### **Planilha de vazamento de dados**

**Resumo do incidente:** Um gerente de vendas compartilhou o acesso a uma pasta de documentos somente internos com sua equipe durante uma reunião. A pasta continha arquivos associados a um novo produto que não foi anunciado publicamente. Também incluía análises de clientes e materiais promocionais. Após a reunião, o gerente não revogou o acesso à pasta interna, mas alertou a equipe para aguardar a aprovação antes de compartilhar os materiais promocionais com outras pessoas.

Durante uma videochamada com um parceiro de negócios, um membro da equipe de vendas esqueceu o aviso do gerente. O representante de vendas pretendia compartilhar um link para os materiais promocionais para que o parceiro de negócios pudesse circular os materiais para seus clientes. No entanto, o representante de vendas acidentalmente compartilhou um link para a pasta interna. Mais tarde, o parceiro de negócios postou o link na página de mídia social da empresa presumindo que eram os materiais promocionais.

|  |  |
| --- | --- |
| **Controle** | **Menor privilégio** |
| **Problema(s)** | O gerente não revogou o acesso à pasta interna após a reunião. O funcionário compartilhou acidentalmente o link para a pasta inteira com um parceiro, que divulgou os dados confidenciais nas redes sociais. |
| **Revisão** | O NIST SP 800-53: AC-6 trata do princípio do menor privilégio, restringindo o acesso às informações estritamente necessárias. Ele também reforça a revisão periódica de permissões para evitar acessos indevidos. |
| **Recomendação(ões)** | Limitar o acesso a recursos sensíveis conforme a função do usuário.  Realizar auditorias regulares nos privilégios de acesso dos usuários. |
| **Justificativa** | Restringir links para arquivos internos apenas a funcionários evita vazamentos de dados. Além disso, auditorias frequentes realizadas por gerentes e equipes de segurança ajudam a monitorar e limitar a exposição de informações sensíveis. |

### **Security plan snapshot**

O NIST Cybersecurity Framework (CSF) usa uma estrutura hierárquica, tipo árvore, para organizar informações. Da esquerda para a direita, ele descreve uma ampla função de segurança, então se torna mais específico conforme se ramifica para uma categoria, subcategoria e controles de segurança individuais.

|  |  |  |  |
| --- | --- | --- | --- |
| **Função** | **Categoria** | **Subcategoria** | **Reference(s)** |
| **Proteger** | PR.DS: Segurança de dados | PR.DS-5: Proteções contra vazamentos de dados. | NIST SP 800-53: AC-6 |

Neste exemplo, os controles implementados que são usados ​​pelo fabricante para proteger contra vazamentos de dados são definidos no NIST SP 800-53 — um conjunto de diretrizes para proteger a privacidade dos sistemas de informação.

Observação: as referências são comumente hiperlinkadas para as diretrizes ou regulamentações às quais se relacionam. Isso facilita aprender mais sobre como um controle específico deve ser implementado. É comum encontrar vários links para diferentes fontes nas colunas de referências.

### **NIST SP 800-53: AC-6**

O NIST desenvolveu o SP 800-53 para fornecer às empresas um plano de privacidade de informações personalizável. É um recurso abrangente que descreve uma ampla gama de categorias de controle. Cada controle fornece algumas informações importantes:

* Controle: Uma definição do controle de segurança.
* Discussão: Uma descrição de como o controle deve ser implementado.
* Melhorias de controle: Uma lista de sugestões para melhorar a eficácia do controle.

|  |  |
| --- | --- |
| **AC-6** | **Menor Privilégio** |
| Controle:  Apenas o acesso e a autorização mínimos necessários para concluir uma tarefa ou função devem ser fornecidos aos usuários. |
| Discussão:  Processos, contas de usuário e funções devem ser impostos conforme necessário para atingir o privilégio mínimo. A intenção é evitar que um usuário opere em níveis de privilégio maiores do que o necessário para atingir os objetivos de negócios. |
| Melhorias de controle:  ● Restrinja o acesso a recursos sensíveis com base na função do usuário.  ● Revogue automaticamente o acesso às informações após um período de tempo.  ● Mantenha registros de atividades de contas de usuários provisionadas.  ● Audite regularmente os privilégios do usuário. |

**Observação:** Na categoria de controles de acesso, o SP 800-53 lista o sexto privilégio mínimo, ou seja, AC-6.