ON OUR RADAR

On Our Radar

By Nat Puffer

The fight to secure information is being lost.

This was at the center of a debate within In-Q-Tel's Infrastructure and Security Practice last summer. Every day we would hear about another epic breach of consumer data or critical company secrets. In an industry that uses analogies as a foundation, all of them have crumbled. The "castle perimeter" has crumbled. The "hunters" are not efficient enough to seek out the persistent and embedded foothold of determined adversaries. A 2013 article cited Mandiant as discovering a foothold in a network that went undiscovered for six years and three months.[1] The same article cited the average time from initial breach to discovery as 229 days. If this isn't an indication of critical systemic failure, I'm not sure what is.

On the other side of the argument, "losing" means something is lost, and implies that there's some idea what winning would look like. But what if we haven't really lost anything? Perhaps breaches and data theft, like power outages or rush hour traffic, are just part of living in the modern world. While the numbers vary for effect, Target was reported to have lost 40 million payment cards in 2013; Home Depot lost 56 million payment cards in 2014; and Anthem lost 69 million patient records in 2015.[2] Yet every time one of these breaches is announced, we go about our days like nothing has happened. We still use our credit cards at Target. We still use our health insurance. We've become accustomed to the idea that companies can't keep our information secure against a sophisticated attacker, and in some cases, even an unsophisticated one.

If we get substantially more out of modern conveniences than they cost us, how is that a loss? Stated differently, isn't instantly streaming movies to a tablet worth having to change a credit card number from time to time?

At the core of the tradeoff is that people on a day-to-day basis value convenience over security. We shouldn't be surprised that this extends to people who develop software; that security lags behind innovation. In 2011, Steve Yegge wrote a blog post at Google capturing this concept, and I cite this post frequently to demonstrate the nature of the information security problem. Yegge asserted that there are two competing forces as systems are developed. The first is how functional and useful the system is, dubbed accessibility. The second is security. Without any external influence, accessibility will always win at the cost of security. As stated in Yegge's post, "[D]ialing Accessibility to zero means you have no product at all, whereas dialing Security to zero can still get you a reasonably successful product such as the PlayStation Network."[3]

It's a strange coincidence that it was also a Sony breach that brought lapses in security to the attention of the general public. Was the most recent breach of Sony Entertainment a game changer? If you are an information security professional, your likely answer is a jaded "no." We have been here before. There was nothing extraordinary about the breach technically. The concept of nation-state attackers penetrating corporate systems has appeared in commercial penetration testing reports since 2004. The only change, if any, is the rate at which we have to respond to new threats with limited resources. If agility is defined as the ability

Without any external influence, accessibility will always win at the cost of security.

to minimize the time required to accomplish a different task, we're finding agility is critical.

However, if you haven't been living in information security or worried about operating system internals and the ways they can be exploited (i.e., the majority of people), your perspective may be that the Sony breach signals a major change. There is a wider awareness that system breaches aren't just about criminal gangs looking to steal credit cards anymore. There is a new world where countries use the Internet as a platform for attack or retribution. This was highlighted by the White House Press Corps asking the President directly about a computer breach of a private company, and being assured that appropriate action would be taken.[4] Similar questions have been echoed in board rooms and C-suite conversations across the country: How would we fare? What's at risk? What are we doing differently today given these revelations?

The next steps after those questions are even more interesting. If you believe that all the investment in current mitigation strategies has been working, something has changed and you need to adapt. If you think that all your investments have failed, it's time to change course. In either case, something needs to change. The constant stacking of security tools hasn't worked. The doctrine of Defense in Depth has to answer for its cost of complexity when measured against a lack of success. While we may not want to abandon the idea altogether, we need to adapt with a new way of operating. This will likely include variable response, situational awareness, and security orchestration.

Belief in Variable Response

Endless stacking of security safeguards is a flawed strategy and every asset cannot be protected equally. For a long time there was a belief that you could secure everything in a reasonably complex network if you put more resources and tools against the problem. This resulted in a limited staff chasing every possible indicator of compromise with equal veracity, which is exhausting. That exhaustion bore little fruit, which bred complacency. That complacency, over time, led to the very thing you wanted to prevent.

Going forward, companies will be faced with developing doctrine based on hard questions. What assets are priorities? Which systems would potentially be sacrificed for others? Is it okay to isolate and restore a user's desktop automatically based on a machine's determination of a threat? The user would lose his or her work, but you would limit chasing ghosts through the system.

At the root of this are questions surrounding "How?" How do I know what to prioritize? How can I create the maximum effect with the minimal resources? Developing a sense of situational awareness to focus operations will be critical in answering those questions.

Situational Awareness

Over the past year and a half, IQT has been tracking the rise of the private threat intelligence market. State of the Internet and Annual Breach reports have existed for a long time, but this space was something new. Vendors were looking to increase the rate and specificity of intelligence into something actionable, forming two camps.

The first camp produced finished products. These were full reports with in-depth analysis and attribution. Actors, campaigns, tools, techniques, and procedures are all tracked and discussed, with fun names created for many of them. There was a focus on attribution, which we weren't convinced would be useful for those without certain authorities. The fact that activity was supposedly part of a People's Liberation Army (PLA) initiative may be interesting, but the overall economics of a private company are more of a driving factor in dealing with China than an IT department's report for the CIO. However, as the Sony breach has raised awareness inside commercial enterprises, so has the

value of attribution. Understanding the larger context of "Who" is suddenly as important as "What" or "Why" even if prosecution isn't an option.

The second camp produced machine-readable Indicators of Compromise (IOC). This information was intended to enrich the detection systems within a network through a couple of mechanisms. First, IOCs could be fed into a central incident management solution. The goal was to correlate indicators like IP addresses with existing log data to determine if network traffic that would normally appear benign is something to worry about. The second use was to add IOCs to detection capabilities to search out new potential compromises.

Both are useful and have a place. We expect to see significant activity as vendors from one camp add capabilities from the other, collection biases in feeds are worked through, and infrastructure for delivery, consumption, and sharing is rolled out. The promise is that focus and prioritization will eventually result from the ability to put global context around local alerts. The reality is that it may be too early to tell if the intelligence is sustainable and provides efficiency, or becomes an overwhelming deluge of data. Ultimately, the indicators need to support and drive action in the organization.

Action Through Security Orchestration

Awareness without the ability to act is useless. Action that consumes all your resources is limiting. The ability to make decisions on the intelligence we have and act with minimal resources in a timely manner is the goal, but has eluded most complex IT organizations. Networks of sufficient complexity are typically built by several generations of employees using products from a number of vendors spanning years. Legacy systems, acquisitions, new initiatives, and day-to-day break-fix cycles consume any available time personnel might have otherwise put towards automation on a system-wide scale. Vendors have added to the problem with protection of their market share by limiting centralized management solutions to work only with products in their portfolio. Bring your own device (BYOD) policies and the Internet of Things (IoT) pile on even more complexity and amplify the problem.

Several third-party vendors are chasing this problem with fresh eyes. The core concept is more in line with a knowledge-based system or workflow management solution than something fully autonomous. Identify actions that are frequent and time consuming, streamline the decision making and sign-off process, and efficiently execute across the infrastructure. While limited, this ability to act, potentially in machine time, on identified threats that are based on a broad view and defined prioritization might begin to tilt the odds back in our favor. However, the ability to capture business process and maintain automation as vendors update their solutions and companies change their infrastructure has been the downfall of these solutions before. These solutions will succeed based on their ability to capture and keep pace with changes in doctrine and business processes.

Rebooting Cybersecurity

Perhaps we need to restart, building upon what we have with variable response, situational awareness, and security orchestration in mind. Doctrine and awareness enable action that can drive up the cost for the attacker by constantly removing their footholds while keeping the defender's resources relatively flat. Tracking, identifying, and attributing attacks changes the political landscape. If winning in this context means establishing a livable equilibrium, changing the economics and politics of the attacker may be a good first step. Q

Nat Puffer *is a Senior Member of the Technical Staff within In-Q-Tel's Infrastructure and Security Practice. He has led investments in network security, data storage, and cloud computing. Prior to IQT, Puffer was with Knowledge Consulting Group, where he was responsible for growing the Cyber Attack and Penetration Division. He previously held consulting roles with Neohapsis and Symantec. Puffer earned a bachelor's degree in Integrated Science and Technology and a master's degree in Computer Science from James Madison University.*

REFERENCES

[1] Lennon, M. (2014, April 10). *Just One-Third of Organizations Discover Breaches on Their Own.* Retrieved from SecurityWeek: http://www.securityweek.com/just-one-third-organizations-discover-breaches-their-own-mandiant
[2] Palermo, E. (2015, February 6). *10 Worst Data Breaches of All Time.* Retrieved from Tom's Guide: http://www.tomsguide.com/us/biggest-data-breaches,news-19083.html
[3] Yegge, S. (2011). *Stevey's Google Platforms Rant.* Retrieved from https://plus.google.com/+RipRowan/posts/eVeouesvaVX
[4] *Remarks by the President in Year-End Press Conference.* (2014, December 19). Retrieved from Whitehouse.gov: http://www.whitehouse.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference