

InformationWeek

How The U.S. Changed Its Security Game

Agencies pool threat data and make practical fixes to common woes

By Alan Paller

June 20, 2009 01:15 AM (From the June 22, 2009 issue)

Alan Paller is director of research for the *SANS Institute*, responsible for projects including the Internet Storm Center and the Top 10 Security Menaces.

On March 12, 2007, the CEO of one of the nation's largest defense contractors learned of a call from the Office of the Secretary of Defense informing his firm that the FBI had evidence that his company had allowed another nation to steal details of some sensitive technology that DOD had contracted to develop. There was no getting the data back. In a meeting at the Pentagon the next week, the executive learned he was not alone. Around the table were other defense contractor executives who had suffered similar breaches.

The meeting was among the catalysts for what has evolved into a change in thinking about information security in U.S. government and the defense industrial base. It includes more emphasis on actions proven to block known or expected attacks, as exemplified in the "20 Critical Security Controls" crafted earlier this year.

The changed thinking involves IT pros from CIO to developer, and is highly relevant to the private sector as well. A bank recently lost \$10 million in less than 30 minutes to hackers who had replicated ATM cards and manipulated internal bank computers to increase limits on the amount each card holder could take in a day. The amount of money lost was limited only by the amount of money in the ATM machines that had been targeted.

Throughout most of this decade, the topic of cybersecurity rarely touched senior management, coming up only in the context of regulatory compliance. The problem has been that many of the steps taken to meet compliance requirements weren't geared to match the emerging threat. Rather than doing the tasks needed to ensure that systems were configured securely and that attacks were blocked or found quickly, organizations were forced to pay consultants to write lengthy compliance reports. The reports met the regulator's demands, and the CIO was told that his organization was in compliance. When the CIO learned that the company's systems had been penetrated and its data looted, surprise was a reasonable response.

The Big Questions

Three questions are usually asked following a cyberattack. The first two are:

1. What do we need to do to fix this problem?
2. How much is enough?

Any CIO will quickly discover security people don't agree on the answers. When outside experts are asked, their opinions also differ, leaving CIOs frustrated and asking the third question:

3. Whom can I trust to answer the first two questions?

The CIOs of the major defense contractors and sensitive government sites faced exactly this uncertainty. They found a solution to this problem that may be of value to those who want to avoid those unwanted FBI calls. While the U.S. defense industry was discovering the extent of penetration into its systems, and thousands of other businesses were hearing from the FBI that they were victims, too, the U.S. intelligence community, the departments of Defense, Homeland Security, and Energy, were leading a national effort to transform cybersecurity.

A theme that shaped the national makeover was that defense must be informed by offense. In other words, organizations should prioritize their security investments on actions that can be proven to block known or expected attacks, or that directly help identify and mitigate damage from attacks that get past the defense. This was a huge shift in thinking and in behavior. Its greatest impact was to change who was considered expert -- it answered question No. 3. In the past, consulting firms armed with checklists of questionable value were let loose to point out missing documentation or incomplete awareness programs.

Under the "offense informs defense" approach, the measures of effectiveness are defined by the people who know how attacks are carried out, and are more specific and more directly related to defenses against known attacks -- such as the speed with which unauthorized systems are identified and removed from the network. Other examples of the new practices include:

- Automated inventory so every connected system is known and monitored.
- Application software testing so that security flaws are removed from Web applications before they're posted.
- Secure configurations of systems and software deployed on the network.

In all cases, the practices include specific tests that can measure the effectiveness of the controls. Most of the new metrics are automated so that CIOs get continuous visibility into their organization-wide security effectiveness, rather than snapshots or compliance summaries. In short, common threats mean common defenses must be implemented first, and extensively automated to continually update.

Another critical change in thinking in government is recognition that, because of the widespread use of common computer and network technology (Windows, Unix, HTML, Secure Sockets Layer, SQL, and so on), all organizations face many of the same threats. Individual organizations may face additional threats, but unless they engineer their systems to withstand the common threats, even targeted attackers need not worry about specialized tactics -- attackers can just use the common attacks that work on any organization not fully prepared.

It's those common threats that make this security challenge a top priority for software development staff. The majority of current attacks exploit programming errors made by developers whose training never included finding and fixing security flaws. One of the most critical controls not in place in most organizations is a secure application training testing program. (Disclosure: SANS Institute operates the Internet Storm Center, the Internet's early-warning system; is a degree-granting institution; and provides training for security professionals and programmers.)

In federal agencies and leading defense industry organizations, these common threats are being countered through a three-part initiative:

- Establish a prioritized set of security controls that the community affirms will stop or mitigate known attacks.
- Use common tools to automate the controls, and even the measurement of the controls, that continuously monitor security.
- Create a dashboard for CIOs and senior managers to be able to monitor the status of security in their organizations.

Agreement On The 20 Most Critical Controls

Although many subdivisions of the U.S. Department of Defense, the civilian government, and various defense contractors have detailed knowledge of attacks that they have experienced, creating an effective national defense means pooling all that knowledge into a prioritized and up-to-date list of critical security controls that represents the most current attack map available.

In February, the Center for Strategic and International Studies (csis.org) announced it had collated that attack knowledge across all relevant agencies and published a first draft of the "20 Critical Security Controls" (the list is at www.sans.org/cag). The controls were the consensus of organizations that understand offense -- including the National Security Agency, DOD Joint Task Force Computer-Global Network Operations, the DOD Cyber Crime Center, US-CERT at the Department of Homeland Security, and the nuclear energy research laboratories at the U.S. Department of Energy, plus top commercial forensics and penetration testing organizations. After public review involving more than 60 organizations, the 20 critical controls were published for government and private use. The U.S. State Department has already implemented software and hardware that automate monitoring of the 20 critical controls and is demonstrating how they can be monitored at every U.S. embassy around the world through a centralized dashboard.

The Developer Role: Control No.7

The Developer Role: Control No.7

Application software security is the control most often weakly implemented. Effective implementation calls for three processes:

- Testing all applications using source-code analysis tools (Ounce Labs, Fortify, Coverity, and Veracode are among the most widely used); Web application scanning tools (such as IBM Rational AppScan, Hewlett-Packard WebInspect, and Cenzic Hailstorm); and, for important applications, application penetration testing. But the control isn't in place when tests are run; it's in place only when the processes can ensure that problems are fixed or vulnerabilities mitigated with other defenses, such as a Web application firewall.
- Training and testing programmers in secure coding skills in their own programming languages. This is focused on finding and fixing the critical errors identified in the "25 Most Dangerous Programming Errors" (www.sans.org/top25errors), developed jointly by NSA, DHS, Mitre, and SANS. The control is in place only if the programmers pass periodic competency exams in each language they use.
- Procurement language requiring software suppliers to implement the first two processes. Putting these requirements into all contracts that result in software being delivered or used on behalf of the organization extends the control to where it can do the most good.

The Way Forward

The outline of a new era is taking shape in security. In the past, security was usually "bolted on" after systems were designed and deployed. That doesn't work. Security is effective only when it's "baked in."

Security is baked in when very large buyers or groups of smaller buyers act jointly to establish minimum security standards for the software and systems and networks they buy, and then demand that vendors deliver technology that meets those standards.

The U.S. Air Force offers the most successful example. With the help of the NSA, the organization that best understands how attacks are launched and why they work, the Air Force identified how Windows should be configured to make it tougher to attack, then persuaded Microsoft to sell 500,000 copies of Windows XP and Vista preconfigured with all key security settings installed. Air Force users could turn on their PCs knowing they were safely configured. The Air Force saved more than \$200 million in acquisition and operations cost, radically improved defense against common attacks, and made users happier because systems failed less often. Today, commercial organizations and governments benefit from the more secure version of Windows.

By replicating and expanding the Air Force process, the federal government can use its buying power to provide incentives to bake security into all products and services it buys with the ultimate goal of making security less expensive and easier and more effective for all buyers of the same technologies.

The 20 Most Critical Security Controls automate the measurement of these baked-in controls and can themselves be purchased baked into network and systems monitoring software.

A new era of buying security baked in and continuous monitoring of focused, offense-informed security controls has begun. In government, it's made possible by sharing attack and defense information across the U.S. government and its contractors, and represents the best hope against increasingly sophisticated cyberspace attacks. Any business trying to answer the questions "What do we need to do?" and "How much is enough?" would do well to focus on implementing and automating the 20 critical controls.