. Cloud-based services made it easier, as device mobility became a part of the organizational scene.

CIO’s usually refuse to get the blame when it comes to shadow IT, but they can minimize, or even eliminate it. Government entities, due to its rotational nature, has difficulty to set policies up and Apps which tools should be in use for its workforce.

Fig.1 –Shadow IT commonly used Apps

The Risk

Another sensitive issue comes from government spying practices by using freemium Apps. As reported by Reuters (1), the Australian intelligence officials had determined that China was responsible for a cyber-attack on its national parliament.

People tend to think a cyber-attack as something ostensive and disrupting, where networks stop working, and connectivity falls down; although it is a possibility, it is not always like this. Malware injection by the usage of vulnerable freemium Apps happens silently, taking weeks or even months to be detected.

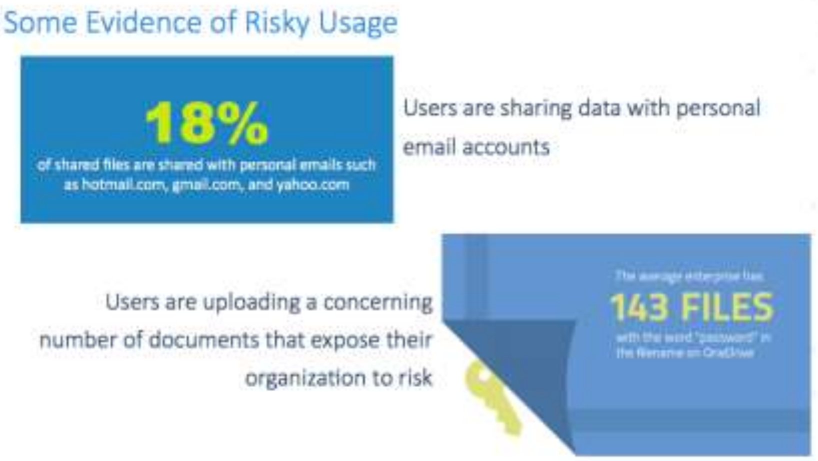

Fig.2 – Risk usage evidence

The above evidence is only about file transfer, but there are higher risks related to communication, where WhatsApp has a massive usage for information sharing on chat and voice/video calls.

At this point, when there is a large user base relying on this kind of Apps, a lot of security issues have been introduced and the whole organization might be compromised or under attack. Prohibiting freemium in the corporative devices is the radical measure to take, and it will disrupt the ongoing operations.

CSO's get wary about the usage of this kind of Apps, due to its insecurity and data leakage. There it is hard to comply with policies or regulations when using external tools to manage sensitive or even organizational information. Australia’s parliament suffered from this kind of behavior (1) and their local network got hacked. Network users had their data exposed and local assets were compromised. The usage of Gmail was banned in the organization network because it was configuring an attack vector.

The Opportunity

Government agencies need the right tools to accomplish their goals. When adopting freemium tools, there are good intentions, but the results will be disastrous. Using professional tools for corporative communication and collaboration reduces the information leakage risk and keep the operations running.

SIKUR Messenger offers the best in class product that fulfills governmental needs, for any hierarchical level, including third parties, making the communication even more secure. The SIKUR Private Cloud model (including the On-Premises), makes the product unique and highly adaptable to a wide range of needs.

References

1. https://mobile-reuters-com.cdn.ampproject.org/c/s/mobile.reuters.com/article/amp/idUSKBN1XO30R