

VULNERABILITY BRIEF 1
BACKGROUND 2
PHASE ONE FINDINGS 3
Vulnerabilities 3
Recommendations 3
PHASE TWO FINDINGS 4
Vulnerabilities 4
Recommendations 4
PHASE THREE FINDINGS 5
Points of Interest 5
Recommendations 6

- + Vulnerability Testing
- + Penetration Testing
- + Video and Voice Telecommunications Testing

INFRASTRUCTURE_SERVICES
vulnerability testing +/- Policy



WWW.IOACTIVE.COM

➤ INFRASTRUCTURE_SERVICES

IOActive
COMPREHENSIVE COMPUTER SECURITY SERVICES

INTERNAL ASSESSMENT RECOMMENDATIONS 9
Network Level 9
Host Level 10
Policies and Process 11
Industry Standard Security Requirements 12
Objective and Scope 13
OBJECTIVE 13
PROJECT SCOPE 13
External Network Parameters 17
Internal Network Parameters 17

INFRASTRUCTURE SERVICES

WHY INFRASTRUCTURE AUDIT SERVICES?

Even the most comprehensive security solutions require maintenance to ensure continued performance that effectively protects your information assets from risk. IOActive offers a suite of Infrastructure Audit Services designed to provide a comprehensive review of an organization's network and technology infrastructure, identifying and helping to mitigate both technical and compliance-related risks, and providing advisory services to help improve overall information security.

Margaret Jane Radin, Professor of Law, Science, and Technology at Stanford University Law School advises that organizations that fail to demonstrate due diligence by performing continuous risk assessments and vulnerability testing will find themselves at increasing risk of civil action for damages incurred from unauthorized use of IT resources that are used to attack others.

Much as financial auditors discover accounting issues before they turn into real problems, IOActive's infrastructure audit teams can help uncover weaknesses in an organization's technical infrastructure before an attacker finds and exploits them.

Forethought

"Act now or risk making the news headlines later", seems to be the current sentiment of forward-looking organizations who view technology as a strategic, profit-generating asset.

The acceptability of reactive security is a thing of the past. Companies are being shut down, lawsuits are becoming the norm, rather than the exception, and the FTC has never been more vigilant when dealing with companies that embraced the "Wait and See" approach to securing their organization from compromise. IOActive's customers see benefit on the bottom line by embracing security, aligning it with competitive business needs, and leveraging it as a market-place differentiator.

Automated network and application scanning is a whitehat activity informed by a blackhat history of known defects and exploits. Trailing-edge awareness will not support forward-thinking security decisions and will fail to adequately maximize security investment. Through IOActive Labs, our team is kept abreast of future trends in the hacker ethos.

Methodology

A secure infrastructure is the cornerstone of protecting an organization's systems, data, and applications, and complying with myriad international, federal, and state laws surrounding data privacy. The success of the modern enterprise depends on the security of the infrastructure. IOActive's highly experienced consultants work collaboratively to build upon our clients' internal policies, incorporate recognized industry leading practices and standards, and align them with applicable regulatory and legislative requirements to develop a gap analysis that identifies areas of weakness and high risk, and produces a roadmap for addressing those exposures with proven solutions. IOActive's professional services go well beyond the approach of commodity scan vendors, and help our clients to effectively understand risk and exposure. Our team performs in-depth technical review of the environment, rigorously exercises security measures, identifies strengths and weaknesses, and delivers a thorough report and presentation that covers current and desired states, corresponding gap-analysis, and detailed recommendations. IOActive delivers these results in a format specifically designed to encourage knowledge transfer that empowers our clients to effectively move forward and reduce their security exposure.

Vulnerability Testing

Network vulnerability testing is a comprehensive examination of the current state of your organization's IT infrastructure to assess effectiveness of security controls, and identify methods that an attacker might use to access your network. Regular assessments are required to identify system changes that might result in an increased attack surface, and to identify isolated target areas in the network that require immediate attention. IOActive's approach to network vulnerability testing is to assess key control components of your network system, identify weaknesses, determine compliance with applicable regulations, laws, and standards, and deliver an in-depth report containing prioritized mitigation strategies.

IOActive's vulnerability testing services include, but are not limited to:

- + SCADA Testing
- + Evaluate security of mail servers, messaging servers
- + Verify security assumptions made in VPN infrastructure
- + Evaluate effectiveness of system event logging
- + Exercise logical and perimeter defense systems
- + Evaluate Wireless Exposure // 802.11a/b/g, BlueTooth
- + Test remote access systems including dial-up
- + Review password strength policies
- + Employ Social Engineering attacks
- + Validate security of back up sub-systems

Video and Voice Telecommunications Testing

The telecommunication infrastructure is the lifeblood of an organization's ability to disseminate and share information, realize efficiencies, and stay ahead of its competition. On a daily basis, incredibly sensitive information passes from the CEO's desk to the accountant's desk that depends on the sanctity of this medium. Having an independent third-party security review of PBX, VoIP, and Video Tele-conferencing systems is the hallmark of a mature enterprise risk management program. IOActive assists Fortune 500 companies with identifying information leaks in their communication infrastructure and recommends appropriate remediation strategies.

Penetration Testing

Protecting customer privacy and preserving the integrity of intellectual property challenges all organizations. Even the most security-savvy corporations have experienced devastating loss of revenue and reputational damage due to serious security breaches. IOActive evaluates an enterprise's security by reviewing infrastructure, protective boundaries and external factors, and identifying weaknesses that can compromise the ability to maintain strong security controls. Effective penetration testing means actively attempting to breach security measures in place, just as an experienced attacker or a malicious insider may attempt to do. Our penetration tests are tailored to each client's specific needs and environment.

IOActive's penetration testing services include, but are not limited to:

- + SCADA Testing
- + Active attempts to retrieve corporate email, phone calls, instant messages, account lists, passwords, accounting records, intellectual property
- + Firewall/IDS/IPS evasion and exploitation
- + Remote access compromise (VPN, PBX, War Dialing)
- + Client side exploitation
- + Phishing attacks / Social Engineering
- + Untrusted media insertion, (USB dongle/CD attack)
- + Wireless key cracking, (WPA, LEAP, WEP)

Fact

According to Gartner, the goal of an effective infrastructure security program is to reduce vulnerability by mitigating attackable weaknesses. If your organization is spending too much time monitoring virus warnings and malicious code attacks, it's highly likely that your IT infrastructure is increasingly vulnerable as your overall systems become out of date.

For more information about our services please contact:

SECURE@IOACTIVE.COM
TOLL FREE (866) 760-0222

About IOActive

Established in 1998, IOActive is a professional services consulting firm specializing in information risk management and application security analysis for global organizations and software development companies.

Unlike commoditized network security services and off-the-shelf code scanning tools, IOActive performs gap analysis on information security policies and protocols, and conducts in-depth analysis of information systems, software architecture and source code by using leading information risk management security frameworks and carefully-focused threat models.

As a home for highly skilled and experienced computer security professionals, IOActive has attracted the likes of Dan Kaminsky, Jason Larsen, Darek Milewski, Ward Spangenberg, and Ted Ipsen; key advisors like Steve Wozniak; and a crew of unequivocally talented "white-hat" hackers who, before being asked to host the infamous Capture the Flag at Def Con, owned the competition three years in a row.

Another data-point reflecting the talent of our consultants is the fact that IOActive is one of only three firms in the world that were tasked by Microsoft with the security code review of the Vista client operating system.

Application Security Services

- + Threat Modeling
- + Application Code Review
{C/C++, .NET, C#, Java, Delphi, ASM, Perl}
- + Web Application Code Review
{ASP.NET, C#, Java, PHP}
- + Black Box Application Pen-Test
- + Product Evaluation {white box/black box}

Infrastructure Audit Services

- + Vulnerability Testing
- + Penetration Testing

Incident Response Services

- + On Call Contracts
- + Network Flow Data Analysis
- + Disk Level Analysis
- + DDoS Mitigation

Advisory & Risk Management Services

- + ERM Development and Implementation
- + ISO 27001 / 17799 Implementation
- + Security, Privacy & IT Audit Co-Sourcing
- + Compliance Assessments
- + PCI Data Security Standard
- + Third-party Due Diligence Reviews

Training Services

- + Advanced Asp.Net Exploits and Countermeasures
- + Writing Secure Code: .NET and Java
- + Rapid Application Threat Modeling
- + The Security Development Lifecycle
- + How to Respond to a Security Breach
- + Security Incident Response Seminar

INFRASTRUCTURE