Colóquio CTIR Gov – 2013

"Os Desafios do atual cenário de tratamento de incidentes"

Data: 17 de maio de 2013
Horário: 8h30 às 17h30
Participantes: Equipes de tratamento de incidentes de segurança em rede de computadores dos Órgãos e Entidades da Administração Pública Federal, dos Estados e Distrito Federal.
Local: Auditório do Anexo I – Palácio do Planalto – Brasília DF.

Programação:

Horário	Evento	Órgão	Responsável
8h30 às 9h	Recepção / Credenciamento	CTIR Gov	CTIR Gov / DSIC
9h às 9h20	Abertura do evento (1)	GSIPR	GSIPR/DSIC/CGTIR
9h20 às 10h10	Avaliação da segurança da informação no âmbito da APF (2)	TCU/ SEFTI	Pedro Coutinho Filho
10h10 às 10h20	Intervalo – Café	--	--
10h20 às 11h10	Anatomia de ataques a servidores SIP (3)	CERT.br	Klaus Steding-Jessen
11h10 às 12h	Coordenação da defesa cibernética pelo CDCiber (4)	MD/EB/CDCiber	Cel Camelo e Maj Jeferson
12h às 14h	Intervalo – Almoço	--	--
14h às 14h50	Tratamento de incidentes de segurança na Rede Acadêmica Brasileira (5)	CAIS/RNP	Atanai Sousa Ticianelli
14h50 às 15h40	Desafios de segurança em plataformas móveis (6)	BMB/FEBRABAN	Antônio Ricardo Gomes Leocádio
15h40 às 16h	Intervalo – Café	--	--
16h às 16h50	Implicações da Lei nº 12.737 no tratamento de incidentes (7)	SRCC/DPF/MJ	SRCC/DPF/MJ
16h50 às 17h30	Debates		Todos os palestrantes e CTIR Gov

(1) ***Abertura do Evento***: Boas vindas aos participantes; ações recentes do CTIR Gov/DSIC/GSIPR;
(2) ***Avaliação da Segurança da Informação no âmbito da APF.*** Abordando, do ponto de vista do TCU, a avaliação da governança de tecnologia da informação no âmbito da administração pública federal, especificamente quanto à implantação da segurança da informação e equipes de tratamento de incidentes de segurança. Constatação de deficiências, oportunidades de melhorias e recomendações;
(3) ***Anatomia de ataques a servidores SIP*** (Session Initiation Protocol): Buscará mostrar o *modus operandi* dos ataques SIP, além de apresentar recomendações para prevenir os diferentes tipos de abusos observados em servidores SIP;
(4) ***Coordenação da defesa cibernética pelo CDCiber:*** Apresentação pelo Centro de Defesa Cibernética (CDCiber), do Exército Brasileiro/MD, dos desafios operacionais para a implantação e coordenação da defesa cibernética de grandes eventos;
(5) ***Tratamento de incidentes de segurança na Rede Acadêmica Brasileira:*** Abordando a abrangência, ferramentas e mecanismos utilizados, especificamente quanto à implantação da segurança da informação e equipes de tratamento de incidentes de segurança. Constatação de precariedades, oportunidades de melhorias e recomendações técnicas.
(6) ***Desafios de segurança em plataformas móveis:*** Apresentação do estudo sobre o entendimento do ambiente *Mobile Malware,* visando a sensibilização sobre os aspectos de segurança da informação em dispositivos móveis.
(7) ***Implicações da Lei nº 12.737 no tratamento de incidentes:*** Apresentação pelo Serviço de Repressão ao Crime Cibernético (SRCC), do Departamento de Polícia Federal, das implicações da Lei nº 12.737, que dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Orientações para a preservação e coleta de evidências; prova pericial e manutenção da cadeia de custódia no tratamento de incidentes de segurança.