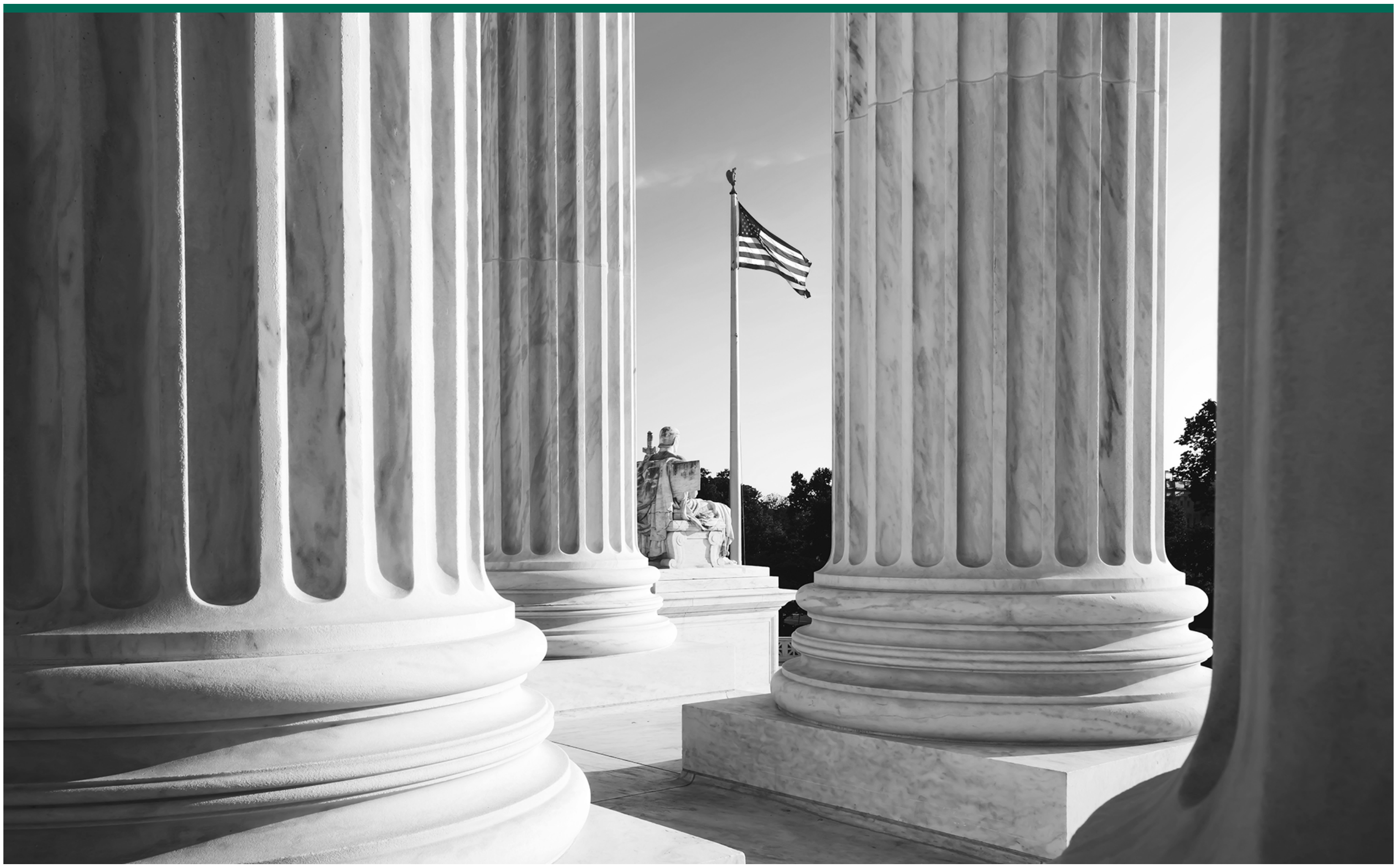
FORTRA

GUIDE (Core Security)

9 Ways Cyber Attackers Look To Exploit Government Agencies



Introduction

While any organization is susceptible to cyberattacks, government agencies can be particularly vulnerable due to the often-sensitive nature of the data they hold. “Government” may conjure images of high-profile agencies such as the Department of Defense or the Department of Energy, but any agency — whether large or small, whether local, regional, state, federal, or interstate — can be a target.

Organizations classified as Public Administration suffered nearly 2,800 cyber incidents, according to a 2022 breach report. Nearly 80% of these breaches are from external sources, and system intrusions surpassed social engineering as the top source of entry.

The Cybersecurity & Infrastructure Security Agency (CISA) “recommends that all organizations — regardless of size — adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets.”

This guide shares nine techniques threat actors use to access data from federal, regional, state, and local government agencies.

#1 Exploiting Misconfigurations

To err is human, but the unfortunate result of human error can be a breach or cyber incident. Misconfigured cloud servers, unchanged defaults, directory listings, and other improperly configured systems are all common, preventable errors that happen due to lack of resources or when appropriate controls and processes are not put in place. A slew of major cybersecurity incidents have occurred as a result of what industry experts call the inadvertent employee. This is a well-meaning IT professional who is often at fault when it comes to misconfigured servers, networks, and databases. It doesn't even take an advanced attacker to detect these weaknesses and use them to gain access to sensitive information. Software-as-a-Service (SaaS) misconfigurations outside a company's network infrastructure can also be the source of a breach, which is why organizations need to ensure the security of vendors.

#2 Circumventing Password Security

Despite the continual drumbeat message from agency leaders and IT about routinely changing passwords and avoiding simple ones like "Password123," many employees still aren't taking the message to heart. Password attacks are a common way for threat actors to gain access to an agency's treasure trove of data using common language dictionaries, brute-force attacks intended to crack relatively short passwords, phishing, or some combination of these approaches.

Taking a password that is known to work for at least one system or application, an attacker will then try it across an agency's environment to see if it will work elsewhere, granting further access. Since passwords are reused so frequently, credential stuffing is often successful.

Employees should only have access to systems critical to perform their jobs, and everyone should safeguard their logins, use a secure login, and, if working remotely, connect from a home network through a VPN before accessing agency resources. Government agencies should conduct security awareness training with staff at least yearly to go over policies and best practices. Efforts should also be made to make it as easy and efficient as possible to allow employees to securely reset passwords while consistently enforcing policies on strong passwords.

#3 Finding Application And Software Bugs

Employees need various applications and software on a day-to-day basis to perform their jobs. Certain applications may be downloaded to a workstation, while others are accessed via the cloud. Oftentimes, bad actors know the weak points that exist within these programs—especially in software that has been around for decades and constantly needs software patches or updates to the latest versions.

Though patching is a basic technique, it is often presented as one of the easiest security measures. However, in practice, patching does have its challenges—it if were that easy, everyone would be doing it consistently. But coordination is a time-consuming process that involves keeping track of updates, scheduling downtime, communicating relevant information to employees, and more. Ultimately, patching is still so foundational to security that having an effective patch management program is worth the effort.

While patching can't be the only line of defense, it's vital to continuously monitor and apply the software patches to programs and ensure virus protection is in place.

#4 Phishing Attacks

Another way that bad actors are looking to get in is by placing malware on a network through a phishing attack. There are different types of phishing attacks such as spear phishing or whale phishing. It all boils down to bad actors contacting employees and tricking them into clicking, downloading, or performing an action that will lead to the wrong people gaining access to the network.

In the second quarter of 2022 alone, the Anti-Phishing Working Group (APWG) observed more than 1 million phishing attacks—the worst quarter the organization has ever observed.

Falling prey to a phishing attack is as easy as downloading a file that looks like it's from a co-worker or clicking on a link that an employee believes is from a friend. The best way to protect against phishing attacks is to train staff to be wary of any and all communication they receive and to consistently test their awareness.

#5 Social Engineering Attacks

Facebook, Twitter, and other social media platforms are great for keeping in touch with friends, catching up on news, and sharing funny memes. However, they are also a trove of information for bad actors looking to engineer their way into a network. Stolen credentials are one of the most common ways that networks are compromised, and they are often stolen through social engineering attacks.

How do they do this? When setting up a user profile, people may be asked questions in order to reset the password such as "What year did you graduate?" or "What's your mother's maiden name?" While these answers seem like genuine questions to ask in order to verify one's identity, bad actors can access much of the information by trolling a worker's social media sites, depending on a user's privacy settings.

An easy way to combat this easy entry is to ensure password reset options are more than generic questions easily found on the internet. Agencies should implement multi-factor authentication for all password resets that relies on more than a question and answer but requires a one-time passcode or biometric authentication that only the appropriate users will have.

#6 DDoS Attacks

Attackers can quickly disable websites using distributed denial of service (DDoS) attacks, overloading servers with more requests than they can handle. These requests can crash servers that may take hours to recover. Since DDoS attacks are commonly used for espionage and state-sponsored operations, government entities are particularly attractive targets.

The problem is multifaceted, but one of the main drivers for this type of attack is the sheer number of embedded devices on networks that are often overlooked from a security perspective. While the number of network devices certainly won't be decreasing, there are things that government agency IT staff can do to make it more difficult for bad actors to penetrate. Quickly detecting weaknesses in the network and determining potential attack paths to critical assets can help staff prioritize vulnerabilities to fix before something bad happens.

#7 Exploiting Connected Devices

Tech-enabled devices like smartphones, smart watches, wearables, industrial devices, and more that make up the Internet of Things (IoT) already have hit 22 billion, a figure expected to rise to 30 billion IoT devices by 2025. To put that in perspective, that's more than 150,000 IoT devices connecting to the internet per minute.

The release of a new iPhone or some other piece of technology can be so exciting that some people don't think about how to protect them and their longevity. No, this doesn't mean buying insurance to protect from breakage, but, rather, ensuring the right types of defense are implemented on devices or properly and securely accessing the different networks a device interacts with on any given day.

Employees can make accessing networks more difficult by switching these devices from automatically connecting to a home or work network. Yes, it's easy and convenient to automatically connect or search for open Wi-Fi locations, but that can be incredibly dangerous for the device and future networks that are connected.

Some government entities have SCADA (supervisory control and data acquisition) control systems that comprise computers, graphical user interfaces, and networked data communications that provide high-level supervision of machines and processes that also are subject to attack.

The National Security Agency (NSA) and CISA have issued new guidance in response to a recent uptick in attacks. The NSA advises companies to be aware of what system information should be publicly available and assume their networks are a target.

#8 Deploying Botnets

Attackers that successfully access agency networks can turn computers into botnets, short for robot network. After deploying malicious software, they can remotely control these machines to conduct malicious acts such as DDoS attacks, cryptomining, deploying malware, spam attacks, spyware, and engaging in click fraud campaigns. More sophisticated botnets can challenge the network infrastructure of government agencies and enterprises, using botnets to move inside a network to mine data or launch ransomware attacks. Botnets often go undetected—unless the agency is regularly monitoring the infrastructure to discover critical threats in real time.

Botnets have become such a huge issue and used for state-sponsored activities that the Justice Department has to step in to sever connections among botnets. Ideally, agencies want a solution with multiple, overlapping detection methods to identify threats quickly so they can be halted immediately.

#9 Deploying Ransomware

Ransomware can be devastating for government entities of any size. Not only can attacks cripple a network, attackers can expose sensitive information, sell data on the Dark Web, destroy data—or even refuse to decrypt data despite payment. Depending on the agency, compromised records include customer and employee data, financial data, and intellectual property.

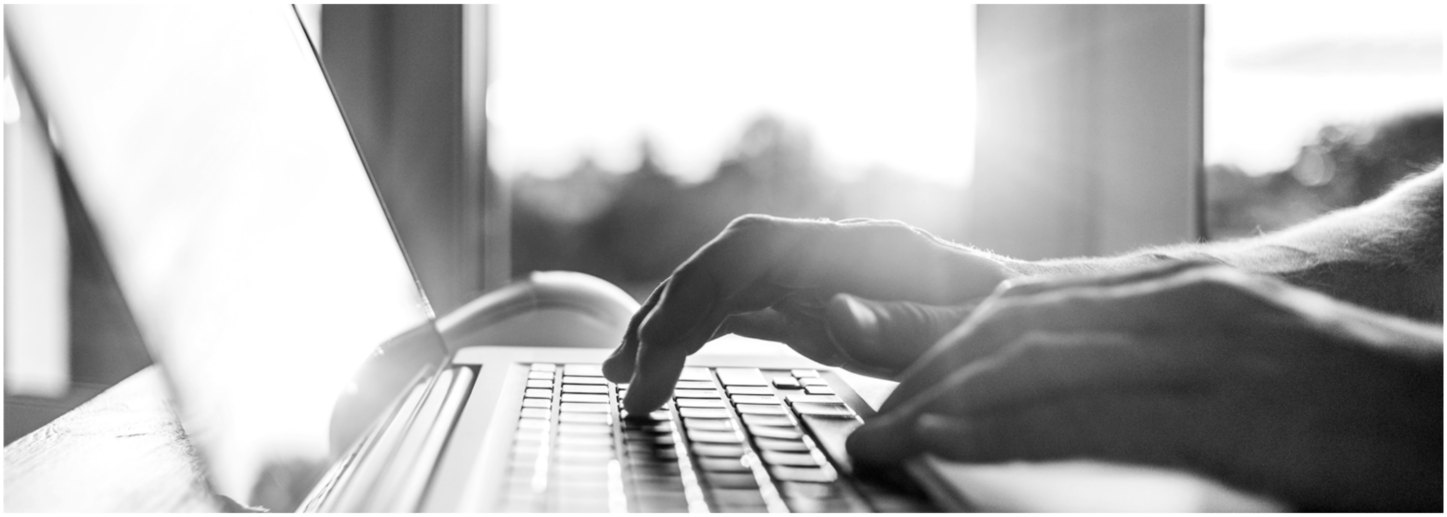
Federal, regional, state, and local agencies still often use legacy software applications, which can be particularly vulnerable. Most attacks start with a phishing email of some type to entice an employee to click on a malicious link or take some action to initiate the hack. Although not as common, other entry points include email attachments, users visiting compromised or malicious websites, and exploit kits.

CISA recommends regular vulnerability scanning, especially on devices that connect to the internet, and regularly updating and patching software and operating systems.

How To Protect Government Data With Proactice Security Solutions

A journey of 1,000 miles begins with a single step. Here are three steps on the road toward a proactive security posture to protect sensitive agency data — and your agency's reputation.

- Using automated tools, a vulnerability scan examines an environment and generates a report of any vulnerabilities that are uncovered. Look for solutions that audit for compliance to security regulations, use external intelligence to prioritize vulnerabilities, and allow you to keep track of changes like remediation measures or asset additions.
- Penetration testing builds upon vulnerability scans to help agencies prioritize patches based upon their unique technology infrastructure. A vulnerability in one area may be considered a critical fix for one agency, while the same vulnerability would be a low priority for another agency. Pen tests can help prioritize remediation plans based on what poses the most risk, then re-examine an environment after remediation to ensure the fixes have been successfully implemented.
- While vulnerability scanning and penetration testing uncover vulnerabilities, red teaming seeks to fully assess the defenses of an organization by simulating an attack scenario. A red team tests the security posture of an organization to see how it will fare against real-time attacks before they actually happen.



Conclusion

Breaches are inevitable at nearly any organization or agency at any time, but the financial and reputational consequences will be much more severe among organizations that didn't take simple and expedient steps to secure and monitor networks and devices. Knowing that bad actors want to breach an agency's sensitive data should compel security teams to protect the agency and the communities they serve. As a starting point, agencies should have a strong understanding of what the current IT environment looks like and what vulnerabilities are high priorities.

To find out how to get started, contact one of our security consultants about our offensive security solutions or our Security Consulting Services.

For more information, visit www.coresecurity.com