FIESP | DEPARTAMENTO DE SEGURANÇA

CARTILHA DE BOAS PRÁTICAS EM SEGURANÇA CIBERNÉTICA

GRUPO DE TRABALHO DE SEGURANÇA CIBERNÉTICA

A FIESP esclarece que as informações apresentadas na presente Cartilha são apenas sugestões para auxiliar as entidades na mitigação de riscos cibernéticos, sendo de suma importância que cada entidade avalie internamente qual a melhor estratégia e regras a serem estabelecidas, conforme seus respectivos interesses, objetivos e áreas de atuação.

SUMÁRIO

INTRODUÇÃO

Em plena Era da Informação, as ameaças cibernéticas são um dos maiores problemas enfrentados pelas empresas e pelos profissionais que vivem o dia a dia de trabalho.

Em se tratando de informação, trabalhamos conectados a maior parte do tempo. O contato com funcionários , clientes, fornecedores, colegas e com toda a cadeia que faz parte do trabalho diário é feito pela internet. Sem dúvida, ela é um grande facilitador na comunicação, pois nos permite realizar, com extrema rapidez, uma série de atribuições, sem que haja comprometimento da agilidade do trabalho. Mas com tais benefícios vêm também riscos.

Um dos problemas é a quantidade e a complexidade de ataques que empresas e governos sofrem no ciberespaço.

Não se trata apenas da rede que compõe a internet, mas sim da informação e de como protegê-la. Por si só, investimento em tecnologia não é o bastante, sendo preciso uma mudança cultural e, principalmente, da forma como avaliamos os riscos a que nossas informações estão expostas.

Pare por um minuto e pense em todos os locais onde se encontram suas informações, tais como agenda de contatos, telefones, fotos e *e-mails* – dispositivos, *smartphone*, *webmail*, nuvem, provedor de internet, etc. Agora, tente responder uma das perguntas a seguir:

- Quantos incidentes de segurança a sua organização sofreu no ano passado? E quais foram as causas?
- A estratégia de segurança cibernética da sua organização é alinhada com a estratégia de negócios? É atualizada de acordo com as necessidades em evolução?
- Você sabe o quanto uma violação de segurança cibernética impacta a organização?
- Ataques cibernéticos são riscos corporativos registrados no relatório anual?

É muito importante, quando consideramos uma informação crítica, pensar nos riscos/ameaças a que estamos expostos, como, por exemplo:

- Furto de propriedade intelectual.
- Furto de dados comercialmente sensíveis ou de posição-chave de negociação.
- Paralisação de serviços prestados ou negócios.
- Exploração das informações sobre falhas de segurança em parceiros, filiais e membros das cadeias de abastecimento, seja no Brasil ou no exterior.

DADOS DE 2014

No segundo semestre e durante a copa do mundo, foram registrados 87,5 mil tentativas de infecção de vírus com objetivo de fraude financeira e mais de 365 mil com foco em dispositivos móveis.

Fonte: http://blog.kaspersky.com.br/brasil-e-lider-em-cibertaques-na-america-latina

O Grupo de Trabalho em Segurança Cibernética do Departamento de Segurança da Federação das Indústrias do Estado de São Paulo (Deseg-Fiesp), elaborou a *Cartilha de Boas Práticas em Segurança Cibernética* com o objetivo de aprimorar a segurança no ambiente de trabalho, fornecer ações e/ou orientações e aprimorar a segurança da informação no ambiente de trabalho, refletindo positivamente no dia a dia da empresa.

Entre outros, a Cartilha explora alguns dos principais aspectos a serem considerados não só pelas indústrias, mas também por todas empresas que se preocupam com o ambiente virtual e queiram preservar a segurança de dados e de trabalho:

• Conscientizar e educar

As políticas de segurança devem cobrir o uso aceitável e seguro dos sistemas da organização, sendo importante a empresa agir sempre de forma transparente com seus usuários, explicando, educando e conscientizando sobre as regras estabelecidas.

• Trabalho remoto (se houver)

Desenvolver uma política de trabalho para funcionários e treiná-los para que haja conscientização de proteção aos dados em trânsito e armazenados.

• Gerenciar incidentes

Estabelecer uma capacidade de resposta a incidentes e recuperação de desastres.

• Gerir riscos de informação

Estabelecer uma estrutura de governança eficiente e que determine o volume de risco.

• Gerenciar privilégios de uso

Estabelecer processos de gestão de contas e limitar o número de contas privilegiadas.

• Controlar mídia removível

Produzir uma política para controlar todo acesso a mídias removíveis.

• Monitorar

Estabelecer uma estratégia de monitoramento e produzir uma política de apoio.

• Configuração de segurança

Aplicar atualizações de segurança e garantir a configuração segura de todas as tecnologias de informação e comunicação.

• Proteger contra *malware*

Produzir política relevante e estabelecer defesas *antimalware* aplicáveis e relevantes para todas as áreas de negócio.

• Segurança de rede

Proteger suas redes contra ataques externos e internos. Estabelecer controles de segurança do monitoramento e testes.

1. REGULAMENTO INTERNO DE SEGURANÇA DA INFORMAÇÃO

A empresa deve ter um regulamento interno de segurança da informação para:

- Agir de forma transparente com os seus usuários.
- Garantir a confidencialidade, integridade e disponibilidade de suas informações.
- Atribuir responsabilidades, definir direitos, deveres, expectativas de acesso e uso das suas informações pelos usuários e terceirizados.
- Definir mecanismos de controle e monitoramento da infraestrutura tecnológica para resguardar a segurança das suas informações.
- Criar cultura educativa de proteção das suas informações.

2. TERMO DE USO DOS SISTEMAS INTERNOS

A empresa deve ter um termo de uso dos seus sistemas internos visando esclarecer ao usuário que:

- A infraestrutura tecnológica é de exclusiva propriedade da empresa.
- Não há expectativa de privacidade sobre a utilização das ferramentas da empresa, as quais devem ser utilizadas exclusivamente para fins profissionais.
- Há monitoramento de todos os acessos e comunicações ocorridos por meio da infraestrutura tecnológica da empresa.

3.
CLASSIFICAÇÃO DAS INFORMAÇÕES E PERFIS DE USUÁRIOS

A empresa deve classificar as suas informações de acordo com seu grau de sigilo.

4.
GUARDA DE INFORMAÇÕES

A empresa deve prever a maneira como as informações são tratadas e armazenadas por seus usuários e ter algumas cautelas, como:

- Períodos de ausência da estação de trabalho.
- Armazenamento de informações em mídias seguras e criptografadas.
- Impressões de informações sensíveis.
- Descarte de mídias que contenham informações sensíveis.

5. UTILIZAÇÃO DA INFRAESTRUTURA

A empresa dever prever algumas cautelas em relação aos seus sistemas físicos e aos equipamentos eletrônicos fornecidos aos usuários como instrumento de trabalho, por exemplo, computadores, *desktops*, *notebooks*, telefones, programas de computador, base de dados, *e-mails*, entre outras ferramentas, que constituem a infraestrutura da empresa.

- Tal infraestrutura deve ser disponibilizada aos usuários na medida de suas necessidades, exclusivamente para desempenho de suas funções profissionais, sendo proibida a utilização para fins pessoais.
- Toda a infraestrutura está sujeita a monitoramento, não possuindo o usuário qualquer expectativa de privacidade em sua utilização, motivo pelo qual seu uso deve se dar tão somente para fins corporativos.
- As contas corporativas fornecidas ao usuário são de uso intransferível, sendo proibido o compartilhamento do acesso com terceiros.
- Proibição de armazenamento de arquivos pessoais ou não relacionados ao trabalho.
- Proibição de armazenamento, acesso e utilização de conteúdo pornográfico, discriminatório, difamatórios, bem como que viole quaisquer direitos de terceiros, especialmente direitos autorais (textos, músicas e imagens copiados sem autorização dos titulares, entre outros).
- Proibição de deleção de banco de dados.
- Proibição de instalação de qualquer *software* nos dispositivos eletrônicos da empresa não homologados por ela.

6.
UTILIZAÇÃO DA INTERNET

A empresa precisa definir como será a utilização da internet e suas aplicações, tais como Facebook, Twitter, Instagram, LinkedIn, YouTube, entre outras, e informar que o acesso provido pela empresa deve ser utilizado pelo usuário apenas para o cumprimento de suas funções profissionais.

7.
UTILIZAÇÃO DO *E-MAIL* CORPORATIVO, ENVIO E RECEBIMENTO DE ARQUIVOS E COMUNICADORES INSTANTÂNEOS

A empresa deve definir que, ao utilizar o *e-mail* fornecido por ela, o usuário deve estar ciente que seu uso está limitado aos fins corporativos, sendo vedado o uso particular. Assim:

- Todas as mensagens enviadas pelo *e-mail* corporativo devem conter a assinatura e o aviso de confidencialidade em padrões configurados.
- Cada usuário é responsável pelo uso de seu *e-mail* corporativo, bem como pelos arquivos que recebe e envia pela infraestrutura tecnológica.
- Sua utilização está sujeita a monitoramento, não subsistindo qualquer expectativa de privacidade.
- A empresa deve ter um regulamento interno de segurança da informação para agir de forma transparente com seus usuários.
- A empresa deve vedar que informações corporativas sejam transitadas por meio dos serviços de comunicação privados dos seus usuários.

8. UTILIZAÇÃO E MANIFESTAÇÃO EM MÍDIAS SOCIAIS

A empresa deve definir como será a utilização das mídias sociais. Apenas os usuários autorizados expressamente poderão acessá-las por meio da internet provida pela empresa. Além disso, a empresa deve:

- Proibir a manifestação de qualquer opinião em seu nome como se fosse uma posição oficial.
- Proibir exposição, divulgação ou compartilhamento de qualquer informação a seu respeito.
- Proibir qualquer imagem, foto, vídeo ou som captado em seu ambiente interno, com especial atenção àqueles relacionados aos usuários e aos clientes.

9. SENHAS

É importante que a empresa explique que:

- As senhas garantem que apenas pessoas autorizadas tenham acesso a determinados equipamentos e informações, validando a identidade e autenticando o usuário para assegurar sua legitimidade de acesso.
- Todas as senhas de acesso são pessoais e intransferíveis, de uso exclusivo do usuário, o qual assume integral responsabilidade pela sua guarda e sigilo, bem como pelo seu uso indevido por terceiros.
- O usuário deve trocar a senha sempre que existir qualquer situação de possível comprometimento dela.

10. ARMAZENAMENTO EM NUVEM

A empresa deverá se atentar aos contratos e ter regras específicas para eventual armazenamento de dados em nuvem, que dizem respeito ao armazenamento de informações, documentos e dados na internet, utilizando-se de ferramentas como Dropbox, SugarSync, SkyDrive e Google Drive, de modo a torná-los acessíveis por meio de qualquer equipamento.

11. ACESSO REMOTO

A empresa deve ter regras específicas para acesso remoto de rede privada do tipo VPN (rede privada virtual [*virtual private network*]), por meio de uma rede pública para conexão à rede interna da empresa.

12. VIDEOVIGILÂNCIA

A videovigilância é atividade consistente no acompanhamento e na verificação do ambiente de trabalho por meio de câmeras de segurança ou outros dispositivos semelhantes, com o objetivo de prevenir, impedir e tratar incidentes envolvendo pessoas ou assuntos referentes à segurança física da empresa e dos usuários, bem como a segurança informação.

A utilização da videovigilância deverá respeitar a dignidade dos usuários, sendo proibida a instalação de câmeras em banheiros e lavabos. As imagens gravadas são confidenciais, podendo ser divulgadas em caso de violação dos regulamentos e da Lei, assim como diante da necessidade de sua utilização como prova. As imagens poderão também ser fornecidas em caso de solicitação por autoridade judiciária ou policial, ou poderão ser espontaneamente apresentadas para investigação de crimes ou de ilícitos civis ocorridos em suas dependências.

A empresa deve deixar o usuário ciente acerca da existência de câmeras de monitoramento no ambiente corporativo, reconhecendo que a videovigilância não constitui qualquer violação à intimidade, vida privada, honra ou imagem da pessoa filmada.

13.
INCIDENTES EM SEGURANÇA DA INFORMAÇÃO

São considerados incidentes em segurança da informação quaisquer eventos que possam expor indevidamente informações da empresa.

Assim, a empresa deve implementar ações de segurança externa, além dos controles internos de proteção. A proteção externa se faz basicamente a partir da atualização contínua de *softwares* e utilização de *firewall*, antivírus e segmentação da rede, ao passo que a proteção interna está consubstanciada nas normas de segurança da informação.

A colaboração dos usuários é de fundamental importância para a proteção das informações da empresa. Assim, o usuário deve comunicar imediatamente à empresa qualquer evento de seu conhecimento que coloque em risco a segurança das informações da empresa e/ou viole suas regras internas.

14.
EXCLUSÃO DEFINITIVA E TRANSFERÊNCIA DE USUÁRIOS

No caso de exclusão definitiva do usuário, a empresa deve adotar procedimentos para revogação do acesso à sua infraestrutura tecnológica.

GRUPO DE TRABALHO DE SEGURANÇA CIBERNÉTICA (GTSC)

DEPARTAMENTO DE SEGURANÇA DA FIESP

MISSÃO

Desenvolver e promover estratégias e ações em prol da segurança cibernética, visando proporcionar à sociedade o uso seguro, consciente e ético da tecnologia da informação.

EQUIPE TÉCNICA

Ricardo Lerner
Diretor Titular do Departamento de Segurança (Deseg-Fiesp)

Rony Vainzof
Diretor do Deseg e Coordenador do GTSC

Cassio Vecchiatti
Diretor do Deseg e Membro do GTSC

Ciro Bueno
Diretor do Deseg e Membro do GTSC

Selma Migliori
Diretora do Deseg e Membro do GTSC

Willian Beer
Diretor Executivo da Alvares & Marsal Brasil e Membro do GTSC

Afonso Coelho
Membro do GTSC

Luciano Coelho
Coordenador do Deseg e Membro do GTSC

FIESP DEPARTAMENTO DE SEGURANÇA

Av. Paulista, 1313 | 6º andar | 01311-923 | São Paulo – SP
deseg@fiesp.com
www.fiesp.com.br