ManageEngine
Desktop Central

COMBATTING **CYBERATTACKS** ON **GOVERNMENT ENTITIES**

EXECUTIVE SUMMARY

The cyberthreat landscape for 2020 looks grim. Ninety percent of organizations believe cyberthreats will worsen next year, and 51 percent of organizations are still unprepared to handle a cyberattack. Businesses are not planning for all possible contingencies, and any organization can be in the crosshairs of a cyberattack.

Some organizations, like those in government, are especially prone to attacks; the government sector is one of the prime targets for cyberattacks in 2020. Digitization has led to extensive usage of the internet in all sectors, increasing the attack surface for all businesses. It's time for all organizations, but especially government agencies, to bolster their cybersecurity strategy.

GOVERNMENT ENTITIES ARE, BY AND LARGE, THE PRIME TARGETS

> Did you know that **95 percent of breached records** in 2016 were predominantly from three sectors, government, retail, and technology?

These sectors are no less diligent than others in terms of security, so why are they so much more attractive to hackers? It all comes down to the vast amount of personally identifiable information (PII) stored within their records. Government agencies at all levels, be it federal, state, or local, hold classified information that could range from citizens' birthdays to their Social Security numbers. At a micro level, loss of this data can cause identity theft, but at a macro level, state secrets can be exfiltrated.

It should come as no surprise that the United States government is highly targeted. The National Security Agency (NSA) was hacked a few years ago, and since then, there have been many high-profile ransomware attacks on US cities. Here's a quick recap of some of the recent cyberattacks on US government organizations.

> In December 2019, a cyberattack on the **city of New Orleans** led to a state of emergency, shutting down all the computers and servers across the city. Earlier in 2019, **Texas was hit by a ransomware attack** that impacted computer systems in 22 municipalities and hackers demanded a whopping $2.5 million to retrieve the files. In June, the small town of **Lake City, Florida was maimed by a ransomware attack** that prevented government employees from accessing their email and making online transactions; the city ended up paying a ransom of $460,000 in Bitcoin. Another Florida city, **Riviera Beach, paid nearly $600,000 in ransom,** while New Bedford, Mass. and Atlanta rejected hackers' ransom demands and are in the process of retrieving their data. The list goes on.

Whether it's the 2009 attack on the Homeland Security Information Network, or the attack on the city of New Orleans ten years later, cyberattacks continue to haunt government entities and endanger the global economy.

> **The Senate report** discloses that government agencies reported 35,277 cyberattacks in 2017 alone, an average of nearly 100 attacks a day.

As mentioned in the report, besides the lack of expertise and shrinking budgets, two major reasons governments fall prey to cyberattacks is that they can't maintain an accurate list of IT assets, and they don't have automated patch systems to install security patches.

Audits by the US Inspector General have also acknowledged that some government agencies use legacy systems that are no longer supported by vendors, making it all the more difficult to secure these systems. Perhaps the most startling fact is that the Department of Homeland Security continues to use outdated systems and has failed to address loopholes within its systems.

HOW CAN GOVERNMENT ORGANIZATIONS COMBAT CYBERATTACKS?

The cornerstone of any organization is its endpoints, be it desktops, laptops, smartphones, tablets, or servers. Government organizations should take the following measures to secure their endpoints and combat cyberattacks.

01 Assess and remediate vulnerabilities

It's important to not get swayed by every vulnerability that is identified, because one vulnerability is identified every 90 minutes. Not necessarily every vulnerability requires immediate attention. The magnitude of vulnerabilities can make it appear almost impossible to assess them, but having a solution that can categorize discovered vulnerabilities and automate the process is nothing short of a blessing for the IT department. The icing on the cake for government agencies is to have one solution that can assess and deploy missing patches automatically.

02 Religiously follow the Zero Trust principle

Government employees use a plethora of portable devices on a daily basis. Insider threats, including exfiltration of classified data using peripheral devices such as USBs, can cost an organization up to $8.76 million a year. While it is true that 34 percent of data breaches are due to insiders, it is also true that 70 percent of insider threats go unreported. The principle of Zero Trust can revolutionize an organization's cybersecurity strategy by protecting against insider threats.

Government entities can avoid many cyberthreats if they assume that no individual or system can be automatically trusted. Organizations should enforce a Zero Trust policy wherein each device has to be scrutinized and deemed fit for usage before it's authorized. Additionally, IT departments should keep track of the data that is copied to and from the peripheral devices. Limiting file transfers based on file size and type can help prevent data loss as well.

03 Secure the one endpoint every organization has, browsers

More often than not, organizations overlook browsers as a potential source of cyberattacks; however, browsers are by far one of the easiest means of planting an attack. Cyberattacks on extensions, such as the Evernote Web Clipper's Chrome extension, could have been fought in hindsight with a solution that can detect the permissions possessed by each extension and automatically disable extensions that could cause a breach.

Phishing accounts for 90 percent of data breaches. Organizations can filter URLs and whitelist trusted sites to prevent end users from accessing malicious sites. To protect browser data, it is highly recommended that you isolate browsers, because even if an end user accesses a malicious site unknowingly, the web session will be opened in a virtual browser, thereby preventing malware from infecting the system; the browser data will also be erased once the session is terminated.

04 Safeguard all applications

Each organization requires various applications for hassle-free operations. It is onerous for the IT department to keep tab on the permissions that are being granted to each of these applications. To ensure only authenticated applications access corporate data, it is important to whitelist applications, automatically uninstall blacklisted ones, and prevent the installation of applications from third-party sources.

In light of bring your own device (BYOD) policies, government organizations should implement a solution that can hold personal applications and corporate applications in two separate virtual containers. In case of lost or stolen devices, organizations need a way to perform a complete data wipe and ensure no corporate data is stolen.

05 Have a bird's-eye view at all times

Unified dashboards can give government organizations a quick glimpse of all possibly vulnerable avenues so they can prevent attackers from exploiting their network. Organizations should monitor device audits, browser usage, potentially harmful add-ons, outdated software, highly vulnerable machines, the number of vulnerabilities in the network, and other important security information.

Government entities should assess what is at stake if a cybercriminal infiltrates their network. Organizations should take an inventory of all their IT assets at least every 24 hours to make anomaly detection a walk in the park. It's also best practice to never grant full access to anyone who doesn't need it. Having a centralized view of all user permissions will help organizations monitor the resources each user can access. Furthermore, frequent and complete backups will ensure that data is saved and protected and that the recovery process, should it be necessary, is as seamless as possible. Backups should ideally occur as often as resources permit.

CONCLUSION

When it all boils down to the question of “Should I pay the ransom or not?”, here are a few disturbing numbers to keep in mind. Out of the 39 percent of security professionals who chose to pay the ransom after an attack, less than one-fifth were able to retrieve their critical data. For instance, NotPetya turned out to be a lose-lose for victims that paid the ransom, as they did not get their files decrypted. Even if an organization manages to retrieve its data, it should still go to great lengths to ensure that no traces of ransomware are left behind. Sadly, over 50 percent of businesses do not have the budget to recover from a cyberattack.

Government organizations have always faced an uphill battle against cyberattacks. Although combatting cyberattacks is a gargantuan task, with the help of a robust unified endpoint management solution, **ManageEngine Desktop Central,** government organizations will be one step closer to stopping attacks.

Reach out to us for a personalized demo of Desktop Central. You can receive a free, 30-day trial to explore Desktop Central.

Schedule a demo **Free trial**