Addressing Insider Threats, Cyber Attacks & Data Security

Aside from eliminating sensitive data from your business process, what are two things you can do to eliminate the risk of a data-breach?

Answer: **A**pplication **L**evel **E**ncryption and **S**trong **A**uthentication.

Longer Answer: While we recognize that encrypting sensitive data helps, most people – even in the security business – don't realize that not all encryption is equal. Even if using NIST-approved algorithms with the largest key-sizes available, data can still get breached. How is that possible?

When encrypting data, all else being equal from a cryptographic point-of-view, two design decisions matter: 1) Where is data being cryptographically processed? and 2) How are cryptographic keys managed?

If data is encrypted/decrypted in any part of the system – the hard-disk drive, operating system, database, etc. – other than the business application using that data, significant residual risks remain despite the encryption. An attacker need only compromise a software layer above the encrypting-layer to see unencrypted data. Since the application layer is the highest layer in the technology stack, this makes it the most logical place to protect sensitive data as it affords the attacker the smallest target. This also ensures that, once data leaves the application layer, it is protected no matter where it goes (and conversely, must come back to the application layer to be decrypted).

The second design-decision is how you protect cryptographic keys. If you use a general-purpose file, database or device to store your keys, this is the equivalent of leaving company cash in a general-purpose desk. Much as you need a safe to store cash in a company, you need a purpose-built "key-management" solution designed with hardened security to protect cryptographic keys. These solutions have controls to ensure that, even if someone gains physical access to the device, getting to the keys will be very hard to near impossible. If the key-management system cannot present sufficiently high barriers, even billion-dollar companies can fail to protect sensitive data – as many did recently!

While cryptography tends to get complex and the details seem burdensome, it is important to recognize that **an encryption solution provides the last bastion of defense** against determined attackers; it is well worth a company's time to give it the proper attention and not attempt to invent it themselves.

Conversely, **the first line of defense should be strong-authentication.** Strong-authentication is the ability to use cryptographic keys combined with secure hardware (in the possession of the user) to confirm that the user is who they claim to be. While digital certificates on smartcards provided such capability for two decades, they are expensive and difficult to use/support even in highly technical environments. An international standards group (fidoalliance.org) is attempting to simplify this with some solutions already making it to market with deployments under way – including StrongAuth's open-source FIDO Certified™ server.

Between application-level-encryption on the back-end and strong-authentication on the front-end, even if attackers manage to slip past network defenses – as they always seem to do – they will have little wriggle-room to compromise sensitive data. While no security technology is one hundred percent fool-proof, implemented correctly, ALESA raises the bar sufficiently high to "encourage" attackers to move onto easier targets.

Arshad Noor
CTO & Founder

StrongAuth®
Securing the Core

Contact Info

www.strongauth.com
(408) 331-2000

Arshad Noor is the Chief Technology Officer of StrongAuth, Inc. and has significant experience in enterprise-scale IT architecture, cryptography and open-source software. He is the architect and creator of many open-source data-protection solutions, such as StrongKey; StrongAuth KeyAppliance; StrongKey CryptoEngine; StrongKey CryptoCabinet; and the StrongAuth Document Protection Appliance. StrongAuth is a privately held company based in Silicon Valley, California and an innovator in encryption, tokenization, key-management and strong-authentication space. They bring new levels of capability and data security at a price point significantly lower than other solutions on the market. StrongAuth's solutions are installed at customer sites around the world and are key components of mission-critical business operations.