

Don't Get Suckered By Lemons

By Andrew Plato, CISSP, CISM, QSA
President / Principal Consultant
Anitian Enterprise Security

One of the more frustrating aspects of working in the security industry is the proliferation of what I call "Security Bricks." These are security appliances or technologies that are, for the most part, useless. They offer limited or very rudimentary protections that do little to safeguard an organization. Typically, these products are bought merely to assuage some auditor.

Bruce Schneier has an excellent essay on this concept. In his article he calls these products "lemons." You can find this story at:

http://www.schneier.com/blog/archives/2007/04/a_security_mark.html

Knowledge Gap

The core problem with most security technologies is the discrepancy in knowledge between buyers and sellers. Sellers tend to know which products are lemons and which ones are decent. Buyers, who are not immersed in information security night and day, are at a significant disadvantage. As a buyer, you do not know which products are good or bad. As such, buyers must rely on comparisons, product certifications, word of mouth or the advice of a technology reseller.

Unfortunately, most of these evaluation methods are flawed. Many certification labs will certify anything for a price. Magazine shoot-outs always favor the manufacturers who are also large advertisers. And don't even get me started on the problems with resellers. Most resellers are simply desperate sales people trying to pawn off goods on the next sucker.

Which leaves word of mouth, as the remaining evaluation method. Oddly enough, this is the most effective way to evaluate a technology. The insights from other experts and users can often tell you a lot more about a product than any marketing brochure or product shoot out.

Collaboration is Key

This is why it is so important for security practitioners to collaborate and exchange ideas. When security practitioners can get together and talk technologies and solutions, they are much more likely to zero in on effective and useful methods and products.

However, even collaboration is difficult as well. Security people need to break out of the mentality that sharing is bad. Sharing is good. Sharing ignites critical thinking. When you share ideas, it forces you to re-evaluate concepts and ideas.

It is unfortunate that many of the security related groups and professional societies are openly hostile to technology discussions. I understand their fear. They worry that technology manufacturers will use the groups as marketing events to merely pitch products. This is easily handled with a modest amount of oversight. I wish these groups would re-evaluate their positions on technology presentations.

Nevertheless, there are some good venues, either on-line or in person, to collaborate with other experts. SecurityFocus, for example has some excellent forums. I have found that visiting vendor forums can yield a wealth of information about the capability (or

ANITIAN

ENTERPRISE SECURITY

stupidity) of a manufacturer. There are also numerous user groups and conferences to attend. The Interface events (www.f2fevents.com) are, in my opinion, one of the best technology-related trade shows available.

Whatever venue you pick, remember that the more you share, the more people will share with you. Remember to share not only your frustrations, but also your successes. Your recommendations and insights may help others. And likewise the insights of others can help you avoid the next security lemon.