Rising Threats

Why ISPs must act now to protect against cyber attacks.

Jason Malmquist

Dec. 26, 2024

- 

Why ISPs must act now to protect against cyber attacks.

The recent ransomware attack on Frontier Communications serves as a critical reminder for Internet Service Providers (ISPs) of the escalating cyber threats pervading the landscape. As cyber attacks continue to rise in frequency and sophistication, it is no longer a question of whether ISPs will be targeted, but when.

Unfortunately, many ISPs remain dangerously unprepared. Instead, the focus on network expansion, spurred by the Broadband, Equity, Access & Deployment (BEAD) initiative, private equity, and M&A activity has prompted ISPs to prioritize building infrastructure and growing their customer base. As important as that may be, it leaves gaps in cyber security measures, leaving networks vulnerable to increasingly bold and organized cyber criminals.

Cyber security isn't just a checklist of tools and protocols; it’s a culture that must permeate every level of an organization. This culture ensures that all employees, from those in the engineering department to those in customer service, understand the critical importance of security in their day-to-day roles. The Frontier incident is a wake-up call, especially for smaller providers, who often would lack the resources to recover from a debilitating breach.

> *…many breaches occur because of simple mistakes: a misconfiguration, a lost device, or an employee falling for a phishing email or mobile phone scam. This underscores the need for continuous training and reinforcement of security best practices.*

The Culture of Security: A Balancing Act

To secure a network, ISPs need to create a culture of cyber security awareness and vigilance. This means training employees continuously and embedding security protocols into every aspect of the business. It's an ongoing process; cyber security isn't a "set it and forget it" task. It's about ensuring that employees are equipped with the knowledge and tools to stop attacks before they turn into full-blown crises. As with disaster recovery, the goal here is prevention: stopping problems at the front door rather than finding them upstairs, after the damage is done.

Building this culture requires balancing security measures with the needs of the workforce. For example, engineers often want flexibility, like having administrative access to their local systems. All well and good, but unchecked access can create vulnerabilities. Therefore, ISPs must find a way to balance the operational needs of employees with stringent security protocols.

If employees cannot do their jobs efficiently, it negatively impacts customers. At the same time, if security isn't taken seriously, a breach can bring the entire operation down.

The Reality of Cyber Threats

Today's cyber threats extend far beyond simple viruses or malware. Using well-coordinated attacks, cyber criminals now operate like professional organizations, with the resources and expertise to penetrate even the most secure networks. These groups often target critical infrastructure, knowing that the disruption of internet services impacts both businesses and consumers.

Human error also comes into play; it is a significant vulnerability. According to the 2024 Verizon Data Breach Report, many breaches occur because of simple mistakes: a misconfiguration, a lost device, or an employee falling for a phishing email or mobile phone scam. This underscores the need for continuous training and reinforcement of security best practices. Employees are the first line of defense, and without the right training, even the most advanced security systems can be infiltrated.

Smaller ISPs, especially those in rural or underserved areas, are at special risk. Regional telcos often lack the IT staff and resources to mount a robust defense, making them attractive targets for cyber criminals seeking the path of least resistance.

Common Cyber Threats Facing ISPs

Cyber criminals deploy a variety of tactics to breach ISP networks, often combining multiple methods in sophisticated attacks:

Ransomware Attacks: Cyber criminals infiltrate networks, encrypt critical data, and demand a ransom for its release. What may begin with a seemingly minor compromise, such as a hacked email account, can quickly escalate into full-scale network outages. According to industry reports, $449.1 million was paid to ransomware groups in the first half of 2023 alone.

Data Theft: In addition to encrypting data, attackers often steal sensitive information and threaten to release it unless a ransom is paid. The pressure to comply is intense but paying a ransom not only funds further criminal activity but also fails to guarantee the safe return of stolen data.

Phishing and Social Engineering: A leading cause of cyber security breaches, cyber criminals craft convincing emails or messages designed to trick employees into clicking malicious links or sharing sensitive information, thus granting attackers access to the network.

Measures to Protect Against Cyber attacks

To combat these evolving threats, ISPs must implement a robust cyber security strategy. The following measures are essential for protecting networks and customer data:

Multi-Factor Authentication (MFA): MFA requires users to verify their identity using multiple methods, significantly reducing the risk of unauthorized access even if log in credentials are compromised.

Endpoint Detection and Response (EDR): Advanced EDR tools leverage artificial intelligence to detect and respond to suspicious network activity in real time, stopping threats before they escalate.

Security Operations Center (SOC): A SOC provides 24/7 monitoring of network activities, enabling immediate responses to potential security breaches. ISPs should consider having a U.S.-based SOC to meet local regulatory requirements.

Employee Training: Human error is a chief cause of cyber attacks. Regular, comprehensive training on recognizing phishing attempts and understanding cyber security protocols is critical. Conducting phishing simulations can further strengthen employee awareness.

Incident Response Plan: Every ISP must have a well-developed incident response plan, outlining the steps to take during a cyber attack. This plan should include immediate shutdown procedures, communication strategies, and recovery protocols to minimize damage.

Advanced Network Security Tools: Leveraging AI-driven security tools can help ISPs detect and block emerging threats. Regular security assessments ensure that defenses are updated to meet new challenges.

Secure Access Controls: Implementing strict access controls, including network segmentation and role-based permissions, helps limit the impact of a breach by containing the spread of an attack.

> *ISPs must find a way to balance the operational needs of employees with stringent security protocols.*

Cyber Resiliency and the Importance of Backups

Cyber resiliency is key to surviving and thriving in the face of cyber threats. At its core, cyber resiliency is the ability to quickly recover from an attack, and that's where backups play a critical role. A strong backup system ensures that essential data can be restored swiftly, minimizing downtime and reducing the impact of the breach.

However, backups alone are not enough. Cyber resiliency also requires a proactive incident response plan that contains damage and accelerates recovery. Integrating robust backups with a well-coordinated disaster recovery strategy is essential to ensuring business continuity and protecting against costly interruptions.

The Intersection of Response and Prevention

Cyber security is unique in that any failure is seen as negligence. If an attack happens, it means the right protections were not in place. This is why it is critical to have systems that catch threats before they evolve into full-scale breaches. Just like airbags and seat belts in a car, multiple layers of security can help prevent a total disaster.

The key is not just having tools, but ensuring that the entire organization—from executives to frontline employees—understands the importance of cyber security. It's an ecosystem that requires constant attention and updates. ISPs must continuously monitor, train, and invest in cyber security to stay ahead of evolving threats.

Act Now or Face the Consequences

The time to act is now. The Frontier ransomware attack was a warning, and the next target could be you. A lax approach to security can lead to catastrophic consequences, especially for smaller providers with limited resources. Building a culture of security, investing in employee training, and implementing a robust disaster recovery plan are not just best practices—they are essential for survival in today's digital landscape.

About the Author

Jason Malmquist
EVP Software & IT, CHR Solutions

Jason Malmquist is EVP Software & IT at CHR Solutions. As Head of CHR's Software and IT portfolios, Jason is responsible for overseeing the adoption of technology, development, business processes and workflows, software implementation, and the continuing support for software and IT clients. With over 25 years of telecommunications and sales leadership experience, he is committed to driving client satisfaction and fostering a partnership culture.

Jason joined CHR Solutions (formerly Martin Group) in 2005 as a Regional Sales Manager, later advancing to Head of Sales and ultimately to his current role. Prior to that, he held sales and sales leadership roles at Eftia OSS Solutions, Simplified Development, and Aerotek's Telecommunications Division. Jason holds a Business degree from Stephen F. Austin, majoring in Marketing and Accounting. For more information, visit www.chrsolutions.com. Follow Jason on LinkedIn. Follow CHR on LinkedIn, Facebook and X @CHRSolutions.

Show more