AGILE1
Managed Breach Protection

Managed Breach Protection for Government Organizations

OVERVIEW

Government organizations at the local, state and federal level have all become prey for advanced hackers. The threat is only growing as malicious actors and nation states recognize that government agencies are often easy targets with thin budgets and few resources. As technology becomes more advanced it's crucial that governments are equipped with the proper cybersecurity to avoid hacking scandals that could have adverse effects on the institution.

What options do government organizations have? The emerging area of SOC-as-a-Service offers governments the opportunity to augment their existing IT staffs and improve their security postures while protecting their entire digital infrastructure including cloud, network, remote workers and on-prem network 24x7.

AT A GLANCE

- The U.S. government plans to spend almost $19 billion on cybersecurity in 2021.
- Only 68% of U.S. states have a documented and approved cybersecurity strategy.
- In 2020 there was a reported 31,107 cybersecurity incidents against U.S. federal agencies.
- The main barrier to effective cybersecurity in the U.S. is due to claims of a lack of budget.

Clement, J. (2020, July 22). Topic: U.S. government and cyber crime. Statista.

Meeting these diverse cybersecurity requirements is a challenge, and governments unable to demonstrate the capabilities of a security operations center (SOC) put their organization in jeopardy. Cybercriminals are now capable of exploiting weaknesses at previously unseen speed and scale by rapidly acquiring new cyber weapons and continuously modifying their attack techniques. As threat actors continue to adapt and evolve, paying attention to cybersecurity strategy is paramount to government organizations regardless of size, branch, and function.

BEATING HACKERS AND MAINTAINING CMMC STANDARDS

Government organizations have significantly benefited from digital transformation. Paper-based records and communications have long been replaced by email, video conferencing, cloud, API's, VoIP, cloud-based software-as-a-service (SaaS) solutions, and more. Unfortunately, these improvements in operational efficiency also come with increased risks. While governments have been relatively quick to adopt and deploy promising digital technologies, they must take increased precautions in order to protect sensitive information and data.

BEATING HACKERS AND MAINTAINING CMMC STANDARDS CONT.

The Cybersecurity Maturity Model Certification (CMMC) is a standard promoted by the U.S. Department of Defense (DOD) that requires their contractors to maintain certain standards of cybersecurity when working with them. The CMMC will be implemented soon and the DoD hopes this will mitigate the risk of cyberattacks after experiencing large information security compromises in the past. Contractors should become familiar with the technical requirements under CMMC and the five tiered levels security. If contractors choose to comply with higher levels, they must also meet the criteria of the lower levels. DOD contractors should start preparing now to meet the minimum CMMC requirements in order to maintain cyber-compliance.

CYBERSECURITY CHALLENGES IN GOVERNMENT ORGANIZATIONS

Today's cybercriminals hold a strategic advantage, as they can launch attacks at a fraction of the cost–in terms of time, complexity, and resources–that governments must typically spend to defend against them. This asymmetric nature of cybercrime is particularly pronounced in smaller governments that may lack the financial resources or have access to skilled security professionals. What's particularly alarming is that in recent years the U.S. government has faced billions of dollars in damages as a result of cyberattacks. With a past a vulnerability, the U.S. government now plans to spend over $92 billion in IT security expenses.

The growing numbers of devices and applications at law firms today further exacerbates the problem:

- **Expanded attack surface:** Every endpoint, network device, server, or application expands the attack surface, especially when government officials are required to work with sensitive information.
- **Hostile insiders:** Weak or non-existent IT security standards for remote workers often lead to hostile rogue insiders jeopardizing the organization and its officials.
- **Human error:** Lack of appropriate internal security training and poor supply chain risk management lets even well-intentioned employees or third-party vendors create accidental exposure

Detecting patterns of anomalous activity and potential compromise requires the deep analysis of several critical log sources, including:

- Firewalls
- IDS/IPS
- Endpoint security (AV)
- Active Directory
- Email security gateways
- SaaS applications
- Cloud workloads

TARGETED ATTACKS ON GOVERNMENT ORGANIZATIONS

While governments of all sizes must comply with frameworks to maintain security and confidentiality, they face even greater risks and challenges from today's cyberthreats. A single data breach can cause widespread harm to an organization, including the exposure of confidential information on a variety of issues and officials.

Cybercriminals continue to devise new attack methods. Below are the top four methods of cyberattacks online retailers have suffered:

- Ransomware is a type of malware that either threatens to block access to a victim's data, publish it, or destroy it unless a ransom in cryptocurrencies is paid. Government organizations may install AV or endpoint protection platform (EPP) solutions on employee endpoints, real-time threat intelligence, or custom threat detection logic, but without having an expert team to carefully analyze alerts and event log data, an attack can go unnoticed. These attacks have become particularly notorious for their ability to evade traditional endpoint controls.

- **Phishing attacks** seek to obtain sensitive information such as usernames, passwords, social security numbers or credit card numbers. Attackers typically operate under the guise of a trustworthy entity, such as a website for a government, or the login page for an email or messaging service. Email security solutions that offer real-time analysis of URLs in emails, email attachments, and web objects can help with detection. But email security solutions are often unable to flag an embedded malicious URL or attachment before the victim interacts with it. In such cases, governments without continuous network monitoring, Active Directory (AD) monitoring, or advanced monitoring for any deployed SaaS applications are left vulnerable.

- **Brute-force login attacks** involve threat actors systematically attempting password or passphrase combinations until finding correct combinations and accessing restricted resources protected by passwords. In-depth analysis of Active Directory logs and SaaS application login activity are the primary methods used to detect such attacks. Unfortunately, working with authentication data logs is complex and may require analyzing terabytes of data.

- **Attacks on unpatched servers** and infrastructure are specifically designed to exploit weaknesses and vulnerabilities in servers and other Internet-facing systems. In a vast majority of such attacks, patches are publicly announced and made available. For appropriate defense, retailers access to advanced vulnerability scanning tools for system hardening and alerting. Ideally, they should also deploy continuous network monitoring tools with customized rules to detect anomalous scanning requests coming into Internet-facing entities.

A NEW APPROACH FOR A SECURE FUTURE: ADOPTING SOC-AS-A-SERVICE

A SOC-as-a-service enables government organizations to address the listed security gaps that result in the cyberattacks covered in the prior section going undetected. Using a managed SOC service gives organizations complete centralized visibility into their networks' security and the ability to leverage existing point products and security investments. It also creates access to regular vulnerability assessments and enables organizations to establish a detailed and customized incident response plan.

What's more, it helps governments provide strong evidence of security processes during technology audits, avoid compliance penalties, and establish trust and security within the organization.

The time for governments to make strategic security improvements is now. Effective cybersecurity makes organizations more prepared, more resilient, and better protected so that they can continue to fulfill their obligations and represent the needs of their community. **SOC-as-a-Service offerings like Agile1's Managed Breach Detection SOC offers government organizations the ability to improve their 24x7 monitoring, detection, and response to cybersecurity threats while meeting their regulatory obligations around mitigating cybersecurity risk and ensuring resilience.**

ABOUT AGILE1

Agile1 is a leading SOC-as-a-Service technology provider redefining monitoring, detection and response. Our Machine Learning and User Behavior Analytics – based SOC analyzes data at the end-points to find security events before they proliferate. The Agile1 SOC includes 24/7 monitoring, alerting, incident investigation, threat intelligence and auto response. For more information visit: www.Agile1.io

AGILE1

Managed Breach Protection