IBM claims breakthrough Z Pervasive Encryption a Paradigm Shift in mainframe Security

BM’s mainframes are widely used in the tech industry for delivery of critical services to the government, including large banks, flight booking website, healthcare companies or an ecommerce platform. However, an increasing danger of our connected, digital world is the rise of hackers, and their potential to inflict serious damage with real-world consequences.

What the company has done for the first time ever with the newly released z14 mainframe is to allow Multiple levels of data encryption at every level of the system, and then storing everything inside encrypted containers, designed to hoodwink even the most diligent hackers out there. IBM, which reported revenue of $79.9 billion in 2016, said that its India hardware and firmware team had made significant contributions to the z14 system and microprocessor development.

Encryption is vital to security as only 4% of the more than 9 billion data records lost or stolen since 2013 were encrypted, According to IBM. A recent Ponemon Institute study found that extensive use of encryption is a top factor in reducing the business impact and cost of a data breach, reducing cost on average by $125 per record.

However, Encryption is perceived as complex. Organizations struggle with determining which data should be encrypted, where encryption should occur and who is responsible for it. Therefore many companies only encrypt what's required for compliance and also at the application layer. This leads to costly implementation and maintenance throughout the application lifecycle because of requirement of highly skilled manpower. As a result, IBM said only about 2% of corporate data is encrypted today, while more than 80% of mobile device data is encrypted.

IBM has introduced Pervasive encryption that provides a transparent and consumable approach to enable extensive encryption of data in flight and at rest to simplify and reduce the costs associated with protecting data and achieving compliance mandates This means it is possible to encrypt data associated with any application, cloud service or data base all the time, which IBM is claiming as a world first.

"The new capabilities being delivered with z14 will allow organizations to encrypt all of the data associated with an application or database, without the need to make any application changes and without impacting service level agreements," says Sardino. "No other platform in the world can do this."

"Strong walls and perimeter defenses are no longer adequate to shield organizations from cyberattacks. We must view data as the new perimeter, and put the security controls for the data on the data itself," says Nick Sardino, program director, IBM Z Offering Management. "That means implementing strong encryption of data wherever it resides."

To achieve this new standard for encryption, IBM Z delivered several new capabilities integrated throughout the z14 stack in the hardware, OS and middleware. The on-chip cryptographic acceleration was enhanced to provide more than 6x more performance than z13 at more than 18x faster than competitive platforms, according to a Solitaire Interglobal report. Bulk file and data set encryption was placed at a point in the OS where the encryption would be transparent to applications and highly optimized for performance. IBM also designed new capabilities to encrypt the data in the z/OS Coupling Facility, and more easily report on the security of z/OS network sessions.

Another concern for users is the protection of encryption keys. In large firms, hackers often target encryption keys, which are routinely exposed in memory as they are used, the company said. It said IBM Z can protect millions of keys, as well as the process of accessing, generating and recycling them. It does this in ‘tamper responding’ hardware that causes keys to self-destruct at any sign of intrusion and they can then be reconstituted in safety.

BM middleware such as Db2 and IMS was enhanced to exploit these new features as well. “Clients can transition Db2 and IMS high availability databases from unencrypted to encrypted without stopping the database or the application,” says Sardino, “which is a huge value for the DBAs that we’ve spoken to.”

BM Security also enhanced the IBM Security zSecure suite to provide administration and audit support for pervasive

encryption. The system also provides an audit trail showing if and when permissioned insiders accessed data. When organizations can quickly and easily demonstrate to auditors all of their data is encrypted, the cost and complexity are significantly reduced.

The suite can feed data into a newly designed QRadar dashboard for auditors. Other IBM Security solutions such as IBM Security Guardium Data Encryption for Db2 and IMS Databases and IBM Security Guardium Data Activity Monitor can be layered on top of pervasive encryption for additional levels of data protection.

Although there is a small chance that determined attackers will find a way of breaking the 256-bit AES encryption to access the stolen data, security commentators say that if the technology lives up to IBM's claims, it could be a big step forward in terms of data protection.

IBM Z is the only platform that offers the protection of pervasive encryption. This no-compromise approach to data protection is at the core of trusted digital experiences. With pervasive encryption you can rest easy knowing your data is secure.

References and Resources also include:

http://ibmsystemsmag.com/mainframe/trends/ibm-announcements/pervasive-encryption/

http://www.computerweekly.com/news/450422750/IBM-claims-breakthrough-in-mainframe-encryption