BIZCOMMUNITY

Five common security threats that demand attention

By Carey van Maanderen

9 Mar 2016

From a corporate standpoint, security is a process that requires management and support for key areas of the organisation. The challenge is never-ending, and security teams have to cover different fronts through which malicious code can infiltrate a network, counting on the use of proactive detection technology, management and education as part of their defence plan.

©Dmitriy Shironosov via 123RF

If you have taken into account that the organisations have finite resources and that IT staff are responsible for information security (among other things), it is important to develop a clear and concise incident response plan. At the same time, it would help to identify the most common points of infection as a way of preparing for any situation.

Below we will take a look at some of the most common threats facing companies, their impact, and some significant recent cases.

1. Emails that carry threats

Email has an almost central role in companies today, forming a core part of communication with customers, providers, services, etc. It also enables workers to share information within the company. Corporate email accounts are usually one of the main channels for receiving malicious code and we have already examined cases of the spread of various types of threats that use this form of communication. On top of this, malware received through attached files create huge problems.

To protect corporate email accounts, we need not only an endpoint security solution that detects malicious attachments, but we also need to protect the email server, and filter these elements before they arrive in people's inboxes. One recommendation for security teams is to use management tools to generate reports on which threats employees are receiving over email, thereby adjusting their response to incidents if any issue arises.

2. External devices that can make files disappear

The spread of USB memory sticks and other types of external devices is also a very common vector in the spread of malicious code. The main method of this type of infection is the abuse of direct access links (LNK), where by connecting the USB device to an infected machine, all files and directories disappear and are replaced by direct access links. If the same USB device is inserted into a new machine, when the user double-clicks on these links, they infect the system (and the folders open so the victim does not realise).

It is important that organisations set out usage policies for external digital storage devices, primarily because this can also pave the way for information theft. Depending on the business or the decisions taken by the organisation, using a solution that enables the selective blocking of their use is highly recommended.

3. Exploits

The exploitation of software vulnerabilities is another way that malicious code is spread, mainly through office applications, browsers, and websites. The challenge regarding the flaws in applications or browsers is that if users fail to update a vulernable application, or where no patch yet exists, companies can remain exposed to threats.

Exploits do not only affect the endpoint. Web servers and other devices directly connected to the inernet can be subject to these kinds of flaws. To combat this type of threat, we need proactive security solutions with functionalities such as ESET Exploit Blocker. These help to prevent the execution of exploits, and protect users from such famous examples of these threats as 0-day exploits. As for other devices such as web servers, databases, and various devices on which security solutions are not often installed, regularly running pentesting services helps prevent all kinds of incidents.

4. Ransomware

Ransomware is one of the most frustrating threats to face large, medium and small companies across the globe. An infection with this type of malicious code can leave a lot of an organisation’s vulnerable points exposed. Whether companies perform the configuration of antivirus solutions or undergo frequent security reviews, an attack of this kind means the very continuation of the company’s business is under threat, depending on what information is hijacked.

Any company seeking to implement a proactive security policy will try to avoid any kind of infection, but when such things occur, damage recovery tools are of vital importance. Before any ransomware infection occurs in a company, the time needed to obtain a backup of the information and get the business up and running again is key for minimising the impact.

5. Unprotected mobile devices

Another factor of renewed concern to companies is their mobile devices. Protecting mobile devices not only protects against infection by malicious code but also helps to continue to protect the internal network when these devices are connected to it. In relation to this point, mobile devices can be managed from a single management console for the endpoints.

It is possible for companies to have effective policies for mobile devices and, therefore, have clear rules governing the use of smartphones and other devices.

What can we do? The challenge for company security teams is to protect the organisation, ensuring that no equipment in their network is infected and, in the event that any infection does arise, that they can respond as quickly as possible to minimise the impact on business. It is a difficult challenge, but not impossible if we take the decision to confront it proactively.

To do this, a good starting point would be to know which threats to an organisation will do them the most harm. This may take some time to achieve, but understanding what detections are made by the security solutions on a day-to-day basis will help booster a support plan to run alongside a company's security policies. Taken together, all this will help to keep businesses – and above all their information – safe.

ABOUT CAREY VAN VLAANDEREN

Carey van Vlaanderen is CEO of ESET Southern Africa. ESET is a global provider of security software for enterprises and consumers and is dedicated to delivering instant, comprehensive protection against evolving computer security threats.

- 4 ways to manage the human threat to cybersecurity - 18 Jul 2023
- A cybercriminal's tricks and trades to get into your phone - 23 Mar 2018
- What is encryption, how does it work and why is it important? - 6 Mar 2017
- Five common security threats that demand attention - 9 Mar 2016
- Face 2016 with a proactive attitude of security awareness - 22 Jan 2016

View my profile and articles...