INTERDEV
Managed IT | Security

Vulnerability Assessment and Management Services

With digital security threats growing at an exponential rate, many business leaders wonder, "Are my company and its assets safe?" If your company is open and operating, the answer is, "You are vulnerable." The million-dollar business question is, "How bad is it?" The InterDev Vulnerability Assessment will answer that question. Using deep inspection tools and our decades of experience, we evaluate every aspect of your enterprise and its systems, from technology infrastructure to personnel behaviors and other potential vulnerabilities. Then, we can help you develop an effective, achievable threat mitigation plan to ensure your firm doesn't end up a statistic.

How Bad Is It?

In its 2015 security survey, PwC (formerly PricewaterhouseCoopers), reported that security incidents are growing at a 66% compound rate, reaching 117,339 incidents per day in 2014. With the average cost of a data breach now costing affected companies $3.5 million for remediation, penalties, and other hard dollar costs (per the Ponemon Institute), there is no doubt that security breaches are frequently crippling. Even "minor" security-related service interruptions result in direct financial losses, damage to corporate reputations and diminished customer confidence.

It's that bad !

The InterDev Vulnerability Assessment

We uncover the current flaws in your defenses, including both internal and external vulnerabilities across all network devices, servers and network services. You'll review these results in a clear, coherent report with functional recommendations to minimize your exposure to cyber attackers and corporate criminals.

- **Network vulnerability:** Comprehensive network scan for security, configuration and access problems.
- **Wireless security:** A wireless network evaluation for encryption issues, rogue (unauthorized) access points and other potential threats.
- **Environmental security:** Risk evaluation of your operating environment including policies for on-premise access by strangers and removal of company assets for any reason.
- **Database and application security:** Vulnerability scan of databases and software such as missing patches or updates.
- **Personnel security:** Personnel risk assessment to reveal behavioral indiscretions, deficient policies and procedures, and other problems that could put your firm at risk.

After the report is in your hands, we will work with you to begin the most important tasks of all—remediation and protection to safeguard the future of your business.

** Last year, it took notification from the FBI for thousands of US companies—from small businesses to leading retailers—to learn they had been victims of cyber intrusions.*

InterDev's Vulnerability Management Program: Remediate, Rescan and Manage

Our comprehensive Vulnerability Assessment and Report covers the first phase in the life-cycle of successful vulnerability management and mitigation. After you receive our report, we can prepare a remediation plan at your request and begin the real work of plugging the holes in your defenses.

Remediate

- Secure your network against outside intrusion, including government-grade security for your wireless transmissions and immediate identification of unauthorized access points.
- Mitigate any damage that could be caused should a threat enter your system.
- Develop an education plan to inform employees of their roles in maintaining a robust defense and make recommendations for changing personnel behaviors, policies and procedures (Currently, bad judgment by unwitting personnel is the #1 source of corporate infection).

Rescan and Confirm

After initial remediation is complete, our security team will probe deep into your systems with a second scan to mitigate any remaining flaws hidden within your business environment. We will then take further corrective action, if necessary, to ensure your system and business assets are secured to the greatest degree possible against the onslaught of threats.

Manage

Depending on the service level you select, InterDev will also periodically reassess your network and IT architecture, policies and procedures to determine if the risk level has increased and further corrective action is required.

ProActive Security™

"Malware is mutating so rapidly and malware attacks are so prolific that not even the most heavily defended national agencies are 100% secure."

The InterDev Vulnerability Lifecycle

- **Network & Environment Discovery:** Understand what assets, people and tools make up your network environment.
- **Vulnerability Scan:** Uncover system and application vulnerabilities and inappropriate device configurations within the network.
- **Vulnerability Report:** Review feedback and recommendations for improvements, prioritized by urgency.
- **Remediation:** Repair and reinforce your defenses to mitigate threats within the environment.
- **Vulnerability Rescan:** Confirm that remediation activities were effective.

Atlanta I Chicago
www.interdev.com | 770.643.4400

CORE SECURITY™ Thinking ahead. QUALYS® On Demand Security Barracuda Trustwave® Information Security & Compliance