Naked emperors and room-elephants

It's no wonder security is hard to get right - budgets are tight, workloads are overstretched, and everything's getting more complex. Employees and customers want access to data and applications from anywhere, on any device, at any time. IT is a commodity, and everyone tries to do the same with security, or bundle it into magical 'products' and 'appliances'. Result: constant, massive security breaches.

The problem is not necessarily that security products don't work, it's just that they don't work the way you need them to.. While spending money on security products year after year might be considered 'doing something', when your threats are no longer simple viruses, firewalls and antivirus software are protecting you from threats that don't matter. If nothing else, it's worthwhile considering whether you should do security a little differently, so let's look at a few examples of how security isn't working and what might help.

APTs

"The difficult thing about APTs is that they exploit employee knowledge gaps, process weaknesses, and technology vulnerabilities in random combinations," he [Jon Oltsik, ESG senior principal analyst] said. "Patient, well-resourced, and highly skilled adversaries take their time to figure out where we are most vulnerable and then use this knowledge as a weapon against us."

- Advanced Persistent Threats Get More Respect, InformationWeek, Feb 2012

The method of compromise in almost all recent high-profile attacks has been the 'Advanced Persistent Threat', which is fairly simple to describe: individuals, teams, or even nation-states want something from you; they target you; learn how to manipulate your people, technology and processes, and achieve their ends. They use stealth and persistence: cycles of covert, deep reconnaissance coupled with security issues gets them from the outside to what their goal is: your sensitive data.

Whilst not a new method of attack, it's definitely used more frequently, and will probably get worse, as the increasing rate of eye-catching headlines suggest.

Social Engineering

The hackers who broke into EMC's RSA Security division last March used the same attack code to try to break into several other companies, including two U.S. national security organizations … [t]he RSA hackers broke in using a basic social engineering attack. They sent an email that looked like it came from an RSA partner, online recruiting firm Beyond.com, with the simple message, "I forward this file to you for review. Please open and view it."

- RSA spearphish attack may have hit US defense organizations, Networkworld, Sep 2011

Social Engineering is a modern take on the 'con job': Attackers manipulate personnel via email, phone calls, or even in person, to get information or perform some action that gets them a foothold in your organization. As part of high-profile 'APT' attacks, it's usually coupled with passive reconnaissance, malware, and zero-days[1], in a coordinated campaign. The RSA attack was a perfect example: masquerading as a recruitment firm, sending plausible and legitimate-looking email with spreadsheets containing data of interest, plus a little extra on the side.

[1] Previously-unknown or non-public security holes in programs

And as with APTs, this is becoming more of a problem, not less, as time goes on.

Security as a Commodity or Blackbox

The problem [with AV] is that most criminals are smart enough to test their attacks against popular antivirus products … it's common for them to completely evade antivirus detection … White Hat's Grossman agrees. "I think we overspend on the wrong security products", he says. "Particularly antivirus. I think we overspend on firewalls and antivirus"

- Is Antivirus Software a Waste of Money, Wired, Feb 2012

Attackers are not static; they are intelligent adversaries, which means that security issues are less like acts of nature and more like the influenza virus. They evolve rapidly, to test and eventually breach at least some part of your organization. Like a virus, deploying a vaccine may protect against a particular strain, but what of the next strain that evolves and adapts? Antivirus products worked against signature-based attacks, but attackers evolved to understand that defense and bypass it. The same happened with firewalls.

Targeted, custom attacks such as seen in APTs are the next front in the battle, and the questions you need to ask yourself are: what do you have in place to defend against those, and how much money do you want to spend on 'old' defenses as opposed to newer, more effective ones.

Too Much Information

The majority of IT and business professionals in large companies are no more than somewhat confident their security systems can detect a threat before it becomes a real problem, a study shows

- How security pros are handling data overload, CSO Online, June 2012

Like the surveyed organizations, you're probably missing something, either because you don't know what you have, or you don't have it. You could always add more devices, and new-fangled correlation systems, but that increases the complexity, and you *still* don't know what you're missing. Attackers know this - that's why they were able to compromise companies that had all these security controls and more.

Put another way, if you can't measure or test your security, how do you know what it's doing? Are you buying snake oil?

Seeing the Light

Most security products are based on the idea that threats are generic, widespread, undirected, and blindly automated. The reality is almost the opposite: your attackers are not mindless programs, but intelligent, motivated human beings, so you should bring the intelligence back into your security. But talk is cheap. You need to challenge yourself by replicating attacks as attackers would and seeing what happens. Let's look at a few things that will help you to *do things right*.

Scenario Planning and Adversarial Modeling

After understanding what your threats are, you need to understand what your attackers will do, and:

- what assets do others want
- what will attackers do to get them
- when and how long will it take

Adversarial modeling is the *who* and *what* aspect, whereas scenario planning is the *how* and *when*.

The first thing to do is classify and value your assets, then to assess your current exposure, coupled with threat intelligence

reflecting the capabilities of your adversaries and their level of skill.

With that, realistic attacks, including likelihood, timing, the effect of multiple attack vectors, stealth, and other factors can be considered and the information used to improve other testing.

Red-teaming

While more focused efforts such as role playing, announced tests, and normal penetration tests can provide some defense, red-teaming is conducted by the military and government for a reason: they replicate skilled adversaries and significant attacks.

Traditional 'logical' security assessments aren't as effective because they don't integrate physical attacks such as social engineering or breaking into sites. Given your attackers will be doing anything they can, in the physical or logical realms, red-teaming is the solution that provides the most insight.

Containment and Isolation Testing

Even the NSA thinks it's been compromised[2], so it's best to deal with it. Understand how you can identify, contain and minimize damage before it happens.

To accomplish that, you need to understand your environment, your business and security processes, and what controls would be involved in attacks.

Then, it's all about the testing. Do defenses work under attack, or do they make things worse? How long do they withstand attack – long enough for you to react? If not, you probably already have a problem.

[2] http://www.eweek.com/c/a/Security/NSA-Assume-Attackers-Will-Compromise-Networks-395027/

OccamSec can help

You'll never solve a problem if you don't understand it – security is a prime example of money and time being spent poorly, resulting in constant breaches. OccamSecs mapping of activity description to service summarizes things nicely:

Activity	Service
Think about who your attackers are, what they want, and how they might will try and get it.	Scenario planning and adversarial modeling
Simulate those attacks	Red-teaming
Test how quickly you can detect, isolate, and eradicate them	Containment and isolation testing

We've helped many organizations improve their security through each of these, and we can probably help your organization, too. Talk to us if you want to do security right, and avoid being another news headline.