From Risk to Resilience: Penetration Testing in Broadband Networks

Identifying Vulnerabilities, Simulating Attacks, and Strengthening Your Network Against Evolving Threats

TABLE OF CONTENTS

INTRODUCTION

Like electricity and water, broadband is now considered critical infrastructure, powering essential services. This emphasis and attention is what makes broadband providers targets for cyberattacks, from ransomware and network invasions. The smallest vulnerability can disrupt service, expose subscriber data, and damage a provider's reputation.

Penetration testing (pen testing) is a proactive way to uncover weaknesses before attackers can find and use them. Pen testing simulates real attacks in a controlled environment giving providers insight into their network defenses and the strength of their security. A pen test will also satisfy regulatory requirements when needed.

WHY PEN TESTING MATTERS FOR BROADBAND PROVIDERS

Penetration testing is a controlled, deliberate cyberattack designed to evaluate the security of a network of system. Pen testing goes beyond the vulnerability scans. While traditional scans highlight weaknesses, they don't demonstrate whether those weaknesses can be exploited. Pen testing mimics real world attacks by using the tactics and methods of attackers and provides analysis of the network's security and where defenses fall short. The goal is to provide a comprehensive understanding of where an organization's defenses may be lacking, and how resilient its network is against cyber threats. These simulated attacks reveal the network response when under the pressure of an attack, exposing any gaps in detection, response, or mitigation.

Demonstrating vigorous cybersecurity practices also strengthens subscriber trust and satisfies the regulatory requirements in some funding programs, such as those in the BEAD and tribal cybersecurity programs. These assessments are particularly valuable in identifying exposure to high profile risks such as ransomware, business email compromise, and fraud, with ransomware often being the foremost concern for organizations across industries.

Simulated external network testing determines threats from outside the organization, while internal testing simulates attacks from within, whether from employees or compromised devices. Applications that manage subscribers and network services are tested for vulnerabilities, along with wireless networks and physical devices, including routers and CMTSs. This demonstrates to providers how both device and human factors could be exploited, so these weaknesses are addressed before they are used by attackers.

REASONS FOR CONDUCTING A PENETRATION TEST

Compliance Requirements

Organizations perform penetration tests for a variety of critical reasons. Compliance is often the primary driver. Many industries impose strict regulatory requirements mandating regular penetration testing. Compliance with standards such as PCI DSS, HIPAA, and GDPR not only enhances an organization's security posture but also mitigates legal, financial, and reputational risks associated with data breaches. Regular testing ensures that security controls remain effective, helping businesses stay ahead of evolving threats and regulatory obligations.

Similarly, for organizations pursuing federal funding, such as the Broadband Equity, Access, and Deployment (BEAD) program, adherence to security requirements often necessitates documented testing. Beyond regulatory compliance, contractual obligations with partners, particularly B2B partners, may require proof of regular security evaluations. Demonstrating that these assessments have been conducted can fulfill contract requirements and reassure partners that sensitive information and operations are protected.

Cyber Insurance

Cyber insurance providers are increasingly mandating documented penetration tests as a prerequisite for coverage. By providing reports from completed tests, organizations can demonstrate that they are actively managing cybersecurity risks. These assessments serve as proof of due diligence, demonstrating an organization's commitment to proactive cybersecurity measures. A well conducted pentest can directly impact policy eligibility, premium costs, coverage terms, and overall risk evaluation, helping businesses secure more favorable insurance conditions while strengthening their security posture.

Ethical Responsibility

Beyond regulatory and contractual requirements, organizations have a fundamental responsibility to safeguard sensitive information and to perform penetration tests simply because it is the right thing to do. Customers, partners, and other stakeholders expect their information to be protected. In the broadband industry, where providers support a chain of downstream services, a security compromise can have cascading effects, potentially disrupting the services customers rely on. Performing regular penetration testing helps ensure these obligations are met, reinforcing trust and demonstrating commitment to cybersecurity best practices.

Supply Chains

Supply chain security has also become significant, recognizing that vulnerabilities in partner systems, third party applications, or shared infrastructure can compromise overall service deliver. Effective penetration testing evaluates not only an organization's internal environment but also the external dependencies and systems that are interconnected.

WHAT MAKES A GOOD PENETRATION TEST?

Not all penetration tests are created equal. An effective test is built on several key principles that ensure the results are actionable and relevant to today's threats.

First, a penetration test must be comprehensive. It should evaluate the full scope of an organization's environment, including networks, systems, applications, and human factors. For organizations that have never conducted a penetration test, this broad approach is essential to gain a clear picture of the potential risks and to prioritize mitigation efforts. While some broadband operators may feel that automated phishing simulations or other occasional tools are sufficient, experience shows that these methods often fail to capture real world risks.

Automated templates are easily recognized over time, and employees become desensitized to repeated alerts. But targeted phishing and SMS based social engineering tests that are executed as part of a thorough penetration test can still identify vulnerabilities that automated tools miss. Regularly testing human factors is critical, even if there are existing security awareness programs.

Equally important is the use of real world attack simulations. A high quality penetration test should go beyond automated scanning and scripted scenarios. Skilled testers emulate the tactics, techniques, and procedures used by today's threat actors, including ransomware gangs, fraudsters, and other malicious groups. Understanding the approach a provider takes is vital. Are they relying primarily on software, or are they applying manual methods to replicate authentic attack behavior? In one notable example, a operator who engaged a provider was told no vulnerabilities existed because the automated tools failed to detect any issues. Yet when a penetration test using real world simulations was performed, multiple potential vulnerabilities were uncovered, even in what was considered a highly secure environment. This underscores the importance of choosing testers who are experienced, methodical, and capable of simulating realistic threats.

Actionable insights are another hallmark of a quality penetration test. Findings should never be presented as a simple list of vulnerabilities. Every discovery should be accompanied by clear remediation steps. Reports should provide detailed explanations of what was found, where it was found, and how it was identified. Screenshots, tool descriptions, and step by step techniques are important to help organizations understand and address their risks. When evaluating a penetration test provider, request a sample report that reveals whether manual, in depth work is included, or if the assessment relies solely on automated results.

In addition to highlighting areas for improvement, penetration tests should identify positive observations. Many organizations have already invested in security controls, training programs, and software tools. Reporting on what is working not only validates those investments but also allows management teams to recognize the practices that are working. Positive findings can include blocked or mitigated attacks, properly configured systems, and staff responses that demonstrate adherence to the protocols. By including both successes and areas for improvement, penetration test reports provide a balanced, constructive perspective that strengthens the organization's overall security.

Finally, retesting is an important component of an effective security strategy. While some penetration tests may not include retesting, it is highly recommended as an option. Once vulnerabilities are addressed, retesting confirms that remediation efforts were successful and that no residual weaknesses remain. This ensures that improvements are valid and allows organizations to maintain a continuous cycle of security evaluation and improvement.

THE TESTING PROCESS

Pen testing is a multistep assessment designed to simulate real world attacks safely. It begins with planning, where providers and testers define the assets included, the depth of testing, and acceptable risk levels. Legal and compliance boundaries are established, and critical infrastructure such as CMTS, OLTs, core routers, and subscriber portals are identified for focused testing.

Pen testers use a combination of open source and commercial tools for thorough testing. Open source tools can expose overlooked vulnerabilities, while commercial solutions provide advanced automation and reporting. Frameworks such as Metasploit, Nmap, and Wireshark are comprehensive platforms used for penetration testing and exploit development. For example, Metasploit provides scanning and packet analysis capabilities. Commercial solutions like Core Impact, Nessus, and Burp Suite allow for advanced exploitation and reporting.

Broadband specific tools are used in testing DOCSIS, GPON, MoCA, and G.hn networks. These specialized tools allow testers to emulate real subscriber behavior and network traffic, revealing weaknesses that generic tools might miss. Scripts written in Python or other languages automate complex testing scenarios, such as simulating traffic patterns or attempting credential brute forcing. For instance, a script may simulate a burst of traffic from multiple compromised subscriber devices to see if network congestion or throttling triggers any security alerts.

Advanced Threat Techniques and Human Factor Testing

Vulnerability Identification

To start the process, intelligence on the network is gathered. Passive reconnaissance collects publicly available information, while active reconnaissance probes devices, establishes all the open ports, and fingerprints services to identify vulnerabilities. In broadband networks, this includes mapping the physical arrangement of how devices and nodes in a network are connected from headend equipment to subscriber devices. This may also include domain registration data, IP address ranges, or open ports on subscriber facing systems, which could be entry points if not properly secured.

Vulnerability identification follows, combining automated tools and manual techniques. Scanners detect missing patches and incorrect configurations, while skilled human testers probe flaws, particularly in vendor hardware and custom configurations. Pen testers then plot potential paths of attack from outside the network, scanning for open ports and outdated versions of software. This helps providers understand not only what could be exploited, but the flow or chain an attacker might follow to reach the critical systems.

Simulating Realistic Attack Paths

The next phase is exploitation, where testers actually simulate attacks to determine if the identified vulnerabilities can be used to gain access, take over privileges, or move laterally through the network. Exploitation can target administrative portals, misconfigured subscriber devices like routers, weak authentication, or firmware vulnerabilities. Inside the network lateral movement is tested, simulating access from compromised customer equipment to core systems. Testing might show that weak default credentials on a subscriber gateway could allow lateral movement to internal management systems if combined with an unpatched CMTS. Wireless networks and access points are evaluated for weak encryption or misconfiguration, while social engineering may also be employed to test personnel awareness.

Multi Vector Threat Simulation

Modern attacks are rarely single vector. Advanced pen tests simulate multi vector attacks, combining exploitations across several network devices, applications, and human touchpoints. For example, testers might try and compromise a subscriber portal while monitoring traffic for weaknesses in a CMTS or OLT, assessing detection and response capabilities in both areas. Simulating these multivector attacks ensures that defenses aren't just tested in isolation but can combat coordinated, real-world threats that combine device, network, and human elements.

Assessing Impact and Mitigation

The post exploitation phase shows just how far a breach could reach. Are attackers able to get into subscriber data or critical network systems? Pen testing turns these findings into recommendations and prioritizes them by severity. Estimations of the possible impact, such as how many subscribers could lose service or what data would be exposed, provides a clear picture of risks and prioritizes fixes.

Retesting then confirms that the vulnerabilities have been effectively closed. For more advanced assessments, red team exercises mimic prolonged attacks, testing both network defenses and incident response readiness in real time. Pen testers don't just find weaknesses, they measure their potential impact and rank them based on ease of access and potential harm. A CMTS or router that's been compromised can obstruct service for hundreds or thousands of subscribers, and a breached subscriber portal can expose sensitive personal information. Ranking the weak spots will show which need to be prioritized. A recommendations report will include better network segmentation, stricter access controls, firmware updates, and fine tuning of incident response plans. These improvements will make the network stronger against future, more sophisticated attacks.

Continuous Security Maturity

Because cyber threats are constantly evolving, penetration testing must be ongoing. Broadband providers benefit from continuing assessments, forming lessons learned into constant security improvements. Regular testing, combined with threat intelligence feeds and managed security services, allow providers to adjust to new ransomware tactics, phishing campaigns, and zero day attacks as they emerge. It is advisable to conduct penetration tests at least once a year or whenever significant IT changes occur. Cybersecurity threats to broadband networks are increasingly sophisticated, but many compromises start with simple, preventable weaknesses like default passwords, misconfigured Active Directory settings, unmonitored IoT devices, or exposed credentials on the dark web. By understanding how attackers operate, from Man-in-the- Middle attacks to exploiting weak service accounts, organizations can better anticipate and block these threats before they escalate.

ATTACK VECTORS AND VULNERABILITIES

Human Factors

Human factors remain one of the most unpredictable and vulnerable elements in any organization's security posture. Even with robust technical defenses in place, employees can unknowingly become the entry point for attackers. Automated phishing simulations are a useful tool, but with the rapid advancements in artificial intelligence, these attacks are becoming more sophisticated than ever. The same AI

advancements that help organizations defend themselves, like AI assisted monitoring, email filtering, and security awareness training, are simultaneously available to attackers, creating continuously evolving threats. AI now enables attackers to generate highly convincing emails, impersonate voices using brief audio samples, and craft personalized messages that are almost indistinguishable from legitimate communications.

Penetration tests that address human factors help organizations identify where their defenses may fail under these realistic conditions. Targeted phishing, SMS based social engineering, and AI generated attacks are increasingly part of high quality assessments. These tests simulate real world tactics that attackers are actively using today, allowing organizations to measure the effectiveness of their training programs and internal controls.

On the technical side, attackers have shifted from the early 2000s model of downloading external malware to a technique known as "living off the land." Modern adversaries leverage built in system tools such as PowerShell or native Windows executables to perform reconnaissance, map networks, and move laterally across systems. By using these tools, attackers avoid detection while gathering critical information, such as domain controllers, administrative accounts, and network permissions. Penetration testers emulate these techniques to ensure that organizations can detect such activity before a real attacker does.

Another common human factor attack is the scenario in which employees receive seemingly legitimate emails or SMS messages containing links to real login pages, such as Office 365. While the website appears authentic and MFA is prompted as usual, attackers intercept session cookies and gain full access to the environment. Once inside, they can send mass emails, manipulate mailbox rules, or access connected services like OneDrive and SharePoint. During penetration tests, this type of attack has exposed passwords, encryption keys, and even corporate banking credentials stored insecurely, often in personal note taking applications like OneNote.

These examples illustrate why comprehensive penetration testing that includes human factors is critical. Even well trained employees can be susceptible to sophisticated social engineering and AI enhanced attacks. Testing against these modern tactics provides organizations with actionable insights, enabling them to shore up both technological and human defenses. It also demonstrates to stakeholders that the organization is prepared for real world threats, not just theoretical vulnerabilities.

Internal Threat Detection

Penetration testing often reveals not just potential vulnerabilities, but evidence of active threats. On occasion, testers encounter attack tools already present on a network during an internal assessment. In these scenarios, penetration testers immediately halt their activities and work closely with the client to confirm the source of the tools and ensure no harm is done. This highlights the importance of clear communication channels and predefined points of contact between the provider and the testing team, ensuring that any suspicious activity can be quickly verified.

One proactive approach to monitoring internal threats is the use of honeypots. A honeypot is a decoy system designed to be attractive to attackers. It may emulate a vulnerable server or service, and any interaction with it like a port scan, login attempt, or other activity will trigger an alert. This lets organizations detect potential internal threats quickly, without relying solely on automated monitoring tools. Deploying honeypots as part of a penetration test can provide immediate insight into whether an environment is already under attack or if new vulnerabilities are being actively targeted.

Active Directory Vulnerabilities

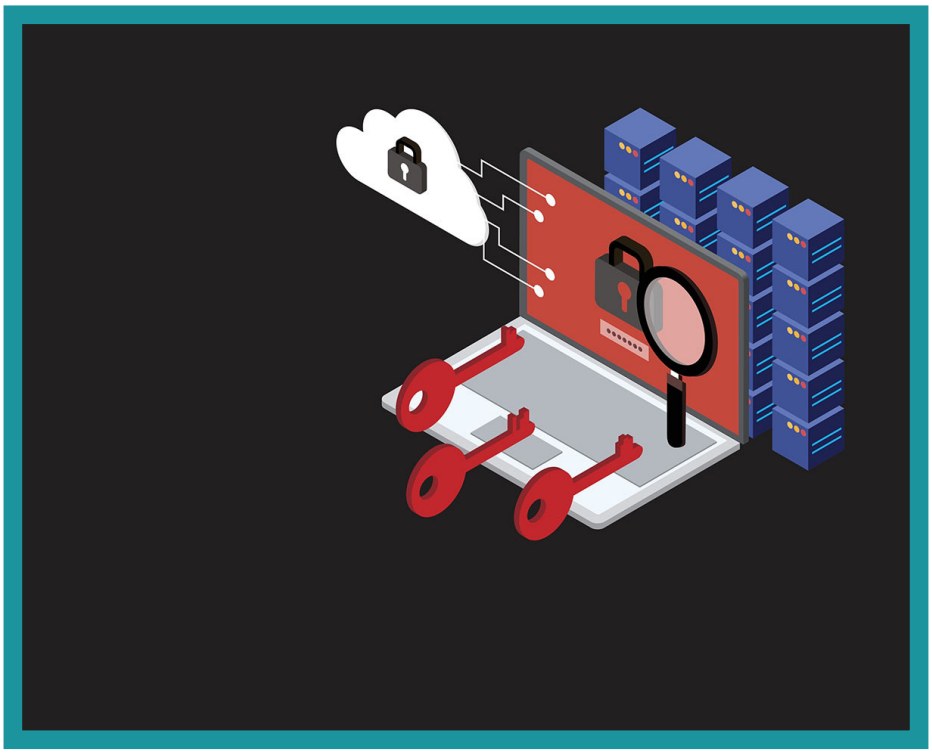
A critical area that consistently emerges as a high risk vulnerability is Active Directory, particularly in long standing environments. Active Directory is technology that has probably been in place in an organization for ten or twenty years. It's been upgraded numerous times, managed by different people, and over time it can become complex and poorly understood due to the multiple upgrades and administrative changes.

One particularly vulnerable component is Active Directory Certificate Services (ADCS). This is an add on that is manually installed and allows organizations to issue certificates for various purposes, including SSL web certificates and machine authentication. A properly configured ADCS provides a secure and integrated way for certificate based authentications. For certificate authentications, a Kerberos ticket is the electronic credential or certificate to prove identity and gain access to network resources without repeatedly providing a password. Like a driver's license, a Kerberos ticket identifies the holder and specifies their network access privileges, ensuring only authenticated clients can get tickets for specific services.

But a common vulnerability is found with a poorly configured ADCS, allowing attackers to request certificates that grant them authority to impersonate other users, including Domain Administrators. For example, in a Pass-the-Certificate Attack, a misconfigured certificate can be used to bypass traditional credential protections, effectively granting the attacker the ability to impersonate any user in the organization. This can lead to full network access within minutes.

And once an attacker can issue a Kerberos ticket, they can basically issue it for any employee in the company. They have full access to the network at that point. Organizations should research if they have Active Directory Certificate Services and if it's needed. If not needed, it should be disabled. And if needed, it should be secured. This is an actively exploited vulnerability by ransomware gangs. Notably, ransomware groups like Akira actively exploit these vulnerabilities.

In observed cases, attackers gain access, exploit ADCS, and encrypt the network within a single day. When they gain access to the network, one of the first things they do is check for the existence of ADCS. If found, they attempt to exploit it. If they are successful, they essentially have full control of the network and within a day they've already encrypted the organization's entire network. It happens very fast. So Active Directory is something all providers should be heavily securing.



Man-in-the-Middle

A frequently observed attack is the Man-in-the-Middle, particularly on Windows networks. IPv6 is enabled by default on all modern Windows devices, and attackers can exploit this to become an IPv6 DNS server. From there, they can relay network traffic, monitor authentication attempts, and even create computer accounts within active directory. Once an account is created the computer is the same as a user. This provides attackers with extensive access to network resources. While Active Directory Certificate Services often represents the first target for attackers, the Man-in-the-Middle attacks are a common alternative when ADCS is not available.

Default Passwords

Another surprisingly frequent vulnerability is default credentials. Devices such as printers, network switches, wireless network devices, cameras, and other IoT devices often ship with default usernames and passwords. When integrated with corporate systems like Active Directory for authentication or email for scanning and sending, these devices can provide a rapid path to network compromise. In one notable penetration test, a team gained domain administrator access within five minutes simply by exploiting a printer with default credentials, escalating through to admin privileges. It's not always complicated attacks. Sometimes it's as simple as a default password.

Although manufacturers have improved security in recent years, with some now requiring unique passwords during setup, vulnerabilities still exist. Even multifunction printers from major brands like Konica and Xerox have recently been released with exploits that cannot be patched, highlighting the ongoing risk posed by seemingly mundane network devices.

IOT Devices

The proliferation of Internet of Things (IoT) devices adds another layer of risk. Employees may unknowingly connect cameras, routers, or storage devices to the network, often without IT or security teams being aware. Such devices can create new entry points for attackers, highlighting the critical importance of network visibility and device management as part of a strong security strategy.

Password Security

Password security remains another key focus. During penetration tests, password hashes are frequently captured from the network and subjected to cracking attempts. Service accounts with elevated privileges are particularly vulnerable when weak passwords are used. This reinforces the need for strong password policies, multi factor authentication, and regular audits of privileged accounts.

File Shares

Open file shares can be a treasure trove for attackers. Passwords stored in spreadsheets, scripts, or backup images on network shares can be discovered and exploited. Even without direct access to an account, penetration testers often find sensitive data by scanning shared files for keywords or known password patterns. Organizations should regularly inventory file shares, limit unnecessary access, and ensure sensitive data is encrypted and properly managed.

Finally, when vulnerabilities are discovered, retesting is an essential step. Retesting should focus primarily on critical and high risk findings to confirm that remediation efforts were effective. Unlike a full retest of the entire network, this targeted approach ensures that organizations confirm fixes efficiently and cost effectively, typically at a fraction of the initial test cost.

SECURING YOUR ENVIRONMENT: PRACTICAL RECOMMENDATIONS

After reviewing the common attack vectors, it's natural to ask what can be done to protect your network today? Here are some of the most effective steps that organizations can implement immediately:

1. Conduct Regular Penetration Testing

A comprehensive penetration test is the foundation of understanding your network's vulnerabilities. If you haven't performed one recently, schedule it without delay. Ideally, assessments should be conducted at least annually to identify new threats and validate existing controls.

2. Implement Multi-Factor Authentication (MFA) Everywhere

MFA should be deployed everywhere, across all internal servers, applications, and virtual environments. Beyond preventing unauthorized logins, MFA can act as an early warning system. When a user receives a prompt they didn't initiate, it signals a potential intrusion. For virtual systems, MFA is critical on hypervisors, and they should not be integrated with Active Directory to prevent lateral movement if a compromise occurs. And if you're not using multifactor authentication on all your systems, you need to have strong passwords that are rotated frequently.

3. Enforce Strong Password Policies and Use Password Vaults

While MFA can reduce the reliance on complex passwords for end users, service accounts must still use robust, hard to crack passwords. These passwords should be stored securely in password vaults. Affordable and free options like 1Password or KeePass allow organizations to manage credentials efficiently while preventing insecure storage in personal notes or spreadsheets. Pen testers find many passwords just written in OneNote and Word documents. Get a free password vault or a low cost one for your organization and ensure that IT is using it for their service accounts. End users should also be encouraged to use it.

4. Monitor the Dark Web for Compromised Credentials

Attackers often exploit passwords exposed on the dark web. Penetration testers routinely search for a client's email domain and identify compromised credentials. In many cases these credentials still work and could provide attackers with external access. Ongoing monitoring allows organizations to identify and remediate compromised accounts before they are abused. When passwords are compromised they often end up on sites on the dark web.

5. Adjust Active Directory Settings

A simple yet effective change is to set the machine account quota to zero in Active Directory. By default, any user can create up to ten machine accounts, a capability the attackers often exploit. Disabling this prevents the creation of unauthorized computer accounts and mitigates common Man-in-the-Middle attacks.

6. Use MFA, Strong Passwords, and Least Privilege in Combination

Implementing MFA, enforcing strong passwords for service accounts, and maintaining strict access controls significantly reduces the risk of compromise. Together, these measures create multiple layers of defense that an attacker must bypass, dramatically improving your overall security posture.

7. Frequency of Testing

Frequent testing is a key consideration. At a minimum, a comprehensive penetration test should be conducted annually, covering internal systems, external attack surfaces, and human factors. However, many organizations are now adopting continuous penetration testing strategies, where critical components are regularly assessed throughout the year. This approach enables detection of emerging vulnerabilities, verification that security controls are functioning as intended, and confirmation that previously identified weaknesses have been remediated.

8. Infrastructure Changes

Penetration testing is also essential following significant changes to an organization's infrastructure, such as cloud migrations, data center transitions, mergers, or acquisitions. These scenarios often introduce new configurations or temporary shortcuts that can create unintended security gaps. Testing post implementation ensures that systems are properly configured, controls are in place, and any changes made during high pressure projects do not compromise security. Focused, scenario-specific assessments following major projects help identify misconfigurations, insecure practices, and residual vulnerabilities that may have been overlooked.

By following these recommendations, organizations can reduce the risk of both internal and external attacks. Proactive measures, combined with routine audits and monitoring, provide both prevention and early detection, helping to safeguard critical systems and sensitive data.

NEXT STEPS FOR BROADBAND PROVIDERS

Proactive penetration testing is an investment that protects networks, subscribers, the provider's reputation, and potentially their bottom line. With an ongoing routine for testing and improvement, broadband providers can can stay ahead of cyberattacks and provide secure services for their subscribers.

Keeping broadband networks secure from invasion is an ongoing process. The good news is that proactive measures work. Regular penetration testing, comprehensive MFA deployment, strong password management, careful Active Directory configuration, and vigilant monitoring of credentials can dramatically reduce risk. Security is not a once and done project, it is a continuous process that combines technology, policy, and user awareness.

Providers should schedule regular pen tests, rectify vulnerabilities and refine policies and procedures. Employee training programs reduces the human factor risks, and real-time monitoring and managed services provide continuous protection. Training employees to recognize phishing and secure password controls is as critical as technical defenses, since many breaches begin with a simple human error.

Ultimately, a secure network is built on layers of defense and early detection. By implementing these strategies, broadband providers can protect critical infrastructure, safeguard subscriber data, and maintain trust across the network. Some steps may seem like a technical challenge, but each one creates a meaningful barrier against attackers. That barrier can be the difference between a contained event and a full scale compromise.

ZCORUM'S APPROACH TO PENETRATION TESTING

ZCorum delivers comprehensive pen testing for broadband providers. The assessments cover all layers of the network, from subscriber devices to DOCSIS and FIBER infrastructure, providing actionable insights for mitigation and risk reduction.

Our reporting turns the technical findings into practical recommendations that comply with regulatory and funding requirements. We also offer guidance to ensure that weak spots are corrected without introducing new vulnerabilities. By adding pen testing into an overall security strategy, providers gain a stronger defense and greater subscriber trust.

For more information about our penetration testing service or our other managed cybersecurity services, contact us at 678-507-5000 or visit ZCorum.com/cybersecurity.

ZCorum™

800-909-9441

ZCorum provides a suite of broadband diagnostics and managed services to cable companies, telephone companies, utilities, and municipalities. As broadband providers face greater complexity and competition, ZCorum continues to help operators increase operational efficiency and re duce co sts, wh ile im proving su bscriber ex perience. This is achieved through ZCorum's diagnostics solutions for DOCSIS, DSL and Fiber networks, plus managed services that include data and VoIP provisioning, residential and commercial VoIP service, branded email and Web hosting, along with 24x7 support for end-users. ZCorum is headquartered in Alpharetta, GA. For more information, please visit **ZCorum.com.**