Encryption in Government

Make the Rules, Play by the Rules

Few entities possess as much personal information as the U.S. government. In 2015, the Internal Revenue Service processed over 150 million tax returns, and the Social Security Administration paid benefits to nearly 60 million Americans. In a sense, the government lays the foundation for every U.S. citizen’s personal data the moment each person receives his or her Social Security number.

State and local government agencies possess a tremendous amount of sensitive personal information, as well. State revenue departments collect financial data in a similar fashion as the IRS. Many agencies have access to SSNs, which, if compromised, obviously give bad actors the foothold they need to steal an individual’s identity. Consider the Department of Motor Vehicles. Consider SNAP (Supplemental Nutrition Assistance Program, formerly known as the Food Stamp Program). Consider law enforcement agencies. At all levels, the government is the steward of its citizens’ personal data.

So, when things go wrong, they go horribly wrong. In 2015, two cyberattacks targeting the U.S. Office of Personnel Management (OPM) resulted in a personal data theft that affected 21.5 million Americans — one in every 15 residents. The hack, regarded as the largest security breach in U.S. history, cost the director of OPM her job.

In an effort to safeguard citizens’ sensitive data, numerous laws and protocols establish requirements for government offices in charge of sensitive information. Compliance isn’t as easy as instructing staff to keep their workstations password-protected. Personal data exists in many states, including when it leaves the confines of a network’s firewall. Data at rest that’s “in the wild” is the leading source of security breaches, so while the OPM cyberattack was unprecedented, real IT professionals must handle everyday security risks (such as a misplaced USB flash drive) with the same vigilance as a large-scale attack. In the following paper, we’ll cover what a government agency must do and what it (really) should do to move data safely on portable devices and drives.
Chasing Compliance: How Regulations and Encryption Fit Together

Encryption is terrific in theory. Data stays protected, and confidential information stays locked away from the wrong eyes. In reality, compliance requires resources, and encryption can constitute its own piece of that cost pie. Encryption may entail purchasing hardware and software, hiring a consultant, adding layers of data management, and more. Government IT professionals saddled with diminished budgets may need to decide between what's mandatory and what's optional.

In some instances, a particular regulation will mandate encryption in clear, unmistakable terms; those that don't adhere to these terms will be in violation of the law. Other times, regulations remain vague about requiring encryption, leaving murky waters for businesses to navigate. For example, a regulation may require that sensitive and/or personal data be “protected” without explicitly stipulating that it be protected via encryption — a less than ideal situation.

For times when the law confounds, security experts can provide clarity. A general consensus among experts regarding data protection protocols results in commonly accepted best practices. The term isn't exclusive to regulations and encryption, but it can nonetheless help guide companies that encounter nebulous regulations. If there are questions about implementing encryption that aren't spelled out in a particular law, following industry best practices will keep a business protected.

The Human Factor

Government offices can reasonably protect themselves against known threats. For example, they can set up firewalls to thwart incoming attacks and use VPNs and HTTPS as measures to keep in-transit data secured. All too often, though, a department's weakest line of defense is its own employees.

To wit, the Ponemon Institute's 2015 Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data report indicated that healthcare organizations (which bear many similarities to their government counterparts) worried more about employee negligence (70%) more than any other security threat. That's ahead of cyber attackers (40%), identity thieves (19%), and system failures (15%). Note that negligent employees aren't the same as disgruntled types, which the report classifies as "malicious insiders." Only 26% of respondents listed these employees as a chief concern.

Pointing the finger at hackers and other devious individuals is easy. IT pros must recognize that well-meaning yet careless employees pose a significant threat, as well. Negligent personnel are the reason laptops with treasure troves of data get stolen, and steps need to be taken to anticipate such events. Equipping portable computing devices with self-encrypting drives is one obvious step, but government offices should go further, particularly with removable storage. One might assume that a portable hard drive or USB flash drive would never be left unattended, but that's precisely the kind of employee negligence that is so dangerous. Disaster could be only a momentary misplacement away.

Meet FISMA, Formerly Known As FISMA

Each industry tends to have a regulation that serves as its cornerstone for compliance. For the federal government, we can turn to the Federal Information Security Modernization Act (FISMA). Passed in 2014, FISMA updates the Federal Information Security Management Act (also FISMA) of 2002. FISMA 2014 authorizes the Secretary of the Department of Homeland Security to aid the Office of Management and Budget (OMB) director in establishing security practices for federal information systems. Government agencies must also inform Congress of major security incidents (defined on page 7 of the October 2015 memorandum from OMB Director Shaun Donovan) within seven days. FISMA 2014 also calls on the OMB director to revise Budget Circular A-130 to streamline incident reporting.

As far as encryption and compliance are concerned, government agencies should turn to the National Institute of Standards and Technology (NIST) for guidance. Like other industries, the U.S. government's Federal Information Processing Standard Publication 140-2 (FIPS 140-2) is the chief standard for government encryption compliance. Federal government agencies and departments that handle sensitive personal data must use FIPS-certified cryptographic modules. A device that meets FIPS 140-2's requirement possesses a cryptographic erase function that "leverages the encryption of target data by
enabling sanitization of the target data's encryption key. This leaves only the ciphertext remaining on the media, effectively sanitizing the data.”

FIPS 140-2 contains four levels of increasing security. Level 1 requires that a solution use an approved algorithm or security function; the device itself requires no physical security. Level 2 requires a form of physical security that can present evidence of an unauthorized access attempt, such as a tamper-proof seal. A Level 3 solution provides a countermeasure that thwarts access, use, or modification of the cryptographic module if the solution itself detects a physical breach. Level 4, the pinnacle of FIPS 140-2, takes protection even further, detecting environmental variations (such as voltage and/or temperature) outside of a specified range and taking action to destroy cryptographic keys when it detects a breach.

When sensitive data leaves the confines of a protected local network, encryption must extend beyond laptops and back- up drives. Before dumping files on a flash drive to move data from system to system, remember that a self-encrypting flash drive which meets FIPS 140-2 requirements is consistent with the NIST’s mobile device encryption policy. Experts concede that banning all removable media isn’t feasible, but offices can nonetheless exercise tight control over what removable media is used. Best practices for removable media include banning personally owned flash drives and an insistence on department-issued drives.

Communicating or sending data over the Internet needs TLS (Transport Layer Security, a protocol for transmitting data over a network) and AES encryption. Using a secure VPN connection is essential when an employee accesses sensitive personal data over an agency’s local network.

FISMA applies at the federal level, but that doesn’t mean state and local governments and private contractors are free to disregard the legislation. Any entity that handles personal data from a federal source or those that administer federal programs at a state/local level (think unemployment insurance, Medicare/Medicaid, etc.) almost certainly must comply with FISMA. For government offices wholly outside of the federal government’s domain, consider hiring an independent consultant to definitively determine whether FISMA compliance is required.

Encryption and Security in Brief
Before learning how to protect data, it’s useful to know a little more about the data itself — specifically where it resides. For our purposes, data exists in the following three “states”: at rest, in transit, and in use. Data at rest refers to data located in persistent storage, such as a hard drive. This could be as simple as a saved document or image. Data in transit is any data sent or received across a network. Downloading a file from the Internet or transferring a file between two computers on a local area network are both cases of data in transit. Data in use is a little trickier, but it essentially means any data that a computer’s CPU is actively processing or data temporarily stored within a system’s RAM.

Encryption is a deep, complicated subject that many experts devote their lives to mastering, but having a rudimentary grasp of the key terms and concepts will help healthcare organizations better understand what it takes to be compliant. Ideally, sensitive data should be secure enough that unauthorized parties can’t even access or obtain it. Even if data falls into their hands, though, they definitely shouldn’t be able to read it. That’s where encryption comes in.

Encryption transforms data to make it unreadable without authorized access. In this case, authorized access comes in the form of a decryption key, which is fairly self-explanatory. When the right people have the key, they can read your encrypted data; the wrong people who don’t have the key cannot.

Many encryption methods exist, as do different instances when encryption is necessary. Encrypting data stored on a hard drive is one example, while accessing a business’s network remotely over a virtual private network is another. Unfortunately, when it comes to compliance, there’s no universal standard for encrypting data. The regulations that govern how each industry handles data may not dictate the same encryption requirements.

People with a passing familiarity with encryption may have heard of 128-bit, 192-bit, or 256-bit encryption. This refers to the “size” of the key, in bits, necessary to decrypt data. A 128-bit key corresponds to a total of 2128 possible keys; a 256-bit key represents 2256 possibilities. Generally, a larger key requires more time to crack via brute force methods (where an attacker uses a computer, or multiple computers, to “guess” the key). Security experts agree that it would take modern computers billions of years to brute-force a 128-bit key. Radical advancements in computing technology (quantum computing, for example) would be necessary to break 256-bit encryption.

Of all the encryption methods, AES (Advanced Encryption Standard) receives the lion’s share of attention, and for good reason. The NSA uses AES to encrypt data, which ought to be proof enough of its security. AES can use 128-bit, 192-bit, or 256-bit keys and thus far has been extremely resistant to attempts at exploiting potential weaknesses. Several cryptographers have tried to break AES, but none have succeeded.

If there’s a downside to AES, it would be in the computational cost of its operation. For many years, most digital encryption on computers was performed “in software,” where the systems CPU performed all of the necessary encrypt/decrypt operations. This work proved exceptionally cumbersome for general purpose processors and could bring a lower-end system to its knees. Only relatively recently have Intel’s AES New Instructions (AES-NI) and other innovations integrated specific encryption acceleration silicon into CPUs (thus running “in hardware”) and made the burden of encryption computation negligible. This also applies to the encryption of external drives, including flash drives. Somewhere, a component crunch those encryption processes, and if there’s no dedicated acceleration behind the work, other applications running on the system may suffer.

In addition to protecting data via encryption, it’s important to authenticate both data and communications (i.e., transmitted files and messages) to ensure that the data received matches the data sent. Verifying data arrived from true and trusted sources is another key aspect of maintaining security, which is why security professionals recommend cryptographic hashing. A hash is a number produced from a string of text that acts like a digital fingerprint. When someone sends a message, for example, they can generate a hash and include it with the message. The recipient of the message can then create a hash of the received message and compare it with the original hash. If the two match, the message’s authenticity is confirmed. Spoofing a hash is virtually impossible, so this tactic offers one way to ensure files and messages weren’t tampered with.

Encryption can — and should — happen in a variety of ways in a variety of situations. Windows BitLocker drive encryption is an example of one essentially free solution in the consumer space. Other times, certain hardware may be handy for encrypting data without the need for separate software. Such “self-encrypting” hardware options exist for large hard drives as well as portable flash drives. Web traffic can be encrypted using SSL (Secure Socket Layer), and the list goes on. Simply put, if desired, diligent users can keep their data encrypted wherever it goes.
Additional Regulations

Aside from FISMA, a handful of other standards and regulations may also affect government departments. Following are several such guidelines:

OMB M-06-16 is another memorandum from the OMB. Addressed to department and agency heads, OMB M-06-16 recommends "encrypting all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing; remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access; a 'time-out' function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity, and logging all computer-readable data extracts from databases holding sensitive information and verify[ing] each extract including sensitive data has been erased within 90 days or its use is still required."

A pair of NIST recommendations dictate security configurations for workstations (desktops and laptops) connected to a government network. The Federal Desktop Core Configuration (FDCC) covers systems running Windows XP and Vista, while the United States Government Configuration Baseline (USGCB) evolved from the FDCC and covers Windows 7 and Red Hat Enterprise Linux 5. Government agencies and others connected to government network can use NIST-validated SCAP (Security Content Automation Protocol) tools to verify compliance. Newer Windows operating systems (Windows 8/8.1 and Windows 10) have yet to be formally addressed, although older protocols can serve as guidelines.

The Director of Central Intelligence Directive (DCID) 6/3 applies more narrowly to classified intelligence data. Here, the manual calls for NSA-approved cryptography when classified data must be encrypted and transmitted.

Good Government

Thanks to the volume of personal data under its care, government networks, computers, and storage media will always be a high-priority target. Whether attackers are individual criminals or hostile foreign governments, cyberwarfare is no longer a science fiction story. It's real, and it's happening right now; just ask the U.S. Office of Personnel Management. Government agencies need to have the appropriate defenses in place, and robust encryption can form a solid first (and even last) line of defense.

SOURCES

https://www.ssa.gov/oact/STATS/OASDIbenies.html