ATARC

WHITE PAPER

Accelerating Endpoint Detection & Response in Government

Summary of Roundtable, hosted by ATARC on August 25, 2021

Since his inauguration on January 20, 2021, White House observers have witnessed a flurry of activity from President Biden and his Administration aimed at shoring up the nation's cyber defenses. Most recently, the President met with a series of private sector and education leaders on August 25, 2021, resulting in large technology vendors like Apple, Google, and IBM pledging to invest billions of dollars in upskilling the American workforce in order to meet emerging cybersecurity challenges. The August 25 meeting follows a May 12 Executive Order outlining the Biden Administration's position that, among other things, "the Federal government should lead in cybersecurity, and strong, Government-wide Endpoint Detection and Response (EDR) deployment coupled with robust intra-governmental information sharing are essential."

In order to help agency leaders understand how they can contend with the shifting threat landscape and Administration priorities, ATARC held a roundtable discussion devoted to highlighting how federal agencies can accelerate the deployment of EDR technologies and policies. Roundtable participants represented a mix of public sector leadership and industry experts with moderation provided by ATARC Founder and President Tom Suder.

During the wide-ranging discussion that took place, roundtable participants weighed in on the cybersecurity implications of the coronavirus pandemic and the opportunities and challenges associated with 'bring your own device' (BYOD) policies in the federal sector.

COVID-19 and Cybersecurity

Roundtable participants were quick to highlight how the coronavirus pandemic has pushed much of the federal workforce into a remote work environment and accelerated existing trends towards the use of personal mobile devices to conduct government business. While this shift can help make federal employees more productive by enabling them to work from anywhere, it is not without its challenges.

One panelist colorfully described threat actors' response to this shift to mobile devices and cloud services as being akin to that of "a kid in a candy store," with an ensuing rise in phishing and ransomware attacks. The panelist cautioned that mobile devices are often 'softer' targets for threat actors due to their smaller screens, on which it can be more difficult to spot the telltale signs of phishing attacks, and the comparative lack of training regarding how to detect these kinds of attacks in a mobile setting.

Protect Your Back Door

> Mobile security should be treated equally among all the other elements of cybersecurity. It should not be left out. If you have a home security system you don't put a sensor on every door and window except the back door.

Other panelists pointed to the relative scarcity of mobile security experts as cause for concern, with one going as far as to say that the number of federal staff with expertise in mobile forensics could be counted on one's fingers. This panelist also argued that, while there has been a great deal of official guidance around telework, remote work, videoconferencing, etc. comparatively little attention has been paid to the security of mobile devices.

The challenge is compounded by the sheer width of the attack surface in a 'perimeter-less' world where federal

info@atarc.org

employees expect to be able to access their work environments from anywhere. In the words of one participant, "people don't think about mobile devices as endpoints but they are. My threat environment in mobile is everyone that has a child or spouse that has a mobile device and is on the same WiFi network as the service member. The threat vector is every mobile device that the service member comes into contact with."

The deployment of EDR solutions is key to solving this challenge, with one panel participant noting that EDR "allows cybersecurity teams to search for and proactively find threats in their environments, rather than waiting for them to be detected." Having a single location that data is fed into in which analysts can track an entire 'kill chain' as it's hitting mobile devices, cloud services, and the server infrastructure is also of critical importance.

Bring Your Own (Approved) Device

Polling showed that roughly half of federal employees were using their personal devices to access email and download work documents irrespective of official agency policy even before the pandemic, behavior that in all likelihood has only increased since early 2020. It is therefore unsurprising that BYOD policies were top of mind for panel participants discussing the best way to secure agencies' mobile footprints.

Participants argued that effective BYOD policies could save the federal government a great deal of money by leveraging employees' existing devices instead of providing them with government-furnished equipment (GFE). Under such a model, the agency or department would be responsible only for providing security for a device, not for furnishing the device itself. However, participants cautioned that such policies were not without potential pitfalls and that great care would need to be taken to ensure user privacy in particular. While federal employees typically know what to expect and consent to a certain degree of monitoring when it comes to GFE devices, personal devices involve a different set of expectations. It will be up to agencies to assure staff that they will not read their private correspondence and that employees can continue to use their personal devices as they have in the past.

Even beyond privacy implications, many questions around BYOD policies have yet to be resolved. For example, some departments have policies which mandate that any device using solid-state storage to retain data, such as emails, needs to be physically crushed at the end of its life in order to prevent data leakage. What happens when such data is stored on a federal employee's personal device and they leave government service? How do agencies contend with staff taking their personal devices with them when traveling abroad? How does an agency or department account for the fact that mobile forensics are currently more limited, with security solutions unable to obtain very low-level access to everything that's happening on a device?

BYOD Security Transparency

> In a BYOD setting we want to be especially clear with users about how we're securing their devices, and just as importantly, what we're not doing.

Given the complexity of these questions it's no surprise that some departments still have policies that prohibit the use of personal devices for government work, or otherwise bar the access of government networks from outside the perimeter.

One participant concluded by cautioning that, whatever policies federal agencies seek to apply today, young service members and other components of the federal workforce are the future of American public service. These young people view mobile as "an integral part of their life," not just a matter of convenience, and will undoubtedly push agencies to adopt policies that better reflect the way they live and work.

How ATARC Can Help

ATARC is a nonprofit with the goal of bringing industry, academia, and the public sector together to drive outcomes. We host guest speakers and enable knowledge exchange to facilitate the sharing of best practices across emerging technology paradigms. We would love to partner with your organization to support your mission.

info@atarc.org