**Análise de relatórios de incidentes - Exemplo**

|  |  |
| --- | --- |
| **Resumo** | Nesta manhã, uma estagiária relatou ao departamento de TI que não conseguiu fazer login em sua conta de rede interna. Os logs de acesso indicam que sua conta está acessando ativamente os registros no banco de dados do cliente, mesmo que ela esteja bloqueada dessa conta. A estagiária indicou que recebeu um e-mail esta manhã pedindo que ela fosse a um site externo para fazer login com suas credenciais de rede interna para recuperar uma mensagem. Acreditamos que este é o método usado por um ator mal-intencionado para obter acesso à nossa rede e banco de dados de clientes. Alguns outros funcionários notaram que vários registros de clientes estão ausentes ou contêm dados incorretos. Parece que não apenas os dados do cliente foram expostos a um ator mal-intencionado, mas que alguns dados também foram excluídos ou manipulados. |
| Identificar | A equipe de gerenciamento de incidentes auditou os sistemas, dispositivos e políticas de acesso envolvidos no ataque para identificar as lacunas na segurança. A equipe descobriu que o login e a senha de um estagiário foram obtidos por um invasor mal-intencionado e usados para acessar dados de nosso banco de dados de clientes. Após a revisão inicial, parece que alguns dados do cliente foram excluídos do banco de dados. |
| Proteger | A equipe implementou novas políticas de autenticação para evitar ataques futuros: autenticação multifator (MFA), tentativas de login limitadas a três tentativas e treinamento para todos os funcionários sobre como proteger as credenciais de login. Além disso, implementaremos uma nova configuração de firewall de proteção e investiremos em um sistema de prevenção de intrusão (IPS). |
| Detectar | Para detectar novos ataques de acesso não autorizado no futuro, a equipe usará uma ferramenta de registro de firewall e um sistema de detecção de intrusão (IDS) para monitorar todo o tráfego de entrada da internet. |
| Responder | A equipe desativou a conta de rede do estagiário. Oferecemos treinamento para estagiários e funcionários sobre como proteger as credenciais de login no futuro. Informamos a alta administração deste evento e eles entrarão em contato com nossos clientes por correio para informá-los sobre o vazamento de dados. A administração também precisará informar as autoridades policiais e outras organizações, conforme exigido pelas leis locais. |
| Recuperar | A equipe recuperará os dados excluídos restaurando o banco de dados do backup completo da noite passada. Informamos à equipe que qualquer informação do cliente inserida ou alterada esta manhã não seria registrada no backup. Assim, eles precisarão inserir novamente essas informações no banco de dados depois que elas forem restauradas do backup da noite passada. |

|  |
| --- |
| Reflexões/Notas: |