Cybersecurity solution evaluation – *A brief discussion*

Cybersecurity has become a huge buzzword in recent years. As more companies move into digitisation, they see a prominent need for safeguarding their IT infrastructures. This has led to a boom in the number of security solutions in the market. Such solutions play their part in the protection of a company's digital assets. However, it is important to carefully examine the claims of solution providers, and even more so, evaluate if a cybersecurity product is the best match for the needs of a company.

In this article, we will highlight some considerations companies should take note of when acquiring a cybersecurity solution for their company. These factors may be overlooked when users decide to acquire a solution. Our considerations might not be exhaustive but could provide a few additional pointers to ensure a more comprehensive evaluation exercise.

Confidentiality, integrity and availability

Many might have heard of the CIA (Confidentiality, Integrity and Availability) triad, a model designed to guide policies for information security within an organisation. They can be used as a guide to identify most of the cybersecurity needs of a company. For example, in terms of a company's data, it would expect its data to be confidential (viewed only by authorised parties). The data should also be untampered with (maintaining the integrity of its original intention). Lastly, the data should be readily available to authorised parties, while being unavailable to those who are not.

Before purchasing any solutions, companies should identify their key assets and clarify their protection needs using the CIA as a guide. For example, they may begin by categorising their data and segregating the classified data from non-classified data. Following that, they can identify the specific security requirements on the classified data and define their required IT policies. The requirements of the purchased solution arise from such exercises.

Availability of the solutions and its information to adversary

When purchasing a solution, an often-overlooked consideration is the availability of information about the solution. When information about the solution is readily available, a hacker may be able to easily locate its vulnerabilities. For instance, information about the defense mechanism used in the enlisted solution could be readily available online if the solution is purely open-source based. Such solutions utilise source codes that are freely available on the internet. A company may face more risks when information regarding its enlisted cybersecurity solution can be easily found, as this creates opportunities for an adversary to formulate strategies to bypass the solutions.

Similarly, some solutions allow users full access rights to their source code and configurations. While it can be good for users to view the solution's source code or even customise the solution, the solution with this feature should be carefully examined, as a determined adversary may again be able to gain information about the solution through a separate purchase.

Furthermore, a company should avoid leaking information related to the solution it has enlisted and its IT infrastructure. These safeguarding measures should cover other processes or items. For

example, procurement documents containing the proposal from the solution providers, emails related to its network configurations and any documents detailing information about its IT infrastructure, are of interest to a determined adversary and should not be easily accessible.

Assumptions on the operating environment

Companies purchasing security solutions should also consider the operating environment of the solution. A solution could be created to address the concerns of a specific operating environment, and may not work for the operating environment in-lined with the company's needs.

For instance, a network intrusion detection solution could be formulated based on some assumptions of how a firewall should work in a given operating environment. If the solution was created with the assumption that a firewall can perform all the filtering and blocking functions, companies will need to evaluate whether the firewall they have fulfils such requirements.

It is important to highlight that the assumptions on the operating environments cover the assumptions on the processes and operators as well. In particular, the need for human intervention could also cause issues with the enlisted solution.

Ease of bypassing the solution

There are many ways of bypassing an enlisted solution, some of which can only be done by professionals. Nevertheless, it is important to do a few simple checks on the solution as a first cut assessment, to verify if the solution can be easily bypassed.

For instance, companies should check which layer the security solution is implemented on. If the solution is running on the kernel level, a hardware vulnerability may enable the adversary to bypass the solution. If the solution is running on the application layer, then a vulnerability in the OS or kernel may cause it to be bypassed. Similarly, a network protection solution that is not located at a "choke-point" of the network may be easily bypassed by the adversary as well.

Hence, companies should be prudent about the ease of bypassing their enlisted solution and seek advice from IT professionals regarding the feasibility of bypassing the solution. This helps them to understand the strength of the solution.

A small case study

To illustrate the considerations above, it is useful to share some of the experiences of the writers from the National Cybersecurity R&D Lab (NCL). The writers are currently involved in a project to develop a platform to assist users in evaluating cybersecurity solutions. By understanding how commercial solutions work, the writers were able to mimic the normal behavior of a user, performing malicious acts without being detected when the overall user behavior in the IT network met certain profiles. This illustrates the importance of safe-guarding information of the solution, understanding its assumptions on the environment and considering if the underlying approach has weaknesses.

Conclusion

No one is exempted from being attacked in the cyberspace and the consequences of the attack can be tremendous. Most companies may already be aware of the importance of cybersecurity and may already have a few measures in place to safeguard their digitised assets. The challenge companies will face, is to continuously be aware of the most recent threats and learn how to protect themselves. Furthermore, while there is no fool-proof cybersecurity product, companies should carefully evaluate the solutions they have acquired, ensuring that they are the best match for their security needs. E

National Cybersecurity Research and Development Lab (NCL)

The National Cybersecurity Research & Development Lab (NCL) is a national lab funded by the National Research Foundation to support the industries, agencies and academia in cybersecurity. Since its launch in 2015, NCL has supported over 80 projects in various areas in cybersecurity. The projects include, amongst others, training of professionals/students, security testing/evaluation, research validation/translation by universities and companies. The support for SME & start-ups are currently fully subsidised.

This article is contributed by Ms Alice Guo and Mr Anand Agrawal from the National Cybersecurity Research and Development Lab (NCL).