

SECURITY EXPERT

Q&A An Ounce of Prevention Beats a Pound of False Positives

Intrusion Prevention Bolsters Network Security

What are the biggest challenges with regards to network security today?

Paquette: “There are many challenges facing network security managers, but there are two clear challenges that are impacting all organizations, regardless of size: Dedicated resources and the increasing sophistication of attacks and intrusions. As companies look to streamline operations and reduce expenses, many companies are cutting back on their IT budgets. This presents a major challenge for companies, as yesterday’s security technology is rapidly becoming obsolete for protecting against the latest cyber attacks. Organizations are realizing that traditional firewalls and intrusion detection devices are unable to adequately protect critical resources.”



MIKE

PAQUETTE

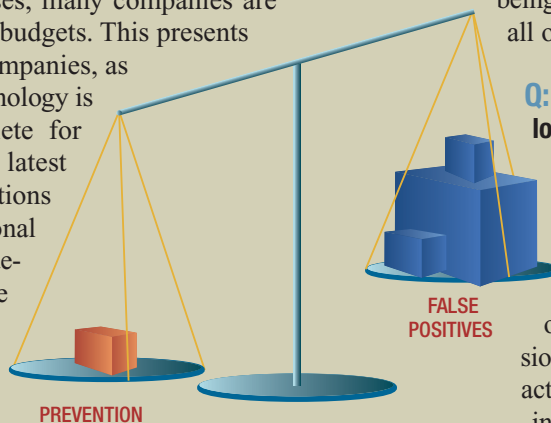
Mike Paquette, vice president of product management for Top Layer Networks, discusses protecting organizations’ valuable network assets with a comprehensive intrusion prevention strategy.

Founded 1997, Top Layer Networks provides comprehensive Network Intrusion Prevention solutions worldwide. Our ASIC-based, high performance products dramatically expand network protection, increase network availability and reduce costs associated with cyber crimes.

Top Layer

perfecting the art of network security

www.TopLayer.com



Q: Why don't firewalls protect the network?

Paquette: “It is important to understand what firewalls do well, and what they are not designed to handle. Firewalls are quite effective at providing policy-based access control via IP addresses and TCP/UDP ports, essentially creating a boundary between critical resources and the outside world. They’re also useful for Network Address Translation (NAT). However, typical firewall deployments leave ports open to intruders and unwanted traffic, and don’t effectively block HTTP worms, DoS attacks, and protocol anomalies. When firewalls are loaded down with extra plug-ins to try to address these issues, the firewall itself can become a performance bottleneck and cause reduced availability.”

Q: Don't typical nIDS (Network Intrusion Detection Systems) provide the required protection?

Paquette: “Network intrusion detection systems are valuable in helping to identify attacks, intrusions, and unwanted traffic, but do not provide the actual protection needed to keep critical resources secure. Because of the manual intervention necessary, typical nIDS deployments

result in an unacceptably long MTTC (Mean Time to Correct) or MTTM (Mean Time to Mitigate) when intrusions and attacks do occur. Well-intentioned security staffs are frustrated trying to extract accurate event information from large IDS log files typically cluttered with many false positives. Properly identifying attacks becomes extremely difficult and often result in real attacks being completely missed amongst all of the false positives!”

Q: What should an organization look for in a network security solution?

Paquette: “Organizations should look for a solution that both detects and prevents intrusions, rather than one that simply detects intrusions and notifies a human to take action. One way to think about intrusions and attacks is to compare them to illness. In medicine, we pay doctors to diagnose our illness or condition

and then prescribe a course of treatment. Ideally, it would be less expensive and more pleasant to prevent illness in the first place. To manage the health of networks and attached resources, organizations pay security staff to diagnose problems (using IDS) and prescribe and implement a plan for correction and/or mitigation. Clearly a lot of time, money, and energy could be saved if a pro-active approach was taken that did not allow the network or resource to get “sick” in the first place.”

“Companies are now recognizing that it costs much less to prevent attacks than to repair the associated damages related to successful attacks to a network. This is the idea behind Intrusion Prevention and the underlying mission of what is being done at Top Layer.”

Contact Top Layer at 508-870-1300 or www.TopLayer.com to see how we can help you increase your security with our Intrusion Prevention solutions.