Avecto Privilege Guard

Al Williams

July 13, 2010

Agenda

- What is least privilege?
- What issues does it address?
- How should you use it?
- Demo

What is Least Privilege

"The least privilege principle requires that each subject in a system be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error or unauthorized use"

US Department of Defense Trusted Computer System Evaluation Criteria (Orange Book)

Issues With Admin

- High risk of computer compromise
- High cost of fixing compromised machines
- Potential loss of data
- Potential exposure of sensitive data

Admin Allows

- Install spyware and adware
- Install kernel-mode root kits
- Install system-level level key loggers
- Install ActiveX controls
- Install and start services
- Stop existing services (such as the firewall)
- Access data belonging to other users
- Replace OS and other program files with Trojan horses
- Disable/uninstall anti-virus virus
- Create and modify user accounts
- Reset local passwords
- Render the machine unbootable

Issues With Standard User

- End user satisfaction
  - I can’t do …
- Possible loss of productivity

Our Solution – Privilege Guard

- Software that the UL has purchased to manage desktop security
- Alleviates many issues of running as Standard User
- Significantly reduces risk of machine compromise
- Reduces cost of managing desktop systems

Information from Avecto

Privilege Guard for Windows Vista & 7

Moderately Managed

- User Driven via UAC
- Administrator Account Required
- Full Admin Privileges
- Fixed End User Messages
- No Auditing

Locked and Well Managed

- Policy Driven via Group Policy
- Standard User Account
- Granular Privilege Control
- Configurable End User Messages
- Privilege Monitoring and Auditing

What Privilege Guard Does

- Allow specified applications to run as Admin
  - TSM for example
- Allow certain users (most of you) to “elevate on demand”
  - Right click on the install package
  - Fill in the reason for installing (this is recorded)
  - Install as Admin
- Block install of some software
- Prevent some users from ever elevating to Admin

What You Might Want To Do

- Install applications on your computer – for example – iTunes
  - Download the iTunes install package (do not run dynamically – that will not elevate)
  - Right click on the install icon
  - Record your reason (e.g. Installing iTunes)
  - Complete installation

What You Should Not Do

- Install maintenance on pre-installed software
  - We will do that with Big Fix
  - We will make sure it works before we put it on you computer
- Install new versions of pre-installed software
- When the Adobe or Microsoft request to update happens – just say no
- Install anything questionable
  - If you are not sure, ask us (help desk)

Instructions for Software Install

- These are on Wikispaces in DLTpublic
  - https://wikispaces.psu.edu/display/dltpub/Installing+Software+with+Avecto+Privilege+Guard

Questions from the presentation

- What happens if I try to install from DVD?
  - Autorun is disabled so it will not automatically install
  - Right click on the setup.exe file on the DVD to install the software to install using Privilege Guard
- Can I install Firefox plug-ins?
  - Yes, that works in Standard User mode
- Is Firefox installed with automatic update enabled.
  - It was, but we are turning it off