From: "Tom Kellermann"
Date: Tue, 10 Mar 2009 15:31:44 -0400
To: [Melissa Hathaway]
Subject: Red teaming idea in detail

As evidenced by specific campaigns carried out against federal agencies in recent years, and further illustrated by trends emerging on the larger cybercrime landscape, a lack of situational awareness and an inability to predict the specific methods being utilized by electronic assailants of all archetypes has been one of the most significant failures in stemming the tide of successful attacks.

While organizations across the federal space, as well as the private sector, have gone to great lengths to employ layered defensive mechanisms aimed at preventing specific classes of threats from infiltrating their IT systems, clearly, based on the successful campaigns that we know of – such as the set of coordinated cyber-attacks emanating out of China beginning in 2003 and labeled “Titan Rain” which compromised assets at the DoD, NASA and Sandia National Laboratories, as well as those of federal contractors– these defenses have been proven vastly insufficient. And as we know there are likely many more incidents along these lines that have not been reported publicly than those we can already cite here today.

To address this dire reality, which has been highlighted most recently by widely publicized electronic data theft carried out against private merchants such as Heartland Payment Systems, which saw thieves make off with millions of its sensitive customer payment card records, the federal government must expand the Federal Information Security Management Act (FISMA) to compel all agencies to undergo more frequent internal assessments to gauge their risk to cyber attacks.

Agencies must further embrace the results of exercises including “Operation Eligible Receiver" – an audit of the Pentagon’s exposure to cyber attack ordered by the Joint Chiefs of Staff in 1997, through which internal security testing specialists, dubbed Red Teams, found it exceptionally easy to circumvent existing defenses to penetrate some of the government’s most heavily guarded IT systems – to better assess their own exposure to hacking techniques of all varieties. Specifically, agencies must be required to conduct security audits using Red Team penetration testing methodologies on at least a quarterly basis to gain a more precise fix on where their most significant weaknesses lie by emulating the same tactics as those being employed by cyber criminals as closely as possible.

These quarterly security and IT systems penetration tests (as defined by NIST special document 800-53A Appendix G) must be applied to all federal networks and computing assets, as well as those of critical infrastructures providers across energy, finance and health sectors, among others, to empower these organizations to gain better a better understanding of where they are most vulnerable to potential attacks. Using classic risk management practices, those critical vulnerabilities that are identified via this process must then be remediated, and we must also create additional systems of accountability for those organizations found to be unable to properly address their critical vulnerabilities.

By compelling federal agencies and their business partners to engage in this proactive security testing, and specifically conduct regular internal assessments mimicking hacker activities, these organizations will be able not only to identify their most pressing instances of IT risk and ward off more attacks, but also to create effective benchmarks that they can refer to frequently over time to mark their progress in improving their security posture, and to channel spending into the most effective resources for doing so.

Tom Kellermann, MA, CISM
Vice President of Security Awareness
Core Security Technologies