

Re: Controls for client machines

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2004-05/0949.html>

From: Jay Ferron (*Support_at_interactiveSecuritytraining.com*)

Date: 05/11/04

Date: Tue, 11 May 2004 13:48:03 -0400

If you have physical access you can do harm to a computer – removing floppy – cd drive or at least not able to boot from is a good first step then lock the bios– but remember I can open case and take drive

Use of encryption of hard dive is a good idea IF you understand all of the issues. and there are lots of issue.

you can in the registry set computer not to cache credentials but this can cause issues.

Hope this helps

--

Jay Ferron ADSI, CISM, CISSP, MCP, MCDBA, MCSE, MCT, NSA - IAM, TCI "paulroper" <anonymous@discussions.microsoft.com> wrote in message news:F0890BA4-C244-40EA-A4AF-86958E8517AD@microsoft.com...
> Hi there, I am a relatively inexperienced IT Auditor for the health service
> in England. Each of our hospitals has its own network and these vary from
> NT, 2000 to 2003. Our server rooms have a high level of physical protection
> however our client machines could easily be accessed by a member of the
> public. I cannot do anything about this - its the nature of the
> organisation.
>
> I am trying to assess the risks that this causes to local data files and network security in general.
>
> I have been reading material and this suggests the following:
>
> For NT workstations it would be possible to use a NTFSDOS boot disk to
> extract the SAM file from the workstation. LC4 could then be used to crack
> to the local administrator account password. For these workstations I intend
> to recommend that all confidential files are stored on file servers and that
> the service pack with SYSKEY is applied.
>
> For 2000 Professional/XP Pro workstations a boot disk is available that
> allows the password of any local account to be set. As all users logon to
> the domain, only administrator and guest account should be stored in the
> workstation's SAM. For these workstations I intend to recommend that the

microsoft.public.security: Re: Controls for client machines

> BIOS is amended so that the machine boots only from the HDD. The BIOS
> should then be password protected. I will also recommend users take
> advantage of EFS.
>
> I would appreciate any comments/critisms on my intended recommendations.
> Are there ways to circumvent my suggestions (I know it may be possible to
> reset BIOS passwords).
> Also, after auditing laptops I realised that users could logon using the
> domain account while disconnected from the network. I assume there must
be
> a hash of the user's domain password stored on the laptop. I cannot locate
> these doamin accounts in the SAM. Are there any tools which can recover
the
> hashed domain account passwords from client machines?
>
>