REDE MOCAMBICANA DOS
DEFENSORES DE DIREITOS HUMANOS
RMDDH

Terça - feira, 9 de Novembro de 2021 I Ano 02, n.° 16 I **Director:** Prof. Adriano Nuvunga I **Português**

RMDDH treina defensores de direitos humanos em segurança digital

No âmbito da sua missão de fortalecer as capacidades de resiliência dos defensores de direitos humanos, a Rede Moçambicana dos Defensores de Direitos Humanos (RMDDH) realizou ontem um treinamento em Segurança Digital. O treinamento contou com a participação de 20 defensores de direitos humanos e decorreu em formato híbrido, sendo que a parte presencial teve lugar na Cidade de Maputo.

O objectivo do treinamento é dotar os defensores de direitos humanos de conhecimentos sobre medidas e ferramentas para proteger informações pertinentes no âmbito

das suas actividades de defender a dignidade humana, lutar contra injustiças e impedir o fechamento do espaço cívico em Moçambique.

O Presidente da RMDDH, Adriano Nuvunga, fez a abertura da sessão de treinamento e salientou a importância do mesmo para que os defensores de direitos humanos tenham capacidade de se prevenir ou reagir em casos de ataques cibernéticos.

O treinamento foi facilitado por Reginaldo Mulamula que, além de menção sobre a importância do treinamento em segurança digital, apresentou a definição de segurança digital, a estratégia de segurança digital, as ameaças à segurança de informação, bem como instruiu sobre como fazer a gestão de risco e medidas de protecção de activos digitais.

A maioria dos ataques tem sucesso porque as pessoas não têm conhecimento ou habilidades para lidar com ataques cibernéticos. Com efeito, o facilitador do treinamento salientou que os ataques virtuais são reais para as organizações, assim como para indivíduos, e podem resultar em perdas financeiras, danos à reputação e exposição social.

Segurança digital é um conjunto de medidas e ferramentas usadas para a protecção de activos digitais (documentos, software, sites, perfis corporativos e pessoais) e infra-estrutura tecnológica no geral contra ataques cibernéticos. (NIST, 1977)

Segundo o facilitador do treinamento, a segurança digital é importante pois permite que os defensores de direitos humanos previnam e se protejam de ataques com o objectivo de aceder e visualizar informação privilegiada sem permissão, roubo, alteração ou eliminação de informação.

Estratégia de segurança digital e ameaças à segurança de informação

O facilitador do treinamento partilhou a estratégia de segurança digital de uma organização, explicando que ela é composta não só pela tríade CIA, mas também pelos colaboradores (as pessoas), pelos processos e pela tecnologia. Segundo o facilitador, os colaboradores devem compreender e estar em conformidade com as políticas de segurança de dados. Afir-

mou que as organizações devem ter políticas de tecnologia de informação e processos a seguir em casos de ataques cibernéticos, sejam eles bem-sucedidos ou não.

Sobre as ameaças à segurança de informação, o facilitador referiu que se trata de evento natural ou causado por humanos com potencial de causar impacto negativo. Existem três principais formas de ameaça à segurança de informação: Phishing, Malware e Engenharia Social.

O phishing consiste na prática de envio de e-mails fraudulentos que se assemelham a e-mails de fontes confiáveis. O objectivo é roubar dados confidenciais, como números de cartões de crédito e informações de login. É o tipo mais comum de ataque virtual. Como soluções para este tipo de ataque, o facilitador sugeriu um software de filtragem de e-mails mal-intencionados. O malwares são softwares mal-intencionados, projectados para obter acesso indevido a sistemas. Fazem parte de malwares os vírus, worm, trojans, rootkits, spyware e ransomwares.

Sobre a engenharia social, o facilitador informou que esta se traduz na tática usada para manipular vítimas a fornecer informações confidenciais. Podem solicitar um pagamento ou obter acesso a dados confidenciais. A engenharia social pode ser combinada a qualquer ameaça listada anteriormente, de forma a manipulá-la a clicar em links, baixar malwares ou confiar em uma fonte mal-intencionada. Para este tipo de ameaça, o facilitador do treinamento sugere que sejam desenvolvidas estratégias de backup e recuperação de dados; softwares de descriptografia, evitar fornecer informações confidências a estranhos e pagar o resgate na esperança de ver os dados descriptografados.

Gestão de risco

Neste ponto, o facilitador do treinamento começou por dizer que risco é a probabilidade de ocorrência de um evento que tenha impacto negativo, especificamente em activos de sistemas de informação. O processo de gestão de risco é interativo (realizado inúmeras vezes), pois o ambiente de negócios é dinâmico, novas ameaças e vulnerabilidades surgem todos

dias. As medidas usadas para mitigação do risco devem estar equilibradas entre o custo, a eficácia e o valor do activo a ser protegido. Não é possível indentificar todos riscos, muito menos mitigar todos riscos, o risco remanescente denomina-se "risco residual".

O faciltador referiu que o processo de gestão de risco consiste em:

- Identificação de activos e estimativa de seu valor. Inclui pessoas, edifícios, hardware, software, dados (electrónicos, impressos, outros), consumíveis;
- Avaliação da ameaça. Inclui actos da natureza, actos de guerra, acidentes, actos maliciosos originados de dentro ou fora da organização;
- Avaliação de vulnerabilidade: Avaliar políticas, procedimentos, normas, treinamentos, segurança física, controlo de qualidade e segurança técnica;
- Cálculo do impacto que cada ameaça teria em cada activo. Usa-se análise qualitativa ou análise quantitativa;
- Identificação, selecção e implementação dos controles apropriados. Fornecimento de uma resposta proporcional. Considera-se a productividade, a relação custo-eficácia e o valor do activo e;
- Avaliação da eficácia das medidas de controlo. Garantir que os controlos forneçam a protecção económica necessária sem perda perceptível de productividade.

Medidas de protecção de activos digitais

Sobre as medidas de protecção de activos digitais, o facilitador recomendou a partilha de ficheiros via servidor ou mapeamentos na nuvem. A partilha de arquivos é uma actividade comum nas organizações e sempre que for necessário faze-lo, deve ser feito por via de partilhas de rede criadas pelo departamento de tecnologias de informação em oposição a dispositivos de armazenamento em massa que podem estar infectados por vírus.

O facilitador também recomendou a utilização de senhas fortes ou complexas. Senhas simples, como datas de nascimento ou sequências numéricas, representam pontos vulneráveis em sistemas de informação. A política de segurança deve forçar a utilização de senhas complexas, que não sejam curtas e que incluam caracteres alfanuméricos. As senhas devem ter período de validade. O facilitador sugeriu ainda ignorar e-mails suspeitos e usar ferramentas de protecção digital.

Autora: Sheila Nhancale

Rua de Dar-Es-Salaam Nº 279, Bairro da Sommerschield, Maputo - Moçambique +258 21 418 336
www.cddmoz.org info@redemoz-defensoresdireitoshumanos.org @CDD_Moz https://web.facebook.com/RMDDHMoz