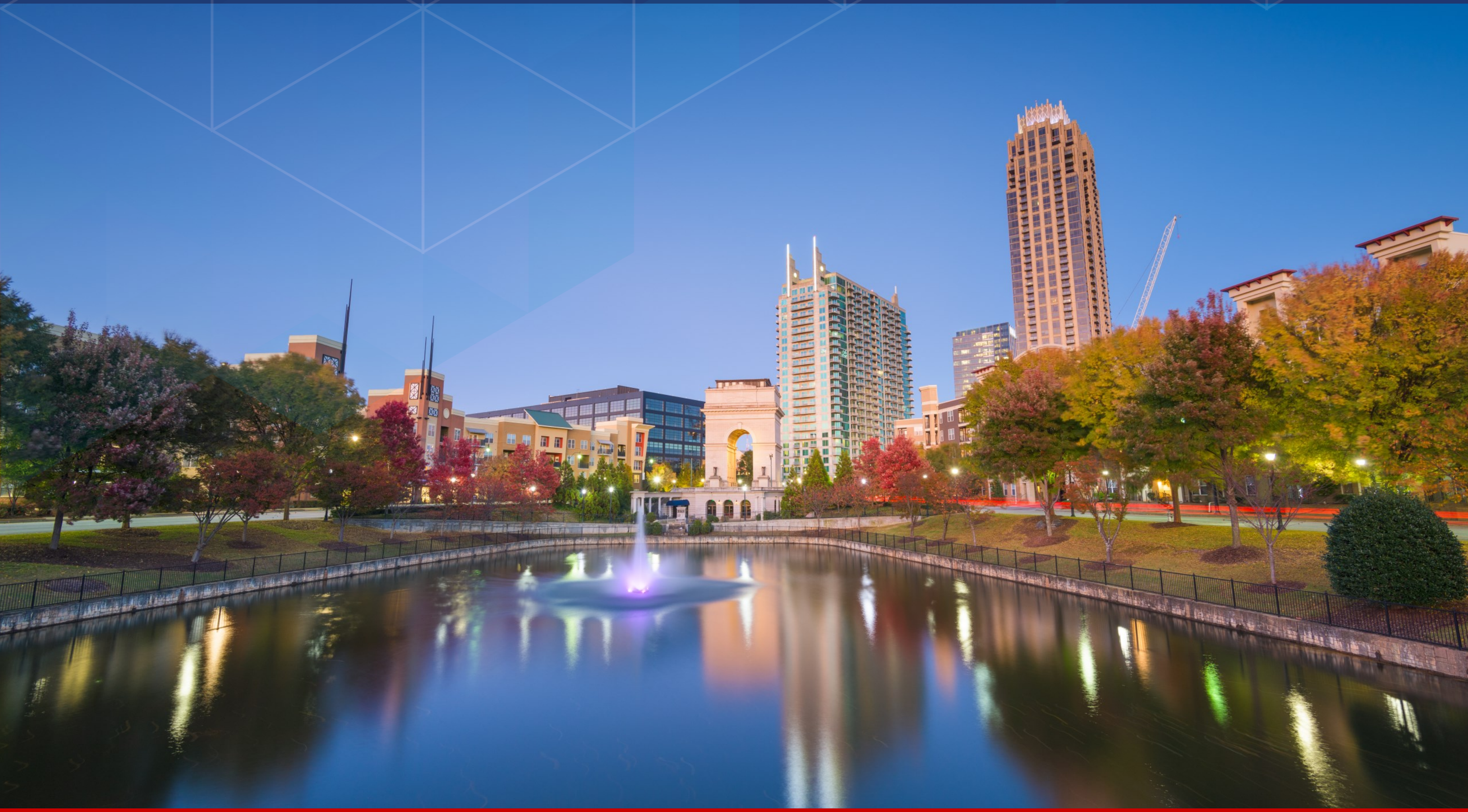
Preventing Ransomware: Strategies for Government

Learn strategies to protect cities, school, and emergency response agencies from ransomware attacks



844.638.7328 | SALES@SECNAP.COM | SECNAP.COM

SECNAP
NETWORK SECURITY

The State of Municipal Government Cybersecurity

Local governments, like schools and hospitals, are particularly enticing targets due to the lack the resources against cyberattacks. From 2019-2020, over 200 local and county governments were victims of Ransomware. Billions of dollars have been paid worldwide in system cleanup and data recovery costs from ransomware attacks.

Notable examples of ransomware attacks that year included:

- **Everything is bigger in Texas, including ransomware attacks.** A coordinated attack that simultaneously paralyzed the functionality of 22 cities and towns in Texas, most of them rural. Critical city services, such as utility payment systems and the printing of identity documents, were knocked offline. The hackers demanded a collective $2.5 million in ransom, which the cities refused to pay.

- **Riviera Beach wasn't too small to get hit.** An attack against the small city of Riviera Beach, Florida (pop. 35,000) took city services and infrastructure offline, including email, some phones, and water utility pump stations. The city paid the nearly $600,000 ransom to regain access and control.

- **Lake City's cyber insurance paid but not all files were restored.** Less than a week after the Riviera Beach attack, the City of Lake City, Florida, agreed to pay a nearly half-million-dollar ransom to the same hacker group; at the time the city voted to pay the ransom, its computer systems had been locked for two weeks.

- **Delaware County took months to detect Ransomware.** In November 2020, Delaware County in Pennsylvania agreed to pay $500,000 in ransom to have gigabytes of data released back to it. It took two months to realize an email with ransomware had infiltrated its system.

Warnings and Predictions

In March 2022, we were warned that Russian cyberattacks on U.S. targets were likely. Security experts told Government Technology magazine that they not only expect ransomware to continue vexing local governments but that the attacks will also evolve and become even more targeted and sophisticated.

Ransom Recap

$570,857
Average Demand

$45.1 Million
Total Demands*

* comparitech.com/blog/information-security/government-ransomware-attacks/

V22

Local Governments are Attractive Ransomware Targets

Hackers like ransomware because attacks require little technical expertise to launch -- cybercriminals who don’t know how to code can even buy “ransomware-as-a-service” packages -- and the payday comes much more swiftly than with data breaches, where hackers must first exfiltrate data, then find a willing buyer.

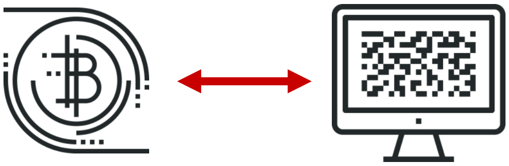
Early ransomware attacks targeted very large enterprises with deep pockets; in response, these organizations hardened their cybersecurity defenses. Now, cybercriminals are heavily targeting budget-strained municipal governments and small and medium-sized businesses (SMB) in the private sector, especially healthcare facilities. Hackers view these organizations as soft targets that lack the resources to prevent, defend against, or remediate cyberattacks, and are thus more likely to pay the ransom than federal government agencies or large private-sector organizations.

Indeed, small municipalities struggle with severe budget limitations, inadequate IT staffing levels, and a lack of in-house security expertise; most states dedicate less than 3% of their IT budgets to cybersecurity, as opposed to more than 10% in the private sector. Budgetary constraints also preclude many municipalities from replacing antiquated legacy equipment and customized systems that are extremely difficult to maintain and secure.

Another factor that puts municipalities at risk is the criticality of their IT systems. Similar to healthcare IT systems, city government systems impact the health, welfare, and even lives of the citizens in the area they serve. This gives municipalities extra incentive to simply pay whatever hackers are demanding to get these mission-critical systems back online as soon as possible. The CARES stimulus bill, passed in March 2020 in response to the COVID-19 pandemic, will likely exacerbate the situation. Knowing that local governments and healthcare facilities are about to get an influx of cash, hackers have added incentive to target those sectors.

Ransom: To pay or not to pay?

Cybersecurity experts and law enforcement professionals strongly advise organizations not to give in to ransomware demands. Doing so only encourages future attacks, and there is no guarantee that hackers will send decryption keys as promised; about 20% of organizations that pay up do not regain access to their data and systems.



Paying the ransom does not guarantee the files will be unlocked.

However, nonpayment has its own risks. The City of Baltimore refused to pay a $76,000 ransom, but incurred over $18 million in system remediation costs and lost revenue. The City of Atlanta spent over $17 million in lieu of paying a $51,000 ransom. Additionally, some hackers are publishing data stolen from organizations that don’t pay on public websites. After a medical research firm working on a COVID-19 vaccine refused to pay a ransom demand, hackers released sensitive information belonging to vaccine trial volunteers, including proof of identification, their medical records, and a list of the vaccination studies in which they had participated.

Proactive Strategies for Risk Reduction

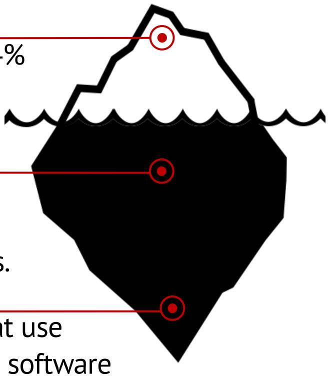
The best protection against ransomware is to take a layered approach that combines proactive security initiatives and technologies to prevent attacks from happening in the first place.

Security Awareness Training

Employees are the weakest link in the cybersecurity chain, and even the most robust security technologies fall short if an employee clicks on a phishing link they receive through email. Since most ransomware attacks can be traced back to a successful phishing attack, local governments must ensure that employees are trained to recognize phishing and other forms of social engineering when accessing company or personal email.

Security awareness training doesn't mean having employees sit through a PowerPoint presentation during onboarding. It's a continuing education process that includes, among other things, simulated but realistic-looking "phishing attacks" to test employees' awareness and knowledge.

90%
of breaches are caused by human error.*



Surface Web makes up less than 4% of content on the internet and is indexed by search engines.

Deep Web makes up 90% of the information on the internet. Sites are not accessible by web crawlers.

Dark Web consist of websites that use public internet but require specific software to access to ensure anonymity.

Dark Web Monitoring

The overwhelming majority of data breaches can be traced back to stolen passwords. However, victims of data breaches are usually the last ones to know that their credentials have been compromised. Dark web monitoring services continually scan the dark web and alert enterprises if employee credentials are found on hacker forums, so that stolen passwords can be changed immediately.

Security Assessments

Network security assessments should be performed at periodic intervals, as well as whenever a major change is made to a network. Some compliance standards, including NIST, HIPAA, and PCI DSS, mandate these assessments. The two primary assessment types are penetration tests and vulnerability scans.

In a penetration test, a security expert simulates the actions of a hacker, attempting to break into a network or application to determine if its security features can be defeated. Conversely, a vulnerability scan is automated, although a human reviews the results. The purpose of a vulnerability scan is to identify and report on security vulnerabilities, not attempt to defeat security defenses.

At a minimum, penetration tests should be performed annually, and vulnerability scans should be run quarterly. However, there are many circumstances under which more frequent scans are warranted.

* Willis Towers Watson

Managed SIEM Solutions

Security incident and event management (SIEM) solutions collect and analyze activity from many different resources across an organization's IT infrastructure, including network devices, servers, and domain controllers, then generate reporting and alerts about security incidents.

Sometimes, resource-strapped SMBs and municipalities subscribe to SIEM services only, without the benefit of a qualified security operations center (SOC) to manage the SIEM, analyze its output, and respond to threats.

While doing without a SOC might seem like a valid cost avoidance strategy, organizations quickly realize this sets them up for failure.

SIEM Functionality

- Active Directory Monitoring
- Threat Hunting
- Real-time Data Analysis
- Data collection & Storage
- Searchable Reporting
- Forensic Capabilities
- Identification of Devices

Common Pitfalls of a SIEM Only Solution

SIEMs only provide reporting and alerts about potential threats.

Without a SOC, it's up to the organization to respond to and protect their network. Usually, organizations that lack the money to outsource SIEM monitoring and response to a SOC also lack the staff to respond to threats.

Alert fatigue is real.

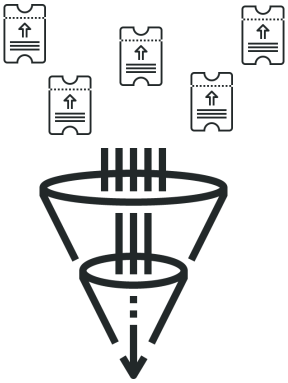
SIEMs generate an extraordinary number of alerts; the average organization receives 10,000 alerts a day, and particularly "noisy" networks can generate over 150,000 alerts. Human analysts are unable to keep up, alert fatigue sets in, and actual threats are allowed network entry.

SMBs and municipalities should avoid "bargain" SIEM-only services and ensure that their SIEM services are tied to a SOC that is staffed by experienced security analysts 24/7. The SIEM should also be paired with MDR services.

Managed Detection & Response (MDR) Services

While SIEM solutions are quite useful for data aggregation, they aren't standalone tools. Alert fatigue is an issue even in SOCs staffed by highly experienced analysts. SIEMs also cannot flag every possible threat; in addition to generating many false positives, SIEMs occasionally produce false negatives.

Managed detection and response (MDR) services address these problems by deploying additional security technologies that feed data into the SOC together with the SIEM alert stream to create an enhanced view into potential activities of malicious intruders in the network. This filters out the majority of false positives, reducing alert fatigue, while flagging false negatives that would otherwise slip through the cracks.



Let Security Experts Filter Through Alerts

The technologies that make up an MDR service include:

An intrusion detection system (IDS) analyzes network traffic flows, comparing activity to a threat database to detect the warning signs of known cyber threats. An IDS is a monitoring and detection tool that works in tandem with an IPS.

An intrusion prevention system (IPS) proactively blocks potentially malicious activity by conducting deep packet inspection, then denying network traffic that fits the profile of a known security threat.

Internal threat detection (ITD) tools are designed to simulate legitimate services, such as servers and file shares, to attract and detect unauthorized access.

Lateral threat detection (LTD) tools enable security analysts to detect hackers who have managed to penetrate the network perimeter and are moving progressively through it.

Deployed together, integrated with a SIEM, and scrutinized with software analytics, these combined technologies eliminate many false-positives, and then transmit the remaining security events into the SOC. At that point, highly-trained security engineers take over, analyze the incoming data stream, and immediately respond to the most important alerts.

Regular System Backups

The ability to restore critical systems and data from backups is essential to recovering from a ransomware attack. However, since new-gen ransomware strains seek to destroy backups, it's critical to set them up properly. Secure backups use a separate authentication system with different passwords, and utilize at least two different backup methods, with one stored at a different location.

Cloud-based services are a popular choice for offsite backup repositories. However, cloud security settings can be tricky, and it is critical that cloud services are configured properly. Misconfigured cloud servers are responsible for a large and growing number of breaches; the Capital One breach was caused by a cloud misconfiguration. Municipalities that do not have cloud computing professionals on staff should outsource this function to a company that specializes in cloud services.

Solid Backups Mitigate The Impact of Ransomware

- Keep an offline backup
- Keep an offsite backup
- Use unique authentication
- Limit Privileges
- Increase the data backup frequency
- Automate testing to the integrity of all backups
- Segment the network to protect against easy lateral movement
- Use immutable backups

Limit Cyberattack Damage and Reduce Scope of Compliance

Network Segmentation

Network segmentation involves splitting a larger network into smaller segments using firewalls, virtual LANs, and other techniques. Networks can be segmented by function, such as separating constituent-facing services from internal services, or data type, which is commonly used to separate sensitive or regulated data from non-regulated data.

While network segmentation doesn't prevent cyberattacks from happening, it protects against lateral movement across a network by ransomware or human intruders. The more virtual barriers a ransomware infection or an intruder must overcome, the more difficult it will be for them to move around.

Key Takeaways and Conclusion

If expertly deployed, managed, and monitored, SIEM and MDR solutions work to detect ransomware, malware, and other advanced persistent threats (APTs), stop hackers from infiltrating the network, and protect the network against both external and insider threats. Since it is impossible to prevent all cyberattacks, these technologies must be paired with proper backups and network segmentation so that organizations can contain attacks and restore systems and data in the event of a successful ransomware attack. Additionally, since the cyber threat environment changes literally daily, appropriate and ongoing network security assessments are necessary to ensure that organizations are protected from new and emerging threats.

These security solutions are not overly expensive; they certainly cost less than remediating systems after a cyberattack.

However, security technology is only as good as the humans operating it. Without a team of security analysts who are trained to use the tools to detect and respond to attacks, security hardware and software just ends up costing organizations money while doing nothing to protect their systems.

The federal government recognizes that a fully implemented cyber security network protection plan is generally beyond the resources of small municipalities and recommends that communities combine and/or outsource this activity to managed security service providers (MSSPs) with expertise in working with SMBs and municipal governments.

Question for Leadership

If cybersecurity does not make the 2023 budget, what will happen when a ransom demand hits your organization?

Ransomware Attacks on US Government Organizations Cost $18.9bn in 2020

* comparitech.com/blog/information-security/government-ransomware-attacks/

SECNAP
NETWORK SECURITY

Get a complimentary and customized consultation regarding your organization’s cybersecurity strategy.

About SECNAP Network Security

SECNAP's mission is to help our clients' achieve a secure posture while keeping expenses and internal IT effort minimum. Our managed and monitored platform, CloudJacket XDR, combines ongoing network security assessments, managed detection and response (MDR) services, patented intrusion detection and prevention system (IDS/IPS), security information and event management (SIEM) solution, and an integrated endpoint agent.

CloudJacket XDR is a proactively managed cybersecurity service powered by patented technology. Our intelligence engines create a data stream to populate a proprietary dashboard that empowers our U.S.-based security operations centers (SOCs) analysts to combine machine intelligence with human analysis and action. CloudJacketX leverages multiple layers of detection and protection, utilizing a continuous learning and feedback process. Our concierge approach allows analys to tune the alert stream while understanding client network organizational requirements, unique conditions, and patterns. Our platform cures your team of alert fatigue, minimizing the involvement of your IT team to just minutes a day.

With Cloudjacket XDR, businesses quickly implement a unified stack of cybersecurity technology managed by a highly-experienced cybersecurity team at a fraction of the cost.

AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations

GSA Advantage!