



Attention I.T. Personnel: How well are you sleeping at night?

The following article includes excerpts taken from a whitepaper written by Patrick Clawson, Chairman & CEO of Lumension Security.

The reactive approach

Information security managers have always had a healthy fear of the unknown threat. But over the last two years that fear has developed into a paranoia, an obsession that keeps them up at night sweating over thoughts of financially-motivated malware that may be slipping past their traditional anti-malware defenses without a blip on the radar. They spend all of their time trying to find better ways to block the threats, and yet most of their efforts end in futility anyway.

This is because the threats keep multiplying. The past several years have brought a wave of unending zero-day attacks designed specifically to silently steal information.

Compounding the near-constant barrage by the criminals is the fact that rogue users are increasingly opening up the enterprise to countless more risks by introducing applications and technologies with exploitable flaws. One big example is the proliferation of social networking sites whose users have become low-hanging fruit to attackers.

Personal applications such as peer-to-peer file sharing applications expose enterprises to software licensing and copyright violations. The same goes for the unfettered use of removable storage devices, which brings the added risk of data leakage.

Hackers and other malcontents can easily take advantage of the fact that these outmoded technologies must know about a particular type of attack before they can protect against it. This is the reactive approach's Achilles heel, one that is being assaulted daily by malicious "boutique" attacks designed specifically to evade traditional defenses by sneaking in with new and unknown approaches.

5 Steps to a Proactive Security Model

1. Discover Assets
2. Develop Policy
3. Eliminate Risks and Threats
4. Enforce Policy
5. Audit and Report



The proactive approach

The principle of proactive security is simple. Rather than chasing every risk and threat in the environment with blocks and denials, the proactive security practitioner blocks everything by default. Only the known good applications are allowed to run. The unknown threat loses its power when it is blocked from systems automatically.

In an ideal setting, the proactive approach will establish the "known good" across the entire IT infrastructure. When organizations establish what they want their systems and configurations to look like at any given point in time, they gain proactive control of their infrastructure.

A proactive model will ensure a desired security posture by settling in advance on matters such as patch levels and vulnerability remediation, port settings and accepted networking equip-



GO WITH JO TRAVEL, INC.

Serving Clients Since 1983
Our Customers are our BEST Referrals
Visa Service & Free Passport Photos

Award Winning Full-Service Travel Agency

Join us for discounted group adventures!
Let Jo know if you want to go

March 8th, 2008
7 Night Silverseas Cruise Dubai from \$2,937

March 17th-22nd, 2008
Carnival - Yucatan/Cozumel

June 29, 2008
7 days MSC Orchestra Italy.

July 4th-16th, 2008
Holland America to Scandinavia Russia

July 6-13, 2008
RCCL 7 night Western Carribean Cruise.

2008 Futures
Tauck Canadian Rockies & Glacier
National Park with rail.
Branson & Africa

ment, along with accepted devices and applications. By doing so, IT administrators gain the visibility and the capacity to manage the infrastructure securely without ever worrying about reacting to new threats.

Reaping the benefits

Clearly, it takes more foresight and effort to replace a reactive model with a more effective proactive security approach. In large part this is why many organizations still persist in relying on traditional techniques or other point solutions.

By combining the power of vulnerability management, automated patching, and whitelist application and device control, any organization can similarly eliminate the risk of the unknown threat.

The chaos of reactivity can be replaced by the order of the known good. This is the true potential of a fully-realized Proactive Security Model. And that means a good night's sleep for everyone. **HB**

Darryl Santa is the President of Alpha & Omega Computer and Network Services, Inc. which has been serving small to mid-sized businesses in Huntington Beach for the past decade. Alpha & Omega takes a proactive approach in supporting your network by customizing a preventative maintenance schedule that fits within your company's budget. Through preventative maintenance and technology planning, we'll spend less time fixing problems and more time utilizing I.T. effectively to grow your business. Whether your company needs to maintain its current network environment or deploy the latest in information technology solutions, Alpha & Omega wants to be the First and Last of all your technology needs. Check us out on the web at www.aobiz.com or contact us at 714-964-6932.

Corporate ♦ Leisure ♦ Group ♦ Wholesale Air ♦ Cruise ♦ Tours

JO ANDREWS, C.C.C., D.S.

Travel Agent Trendsetter of the Year 2003
Athena Award HB Chamber of Commerce 2006

5500 Bolsa Avenue #130 ♦ Huntington Beach, CA 92649

714.379.3755

CST 205048 40

Season's Greetings

"Your one-stop business center"

THE Mail SECRETARY

Serving Huntington Beach Since 1980

- Private Mail Box Rentals
- Mail Forwarding
- FedEx, UPS
- Custom Packaging
- Fax Service
- Notary Public

PRIVATE & SECURE

One Free Month Private Box Rental
(w/min. 3 month rental, new customers)

MENTION THIS AD, RECEIVE \$1 Off UPS under 10 lbs; \$2 Off over 10 lbs.

714-846-5513

FAX: 714-840-3678

5901 Warner • Huntington Beach
(just West of Springdale)

