Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

The Bottom Ten List - Information Security Worst Practices – Getting Even Worse

Worst practices – year 2

A year ago, we published the bottom 10 list of information security worst practices in the hopes that things would change for the better. So here we are a year later... let's see.

Don't write down your passwords – who are they kidding?

When people had only one computer that they accessed from one physical location, they could remember their password and not write it down. But today – that ship has sailed. I recently did a bunch of updates and found that I have access to various accounts on about a hundred systems, most owned and operated by people I don't know or particularly trust or distrust. That means that I have to have different passwords to fend of the risk aggregation (see below) of any of them doing bad things and effecting others of them. For some reason, I find it hard to remember and associate a hundred different user identities and passwords, so I "write them down" - in combination of password management systems of various sorts. So stop telling users not to write them down and start helping them do it in a safer way.

Risk aggregation – it's far too theoretical to think about in our programs

I even wrote my New Year's article about it this year. And of course, I just discussed it a bit in finding ways to keep track of passwords. The other side of the password risk aggregation is that if you don't use the same password from place to place, wherever you write them down becomes a risk aggregation point at which they may all be exposed. So you have choices: (1) put all your eggs in one basket and protect the basket really well, (2) put one egg in each basket and have lots of baskets (which you then have to deal with), or (3) use different baskets for different groups of eggs and protect them commensurate with the risks. Obviously I prefer option 3. Find a mix of risk management approaches keep track of them, recognizing that the cost of risk management limits the extent to which this can be done for low risk items but watching out for the aggregation of low risk items into high risks. Revisit your decisions periodically with shorter periods for higher risks.

Leaking – it's the ethical thing to do

I generally support the notion of whistle blowers – when there is a crime – to the proper law enforcement officials. And I generally support public disclosure of vulnerabilities – in generic form – with examples that can't be directly used to launch an attack. But this has been a year of massive leaks, many of which, in my view, don't fall into the "responsible" category. Many people have been highly supportive of leakers – and that's fine – but some have launched denial of service attacks against companies that cut off leaker accounts – trying, in essence, to extort various companies and governments to gain what they want. The notion that anarchy is preferable to government over-reaching takes hold at some point, but that point has not been reached in the leakage arena. Ethics in security are not simple and there are many viewpoints that deserve attention. But harming others is almost always on the wrong side.

The law doesn't apply to me – I'm in security

This plays into the last issue – but the problems run a lot deeper than simply launching denial of service attacks as a protest. I have been to several conferences and similar meetings over the last year in which security researchers have described their interesting approaches to achieving improved protection and discussed how they have put these into action. The talks are quite interesting, but when I ask them about why they think they are allowed to break the law, they seem to be befuddled by the idea that the law applies to them. We have the folks who think they can intercept real-time communications and put up deceptive computers because they are trying to catch fraudsters. Of course they also catch others in their nets and there are laws about wiretapping and frauds that they themselves acknowledge they are breaking. Then we have the folks who are taking authentication data and credit card information from people and then telling them that they were about to be defrauded – but that since they are the good guys, it won't happen. It turns out there are also laws about possession of access devices – like credit card details and user IDs and passwords. The list of criminal acts by so-called security folks goes on and on, but the excuse remains the same – we are the good guys so it's OK for us to to break the law. No it's not!

Let's use more surveillance to solve it

It seems that people who are unwilling or unable to do a better job of deter, prevent, detect, and react, have decided that rather than try to be competent in these areas, they will simply surveil everything and go for prosecution when they find things they don't like. Eternally increased surveillance is the hallmark of failed security, and we are seeing it more and more today. It relates to a long-time strategy of increasing punishments to deter crime – but of course neither strategy deters crime, they just make non-criminals more afraid, suppresses dissent, and drives the real criminals to better and better methods. I think that surveillance is fine, in appropriate measure and in appropriate places. But moving to the surveillance society seems to me to be problematic for all sorts of human rights and dignities. Whether it is being viewed nearly naked in and airport scanner or being patted down in the genitals by the guards the outcome is harmful to all parties. It harms the folks doing the searches as much as those being searched. At some point we are simply abandoning all notions of trust and becoming entirely cynical as a society. And at the end of the day, this signals the end of the social contract. The bankers see it – the politicians see it – and eventually the people will get it.

E-discovery will take care of our legal obligations

It might if it were a sound discovery process, but it's not. Long ago, the government sued IBM for antitrust, and as the story goes, in the discovery process IBM printed out all of their corporate communications over the relevant period and filled an enormous warehouse across the street from the justice department offices with the results. The DoJ ultimately had no way to search it all and find the needles in the haystack that might have made a case. Today the data has to be provided in searchable digital form – and can typically be required to be in the same form in which it was originally stored. The emerging e-discovery process and business is about finding the needles in the haystack. But to understand the legal issues for relevancy, people have to read the material and understand it in context. And that's what the e-discovery process today does not do. It may be faster and cheaper, but it's not better. Don't bet that a search engine meets your obligations to provide relevant records. The bet may lose big time.

We use return on investment as a security metric

I still read posting after posting telling me different ways to compute the return on investment (ROI) on security, and I still shudder to imagine the security geeks trying to come up with the magic numbers required to get executive management to give them their security budgets. It's all based on some sort of risk analysis – which has been well characterized in the past as a guess multiplied by an estimate taken to the power of an expert opinion. But as if that wasn't bad enough, we now have to call the costs investments and expect a positive return in excess of the ROI on improved sales efforts. I wonder with the ROI on the CEO is. If we replaced the CEO with someone who was paid half as much, would we have less or more profit? And by how much? And the ROI on anything like roads is just terrible – unless you consider the long-term indirect effects which are not quantifiable. I know – let's put all on reputation – the return is in maintained and improved reputation – which we can take as the total valuation less the real property and cash on hand. Gee – the company is capitalized at a 20-1 PE ratio, so 95% of the value is in the reputation, which is the return on information protection (it would be lost if not for the protection program – so it is all accrued as a benefit to having the program). That means that we need a security budget of 18 times total earnings for an ROI of 20%...

Nobody would ever want to attack us

Believe it or not – I still hear people tell me that nobody would bother to attack their computer. It has long been the case that automated attacks will go after any computer connected to the Internet, and yet I still hear people telling me about how they are safe because nobody would bother to attack them. Hello!!! It would be a great inconvenience to try not to attack you with current attack technologies. It's no bother at all to attack your computers – just part of the overall service criminals provide to each other – no extra charge. Anybody who does a threat assessment and comes to the conclusion that they don't have to worry is either not dependent on anything on a computer or missing something big. Everybody is under threat today.

The cloud will save me

We just moves our Web servers and email to the cloud. But we don;t have the misimpression that the cloud makes us safe. In fact, it's a complex tradeoff that we evaluated for a good long time before making the move to a trusted provider. The things we looked at included operational costs, long-term outages, email hosting factors, functionality differences, integrity and availability issues, use control, accountability, data center controls, performance impacts, business focus, confidentiality issues, and short-term outages. We moved some things but not all of them. The truth is, the cloud will not save you, but it might be a good tradeoff for some commodity items in some business models. But like anything else, security has to be closely examined – in the clouds as anywhere else.

We use "best practice"

This remains the worst of the worst practices... because we still don't know exactly what practice that is. In reality, there is no such thing as "best practice" in information protection,but there are reasonably sound practices. We see increasing standards and efforts in many areas to bring reasonable protection into widespread use. Decision-making has been codified in more and more books, analytical frameworks, and reference architectures. But the best practice is and has long been to get the best experts and listen to them. If you can find them...

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.

My company has the best security experts – we don't need any help

Actually – mine does... or so the claims must go. Getting the best experts is always a problem because it takes one to know one. But interestingly, the courts have a way of sorting this all out when they determine who is qualified as an expert witness. They look at knowledge, experience, education, training, and skills – in the specific areas related to the issues at hand – and the more of more of them, the better. So taking pride aside, when you look at a security issue that's important, using your internal expertise is great, but it's a good idea to bring in an outside expert or two in the specific area of import to the issues at hand. That means identifying an individual – not a company – that has the proper:

- **knowledge** as evidenced by their published and peer reviewed works,
- **experience** as evidenced by the specifics of what they have done before as attested to by those for or with whom they did them,
- **education** as evidenced by degrees from appropriate institutions,
- **training** as evidenced by certifications from credible training programs, and
- **skills** as evidenced by historical examples,

all in the specific areas at issue in the matter at hand. That's 3 times I've indicated the specific area at hand, and it's worthy of note. Information protection today is too large and broad a subject for any one person to know all there is to know, and that has been true for a long time. As good as your expert is, they don't know everything there is to know, and neither do any of our experts. When good people focus on difficult issues for a long time, they usually gain understandings that others don't have, and that can be leveraged to advantage. That's what you should be looking for, and if it costs a lot per hour, consider the time it took to get there and compare it to spending the time and money for all of those hours for your internal experts.

The new "advanced persistent threat" (apt-ly named)

In 2010, I heard a lot of hyperbole about the advanced persistent threat – as if that were something new. The "apt" threat is a breakthrough in marketing security. There are actually a lot of different threats (actors – individuals or groups) that are increasingly advanced and have long been persistent. These include, among others, threat types like fraudsters, insiders, industrial espionage experts, organized criminal groups, professional thieves, customers, competitors, and nation states. These sorts of threats have existed for a long time, and they will continue to exist for the indefinite future. They are nothing new, and if you weren't aware of them before, it's because you weren't looking at the issues. What is new is the use of the apt term to describe these threats – it makes a lot of sense to management – I guess. But lumping all of these threats together is also problematic, because it also lumps together our approaches to dealing with them, and that means allocation of resources less aligned to the specifics of the situation. While finer granularity is not always needed – it often helps.

Security theater and security through obscurity are bad things

I have been more or less properly quoted as having said that there are really only two types of security; (1) physical security and (2) security through obscurity. While I have had many discussions on this point, none have really moved the ball. Some claim that the definition of obscurity doesn't include keeping cryptographic keys or passwords secret, but if people knew what they were, protection would likely fail. Some claim that it's only obscurity if you know it is a vulnerability and let it go unmitigated because you think nobody will figure it out, but there are lots of vulnerabilities that go unmitigated that have nothing to do with whether anyone else can figure it out. Security theater is another way of saying that appearances are used to deter threats, and of course this has always been true. In the animal kingdom we see all sorts of displays intended to stop predators from attacking, and they work. In human personal interactions, we see lots of posturing, puffery, and bluffing, and people often do back down. When someone threatens you with a gun that happens to be unloaded, it's security theater, and you how many of you will decide it's worth the risk of testing it out? Security theater works unless and until someone points it out in detail, and even then it still works, albeit a bit less well. Pointing out that security theater is in use in specific instances and with particulars is just like publishing details of any other vulnerability. Do we really want to live in a society in which we have really effective physical security at all places at all times? I don't think so, and I bet if you thought about it for a bit, you would agree.

Summary and conclusions

In the information security space, there are many valid approaches to protection. Worst practices are our way of pointing out the biggest differences between what's popular in the field and what may actually work. Can anybody really remember and properly associate 100 individually obscure and different in every reasonable way user passwords? Should you really put all those eggs in one basket? Does leaking secrets really benefit society more than it harms it? Does being in security really exempt you from the laws of our society? Will more and more surveillance really make us safer, or will it merely make us more susceptible? Will electronic discovery automate an essentially human process, and if so, when will computer vision be ready for prime time? Can you truthfully tell me with any reasonable degree of certainty or accuracy what the return on investment is for any particular security mechanisms or even the whole program? Does anybody really think that criminals avoid targets that are insignificant or know or believe before attacking that your systems aren't worth it? Do you really believe that trusting others with your most precious information makes it safer? And do you think that just because people claim that they are using “best practices” that the practices they are using are better than any others – or even widely accepted by real experts? Does your company really have the best security experts in every aspect of the field? Do you think that the advanced persistent threat is anything new other than an “apt” name? Do you believe that security through obscurity is a bad thing and are you willing to completely abandon it in your enterprise?

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!

