Reducing Your Risk – Email, Disk, and Device Encryption

Overview

You wouldn't mail a postcard covered with a patient's medical history, an employee's W-2 information or a customer's credit card number, but what if you found out that unencrypted email is an equally unsecure way to send information-if not worse? With unencrypted email, not only can an attacker intercept and read your message in plain text, but you won't know how many places the message is stored or even if it was intercepted. Email encryption scrambles information into an unintelligible mess of characters while it travels from the sender across the network, to the email server, to the recipient. It unscrambles it only for the person with the proper private key-the intended recipient of the message. Similarly, full-disk encryption renders your files illegible unless the proper secret key (your login password) is entered. This prevents an attacker who is in physical possession of a device from accessing the data stored on it. Since mobile devices are more likely to be lost or stolen than desktop computers, mobile device encryption is a critical component of your security plan.

Email Encryption

Many organizations avoid email encryption because it is seen as difficult or unnecessary. In fact, encryption is simple to set up, and by setting a user's mail client to encrypt email automatically, users will not even notice encryption at work. In addition, encryption will provide your organization with protection that far outweighs the minor setup cost. Often, federal and state data breach notification laws require entities to send data breach notifications to the media or customers only if the breach involved unencrypted information. Encryption is not only the right thing to do, but it can also save you from the reputational damage that comes with breach notifications.

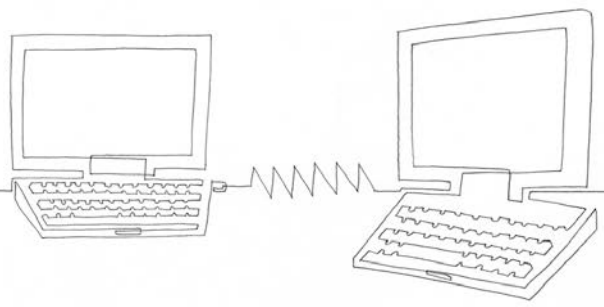
Considerations for SMEs

Open-source encryption tools Gpg4win for Windows and GPGTools for Mac encrypt your emails with industry-standard algorithms at no cost. These tools work with the most common email clients (Outlook for Windows and the Mail application for Mac) to secure your messages.

Email Encryption Options

Three common types of email encryption exist: web-based email encryption; attachment-based email encryption; and true end-to-end email encryption, in which the body of the email message is encrypted as it is sent across the Internet. With web-based encryption, the message is encrypted with SSL/TLS and uploaded to a web site. The recipient receives an email with a link to view the secure message, which is stored on a web server. The recipient logs into the web site with a username and password and views the message using a web browser. As you can see, this is a roundabout process that requires you to log on to a different website to view your messages. This also introduces a security concern, a third party. The Internet-based encryption service now has a copy of the message. SSL/TLS encrypts the message only in transit and not "at rest." However, the benefit of web-based email encryption is that it is very portable. The recipient needs only to have a web browser installed in order to view the "encrypted" message. No additional software is required.

With attachment-based email encryption, the encrypted message is sent as a file (such as an encrypted PDF or zip file) and attached to a normal, unencrypted email. Common software on the recipient's end, such as a PDF reader, can decrypt the file. The decryption password must be communicated separately to the recipient. This can



introduce significant risk, because often the sender sends the password in an email as well, which means that any attacker that gains access to the email account has both the encrypted file and the passphrase. A better solution is to transmit the password using a different form of communication, such as phone or in-person conversation.

True end-to-end email encryption can be integrated directly in your email software. Once you have it set up and working, it requires little or no effort to send an encrypted email to a recipient who also has end-to-end email encryption set up. Without involving a third party, your email client will scramble your messages so that they can only be read by you and the intended recipients. Quality encryption solutions work with your email client and are available for all major clients including Outlook, Gmail, and Apple's Mail application.

Ultimately it saves time to set up true end-to-end email encryption for parties with whom you communicate frequently. However, since you can't always control email environments outside of your organization (and both parties must implement true email encryption in order to send encrypted messages), web- and attachment-based encryption provide working substitutes so you can exchange secure messages with someone outside of your organization.

Disk Encryption Options

If criminals take possession of an unencrypted computer, tablet, phone, or a removable storage disk (USB thumb drive, external hard-drives etc.), there is no barrier between them and all of the valuable data stored on the machine. Full-disk encryption protects data by putting up that barrier, preventing access to files unless the user knows a secret passphrase that unlocks the machine. If a device gets into malicious hands, a passphrase may be all that stands between an attacker and an organization's confidential data, so it is critical that user passwords meet the following criteria:

- At least 14 characters (longer is better!)
- Contains no easy-to-guess passwords (i.e. summer16, username, dog's name, birthdays)
- Contains no default passwords (i.e. admin, password, 1234)
- Whenever possible, includes a complex mix of lowercase and capital letters, numbers, and special characters

Password habits are also very important. Make sure users are trained to avoid the following password pitfalls:

- Don't reuse work passwords for personal accounts and devices, or vice versa
- Don't tell anyone your password, regardless of who is asking
- Don't keep the secret passphrase physically with the mobile device (e.g., on a piece of paper). This mistake has caused organizations to be breached in the past, as the attacker was able to steal both the device and its private key together.

Desktop and Laptop Computers

These days, many servers, desktops and laptops include encryption software by default (although it may not be enabled). For example, the BitLocker full-disk encryption program comes preinstalled on most professional and enterprise versions of Windows. On Apple computers, FileVault 2 provides full-disk encryption, and comes enabled by default on the latest versions of Mac OS X.

If your operating system does not have built-in encryption, you can use third-party software to create encrypted volumes within a normal file system, encrypt partitions, or encrypt the full disk. The free, open-source software called VeraCrypt is a popular tool for this purpose. There are also a variety of commercial software solutions available.

Mobile Devices

Many of the most popular mobile device manufacturers, including Apple and Android, include an encryption feature into their operating systems. However, it may not be enabled by default, so organizations must make sure it is in effect. For the most recent Apple devices, encryption is currently enabled by default. Always set up a password to lock the screen on mobile devices. Password length is critical; require users to pick a long password.

USB Thumb Drives, External Storage Devices, etc.

In the case of removable storage devices, such as USB drives or external hard drives, consider devices with built-in encryption, for ease of management. For instance, Kingston makes IronKey encrypted flash drives that provide industry-standard encryption and self-destruct after ten unsuccessful password attempts, to thwart anyone that tries to guess the password.

If you buy laptops or USB drives without encryption already built in, you can use special encryption software to create encrypted volumes within a normal file system, or encrypt the whole device. VeraCrypt, BitLocker and FileVault 2 can all be used to encrypt USB devices.

Encryption Checklist

Encrypting your sensitive data consistently, with strong passwords, requires considerable effort, but quality encryption software can make this task easier for IT staff. Organizations should research which encryption option works best for their size, budget, and technical needs. Here are some tips for implementing encryption throughout your organization:

- Start by identifying the data in your organization that needs to be encrypted, and determine what type of encryption you need.
- Determine your encryption budget. Encryption products range from free open-source tools to paid solutions designed for use by large organizations.
- Look for a solution that implements the Advanced Encryption Standard (AES) algorithm, the industry standard specified by the National Institute of Standards and Technology in 2001. All three of AES's standard key lengths-128, 192, and 256 bits-provide robust, industry-standard encryption. Often, when encryption fails, it is not because of a deficiency in the algorithm but because of human error in its implementation.
- Configure email software to encrypt messages automatically so that it won't get in the way of employees' regular email use. This way, employees won't forget to encrypt or be tempted to skip encryption.
- Encourage parties with whom you communicate frequently to set up compatible email encryption systems so you can send each other secure messages easily.
- Enforce a password policy that requires users to use long passwords (not just the 4-digit PINs or geometric patterns that are often the default on smartphones).
- Train employees! Teach them how encryption works, why it is a critical component of your cybersecurity policy, and what they can do to help your organization stay secure.

Additional resources

eSecurity Planet, "Buyer's Guide to Full Disk Encryption"

GPGTools, open-source encryption tool for Mac

Gpg4win, open-source encryption tool for Windows

National Institute of Standards and Technology, *Announcing the Advanced Encryption Standard (AES)*

Top Ten Reviews, "Encryption Software Review"

Top Ten Reviews, "Mobile Encryption Software Review"

U.S. Department of Health and Human Services, "Breach Notification Rule"