Encryption backdoors will make us all more vulnerable

Muller, Nathan . Network World (Online) ; Southborough (Dec 3, 2015).

ABSTRACT

The author has written 29 technical books and is Managing Partner of Ascent Solutions, which provides marketing services to tech sector companies In the aftermath of the Paris attacks, one of the memes being perpetuated by "security professionals" is that the terrorists used encrypted communications, enabling them to plan and coordinate their activities without raising suspicion among the intelligence community. Another alternative is steganography, which encrypts messages that can be hidden within images of puppies, kittens and bunnies posted in plain sight on the Internet - all innocuous enough to avoid the scrutiny of law enforcement agencies.

FULL TEXT

The author has written 29 technical books and is Managing Partner of Ascent Solutions, which provides marketing services to tech sector companies

In the aftermath of the Paris attacks, one of the memes being perpetuated by "security professionals" is that the terrorists used encrypted communications, enabling them to plan and coordinate their activities without raising suspicion among the intelligence community.

Now there is a knee-jerk reaction among politicians in Washington to force encryption providers to build "backdoors" into their software that would allow government agencies to easily decode communications in their effort to identify potential terrorists. They say this is essential to keeping us all safe and that we must stop crying about the loss of personal privacy.

Left unsaid in all this clueless scare-mongering is that once a backdoor is built into encryption software anyone can enter, not just intelligence agencies.

A backdoor would make it easier for hackers everywhere to wreak even more havoc on financial, healthcare and retail sectors. They can use the backdoor to breach government, military and law enforcement agencies. They can tinker with our utility grid and shut down critical parts of our communications infrastructure, including vast chunks of the Internet.

Skilled hackers worldwide have already demonstrated that they can do all this and more, so imagine what they and dedicated terrorist organizations can do once our government mandates that all encryption providers equip their software with a backdoor. It is just a matter of finding the backdoor they know is already there and employing brute force methods to gain entry. The power of today's computer networks makes this a sure thing.

Perhaps the most asinine aspect of this discussion about backdoors is that the terrorists already use the strongest encryption and they are not about to "upgrade" it with a broken version that includes a backdoor.

If the tech sector is forced to equip their products with backdoors, how does this solve anything? Terrorists and criminals can turn to alternative methods to hide their communications, as they have already done with social gaming networks. Another alternative is steganography, which encrypts messages that can be hidden within images of puppies, kittens and bunnies posted in plain sight on the Internet - all innocuous enough to avoid the scrutiny of law enforcement agencies.

If you think the world is a bit too chaotic, you haven't seen anything yet. Under a backdoor mandate, computer systems, networks and devices will be rendered totally insecure, making all of us more vulnerable to the whims of criminals and terrorists.

There is ample reason for Americans to value their privacy. They do not like the idea of risking their bank accounts, credit cards and retirement funds to cyber-looters. They do not want their identities stolen, and then putting their lives on hiatus while they painstakingly sort it all out. They do not want to become bombarded with yet more scams, or become targets of new social engineering schemes that trick them out of their money.

The strong encryption currently employed in backend systems and on networks everywhere goes a long way to keeping criminals and terrorists out of our daily lives. A caution to our representatives in Congress: Know what the heck you are doing before deciding that backdoors will solve our national security problems. You may be opening the proverbial Pandora's Box - unleashing more chaos on the American public than you can possibly imagine.

Contact Muller at nmuller@ascent-llc.com

Credit: By Nathan Muller

DETAILS

Subject:	Law enforcement; Intelligence gathering
Publication title:	Network World (Online); Southborough
Publication year:	2015
Publication date:	Dec 3, 2015
Publisher:	Network World Inc.
Place of publication:	Southborough
Country of publication:	United States, Southborough
Publication subject:	Communications--Computer Applications, Computers--Computer Networks
e-ISSN:	19447655
Source type:	Trade Journals
Language of publication:	English
Document type:	News
ProQuest document ID:	1738847059
Document URL:	https://search.proquest.com/docview/1738847059?accountid=10378
Copyright:	Copyright Network World Inc. Dec 3, 2015
Last updated:	2016-03-13
Database:	Career &Technical Education Database

LINKS