MARYLAND

Minutes
Maryland Cybersecurity Council Meeting
May 22, 2019
10:00 am – 12:00 pm
Chesapeake Room
College Park Marriott Hotel and Conference Center
At University of Maryland University College
Hyattsville, Maryland

Council Members Present or Represented
Attorney General Brian Frosh (Chair), Dr. David Anyiwo, Calvin Bowman (for Walter Landon), Judi Emmel, Delegate Ned Carey, Robert Day, John Evans (for Secretary Michael Leahy), Professor Michael Greenberger (for Markus Rauschecker), Fred Hoover, Clay House, Brian Israel, Dr. Kevin Kornegay, Mathew Lee, Belkis Leong-hong, Delegate Mary Ann Lisanti, Anthony Lisuzzo, Michael Lore (for Senator Susan Lee), Mark Miraglia (for Kenneth McCreedy), Jonathan Powell, Jonathan Prutow, Martin Rosendale, and Paul Tiao.

Staff Attending
Patrice Drago (Legislative Assistant, Office of Delegate Carey), Howard Barr (Assistant Attorney General and Principal Counsel, DoIT), Hannibal Kemerer (Director, Legislative Affairs, OAG), Nettie Squires (Senior Law & Policy Analyst| NCR Emergency Preparedness Specialist, Montgomery County Office of Emergency Management & Homeland Security), and Dr. Greg von Lehmen (Council Staff, UMUC).

Subject Matter Expert Presenter
Mr. Eugene Kipniss, Senior Program Specialist, Multi-State Information Sharing and Analysis Center (MS-ISAC).

Council Meeting

Opening Remarks by the Chair
The Attorney General opened the meeting, thanking members of the Council for their commitment. In particular, he welcomed Martin Rosendale, the CEO of the Maryland Tech Council, as a new member. The Attorney General noted that the Council had a crowded agenda with the updates, the subcommittee report-outs, and the speaker. Before turning to the Council's business, he called for the minutes of the January 17, 2019, meeting, which were approved after a motion duly made and seconded.

Council Updates

The agenda updates were reserved for the Baltimore City ransomware attack. Seeing no one from the City in attendance, John Evans, DoIT CISO, was asked to brief the Council to the extent he appropriately could. Mr. Evans indicated that he would redact his remarks since the Council meeting was a public forum, and he did not want to preempt possible announcements by the City or in any way compromise its efforts. His comments included the following:

- The state was taking a whole-of-government approach to assisting the City. DoIT and several other state agencies, have teamed up with the City as part of the incident response. Specifically, at any given time, there are four to five state personnel, working more or less around the clock to assist. As part of the remediation, they are involved with security administration, policy, tool evaluation, vulnerability management and incident response planning. Baltimore has engaged multiple vendors to assist in their remediation and restoration.
- The attack occurred on May 7th. The perpetrators asked for 13 Bitcoins (about $75,000), with a $10,000 premium for every day after the first four days, if the ransom was not paid. The City declined to pay.
- The ransomware variant is Robinhood.
- There have been suggestions in the media that the City did not have back-ups and/or the structures and routines in place to more quickly bring back affected systems. But Mr. Evans cautioned that this is speculation. The City has not addressed that question.
- On May 12th, a Twitter account was set up that claimed to publish passwords, usernames, and screenshots of sensitive documents from the City. These have not been confirmed as genuine, but if they are, this would indicate a deeper penetration than thought.
- Multiple state agencies severed relationship with Baltimore as a precaution. However, given the way Robinhood spreads—namely, via control of a domain controller—it is very unlikely that it could infect state agencies. Importantly, DoIT received patches on May 6th for this ransomware signature through MacAfee and Palo Alto, applying them on May 6th to state systems. As an additional safeguard, DoIT has also created a tool that would inoculate state systems against this strain of ransomware and is currently evaluating the tool's impact on the network before deployment. In general, the state has been on high alert, scanning for indicators of compromise. It has also been exercising, doing full restorations of its systems from backups.

  In the discussion following Mr. Evans remarks, it was noted that:

  - The state has a Security Operations Center (SOC). While the Center does not have machine learning tools, alerts are set up around behaviors to afford broader protection than looking for particular strains of ransomware.
  - Based on other ransomware attacks, the Baltimore attack might have succeeded via a phishing campaign or a remote desktop protocol compromise. Exactly how has not yet been reported.

- The state has been implementing a security awareness training program for its employees. This training covers phishing and other attack vectors. The University of Maryland Law School uses the same or a similar training system, as may other USM institutions.
- The state does have standards in place that IT vendors to the state must meet (e.g. SOC 2 audits).
- DoIT is kicking off an evaluation next fiscal year to gain a deeper understanding of agency cybersecurity-related practices so that it can provide more targeted recommendations to remediate potential problems. While agencies have security standards and practices, there is no uniformity. DoIT's effort, which will start with six agencies, will help create more uniformity across the state and build relationships that will useful in responding to any future attack.
- The state has been sponsoring, through the Department of Commerce, similar awareness campaigns for small- and medium-size businesses.
- Delegate Lisanti suggested that the General Assembly consider the need for a rapid response model that would be available to any entity in Maryland, including local governments, disabled by an attack. Mr. Hoover observed that at a minimum, there should be a formal finding of lessons learned from the attack.
- Mr. Tiao commented that the perpetrators speculated to be behind the attack seemed to have a record of releasing systems once the ransom is paid. He understood the law enforcement reasons for not paying, but he was curious whether other entities in a similar position had paid. Mr. Evans mentioned that another state he was familiar with had paid the ransom after being advised by its cyber insurance company it was the least expensive way to resume operations.

Within the discussion, the Attorney General noted that several Council members had indicated that they would be willing to assist Baltimore City's ad hoc security committee on a pro bono basis. On a motion duty made and seconded, the Council approved sending these names to the City Council.

Subcommittee Reports.

The subcommittees were asked to report out on recommendations to be included in the Council's 2019 July 1 Activities Report.

Michael Lore for Senator Susan Lee, Co-chair, Law, Policy and Legislation Subcommittee.

Mr. Lore indicated that Senator Lee was unable to attend due to personal obligation that she was unable to change. The subcommittee's recommendations include the following:

- Renewing the effort in the next session to pass SB 376/HB 456 (Criminal Law - Crimes Involving Computers - Cyber Intrusion and Ransomware) that did not advance in the last session.
- Updating MPIPA to include the relevant provisions in SB 786/HB 1127 (Financial Consumer Protection Act) which was not voted on in committee last session.

- Reintroducing legislation in 2020 ala SB 553/HB 1276 (Security Features for Connected Devices) to implement de minimis security standards for IoT devices.
- Renewing the effort to protect consumer privacy through some form of SB 613/HB 901 (Online Consumer Protection Act) that was introduced last session.
- Encouraging state action, if not already underway, to examine the security of Maryland's absentee balloting system in light of expert testimony so that any confirmed vulnerabilities are remediated and any issues of trust in the system are foreclosed before the next election.
- Offering legislation that would ensure that all branches of state government and localities are better protected against intrusions.

John Evans for Secretary Michael Leahy, Chair, Cyber Operations and Incident Response Subcommittee.

DoIT has begun an assessment to confirm the security posture of agencies, their practices and capabilities, and their governance structures, processes, and documentation, among other things. The Department has simultaneously laid out a number of specific goals that it hopes to implement. These include:

- Consolidation of security tools across state agencies. This will reduce cost and improve efficiency.
- Standardizing governance processes, structures and documentation. This will enhance the state's ability to respond to an incident since agencies will be operating from a common framework.
- Institutionalization of pen testing and red/blue exercises to support a proactive security posture.
- Continuing to build stakeholder collaboration across state agencies.
- Implementation of a modern data privacy bill to apply to state government. An example is HB 716 (State Government - Protection of Information - Revisions (Maryland Data Privacy Act) that narrowly failed in the 2019 session.
- Breach notification requirements applying to all three branches of state government and to state and local jurisdictions. The rationale is that reporting produces greater awareness of the threat landscape—who has been compromised and how—and contributes to collective security.

Michael Greenberger for Markus Rauschecker, Chair, Critical Infrastructure Subcommittee

Professor Greenberger mentioned two goals for the subcommittee the next two years:

- An ongoing effort to add resources to the cybersecurity repository hosted on the Council's website. This would be a joint effort with the Public And Community Outreach Subcommittee.
- A particular focus on recommendations that the Council could make to enhance the security of the electric utility sector serving Maryland. Within time and resources, the subcommittee also will focus on the hospital cybersecurity.

Bel Leong-hong, Chair, Economic Development Subcommittee.

Ms. Leong-hong referenced her subcommittee meeting prior to this Council meeting (see minutes for March 12, 2019) and that in the interests of time she would be brief. The Subcommittee's effort has included both examining barriers to entry and incentives to promote growth. In that connection, she drew attention to the subcommittee's effort to streamline the security clearance process that has included meetings of subcommittee members with Congressman Ruppersberger. It has also included active support for SB 228 (Cybersecurity Incentive Tax Credits) passed in 2019 and for expanding internships to build the cybersecurity workforce. These efforts related to barriers and incentives will continue in the next two years.

Dr. Greg von Lehmen for Dr. Jonathan Katz, Chair, Economic Development Committee.

Dr. von Lehmen noted that Dr. Katz was not able to attend the meeting because of a professional conflict and conveyed his regrets. The principal recommendation of the subcommittee is for the state to undertake a strategic investment in computer science and cybersecurity education within the state public university system. It will consider ways to advance this recommendation. The subcommittee commends the investments in this area that the state has made at the K12 level.

Dr. Von Lehmen for Sue Rogan, Chair, Public and Community Outreach Subcommittee.

Dr. von Lehmen gave Ms. Rogan's regrets for not being able to attend the meeting because of other professional commitments. In the upcoming two years, the subcommittee will continue to identify resources for the Council's cybersecurity repository and to create outreach or co-sponsorship opportunities for the Council in general cybersecurity awareness and hygiene.

<u>Subject Matter Expert Presentation</u>

The Attorney General welcomed Mr. Eugene Kipniss to the Council and thanked him in advance for his presentation. Mr. Kipniss expressed his appreciation for the opportunity to talk to the Council about the work of the MS-ISAC. He delivered a PowerPoint presentation (accompanying these minutes) that covered the following points:

- An overview of the MS-ISAC and its mission
- The Threat landscape confronting SLTT entities in 2019
- Early findings from the 2018 National Cybersecurity Readiness Report.

Mr. Kipniss indicated that he would provide a version of his slides for reference by the Council and for public posting.

<u>Other Business and Adjournment</u>

Dr. von Lehmen reminded about the deadlines related to the preparation of the Council's July 1, 2019, Activities Report.

There being no further business, the Attorney General adjourned the Council at 12:00 pm.