www.pipelinepub.com
Volume 21, Issue 1

Cyber Attacks are Rampant: Here’s What ISPs Can Do to Stop Them from Happening

By: Jason Malmquist

Cyberattacks are increasingly more sophisticated and frequent, and they are posing significant threats to Internet Service Providers (ISPs). The critical infrastructure managed by ISPs makes them prime targets for cybercriminals seeking to disrupt services, steal sensitive data, or extort money through ransomware attacks. In the first six months of 2023 alone, $449.1 million was paid to ransomware groups. The bottom line is that cyberattacks are having a profound impact on business.

Unfortunately, regional telcos and ISPs often have limited resources or the requisite IT staff to combat this scourge, and cybercriminals know it, which explains why they attack the low hanging fruit easily. They choose the path of least resistance and target their victims carefully. The results are serious service outages or DDoS (Denial of Service) attacks that impact business and customers alike.

Drawing insights from CHR Solutions' white paper on cybersecurity, this article explores the measures ISPs can take to prevent cyberattacks and safeguard their networks and customer data.

The Reality of Cyber Threats

Cybersecurity threats have evolved beyond simple viruses and malware. Today, ISPs face complex and persistent threats from highly organized cybercriminal groups who operate as professional entities, often working from sophisticated offices, not basements. They possess the expertise to infiltrate even the most secure networks.

According to the 2024 Verizon Data Breach Report, one of the ways cybercriminals work is by relying on human error — the leading factor in breaches. Simple mistakes, such as misconfigurations, lost devices, or unintentional data exposure, can open the door for cybercriminals to exploit a company’s vulnerabilities. For instance, a well-crafted phishing email disguised as a message from a trusted colleague might lure an employee into clicking a malicious link, unknowingly granting hackers access to the company's network. Other phishing attacks might involve fake alerts about account suspensions, prompting victims to enter their credentials on a fraudulent site. This highlights the importance of not only maintaining technological defenses but also providing frequent and comprehensive training and awareness programs for employees.

Common Cyber Threats Facing ISPs

Ransomware Attacks: These attacks involve cybercriminals infiltrating a network, encrypting data, and demanding a ransom for its release. What may start as seemingly harmless actions, such as a compromised email account with notifications of logins from unfamiliar locations or devices, can quickly escalate into full-scale network breaches with devastating consequences.

Data Theft: Beyond encryption, attackers also exfiltrate sensitive customer and operational data, threatening to release it unless a ransom is paid. The dual threat of encryption and data theft places immense pressure on ISPs to comply with cyber criminals' demands, though paying ransom is strongly discouraged as it funds further criminal activity and does not guarantee data recovery.

Phishing and Social Engineering: Cyber criminals often use deceptive emails and social engineering tactics (manipulative techniques used by attackers to get individuals to divulge confidential information) to gain access to networks. Employees unknowingly clicking on malicious links or providing sensitive information can give attackers the foothold they need to infiltrate systems.

Measures to Protect Against Cyberattacks

To mitigate these threats, ISPs must implement a multi-faceted cybersecurity strategy that includes the following measures:

Security Operations Center (SOC): A SOC provides continuous monitoring of network activities, looking for signs of unauthorized access or suspicious behavior. It's essential to monitor the creation of high-level user accounts by having a security team monitor it at all times. This allows for immediate response to potential threats, minimizing the impact of any breach or shutting down the access before their planned day and time of attack. Having a U.S.-based SOC can be advantageous due to specific regulatory requirements and the need for localized response capabilities.

Incident Response Plan: ISPs must have a comprehensive incident response plan in place. This plan should outline the steps to be taken in the event of a cyberattack, including immediate shutdown procedures, communication strategies, and recovery protocols. Having a third-party expert assist in developing and implementing this plan is invaluable. CHR Solutions emphasizes the importance of disaster recovery planning to ensure quick restoration of operations and minimize downtime in the event of a cyberattack. Additionally, having action and communication plans for "suspected" incidents or suspicious activity is crucial. While having a comprehensive response plan for a full-scale attack is important, preventing such a scenario requires early detection. ISPs must be able to identify warning signs and have escalation and containment protocols in place to address these issues before they evolve into a full-blown attacks.

Secure Access Controls: Implementing strict access controls ensures that only authorized personnel can access sensitive parts of the network. This includes using role-based access controls, regularly updating access permissions, and auditing access logs to detect any unauthorized attempts. Network segmentation, another key recommendation from CHR Solutions, limits the spread of an attack and protects critical assets.

The Importance of Resilience

In an era of rampant cyberattacks, ISPs must prioritize cybersecurity to protect their networks and customer data. Implementing robust security measures, educating employees, and having a solid incident response plan are essential. Lax cybersecurity is a major issue, especially for regional telcos and ISPs with limited resources. Waiting to act is not an option; it will be costly and overburden IT staff, at a minimum. ISPs cannot underestimate the destruction that could be done to their business when a cyberattack hits. Strengthening IT teams or partnering with cybersecurity experts is crucial. The warning light is flashing for local telcos and ISPs. The time to act is now.