**Análise de Relatório de Incidente**

| **Resumo** | Nesta manhã, uma estagiária relatou ao departamento de TI que não conseguia fazer login em sua conta na rede interna. Os logs de acesso indicaram que a conta dela estava ativamente acessando registros no banco de dados de clientes, mesmo com o acesso bloqueado.  A estagiária informou que recebeu um e-mail pedindo para acessar um site externo e inserir suas credenciais da rede interna para recuperar uma mensagem. Acreditamos que esse foi o método usado por um agente malicioso para obter acesso à nossa rede e ao banco de dados de clientes.  Outros funcionários também notaram que diversos registros de clientes estavam faltando ou continham dados incorretos. Isso indica que, além do vazamento de informações, dados foram excluídos ou manipulados. | | |
| --- | --- | --- | --- |
| Identificar | A equipe de gerenciamento de incidentes realizou uma auditoria nos sistemas, dispositivos e políticas de acesso envolvidas no ataque para identificar falhas de segurança.  Foi identificado que o login e a senha da estagiária foram capturados por um invasor e utilizados para acessar dados no banco de clientes. A revisão inicial aponta que houve exclusão de dados. | | |
| Proteger | A equipe implementou novas políticas de autenticação para evitar futuros ataques:   * Ativação de autenticação multifator (MFA) * Limitação de tentativas de login a três * Treinamento obrigatório para todos os colaboradores sobre proteção de credenciais   Além disso, uma nova configuração de firewall será aplicada e será feito investimento em um sistema de prevenção de intrusão (IPS). | | |
| Detectar | Para detectar acessos não autorizados futuros, a equipe utilizará:   * Ferramenta de registro de logs do firewall * Sistema de detecção de intrusos (IDS) para monitorar todo o tráfego de entrada da internet | | |
| Responder | A conta de rede da estagiária foi desativada. Todos os estagiários e colaboradores passaram por treinamento sobre segurança de credenciais.  A alta gestão foi informada e irá contatar os clientes por correspondência sobre a violação de dados. A organização também notificará as autoridades competentes, conforme exigido por lei. | | |
| Recuperar | A equipe realizará a recuperação dos dados excluídos por meio do backup completo da noite anterior.  Os colaboradores foram informados de que quaisquer alterações feitas no sistema durante a manhã não estarão no backup, e essas informações precisarão ser inseridas novamente após a restauração. | | |

| Observações e Reflexões:  Este incidente ressalta a importância de treinar os colaboradores sobre phishing e engenharia social. Reforçar políticas de segurança e implementar camadas adicionais de proteção é essencial para reduzir riscos e aumentar a resiliência da organização. |
| --- |