ALLIANT
CYBERSECURITY

SECURITY BULLETIN

Phishing Attacks

Attackers send fraudulent emails resembling those from reputable sources to steal sensitive data, like login credentials or credit card information.

- **Can we defend against malicious emails?**
  - § Phishing Simulation

Ransomware Attacks

Malware that encrypts the victim's files, with the attacker demanding a ransom to restore access. It often spreads through phishing emails or exploiting vulnerabilities.

- **What is the impact of a ransomware attack on my organization?**
  - § Vulnerability Assessment

Insider Threats

Threats coming from individuals within the organization, such as employees, contractors, or business associates, who have inside information concerning the organization's security practices, data, and computer systems.

- **Can we protect our organization from an attack on our internal network?**
  - § Internal Penetration Test

Advanced Persistent Threats

These are prolonged and targeted cyberattacks in which an intruder gains access to a network and remains undetected for an extended period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization.

- **Can my organization defend against a highly advanced threat actor?**
  - § External Penetration Test

PENETRATION TEST COMPONENTS

External Network Penetration Test:

- **Objectives:** This test aims to protect your digital perimeter by identifying potential security breaches and weaknesses in your organization's external-facing assets. It ensures that your network's first line of defense is solid.

- **Methodology:** We use simulated cyber-attacks from an external viewpoint, systematic reconnaissance, targeted vulnerability scanning, and controlled exploitation techniques to assess the resilience of your network perimeter.

- **Reporting:** Our report offers a clear, detailed analysis of vulnerabilities, the methods used to identify them, their potential impact on your organization, and prioritized recommendations for remediation to enhance your security posture.

Internal Network Penetration Test:

- **Objectives:** This test focuses on evaluating the security of your internal network by simulating internal threat scenarios to identify vulnerabilities that could be exploited by an attacker already inside your network.

- **Methodology:** We conduct a thorough assessment using tools and techniques designed to mimic an internal actor, aiming to discover and exploit vulnerabilities within your internal network.

- **Reporting:** The final report provides actionable insights into detected vulnerabilities, exploitation outcomes, risk assessment, and targeted recommendations for strengthening your internal network security.

Phishing Simulation:

- **Objectives:** Our phishing simulation assesses your organization's resilience against social engineering and phishing attacks, crucial for fostering a culture of security awareness among employees.

- **Methodology:** By designing and deploying controlled phishing campaigns, we measure the effectiveness of current training programs and identify areas for improvement in employee response to deceptive emails.

- **Reporting:** You receive a comprehensive analysis of the simulation results, including employee response rates, susceptibility to phishing, and customized training recommendations for bolstering your human firewall.

Web Application Penetration Test:

- **Objectives:** This test identifies security vulnerabilities in your web applications that could potentially be exploited, ensuring they are robust and secure against malicious attacks.

- **Methodology:** Through targeted examination and exploitation of web application vulnerabilities, we aim to uncover security gaps in application logic, authentication, and data protection mechanisms.

- **Reporting:** Our detailed report outlines identified vulnerabilities, exploitation techniques used, the potential impact, and recommendations for securing your web applications against future threats.

Wireless Penetration Test:

- Objectives: Designed to ensure the security of your wireless networks, this test identifies vulnerabilities that could allow unauthorized access or data compromise, which is essential for maintaining a secure wireless communication environment.

- Methodology: We evaluate your wireless infrastructure using advanced techniques to detect and exploit vulnerabilities, assessing the security of your Wi-Fi networks comprehensively.

- Reporting: The report provides a detailed analysis of vulnerabilities found, their implications for security, and actionable recommendations for hardening your wireless networks against unauthorized access.

Physical Penetration Test:

- Objectives: This test evaluates the effectiveness of physical security controls at protecting sensitive information and assets, identifying any breach opportunities that could be exploited.

- Methodology: Mimicking real-world intruder techniques, we attempt to bypass physical security measures to assess the vulnerability of your physical defenses.

- Reporting: You'll receive a report detailing the vulnerabilities discovered in your physical security, the methods used for testing, and practical steps to enhance physical security and mitigate identified risks.

Vulnerability Assessment:

- Objectives: The goal is to provide a comprehensive assessment of vulnerabilities across your networks, systems, and applications, offering a clear view of your current security posture and areas for improvement.

- Methodology: Using a blend of automated tools and expert analysis, we identify, categorize, and prioritize vulnerabilities based on their potential impact on your organization.

- Reporting: Our report delivers a prioritized list of vulnerabilities, accompanied by actionable recommendations for remediation, helping you proactively address security weaknesses and strengthen your defenses.

CALL TO ACTION

Understanding the complexities of cybersecurity and recognizing the multitude of potential threat scenarios you might face can be alarming. However, the good news is that you're not alone in navigating these challenges. To ensure that your organization is well-prepared and resilient against such threats, it's crucial to take proactive steps in assessing and enhancing your cybersecurity posture.

This is where Alliant Cybersecurity steps in. With a team of seasoned cybersecurity experts and a comprehensive portfolio of penetration testing services, Alliant Cybersecurity is equipped to identify vulnerabilities within your network, systems, and applications before they can be exploited by malicious actors.

So, why wait for an attack to reveal the weaknesses in your cybersecurity armor? Taking action now can prevent significant financial loss, protect your reputation, and ensure the continuous operation of your business. Contact Alliant Cybersecurity to conduct a thorough penetration test tailored to your unique needs. By simulating real-world attacks, you'll gain valuable insights into how your defenses stand up against the most pressing cybersecurity threats and what steps you can take to fortify your security.

Don't leave your cybersecurity to chance. Reach out to Alliant Cybersecurity today and take a significant step towards safeguarding your organization's future. Together, let's build a security strategy that not only addresses today's challenges but also anticipates tomorrow's threats.

Contact ACS and secure your organization.

BE AWARE. BE SECURE.

Contact us to learn more: alliantcybersecurity.com | (877) 84-CYBER |

An alliantgroup Company