APRIMORAR SEGURANÇA DE SISTEMAS DE INFORMAÇÃO A PARTIR DOS PILARES: AUDITORIA COM APOIO DE FERRAMENTA PARA TESTES DE INVASÃO E CAPACITAÇÃO DE EQUIPES DE DESENVOLVIMENTO DE SISTEMAS

Denis Clayton Alves Ramos
CCUEC/UNICAMP
E-mail: clayton@ccuec.unicamp.br

Resumo: A plataforma WEB revolucionou os sistemas de informação facilitando o acesso a estes de qualquer ponto na internet. Contudo, tanto as características dela como as tecnologias envolvidas na construção de sistemas para esta plataforma, potencializam vulnerabilidades de segurança. Apesar dos recursos complementares a plataforma para reforço da segurança (firewall, SSL etc.), é imprescindível, sob a perspectiva de codificação / programação, que desenvolvedores tratem deste assunto durante todo o ciclo de desenvolvimento e ao longo da vida útil dos sistemas em produção. Existe uma infinidade de vulnerabilidades e técnicas de invasão de sistemas a serem usadas, tornando este assunto complexo. Como resposta a estes desafios, algumas medidas são: difundir conhecimentos práticos sobre o tema. Nesse sentido, foram realizadas quatro capacitações: a) Café Cinfotec 02/2014; b) 3º Cinfotec UNICAMP 05/2014; c) Treinamento Diretoria Desenvolvimento Sistemas (DDS) do CCUEC por duas vezes, abrangendo ao todo mais de 100 analistas de sistemas desta universidade. Foram elaborados guias de boas e más práticas de codificação desenvolvidos in house; além da criação de canal de divulgação de vulnerabilidades em APIs, frameworks etc. via Redmine acessível a qualquer usuário com conta no LDAP UNICAMP. Nestas capacitações, foi demonstrado a invasão de um sistema de exemplo. Outra ação foi a prospecção de ferramenta para teste de invasão de sistemas e a criação de um processo de auditoria de sistemas na DDS/CCUEC baseado na ferramenta escolhida. Há quase um ano este processo é executado periodicamente analisando vários sistemas corporativos desenvolvidos e mantidos por esta unidade.

Palavras-chave: Segurança de sistemas de informação. Programação segura. Auditoria. Teste de invasão. Difusão de conhecimento. Boa e má prática de segurança

Eixo 1: Administração e gestão