cnet NEWS.COM http://www.news.com/

Cybersecurity plan lacks muscle

By Robert Lemos and Declan McCullagh
Staff Writer, CNET News.com
http://news.com.com/2100-1023-958545.html

Story last modified September 19, 2002, 4:00 AM PDT

After Sept. 11, 2001, cybersecurity czar Richard Clarke crisscrossed the country berating technology companies for failing to do enough to shore up the Net against potential terrorist attacks.

In unveiling a highly anticipated White House cybersecurity proposal on Wednesday, however, Clarke left his firebrand at home. Rather than target specific industry segments and require that they secure themselves by recommending tough new laws and regulations, the administration's plan recommends that industry and individuals simply take greater care.

THE BIG PICTURE
Read more about cybersecurity

"It has no teeth," said Steven Kirschbaum, CEO of Secure Information Systems, a small Fremont, Calif.-based security consulting firm. "It has no enforcement. The first rule of having any security policy is you have to have enforcement. Without it, it's just a nice press release."

Nearly a year after President Bush sent Clarke out to stump for tougher security, experts say little has been done to address many of the fundamental causes that lead to persistent vulnerabilities that expose Net users to myriad threats, from Web site defacements to viruses to denial of service attacks.

Although there is considerable debate over the potential for harm in a cyberattack as compared with a physical attack, numerous new industry and company-led initiatives have been announced in a bid to turn security into a top industry priority.

Neverthless, with Wednesday’s announcement, the White House made it clear that it would not scope out any bold new ground in this effort.

In many ways the plan punts the responsibility to those least capable of doing it: individual users. A previous draft of the plan reportedly would have required Internet service providers (ISPs) to ensure that subscribers are secure by offering them firewalls and antivirus protection. The current version suggests only that ISPs offer such security.

The report was widely praised by technology companies on Wednesday, with many, including Kirschbaum, calling the report an important first step in building a secure foundation for the Net.

FACE to FACE with Richard Clarke

Clarke: Cyberattack threat is real

Still, the focus on voluntary measures drew a tart response from a handful of critics.

"It's like asking every passenger on an airplane to bring along their own parachute," said Alan Paller, director of research at the SysAdmin Audit Network Security (SANS) Institute.

While that may not lead to better security, he stressed that the Bush administration wouldn't try to regulate the industry. "This administration is not going to do any company bashing except for the Securities and Exchange Commission," he said.

Paller argues that although the Bush administration doesn't want to bludgeon the industry with policy, it is more than willing to push it around with procurement. Rather than list the requirements, the report recommends that government agencies force companies to provide better software by awarding contracts only to those companies that deliver.

The plan even suggests that businesses should follow suit. Using the acronym ACTIONS, the plan calls for companies to implement authentication on their networks, manage their configuration, train their employees in smart security practices, develop an incident response team, organize a security management team, periodically analyze the network and use smart--that's the 'S'--procurement to ensure that proper security is built into products.

DOCUMENTS

PDF PDF document
WhiteHouse.gov

Read a draft of the "National Strategy to Secure Cyberspace" in PDF format.

Paller figures such tactics maybe the only way to get information technology companies to produce better products.

Paller said the plan changes a critical philosophy in security policy: Rather than focusing on minimizing risk, the plan focuses on making patching a priority. "A risk-based approach is characterized by fixing critical machines and leaving others unprotected or not as protected," he said. Instead, the plan wants to turn today's untenable problem of continuous patching into a manageable process.

Echoes of the past
Instead of making substantive changes in the executive branch's stance on electronic security, the 64-page report echoes the hands-off approach established by the Clinton administration in a 1997 report.

That paper, titled "A Framework for Global Electronic Commerce," adopted a similar laissez-faire perspective. Its first principle was straightforward enough: "The private sector should lead."

"There is no single 'magic' technology or technique that can ensure that the (Internet) will be secure and reliable," it said. "Accomplishing that goal requires a range of technologies--encryption, authentication, password controls, firewalls, etc.--and effective, consistent use of those technologies."

Similarly, the report that the Bush administration released Wednesday lists as a guiding principle: "Avoid regulation."

"The government cannot dictate. The government cannot mandate. The government cannot alone secure cyberspace," Clarke said Wednesday at a Stanford University event designed to highlight the report. Clarke was pointing out the obvious: The infrastructure that keeps the Internet working is almost entirely owned and operated by private companies, not the government.

The administration's plan, called the "National Strategy to Secure Cyberspace," stresses that primary responsibility for Internet security must come from individuals and corporations, rather than the government. It does not call for new laws or regulations aimed at the private sector.

In other words, little has changed.

No new laws
The most important effect of the Bush administration's strategy, which is still officially just a draft, may be to focus public attention on the topic of Internet security.

As more and more commerce moves online, and as denial-of-service attacks and intrusions increase, online security has become a far more visible topic than it was five years ago. Unlike the Clinton administration report, which devoted just a chapter to security, the new report discusses nothing else.

Wednesday's report does hold out the option of new laws and regulations in the future, saying, "As appropriate, the executive branch may ask Congress to enact legislation to advance this strategy." But because it does not go any further, its impact is muted.

Earlier draft versions were far more detailed and had far more specific recommendations about what the private sector should do.

Pressure from the private sector, coupled with critical news reports based on leaked drafts, led to some controversial sections being deleted from the report. It does not, for example, ask for new laws compelling Internet providers to offer firewalls or other security devices to their users.

Two months ago, Clarke slammed the lack of security in wireless networks as a major vulnerability, but in the draft released

Wednesday, the plan recommends only that federal agencies "be mindful of the security risks when using wireless technologies."

An August version of the draft seen by CNET News.com said the government should improve the security of key Internet protocols and spend tens of millions of dollars on centers to recognize and respond to cyberattacks.

A single chapter of the earlier draft was about 100 pages--the far shorter report released Wednesday was 64 pages total including graphics--and singled out technologies like the Border Gateway Protocol and the Domain Name System as candidates for improvement. It even said that it's time for the federal government to become more involved in the development of Internet protocols, security and standards--a role currently assumed by the Internet Engineering Task Force.

All those specific recommendations are absent from Wednesday's report, which includes roughly the same level of detail as the executive summary from last month's version. The more specific version may reappear when President Bush receives the document for approval after a two-month comment period.

The intentionally noncontroversial nature of the report drew sharp and immediate criticism.

Michael Overly, a partner at the law firm Foley & Lardner in Los Angeles, said it's too little, too late.

"The plan was expected to provide specific recommendations regarding cybersecurity," Overly said. "Instead, the plan offers little more than a rehash of ideas that have been expressed many times in the past. Recommending that users employ antivirus software and firewalls is hardly ground-breaking information."

Referring to a speech in August, Overly said, "Clarke noted that changes in federal law were needed to make sure valid security researchers were not held in violation of existing law. We expected the new plan to address those protections for security researchers. It did not."

Tech companies, especially ones that stand to benefit from increased security spending, expressed general support for the White House's strategy, saying it was a positive sign. But defense hawks suggested the White House had sold out to the private sector.

The Center for Strategic and International Studies (CSIS), a hawkish think tank in Washington with close ties to the military, called the report flawed since it did not demand new laws or regulations aimed at Internet companies. CSIS is headed by John Hamre, deputy defense secretary under President Clinton, who spent years telling legislators about "the future electronic Pearl Harbor that might happen to the United States" if extreme measures were not taken.

"Cybersecurity is too tough a problem for a solely voluntary approach to fix...," said James Lewis, director of the CSIS Council on Technology and Public Policy. "Companies will only change their behavior when there are both market forces and legislation that cover security failures. Until the U.S. has more than just voluntary solutions, we'll continue to see slow progress in improving cybersecurity."

Related News

- Government unveils cybersecurity plan September 18, 2002
  http://news.com.com/2100-1023-956353.html
- White House preps cybersecurity plan September 16, 2002
  http://news.com.com/2100-1023-958159.html
- E-terrorism: Digital myth or true threat? August 26, 2002
  http://news.com.com/2009-1001-954728.html
- Tech pros: Cyberbomb's ready to go off July 24, 2002
  http://news.com.com/2100-1001-946161.html
- Homeland defense focus shifts to tech July 10, 2002
  http://news.com.com/2100-1023-942686.html
- Get this story's "Big Picture"
  http://news.com.com/2104-1023-958545.html