CST0208-Políticas e procedimentos de Segurança Cibernética

Data do Post	@August 12, 2022 9:00 AM
Status	Not started
Palavras-chave	Políticas e procedimentos de Segurança Cibernética
Fonte	
Pronto	Preparado
IG post	☑
Publicado	☐

Post-Linkedin

A Política de Segurança Cibernética e da Informação é o documento que estabelece conceitos, directrizes e responsabilidades sobre os principais aspectos relacionados à segurança cibernética e segurança da informação, visando preservar os três pilares da segurança cibernética.

Esse artigo, retratará a de forma síntese as políticas e procedimentos da Segurança cibernética. Leia o artigo na íntegra.

Siga-me e veja outros posts no meu Instagram https://www.instagram.com/idaleciosilvatech/

Deixe o like para medirmos a repercussão do conteúdo.
Guarde para rever noutro momento.
Compartilha o conteúdo com os amigos e não só
Comente o que acha do conteúdo e da iniciativa e deixe sugestões.
Link do perfil no IG: https://www.instagram.com/idaleciosilvatech/
#cybersecurity #technology #linux #ataquescibernéticos #hacking #crimesvirtuais #despositivosmóveis #mobilidade #protection

Introdução

No processo de implementação de estratégias de segurança as empresas devem dedicar-se ao máximo para se que tomem as decisões mais acertadas e que todas elas sirvam para a protecção de todos os usuários dos serviços, sistemas e redes. Desse modo, devem ser definidas políticas e procedimentos estabelecem os comportamentos adequados dos usuários e os termos de uso de tais activos de TI.

Políticas

Uma política de segurança é um conjunto de objectivos de segurança para uma empresa que inclui regras de comportamento para os usuários e administradores e especifica os requisitos do sistema. Esses objectivos, regras e requisitos garantem, juntos, a segurança da rede, dos dados e dos sistemas de computador de uma organização.

Uma política de segurança abrangente realiza várias tarefas:

- Demonstra um comprometimento da empresa com a segurança.
- Define as regras para o comportamento esperado.
- Garante a consistência nas operações do sistema, nas aquisições, no uso e na manutenção de hardware e de software.
- Define as consequências jurídicas das violações.
- Dá o apoio da gestão à equipe de segurança.

Políticas de segurança informam os usuários, funcionários de uma empresa para a protecção de activos de tecnologia e de informação. Uma política de segurança também especifica os mecanismos necessários para atender aos requisitos de segurança.

Uma política de segurança normalmente inclui:

- **Políticas de identificação e autenticação** - Especifica pessoas autorizadas para acesso aos recursos de rede e define procedimentos de verificação.
- **Políticas de senhas -**Garante que as senhas atendam aos requisitos mínimos e sejam alteradas regularmente.
- **Políticas de uso aceitável -** Identifica os recursos e o uso da rede aceitáveis para a empresa. Também pode identificar ramificações para violações de política.
- **Políticas de acesso remoto -**Identifica como os usuários remotos podem acessar uma rede e o que é remotamente acessível.
- **Políticas de manutenção de rede -**Especifica procedimentos de actualização de sistemas operacionais e de aplicativos de usuários finais dos dispositivos de rede.
- **Políticas de tratamento de incidentes -**Descreve como os incidentes de segurança são tratados.

Um dos componentes de política de segurança mais comuns é uma política de uso aceitável (AUP). Esse componente define o que os usuários podem ou não fazer nos vários componentes do sistema. A AUP deve ser o mais explícita possível, para evitar mal-entendidos. Por exemplo, uma AUP lista sites, grupos de notícias ou aplicativos específicos de uso intensivo de largura de banda que os usuários não podem acessar usando computadores ou a rede da empresa.

Padrões

Os padrões ajudam uma equipe de TI a manter a consistência no funcionamento da rede. Documentos de padrões proporcionam as tecnologias que usuários ou programas específicos precisam, além de qualquer requisito ou critério de programa que uma empresa deve seguir. Isso ajuda a equipe de TI, melhorar a eficiência e simplicidade no ‘design’, manutenção e solução de problemas.

Um dos princípios de segurança mais importantes é a consistência. Por esse motivo, é necessário que as empresas estabeleçam padrões. Cada empresa desenvolve padrões para suporte de seu único ambiente operacional. Por exemplo, uma empresa estabelece uma política de senhas. O padrão é que as senhas requerem um mínimo de oito caracteres alfanuméricos maiúsculos e minúsculos, incluindo pelo menos um caractere especial. Um usuário deve alterar a senha a cada 30 dias e um histórico das 12 senhas anteriores garante que o usuário crie senhas exclusivas durante um ano.

Directrizes

As directrizes são uma lista de sugestões sobre como fazer as coisas de forma eficiente e com segurança. Eles são semelhantes aos padrões, mas mais flexíveis e, geralmente, não são obrigatórios. As directrizes definem como os padrões são desenvolvidos e garantem adesão às políticas de segurança gerais.

Algumas das orientações mais úteis compõem as melhores práticas de uma empresa. Além das melhores práticas definidas de uma empresa, as orientações também estão disponíveis das seguintes instituições:

- Centro de recursos de segurança de computador do Instituto Nacional de Padrões e Tecnologia (NIST)
- Orientações de configuração de segurança nacional (NSA)
- O padrão de critérios comuns

Usando o exemplo de políticas de senha, uma directriz é uma sugestão de que o usuário use uma frase como "I have a dream" e converta-a para uma senha forte, Ihv@dr3@m. O usuário pode criar outras senhas com essa frase, alterando o número, movendo o símbolo ou alterando o sinal de pontuação.

Procedimentos

Documentos de procedimentos são mais longos e mais detalhados que os padrões e directrizes. Documentos de procedimentos incluem detalhes de implementação que normalmente contêm instruções e gráficos passo a passo.

Grandes empresas devem usar documentos de procedimentos para manter a consistência de implantação necessária para um ambiente seguro.

Conclusão

Compreender, não apenas o que são as políticas e procedimentos de segurança, mas também o motivo deles serem implementados é um factor de sucesso quando pretendemos nos defender contra-ataques cibernéticos. Nossa atitude perante a elas podem terminar os níveis de vulnerabilidades e ameaças que os activos de TI, podem ter.

A observância a essas politicas, garantem a segurança pelo que as pessoas, quer físicas ou jurídicas devem levar em consideração para poderem reduzir o risco de ataques cibernéticos.