GUIA

BOAS PRÁTICAS DE SEGURANÇA

eConsig©

Guia de Boas Práticas de Segurança

Prezado cliente,

O Sistema Digital de Consignações – eConsig foi criado para tornar o processo de consignação mais ágil e seguro, reduzindo o tempo de liberação do consignado e tornando o gerenciamento mais simples para as entidades financeiras, para os gestores de Folhas de Pagamento e também para os servidores/funcionários.

O mercado do Consignado no país tem crescido num ritmo elevado e movimenta quantias suntuosas.

Um cenário favorável e com movimentação elevada de recursos financeiros, desperta a atenção e o interesse de criminosos, que buscam tornar seus golpes cada vez mais sofisticados.

A proteção desta modalidade de crime é uma tarefa que exige o comprometimento e esforço de todos.

Acreditamos que a chave para proteção contra fraudes em consignados consiste no compartilhamento de conhecimento. Sendo assim, este guia possui o objetivo de orientar usuários de consignatárias, correspondentes e gestores de Folhas de Pagamento, que utilizam o eConsig em seu cotidiano, no sentido de reduzirem riscos de ataques, fraudes e comprometimento de informações.

Para que seja possível reduzir riscos de ataques, fraudes e o comprometimento de informações, são necessários cuidados em relação aos equipamentos de rede da entidade, a liberação e gerenciamento de acessos e sobretudo a realização de programas de conscientização com os usuários, sendo estes os temas abordados neste Guia.

Boa leitura!

Proteção de equipamentos e da rede

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

Neste tópico, segue algumas recomendações em relação a Segurança da Informação que devem ser adotadas pelos Administradores de Rede para proteção da infraestrutura tecnológica da entidade:

- Instalar e manter atualizado um software antivírus em todos os computadores.
- Configurar o software antivírus para realizar um scan completo em todos os computadores periodicamente.
- Manter todos os sistemas atualizados com as correções do fabricante.
- Não utilizar softwares não confiáveis em seu ambiente.
- Não manter servidores, sistemas operacionais e dispositivos de rede com a configuração padrão de fábrica, pois esta não é segura, devendo ser trocada.
- Configurar os ambientes de acordo com as necessidades do negócio e manter um processo contínuo de atualização de todos os sistemas com as correções disponibilizadas pelo fabricante.
- Criar barreiras que limitem os acessos dentro da empresa.
- A primeira barreira deve ser estabelecida na rede, através de dispositivos como firewalls.
- A segunda barreira, que não substitui o uso de firewalls mais complementa a sua proteção, é a ativação de mecanismos de controle de acesso.
- Desenvolver permissões de acesso de acordo com as atribuições do usuário.
- Analisar o desempenho de sua rede e segregar ativos quando necessário.
- Evitar o uso de portas de comunicação reconhecidamente consideradas como vulneráveis, tais como Telnet e FTP.
- Estabelecer quais são as portas permitidas para a comunicação entre seus dispositivos.
- Configurar os pontos de acesso wireless para uso somente de padrões de criptografia de autenticação com chaves longas.

- Manter servidores de dados em uma rede segregada.
- Utilizar mascaramento de IP (NAT) para todo o tráfego de saída de internet.
- Configurar os dispositivos de rede para gerar logs de todos os eventos realizados com privilégios administrativos.
- Configurar os dispositivos para gerar logs de todos os eventos cuja tentativa de acesso resultou em falha.
- Desabilitar as funções Source-Routing e Proxy-ARP em roteadores.
- Instalar um software de IPS/IDS e monitorá-lo.
- Somente realizar a troca de arquivos entre dispositivos utilizando protocolos de criptografia.
- Revisar padrões de configuração periodicamente.
- Somente conceder acesso remoto (através da internet) aos empregados e prestadores de serviço por meio de VPNs.
- Desabilitar todos os acessos dos empregados e prestadores de serviço imediatamente após o seu desligamento da empresa ou encerramento do contrato de prestação de serviços.
- Executar scans de vulnerabilidade periodicamente.
- Tratar vulnerabilidades reportadas / detectadas.
- Realizar testes de intrusão.
- Definir uma política de Controle de Acesso.

Controle de acesso ao eConsig

O sistema eConsig oferece a estrutura necessária para garantir que nossos clientes possam realizar uma gestão de controle de acesso segura e eficaz. Para isso o sistema conta com vários recursos, estando os principais relacionados:

- Captcha na tela login;
- Expiração de sessão após alguns minutos;
- Bloqueio da opção "voltar" do browser durante a navegação;
- Bloqueio do usuário após um determinado número de tentativas de login;
- Utilização de política de senha com comprimento mínimo de 8 caracteres, com período de expiração de no máximo 90 dias;
- Bloqueio de usuários por inatividade;
- Validação de IP ou endereço de acesso por usuário, entidade ou função;
- Utilização de certificado digital (e-CPF) com possibilidade de implementação por usuário ou por entidade;
- Inserção de data de validade (expiração) para os acessos do usuário;
- Relatórios de conferência de usuários.

No entanto, além dos recursos já mencionados, são necessários alguns cuidados extras, tais como:

- Definir uma política de Controle de Acesso para a entidade que contemple processos de liberação, revalidação e remoção de acessos lógicos;
- Definir perfis de acesso de acordo com as funções exercidas pelos colaboradores, restringindo ao máximo possível a criação de usuários com perfil Master;
- Criar um padrão único para o cadastro dos usuários da entidade (consignante, consignatária ou do correspondente). Exemplos: utilizar nome e sobrenome (jose.silva), a matrícula funcional do colaborador (MF000015) ou outro padrão;
- Preencher todos os campos do cadastro de usuário: nome completo, CPF, telefone, e-mail;
- Coibir o compartilhamento de senhas entre usuários e a criação de usuários genéricos, tendo em vista que em casos de fraudes ou incidentes, isto torna mais difícil determinar quem efetuou a ação;
- Não fornecer senhas por e-mail;
- Orientar os usuários a não salvar senhas nos navegadores de internet e nem anotá-las em papéis, agendas ou locais de fácil acesso;
- Promover treinamentos periódicos de conscientização;
- Efetuar bloqueio e/ou exclusão imediata de usuários em casos de desligamento; e
- Revisar os acessos dos usuários periodicamente.

Revalidação de acessos:

A revalidação dos acessos de usuários do eConsig pode ser realizada com auxílio dos relatórios de Conferência de Cadastro de Usuários e de Ocorrência de Usuário, que traz as seguintes informações:

Relatório de Conferência de Cadastro => nome, login, CPF, data de cadastro, data de expiração, e-mail, telefone, perfil e status do usuário.

Relatório de Ocorrência de Usuário => mostra as ações realizadas por um usuário, como reinicialização de senha, inclusões, exclusões, bloqueios, desbloqueios, mudanças de perfil.

Outra funcionalidade que pode ser utilizada para auxiliar as entidades na revalidação de acesso é o campo para inserção de validade deste, presente na parte inferior da tela de cadastro de usuário.

Relatórios de monitoramento:

O eConsig possui vários relatórios que permitem às consignatárias e correspondentes, assim como ao consignante, checar e auditar as operações realizadas no sistema.

Estes relatórios podem ser agendados para envios automáticos na periodicidade desejada, bastando para isso que o usuário ao gerar o relatório preencha os campos referentes à periodicidade desejada e informe o e-mail para o qual o relatório deve ser enviado.

Os relatórios aos quais os usuários possuem acesso são exibidos no menu "Relatórios" do eConsig.

Para mais informações sobre os relatórios que o eConsig possui, entre em contato conosco.

Conscientização dos usuários

Os usuários são os responsáveis pela operação do eConsig e demais sistemas utilizados pelas entidades, sendo assim, é fundamental que tenham consciência em relação às atitudes corretas a serem tomadas para garantir a Segurança da Informação nas operações que realizam.

Recomendamos que treinamentos periódicos, sejam realizados para mantê-los cientes sobre como agir de forma segura e preventiva.

Conscientização dos servidores públicos / funcionários

É importante também a realização de iniciativas para conscientização dos servidores públicos / funcionários em relação a possíveis golpes.

Os servidores públicos/funcionários precisam ter ciência de que:

- Senhas não devem ser fornecidas às instituições financeiras em nenhuma hipótese;
- Renegociações devem ser realizadas preferencialmente nas instituições financeiras e pessoalmente;
- Deve-se ter cautela na confirmação e fornecimento de dados pessoais por telefone;
- Deve-se desconfiar de empréstimos com taxa muito abaixo das praticadas pelo mercado e oferecidos através de abordagens não convencionais.

Procedimento em caso de suspeitas ou ocorrências de operações indevidas

Em caso de suspeita de operações indevidas no sistema eConsig, entre em contato com a ZETRASOFT através do e-mail **seguranca@zetrasoft.com.br** ou do telefone (31) 3194-7700 para podermos analisar o caso e orientá-los.

Glossário:

ANTIVÍRUS: Programa utilizado com o objetivo de proteger o computador contra vírus.

e-CPF: É a versão eletrônica do CPF, utilizada para garantir autenticidade em operações eletrônicas.

COOKIE: Mecanismo utilizado em aplicações web que armazena dados de acesso no computador do usuário. Exemplo: armazenam informações de uma conexão para que o usuário não tenha que informá-las novamente em outras visitas ao site.

CRIPTOGRAFIA: Conjunto de técnicas utilizadas com o objetivo de proteger informações, de modo que só possam ser entendidas pelo remetente e pelo destinatário.

FIREWALL: Dispositivo que tem como função segregar redes realizando a proteção de perímetros, através da determinação das conexões que são permitidas entre uma rede e outra.

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 que permite que os dados sejam transmitidos por meio de uma conexão criptografada. Utiliza SSL/TLS.

IDS: Sistema de detecção de intrusos ou também conhecido como Sistema de detecção de intrusão (em inglês: Intrusion detection system - IDS) refere-se aos meios técnicos de descobrir em uma rede acessos não autorizados que podem indicar a ação de um cracker ou até mesmo de funcionários mal intencionados.

IPS: Intrusion Prevention System – Mecanismo semelhante ao IDS, possuindo a funcionalidade de executar uma determinada ação (exemplo: bloqueio da comunicação), quando um possível ataque é evidenciado.

NAT: Network Address Translation – é uma técnica que consiste em reescrever, utilizando-se de uma tabelahash, os endereços IP de origem de um pacote que passam por um router ou firewall de maneira que um computador de uma rede interna tenha acesso ao exterior (rede pública).

PROTOCOLOS: Conjunto de regras que controla e possibilita uma conexão, comunicação entre computadores.

PROXY-ARP: Mecanismo que possibilita que uma organização possua somente um endereço

IP para suas diversas redes.

ROTEADOR: É um dispositivo que encaminha pacotes de dados entre redes de computadores, criando um conjunto de redes de sobreposição. Um roteador é conectado a duas ou mais linhas de dados de redes diferentes.

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

SWITCHES: Equipamentos utilizados para conectar computadores em uma rede.

TELNET: O protocolo Telnet é um protocolo standard de Internet que permite a interface de terminais e de aplicações através da Internet. Utilizado geralmente para o gerenciamento de servidores e dispositivos de rede à distância.

TESTE DE INTRUSÃO: Procedimento executado por profissional qualificado onde técnicas de ataque à rede ou sistemas do cliente são executados

VÍRUS: Software malicioso desenvolvido por programadores que, tal como um vírus biológico, infecta o sistema, faz cópias de si mesmo e tenta se espalhar para outros computadores, utilizando-se de diversos meios.

VPN: É uma rede de comunicações privada normalmente utilizada por uma empresa ou um conjunto de empresas e/ou instituições, construída em cima de uma rede de comunicações pública (como por exemplo, a Internet).

zetra®