the cyberwire

The CyberWire
621 East Pratt Street, suite 300
Baltimore MD 21202–3140
editor@thecyberwire.com
www.thecyberwire.com
@thecyberwire

NYC Cyber Summit

September 18-19, 2014 New York, New York

September 18

ThreatTrack's CEO Julian Waits opened the conference this morning and introduced the first keynote speaker, Jim Penrose, Darktrace's EVP for Cyber Intelligence.

Penrose took as his topic "the Enterprise Immune System," and sounded an increasingly familiar note. The old vision of cyber security — a walled city impregnable to attack — is obsolete. We need, he argued, a new organizing metaphor: we should conceive cyber security as an immune system.

Compromise is inevitable. People need to connect, interact, and innovate. The average time to detect a cyber attack is 243 days. When an attack is detected, that detection is often made and reported by some third party, not the victim. And only then do we react, cleaning up the damage.

This won't do, Penrose asserted. We need to get faster, because time is on the attackers' side. They're brazen and tenacious, constantly looking for moments of weakness. Their objective is usually the enterprise's data. And the enterprise needs to be concerned not merely about losing data, but also about the integrity of its data.

Penrose illustrated the problem by inviting the audience to consider the much-discussed advanced persistent threat (APT). What makes APTs advanced are big resources, laboratories, equipment, security products, and experts. You cannot expect security if you assume your users will always make the right decisions with respect to security. Advanced attackers will find and exploit users' mistakes.

To compensate for inevitable human weakness, we need, Penrose argued, to build a self-learning capability - a machine-learning capability for enterprise awareness. Specifically, we need mathematically enabled self-knowledge. Only a sound, probabilistic, and automated approach to enterprise security holds promise.

This approach is essentially an intelligence approach. Intelligence seeks to deliver timely indications and warnings, and risk management is the outcome of these.

The adversaries will adapt and evolve. We defenders need to adapt and evolve, too, and faster.

We'll be live-tweeting other presentations throughout the day. Watch the hashtag #cyberNYCSummit for updates. Tomorrow's CyberWire will include a comprehensive wrap-up of the summit's proceedings.

September 19

Following the morning keynote (described in yesterday's issue of the CyberWire) a panel addressed the challenges of "Securing the Human." Panelists offered sensible counsel on the need for buy-in, the importance of fixing executive responsibility and deploying metrics to ensure accountability, and the futility of checkbox approaches to inspiring sound security practices.

CrowdStrike co-founder and CEO George Kurtz delivered the afternoon keynote, "Hand-to-Hand Combat with a Targeted Attacker." The combat he described involved detection, response and remediation, and, ultimately, attribution – not hacking back.

© 2015 The CyberWire

Kurtz would take the Chinese attackers Hurricane Panda and Deep Panda as his case studies of advanced attackers engaged in highly targeted campaigns. Such advanced operators evade traditional defenses: they use little or no malware (in the strictest sense), little or no command and control, and leave no file-based artifacts. The advanced attacker, Kurtz noted, "wants to be you." They seek to gain and escalate privileges, and then operate as if they were one of your own.

The lesson he drew from this is that most enterprises don't have a malware problem. They have instead an adversary problem. To return to his two Chinese case studies, Kurtz described Deep Panda as very active across many sectors, focused on IP theft. Hurricane Panda, tracked since 2013, has focused on telecoms and tech companies. It specializes in webshells, an important tool in the advanced attacker's kit. In the summer of 2013, Hurricane Panda installed webshells on its targets and successfully maintained persistence undetected for one year.

Such elusive campaigns, Kurtz argued, are better detected by looking for indicators of attack — adversary activity detection — as opposed to the more commonly sought-out indicators of compromise. In the case of the Hurricane Panda attack, the victim couldn't figure out how the attackers kept getting back in (there was, after all, no malware). Once in, the attackers would dump credentials, then pass the hash to move laterally, or crack passwords. They also adapted: once we had found them, they changed their tactics, techniques, and procedures.

He concluded by predicting that targeted attacks would continue to grow in sophistication and stealth. He advised focus on indicators of attack: observe the adversaries' attack tradecraft, and then move to remediation. And remember, he said, the limitations of common defenses: what happens in a virtual container isn't necessarily what happens in your endpoints.

A panel discussion on social computing opened with general agreement that network boundaries were fading. Some disagreement over the efficacy of policy in modifying user behavior in social media was resolved with the conclusion that data were manageable through policy, but people could only be moved (imperfectly) through guidance. The panel showed considerable interest in social media's potential for identity management and authentication, perhaps replacing those familiar security questions — your pet's name? your junior high school? — they have done so much to undermine. Your social network, or your geolocation, could serve to help determine your identity.

Leo Taddeo (Special Agent in Charge, Cyber/Special Operations, FBI — New York) offered a law enforcement perspective. He deplored continuing unwillingness to disclose breaches: only 56% of companies notify the FBI of a breach when they're not required to do so by law. He also wanted to clarify, in brief, federal roles and missions in cyberspace. The Department of Homeland Security mitigates, shares information, and develops intelligence. The Department of Defense performs foreign collection, conducts cyber operations, and generally works in the cyber battlespace. The Department of Justice is responsible for attribution.

The final panel addressed threats to the financial sector. No one has any idea how many threat groups are out there, let alone what those groups are up to. Nation-states tend to commit cyber exploitation. Hacktivists tend to commit cyber attacks.

Eastern Europe, panelists said, is a leading source of threats, but Brazil is rising, and so is Africa (where rapid growth and weak governance combine to offer a crime-friendly environment). Exploit kits and denial-of-service (DDoS) remain common attack methods. DDoS is a particularly low-cost attack: we're seeing 100 Gbps attacks daily, 2-300 Gbps attacks aren't uncommon, and some believe we've even seen Tbps-range attacks.

Unpatched systems remain a source of commonly exploited vulnerabilities, with poor network hygiene a problem at smaller, under-resourced enterprises.

Nation states represent some of the most capable attackers. Unlike the smash-and-grab cyber criminals who want to get in, get out, and monetize their take quickly, national cyber services opt

© 2015 The CyberWire

for complex, difficult to detect, and mitigate persistent attacks. China's attack on NY Times was a watershed — the Chinese service was embarrassed by its outing, and moved to more sophisticated attacks.

Much of a CSO's budget, unfortunately, goes to compliance as opposed to defense, and mere compliance is poor defense against the more sophisticated, multi-vectored attacks we're seeing.

The panel thought that the recent JPMorgan hack should offer an instructive use case, especially as boards in the financial sector grapple with cyber risk. Panelists urged the community to develop some communication paradigm that enables cyber attack disclosures to be unmediated by lawyers. FS-ISAC is a step in the right direction, panelists thought, but it generates so many alerts that you've got to dedicate people to reading them: valuable, if you've got the resources to consume what FS-ISAC produces.

In response to questions about pricing in cyber risk, the panel said that companies tended to pay enough for insurance to mitigate catastrophe, and then self-insure the rest. Sustaining a breach tends to induce budgeting for security in the next cycle, however, not as a cost of doing business but rather as a cost of saving the business.

Deborah A. Snyder, Acting CISO, New York State Office of Information Technology Services, Enterprise Information Security Office, closed the conference with a keynote that described interstate cyber security cooperation and the cyber support that the state provides to businesses and citizens.

the cyberwire

editor@thecyberwire.com
www.thecyberwire.com

@thecyberwire
+TheCyberWire

About The CyberWire

The CyberWire is supported by CyberPoint International and its community partners. We invite the support of other organizations with a shared commitment to keeping this informative service free and available to organizations and individuals across the globe.

Revised 8.4.15

© 2015 The CyberWire