Microsoft Solution Case Study

DecryptNaBox

Enhancing on-premises email decryption solution with Microsoft Azure services

Solution Name: DecryptNaBox
Partner: Zeva
Website: www.decryptnabox.com
Country or region: United States

Company profile
Zeva enables organizations to access encrypted email for investigations and security scanning.

Supporting Microsoft software and services

- Microsoft Azure Key Vault
- Microsoft Exchange Server 2013
- Microsoft Windows Server 2012 R2
- Microsoft SQL Server 2014

"We found a way to decrypt emails without exposing the private key of the user, which was a huge security improvement."

Sam Andoni, Founder, Zeva

"With Microsoft Azure services, our customers can now use DecryptNaBox on an as-needed basis to handle investigations and avoid making a large investment in infrastructure."

Sam Andoni, Founder, Zeva

Though email encryption is increasingly important to governments and companies, it hampers an organization's ability to inspect documents for security or compliance. DecryptNaBox solves this problem by enabling access to encrypted email while preserving the integrity of the organization's public key infrastructure. DecryptNaBox facilitates eDiscovery, audits, mobile access to encrypted emails, and antivirus scanning, enabling companies to secure their emails while maintaining the ability to inspect them when necessary.

Lifting the covers off encrypted email
Unencrypted data is always at risk of being made public, as was made painfully obvious with the public release of emails from the Sony Corp in late 2014. With each new incident of confidential corporate information being made public, companies can no longer delay implementing email encryption, whether through a traditional public key infrastructure (PKI) or personal identity verification (PIV) using smart cards.

However, when organizations are considering email encryption, they must consider the implications for their security and compliance procedures. Encryption causes many problems that are not easy to address. After an email is encrypted, applications that deliver security and compliance by analyzing email content can no longer access the email. Antivirus scans aren't possible, and encrypted emails won't show up in search results or eDiscovery queries. Today, organizations often forgo implementing encryption to preserve their ability to inspect email for investigations or security.

Zeva is helping government agencies and corporations solve these issues and move forward with encryption programs with its groundbreaking DecryptNaBox solution. DecryptNaBox enables organizations to access the content of encrypted emails

Microsoft

while keeping each user's private key protected. The technology even works with hardware-based encryption, such as smart cards.

Creating a new technology

Zeva got its original ideas for the DecryptNaBox technology from an email migration tool that Microsoft released to facilitate adoption of Exchange 5.5. When security teams understood that they could use SecTool to decrypt and encrypt large amounts of Exchange data quickly and easily, the SecTool became one of the most popular tools in the security business. However, after Microsoft moved to new file formats with the release of Office 2007, SecTool no longer worked.

Many organizations had come to depend on SecTool, including many large departments within the US government. Zeva had contacts within these government organizations and within Microsoft and saw the opportunity to build a replacement. "We started from scratch to build a tool to help companies with eDiscovery of encrypted email," says Sam Andoni, founder of Zeva. "We found a way to decrypt emails without exposing the private key of the user, which was a huge security improvement." The technology, which is the basis of DecryptNaBox, has multiple patents pending, and has been approved for use by the US Government and meets FIPS 140-2 Level 3 standards.

DecryptNaBox works by taking advantage of the way email messages are encrypted in Microsoft Exchange. Exchange uses a message session key to encrypt and decrypt individual messages. The message session key is encrypted and decrypted with the user's private key from the organization's public key infrastructure (PKI) certificate authority (CA). Rather than providing the private key to use for encryption, DecryptNaBox pulls the message session key from each message and decrypts it within a hardware security module (HSM) that acts as an extension to the certificate authority.

With DecryptNaBox, private keys never leave the certificate authority. They stay within the HSM. Only the message session key is sent over the network. Email is decrypted by the DecryptNaBox client while keys are decrypted within the CA by the DecryptNaBox server. The server can be a physical server at the organization's data center or hosted by the PKI service provider.

Solving the government's problems

DecryptNaBox solves several problems for government agencies. "Federal regulations make it very difficult to get possession of an employee's private key, which slows down investigations," says David Spannare, Program Management Director at Zeva. "The other problem was responding to Freedom of Information Act requests, which required searching across all emails for specific keywords. It wouldn't be possible to get every employee's private key with current policies." By allowing the private key to remain inside the CA, DecryptNaBox solve these problems, enabling fast large-scale investigations.

Another problem government organizations face is the implementation of Homeland Security Presidential Directive 12 (HSPD-12), which calls for all government agencies to use a common hardware-based ID for access to computers and buildings. "When you use a hardware-based private key for encryption, the key has to remain on the hardware. Now you have to give someone a copy of the smart card to do an investigation that requires decrypting email, which isn't feasible and is delaying implementation of the directive," says Andoni. DecryptNaBox keeps the private keys within an HSM so this is not an issue.

Reaching beyond government

Organizations that want to protect proprietary information face the same email encryption issues as the government. Many Fortune 100 companies are using DecryptNaBox today to facilitate the use of encrypted email. But small companies need these capabilities as well, though they have struggled to justify the expense of on-premises servers and HSMs.

To better address the needs of its customers, Zeva has released a version of DecryptNaBox that runs on Microsoft Azure. It uses the Azure Key Vault service, which enables companies to store encryption keys in HSMs certified to FIPS 140-2 Level 2 standards. "With Microsoft Azure services, our customers can now use DecryptNaBox on an as-needed basis to handle investigations and avoid making a large investment in infrastructure," says Andoni.

Making decryption mobile

The growing adoption of hardware-based encryption using PIV poses significant challenges for mobile users. Mobile devices generally cannot host hardware keys or access smart-card readers. While solutions are available that use derived credentials to allow authentication, they do not address the needs of organizations with Medium Hardware Assurance policies, which is becoming more prevalent. The MobileDecrypt client works with mobile device management (MDM) solutions to enable mobile devices to read decrypted email without accessing user private keys. MobileDecrypt can be integrated into an MDM solution and works on any device supported by that solution.

Enabling encryption for everyone

The demand for email encryption—especially with the latest PIV technology that provides the best security—is growing, but the complexities it creates are slowing or preventing implementations. DecryptNaBox solves the problem of accessing encrypted emails within the organization for eDiscovery, audits, antivirus, data leakage, mobile access, and many other uses. The new Azure-based options mean any organization can easily take advantage of this solution without making significant infrastructure investments, enabling more organizations to implement the protection they require.

Document published May 2015

Microsoft