HEALTHCARE INDUSTRY

Integrated Technology = Integrated Dangers

RHINO SECURITY LABS

The growing dependence on technology has brought a similar upsurge in cyberattacks, particularly in the healthcare industry. Even small clinics can store records for thousands of patients, which contain names, DOB, and social security numbers – valuable commodities on the underground market. To make matters worse, the traditional culture of many healthcare facilities often leaves IT behind the times – and vulnerable to attack. There are many specific challenges related to security in the healthcare ecosystem.

COMPLIANCE REQUIREMENTS

The medical industry is one of the most widely regulated industries in the U.S. due to the quantity and sensitivity of medical information in healthcare companies. The primary regulation for these organizations is HIPAA, which mandates all organizations holding PHI to adhere to a standardized set of controls – a compliance mandate which can be a burden for even the most prepared.

ATTRACTIVE AND READY TARGETS

There are significant risks to electronic patient health information (ePHI) and other sensitive data. A manual penetration testing engagement can uncover vulnerabilities that may pose a threat to your network and patient's data.

POTENTIAL IMPACTS

- HIPAA / HITECH Penalties
- Breach Lawsuits / Legal Fees
- Operational Downtime / Medical Impact
- Negative Press / Public Relations

BUDGET AND CULTURAL CHALLENGES

Limited tech budgets and slow-moving culture are both common challenges in healthcare. These can often be addressed with management by identifying the costs incurred by hacked medical companies – such as Anthem and Premera.

HEALTHCARE TARGETS

- Workstations & Smartphones
- Healthcare Databases
- File Servers
- Patient Apps & Websites
- Embedded Systems (Medical Devices)

RELATED ASSESSMENT SERVICES

To support the security needs of the industry, we have a range of penetration testing services. Below are a few of these recommendations, customized around your business business and technology needs.

1. Penetration Testing

Our world-class penetration testing and research has been covered in Wired, Forbes, CNN and other outlets, showcasing our comprehensive assessment package. Identify the weaknesses– and strengths – of your security infrastructure before attackers do.

2. Social Engineering

While security assessments are typically focused on technology, many attacks begin with a phishing email or phone call. Test employee education, security policies, and technical controls to identify gaps in phishing prevention.

3. Application Assessment

Each application assessment starts with the OWASP Top 10 risks, but includes more advanced vulnerabilities to ensure all attack vectors have been identified. Whether web, mobile, or IoT, we have the experience to address the unique security challenges you face.

4. Secure Code Review

Identify and remediate software vulnerabilities early and often. With a hybrid approach, we use both automated code scanners and hands on, manual analysis to conduct a thorough security review of your application.

PAST ATTACKS ⚠

2011

SAIC

4.9 million medical records stolen

2013

ADVOCATE MEDICAL GROUP

4 million records stolen

2014

COMMUNITY HEALTH SYSTEMS

4.5 million records stolen

2015

ANTHEM

80 million records lost

OCTOBER 2015

BC/BS OF TENNESSEE

1.2 million patient records lost

ABOUT RHINO SECURITY LABS

Rhino Security Labs is a top penetration testing and security assessment firm, with a focus on web applications, cloud/AWS, network, mobile apps and phishing testing. With manual, deep-dive engagements, we identify and demonstrate security vulnerabilities which put clients at risk.

Endorsed by industry leaders, Rhino Security Labs is a trusted security advisor to the Fortune 500.