



GUIA DE BOAS PRÁTICAS DE SEGURANÇA PARA E-COMMERCE

Realizar **negócios através da Internet** é uma alternativa de **alto valor estratégico** para os empresários que optaram por investir neste segmento. Os limites geográficos são removidos e os **custos operacionais** são consideravelmente **menores em comparação com os negócios baseados em lojas físicas**.

Este é um mercado que tem se **desenvolvido em ritmo elevado** e a tendência é que este curso de elevação seja mantido pois, com o crescimento da economia e as ações do governo federal no sentido de democratizar o acesso a tecnologia se espera um **aumento expressivo** no volume de **novos consumidores na Internet**, sobretudo aqueles que recentemente alcançaram a classe média.

Um cenário tão favorável para novos negócios e com alta circulação de dinheiro **desperta o interesse de criminosos** que buscam tornar seus golpes cada vez mais sofisticados à medida que a tecnologia evolui.

Se proteger desta modalidade de crime é uma tarefa que exige o esforço de todos. No entanto, **as pequenas e médias empresas são as que se tornam mais vulneráveis ao crime eletrônico**, devido ao fato de que, para manterem custos competitivos, geralmente não possuem profissionais com foco em desenvolver e manter ambientes e sistemas seguros.



Acreditamos que a chave para a proteção do mercado, sobretudo o do comércio eletrônico, reside no **compartilhamento do conhecimento**. Desta forma, este guia possui o objetivo de orientar **empresários, profissionais de infraestrutura tecnológica e desenvolvedores de sistemas** ligados ao Comércio Eletrônico no sentido de proteger suas aplicações web **reduzindo riscos** de ataques, comprometimento de informações e fraudes. Serão descritas aqui as formas mais comuns de ataques na Internet e **formas de proteção** com uma linguagem acessível, de acordo com a atividade desempenhada por cada profissional.

Boa leitura





GUIA DE BOAS PRÁTICAS DE SEGURANÇA PARA E-COMMERCE

VERSÃO DO EXECUTIVO

Sistemas para computadores possuem falhas. Em uma venda através de um portal de comércio eletrônico estas falhas podem estar presentes no computador do cliente, no caminho entre o cliente e a loja virtual, ou na forma em que a loja virtual foi desenvolvida e configurada

Os criminosos que agem na internet procuram explorar estas falhas. Geralmente estas pessoas utilizam aplicativos específicos para levantar informações sobre um determinado site, entendendo assim como ele funciona e buscando vulnerabilidades em sua operação

Os ataques podem ter os mais variados objetivos (tornar o site alvo indisponível, utilizá-lo como disseminador de vírus, etc). No entanto, para efeito deste guia, iremos manter o foco no **crime que possui o objetivo de obter dados de cartão no comércio eletrônico**. Este pode ocorrer por meio de um dos tipos de ataque abaixo ou, **em casos mais sofisticados, utilizar a combinação de elementos de todos os tipos relacionados**

Captura de dados em trânsito

Ataques ao cliente

Ataques ao Comércio Eletrônico



FORMAS DE ATAQUE VISANDO DADOS DE CARTÃO

CAPTURA DE DADOS EM TRÂNSITO

Uma venda através de um site de comércio eletrônico pode ser considerada, em uma perspectiva simplificada, como um conjunto de dados que partem da estação do cliente que realiza a compra com destino a loja virtual e posteriormente desta para as instituições responsáveis pela autorização da transação.

Na internet existem pessoas que se dedicam a interceptar informações no tráfego de maneira criminosa. Desta maneira, é importante que todos os canais pelos quais os dados são trafegados estejam protegidos e a melhor solução para este caso é tornar o tráfego criptografado.

Por isso, todas as páginas que lidem com **dados confidenciais** (aqueles que dizem respeito somente a você e seu cliente, como por exemplo, a página onde se solicitam os dados do cliente, os dados do cartão, etc), **devem trafegar em páginas conhecidas como “conexão segura”,** ou seja, as que usam o protocolo **HTTPS – SSL (Secure Sockets Layer).**

Peça ao seu desenvolvedor do site para que estas páginas ou formulários trafeguem desta maneira.

É um procedimento comum e simples de ser utilizado.



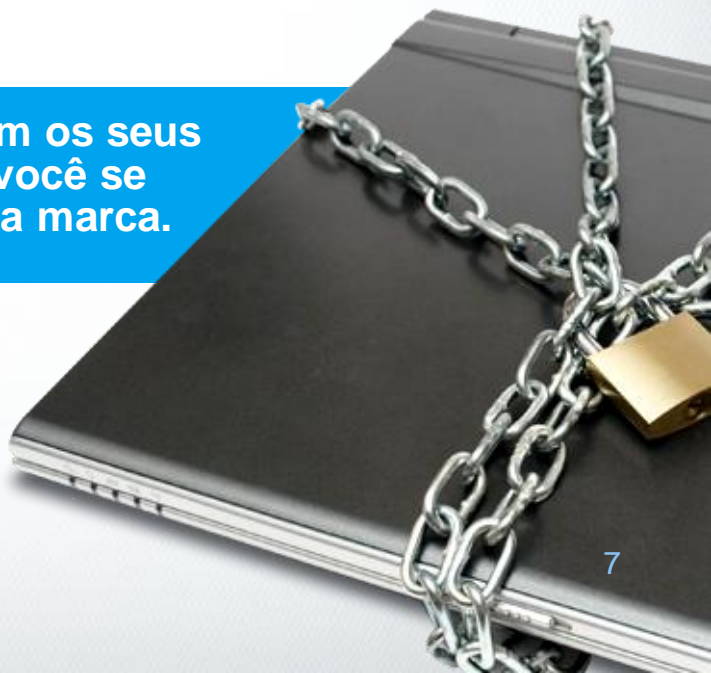
ATAQUES AO CLIENTE

Com a modernização dos dispositivos de segurança presentes nas empresas, os fraudadores geralmente **migram o foco de seus ataques para o lado do cliente**, que na maioria dos casos possui o menor nível de proteção.

Os criminosos buscam se aproveitar da **ingenuidade do usuário para enviar mensagens que ocultam vírus**. Estes vírus possuem a função de obter dados pessoais e de cartão, na maioria dos casos exibindo telas para que o próprio usuário **forneça estas informações para o programa que as envia para o fraudador**.

A melhor arma contra este tipo de técnica é elaborar os seus processos de negócio de modo que **não seja necessária a obtenção de nenhum dado pessoal após o seu cadastro inicial** e que seu cliente seja constantemente informado em todos os canais de venda que sua empresa **não envia** solicitações de recadastramento ou solicitação de dados pessoais por e-mail ou redes sociais.

Assim sua relação de parceria com os seus clientes se torna mais próxima e você se protege do uso inadequado de sua marca.



ATAQUES AO SITE DE COMÉRCIO ELETRÔNICO

Uma empresa pode sofrer ataques por meio de **vulnerabilidades em sua infraestrutura tecnológica** (servidores, equipamentos de rede, etc.), **vulnerabilidades em seus processos internos e vulnerabilidades em seus sistemas**.

VULNERABILIDADES NA INFRAESTRUTURA

Todo servidor, sistemas operacionais e dispositivos de rede, ao serem instalados **possuem uma configuração básica de fábrica**. Este tipo de configuração não é a mais segura e geralmente é mantida em boa parte das empresas, pois é de **interesse dos administradores que todos os equipamentos estejam disponíveis o mais rápido possível**.

Estes ambientes são os que os criminosos mais procuram, pois há muita **documentação disponível sobre suas fragilidades como vulnerabilidades conhecidas e senhas padrão**. Portanto é importante configurar os ambientes de acordo com as necessidades pelas quais estes foram designados e manter um **processo contínuo de atualização de todos os sistemas com as correções disponibilizadas pelo fabricante**.

Caso o criminoso obtenha **acesso não autorizado a um determinado equipamento**, este buscará acessar o maior número de computadores da empresa alvo de seu ataque. Desta maneira, é importante que existam **barreiras que limitem os acessos dentro da empresa**.



A primeira barreira deve ser estabelecida na rede. **Dispositivos como firewalls cumprem esta função** agindo como a primeira camada de proteção do perímetro. Através do uso de firewalls é possível determinar quais equipamentos podem estabelecer conexão com os servidores mais críticos de sua empresa.

A segunda barreira, que não substitui o uso de firewalls mais completa a sua proteção, é a ativação de mecanismos de **controle de acesso**. Nem todos os empregados da empresa e prestadores de serviço precisam ter acesso a todas informações para desempenhar as suas atividades.

Desta maneira é importante configurar os sistemas para conceder os acessos às equipes de acordo com a sua função. Quanto maior for o acesso concedido de maneira inadequada, maior será o potencial para a ocorrência de fraudes e erros operacionais com base neste acesso

Uma política de acessos bem estabelecida pode ser inútil caso os empregados e prestadores de serviço possuam o comportamento de compartilhar usuários e senhas. Em caso de fraudes ou outros tipos de incidente não será possível determinar quem realizou a ação. Desta forma os empregados e prestadores de serviço devem ser encorajados a **considerar as senhas como uma informação individual e intransferível**.

Mais informações e regras para a proteção de sua infraestrutura na **versão do “Administrador de Rede”** presente neste guia.



FORMAS DE ATAQUE VISANDO DADOS DE CARTÃO

VULNERABILIDADES EM SISTEMAS

A existência de falhas em sistemas de mercado, os expondo a ataques remotos é de conhecimento de boa parte da comunidade que interage diariamente com a tecnologia pois alcança a mídia e se torna um assunto do cotidiano.

No entanto, a maioria das empresas desenvolvem sistemas internos que, ao contrário do que o senso comum acredita, **possuem vulnerabilidades tão graves quanto as que ocorrem em sistemas de mercado**. Atualmente muitos dos ataques aos servidores disponíveis na internet ocorrem porque o sistema desenvolvido possui falhas que ao serem exploradas resultam no acesso não autorizado ou na possibilidade de tornar o sistema indisponível.

Nenhum software é inviolável. Desta maneira, o que realmente protege um sistema é uma rotina que privilegie a **segurança em todo o ciclo de vida do software** (especificação, desenvolvimento e manutenção).



DADOS DOS CARTÕES DE PAGAMENTO

São considerados como dados de cartões utilizados em operações de comércio eletrônico, as seguintes informações:

Número do Cartão, ou PAN (Primary Account Number)

Código de Segurança



Nome do Portador


Data de validade do cartão



Criminosos que realizam fraudes com cartões na Internet geralmente atacam ambientes de Comércio Eletrônico em busca de **dados de cartão armazenados em seus servidores**.

O armazenamento **destas informações não é recomendável, porém ao se cogitar a possibilidade de armazená-las**, sugerimos que seja feita **uma análise crítica** em que seja questionado se estes dados são realmente necessários lembrando que a Cielo oferece o TID ou código de transação o qual pode ser usado para **identificar qualquer transação** em nossos sistemas **sem a necessidade do número do cartão**.

Caso seja necessário armazenar alguma informação do cartão esta deve ser feita somente da seguinte maneira:

INFORMAÇÕES	REGRAS PARA ARMAZENAMENTO
 Número do Cartão PAN (Primary Account Number)	Armazenamento permitido somente de maneira parcial mantendo as quatro últimas posições (ex.: ***** 1234) ou em modo criptografado
Nome do Portador	Se armazenado em conjunto com o número do cartão completo este precisa ser criptografado
Data de vencimento do cartão	Se armazenado em conjunto com o número do cartão completo este precisa ser criptografado
Código de segurança	Armazenamento não permitido em hipótese alguma

Mais informações e regras para o desenvolvimento de sistemas com segurança na “Versão do Desenvolvedor de Software” presente neste guia

PADRÃO DE SEGURANÇA DE DADOS DA INDÚSTRIA DE CARTÕES DE PAGAMENTO



O **PCI Security Standards Council**, conselho internacional com a representação de diversas entidades ligadas ao mercado de cartões, possui a função de criar padrões de segurança aplicáveis a todas as empresas que processam, transmitem ou armazenam dados de cartões.

O principal destes padrões é o **Payment Card Industry – Data Security Standard (PCI DSS)**, em português Padrão de Segurança de Dados da Indústria de Cartões de Pagamento. O PCI DSS contempla de forma detalhada todas as regras para a segurança de um ambiente que atua com dados de cartão.

A Cielo é certificada no PCI DSS e motiva fortemente os seus clientes a fazerem o mesmo para que o mercado brasileiro continue buscando ser um ótimo lugar para a realização de negócios com meios eletrônicos de pagamento e com baixos riscos de segurança das informações.

PROCEDIMENTOS BÁSICOS EM CASO DE COMPROMETIMENTO DE INFORMAÇÕES

Em caso de suspeita de vazamento de dados de cartão no ambiente de sua empresa ou prestador de serviços, entre em contato com a Cielo através do e-mail csirt@cielo.com.br para podermos analisar o caso e definir as medidas para solução do problema



GUIA DE BOAS PRÁTICAS DE SEGURANÇA PARA E-COMMERCE

VERSÃO DO DESENVOLVEDOR DE SOFTWARE

VULNERABILIDADES NO DESENVOLVIMENTO DE SOFTWARE

Atualmente boa parte dos ataques contra aplicações web ocorrem devido a falhas no desenvolvimento de software **que deixam brechas para a entrada de um invasor. Estas vulnerabilidades podem ter origem em todas as etapas do processo de desenvolvimento de software, desde ao design até a administração do sistema.**

FALHAS NO DESIGN

São os problemas gerados no planejamento da Aplicação Web, quando estas são desenhadas e desenvolvidas sem que haja uma preocupação adequada com o nível de segurança. Controlar acessos aos aplicativos somente por meio de quais menus cada usuário poderá ver ou simplificações no acesso a bases de dados são exemplos comuns de falhas deste tipo.

FALHAS NA ARQUITETURA

São as vulnerabilidades associadas à segmentação de redes, implementação de ativos de TI e informações que possam comprometer o ambiente. Manter o banco de dados que suporta um web site na DMZ possibilitando o acesso remoto externo sem autenticação, é um exemplo comum deste tipo de problema.



VULNERABILIDADES NO DESENVOLVIMENTO DE SOFTWARE

FALHAS NO CÓDIGO

São as falhas relacionadas à maneira em que as empresas constroem suas aplicações corporativas, frameworks e demais componentes de software. É a camada onde são identificadas as falhas mais comuns.

FALHAS NA ADMINISTRAÇÃO

São problemas gerados não pela Aplicação Web em si, mas pela forma como ela é administrada. Exemplos comuns deste tipo de problema ocorrem quando controles de segurança previamente implementados são removidos no curso do ciclo de vida do sistema.



Proteger aplicações web requer a implementação de controles de segurança em todo ciclo de vida do desenvolvimento de software.

Abaixo as principais regras para melhorar o nível de segurança do software desenvolvido em sua empresa, recomendamos a inclusão delas em sua metodologia de desenvolvimento de software.

Obs.: As regras definidas neste documento, embora garantam uma elevação considerável do nível de segurança em aplicações web, não encerram completamente a questão. É importante que os desenvolvedores se mantenham atualizados com relação às novas vulnerabilidades e contramedidas a serem aplicadas em seu software. A participação em fóruns como o OWASP, o estudo e a constante atualização em sites especializados são altamente recomendáveis.



Mantenha os desenvolvedores sempre atualizados com relação às novas vulnerabilidades e formas de proteção.

Nunca armazene usuários e senhas ou chaves criptográficas de sua aplicação no código fonte. Procure utilizar serviços de autenticação como o RADIUS ou criptografar estes dados.

Nunca permita que a sua aplicação receba dados de usuários e senhas em texto claro. Utilize sempre o protocolo SSL.

Estabeleça **uma política de senhas para a sua aplicação** de acordo com as regras abaixo;

— **Comprimento mínimo** de 8 caracteres.

— **Período de expiração** de no mínimo 45 dias.

— Obrigatoriedade de que a senha seja composta de **letras e números**.

— Obrigatoriedade de o usuário, ao compor uma nova senha não utilize **nenhuma das quatro senhas anteriores**.



Não envie a senha por e-mail nos casos em que o usuário executa a função “esqueci minha senha”. Procure usar mecanismos como o de pergunta secreta.

Não armazene cookies com o usuário e a senha, mesmo que criptografados, na estação do usuário.

Se certifique que a função de “logout” de sua aplicação realmente encerra completamente a sessão.

Insira um botão de **“logout” em cada uma das páginas** de seu site.

Conceda ao usuário de serviço de sua aplicação somente os acessos mínimos para o seu funcionamento. Nunca o defina como “root”, “administrador” ou “sa”.

Desenvolva permissões de acesso de acordo com cada funcionalidade da aplicação e não por menus.

Implemente mecanismos de validação da entrada de dados em sua aplicação impedindo que seja possível a inserção de dados de um tamanho ou tipo (numérico, alfanumérico, data/hora, etc.) que contrarie a regra de negócio estabelecida no sistema.

Implemente mecanismos de geração de logs, sobretudo para as transações críticas.



Armazene os logs em arquivos ou bancos de dados com acesso disponível **somente às equipes de infraestrutura**.

Realize o tratamento de erros impedindo a ocorrência de mensagens de erro com origem no sistema de banco de dados ou no webserver.

Impeça que sua aplicação armazene o número do cartão completo. Somente o armazene de maneira parcial mantendo as quatro últimas posições (ex.: ***** 1234) ou em modo criptografado.

Se o nome do portador do cartão e a data de vencimento forem armazenados em conjunto com o numero do cartão estes **deverão estar em modo criptografado**.

Não armazene em hipótese alguma as informações do código de segurança.

Estabeleça uma **política de descarte dos dados do cartão** em no mínimo um ano.

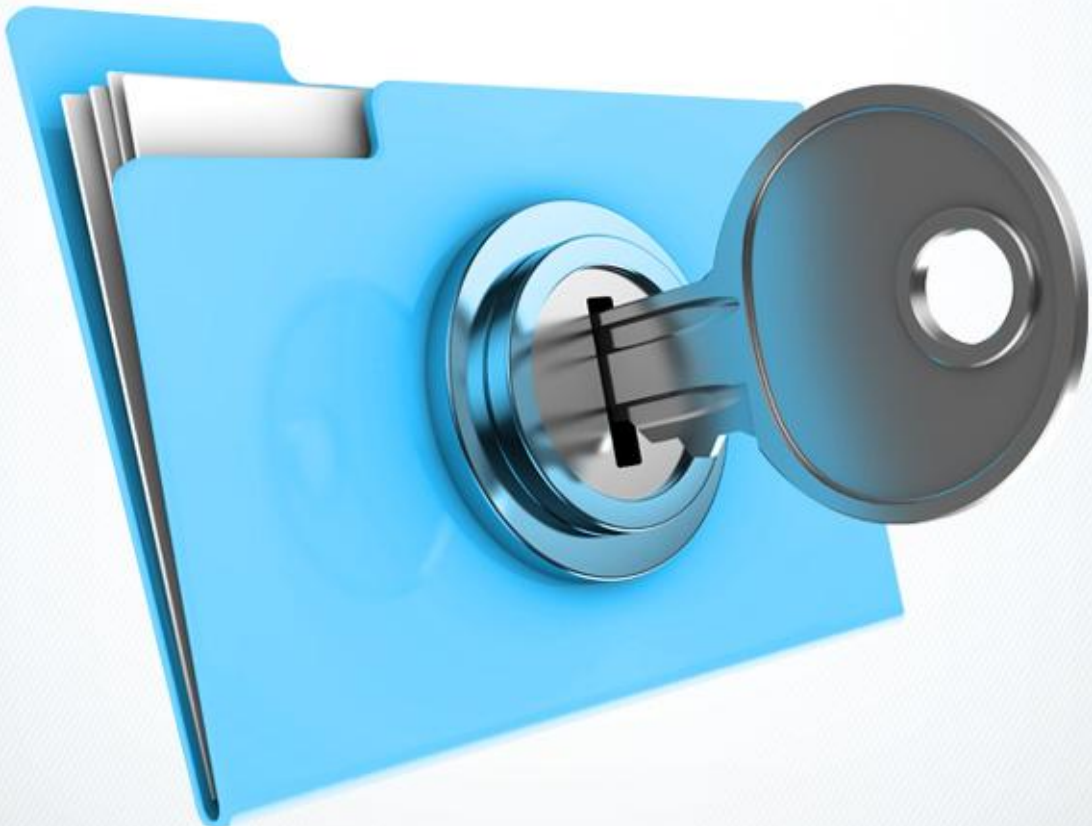
Não armazene informações de produção nos ambientes de desenvolvimento e homologação.



Remova todas as informações e contas de usuário de testes ao migrar o sistema para o ambiente de produção.

Estabeleça procedimentos, com periodicidade ao mínimo anual, de teste de intrusão com foco na tentativa de exploração de vulnerabilidades em aplicações web.

Elimine as vulnerabilidades reportadas em, pelo menos um mês após a detecção.





GUIA DE BOAS PRÁTICAS DE SEGURANÇA PARA E-COMMERCE

VERSÃO DO ADMINISTRADOR DE REDE

O trabalho dos administradores de infraestrutura envolve, na maior parte do tempo, o esforço para **manter servidores, estações de trabalho e dispositivos de rede disponíveis**.

No entanto, deve fazer parte das atividades destes profissionais a padronização e parametrização dos dispositivos com foco em protegê-los de ataques.

ABAIXO ESTÃO DISPOSTAS AS REGRAS PARA A PARAMETRIZAÇÃO DE AMBIENTES COM FOCO NA SEGURANÇA DAS INFORMAÇÕES

PROTEÇÃO DO PERÍMETRO

Ao iniciar o trabalho de proteção de uma plataforma tecnológica se deve **definir um perímetro de segurança** no qual serão agrupados os dispositivos de acordo com a sua **função e interação com informações críticas**. A partir do estabelecimento deste perímetro devem ser concedidas as **permissões de acesso adequadas para cada dispositivo**.

ABAIXO AS REGRAS PARA O ESTABELECIMENTO DE UM PERÍMETRO DE SEGURANÇA

Utilize firewalls para segregar as redes do ambiente. Evite usar roteadores para realizar esta função.

Procure utilizar firewalls com a função de **“stateful inspection”**.

Analise o desenho de sua rede criticando se os dispositivos (servidores, switches, etc.) **estão devidamente agrupados em redes específicas de acordo** com a sua importância para o negócio. Caso estes ativos não estejam segregados desta maneira, considere separá-los. Esta atividade cria zonas de segurança por função, o que limita o alcance de um possível ataque.



Implemente uma DMZ com o objetivo de abrigar todos os dispositivos expostos à internet. **Limite todo o tráfego de entrada somente para a DMZ.**

Concentre os servidores de banco de dados em uma rede apartada, **nunca os deixem expostos à internet.**

Segregue através de firewalls os ambientes de desenvolvimento, homologação e produção.

Estabeleça **quais são as portas permitidas para a comunicação entre seus dispositivos e as documente.** Esta atividade aumenta o controle e torna formal qual tipo de comunicação é permitida em seu ambiente

Evite o uso de portas de comunicação reconhecidamente consideradas como vulneráveis como TELNET e FTP. Prefira soluções com criptografia como SFTP e SSH,

Determine formalmente quais as pessoas que possuem a função de administrar os firewalls e outros dispositivos de rede.



Defina um **processo formal** para a manutenção e alteração de **regras** nos firewalls. Este processo deve contemplar uma solicitação de **mudança** para cada regra com a **aprovação de pelo menos um gestor**.

Caso possua redes sem fio em seu ambiente, segregue-as através de firewall concedendo somente os acessos necessários para os equipamentos com origem nestas redes.

Configure os pontos de acesso wireless para **usar somente o padrão de criptografia de autenticação WPA2** com chaves longas.

Nunca utilize o padrão de criptografia de autenticação **WEP**.

Proíba qualquer acesso originado na internet que tenha como destino algum equipamento da rede interna.

Utilize o mascaramento de IP (Network Address Translation - NAT) para todo o tráfego de saída para internet.

Não utilize senhas padrão de fábrica em nenhum dos equipamentos.

Configure os dispositivos de rede para gerar logs de todos os eventos realizados com privilégios administrativos.



Configure os dispositivos de rede para gerar logs de todos os eventos cuja tentativa de **acesso resultou em falha**.

Configure os logs para manter os dados de data/hora do evento, identificação do usuário, tipo de evento, indicação de sucesso ou falha e a indicação de qual componente foi alterado ou sofreu uma tentativa de alteração.

Centralize os logs dos dispositivos de rede e servidores em um **servidor com esta função**

Desabilite a função **SOURCE-Routing** em roteadores, evitando a possibilidade de **inserção não autorizada de rotas nos dispositivos**

Desabilite a função **PROXY-ARP** em roteadores, evitando a possibilidade **obtenção não autorizada de informações do dispositivo**

Instale um software de IPS/IDS **e o monitore constantemente**



Os controles abaixo possuem o objetivo de **evitar que informações sensíveis sejam obtidas de forma não autorizada** através da captura de dados em trânsito

Utilize obrigatoriamente a criptografia SSL V3 impedindo a conexão por meio do uso de versões antigas do SSL.

Esta regra é aplicada através da alteração da configuração de seu Webserver.

Somente utilize certificados digitais de **autoridades certificadoras válidas**.

Monitore a validade do certificado digital e busque adquirir um novo com antecedência à expiração do certificado instalado.

Somente administre dispositivos **utilizando protocolos com criptografia como SSH**.

Somente realize a **troca de arquivos** entre dispositivos **utilizando protocolos com criptografia** como SFTP.

Proíba o tráfego de dados de cartão via e-mail, instant messaging, Skype, etc.



PROTEÇÃO DE SERVIDORES E ESTAÇÕES DE TRABALHO

Os controles abaixo possuem o objetivo de estabelecer **padrões para a configuração de servidores e estações de trabalho** sob a perspectiva da segurança das informações

Sempre que possível, determine, sobretudo na DMZ, **uma função por servidor. Manter diversos serviços** em um servidor (web server e banco de dados, por exemplo) acarreta na ativação de diversos serviços por máquina, o que **pode torná-la vulnerável**.

Sempre **altere as configurações de qualquer dispositivo antes de instalá-lo** em produção evitando manter qualquer configuração de fábrica como usuários e senhas, acessos, etc.

Desabilite todos os serviços e protocolos **desnecessários para a funcionalidade do servidor**.



ESTABELEÇA UMA POLÍTICA DE SENHAS PARA A SUA APLICAÇÃO DE ACORDO COM AS REGRAS ABAIXO

— **Comprimento mínimo** de 8 caracteres;

— **Período de expiração** de no mínimo 45 dias;

— Obrigatoriedade de que a senha seja composta de **letras e números**;

— Obrigatoriedade de o usuário, ao compor uma nova senha **não utilize nenhuma das quatro senhas anteriores**;

— **Bloquear a conta do usuário** após cinco tentativas de acesso sem sucesso;

— **Manter o usuário bloqueado** de acordo com a regra acima por 30 minutos ou até o desbloqueio pelo administrador.



A prática de **compartilhamento de senhas** entre os funcionários **deve ser proibida**.

Contas de acesso de serviço devem ser utilizadas somente para o uso em sistemas **específicos, nunca devem ser usadas para o logon por usuários**.

Configure os servidores para **gerar logs** de todos os eventos realizados a partir de **usuários com privilégios administrativos**.

Configure os servidores para gerar logs de todos os eventos realizados a partir de **usuários de serviço**.

Configure os logs para manter os dados de data/hora do evento, identificação do usuário, tipo de evento, indicação de sucesso ou falha e a indicação de qual componente foi alterado ou sofreu uma tentativa de alteração.

Estabeleça **mecanismos de controle de acesso** para proteger os arquivos de log do acesso não autorizado.

Defina e documente um **padrão de configuração** para cada tipo de dispositivo de sua rede.



Revise os padrões de configuração periodicamente.

Não utilize softwares não confiáveis em seu ambiente.

Instale e mantenha atualizado um software de antivírus em todos os computadores que se apliquem.

Configure o software antivírus para realizar um **scan completo em todos os computadores**, pelo menos uma vez por semana.

Estabeleça medidas de controle de acessos, considerando que se deve limitar os acessos ao mínimo necessário para que os empregados e prestadores de serviço realizem as suas atividades.

Revise todos os acessos, ao mínimo anualmente.

Mantenha todos os sistemas atualizados com as correções do fabricante.

Somente conceda acesso remoto (através da internet) aos empregados e prestadores de serviço **por meio de VPNs**.

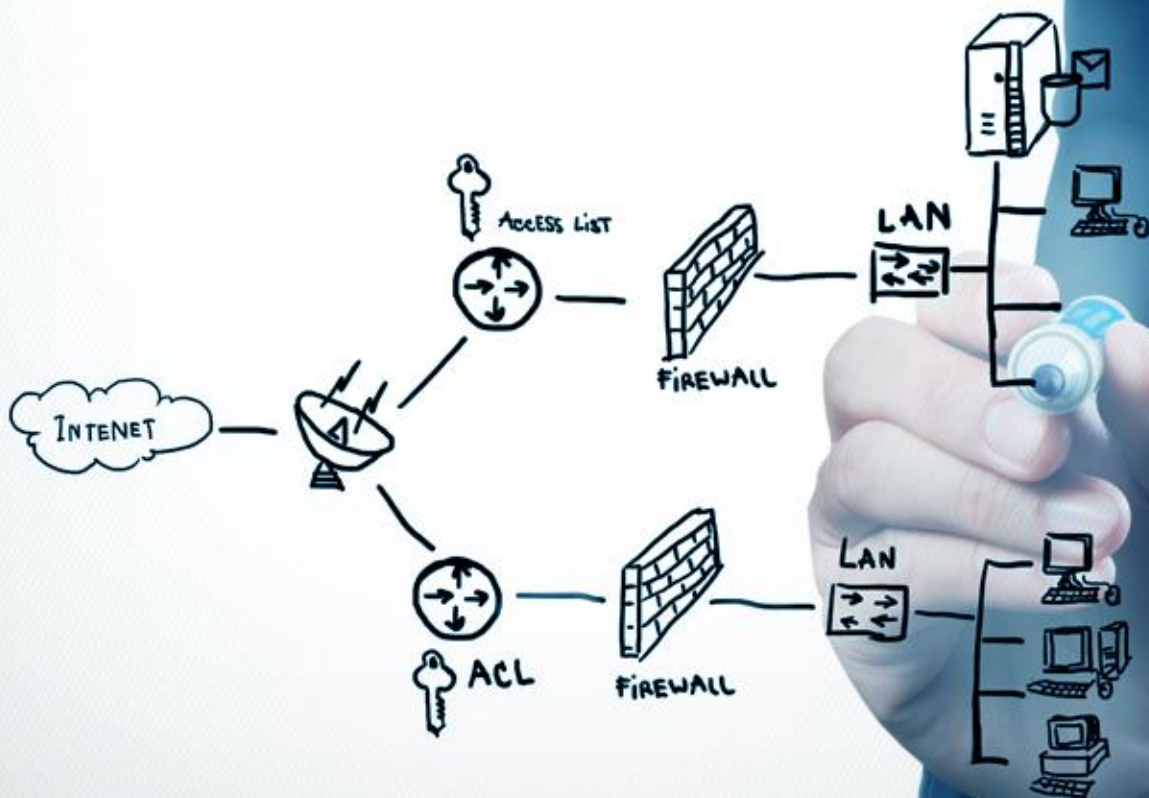


Desabilite todos os acessos dos empregados e prestadores de serviço **imediatamente após o seu desligamento** da empresa ou encerramento do contrato de prestação de serviços.

Execute **scans de vulnerabilidade** no mínimo trimestralmente.

Estabeleça procedimentos, com periodicidade no mínimo anual, de teste de intrusão com foco na **tentativa de exploração de vulnerabilidades** em redes de sistemas operacionais.

Elimine as vulnerabilidades reportadas em, pelo menos um mês após a detecção.



ARMAZENAMENTO DE DADOS DE CARTÃO

A Cielo recomenda fortemente que seja analisada a necessidade de se armazenar dados de cartão.

Armazenar estas informações acarreta no risco de fraude e em investimentos destinados a proteção destes dados.

Se este tipo de informação não é necessária para a continuidade dos processos de negócio de sua empresa, **considere sua remoção**. Caso contrário aplique as regras abaixo.

Somente armazene o número do cartão de **maneira parcial** mantendo somente as quatro últimas posições (ex.: *****1234) ou **em modo criptografado**.

Se o **nome do portador do cartão** e a **data de vencimento** forem armazenados em conjunto com o número do cartão estes deverão estar em **modo criptografado**.

Não armazene em hipótese alguma as informações do código de segurança.

Estabeleça **uma política de expurgo** dos dados do cartão em no mínimo um ano.

Monitore o acesso ao dado de cartão e investigue casos de acessos suspeitos.



O armazenamento do número de cartão completo em conjunto com o nome do portador e data de vencimento **requer o uso de criptografia destas informações**. Abaixo os requisitos para a criptografia de dados de cartão.

Determine um reservatório central para os **dados criptografados**.

Obtenha uma **solução de criptografia robusta** que utilize algoritmos públicos com chaves de no mínimo 128-bits para criptografia simétrica e 1024-bits para criptografia assimétrica.

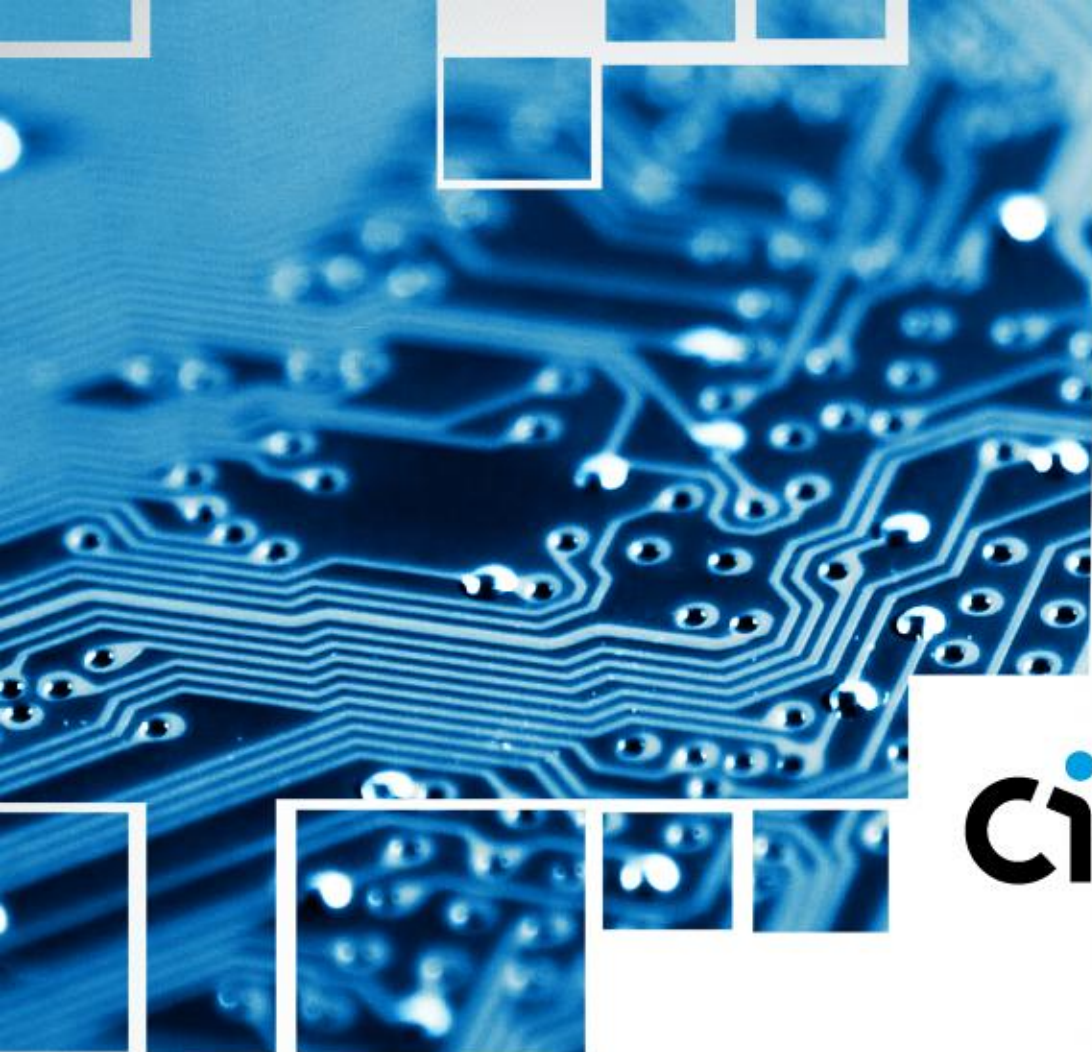
Garanta que a informação seja encriptada e decriptada no momento do acesso ao repositório e **não haja cache com informações em texto claro em memória não volátil**.

Estabeleça um processo formal de, no mínimo **dupla custódia**, para a definição das chaves de criptografia.



Proteja as partes da chave, limitando seu acesso ao menor número de pessoas possíveis.

Troque as chaves criptográficas pelo menos uma vez por ano ou imediatamente para os casos de suspeita de seu comprometimento .



GLOSSÁRIO

ANTIVÍRUS

Programa com o objetivo de proteger o computador contra vírus

AUTENTICAÇÃO

Mecanismo de validação da identidade de um usuário no momento que este acessa um sistema.

CERTIFICADO DIGITAL

Mecanismo utilizado para estabelecer a comunicação entre computadores com segurança.

CÓDIGO FONTE

Instruções em uma determinada linguagem de programação que, em conjunto compõem um software.

COOKIE

Mecanismo utilizado em aplicações web que armazena dados de acesso na estação do usuário possibilitando a persistência de uma sessão de acesso. Um exemplo, são os cookies que armazenam informações de conexão para que o usuário não tenha que digitá-las novamente em outras visitas ao site.

CRIPTOGRAFIA

Conjunto de técnicas com o objetivo de proteger uma informação de modo que esta só possa ser compreendida pelo remetente e pelo destinatário. O que protege a mensagem criptografada é a chave criptográfica, esta seria um segredo trocado previamente entre o remetente e o destinatário por meio do qual as mensagens serão criptografadas.

CRIPTOGRAFIA ASSIMÉTRICA

Forma de criptografia na qual o remetente e o destinatário não possuem a chave inteira mas sim partes dela que quando combinadas permitem decifrar a informação.

CRIPTOGRAFIA SIMÉTRICA

Forma de criptografia na qual tanto o remetente quanto o destinatário compartilham a mesma chave para criptografar e decriptar informações.

DMZ

Abreviação de demilitarized zone (em português, zona desmilitarizada). Termo com origem no vocabulário militar que foi adaptado na informática para definir uma área de rede entre a rede interna e a internet.

DUPLA CUSTÓDIA

Processo no qual uma chave de criptografia ou senha é elaborada por duas pessoas. Cada uma delas insere no sistema uma parte da chave. As duas partes são escritas e lacradas em envelopes separados e armazenados em cofre.

FIREWALLS

Dispositivos com a função de segregar redes realizando a proteção de um determinado perímetro. Nos firewalls os administradores determinam quais conexões são permitidas de uma rede para a outra.

FRAMEWORK

Conjunto de conceitos técnicos que orienta o desenvolvimento de software.

FTP

File Transfer Protocol - Protocolo utilizado em redes de computadores para a transferência de arquivos.

HTTPS

HyperText Transfer Protocol Secure - Protocolo de acesso a páginas na internet com criptografia.

IDS

Intrusion Detection System - Mecanismo utilizado para analisar o comportamento do tráfego em uma rede e, com base em uma biblioteca de comportamentos conhecidos detectar e alertar o administrador sobre uma possível invasão.

IPS

Intrusion Prevention System - Semelhante ao IDS, entretanto com a funcionalidade de executar uma ação (o bloqueio da comunicação, por exemplo) quando um possível ataque é detectado.

LOGON

Ato de acessar um sistema após o processo de autenticação (digitação do usuário e a senha, por exemplo).

LOGOUT

Ato de encerrar o acesso a um sistema.

MEMÓRIA NÃO VOLÁTIL

Memória na qual o conteúdo armazenado não é eliminado após o computador ser desligado. Por exemplo, discos rígidos, pendrives, CD-ROM, etc.

NAT

Network Address Translation - Técnica que consiste na conversão do endereço IP de origem em meio a uma conexão. Muito usado em situações nas quais computadores de uma rede interna precisam cessar endereços da Internet. Nestes casos, embora a conexão parta de um determinado endereço, este é alterado na saída para a Internet de modo que o endereço interno não é divulgado externamente.

OWASP

Fórum internacional, aberto e sem fins lucrativos que reúne profissionais com o objetivo de documentar vulnerabilidades em aplicações web e suas formas de prevenção. Anualmente o OWASP divulga o Top 10 com as dez falhas mais exploradas globalmente. Mais informações em https://www.owasp.org/index.php/Main_Page.

PORTAS TCP/IP

Elemento utilizado em redes de computadores para separar a comunicação de protocolos. Exemplo: o protocolo FTP utiliza por padrão a porta 21.

PROTOCOLOS

Conjunto de regras que determinam formas de comunicação entre computadores.

PROXY-ARP

Mecanismo que possibilita a definição de somente um endereço IP para várias redes.

RADIUS

Remote Authentication Dial In User Service – Mecanismo com o objetivo de autenticar acessos a um determinado sistema. Mais informações em <http://freeradius.org/>.

ROOT

Usuário administrador padrão de sistemas operacionais UNIX e Linux.

ROTEADORES

Equipamentos utilizados para estabelecer a comunicação entre duas ou mais redes de computadores.

SA

Usuário administrador padrão de sistemas de banco de dados SQL da Microsoft.

SCAN

Atividade de varredura presente em sistemas de antivírus ou ferramentas de análise de vulnerabilidades que realizam uma varredura em vários detalhes de um computador em busca de falhas.

SFTP

Protocolo FTP com uma camada de criptografia.

SOFTWARE

Programa ou código executável para computador ou dispositivo semelhante.

SOURCE-ROUTING

Propriedade presente em alguns roteadores que possibilita ao usuário do computador de origem determinar uma rota de acesso remotamente. Seria como se este usuário tivesse a possibilidade de definir qual caminho seguiria em uma determinada conexão. Este é um mecanismo usado para ataques.

SSH

Protocolo que permite o estabelecimento de uma sessão remota com criptografia. Geralmente utilizado por administradores para gerenciar servidores e dispositivos de rede à distância.

SSL

Protocolo que estabelece criptografia em uma conexão a sites na internet. A presença da expressão HTTPS:\\ no endereço de um site geralmente é um indicativo de que a conexão está criptografada com SSL.

SSLV3

Versão 3 do SSL.

STATEFUL INSPECTION

Mecanismo presente em alguns firewalls no qual cada fragmento da conexão é inspecionado em busca de ataques.

SWITCHES

Equipamentos utilizados para conectar computadores em uma rede.

TELNET

Protocolo que permite o estabelecimento de uma sessão remota. Geralmente utilizado por administradores para gerenciar servidores e dispositivos de rede à distância.

TESTE DE INTRUSÃO

Procedimento no qual um profissional aplica técnicas de ataque na rede ou sistemas de seu cliente com o intuito de reportar as vulnerabilidades do ambiente.

TRATAMENTO DE ERROS

Atividade do processo de desenvolvimento de sistemas que consiste em prever falhas na aplicação e definir mensagens de erro específicas para cada cenário de erro.

USUÁRIOS DE SERVIÇO

Contas de acesso utilizadas por sistemas.

VÍRUS

Softwares com o objetivo de danificar computadores.

VPN

Virtual Private Networks - Meio de conexão remota criptografada na qual computadores podem estabelecer conexão entre si através da internet.

WEBSERVER

Servidor com o objetivo hospedar páginas ou outros serviços disponíveis na internet.

WEP

Wired Equivalent Privacy - Mecanismo de autenticação em redes wireless obsoleto e com baixo nível de segurança.

WPA

Wi-Fi Protected Access - Mecanismo de autenticação em redes wireless o qual substituiu o WEP, mas também é considerado pouco seguro.

WPA2

Evolução do WPA, com maior nível de Segurança.

CONTEÚDO DESENVOLVIDO EM PARCERIA COM:

