How State and Local Agencies Can Ramp Up Ransomware Defenses

A recent cybersecurity study from the National Association of State CIOs (NASCIO) and Deloitte found 75% of state CISOs view ransomware as a threat. There's good reason for that, as a number of factors combine to make state, local, tribal and territorial (SLTT) governments vulnerable to this type of attack:

- **High impact:** Ransomware is uniquely capable of bringing an organization's operations to a halt and is one of the most likely threats facing SLTTs. Ransomware incidents also grab media headlines, increasing pressure on the victim.
- **Low bar of entry:** With "Ransomware-as-a-Service" or commercialization, even non-technical threat actors can easily profit from ransomware operations.
- **Emergence of distributors:** Malware families like Emotet are prolific info-stealers and downloaders of other malware, and are demonstrably linked to ransomware operators and affiliates. Emotet has recently re-emerged from a long period of dormancy.

In this environment, SLTTs need to revamp their defensive strategies.

govloop

CIS Center for Internet Security®

The Challenge: A Perilous Landscape

A number of emerging challenges create a perilous ransomware landscape for SLTTs, including:

- **Known attractive targets:** SLTTs hold valuable data, from legal information to health care records. Their responsibility for critical infrastructure increases this vulnerability: The threat of disrupting transportation, water or sewage treatment operations, for example, gives cybercriminals leverage.
- **Evolution from opportunistic to targeted attacks:** Ransomware has evolved, with attackers these days casting a wide net to identify victims and then focusing their ransomware efforts toward potentially high-yield targets.
- **Transparency becomes a liability:** Many SLTT entities are compelled by statue to disclose a range of financial details. That can act as bait to ransomware gangs. How much cyber insurance does this organization have? Attackers can tailor their ransom demands accordingly.

"SLTTs are widely known to be attractive targets. They're often target-rich and resource-poor."

– **T.J. Sayers**, manager of the Cyber Threat Intelligence (CTI) team at the Multi-State and Elections Infrastructure Information Sharing and Analysis Centers (MS-ISAC and EI-ISAC)

The Solution: A Robust Strategy of Prevention and Remediation

SLTTs need a robust ransomware strategy. This may include:

- **End-user awareness:** End users can enable ransomware operations by clicking suspicious links or downloading emailed files that attackers then use to execute malicious code. User awareness is key, including training for all new hires and periodic refreshers that vary in frequency based on an end user's responsibilities.
- **Close the threat information gap:** New attack vectors and exploits are emerging all the time. SLTT technology leaders need to engage with information-sharing bodies to keep themselves abreast of the ever-changing threat landscape.
- **Security controls:** SLTTs should seek to implement basic security controls, network monitoring, and host-level detection and response capabilities. Another key best practice is logging: Maintaining event logs greatly increases an organization's ability to detect, respond to or recover from an attack. These logs should be exported to an out-of-bound location that's properly secured and not easily accessible; otherwise, attackers can delete logs during the attack, greatly inhibiting incident response.

Best Practices

Tailor training

Fine-tuning can help SLTTs derive maximum benefit from end-user training. Frequency matters: Depending on the size and complexity of the organization, some will do it on an annual basis, and others on a quarterly basis, Sayers said.

And it makes sense to tailor training by role. "Certain users have access to more sensitive information, for example, and those users may get the training more frequently than others who don't have as much access," Sayers said.

Secure external ports and services

Any number of ports and services within the IT infrastructure are accessible to threat actors. "We see remote desktop protocol or RDP used quite heavily," Sayers said. "The IT folks may be legitimately using these or other services for remote access into the network, but threat actors are looking to exploit that access."

Look at anything externally facing and ensure those are either closed if they're unnecessary or else secured with multifactor authentication and a strong, complex password.

Take patching seriously

Any time a vendor identifies a vulnerability, new attacks spring up. IT leaders and cyber defenders need to be vigilant in their patching.

"Bad actors look at the patch notes and try to reverse-engineer them. When patch notes or a vulnerability disclosure comes out, we see threat actors with working exploit code for that vulnerability within hours," Sayers said. "That means you need a vigorous, routine and timely patching schedule."

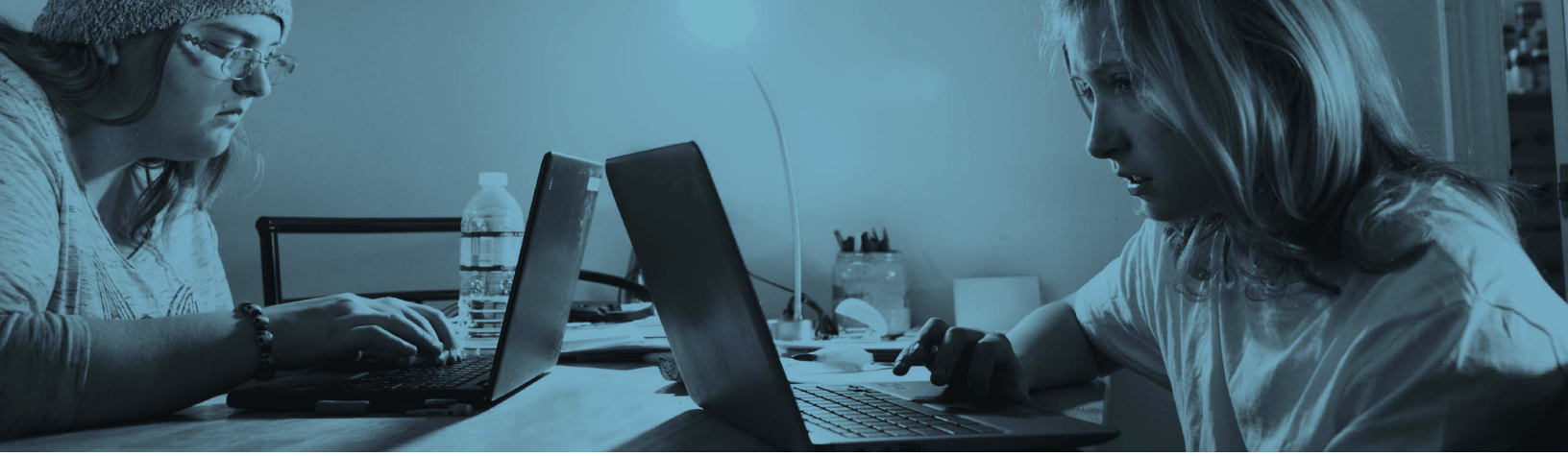
Double-down on backup

Backups need to be regularly tested and should be stored offline, and segmented from the larger IT environment.

"It can be extremely complex for an organization to have backups, but they are an absolute necessity when it comes to ransomware," Sayers said. "It's the single best thing to have in place if you do experience a ransomware incident — it's what gets you back up and on your operational feet quickest.

"We still see a lot of ransomware attacks begin with something as simple as a malicious email, trying to get the end user to click on a link or download a file."

– T.J. Sayers



Case Study: A K-12 Success Story

A K-12 school recognized the education sector was increasingly targeted during large student-focused operations, such as exam periods or back-to-school events. But there were challenges, including a limited IT team, and a lot of disparate infrastructure — specifically, the remote-education environment necessitated by the pandemic.

The IT team properly segmented the network, with a separate local area network for teachers and students. They implemented end-user training and regularly patched assets. They also ensured key defensive tools such as antivirus and network firewalls were in place, and stored offline backups and centralized logs out of bound from the rest of the network.

Ransomware actors were able to get in via a malicious email to a remote teacher, but were unable to quickly identify the high-value data they sought to ransom. The teacher subsequently notified the IT administrators of the odd email, and they were quickly able to identify how far and wide the attackers made it using the centralized logs. With the compromised network segment walled off from where backups and logs were stored, the school was able to quickly remediate impacted systems and restore from backups the small subset of systems impacted by the ransomware.

"Network segmentation was key. It meant the ransomware actors didn't have easy access to the backups and logs."

– T.J. Sayers

How CIS Helps

The MS-ISAC offers SLTTs intrusion detection, endpoint detection and response tools, as well as a 24/7/365 security operations center; with a team dedicated to incident response, forensic analysis and cyber threat intelligence. The CIS Critical Security Controls offer a prioritized set of actions to help fend off cyberattacks. The CIS Benchmarks offer best-practice security configurations developed by government, business industry and academia experts.

govloop

CIS Center for Internet Security®