IT2TA de maio apresenta o Quadro Nacional de Certificação em Cibersegurança

Lisboa - 13 de junho, 2022 - O itSMF Portugal realizou mais uma edição do **It's Time To Talk About a 24 de maio**. A sessão contou com a participação de **Vasco Vaz**, consultor no Centro Nacional de Cibersegurança desde 2020, e de **António Costa**, Consultor no Departamento de Desenvolvimento e Inovação também do Centro Nacional de Cibersegurança, que nos falaram sobre a Edificação do Quadro Nacional de Certificação em **Cibersegurança**.

O CNCS foi criado em 2014 e é a Autoridade Nacional de Cibersegurança que **promove um uso do ciberespaço de forma livre, confiável e segura**, nomeadamente através de mecanismos de cooperação nacional e internacional para a criação de políticas públicas que conduzam ao cumprimento do seu objetivo primordial. As pessoas são o principal fator de preocupação e foco com a sensibilização e com a capacitação em matéria de cibersegurança.

Na área das políticas públicas, o CNCS desenvolve várias diretivas e quadros de referência para as organizações implementarem soluções de cibersegurança em fases diferentes.

O Decreto-Lei 65/2021 regulamenta o Regime Jurídico da Segurança do Ciberespaço e vem dar corpo a algumas atribuições, nomeadamente a designação de uma Autoridade Nacional para a Certificação de Cibersegurança, o que lhe permite **desenvolver esquemas de certificação nacional**, por exemplo.

Para divulgação desta parte da regulamentação foi feito o Roadshow 2022 (com a duração de quatro horas por sessão, em média) que teve como principais destinatários a Administração Pública, os operadores de infraestruturas críticas, os operadores de serviços essenciais e os prestadores de serviços digitais. **Os conteúdos incluíram medidas constantes nos diplomas legais, plano de segurança e determinação de quem deverão ser os responsáveis pela área no seio dessas mesmas entidades.**

Os principais desafios que atualmente se encontram em matéria de cibersegurança em Portugal passam pelos ataques de *phishing* e *ransomware*; o cibercrime é cada vez mais profissional e quase sempre tem ligações ao contexto geopolítico e pandémico. Face a esta análise, as tecnologias emergentes ainda colocam novos desafios. Os ciberataques são cada vez mais automatizados e o fator humano continua a ser o que obriga a uma crescente

sensibilização, maior ainda depois do contexto de teletrabalho que, em muitos casos, veio para ficar.

A atual Estratégia Nacional de Segurança no Ciberespaço está válida até 2023, mas não é um documento estanque; sofre anualmente uma revisão através dos seus planos de ação, decorrentes da entrada de novos atores no universo da cibersegurança, massificação dos mesmos e rapidez do desenvolvimento tecnológico.

Outra área do CNCS em que é feita uma análise crítica dos acontecimentos é o observatório que olha para a cibersegurança num contexto multidisciplinar, desde a política à sociedade, ética, economia ou direito, mas sem esquecer a importância do desenvolvimento de novidades. **Este observatório publica anualmente um conjunto de relatórios, identificando riscos e propondo políticas públicas para a área da capacitação, inovação e digitalização**. É com base nestes relatórios que se concluiu que o nível de incidentes tem vindo a crescer, tal como o cibercrime (numa curva oposta ao crime físico), o que é um ponto de alerta para o CNCS.

Outro número preocupante que o relatório revelou foi o de 2% de alunos formados em 2020, no universo total de diplomados em tecnologias de informação e comunicação com cursos denominados de cibersegurança. “Há poucos cursos e uma necessidade de criar políticas para o desenvolvimento desta área”, sublinha António Costa.

Em breve serão instalados sete centros de competência no país para se criar uma ligação contínua com o CNCS, ajudando a estabelecer relações próximas às entidades.

O esquema de certificação para o Quadro Nacional de Referência para a Cibersegurança destina-se a organizações abrangidas pelo regime jurídico da segurança do Ciberespaço, nomeadamente organizações da Administração Pública, local e central, sobretudo os organismos TIC e prestadores de serviços digitais.

Quais são os objetivos de obter um certificado em cibersegurança? Atestar a conformidade da implementação das medidas estabelecidas contra ameaças e ajudar a cumprir com as exigências legais para prevenir e resolver incidentes de cibersegurança. “O processo de análise e gestão de risco é fundamental e tem de ser feito logo no início para as organizações perceberem os riscos a que estão expostas e perceberem do que necessitam em termos de medidas complementares”, nota Vasco Vaz.

O próximo evento do itSMF Portugal é um HOT – Hands on Talk a 21 de junho sobre “R&D on paper and cellulose IoT devices for secure asset management and track & trace”. Esta sessão contará com a participação de Carlos Silva, Luís Pereira e Yoni Engel, da Almascience que, no âmbito dos projetos para a inovação sustentável, irão abordar o tema.