Sumário

1. PROPÓSITO
2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
3. CÓDIGOS MALICIOSOS
4. ANTIVÍRUS
5. FIREWALL
6. SENHAS
7. CRIPTOGRAFIA DE LOGON E SENHAS NO BANCO DE DADOS
8. BACKUP
9. CÓDIGO FONTE
10. HTTPS
11. ACORDO DE CONFIDENCIALIDADE

1. PROPÓSITO

A SCC Check está comprometida em assegurar a disponibilidade, a integridade e a confidencialidade das informações compartilhadas com parceiros de negócios.

Pequenas e médias empresas são mais vulneráveis ao crime eletrônico e incidentes de Segurança da Informação, pois geralmente possuem uma estrutura robusta para manter sistemas e informações adequadamente protegidos.

Este guia foi desenvolvido para divulgar os requisitos mínimos de segurança da informação que sua empresa necessita implementar para estar em conformidade com os padrões de Segurança da Informação recomendados pela SCC Check para atender nossos clientes e parceiros de negócio de forma adequada e segura.

2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Descrição:

É um documento que apresenta as boas práticas adotadas pela empresa para nortear a segurança da informação. Sua adoção por todos colaboradores é primordial. As boas práticas indicam que toda companhia deve criar regras sobre como todos os colaboradores devem lidar com a proteção das informações da empresa, incluindo os dados e informações de seus clientes e parceiros de negócios. O conteúdo deve ser disseminado entre todos, e explicado no momento da contratação. Recomenda-se solicitar a assinatura de um termo de compromisso para o cumprimento das normas.

3. CÓDIGOS MALICIOSOS

Descrição:

Códigos maliciosos, também conhecidos como *malwares,* são usados como intermediários e possibilitam a prática de golpes, a realização de ataques e o envio de spam. São programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador.

Um usuário mal-intencionado pode instalar um código malicioso no seu computador, após invadir sua rede ou explorando alguma vulnerabilidade existente seu ambiente.

Seu ambiente de tecnologia também pode ser infectado caso você:

- Acesse páginas maliciosas na Internet, usando navegadores vulneráveis;
- Acesse mídias removíveis infectadas, como pen-drives;
- Execute arquivos infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas na Internet, redes sociais ou diretamente de outros computadores.

Após infectar o seu computador, o código malicioso pode executar ações como se fosse você, tais como: acessar informações confidenciais, apagar arquivos, conectar-se à Internet, enviar mensagens e/ou instalar outros códigos maliciosos.

Outros dispositivos também podem ser infectados por códigos maliciosos: tabletes e smartphones, por exemplo.

Tipos Principais:

Vírus

Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.

Cavalo de Tróia (*trojan*)

Programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

Rootkit

Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

Backdoor

Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

Worm

Programa capaz de se propagar automaticamente pelas redes, explorando vulnerabilidades nos programas instalados e enviando cópias de si mesmo de computador para computador.

Bot

Programa similar ao *worm* e que possui mecanismos de comunicação com o invasor que permitem que ele seja remotamente controlado. Zumbi é como é chamado um computador infectado por um *bot*, pois pode ser controlado remotamente, sem o conhecimento do seu dono. *Botnet* é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos *bots.*

Spyware

Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

Keylogger

É um tipo de *spyware* capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador.

Screenlogger

É um tipo de *spyware*, similar ao *keylogger*, usado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em *sites* de *Internet Banking.*

Adware

É um tipo de *spyware* projetado especificamente para apresentar propagandas.

4. ANTIVÍRUS

Descrição:
O Antivírus é um software essencial que protege os computadores e suas informações de diferentes tipos e níveis de ataques maliciosos.

É extremamente importante certificar-se de que este programa é atualizado pelo menos uma vez por semana, não basta apenas ter um antivírus instalado no computador, é preciso mantê-lo atualizado e seguro para que não haja problemas na sua rede. Mesmo porque, quando seu computador é infectado por vírus há grande chance de perder documentos e arquivos importantes, além da possibilidade de indisponibilidade do seu sistema.

Dicas:

- Escolher e selecionar um antivírus de renome;
- Não utilizar antivírus sem licença;
- Estar sempre com o programa e as proteções atualizadas;
- Executar uma varredura periodicamente completa de seu sistema;
- Manter-se longe a pirataria de software dos seus computadores e da sua rede;
- Utilize o antivírus antes de abrir arquivos baixados da internet, anexos, ao conectar mídias em seu computador e pen-drives.

5. FIREWALL

Descrição:

Um firewall é um sistema de proteção de um computador ou de uma rede de computadores contra ataques provenientes de diferentes redes (principalmente da Internet). O Firewall verifica cada pacote recebido e decide se o mesmo pode ser enviado ao destino ou se deve ser barrado, de acordo com parâmetros de segurança definidos.

Dicas:

- Adquirir e manter atualizado um programa firewall ou um dispositivo de firewall;
- Implementar regras a política de segurança da rede em questão;
- Fazer registros de log de todos os eventos suspeitos;
- Emitir alertas sobre tentativas que comprometem a política de segurança.

6. SENHAS

Descrição:

Contas e senhas são os principais mecanismos de autenticação utilizados. Por meio de contas e senhas os sistemas conseguem saber quem você é, confirmando sua identidade e definindo as ações que você pode realizar.

Proteger a sua identidade virtual (conta e senha) é essencial para proteger o acesso às informações e a segurança do sistema, prevenindo riscos de alteração indevida, vazamento de informação e indisponibilidade do sistema. A confidencialidade assegura-a sua identidade.

Se uma outra pessoa souber a sua conta de usuário e tiver acesso à sua senha, ela poderá usá-las para se passar por você na Internet, e/ou nos demais sistemas, e você poderá ser responsabilizado pelos acessos.

Algumas das formas como sua senha pode ser indevidamente descoberta são:

- Quando usada em computadores infectados
- Quando usada em computadores invadidos
- Quando usada em sites falsos
- Por meio de tentativas de adivinhação (principalmente, quando a senha é fraca, ou seja, de fácil adivinhação)
- Ao ser capturada enquanto trafega na rede
- Por meio do acesso ao arquivo onde foi armazenada
- Com o uso de técnicas de engenharia social pela observação da movimentação dos seus dedos no teclado

Algumas das ações que um invasor pode realizar, caso tenha acesso às suas senhas, e os riscos que estas ações podem representar são:

- Ler e/ou apagar seus *e-mails*
- Furtar sua lista de contatos e enviar *e-mails* em seu nome
- Enviar mensagens de spam e/ou contendo *phishing* e códigos maliciosos
- Pedir o reenvio de senhas de outras contas (e assim conseguir acesso a elas)
- Trocar sua senha, dificultando que você acesse novamente sua conta
- Apagar seus arquivos e obter informações sensíveis, inclusive outras senhas, instalar códigos e serviços maliciosos
- Acessar redes sociais e denegrir a sua imagem e explorar a confiança de seus amigos/seguidores
- Enviar mensagens de *spam* ou contendo boatos e códigos maliciosos
- Alterar as configurações feitas por você, tornando públicas informações privadas
- Acessar sua conta bancária e verificar seu extrato e seu saldo bancário
- Acessar seu *site* de comércio eletrônico e alterar informações de cadastro, fazer compras em seu nome e verificar informações sobre suas compras anteriores.

Evite usar:

- Dados pessoais, como nomes, sobrenomes, contas de usuário, datas, números de documentos, placas de carros e números de telefones, dados que possam ser obtidos em redes sociais e páginas na Internet, sequências de teclado, como “1qaz2wsx” e “QwerTAsdfG”, palavras que fazem parte de listas publicamente conhecidas, como nomes de músicas, times de futebol, personagens de filmes e dicionários de diferentes idiomas.

Recomendamos:

- A senha deve ser pessoal e única para cada usuário.
- Não compartilhe sua senha com ninguém.
- Combinar letras, números e símbolos (ex.: @, #, $) para formar sua senha;
- Utilizar o máximo de caracteres permitidos (quanto maior a senha, mais difícil para ser “quebrada” por pessoas mal-intencionadas).
- Troque suas senhas regularmente
- Utilize senhas diferentes para sistemas importantes (bancos, e-mails, sites,etc).
- Não compartilhe sua senha com ninguém.
- **Nunca anotar sua senha em agendas, arquivos, post-its ou em lugares a que outras pessoas possam ter acesso. O indicado é memorizá-la.**

7. CRIPTOGRAFIA DE LOGON E SENHAS NO BANCO DE DADOS

Descrição:

As senhas desses usuários geralmente estão entre as informações mais valiosas que se pode obter desses serviços, portanto, armazená-las em um local de fácil acesso (ex. formato texto) é uma atitude irresponsável dos desenvolvedores desses serviços.

A incorporação de recursos de segurança, principalmente a criptografia, é a prática mais recomendável para a proteção das suas senhas e de seus clientes.

8. BACKUP

Descrição:

Um backup não serve apenas para ser usado no lugar de um arquivo danificado ou inacessível. A cópia também pode ser usada para consultar informações. Por isso, é importante ter em mente qual a finalidade do arquivo e com que frequência ele é atualizado para definir o intervalo no qual as cópias de segurança devem ser feitas.

Guardar os arquivos em local seguro e efetuar backup periódico é o nível de segurança mais simples e barato para garantir um mínimo de contingência para seu sistema, em caso de algum evento que possa impactar o serviço.

As empresas precisam ter a preocupação de armazenar em segurança todas as informações envolvidas no contexto da organização. Lembrando que as informações são bem mais valioso da empresa, principalmente se estas informações estão armazenadas em bancos de dados, é fundamental ter uma estratégia bem definida para a proteção deste bem tão valioso.

Devemos nos preocupar não apenas com a perda dos dados, mas também com acessos indevidos, alterações não autorizadas e/ou roubo de informações.

Alguns exemplos:

- Invasões e ataque de hackers;
- Acesso indevido às informações;
- Desastres naturais;
- Incêndios;
- Inundações;
- Alterações indevidas (quebra de integridade);
- Falhas de hardware.

Um importante fator que devemos levar em consideração, na hora de montarmos a nossa estratégia de backup/restore é a proteção dos dados. Se a informação a ser protegida tem valor estratégico para a empresa, é vital que os dados precisam estar disponíveis e bem protegidos, dessa forma, mesmo que os custos para proteção sejam elevados, serão facilmente justificáveis.

Lembramos ainda que, não basta fazer o backup, precisamos de uma estratégia de testes e simulação de restauração dos dados, pois muitas vezes, apesar do procedimento de backup ser realizado com sucesso, no momento de restaurar os dados é que ser verificam os problemas. Por isso, uma prática recomendável, é realizar uma rotina de testes periódicos de restauração dos dados de backups como parte da estratégia de segurança.

9. CÓDIGO FONTE

Descrição:

Na busca por melhor desempenho e controle de suas operações, as empresas têm investido cada vez mais em softwares, que se tornam essenciais para gerir o negócio. Adquirir um software feito sob medida é uma atividade de grande risco. Não apenas porque o programa deverá se encaixar o mais perfeitamente possível às necessidades da empresa, mas porque esse software vai criar uma dependência com o desenvolvedor, incluindo manutenções, reparos e atualização de novas tecnologias e necessidades. Se o desenvolvedor falir ou encerrar suas atividades, ou mesmo em casos de desacordo comercial, o negócio poderá ser grandemente afetado.

Ao se contratar uma empresa para desenvolvimento de software, o adquirente poderá exigir por contrato, que o código-fonte seja entregue aos cuidados de um terceiro de confiança das partes (terceiro depositário). O contrato deve prevê as condições nas quais o adquirente pode reivindicar o código-fonte do software, caso o adquirente não poder contar mais com a assistência do desenvolvedor poderá utilizar sua equipe de TI própria ou até mesmo contratar outra empresa de desenvolvimento para dar manutenção ao programa. Isso diminui consideravelmente o risco de prejuízos oriundos da interrupção do funcionamento do software.

O terceiro depositário precisa ser de confiança de ambas as partes, idôneo e com experiência no ramo. Isso porque o código-fonte é a alma do software, objeto de proteção da lei de direitos autorais. Se uma pessoa de má-fé se apropriar dele, poderá reproduzir o programa livremente, o que gerará grandes prejuízos à empresa. É conveniente também verificar o nível de segurança da informação oferecido, já que a ação de hackers poderia fazer vazar as informações estratégicas.

O acesso ao código-fonte de programa deve ser controlado, com a finalidade de prevenir a introdução de funcionalidades não autorizadas e para evitar mudanças não intencionais.

Os seguintes requisitos de segurança da informação devem ser considerados para o controle de acesso ao código fonte, com a finalidade de reduzir o risco:

- Manter o acesso restrito ao código-fonte;
- Manter o código-fonte em um ambiente seguro;
- Manter um registro de auditoria de todos os acessos e alterações ao código-fonte.

10. HTTPS

Descrição:

O HTTPS (***Hyper Text Transfer Protocol Secure)*** é o protocolo ou conjunto de regras e códigos com uma camada de segurança que torna a navegação mais segura. Essa camada adicional de segurança permite que os dados sejam transmitidos por meio de uma conexão criptografada e que se verifique a autenticidade do servidor e do cliente por meio de certificados digitais

O HTTP (protocolo normal) não oferece a mesma segurança do HTTPS porque as informações navegam na rede de uma forma muito parecida com a apresentada na tela ou digitadas pelo usuário. Por exemplo, se o usuário digita um *login* "xxx" e uma senha "1234", essa informação é enviada através de pacotes de dados pela rede. Alguém pode interceptar esses dados no meio do caminho e acessar informações confidenciais de forma não autorizadas.

Interceptar pacotes entre a origem e o destino não é muito complicado na internet. Eles passam por diversas redes de uma ponta até a outra, como a rede de nossa casa ou empresa, a rede do nosso provedor e a rede onde está o servidor de Internet, por exemplo. Em qualquer desses pontos um indivíduo mal-intencionado pode encontrar meios de visualizar os pacotes de dados que trafegam.

11. ACORDO DE CONFIDENCIALIDADE

Descrição:

Os acordos de confidencialidade podem preceder não apenas eventos estratégicos, como parcerias comerciais, avaliações para aquisição de empresa ou o desenvolvimento conjunto de um produto, mas também eventos corriqueiros, como a contratação de serviços ou a realização de uma grande compra, hipóteses nas quais o fornecimento de informações pode ser necessário para a execução do serviço ou para a cotação junto ao fornecedor. Em qualquer dessas hipóteses a atenção deve ser a mesma, pois a importância desta espécie de acordo não está relacionada

com o projeto ao qual ele está vinculado, mas com a proteção da informação estratégica.

Este acordo é um controle administrativo extra judicial que impõem a aplicação da confidencialidade entre contratada e contratante sobre as informações envolvida em um contrato de prestação de serviços.