Debby Wadsworth
Writer & Consultant
DW-writer.com
debby@DW-writer.com
cell 763-350-8506

Project: Blog Post
Client: Velocity Tech Solutions
Writer: Debby Wadsworth, Freelancer
SME: Dylan Kerling, VTS Technician
Date: 3/2019

Secrets of How SED's can Save your Data

The loss of data is a concern for pretty much everyone. It can affect you and your business in many ways. The inability to find data can affect your ability to call people, treat patients, produce products, fill orders, send invoices, and much more. Taking measures to keep this from happening is a prudent step toward avoiding computer network downtime and having peace of mind. So, what is the secret to success?

"One effective step you can take is incorporating Self-Encrypting Drives (SEDs)," according to Dylan Kerling, Dell Certified Technician. "SEDs, as compared to your standard Hard Disk Drive (HDD), have a circuit built into the drive's controller chip." The circuit encrypts all data that is processed through the drive, eliminating the need for third-party software to encrypt your data on standard HDDs.

"SEDs work by effectively having two keys, with one key called the MEK or Media Encryption Key, and the other key is a KEK or Key Encryption Key," Kerling said. These keys work in tandem to encrypt the drive. The MEK is the key that encrypts and decrypts the drive and is set at the factory.
The KEK is a key you set during the configuration of your system. What the KEK does is encrypt and decrypt the MEK. Without the KEK during the initial setup, there is no way for the drive to decrypt the MEK. As a result, your data becomes unrecoverable.
Benefits of SED's:

1. **Limit Attack Surface** - SEDs enable you to limit the attack surface of the encryption. Encryption is all done locally on the drive, and nothing is processed within the processor or RAM, limiting the attack surface of the encryption.
2. **Transparent Process** - The process is also completely transparent to the user outside of providing the KEK. Furthermore, no applications or programs need to be run locally within the Operating System.
3. **Secure Erase in Seconds** - SEDs give you the ability to Instant Secure Erase a drive within seconds rather than hours. It clears the KEK and resets the encryption, effectively wiping the drive. It saves hours, especially for businesses that wipe drives before reuse or destruction. By running the instant secure erase command, you effectively change the key used to decrypt the drive rendering all the previous data unrecoverable.

Deployment strategy with SEDs should be a well thought out plan. The precise attention to the specific security problems they mitigate can be useful. Still, "they're not a defense against data theft or loss, nor are they by themselves a compliance procedure," Kerling said.

Security is a process, not a product, and while you can buy products that make the process easier, most of the heavy lifting is still yours to do. With SEDs the only way to protect against data theft is always the combination of firewalls, SEDs, actual monitoring (not just software), but

actual eyes-on monitoring. Annual, biannual, or monthly penetration testing. "Remember, the hack comes before the fix," Kerling stated. Although the costs are high for security, how much would a breach or theft cost?