ACADEMIA HUMANITÁRIA · HUMANITAIRES JOBS

Mini MBA Segurança e gestão de riscos: proteger as equipas e manter o acesso

Material do curso · Semana 9 : Segurança digital e proteção da informação

Programa de exatamente 3 meses (12 semanas, 144 horas) para gerir a segurança e os riscos de uma organização humanitária: dever de proteção, análise do contexto, avaliação dos riscos, planos e procedimentos, aceitação e negociação do acesso, incidentes, gestão de crise e rapto, saúde e bem-estar do pessoal, segurança digital e proteção de dados, riscos da organização e conformidade, partilha do risco com os parceiros, governação e continuidade de atividade. Exercícios numéricos corrigidos, três exames mensais com estudos de caso e um diploma verificável da Academia Humanitária.

https://humanitairejobs.org/pt/academia/mini-mba-securite-risques/semaine-9/

Documento gratuito da Academia Humanitária. Pode ser impresso e partilhado livremente para fins de formação, sem modificações.

Semana 9 : Segurança digital e proteção da informação

Objetivos

- Identificar as ameaças digitais próprias das organizações humanitárias: phishing, fraude na transferência bancária, vigilância, fuga de dados.
- Pôr em prática medidas de base proporcionadas: autenticação, cópias de segurança, cifragem, gestão de acessos, dispositivos.
- Proteger os dados das pessoas assistidas e do pessoal, e reagir a um incidente digital.

Porque é que o digital é um risco de segurança

As organizações humanitárias detêm informações muito sensíveis: listas de beneficiários (por vezes com biometria e localização), testemunhos de violações, dados médicos, informações sobre o pessoal, análises de segurança, movimentos. Uma fuga ou um ataque informático pode pôr **vidas** em perigo, não apenas dados.

Vários ciberataques conhecidos visaram organizações humanitárias, incluindo o roubo de dados de centenas de milhares de pessoas vulneráveis. As organizações são também alvo de fraude financeira em linha e de **vigilância** das comunicações por atores estatais ou não estatais.

Principais ameaças:

- **Phishing** (mensagens fraudulentas): falsos e-mails ou mensagens que roubam credenciais ou instalam software malicioso.
- **Fraude na transferência bancária**: falso fornecedor, falso diretor a pedir um pagamento urgente, alteração fraudulenta de dados bancários.
- **Ransomware**: cifragem dos dados em troca de resgate.
- **Roubo ou apreensão de dispositivos** (computadores, telemóveis) nos postos de controlo ou durante assaltos.
- **Vigilância** das comunicações e das redes sociais.
- **Erros internos**: partilha por engano, ficheiro enviado ao destinatário errado, palavra-passe à vista.

As medidas de base

Algumas medidas simples bloqueiam a grande maioria dos ataques comuns:

- **Autenticação multifator** (MFA) no correio eletrónico, no armazenamento em linha, no banco e no software de contabilidade.
- **Gestor de palavras-passe** e palavras-passe longas e únicas.
- **Atualizações** automáticas dos sistemas e das aplicações.

- **Cópias de segurança** regulares, das quais uma cópia offline ou isolada, e testes de restauro (regra 3-2-1: três cópias, dois suportes diferentes, uma cópia fora do local).
- **Cifragem** dos discos dos computadores portáteis e dos telemóveis.
- **Gestão de acessos**: cada pessoa só acede ao que precisa; remoção dos acessos no dia da saída de um trabalhador.
- **Formação** regular, com exercícios de phishing simulados.

Exemplo de exercício. Um falso e-mail de phishing é enviado a 120 trabalhadores: 38 clicam na ligação (31,7 %), 14 introduzem as suas credenciais (11,7 %), 9 comunicam o e-mail ao serviço informático (7,5 %). Após uma formação direcionada, um segundo exercício dá 12 cliques (10 %), 3 introduções de credenciais (2,5 %) e 41 comunicações (34,2 %). O aumento das comunicações é tão importante como a descida dos cliques: transforma o pessoal num sistema de alerta.

Fraude na transferência bancária e procedimentos financeiros

A **fraude do CEO** e a fraude nos dados bancários custam todos os anos somas importantes às organizações, incluindo as humanitárias. Os procedimentos financeiros são a melhor defesa:

- Qualquer **alteração dos dados bancários** de um fornecedor ou de um trabalhador é verificada por uma chamada para um número já conhecido, nunca para o indicado no pedido.
- Nenhum pagamento urgente fora do procedimento, mesmo a pedido aparente de um diretor: a dupla validação continua obrigatória.
- Os acessos ao banco em linha utilizam dispositivos e contas dedicados, com dupla assinatura eletrónica.
- O pessoal sabe que será **apoiado** se recusar um pagamento suspeito, mesmo pedido por um superior.

> A urgência e a confidencialidade são as duas alavancas preferidas dos burlões: «Estou em reunião, faz já esta transferência e não digas nada a ninguém.»

Dispositivos, postos de controlo e vigilância

No terreno, os riscos digitais são também **físicos**:

- Nos postos de controlo, os telemóveis podem ser revistados. Um telemóvel que contenha fotografias de posições militares, mensagens críticas em relação a uma das partes ou listas de beneficiários pode levar a uma detenção. Regra: transportar apenas o necessário, apagar os dados sensíveis dos dispositivos de terreno, utilizar dispositivos dedicados ao trabalho.
- As **redes sociais** do pessoal revelam informações exploráveis: localização em tempo real, opiniões políticas, fotografias de colegas, sinais de riqueza. Uma política sobre a utilização das redes sociais, explicada e não punitiva, reduz estes riscos.

- As **aplicações de mensagens** cifradas de ponta a ponta protegem o conteúdo, mas não o facto de se estar a comunicar, nem o próprio telemóvel se for apreendido desbloqueado.
- A utilização de certas ferramentas (satélites, VPN, drones) pode ser proibida ou suspeita: verificar a legislação e a aceitação.

Proteger os dados das pessoas

A **proteção dos dados** dos beneficiários e do pessoal assenta em princípios reconhecidos (nomeadamente o manual do CICV e do Brussels Privacy Hub sobre a proteção de dados na ação humanitária):

- **Licitude e finalidade**: base legítima e finalidade precisa para cada recolha.
- **Minimização**: recolher apenas o que é necessário.
- **Consentimento informado** quando é essa a base escolhida, tendo em conta as relações de poder (um agregado familiar que precisa de ajuda não é livre de recusar).
- **Segurança**: cifragem, acessos limitados, registo de atividade.
- **Conservação limitada** e eliminação no fim da finalidade.
- **Partilha enquadrada** por acordos de partilha de dados, com uma análise dos riscos (incluindo pedidos de autoridades ou de partes no conflito).
- **Avaliação de impacto** antes de qualquer novo sistema (biometria, pagamento móvel, plataforma partilhada).

Exemplo de minimização. Para uma distribuição de kits, é preciso identificar o agregado familiar e verificar que ainda não recebeu o kit. A pertença étnica ou religiosa não é necessária e não deve ser recolhida; a fotografia e a impressão digital geralmente também não.

Reagir a um incidente digital

Um incidente digital (conta pirateada, computador roubado, ransomware, ficheiro enviado por engano) trata-se como um incidente de segurança:

- **Conter**: mudar as palavras-passe, revogar as sessões, isolar o dispositivo infetado, apagar remotamente um dispositivo roubado.
- **Avaliar**: que dados, que pessoas, que risco para elas?
- **Informar**: direção, encarregado da proteção de dados, pessoas em causa se estiverem expostas a um risco, autoridades de controlo segundo o direito aplicável, doadores segundo os contratos.
- **Restaurar** a partir das cópias de segurança; não pagar um resgate sem decisão da direção e análise jurídica.
- **Aprender**: análise, correções, formação.

Exemplo. Um computador portátil não cifrado com a lista de 3 200 agregados familiares, os seus números de telefone e a sua localização é roubado durante um assalto. O risco para as pessoas depende do contexto: se certos agregados pertencerem a um grupo visado, é elevado. Ações: avaliação imediata, informação das comunidades em causa por canais seguros se

estiverem expostas, alteração das modalidades de contacto, cifragem obrigatória de todos os computadores portáteis.

Exercício: um e-mail urgente do diretor

Situação. Numa sexta-feira às 17 h, a contabilista recebe um e-mail aparentemente do diretor de país, que está em deslocação: «Confidencial. Temos de pagar hoje o adiantamento de 48 000 USD ao novo fornecedor de combustível, senão perdemos o contrato. Dados bancários em anexo. Não estou contactável, reunião com o ministro.» O endereço de envio difere numa letra do endereço habitual. No mesmo dia, um fornecedor habitual pediu por e-mail para alterar os seus dados bancários. O correio eletrónico da organização não tem autenticação de dois fatores.

Trabalho pedido. 1) Sinais de alerta. 2) Conduta imediata. 3) Medidas duradouras.

Correção. 1) Urgência, confidencialidade, indisponibilidade do requerente, novo fornecedor sem processo de compra, endereço de envio ligeiramente diferente, pedido paralelo de alteração de dados bancários. 2) Não pagar; ligar ao diretor para o seu número conhecido (ou ao seu adjunto); não alterar os dados do fornecedor habitual sem chamada de verificação para um número já conhecido; comunicar ao responsável informático e às finanças; conservar os e-mails como provas. 3) Autenticação de dois fatores em todo o correio eletrónico; regra escrita: nenhum pagamento fora do procedimento, dupla validação, verificação telefónica de qualquer alteração bancária; formação e exercícios de phishing; filtragem dos domínios semelhantes; mensagem clara da direção: recusar um pagamento suspeito será sempre apoiado.

A reter

- Os dados humanitários são sensíveis: uma fuga pode pôr vidas em perigo.
- MFA, palavras-passe únicas, atualizações, cópias de segurança 3-2-1, cifragem, acessos mínimos, formação.
- Fraude na transferência: verificação por um número conhecido, dupla validação, apoio a quem recusa.
- Terreno: dispositivos aligeirados nos postos de controlo, política sobre as redes sociais.
- Proteção de dados: finalidade, minimização, segurança, conservação limitada, avaliação de impacto.

Quiz

1. 150 trabalhadores recebem um falso e-mail; 24 clicam. Taxa de cliques:
   A. 24 %
   B. 16 %
   C. 6,25 %
   D. 15 %

2. A regra de cópias de segurança 3-2-1 significa:
   A. 3 cópias, 2 suportes diferentes, 1 cópia fora do local
   B. 3 palavras-passe, 2 fatores, 1 conta
   C. 3 dias, 2 semanas, 1 mês
   D. 3 servidores, 2 países, 1 nuvem

3. Um fornecedor pede por e-mail para alterar os seus dados bancários. O que faz?
   A. Altera imediatamente
   B. Paga em numerário
   C. Responde ao e-mail
   D. Verifica por uma chamada para o número já conhecido

4. Para uma distribuição de kits, recolher a pertença étnica dos agregados familiares é:
   A. Obrigatório
   B. Recomendado
   C. Contrário ao princípio de minimização se não for necessário
   D. Sem risco

5. É roubado um computador não cifrado com listas de beneficiários. Primeiro passo:
   A. Comprar outro computador
   B. Avaliar os dados expostos e o risco para as pessoas, e depois informar
   C. Não dizer nada
   D. Publicar um comunicado

Respostas do quiz : 1. B · 2. A · 3. D · 4. C · 5. B