

RE: The VA Stolen Laptop – Lessons Learned

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2006-09/msg00171.html>

- *From:* "Isaac Van Name" <ivannname@xxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 15 Sep 2006 08:13:59 -0500
-

As always, I am glad to receive input on my opinions stated here as I use them to better myself and my pursuit of knowledge. That being said, I think there was a bit of a misunderstanding between my post and yours, and I would like to address that now.

If the laptop is stolen, and off the network when you disable the account, how the heck do you think the fact the account has been disabled reaches the laptop?

Let me put this in simpler terms... It makes a lot more sense when I simply say something like: "Sensitive data such as that should not be present on the laptop itself." Then, statements such as disabling the network account make a lot more sense when data is housed on the "work" network and NTFS file rights and encryption are applied. After all, what point is there to put sensitive data such as that natively on the laptop? Will that person need to work on the information in a location where he has no internet access to VPN into the "work" network?

"encrypt it as the roaming profile"? The roaming profile is very specific files. If you're talking about using EFS, you have other concerns as well.

Encrypt it with whatever you like... as I am no expert in encryption, I have no advice on what to use or not to use. And, the "encrypt it as the roaming profile" statement was made with relevance to my overall solution of having the data housed on the "work" network under a "work" user account.

If you encrypt a user's profile with EFS, the key would have to be on the machine or the user couldn't get to their profile off the network.

Not the profile, just the data. And, maybe I'm using the wrong lingo here... maybe "roaming profile" is not the phrase I'm looking for. Please feel free to correct me here... My intent is a profile local to the "work"

RE: The VA Stolen Laptop – Lessons Learned

network that the user can remote into the network with, so maybe I just need to say a "VPN account".

If the key is left on the machine, then anyone with physical access to the machine can reset the admin password, login as the admin, and grab the user's key and get to the files.

See above. The whole point of my "rant" was to eliminate the point of failure that is created by both the presence of sensitive data on the physical laptop as well as the ease of compromise associated with physical access to the laptop.

The encryption used should be something other than EFS, and should be on a directory outside the profile (so copies aren't flung onto the user's network share).

Okay, I can agree with that. :-) See, I'm not so stubborn as to dispute EVERYTHING.

Basically, the users should be trained, and the plan should be created by someone who knows what they are doing, and people should stop pointing fingers when something goes wrong, and instead address the issues.

Yes, this is the rule whenever a security policy is created in a corporate environment. I couldn't agree with you less. And, maybe I don't completely know what I'm doing or how I would fix the problem... however, this is a mailing list, and I am offering bits and pieces. After all, it is not my job to fix it... only to fling around ideas and get back input.

Good slam on the Prez, BTW, both pertinent and relevant, and about as thoughtfully consistent as the rest of your rant.

As I do not like discussing politics (and it would not be relevant in this mailing list), I will refrain from stating my reasons for disliking Bush. As for its pertinence and relevance, please refer to the poster before me, as he posed the question of how Bush defines "data". Last I checked, that isn't the President's job so, really, both your comment and my own are irrelevant and pointless...

As for the thoughtful consistency of my rant, thank you for your input. You obviously took the fact that I was suggesting a possible solution rather than solving the whole problem as inconsistency; if you had looked at my

RE: The VA Stolen Laptop – Lessons Learned

"rant" as something other than a "juicy retort just waiting to happen", then you would've realized that I was going in a general direction with it.

Now that we have all of the responding out of the way, can we continue the discussion in a manner that does not assume that the poster is a moron?

Thanks. :-)

Isaac Van Name
Network Assistant / Programmer
Southerland, inc.
ivanname@xxxxxxxxxxxxxxxxxxxxxx

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

From: Scott Ramsdell [<mailto:Scott.Ramsdell@xxxxxxxxxxx>]
Sent: Thursday, September 14, 2006 4:35 PM
To: Isaac Van Name; evb; security-basics@xxxxxxxxxxxxxxxxxxxx
Subject: RE: The VA Stolen Laptop – Lessons Learned

If the laptop is stolen, and off the network when you disable the account, how the heck do you think the fact the account has been disabled reaches the laptop?

"encrypt it as the roaming profile"? The roaming profile is very specific files. If you're talking about using EFS, you have other concerns as well.

If you encrypt a user's profile with EFS, the key would have to be on the machine or the user couldn't get to their profile off the network.

If the key is left on the machine, then anyone with physical access to the machine can reset the admin password, login as the admin, and grab the user's key and get to the files.

The encryption used should be something other than EFS, and should be on a directory outside the profile (so copies aren't flung onto the user's network share).

Basically, the users should be trained, and the plan should be created by someone who knows what they are doing, and people should stop pointing fingers when something goes wrong, and instead address the issues.

Good slam on the Prez, BTW, both pertinent and relevant, and about as thoughtfully consistent as the rest of your rant.

–Scott Ramsdell

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

From: listbounce@xxxxxxxxxxxxxxxxxxxx [<mailto:listbounce@xxxxxxxxxxxxxxxxxxxx>]
On Behalf Of Isaac Van Name

RE: The VA Stolen Laptop – Lessons Learned

RE: The VA Stolen Laptop – Lessons Learned

Sent: Thursday, September 14, 2006 8:18 AM
To: 'evb'; security-basics@xxxxxxxxxxxxxxxxxxxxx
Subject: RE: The VA Stolen Laptop – Lessons Learned

Bush hasn't defined "data"... he can't define anything because he's a moron.

Does data include OS files, log files, cab files, drivers, etc.?
IMO, no. None of it. Screw the OS and its files; those things don't count as "sensitive data". Okay, so there's the argument that "these things can be used for a compromise". Really, I don't see why someone can't just use a roaming profile and a VPN connection on the laptop to connect to their workplace and, anytime sensitive data like that is put on a laptop, encrypt it as the roaming profile and set the file rights to only allow that roaming profile to access it. That way, when the laptop is stolen, just disable the roaming account... that should protect the encrypted files for long enough for the laptop to be recovered. True, this is more work, but then, isn't proper security just making your everyday tasks take longer?

Of course, this is all said with a cup of coffee in one head and my hungover head in the other, so please feel free to correct me. As it seems to me, though, I think you have to plan out system security before you implement file security... otherwise, you're just playing smoke and mirrors.

Isaac Van Name
Network Assistant / Programmer
Southerland, inc.
ivanname@xxxxxxxxxxxxxxxxxxxxx

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

From: listbounce@xxxxxxxxxxxxxxxxxxxxx [<mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx>]
On
Behalf Of evb
Sent: Wednesday, September 13, 2006 3:47 PM
To: security-basics@xxxxxxxxxxxxxxxxxxxxx
Subject: RE: The VA Stolen Laptop – Lessons Learned

:1. Encrypt all data on mobile computers/devices which carry

RE: The VA Stolen Laptop – Lessons Learned

RE: The VA Stolen Laptop – Lessons Learned

:agency data unless the data is determined to be non-sensitive,
:in writing, by your Deputy Secretary or an individual he/she
:may designate in writing
:

And does "data" include operating system files, log files, cab files,
drivers, etc., or does it only include eg xls, doc, pdf and wpd files,
etc.?

How has Bush defined "data"?

Thx,

Eric

This list is sponsored by: Norwich University

EARN A MASTER OF SCIENCE IN INFORMATION ASSURANCE – ONLINE

The NSA has designated Norwich University a center of Academic
Excellence

in Information Security. Our program offers unparalleled Infosec
management

education and the case study affords you unmatched consulting
experience.

Using interactive e-Learning technology, you can earn this esteemed
degree,

without disrupting your career or home life.

<http://www.msia.norwich.edu/secfocus>

This list is sponsored by: Norwich University

EARN A MASTER OF SCIENCE IN INFORMATION ASSURANCE – ONLINE

The NSA has designated Norwich University a center of Academic
Excellence

in Information Security. Our program offers unparalleled Infosec
management

education and the case study affords you unmatched consulting
experience.

Using interactive e-Learning technology, you can earn this esteemed
degree,

without disrupting your career or home life.

RE: The VA Stolen Laptop – Lessons Learned

<http://www.msia.norwich.edu/secfocus>

This list is sponsored by: Norwich University

EARN A MASTER OF SCIENCE IN INFORMATION ASSURANCE – ONLINE

The NSA has designated Norwich University a center of Academic Excellence in Information Security. Our program offers unparalleled Infosec management education and the case study affords you unmatched consulting experience. Using interactive e-Learning technology, you can earn this esteemed degree, without disrupting your career or home life.

<http://www.msia.norwich.edu/secfocus>
