State of the Hack – 2014

Almost twenty years ago I attended the 2600 HOPE hacking conference at New York City's Pennsylvania Hotel. Fast forward to the present, and I oversee a company that provides computer security solutions to multinational organizations and sovereign governments. Our clients frequently begrudge having to expend time and revenue for such services. This refusal by organizations to acknowledge the reality of their situation often perturbs security professionals. Experienced security professionals, however, cannot help but feel somewhat guilty. Those young hackers from twenty years ago were in large part responsible for the computer security situation that we face today. It might be fair to say that we brought the current computer security circumstances upon ourselves.

Back in the day (as we sometimes refer to a couple of decades ago) groups of bedraggled young men (sorry ladies, it has been almost exclusively a men's club) would congregate in shopping malls and outside retail establishments sharing and comparing the latest vulnerabilities, exploits, and compromises. We seldom if ever conceived of or concerned ourselves with (or at least I don t ever recall it being openly discussed) rogue nation state actors, state sponsored hacking, government corruption, organized criminal activity, or any of the plethora of real threats that corporations and governments face today. We impressed ourselves with our nimble and sometimes grandiose efforts to subvert and circumvent the poorly conceived attempts to restrict us from the early computer systems that we perceived as being owned and used by people of lesser merit and lesser intelligence. We were young, arrogant, competent, and unrepentant. Moreover, we were naïve.

Fast forward to today, and client organizations continue to be under constant attack from competent adversaries. What were real threats to security twenty years ago continue to be real threats to security today. Global businesses and sovereign governments remain just as vulnerable (if not more so) to attack and compromise of their intellectual property as they were twenty years ago. This situation continues despite those organizations employing tens of thousands of so-called 'security professionals' (many of whom have no business performing such tasks) and spending billions of dollars on so-called 'security solutions' (many of which are either non-functional or improperly deployed). Perhaps because of excessive costs or perhaps due to a fundamental misunderstanding of the role of technology by engineers, businesses and governments are not responsive to those real threats and seldom if ever undertake he necessary steps to protect themselves against those competent adversaries – except in cases or regulatory compliance requirements or, more significantly, after a breach.

Pundits can debate the reasons for the lack of response to emerging and ongoing security threats. Rather than go down that road, it seems more useful to take this opportunity to deliver an overview of observations and suggestions for the security landscape that awaits us in 2014.

We hope that some of these observations will provide adequate evidence to permit competent security professionals to make a case to their business counterparts to respond to these real threats before their organization finds itself in the unenviable position of having to respond to a very public, and very costly, breach.

Until then, best wishes for a safe, happy, and prosperous 2014!

Gregory W. MacPherson, President
Constellation Security LLC

Threats and Observations for 2014

Vulnerability Half-life

Despite the prevalence of attention to "advanced persistent threats (APT)" there continue to be a slew of compromises caused by lesser-known and more prevalent exploits. Cross-site scripting, cross-site request forgery, SQL Injection, local program exploitation, and plain old weak passwords have been the causes of more number of compromises than the vaunted APT attacks. Spear phishing, watering holes, and a variety of Microsoft DLL vulnerabilities are all valid attack vectors to guard against, but the emphasis on certain vulnerabilities have produced a mindset in corporations and governments that equates to 'blacklisting'.

Vulnerabilities in government and corporate infrastructures continue to exist for reasons ranging from plain old unwillingness to invest in technology to lazy business practices ("That's mission critical, we cannot patch that!") Preparing for or responding to every potential threat is both impractical and unnecessary.

Stop thinking that the advent of "Patch Tuesday," an ATO, or being certified with some compliance requirements means that your infrastructure is secure against the most recently discovered and published threats. Gain the credibility of your board or superiors to justify the expenditures on you and your improvements to align the infrastructure with the goal of allowing the organization to perform while maintaining a security posture that protects their investments.

Start thinking about security with a proactive posture, focus on identifying and strengthening the security posture of your organization. Require your engineering team to explore below the surface for significant issues such as services running on internal appliances, back level services running on internal appliances, performing detailed monitoring of traffic on individual network segments, evaluating and verifying firewall and router ACL policies, and doing other proactive work to determine the areas of your security posture that require some attention.

Monitoring

While vulnerabilities continue to stick around far longer than their supposed 'patch dates', the next greatest weakness in computer security is the lack of real network monitoring. Governments and corporations spend billions of dollars on equipment and people tasked with observing, detecting, and cataloging real or perceived threats. The failure results from the same strategy as above, an attitude that dictates a 'black list' mentality to response.

Stop simply purchasing an appliance and sticking it on the Internet backbone, confident that everything traversing it in both directions is (a) normal, (b) safe, and (c) already supposed to be there. Few organizations actually make the effort to identify the protocols and paths that their network traffic ought to be taking so that they can spot traffic that is 'abnormal' or anomalous.

Start using the intelligent, skilled, and highly motivated (or not) staff to catalog what constitutes 'normal' network traffic on their enterprise networks. Network traffic analysis is a field that has been studied and written about extensively. Instead of just watching pretty graphs, detailing how much HTTP/S and mail and DNS and ICMP traffic was processed, examine what should be traversing the network, and take steps to monitor the traffic that contradicts what is expected.

Communication

The business of widget makers is…making widgets. That is probably why business people “don’t listen” when the CSO/CISO/CTO starts banging on the desk and declaring. “We’re screwed if the <insert adversary here> decides to paint a target on our back!” Business people speak one language – profit and loss – and they are not inclined to see how spending a ton of cash on a perceived revenue drain like ‘computer security’ does their bottom line any good.

Stop using fear, uncertainty, and doubt to buttress your request for several hundred thousand dollars for this piece of gear or that SaaS offering. Computer security professionals who take this approach are the wrong person for that position and they should consider updating their resume.

Start thinking not like an insurance sales person (AKA fear uncertainty and doubt) but rather thinking like a lawyer (preponderance of evidence). It is easy to collect the salient facts for the attacks in 2013 (try Infosecnews.org) and categorize those that affect your particular industry. Then make your case – this competitor got hacked and lost this much market share/stock price/revenue.

Blame the Lawyers (and the CFO)

In a litigious environment, organizations become risk averse, so they tend to make contractual agreements with various other business organizations to push the risk onto their business partners. The problem with that strategy is that it is not ‘security’ per se – call it ‘regulation’, ‘compliance’, or ‘CYA’ but it does not solve the security problem! What solves the problem is acknowledging that it is YOUR competitive advantage that you have to protect and starting to protect it. That means identifying it, securing it, monitoring all access to it, and being ready to pull the metaphorical plug when someone tries to get to it without adequate permissions. Only THEN should organizations and governments put into place the other paper safeguards which are, de facto, reactive and useless until after the proverbial horse and barn have escaped and burned respectively. There is a place for risk aversion but it is NOT a replacement for security, it is a compliment to an effective and well thought out security strategy.

Stop listening to the promises of the vendor salespeople, the compliance enforcers, the finance people, the attorneys, and the other naysayers in the chorus of business that work to avoid risks when the security discussion becomes the central focus. Companies and governments already spend huge amounts of money for supposedly skilled people and supposedly feature rich equipment to prevent unauthorized intrusions. Make it a priority that some of that money be spent in the initial planning and detailed analysis that ensures that those expensive investments produce returns.

Start listening to your CSI/CISO (who you pay a lot of money) when they advise you to rethink the design and deployment of your infrastructure in order to secure that precious competitive advantage that makes your business competitive or secures the integrity of your government. Make them gain credibility by requiring them to evaluate your infrastructure as a vehicle for facilitating communications among the various parts of your business. Have the well-compensated engineers specifically identify – by protocol and direction - the communications that should and should not be transiting the various network segments. Then have the engineering staff configure the network to permit that traffic, for both ingress and egress, consequently eliminating or identifying traffic that does not belong.

Denial is not a River in Egypt

Given the previous points, one would think it easy to make the argument. Wake up, people! The Twenty-First Century began with a bang (9/11) and developed into a crisis laden conflict driven ever-changing environment requiring ‘cyber security’ (how security professionals loathe that phrase). For businesses and sovereign governments, securing their position in this new frontier against competent adversaries is a REQUIREMENT. Sovereign governments, radical political movements, organized and opportunistic criminals, rogue nation states with political agendas, and curious and intellectually brilliant hackers are all banging on your front door, side door, and all of the doors of every other office, group, and organization with whom you do business. The number of automated attacks implemented solely during the time that it takes to read this report is in the thousands. A fundamental change in the attitude towards computer security – an acceptance that you *WILL* be compromised – is the starting point for businesses and governments to better protect themselves. Implementing strong perimeter security while tolerating weak internal controls or, worse, relying on ‘compliance and regulations’, is a strategy guaranteed to lead to defeat when (not if) a competent adversary decides to target your organization. The failure to acknowledge that not only can a network infrastructure be compromised but likely will be compromised is a failure of the organization to acknowledge reality.

Stop vilifying computer security as an expensive revenue drain in the boardroom. Security of the intellectual property of a business is just as viable as securing a brick and mortar enterprise with locks and gates. Failure to evaluate the security of your competitive advantage or the chartered government services that your organization provides is actively ignoring an integral component of your business model. In a competitive environment full of real threats and competent adversaries, all that it takes is one concerted effort on the part of the bad guys to completely compromise the integrity of your ENTIRE infrastructure to the point where your organization very well could either lose significant market share, effectiveness, or possibly shut down completely.

Start acknowledging that whatever you do whether it be business or government your organization has some ‘crown jewels’ or ‘keys to the kingdom’ that require security. Determine what needs to be secure, and what can be lost without significant damage to credibility. Then challenge your engineering staff to build the model to support the business needs using primarily the equipment and tools that you already have installed. Get the plans documented in writing, and require the engineers to explain (again, in writing) the theory and the implementation behind any improvements or changes.

Ignore the Threats at your own Peril

The year 2013 saw some of the most egregious violations of computer security in the history of the public Internet. The evidence in favor of securing and monitoring infrastructures is more than adequate. Engineers and their management need to start producing real results within a business context, and to do that business people need to identify what merits securing. Attempting to measure, identify, categorize, and detect anomalies in the entire network is both unrealistic and wasteful in the face of business realities. Discarding one technology for another does not solve the problem. Solving the problem requires that security professionals understand the network and the traffic it supports, then produce real measurements of what constitutes ‘normal’ so that aberrant network traffic becomes the focus of the limited security team’s exploration, observation, and research.