Are encryption keys more important than your data?

Or all for the want of a crypto key!

Today, more than ever, protecting data and systems is extremely important – corporate reputations, and in turn their business, can depend on it.

There are many layers to data security and, for companies who rightly don't trust perimeter security, data encryption is the most important layer. Even at this layer however, there's an even more important level that many companies don't protect: *the encryption key.* With this in mind, I ask this question: Are your encryption keys more important than your data?

When faced with this question, most likely the immediate respond will be "The data of course." Upon further contemplation however, most people might change their answer. It's not as black and white as you might think.

Let's begin by asking two more questions: Would people disclose private information if they knew that it would be compromised? Could modern commerce be conducted without the promise of privacy? The answer to both of these questions is of course "No".

"While most security professionals understand the role of encryption, they are not so aware of the singular importance of keeping the key protected."

Something that people might not completely understand, because it's not often discussed, is that all modern encryption processes are publically known. Gone are the days of security by obscurity. The processes for today's popular cryptographic algorithms like ECC, AES, DES and RSA are well documented and understood. For thousands of years however, encryption processes themselves were considered secret. The problem with this practice is that the processes couldn't be sufficiently tested. These old solutions were secure until someone cracked them, and then they were obsolete. All it took was one person to crack the system – and no one knew who that one person was or when the process was cracked. This was of course what happened in WWII with the Enigma machine used by the Nazi regime. Both the process and the key were secret until the Allies cracked them – and the Nazis never knew when their process was compromised.

Modern cryptographers realized the folly of securing something by using a secret process AND a secret key. Some might argue that doubling the complexity is a good thing but it's the lack of vetting by peer review that make a secret process so vulnerable. The other thing to consider is that in a secret process there is always at least one person who knows the secret. What is stopping that person, and therefore the

secret, from being compromised or having the perception of compromise? A secure encryption solution can only have one secret in order to be secure. This is why a new process needed to be developed and the process needed to be tested with only one secret: *the key*. The only secret is the cryptographic key generated by the known process and subsequently used in a complex mathematical equation to make the data unreadable to anyone other than those who know the secret key. Another way to look at this is that the data may or may not be confidential, but in all cases the key must be secret. If the secret key is disclosed, then all of the data is disclosed.

The English language is full of Idioms for different situations. There is a reason why the term “weakest link” has so many other alternatives: Achilles’ heel, house of cards, kryptonite, single point of failure, fatal flaw, soft underbelly, gaping hole, etc. It is primarily because this situation occurs so often in real life that one expression would end up being redundant and boring. In the case of a cryptographic key, there aren’t enough idiomatic expressions to sufficiently express the modern-world devastation resulting from the compromise of a cryptographic key.

One of today’s data protection challenges is that while most security professionals understand the strength of standardized encryption through peer vetting, they are not so aware of the singular importance of keeping the key protected. There’s a very old little ditty that ends with “And all for the want of a horseshoe nail.” It’s a cautionary tale about how something as simple as a horse shoe nail can take down an entire kingdom. Cryptographic secrets are just as underappreciate and much more important. I’d like to offer a modern equivalent to make my point:

For the want of a crypto key the data was lost,

For the want of the data a reputation was lost,

For the want of a reputation the sales were lost,

For the want of the sales the revenue was lost,

For the want of the revenue the business was lost,

And all for the want of a crypto key*.*

Unlike a horseshoe nail, a cryptographic key can be protected with something as simple as a hardware security module (HSM) but unfortunately, in most companies, they are not. Organizations who wish to protect their data or systems using cryptography must begin to realize that the key used to protect the data or systems is more important that the data itself. Until they do, our personal data, corporate data and systems are open to compromise. Is the key more important than the data?

It’s not black and white after all is it?

Brad Beutlich
Vice President of Western and LATAM Sales, nCipher Security

To find out more how nCipher Security can deliver trust, integrity and control to your business critical information and applications, visit www.ncipher.com

Search: nCipherSecurity