A GOVERNMENT TECHNOLOGY Q&A

government technology

CYBERSECURITY RESILIENCE

To Strengthen Cybersecurity, Governments Need to Be Proactive

Ransomware attacks cost governments in the U.S. more than $18.9 billion in 2020.[1] Government agencies also face many other types of incursions that interrupt their operations, enable identity theft, increase expenses and cause other issues.

***Jared Pane,** senior lead solutions architect at Elastic in Mountain View, Calif., says that to avoid damaging attacks, state and local governments need to do more than merely react to cyber threats. In this Q and A, Pane shares his thoughts on how to enhance cybersecurity with a more proactive approach.*

What's the difference between taking a reactive or proactive approach to cybersecurity?

Due to competing priorities and resources constraints, many state and local governments wait for something to infiltrate the IT environment before they take countermeasures. They suffer a ransomware attack, or they detect a threat actor when it's already moving through the infrastructure. Cybersecurity solutions point out malicious activity they need to check out, but busy analysts and administrators can respond to only so many alerts. The rest can fall through the cracks, leaving systems vulnerable.

When you take a proactive approach, you don't wait for something bad to happen and then fix it. You keep bad things from occurring in the first place. Done right, proactive measures are simple for security teams to take on and are affordable.

What preventative measures should governments deploy?

Implement antivirus software or malware protection. Stay up to date on your patch management life cycle. Develop a comprehensive incident response plan. Implement a strong perimeter defense with security controls. Install a virtual private network (VPN) and implement a mobile device management tool that can track devices if they're lost or stolen. And use machine learning to spot anomalous patterns in network activity that human observers would never catch.

What are some solutions from Elastic that strongly support the proactive approach to cybersecurity?

More and more, we are seeing cyber intruders take hidden footholds on systems and move laterally through the network. Being proactive requires the ability to retain and look back at older data.

Elastic's "searchable snapshot" and "frozen tier" features let you retain large data volumes for years in a format that's immediately searchable. You don't need to go through the time-consuming process of rehydrating stored system activity data that has been migrated off into a non-searchable snapshot. Instead, that data is available immediately for audit or investigative purposes. You can also use stored data to compare current and past activity, helping you spot anomalies or malicious activity before it spreads throughout your data center. Besides helping you gain better insight into potential threats, these features can reduce costs. Elastic's technology allows you to ingest as much data as you'd like, but also allows you to retain your data on inexpensive media.

Elastic also helps you be proactive by automating and actioning routine cybersecurity tasks. For example, when you want to investigate network activity and hunt for threats, rather than build queries from scratch, you can use our Timeline feature in Elastic Security to design queries by dragging and dropping fields. Our Kabana Lens product lets you leverage drag-and-drop capabilities to quickly develop cybersecurity dashboards for use in a security operations center (SOC).

Do you have any final advice for state and local governments?

Create an incident response plan and security policy. Have a centralized SOC where you can collect all of your important data and proactively monitor as well as threat hunt. Backups are extremely important, especially as a defense against ransomware attacks. Instead of paying a ransom, you can roll back to the last available good timing of your system. All these measures, coupled with employee training and awareness, can help state and local governments head off cyber attacks before they have a chance to cause serious damage.

elastic

Elastic is a search company that maximizes data utility in real time. Customers worldwide use our search, observability, and security stack to achieve data-dependent use cases like website search, application performance monitoring, user behavior analysis, security investigations, and threat hunting. Deployable on cloud or on premises, Elastic delivers powerful insight, no matter the mission.

[1] https://www.comparitech.com/blog/information-security/government-ransomware-attacks/

Photo provided by Shutterstock.com