

BEYOND THE MOAT - COMPREHENSIVE SECURITY STRATEGIES

The first steps in constructing a hardened perimeter are to discover your network and your perimeter, know what you are protecting! What we find is that it can be difficult for banks to truly understand their environment. A heuristics based IPS is the most important component of a perimeter defense, to catch the new and unknown threats and stop them before they can cause damage. Banks must ensure that any system be configured by experienced personnel: a mis-configured firewall is worse than no firewall at all. Finally, train all your personnel, at all levels, to the dangers of the Internet. Teach them what behaviors can compromise the security of your data, tell them about social engineering. It will be the best money you'll ever spend.

Financial institutions usually have a few employees or vendors who need access to many applications. IPSEC 3DES is the solution in such cases. Strong authentication may also be in order. Again, educate your employees (and executives) to the dangers of social engineering, and implement strict procedures in case a laptop is stolen.

We tend to focus on Internet threats, and we either forget or underestimate that most security breaches come from inside the network. Know what assets you are protecting and adopt different measures depending on the importance of what you are trying to protect. The technology is almost irrelevant, as long as you adopt a comprehensive and relevant solution. Keep your systems patched and Anti-Virus defense regularly updated. Again, at the perimeter, a heuristics-based IPS is key to preventing intrusions.

The key pieces of a defense-in-depth strategy definitely include Anti-Virus and firewall, because of the erroneous common perception that a firewall is enough to protect the perimeter. We are seeing an increased attention to anti-spyware software, given the threat spyware represents. The notion that viruses and threats are more effectively stopped at the gateway with an all-in-one appliance is one that is making inroads in the Small and Medium Enterprise landscape.

Viruses, vulnerabilities, social engineering - these words were used when I was in college, and they still exist today. The race between hackers and security companies is perpetual. Security is not a financial institution's core business, indeed it is a round the clock job which should be entrusted to companies like Network Box who make it their business to ensure the safety of our clients' data. The worst mistake an FI can make is to do something once and believe that's all it needs.

A Network Box is a perfect fit for the perimeter security of small banks with its low total cost of ownership. Furthermore, our clients are pleased with our commitment to helping them meet their regulatory scrutiny by having achieved SAS 70 Type II attestation. Network Box logs and reports have met IT examiner's needs at both State and Federal levels.



Pierluigi Stella is CTO of Network Box USA. An experienced IBM Certified Senior Consultant, Pierluigi has more than 15 years of international experience primarily in the oil and manufacturing sectors. With a sterling track record of successfully accomplished projects, an extensive technical know-how, and three years as head of both the technical as well as customer service divisions of Network Box USA, Pierluigi has been helping financial institutions and health care providers develop their security policies, and has accumulated extensive experience and knowledge of security issues. He is one of the founders of Network Box USA. Pierluigi graduated magna cum laudae with a Masters in Electrical Engineering and has received numerous industry recognitions for notable career achievements including 2 Excellence Awards for innovative design.