Planilha de vazamento de dados

Resumo do incidente: Um gerente de vendas compartilhou o acesso a uma pasta de documentos internos (apenas para uso interno) com sua equipe durante uma reunião. A pasta continha arquivos relacionados a um novo produto que ainda não havia sido anunciado publicamente. Ela 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 aprovação antes de compartilhar os materiais promocionais com outras pessoas.

Durante uma chamada de vídeo com um parceiro de negócios, um membro da equipe de vendas esqueceu o aviso de seu gerente. O representante de vendas pretendia compartilhar um link para os materiais promocionais para que o parceiro de negócios pudesse distribuí-los aos seus clientes. No entanto, o representante de vendas compartilhou acidentalmente um link para a pasta interna. Posteriormente, o parceiro de negócios publicou o link na página de mídia social de sua empresa, presumindo que se tratava dos materiais promocionais.

Controle	**Privilégio mínimo**
Problema(s)	*A falta de escalonamento de privilégios no uso da pasta e o seu compartilhamento, pois o parceiro comercial não deveria ter acesso a tal informação e falha humana, onde houve o esquecimento do aviso do gerente sobre tal link.*
Revisão	*O que a NIST SP 800-53: AC-6 aborda? Aborda a privacidade da situação, sugerindo controles para aumentar a segurança na situação, pois se houvesse tais controles que impedissem que o membro da equipe compartilhasse o link com pessoas não autorizadas, o acesso seria restrito a pessoas da organização.*

Recomendação(ões)	*Como o princípio do privilégio mínimo poderia ser aprimorado na empresa? A empresa poderia implementar um método para restringir pessoas não autorizadas de compartilhar informações/links com terceiros, também uma forma de impedir que terceiros tivessem acesso sem autorização prévia, um controle que mantivesse acesso temporário a tais informações e um método de auditoria de acessos/privilégios.*
Justificativa	*Como essas melhorias poderiam resolver os problemas? Os problemas de acesso indevido seriam evitados, pois, se um usuário não possuísse as permissões necessárias para visualizar/editar/compartilhar tal informação seria necessário que um auditor liberasse seu acesso, o que por sua vez impediria que o vazamento ocorresse.*

Visão geral do plano de segurança

O NIST Cybersecurity Framework (CSF) utiliza uma estrutura hierárquica, semelhante a uma árvore, para organizar as informações. Da esquerda para a direita, ele descreve uma função de segurança ampla e, em seguida, torna-se mais específico à medida que se ramifica em categoria, subcategoria e controles de segurança individuais.

Função	Categoria	Subcategoria	Referência(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 na NIST SP 800-53 — um conjunto de diretrizes para proteger a privacidade dos sistemas de informação.

Observação: As referências geralmente contêm links 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 referência.

NIST SP 800-53: AC-6

O NIST desenvolveu a SP 800-53 para fornecer às empresas um plano personalizável de privacidade da informação. Trata-se de um recurso abrangente que descreve uma ampla variedade de categorias de controle. Cada controle fornece algumas informações essenciais:

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

AC-6	**Privilégio mínimo**
	Controle: Somente 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 aplicados conforme necessário para alcançar o privilégio mínimo. A intenção é evitar que um usuário opere em níveis de privilégio mais altos do que o necessário para cumprir os objetivos de negócio.
	Aprimoramentos do controle: • Restringir o acesso a recursos sensíveis com base na função do usuário. • Revogar automaticamente o acesso às informações após um período de tempo. • Manter registros de atividades das contas de usuários provisionadas. • Auditar regularmente os privilégios dos usuários.

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