Highlights from a recent webcast on mobile security

MOBILE APPS MAKE GAINS IN SECURITY, IDENTITY

Application management and trusted credentials can revolutionize the way government agencies interact with citizens

Cloud computing has become a critical element in enterprise IT, changing the way organizations use and consume IT resources. IDC estimates that worldwide spending on cloud services will reach more than $100 billion this year.

With the use of mobile devices outpacing that of less portable technology, officials at government agencies are working to provide constituents with the services they want and expect.

This effort has two parts. First, there's the information provider – the government, securing mobile applications and data at rest and in transit. Then there's the consumer – citizens, looking to obtain a trusted identity to prove who they are and to use across websites, organizations and the public and private sectors.

Symantec Corp. has solutions that address these needs, said David Hurley, mobility and identity sales lead at Symantec, and Lewis Etheridge, the company's national practice manager for public health, during a June 24 webinar titled "Enabling Government to Citizen Engagement through Mobility and Identity Solutions."

"What we find is if the user is expecting a certain experience, whether it's an [Apple] iOS, [Google] Android or even a [Microsoft] Windows device, if they don't get that on the device, then they're less likely to use the tool," Hurley said. "The focus that Symantec is taking toward mobile, and our vision, is really any device, anywhere at any time. That is the goal."

Mobile apps are not really new, he said, but their functions are. Historically, apps have been informational, telling users the hours of operation at the Smithsonian Institution or what they can bring into a national park, for example. The need for security and management on these is low.

Now apps are becoming more transactional, incorporating sensitive data, such as payments, health records and personally identifiable information, making app policies are necessary. Symantec App Center, which puts mobile device management, mobile threat protection and mobile app management into one solution, can help create them.

"What we're addressing here is what type of policy do we need around that application? How secure do we want it?" Hurley said. "We are taking that mobile application to do whatever you may need it to do."

App Center can protect apps against data loss through encryption, removal control and separation of corporate data. It's flexible, letting the agency set the rules. For instance, an agency might set a policy securing information in an app to its server so nothing can be leaked, he said.

Sometimes agencies' apps aren't enough or a commercial version already in existence is better. In those cases, the government turns to apps from third-party developers, and those also need to be secured. Symantec's Sealed Program covers that.

"What Symantec is doing is working

MOBILE APP USE-CASES IN THE FEDERAL GOVERNMENT

The government is transitioning its app offerings from straightforward informational to more complex transactional setups. As more agencies embrace mobile apps, their possibilities become apparent, said David Hurley, mobility and identity sales lead at Symantec.

Here are a few examples:

- The Veterans Affairs Department could use mobile apps on a tablet at a veteran's home for updating health information.
- The Federal Emergency Management Agency's network of local citizens responding to a disaster could collect and send data back to the agency so it can adjust resource allocation.
- As it prepares for the 2020 census, the Census Bureau could incorporate mobile apps for secure data gathering.
- The Agriculture Department could deploy an app to a contractor in a particular area and pull information securely back to its data center.
- The Forest Service uses third-party apps for preventing and fighting fires.

LISTEN/LEARN:

For a replay of the webcast, go to: GCN.com/2014SecureMobileEngagement

> "The focus that Symantec is taking toward mobile is, 'Any device, anywhere, any time.'"
>
> *– David Hurley, mobility and identity sales lead at Symantec*

directly with third-party app vendors to embed our security, our code, so to speak, around their application so when users pull it down to their device or when a citizen pulls it down to their device, they can adopt the policies you've set," Hurley said.

Identity crisis

One reason why mobile apps used to be informational was because agencies didn't know who their consumers might be, Symantec's Etheridge said. That's less of an issue today and leads to two questions: What could you do differently for your citizens if you knew who was on the other end of the connection?

The answer is a lot – as long as certified identities are involved.

To get started, agencies first need an e-government vision, and officials must decide what could be moved to an electronic format for mobile consumption. They must consider the sensitivity of the information involved, and they should look at authentication measures beyond user names and passwords, which are easily hacked, Etheridge said.

The real heart of the problem, however, he said, is proving the identities of citizens wishing to access services.

"Any time in the history of the computer industry that you've dealt with any kind of certified identity, it's usually dealt with something that's called in-person proofing," which means physically bringing ID such as a driver's license or passport for someone to examine and approve as legit, he said.

Moving that process online requires government at all levels to accept trusted credentials. Plenty of benefit can come from that, Etheridge said. For example, managing the provisioning of contractors' credentials would become easier; law enforcement, public safety and first responders could share information on external portals; and students could access their entire education history.

"The departments of Justice and Homeland Security, I believe, are operating some programs now that are affecting what states and municipalities have to do to prove identity before granting access to criminal justice information systems," he said. "That identity should be, we believe, reusable at a very high level, not just a credential issued so that you are certified to be an officer in Travis County, Texas, for instance."

A trusted identity means "it's a validated, person-specific user," Etheridge said. It also means it's interoperable across the web so websites no longer have to require their own passwords, and it's certified according to the Federal Identity Credential and Access Management initiative, which provides a list of requirements developers must meet. Additionally, a trusted identity must come from a trusted source, meet government and health care security requirements, and embed privacy.

Symantec has implemented Norton Secure Login. To sign up, users go to the website of a Symantec customer and follow a process called Precise ID from Experian, a credit bureau that asks applicants questions based on their credit history to vet them. Experian sends a success or fail message back to Symantec. If a user passes, Symantec provisions an account that can be used at multiple websites.

If they want, users can add another layer of protection: two-factor authentication. A hard token can be issued or a soft one installed on a mobile device. Then when users log in, they must enter their user name, password and the code from the token.

What sets Symantec apart

Mobile apps that are secure and being used by honest consumers are growing both in need and in ease of creation. Symantec's solutions are based on the 32-year-old company's established portfolio of anti-malware, authentication, data loss prevention and managed public-key infrastructure that it's bringing to the mobile market.

"Other vendors don't have this portfolio that we've developed over the years," Hurley said. "What we're trying to do here is very seamless. Instead of trying to cobble together four or five vendors to make a solution work, you're dealing with one vendor and an end-to-end solution." •