DHS Works Through Gaps New Tech Presents in R&D

The agency plans ways to incorporate user feedback and security testing throughout the development process.

James Mersol

Tue, 03/19/2019 - 15:52

Photo Credit: Funtap/istock.com

The Department of Homeland Security's Science and Technology division has funded the development of products based on new technologies to assist with the agency's mission. However, as these technologies reach the market, they routinely come with gaps — both gaps between the technologies' capabilities and their purpose for the end user — as well as security gaps that leave the government open to data breaches and other attacks.

A common gap with new technologies in the Secret Service's Office of Technological Development and Mission Support comes from a disconnect between the researchers and the users, said the office's Assistant Special Agent in Charge Scott Gee. In one case, the Secret Service built cutting-edge servers for the investigative branch to store and examine forensic data.

"The problem became … I don't have a tool to be able to exploit [the servers' processing power] effectively," Gee said at the DHS S&T Cybersecurity and Innovation Showcase on March 18. "We're breaking things and looking for someone to help us fix them."

While S&T can create these tools, and has incorporated feedback from users in building them, the development process takes weeks to months. In the meantime, users rely on older technologies to do their jobs.

"I looked at a lot of spreadsheets most days," Gee said when asked about what he did while waiting for the new tool.

Research and development teams need to concentrate on connecting the initial project to the final product to ensure the result is worth S&T's investment, said Nadia Carlsten, director of commercialization for the division. Her office is encouraging researchers to incorporate user feedback throughout the development process to ensure that the product will be useful to its target audience and will not immediately require the development of new tools to harness their potential.

Even when DHS S&T or the projects it funds can deliver complete products, they must balance rollout with taking the time to ensure the new technologies are free of vulnerabilities. Alma Cole, chief information security officer for Customs and Border Protection lauded the progress of new technologies, including devices for border patrol agents that record their movements in real time, as well as systems that have streamlined the authorization process for those crossing the border. He also cautioned, "as we create these efficiencies, the risk … is also going up dramatically," highlighting that as these technologies become critical to accomplishing their mission, an attack on any of them becomes more and more disruptive.

For DHS' private-sector partners, however, delaying a technology's release to test for security flaws is hard to sell as a business model. "Filling the gaps … has very little ROI," said Robert Schmidt, a founding member of cybersecurity firm CyVantage.

One solution DHS is examining is better integrating vulnerability and penetration testing as part of the development process for any new technology. Cole said that CBP is testing the security of new technologies throughout the process so that a product is secure as it is released, rather than waiting until the product is complete before testing it. He also mentioned that CBP launched a pilot program late last year for white-hat hackers to conduct penetration testing on DHS's systems.

"I'm making that a key part of that information testing program," Cole said. "We really like what we've seen so far."

View printer friendly version
Federal Cybersecurity
innovation
national security
Department of Homeland Security
Standard