TECHNOLOGY INDUSTRY

Prepared For A Dedicated Cyberattack?

The growing dependence on technology has brought an upsurge in cyberattacks, particularly in the technology industry. Whether semiconductors, eCommerce, or software-as-a-service (SaaS), tech firms handle a range of unique sensitive assets – and security issues. The fast-paced nature of these organizations can leave security as an afterthought.

COMPLIANCE REQUIREMENTS

Due to the range of sensitive information stored, compliance requirements for tech companies can vary widely. Needs range from PCI-DSS for handling card data to SOC2 and a range of customer compliance requirements. In many cases, ISO 27001 is a necessity to demonstrate proper controls to investors and other key stakeholders.

POTENTIAL IMPACTS

- Service Downtime / Operational Impact
- Customer Dissatisfaction
- Increased Client Acquisition Costs
- Breach Lawsuits / Legal Fees

ATTRACTIVE AND READY TARGETS

With large, sensitive databases and code repositories, the tech industry faces a number of security adversaries. But outside threats aren't the only security concern to IT. Poor development practices, weak passwords, and network complexities all provide weaknesses to be exploited by attackers. Even the largest tech giants aren't immune to such issues – as shown with major breaches at Adobe, Apple, and Google.

TECHNOLOGY TARGETS

- Source Code Repositories
- End User Databases
- Application Environments
- Payment Portals
- Sensitive Backups

info@RhinoSecurityLabs.com | 888.944.8679

464 12th Ave, Suite 300 | Seattle, WA 98122

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

DECEMBER 2010

GAWKER

details on 1.3 million users exposed by 4chan hackers

OCTOBER 2013

ADOBE

38 million users compromised

SEPTEMBER 2014

APPLE

Breach leaks sensitive photos of 20 celebrities

OCTOBER 2015

GOOGLE

5 million gmail credentials stolen from partner

DECEMBER 2015

VTECH

Info on 5 million children and parents 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.

info@RhinoSecurityLabs.com | 888.944.8679

464 12th Ave, Suite 300 | Seattle, WA 98122