Increasing Windows security by hardening PC configurations

Pablo Martín Zamora, Michal Kwiatek, Vincent Nicolas Bippus, Eneko Cruz Elejalde
IT-CDA Applications and Devices

Did you know that over 8000 Windows PCs are used at CERN everyday?

They perform critical tasks ranging from controlling the accelerator facilities to processing invoices and payments. The configuration of CERN’s PCs is based on centrally managed machines and a lot of autonomy is given to end-users. This poses a risk for administrative departments dealing with lots of e-mail attachments that can be potentially dangerous.

Beginning of the hardened PCs

The project began in November 2016 in collaboration with CERN Computer Security Team. The goal has been to develop and deploy a specific hardened PC configuration to provide stronger resilience against external attacks.

Over the past year and with the help of local supporters, CERN has deployed the hardened PC configuration to over 300 computers in administrative departments and public areas around the organization.

Features

CERN hardened PC configuration is based on Windows 10 which is more secure than Windows 7. Additional security policies and anti-exploit techniques are built into the operating system.

The main user of a hardened PC is never a member of the Built-in Local Administrators group. This ensures that applications are never run with elevated privileges.

Adobe Flash is disabled on all supported browsers.

AppLocker rules allow execution of programs from certain paths of the system and deny execution of potentially dangerous files from the user profile, temporary folders and removable storage devices.

PowerShell scripting activity is logged and audited.

Disk encryption is enforced using Microsoft’s BitLocker, which allows users travelling with laptops to safeguard their data and in addition protects PCs against attackers who might gain physical access to the PCs.

An alternative PDF reader was introduced as a replacement of the existing PDF suite, to avoid running potentially dangerous files from the user profile, temporary folders and removable storage devices.

LAPs, a Local Password Management Solution, was deployed to all CERN machines to ensure that passwords for the Built-in Local Administrator account are frequently changed and randomized.

An administrative bastion host was deployed to handle connections from supporters, to protect powerful credentials against pass-the-hash attacks.

Bloodhound uses graph theory to reveal the hidden relationships within an Active Directory environment.

Next steps

Deploy GRR Rapid Response: a forensics agent to analyse machines showing signs of suspicious activity and enable quick incident response.

Implement PowerShell Constrained Language, designed to support day-to-day administrative tasks, yet restrict access to sensitive language elements that can be used to invoke arbitrary Windows APIs.

Investigate Windows Defender Application Guard for Microsoft Edge. This will open untrusted sites in an isolated Hyper-V-enabled container, which is separate from the host operating system.

Propose Chrome as the default web browser.

Use CredSSP with Kerberos rather than NTLM.

Did you know that over 8000 Windows PCs are used at CERN everyday?

They perform critical tasks ranging from controlling the accelerator facilities to processing invoices and payments. The configuration of CERN’s PCs is based on centrally managed machines and a lot of autonomy is given to end-users. This poses a risk for administrative departments dealing with lots of e-mail attachments that can be potentially dangerous.

Beginning of the hardened PCs

The project began in November 2016 in collaboration with CERN Computer Security Team. The goal has been to develop and deploy a specific hardened PC configuration to provide stronger resilience against external attacks.

Over the past year and with the help of local supporters, CERN has deployed the hardened PC configuration to over 300 computers in administrative departments and public areas around the organization.

Features

CERN hardened PC configuration is based on Windows 10 which is more secure than Windows 7. Additional security policies and anti-exploit techniques are built into the operating system.

The main user of a hardened PC is never a member of the Built-in Local Administrators group. This ensures that applications are never run with elevated privileges.

Adobe Flash is disabled on all supported browsers.

AppLocker rules allow execution of programs from certain paths of the system and deny execution of potentially dangerous files from the user profile, temporary folders and removable storage devices.

Local firewall is configured to lock down PowerShell connections to non-CERN IPs.

PowerShell scripting activity is logged and audited.

Disk encryption is enforced using Microsoft’s BitLocker, which allows users travelling with laptops to safeguard their data and in addition protects PCs against attackers who might gain physical access to the PCs.

An alternative PDF reader was introduced as a replacement of the existing PDF suite, to avoid running potentially dangerous files from the user profile, temporary folders and removable storage devices.

LAPs, a Local Password Management Solution, was deployed to all CERN machines to ensure that passwords for the Built-in Local Administrator account are frequently changed and randomized.

An administrative bastion host was deployed to handle connections from supporters, to protect powerful credentials against pass-the-hash attacks.

Bloodhound uses graph theory to reveal the hidden relationships within an Active Directory environment.

Next steps

Deploy GRR Rapid Response: a forensics agent to analyse machines showing signs of suspicious activity and enable quick incident response.

Implement PowerShell Constrained Language, designed to support day-to-day administrative tasks, yet restrict access to sensitive language elements that can be used to invoke arbitrary Windows APIs.

Investigate Windows Defender Application Guard for Microsoft Edge. This will open untrusted sites in an isolated Hyper-V-enabled container, which is separate from the host operating system.

Propose Chrome as the default web browser.

Use CredSSP with Kerberos rather than NTLM.