CASE STUDY

Cybersecurity Assessment Enables State Agency to Improve Security Posture and Compliance

To satisfy state information technology security standards, a state agency engaged AIS Network's cybersecurity engineers to perform their annual third-party security assessment. These tests are designed to uncover gaps and vulnerabilities, strengthen security posture and promote best practices within the agency. The assessment performed included recommended modifications that allowed the agency to improve its security posture and its compliance with state standards.

Client

A $2.2 billion state health agency with 6,000 employees and 119 local districts is dedicated to protecting and promoting citizen health. Generating public awareness about emergency preparedness, health threats and disease outbreaks is a critical responsibility.

Challenge

Maintaining cybersecurity compliance is critical for state agencies, and they are required to conduct a third-party security assessment annually – or more frequently if addressing environmental changes on systems housing state data. A large agency engaged AISN to conduct its annual security assessment. Such testing is intended to authenticate vulnerabilities or determine the degree of resistance that organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources and/or skills) and/or provide more in-depth analysis of weaknesses and deficiencies.

Solution

AISN performed a pretest analysis on the target system, a detection of likely exposures based on the analysis and testing designed to verify exploitability of related vulnerabilities. The team used tools, techniques and procedures to simulate real cybersecurity scenarios and attacks. To test the agency staff's security awareness, a phishing exercise was sent to 4,000 employees agencywide. Engineers then tracked those who clicked on the link and/or provided credentials to a false site.

Results

The agency's annual security assessment followed the state's very specific IT security standards and included network/host (Section CA-8) penetration testing, web application testing and social engineering. AISN's experienced engineers developed a formal, in-depth analysis of the agency's security environment, including weaknesses and deficiencies. The team then briefed agency executives on recommended remediation steps. This security assessment enabled the client to resolve security disparities quickly, satisfy state compliance requirements and improve the agency's overall security posture.

A I S
Network

Operationalizing
Your IT Strategy

P: 847.202.1400 E: sales@aisn.net
W: https://www.aisn.net