Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

The Bottom Ten List - Information Security Worst Practices

Worst practices

In the information security space, there are many valid approaches to protection. But some of the approaches in use today are not, will not be, and likely never really were effective, while at the same time, cause failures, are expensive, or otherwise do more harm than good. There are many of these things, but only so much time and space - so here is the bottom ten list:

Change your passwords - how often?

When there is a rule that says passwords must be changed every (define the time frame), it is almost never justified by any actual analysis and has no real basis. This whole notion stemmed from cryptographic systems and assumptions that are almost never valid for passwords. Here's the problem. If they don't know the password, there is no reason to change it. If they do, how much damage can they do between then and when you eventually change it? The right answer is - in essence - no regularly scheduled password change makes sense. For more details, see: http://all.net/journal/netsec/1997-09.html

Use reverse DNS lookup to authenticate a source

Many security mechanisms are configured to do a reverse DNS lookup to "authenticate" the source of an email message. For example, if my mailer declares "HELO all.net" (which is legitimate) and the packets come from an IP address that does not indicate as all.net when your firewall looks it up, this does not indicate that the message or its origin is illegitimate in any way. People running firewalls using these rules will find that they eliminate large numbers of legitimate messages, prevent legitimate users from legitimate uses, and get complaints from their users (unless their users are too scared to complain). This and innumerable other such things do not make you more secure, but they do cause failures to communicate.

Attack back - it's self defense

No it's not. Unless you are a military or intelligence organization sanctioned for the activity, it's likely illegal. But even if it were legal, the best defense is not necessarily a good offense. Two wrongs do not make a right. Be careful what you escalate, because you likely have more to lose than they do. Besides - how do you know how skilled they are or how far they are willing to go? But rationalization aside, attacking others is almost never defending yourself.

Let the user decide about technical matters

I have asked hundreds of folks who design and implement security products what the right answer is to a pop-up box from their product alerting the user to some real-time condition. Not one of them knew the right answer without asking a whole series of questions. If the expert who designed the thing doesn't know the right answer, how is the user who did not design it supposed to make the right decision? I can't, you can't, and nobody else can! So stop asking.

We can pull the plug if there's an incident

Yes - believe it or not - there are still people who believe they can simply "pull the plug" on their information infrastructure. Now, of course, there are exceptions - and I have systems that fall into that exception. Like the computers in my museum that aren't used for anything or connected to anything else. But for the most part, we live in a highly interconnected and interdependent computing environment, and when we pull the plug, we lose more than the attacker is likely to be able to gain. Unless we plug back in pretty soon, we continue to lose.

Use the number of vulnerabilities detected as a metric

I cannot tell you how many organizations I know that plug in a vulnerability scanner, measure the number of vulnerabilities found, and apply the result as a metric to measure their security program. And I cannot adequately express how useless and problematic I think this is. But here are some of the reasons not to do it; (1) The actual number is meaningless (suppose it's 250,000 - what use is it?) (2) Relative values of the number are meaningless (suppose now it's 300,000 - what use is that?) (3) Once you identify a vulnerability, you have potential liability for not fixing it, (4) All vulnerabilities are not equal, so now you need some sort of weighting system. The mechanisms to do that are expensive and the resulting "weighted" number is also meaningless (suppose the weighted number is 75,000 - what use is it?).

Trust vendor security claims (the last defense you will ever need)

Believe it or not - people tasked with making decisions about security actually believe vendor security claims. The one I liked the best was one from a few years ago that went "The last defense you will ever need" - which I take it to be a true claim. If you buy things that have advertisements like this, you are almost certainly going out of business, and then you won't need any more defenses! Which reminds me - I have this swamp land in Florida for sale ...

The NSA bought it (uses it) - so you can trust it!

This one comes up every few years. First, the NSA likely buys at least one of every security product in widespread use - so they can figure out how to get around it! Second, the NSA's job is to gather intelligence, and it has been widely and wisely asserted that the best system for them is one that only they can break into. Third, if the NSA uses it at all, they aren't likely to tell you or me what they use it for - it might be a really good doorstop or a sample they use for testing electromagnetic pulse weapons. And in what world did you come from that made you believe that you (unless you are the NSA) need the same security as the NSA? The list goes on, but this item does not...

We use "best practice"

And what practice exactly is that? Why is it you think there is no other practice that could ever be better? In reality, there is no such thing as "best practice" in information protection, other than perhaps using someone who knows that the use of the term "best practice" is at best a dodge used to excuse whatever you decided to do. Most things I have seen that are claimed to be "best practice" are more like minimally acceptable practices. It may be best practice to claim best practices to your management because they don;t know any better, unless of course they read this article. Better hide it!

It's for your security

How exactly does it make me more secure when you search me? Searching me is not for my security at all. Searching you may be for my security, but that's a different matter. And how does giving you more of my personal information so you can ask me about it later make me more secure? It doesn't! In fact, banks make these claims all the time nowadays, but it's ridiculous. If you can't keep my password safe, what makes you think you can keep more of my personal information safe? And if you can keep my personal information safe, why do you need anything more than a password?

BONUS ITEMS!!!

Yes, that's right! There's room at the bottom! Exclusively here at **Fred Cohen & Associates**, we deliver more foolishness than we promise! We've reached ten, but the page is not yet full!!! So in case you don't agree with a few of the above, here are some replacements.

We trust our people, so we don't need insider defenses

I trust my people too, but that doesn't mean I don't defend against them. The best available facts, and many years of experience, show that insiders are involved in the majority of losses from information-related attacks (typical figures run the the 75%-80% range). Of course today, we have Bernie Madoff to tout as the consummate insider doing wrong for years. But this is only the tip of the obvious iceberg that has dragged down the global economy.

We pay people a lot to assure their loyalty

Of course it turns out that the highest paid people are the most likely to commit bigger crimes. And loyalty does not come from money anyway. It comes from social commitment to a group, which is something that money does not bring.

"We know how to secure the Internet" and other such foolishness

This is actually a direct quote from a representative of a major vendor at a professional forum. I was there and wrote it down as it was said - and it is also on videotape. The point I am trying to make is that lots of people say lots of foolish things, and many of them get away with it because they are not challenged. Listeners assume that speakers invited to speak in a professional forum know what they are talking about, particularly when the audience is not full of experts and the speakers are asserted to be experts. My point is that allowing such foolishness to pass is a failure to be diligent in your security practices.

Summary and conclusions

I have now blown what could have been a year's worth of analyst newsletters in one shot. But fear not. There are plenty of other things to talk about, and plenty of other security practices and claims that could fit on the bottom of the security barrel.

The real bottom line of this article is simple enough. Those of us in the security space have a responsibility to our profession and our societies to challenge bad practices and to do so in a way that helps to eliminate them. Keeping quiet will not stop foolishness. The bottom line is:

Speak out against bad practices or we will all suffer under them!