Network Access Control

Principles and implementation for the Corporate Defence Network

Maj LIPPENS Peter, Ing – MRC&I-CIS/C/P/D
peter.lippens@mil.be

I. INTRODUCTION

Since many years the access policy for the Corporate Defence Network (CDN) is published and very clear: it is not allowed to connect devices to the network, unless the device respects the minimal software configuration requirements and the request has been formally approved. The practice seen by CC V&C is however very different: DHCP and network scanning logs frequently show rogue devices like personal laptops and unknown technical systems. Some of them have unsupported OS versions, are misconfigured or are accessing the network for nefarious reasons and represent a clear risk for the confidentiality, integrity and availability of our corporate data.
Network authentication mitigates these risks by authenticating devices and/or users as they access the network. The Network Access Control (NAC) implementation for CDN uses device authentication based on 802.1X: this approach allows us to restrict guests to a guest network and to enforce our access policy for wired and wireless networks.

II. GREAT PLAN, BUT HOW DO YOU IMPLEMENT IT

This project, originally started in 2010 as a case study, was approved in 2011 and started in 2012 with a proof of concept: is the conceptual idea feasible for implementation on our corporate network? Luckily the moment was right: the new workgroup switches needed for the project VoIP (Voice-over-IP) supported 802.1X, VLAN switching and MAC authentication (for devices that do not support 802.1X), and at the same time all our corporate PC end printers were replaced by standardized leasing hardware. Although the first testcase was not a striking success, thanks to the thorough research of the CC V&C and the maintained commitment of the higher management the entire process is finalized mid-2014 and the first sites are migrated. Actually more than 20 sites are already migrated, and all territorial sites will be migrated NLT end 2016.

III. DOES IT ENDS WITH GUEST NETWORKING?

No: guest networking alone does not guarantee that the managed device is correctly patched or that the antivirus software is running and up-to-date. Although the recently deployed SCCM 2012 R2 and other existing controls check those parameters, this is not sufficient for mobile devices that frequently connect directly to the Internet or to other foreign networks: those should be checked and patched before they reconnect to CDN. The technology is also not reserved for CDN only: it will allow in the future to provide connections to other networks on the same workgroup switch by using the same physical infrastructure of the campus.

IV. CONCLUSION

NAC is a useful technical control that leverages the existing infrastructure and adds an effective security layer for the information assets on the internal network.