EVOLUTION TO A MORE EFFECTIVE DEFENSE: PREDICT. PREVENT. PERSIST.

By Carlos Fernandes, CEO, Agile Cybersecurity Solutions

We continue to read news reports of nation-state sponsored cyber activities, targeting U.S. public and private sector organizations, allegedly from Russia, China, Iran, and North Korea. Published open source reports claim that over 200 nations have active "cyber intelligence" capability and that Iran has recruited the largest army of hackers on the planet. Cyber tools, used for computer network exploitation, can also be used for cyber-attacks. These capabilities are "dirt cheap" and are being built by the thousands. Among the recent highest profile incidents were companies such as Equifax, Pizza Hut, and Deloitte, just to name a few. The alarming reality is that today, many U.S. corporations have been hacked.

In cyberspace, the term "exfiltrate" is defined as the removal of information (digital data) by stealth, deception, surprise, or clandestine means. Other terms used to conduct these types of activities are Computer Network Operations (CNO) and Computer Network Exploitation (CNE). The stakes have never been higher. The advanced persistent threat (APT), defined as a dedicated and motivated adversary, has matured from disruption (DDoS) to destruction (Stuxnet, Saudi Aramco), where either a malicious insider or outsider will launch a cyber-attack with the intent to destroy data and/or hardware assets. The 2010 cyber incident at Saudi Aramco (Saudi Arabian Oil Co.), the world's largest state-owned crude oil exporter, serves as an example of what is possible. It is alleged that the cyber-attack destroyed over 30,000 computers.

Critical infrastructure (power, water, nuclear, communications, etc.) is at risk. Like the nuclear threat, mutually assured destruction is a deterrent for nation states. Cyber terrorists and/or rogue actors are not deterred. We can no longer afford to stand idly by and wait for a cyber-attack to occur before we respond.

We must develop cyber early warning capabilities to forecast (AKA: predict), detect, and respond to emerging threats before they strike their intended targets.

Admiral Mike Rogers, Director of the National Security Agency and Commander of U.S. Cyber Command, has told the Senate Armed Services Committee that our adversaries can launch cyber-attacks against the United States without fear of retaliation. "We focus primarily on the defensive, but I think now we're at a tipping point where we not only need to continue to build on the defensive capability, but we've also got to broaden our capabilities to provide policymakers and operational commanders with a broader range of options."

Senator John McCain of Arizona, Chairman of the Armed Services Committee, echoed Admiral Rogers' sentiments … "I am concerned that a strategy too heavily weighted towards defense is a losing strategy."

Providers of cybersecurity solutions and services must focus on innovations around the concept of "precognition," a holistic approach to cyber security, bridging the gap between social sciences and artificially intelligent technologies, utilizing

mathematical algorithms and top industry cyber professionals, all of it with a laser focus on PREDICTING (situational awareness), PREVENTING (active threat management solutions), and PERSISTING (continuous monitoring) against cyber incidents, anytime and from anywhere.

Precognition or precognitive capabilities can be defined as a systematic way to build and organize knowledge from historical data in order to predict (forecast) future events before they occur.

Precognitive capabilities and the subsequent three pillars of PREDICT, PREVENT, and PERSIST (PPP) comprise a framework that can quickly be made actionable and operational. These pillars can aid in broadening capabilities to provide decision-makers with a range of options for taking action to proactively suppress threats.

PREDICT (Situational Awareness)

- Threat intel/threat forecasting (big data analytics)
- Sources and methods (people and machine)
- Behavior modeling (cyber psychology)
- The application of traditional intelligence in cyberspace (leverage historical perspectives)
- Sensors feeding into a visual aid (Security Event Management [SEM], Security Information & Event Management [SIEM])

PREVENT (Active Threat Management Solutions)

- Know what new solutions will best protect your network against malicious activity
- Select and deploy the most efficient and cost effective threat defense technologies
- Combine solutions that will provide real-time protection (monitor and detect), as well as security event analysis and incident response
- Implement "lean forward" technologies from at least two of the three architecture framework layers: (1) network (2) payload (3) endpoint

PERSIST (Continuous Monitoring)

- Discipline and vigilance
- Policies, processes, and practices
- Patching holes and bridging gaps
- Vulnerability assessments
- Penetration testing
- Secure code review
- Security awareness training

Agile Cyber Solutions can provide you with the guidance and expertise to assist you in the development of a PPP security framework for your organization.

ABOUT THE AUTHOR

Carlos Fernandes has over 25 years of experience in information security and over a decade of experience in international project management supporting a variety of U.S. government entities. Currently, he serves as Founder and Managing Principal/CEO of Agile Cybersecurity Solutions located in Washington, D.C., and provides cybersecurity consulting services to government and commercial clients. Mr. Fernandes is a subject matter expert with extensive expertise in the development and implementation of cybersecurity growth strategies.