

RE: Home laptops on a corporate network

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2007-05/msg00216.html>

- *From:* "Adam Rosen" <ajrosen@xxxxxxxxxxxx>
 - *Date:* Wed, 9 May 2007 14:32:39 -0400
-

I think a properly secured (i.e. no access to local drives) Terminal Server is the way to go with this if they are wanting this ability.

Adam

-----Original Message-----

From: [listbounce@xxxxxxxxxxxxxxxx](mailto:xxxxxxxxxxxxxxxx) [<mailto:xxxxxxxxxxxxxxxx>]
On Behalf Of Christopher Kelley
Sent: Wednesday, May 09, 2007 8:58 AM
To: gjgowey@xxxxxxxxxxxxxxxx; pbruland@xxxxxxxx;
[listbounce@xxxxxxxxxxxxxxxx](mailto:xxxxxxxxxxxxxxxx); [security-basics@xxxxxxxxxxxxxxxx](mailto:xxxxxxxxxxxxxxxx)
Subject: Re: Home laptops on a corporate network

Keep in mind the original question.... We are talking about PERSONAL laptops here. Doing all of these things to non-company assets is unfeasable. Not to mention, you would be liable if a patch rendered the system (or any part of it) unuseable, or if the employee was no longer able to install things to the system, or whatever. This could be reduced by an aggressive AUP/EULA, but in the end the risk is most definately NOT worth the reward.

You need to think about all the things that this laptop would encounter, and how you would safeguard the EPHI that is on the system. It is just not possible with a non-company asset.

Heck, it is hard enough with a _company_ owned asset.

Trust me on this, your client and your client's IT people will be very thankful in the long run if you squash this right now.

From: gjgowey@xxxxxxxxxxxxxxxx
Reply-To: gjgowey@xxxxxxxxxxxxxxxx
To: "Petter Bruland" <pbruland@xxxxxxxx>, [listbounce@xxxxxxxxxxxxxxxx](mailto:xxxxxxxxxxxxxxxx),

[christopherkelley@xxxxxxxxxxxx](mailto:xxxxxxxxxxxxxxxx), [security-basics@xxxxxxxxxxxxxxxx](mailto:xxxxxxxxxxxxxxxx)
Subject: Re: Home laptops on a corporate network
Date: Tue, 8 May 2007 23:42:17 +0000

RE: Home laptops on a corporate network

MIME-Version: 1.0

Received: from smtp05.bis.na.blackberry.com ([216.9.248.52]) by bay0-mc5-f2.bay0.hotmail.com with Microsoft SMTPSVC(6.0.3790.2668); Tue, 8

May 2007 16:42:24 -0700

X-Message-Info:

oG9qAjD2BNG0yVIB517PPNHctMVimjpzoMreuYyIO2oP8zkmi6D3iEQ4Sb8YSCTqzgGU4VnnNk4=

References: <20070508171132.25067.qmail@xxxxxxxxxxxxxxxxxxxx>

<2EE61832B235C64F81A04C68DEE1C0990BDC4F@xxxxxxxxxxxxxxxxxxxx>

Sensitivity: Normal

Return-Path: gjgowey@xxxxxxxxxxxxxxxxxxxx

X-OriginalArrivalTime: 08 May 2007 23:42:24.0079 (UTC)

FILETIME=[872F3DF0:01C791CA]

One of the advantages of using SMS for patch management is you can force a patch scan and push as soon as they connect to the network (vpn, dial up, or regular). SMS is a pain to configure for patch management, but it's worth it.

Geoff

Sent from my BlackBerry wireless handheld.

-----Original Message-----

From: "Petter Bruland" <pbruland@xxxxxxxx>

Date: Tue, 8 May 2007 10:51:40

To: <christopherkelley@xxxxxxxx>, <security-basics@xxxxxxxxxxxxxxxx>

Subject: RE: Home laptops on a corporate network

Totally agree, not recommended.

Earlier we had some posts about patch management, and from what I gathered, you could get some control by using PatchLink. Although, that does not protect you 100%, you could place the VPN users on their own VLAN where you can restrict the amount of access to internal servers/services.

I've seen a different "solution" (not sure how much of a solution that is) where the firewall is a high end Sonicwall, like the 4060 etc, and the VPN clients were terminated to their own LAN segment. Then the Sonicwall would use it's Security Services (Content filter, gateway AV, Client AV enforcement, anti-spy ware, intrusion prevention) to filter traffic between the VPN users and the rest of the network.

Also I'm not too familiar with the restrictions of HIPAA and SOX, so the above might not event be "allowed" according to HIPAA/SOX.

I think this is a very common scenario, so any feedback (NOT FLAMING) is

RE: Home laptops on a corporate network

RE: Home laptops on a corporate network

appreciated.

–Petter

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxxxxxx [mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx]

On Behalf Of christopherkelley@xxxxxxxxxxxxx

Sent: Tuesday, May 08, 2007 10:12 AM

To: security-basics@xxxxxxxxxxxxxxxxxxxxx

Subject: Re: Home laptops on a corporate network

I'd recommend NOT doing this. Especially if you are trying comply with HIPAA. Keep in mind that you will have little to no management capability over these personal laptops, which means you have no ability to verify patch level and AV update on these machines that may have EPHI on them. Not to mention the fact that these employees are probably taking them home and plugging them into their home networks, where they (or their kids) are running bearshare, gnutella, grokster, bitorrent, and surfing to unfiltered web sites. Not only does this mean that they are potentially exposing critical data in this manner, it also means they are bringing potentially infested computers into the soft chewy center of your network.

Whenever you have an employee with a laptop, you create a liability to your network, allowing them to use personal laptops presents an even bigger liability. IMHO, this level of risk is unacceptable, especially from a HIPAA compliance standpoint.

Like the way Microsoft Office Outlook works? You'll love Windows Live Hotmail.

http://imagine-windowslive.com/hotmail/?locale=en-us&ocid=TXT_TAGHM_migration_HM_mini_outlook_0507