How Secure it Encrypted Data? From the Sound of it, Not Very Secure at All.

December 26, 2012 - There are a wide variety of data encryption programs available commercially, but the one that has attained the largest portion of the market is called Secured Shell (SSH). It is used by most large corporations and by the federal government to encrypt classified data. There is just one little problem with it. According to the inventor of SSH - Tatu Ylonen - the way that companies and the government have been using the program, a single hacker could write a fairly simple virus and steal or destroy nearly all stored encrypted data worldwide in just a matter of days.

SSH is considered to be the industry standard for data encryption. The way that it works is fairly simple. SSH scrambles data into a seemingly random series of digits and numbers. When it does this, it generates several lines of computer code. This code is called an encryption key and it is needed by anyone who wants to view the encrypted data in its original form. This portion of the program works as designed. It would be nearly impossible for any hacker to break an encryption key.

Unfortunately, every time SSH generates an encryption key, that key winds up getting stored someplace. These keys can be stored by computer browsers and in files on corporate and government servers. The keys don't expire so, once they are generated, if a hacker can find an active key then he can also gain access to the computer server that generated it.

Some companies have millions of these keys stored on their servers. The same is true with the government. And in tests run by the inventor of SSH, around 10% of the stored keys that they have been able to find will grant access to the core processes on the servers of the companies that issued them.

If you are not technical and you still don't really understand this, there is another way to look at it that is more comprehensible. The findings mean that approximately 90% of companies in the United States are violating federal compliance standard for financial institutions as a result of this issue.

Any hacker gaining access to world financial markets due to this vulnerability could create absolute havoc. Customer databases could be stolen, along with the identities of people in them. Even worse, all of the data could be destroyed; bringing all activities both government agencies and corporations to a grinding halt.

According to Mr. Ylonen, the problem has not been created by SSH. The problem is due to sloppy data management practices by the companies and agencies responsible for using SSH. Specifically, these organizations have not put in

place any mechanism to manage their SSH keys. The problem is now so large that he has come out of retirement to help find a solution to it. But until that happens, data worldwide will be vulnerable to this weakness.

byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS