Date: August 3, 2020
Time: 10:00am - 11:00am
Location: Virtual

Maryland Cybersecurity Coordinating Council

Meeting Minutes

Council Member Attendance:

Council Member	Title	Organization	Status
Charles “Chip” Stewart	SCISO & Chairman	DoIT	Present
Walter “Pete” Landon	Director	GoHS	Represented by Yesim Karaman
David Brinkley	Secretary	DBM	Absent
Ellington Churchill	Secretary	DGS	Represented by Eric Lomboy
Lourdes Padilla	Secretary	DHS	Absent
Robert Green	Secretary	DPSCS	Present
Robert Neall	Secretary	MDH	Represented by Herb Jordan
Timothy Gowen	Adjutant General	DMIL	Represented by Col. Reid Novotny
Russell Strickland	Director	MEMA	Present
Woodrow Jones	Superintendent	MSP	Represented by Maj. Tawn Gregory
Gregory Slater	Secretary	MDOT	Represented by Ken Hlavacek

Call to Order: Chip Stewart

Vote to Approve Meeting Minutes (February 24, 2020)

Council approved minutes, no objections.

Major Cybersecurity Incident Review

Maryland is moving from the Lockheed model (Kill Chain) to the MITRE ATT&CK Framework.
The Kill Chain Model is displayed on a slide, and includes the following information:

1. *Recon*
2. *Weaponize*
3. *Deliver*
4. *Exploit*
5. *Install*
6. *C&C*
7. *Action*

Changing Threat Landscape

Changes are seen in attacks against Enterprise, using access points to gain entry. Ransomware—nationally, there has been about a 180% increase in incidents since last year.
Two State agency incidents and one county incident occurred. Two of these incidents were running outdated remote desktop protocol, and one outdated VPN--both appeared in Shodan.

- We must guess what may have happened, because it is difficult to go back in time when logs are not good.
- All attacks involved admin level access.
- How do we break the chain?
    - Through layers of security—adding and providing compensation to another layer; this does not always mean multiple firewalls, other controls are also important.
    - Through patch and vulnerability management—ensuring patches are deployed as soon as they have successful passed internal testing
    - Prohibiting at boundary of web applications (remote desktop)
    - Utilizing Shodan (search engine)—identifying potentially vulnerable State devices, and identifying unauthorized network boundaries.
- Technical debt involves postponing activities and investing in necessary infrastructure and governance initiatives.
    - Stewart says cybersecurity risk is the interest accrued on technical debt.
    - Essentially, the risk associated with technical debt compounds over time.

COVID Cybersecurity Response

DoIT is thankful to the National Guard's support, regarding the internet attack surface. The National Guard reviewed the security of the State's web applications (over 200), and identified important vulnerabilities.

The Security Operations Center (SOC)—internet attack assessment (30 applicants, 40 organizations)

New Business

Russell Strickland, Executive Director of MEMA, mentioned that MEMA still has grant money from the National Capital Region. Director Strickland would like to move this forward. Chip Stewart, SCISO of DoIT, indicated that DoIT will be assigning resources to initiate the project shortly.

Close

Meeting adjourned: 10:30am

Chairman of Board APPROVAL Charles I Stewart IV Charles I Stewart IV (Feb 1, 2021 15:26 EST) Date: Feb 1, 2021