5 Key Computer Network Security Challenges For 2013

Tom Cross is director of security research at Lancope, a security software firm.

With each passing year, the security threats facing computer networks have become more technically sophisticated, better organized and harder to detect. At the same time, the consequences of failing to block these attacks have increased. In addition to the economic consequences of financial fraud, we are seeing real-world attacks that impact the reliability of critical infrastructure and national security. With these observations in mind, here are five key challenges that computer security professionals face as we move into 2013.

- ***State-sponsored espionage and sabotage of computer networks***

Current security technologies and best practices are not effective at preventing sophisticated, targeted attacks from being successful. This fact was underlined earlier this year when a malicious program called Flame was discovered after evading detection by anti-virus software for years. Similarly, a recent study by Symantec Research Labs identified 18 undisclosed security vulnerabilities that were used to target computer networks in the wild for up to 30 months before they were discovered. The consequences of missing these attacks can be significant, as demonstrated by the Shamoon malware that recently hit several companies in the oil and energy sector. Shamoon erases data and renders machines unbootable.

New strategies are clearly needed to fight advanced attacks. Looking for known malware and attacks that target known vulnerabilities is not effective in this context because we don’t know exactly where the next vulnerability will be found or what the next attack will look like. Instead, we need to develop tactics that focus on the behavior of software, systems and actors on the network. By investigating both specific, suspicious behaviors that we know to be associated with malicious activity, as well as general anomalous behaviors that are unusual or unexpected, we can uncover evidence of attack activity even when we are not exactly sure what to look for at the outset.

- ***Monster DDoS attacks***

Distributed denial-of-service attacks have become increasingly popular with attackers, and the size of the attacks keeps getting larger. The DDoS mitigation firm Prolexic reported an 88% increase in the number of DDoS attacks launched in Q3 2012 versus a year earlier, with substantial increases in both the duration of the attacks as well as the amount of bandwidth involved. Furthermore, early this fall, the websites of several large U.S. financial firms were disrupted by a DDoS attack that reportedly exceeded 60 Gbps – much larger than the typical 5-10 Gbps attack.

The time to prepare for a DDoS attack is not the day that one's website goes down. Firms that are effective at protecting their networks against these incidents have: Assessed the risk of several different kinds of DDoS attack scenarios well in advance; developed processes for responding in the event that one of those scenarios occurs; and have tested those processes with real drills in order to ensure that they work as expected when needed. Getting this right is a top priority for any firm with a large Internet presence in 2013.

- ***The loss of visibility and control created by IT consumerization and the cloud***

When workloads move into the cloud, organizations lose control over who can access the computer systems that those workloads are running on. They also often lose visibility into what resources were accessed, when they were accessed and from where. The providers of cloud services and technology tell us not to worry about all of that, but seasoned IT security professionals know better. And this problem isn't limited to the cloud. With bring-your-own-device (BYOD) programs, IT is losing control over the software load, configuration and patch level of network endpoints. IPv6 is going to create its own visibility gaps, beginning with vulnerability assessment, as large address ranges are more difficult to scan.

Organizations have to start demanding their network visibility back. There is no reason that new information technologies cannot be designed with the capability of providing security controls and audit trails to people who need them. The best approach to providing those basic capabilities might be different than in legacy systems, but at the end of the day, it is not impossible to solve these problems. It is all a matter of exposing the right information and regaining control in the right way.

- ***The password debacle***

2012 was rife with large disclosures of passwords and password hashes from major websites that were breached, including Zappos, LinkedIn, eHarmony, Last.fm, Yahoo Voice and Formspring. In addition, attackers are constantly scanning the Internet for exposed, password-protected services like Secure Shell (SSH) and Remote Desktop Protocol (RDP). Accounts on these services are subject to brute-force cracking, and have a tendency to show up on the black market.

The fact is that passwords, as a security technology, are reaching the end of their useful life. Moving to a world where alternative authentication systems are the norm is incredibly difficult, and as a consequence we are entering into a period of time when we are going to have to continue to rely on a security control that doesn't work. Encouraging users to pick longer passphrases, and proactively auditing networks for weak passwords are steps that can be helpful during this time. Increasingly, we are going to see attackers entering networks with legitimate access credentials without ever having to fire an exploit that would trigger an intrusion detection system. We need to be prepared for this type of attack activity.

- ***The insider threat***

The insider threat has traditionally been viewed as a high-consequence but low-frequency risk, and many IT organizations have found it challenging to develop effective programs that manage that risk. Even the concerns that were raised over WikiLeaks have failed to create much of a response, because security professionals don't agree on the right approach. However, some good answers have finally started to appear.

For years, researchers at the CERT Insider Threat Center at Carnegie Mellon's Software Engineering Institute have been collecting and studying data on real-world insider incidents. This year, they published a book cataloging the results of their research, called The CERT Guide to Insider Threats. This book is an invaluable guide to establishing effective processes for managing the risk of insider attacks, and it should be on every security professional's wish list this year. In general, the insider threat drives home the point that perimeter defenses are no longer enough. IT organizations also need to be able to see into their internal networks to identify suspicious activity.

In a recent public comment, former U.S. Cybersecurity Czar Howard Schmidt spoke of the important role that security professionals are playing in keeping infrastructure up and running. "Security professionals day after day, not withstanding disruptions, still keep the machine running," he said. "We are able to do online banking and shopping most of the time – and it's a direct result of the security professionals…" To be sure, 2013 promises to be another challenging year for those professionals, but being adequately prepared to address the above threats will help keep businesses running and critical infrastructure secure.