DMZ Evolutions

How we try to keep up with the digital threat environment

Kapt Jef MOONEN – MRC&I-CIS/C/P/DMZ
Jef.Moonen@mil.be

I. INTRODUCTION

To connect our networks to the internet, we use several devices to secure this interconnection. As cyber criminals and hackers permanently evolve and adapt their methods to bypass known security devices and techniques, so does – fortunately - the industry. As we – BEL Defence – need to protect our networks from these evolving threats, we regularly have to update our equipment, or even buy some new devices, in order to stay as secure as possible. In this year, we will implement some new or adapted devices, which will also have an impact on the user experience. The two things I want to talk about are our new Sandbox solution, and the new way to connect via VPN.

II. SANDBOX

A Sandbox is a Virtual Machine, in which we will run all incoming and downloaded attachments. Common files, like Office or Pdf, can contain active content, that can be necessary – such as macros, but it can also contain malicious active content. In the Sandbox, we will examine the behavior of these files. We will specifically look for actions that address the Registry, create network connections, run unwanted processes. In addition, we will check if any of the code abuses exploits, that try to bypass OS and CPU security controls. If the system finds malicious code, the file will be quarantined and deleted.

As this scanning takes some time, we have the possibility to immediately deliver a cleaned copy of the file, which is stripped from all active content. In this way, we can avoid unacceptable delays, without giving in to security.

III. VPN NEW STYLE

Before we can allow anyone on our network, we want to be as sure as possible that whoever connects is someone we know and allow, and that he does it with a machine that we can trust.

In a first step, we will check if the device is compliant. Depending on the resources one wishes to address, this as to be an SBO machine, or at least a machine with an OS that is supported and patched, it has to run an antivirus software, and in some cases, we only allow specific IP addresses. Next we will verify the identity of the user, preferably by "Strong Authentication". We prefer the options that FAS[1] provides, like the use of eID. In exceptional cases (foreign contractors, …) we can enforce the use of a "One-Time-Password". Once one has successfully logged on, we have to make sure he can only perform actions he is authorized to. Therefore we integrate with Active Directory. After a session, we will make sure all temporary data is deleted, like the Recycle Bin, Form and Password Autocomplete, Session termination, …

IV. CONCLUSION

Security is something that permanently has to evolve. Hackers will always try to get ahead of security; which means that devices and technologies permanently have to be updated.

[1] FAS: Federal Authentication Service