1.Gestão de incidentes de segurança da informação e de melhorias

Os funcionários da empresa podem desempenhar um papel importante na detecção de deficiências na segurança e na percepção de incidentes de segurança. Eles são, afinal, os primeiros a ver incidentes como:

- Alguém deixou um documento confidencial na impressora
- Um arquivo com informações pessoais desapareceu
- Há um cheiro incomum na sala onde o triturador de papel é mantido
- Uma porta que deveria estar fechada foi deixada aberta
- Um colega está se comportando de forma errática
- A tela do computador está apresentando mensagens estranhas

Membros da empresa devem ser capazes de denunciar incidentes e essas denúncias precisam resultar em ações. Normalmente os funcionários da empresa reportam tais incidentes a uma central de atendimento. O funcionário da central de atendimento identifica se este é, de fato, um incidente de segurança da informação e então realiza o procedimento pertinente para a solução do incidente e o reporta em seguida. Se o funcionário da central de atendimento não for pessoalmente capaz de lidar com o incidente, o incidente pode ser reportado a alguém com mais conhecimento, que possa ser capaz de solucionar o problema.

Isso é chamado de escalonamento funcional (horizontal). Um incidente também pode ser reportado a alguém que tenha mais autoridade e que possa tomar uma decisão. Isso é chamado de escalamento hierárquico. O propósito desse processo de gerenciamento de incidentes é ganhar conhecimento sobre os incidentes e aprender lições com eles para o futuro. Tais notificações também podem iniciar outro processo de segurança da informação, tal como a recuperação de um arquivo, uma investigação de segurança ou mesmo se mover para um estado de prontidão.

2.Reportando incidentes de segurança da informação

Há vários tipos de incidentes e eles ocorrem em diversos graus. O padrão ISO/IEC 20000 descreve como incidentes podem ser geridos no processo de gerenciamento de incidentes. Mas nem todo incidente é um incidente de segurança. Então, deve ser feita uma avaliação do incidente para determinar se realmente há um incidente de segurança.

O propósito de um processo de gerenciamento de incidentes é garantir que os incidentes e as deficiências relacionadas aos sistemas de informação sejam conhecidos, de forma que as medidas apropriadas possam ser tomadas em tempo hábil. Funcionários, pessoal temporário e usuários externos devem estar todos cientes dos

procedimentos para reportar vários tipos de incidentes e deficiências que possam influenciar a confiabilidade da informação e a segurança dos ativos da empresa.

Deve ser requerido aos funcionários e usuários que reportem o mais rápido possível todos os incidentes e deficiências à central de atendimento ou a uma pessoa de contato. Naturalmente, é do interesse de todos que a organização responda rapidamente.

Duas questões são de grande importância e têm de ser clareadas pela administração: Informar incidentes de segurança é, principalmente, uma forma de aprender com eles, a fim de evitar que incidentes semelhantes ocorram novamente; Denunciar um incidente não tem por objetivo ser uma forma de punir o autor do incidente.

Se um empregado sabotar intencionalmente um sistema de informação, vazar uma informação ou causar dano, ele(a) deve ser denunciado(a) às autoridades oficiais, ou seja, à polícia. É importante não ter medo de relatar um incidente por temor da resposta da gerência, ou por não querer ser visto como um delator. O processo também deve garantir que a pessoa que relata um incidente de segurança da informação seja informada dos resultados depois de ter sido tratado.

Relatos de incidentes também são úteis quando se realiza uma análise de riscos. Pode ser que as medidas adotadas até então não sejam suficientes para prevenir certos incidentes. Um formulário padrão para reportar tais incidentes na Intranet pode ajudar a reduzir qualquer medo e resistência associados à elaboração desses relatos. O formulário pode ser usado não só para dar instruções sobre qualquer resposta imediata ao incidente que se faça necessária, mas também para obter vários detalhes relacionados ao incidente.

Um formulário para relato de incidentes deve, no mínimo, permitir que as seguintes informações sejam inseridas.

- Data e hora
- Nome da pessoa que fez o relato
- Localização
- Qual é o problema
- Qual o efeito do incidente
- Como foi descoberto
- Tipo do sistema
- Nome e número do sistema
- Quem mais foi informado

Muitas outras questões são possíveis, dependendo do tipo de relatório. É importante que informações suficientes sejam coletadas de forma que o incidente possa ser remediado corretamente. Exemplos de incidentes incluem:

- Nenhuma manutenção é feita no equipamento
- A fonte de alimentação de emergência não tem sido testada
- Um colega perdeu um laptop
- Um colega não adere à política de mesa limpa
- Um colega traz com ele um visitante não autorizado
- Novo software é lançado antes de ser completamente testado
- Um vírus conseguiu entrar no sistema de informação
- Devido a dados incompletos da empresa, os resultados dos lucros não são confiáveis
- Os direitos de acesso de um funcionário não são modificados após uma mudança de função
- Um colega escreve sua senha no papel de anotações que está pousado sobre o PC

Instruções sobre o que fazer no caso de um incidente normalmente não são formalizadas nos procedimentos publicados. Um procedimento, afinal, descreve quem faz o quê. Tal procedimento deve incluir:

- A análise do incidente, estabelecendo a causa
- Quais passos devem ser tomados para minimizar as consequências do incidente
- Quais passos devem ser tomados a fim de determinar se são necessárias medidas corretivas para prevenir que o incidente ocorra novamente e, se houver, quais são
- Quais partes devem ser informadas no caso de um incidente
- O que é reportado sobre o incidente e a quem
- Procedimento de escalonamento no caso da situação ficar pior ou não ser resolvida em tempo hábil.

3.Relatando as fraquezas na segurança

Quando funcionários, pessoal ou temporário e usuários externos dos sistemas e serviços de informação notam que existem fraquezas nos sistemas ou serviços, é importante que eles reportem tais fraquezas o mais rápido possível. Só assim os incidentes podem ser evitados. Quando um incidente de segurança da informação é descoberto, muitas vezes não é imediatamente claro se o incidente levará a uma ação

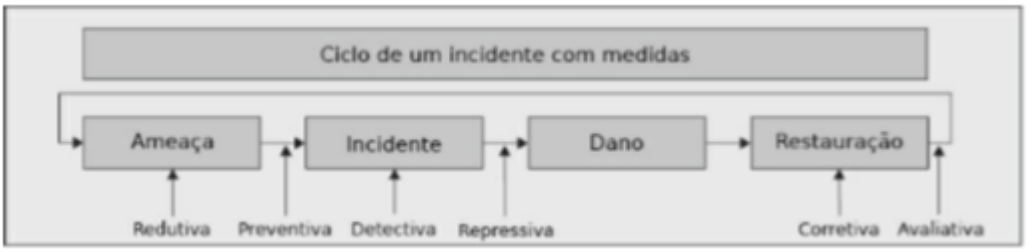
legal. Existe ainda o perigo de evidências críticas serem destruídas, intencionalmente ou não, antes da gravidade da situação ser percebida. Por isso, é importante primeiro relatar o incidente e depois pedir conselhos sobre as medidas a serem tomadas. É possível que um advogado ou a polícia precisem ser envolvidos no estágio inicial e que provas tenham que ser recolhidas.

4.Registro de interrupções

Para ser capaz de analisar uma interrupção, é importante que as informações relevantes sejam coletadas. Essa informação é frequentemente armazenada em arquivos de log. Essa é a versão moderna dos tradicionais livros de registro que ainda podem ser usados hoje. Imagine que acontece uma falha de energia e que não há outra maneira de registrar eventos e ações realizadas a não ser no papel. Em grandes organizações, interrupções são reportadas para a central de atendimento (helpdesk). Se eles forem capazes, eles irão resolver a interrupção imediatamente. Se isso não for possível, eles passarão as informações relevantes para um departamento que possa resolver a interrupção.

5.Incidentes de segurança da informação

O ciclo de um incidente possui os seguintes estágios: ameaça, dano e recuperação. Medidas de segurança visam um certo momento no ciclo de incidentes. As medidas objetivam prevenir incidentes (preventivas) ou reduzir as ameaças (redutivas), detectar incidentes (detectivas), responder a incidentes, parar ameaças (repressivas) e corrigir danos (corretivas). As medidas são tomadas a fim de garantir a disponibilidade, a integridade e a confidencialidade da informação da empresa. Após a ocorrência de um incidente, é necessário recolher provas seguindo procedimentos internos, para poder investigar o incidente de segurança da informação. Certifique-se de que todas as etapas são registradas para ajudar na análise do próprio incidente e para se aprender com a resposta ao incidente de segurança da informação.



6.Vazamento de informações

É possível que informações vazem por meio de canais de comunicação escondidos. Entretanto, seria incomum para o funcionário médio estar ciente da presença de tal canal de comunicação. Canais de comunicação secretos não se

destinam ao processamento de informações, mas podem, contudo, existir em um sistema ou uma rede. É difícil, senão impossível, impedir todos os possíveis canais secretos de comunicação. O uso de canais é uma característica comum dos trojans. É possível que o fornecedor de um programa feito sob encomenda deixe um método de acesso secreto para realizar a manutenção da aplicação, sem informar o comprador. Isso é referido como porta de manutenção (backdoor), e é uma prática que normalmente não é apreciada pelos clientes. Se a aplicação encomendada for utilizada para processar informações altamente confidenciais, então um órgão independente pode ser contratado para inspecionar o código-fonte da aplicação em busca desses canais de comunicação secretos.

7.Divulgação responsável

Vulnerabilidades de um sistema de informação são tipicamente encontradas por várias partes, como hackers éticos ou profissionais de TI que investigam software e hardware, embora às vezes elas sejam também encontradas por pura coincidência. A divulgação responsável é diferente da divulgação completa. Trata-se de um processo no qual as partes interessadas ganham tempo para corrigir seus sistemas de TI enquanto a vulnerabilidade não é divulgada. Essa não divulgação é especialmente importante quando o impacto na vulnerabilidade é alto. Parte da divulgação responsável envolve também um acordo no qual o hacker ético obtém seu momento de fama ao ir a público com vulnerabilidade.