Reforço na cibersegurança e preocupação estadunidense?

Raquel Spiri

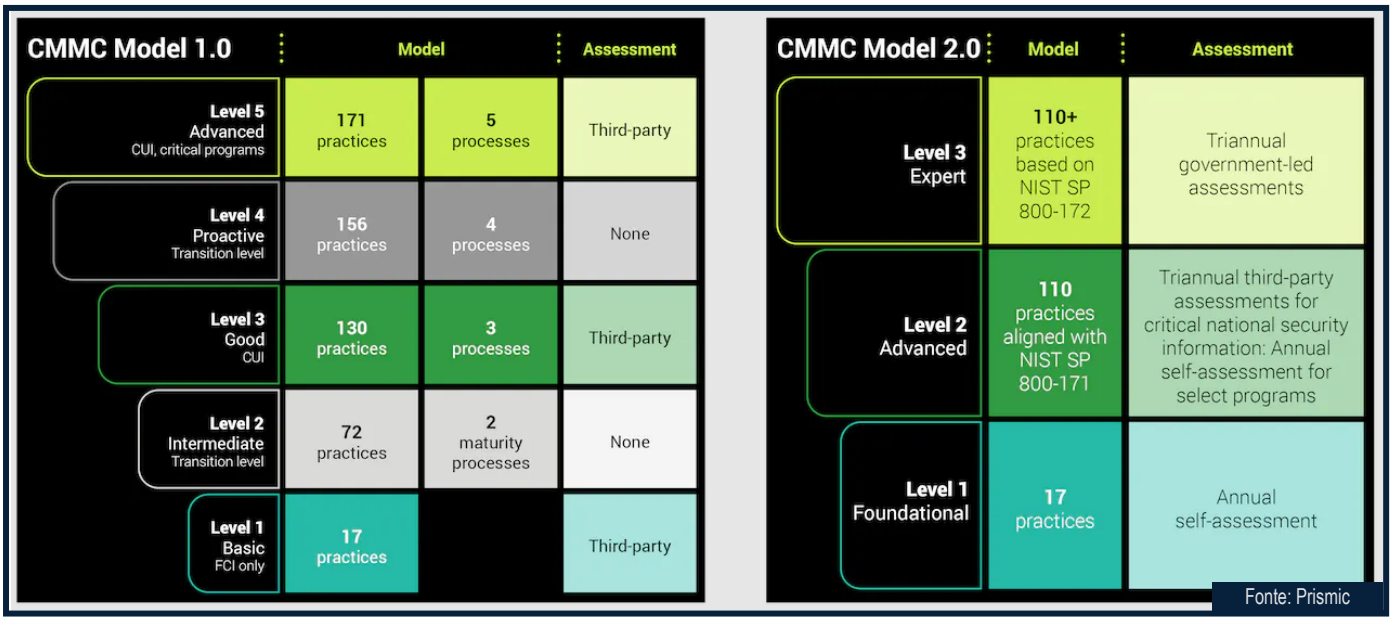
Em setembro de 2022, o Departamento de Defesa dos Estados Unidos (EUA) passou a exigir uma atualização da certificação que comprova a segurança cibernética das entidades com as quais mantém relações. O Modelo de Certificação de Maturidade de Cibersegurança 2.0 (CMMC, sigla em inglês) é uma revisão do primeiro, com adições que possuem como objetivo comprovar que qualquer entidade, em toda sua cadeia de organização, tem condições de promover os maiores níveis de cibersegurança de acordo com os moldes estabelecidos pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos. Segundo especialistas de segurança, o principal argumento favorável à CMMC é que a certificação garante a cibersegurança marítima, pois todos os parceiros comerciais neste setor deverão se atualizar no que diz respeito à área.

Considerando essa recente mudança nas exigências em cibersegurança do Departamento de Defesa dos Estados Unidos, tem-se a seguinte hipótese: a necessidade de se comprovar a segurança cibernética, especialmente no mar, pode ter relação com a crescente presença de atores internacionais, como o Irã, em incidentes cibernéticos e roubo de informações.

Compreende-se que ainda em agosto de 2022, carregamentos israelenses sofreram ciberataques que foram atribuídos a um grupo de *hackers* iranianos. Mais recentemente, a Albânia tem sido alvo de ciberataques igualmente atribuídos ao Irã. Forças estadunidenses afirmam que os tipos de ataques não foram apenas para indisponibilizar serviços, mas também obter inteligência sobre os países.

Portanto, a conexão que se faz é entre o aumento dos ciberataques envolvendo o Irã e parceiros estadunidenses e a reação do Departamento de Defesa dos EUA em exigir legalmente o investimento em cibersegurança daqueles contratados pelo país. Isto, pois, fundamentalmente, a exigência da CMMC incluiu a contabilização da postura de segurança cibernética de parceiros terceirizados do Departamento de Defesa dos EUA, que devem fornecer informações ao governo sobre todas as suas operações, incluindo seus provedores de serviços gerenciados.

Dessa forma, entende-se que os Estados Unidos, tendo o controle sobre todas as informações que envolvem o Departamento de Defesa e seus contratados, podem sofisticar planos de resposta a incidentes cibernéticos, especialmente no mar, onde a cibersegurança ainda tem muito a ser desenvolvida.



DOI 10.21544/2446-7014.n169.p16.

REFERÊNCIAS

- **Reforço na cibersegurança e preocupação estadunidense?**

ACOHIDO, Byron. The cybersecurity sea change coming with the implementation of 'CMMC' - Security Boulevard. **Security Boulevard**, 07 set. 2022.. Acesso em: 13 set. 2022.

Suspected Iranian Actor Targeting Israeli Shipping, Healthcare, Government and Energy Sectors. **Mandiant**, 17 ago. 2022. Acesso em: 13 set. 2022.