Print This Article

<< Return to Encryption bans in the name of fighting terrorism hurt security

Encryption bans in the name of fighting terrorism hurt security

Rainer Enders, CTO of Americas, NCP Engineering
December 28 2011

The recent government crackdowns against encrypted communications are creating universal security risks for businesses.

In late August, Pakistan's Telecommunications Authority moved to inhibit terrorist communications by ordering the country's internet service providers (ISPs) to turn in customers who use virtual private networks (VPNs).

Unfortunately, banning encryption software seems to be gaining steam in other countries as well. India, China and Iran are just a few of the other nations that require anyone who wants to use encrypted software to obtain the state's permission.

Encryption bans are blanket solutions intended to prevent terrorist communications, but logically, this doesn't make any more sense than banning cars because of car bombing threats or planes because of hijacking risks.

Instead of solving the problem, these bans create more security risks.

Why is encryption important?

Encryption, a fundamental piece of IT and business security, is used to safeguard innumerable amounts of sensitive data every day. For instance, it protects personal data for e-commerce sites at universities, government entities, health care organizations and financial institutions, just to name a few examples.

For these industries and others, encrypted VPNs provide a safe way to enable communications over a shared network by making any transmitted information unreadable to anyone other than authorized parties. This includes distributed employees connecting to a centralized network, or approved third-parties connecting as customers or consultants.

Without encryption, these communications would happen over an open network vulnerable for hackers to intercept the data.

Globalization and mobility require encryption

Globalization and mobile employees intensify the urgency for secure, encrypted technology. After all, consider how many corporations are globally distributing their data, adding remote offices across several continents and creating public networks with worldwide users.

Additionally, employees now typically stay plugged into the company network, so they can work from anywhere, anytime. On top of that, an increasing number of people are using their mobile devices to share or access sensitive personal data.

Each of these scenarios could be a potential security threat and points to the need for encrypting data and using VPNs. The technology supports a mobile and globalized workforce by allowing employees to securely send and receive confidential information from remote locations.

Consequently, this severely cripples the ability to do business in any country with an encryption ban. Companies will not want to risk being exploited, so they will refuse to conduct transactions with businesses that leave their assets open on a shared network.

The rise of the hacker

The recent slew of phone hacking scandals and embarrassing company data breaches, plus the growth of prank hacking groups attacking both public and private sector entities, further demonstrates the necessity of encrypting information.

Every year seems to bring a new hacking scandal.

In 2007, the TJX hack exposed more than 45 million payment card numbers to criminals, bringing the issue of unsecure branch networks into the spotlight. In a breach that lasted from October 2008 to April 2009, the University of California at Berkeley faced a mortifying situation when overseas hackers gained access to data on tens of thousands of people who received health care from the university, exposing their medical information and Social Security numbers. The past several months have seen multiple data breaches against Sony, Amazon, Google and Citigroup.

The sophistication of hackers has been a wake-up call to security experts, who realize they are operating in a new world. The days when enterprises could feel comfortable behind vague security assurances are over. If hackers are able to breach encrypted data, then sending data with no encryption is like giving bank passwords to criminals. It's begging hackers to access all of your sensitive data.

The secure solution

As Black Hat technical director Travis Carelock said during the August conference, the three most important words to remember in regard to protecting data is encryption, encryption and encryption.

Securing communication has to take place as early as internet dial-up, which is the most frequent point of entry for hacker attacks. Additionally, using end-to-end VPN data encryption is essential for creating protected connections.

In the end, the potential for this ban to have widespread damaging effects makes me hope that it will only be used as a warning to terrorists — and not be strongly enforced.