BOAS PRÁTICAS DE SEGURANÇA

Este documento tem como objetivo auxiliar na condução das decisões para boas práticas de segurança da informação.

O que envolve a segurança da informação?

A segurança da informação se baseia nos seguintes pilares:

- confidencialidade;
- integridade;
- disponibilidade;
- autenticidade.

Ou seja, é necessário que as ações realizadas se dediquem a garantir esses quatro aspectos anteriores, e não é difícil compreender seu contexto na área de segurança.

Por exemplo, um erro de confidencialidade pode expor dados estratégicos da organização para concorrentes, ou então um vazamento de dados de clientes realizado por hackers.

O primeiro ponto que deve ser abordado é a cultura de confiança dos usuários: *"se só eu uso esse computador, por que não posso personalizar com a minha foto do final de ano?", "mas eu sou o gerente, não posso ter restrição!", "eu preciso ter acesso a internet liberado.", "eu tenho que poder instalar aplicativos!", "preciso desse software mesmo que não tenha licença."*.

TODOS DEVEM ESTAR CIENTES E ENGAJADOS NA MELHORIA DA SEGURANÇA DA INFORMAÇÃO, por isso é preciso educar os colaboradores. Muitas vezes dados são roubados ou perdidos por pura inocência e falta de conhecimento do usuário, seja consciente - ao acessar sites impróprios e não seguros - ou inconscientemente, ao utilizar um pen drive infectado ou abrindo e-mails recebidos.

DEIXE CLARO O QUE É E NÃO É PERMITIDO NAS MÁQUINAS DA EMPRESA: não é porque o usuário está usando seu próprio dispositivo (*celular, tablet, notebook, etc*) que ele pode fazer o que bem entender com os recursos da empresa. Um dispositivo infectado pode comprometer toda a rede em que ele se conectar.

É IMPORTANTE QUE SEJAM DEFINIDAS POLÍTICAS E PROCEDIMENTOS VISANDO A SEGURANÇA DA INFORMAÇÃO. Uma política de segurança consistente vai permitir que os administradores de rede, os

profissionais de segurança em TI e outros técnicos possam entender as regras e aplicá-las, colaborando também para a divulgação delas entre os usuários.

Não basta implementar as práticas de segurança da informação — **é necessário assegurar que não há brechas**. Para isso, é preciso que sejam aplicadas as melhores ações nessa área.

Caso julgue necessário, pode-se firmar junto a cada funcionário um documento de responsabilidade para casos de negligência, má utilização dos recursos e/ou vazamento de informações.

É IMPORTANTE CONHECER A DIFERENÇA ENTRE AS AMEAÇAS

VÍRUS

Um vírus de computador é um programa 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. **O vírus de computador se instala com o objetivo de prejudicar o desempenho de uma máquina, destruir arquivos e infectar outros dispositivos, podendo prejudicar todos os aparelhos que estejam conectados à mesma rede de uma empresa.** Com isso, um computador que tem um vírus instalado pode ficar vulnerável para pessoas mal-intencionadas, que podem vasculhar arquivos do sistema, roubar dados, como senhas, números de cartões de crédito ou outras informações confidenciais.

ATENÇÃO: A maioria das contaminações ocorre pela ação do usuário executando o arquivo infectado recebido como anexo de um e-mail. A contaminação também pode ocorrer por meio de arquivos infectados em Pen Drives ou CDs.

WORM

Um *Worm* (verme, em português), na área da informática, é semelhante a um vírus, porém com um diferencial: **é um programa auto-replicante**. Enquanto um vírus infecta um programa e necessita deste programa hospedeiro para se propagar, o *Worm* é um programa completo e autossuficiente.

Um *Worm* pode ser projetado para tomar ações maliciosas após infestar um sistema: além de se auto-replicar, pode apagar arquivos, enviar documentos por e-mail, etc.

SPYWARE

Spyware (aplicativo ou programa espião) consiste num programa automático de computador, que **coleta informações sobre o usuário, sobre os seus costumes de navegação e as transmite para uma entidade externa na Internet, sem o conhecimento ou consentimento do usuário**. Diferem dos Cavalos de Tróia (*Trojan*) por não terem o objetivo de "sequestrar" ou manipular o sistema do usuário.

Os *Spywares* podem ser desenvolvidos por firmas comerciais que desejam monitorar o hábito dos usuários para avaliar seus costumes e vender estes dados pela Internet.

PHISHING

Em computação, ***Phishing (lê-se fishing)* é uma forma de fraude eletrônica, caracterizada por tentativas de adquirir informações sigilosas, tais como senhas e números de cartão de crédito**, ao se fazer passar como uma pessoa confiável ou uma empresa enviando uma comunicação eletrônica oficial, como um correio ou uma mensagem instantânea.

Na prática do *Phishing* surgem artimanhas cada vez mais sofisticadas para "pescar" (do inglês *fish*) as informações sigilosas dos usuários. É necessária atenção redobrada a e-mails de bancos que solicitam números de tokens, renovação de cartões de crédito, ou de destinatários desconhecidos emitindo boletos, relatórios e orçamentos. Não se deve clicar, baixar e nem executar nenhum arquivo anexado nestes e-mails.

BOTNET / STORM WORM

O *Botnet* é muito difícil de ser detectado e também analisado, pois ele se reconfigura rapidamente e pode ser transmitido através de links que apontam para endereços IP de sites infectados. Atualmente ele é considerado o pior meio de infecção de um computador, pois pode atacar uma quantidade extremamente grande de vítimas.

INFECÇÃO POR RANSOMWARE

Ransomware é um software malicioso que infecta seu computador e exibe mensagens exigindo o pagamento de uma taxa para fazer o sistema voltar a funcionar. Essa classe de malware é um esquema de lucro criminoso. Um *ransomware* pode se instalar ao se abrir links em e-mails, redes sociais e mensagens instantâneas, baixar conteúdo de sites duvidosos, ou acessá-los usando navegadores vulneráveis. Também é possível ser infectado por anexos de e-mails e arquivos compartilhados. No entanto, o código não se propaga sozinho, sendo necessário um desses canais como condutores.

SUGESTÕES

SEGURANÇA LÓGICA OU DE SOFTWARE

- Cada usuário do sistema deve acessar somente aquilo que lhe é necessário;
- Limitar quem pode acessar o quê;
- Implementar domínio para controle centralizado com restrições aos usuários;
- Usuários comuns não podem fazer nenhum tipo de instalação ou alteração no sistema operacional;
- Restringir os tipos de arquivos permitidos nos equipamentos e pastas de rede:

  Ex.: bloquear o salvamento de arquivos com extensões, .exe .bat. .script, .vba;
- Restringir acesso a pastas no computador local e de rede;
- Para recebimento de e-mails, utilizar regras de lista negra e lista branca, onde somente e-mails da lista de contatos serão permitidos.

CRIAR POLÍTICA DE SENHAS FORTES

- Senhas com no mínimo 8 caracteres;
- Ter ao menos um caractere especial (*Ex: $, &, %, (, #*);
- Ter ao menos um número e uma letra maiúscula;
- Tempo de utilização máximo de 45 dias e mínimo de 20 dias;
- Restrição de repetição das últimas 30 senhas;
- Não escrever senhas em post-its e deixar em locais de acesso geral.

CRIAR POLÍTICA DE SEGURANÇA FÍSICA DOS EQUIPAMENTOS

Os equipamentos devem ser mantidos em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

- Lacre em CPUs;
- Desativação de portas USB (quando possível);
- Restrição de acesso a pendrives e cartões SD;
- Desativação de drives de DVD;
- Desativar o acesso wi-fi da rede interna;
- Restringir o acesso a e-mails externos.

UTILIZAÇÃO DE ANTIVÍRUS

Preferencialmente não utilizar versões gratuitas de antivírus, optar sempre por versões pagas. Versões gratuitas possuem restrições e não fornecem todas as garantias quanto a remoção de vírus e spyware. **Manter estes softwares SEMPRE atualizados.**

Para os equipamentos que terão acesso a internet, recomendável a utilização de restrições a sites não confiáveis e redes sociais.

BACKUP

Indicado sempre manter 3 cópias de arquivos, uma local, uma cópia física (HD externo, DVD, etc.) e uma cópia em nuvem. **É imprescindível que o dispositivo físico externo NÃO FIQUE conectado ao computador após a execução do Backup, guarde-o em um local seguro, preferencialmente fora da empresa.**

FIREWALL

Utilizar um programa especifico de Firewall no servidor, ter um firewall físico (equipamento especifico pra este fim), controlando as portas de entrada e saída. Em nenhuma hipótese desativar o firewall do Windows porque está gerando algum conflito com determinado programa.

PROXY

Utilizar proxy para controle de acesso dos usuários e convidados. Restringindo o acesso somente a sites necessários para o trabalho. Bloquear sites maliciosos e desnecessários utilizando listas pré-definidas. Uma das mais utilizadas é a Shallalist que pode ser encontrada no endereço abaixo. "www.shallalist.de/Downloads/shallalist.tar.gz". Entre em contato com seu técnico para maiores informações de utilização.

VLAN

Desenvolver uma estrutura segmentada através de lans virtuais. Limitando o acesso de determinado grupo de usuário a áreas especificas da rede.

QUAL SERVIDOR UTILIZAR?

Para uma correta e eficaz implementação dos itens acima, será necessário a utilização de um servidor. Para isso, deverão ser considerados os valores de aquisição e manutenção, pois alguns lugares carecem de mão-de-obra qualificada para prestação de serviços de TI.

SERVIDORES LINUX (LICENÇAS FREE)

Prós: Não tem custo de aquisição (Gratuito), é um servidor robusto que permite todas as configurações sugeridas. Mais seguro se comparado com a plataforma Windows.

Contras: Exige mão-de-obra especializada, com valor mais alto de hora técnica, e dependendo da região não existem técnicos com conhecimentos suficientes para manutenção servidor.

SERVIDORES WINDOWS (LICENÇAS PAGAS)

Colégio Registral
RIO GRANDE DO SUL

IRIRGS
Instituto de Registro Imobiliário do Rio Grande do Sul

Prós: Mais simples de configurar, fornece suporte via telefone, e-mail ou chat. Possui maior número de técnicos qualificados para configuração, consequentemente o valor de manutenção é mais baixo.

Contras: Alto custo de aquisição (valores variam de U$ 500,00 a U$ 6.000,00). O valor da licença vai depender do tipo e destinação de uso.

O Colégio Registral do RS e o IRIRGS colocam à disposição sua área de TI na forma de consultoria para que seus associados tenham auxílio na análise de cenário e verificação de qual solução se enquadra melhor para sua serventia.

Qualquer dúvida, favor encaminhar e-mail para os endereços
webmaster@colegioregistralrs.org.br **e** **ti@irirgs.org.br**

"Devemos sempre pensar na rede de computadores como uma corrente que é tão forte quanto seu elo mais fraco, por isso a melhor regra de segurança ainda é conscientização e bom senso ao utilizar os equipamentos no trabalho."