SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

INFORMATION SYSTEMS SECURITY

FABIANE RODRIGUES[1]
MARCELO TEIXEIRA TORRES[2]
FABIANA FLORIAN[3]

RESUMO: Atualmente, diante da expansão da internet, milhares de vulnerabilidades são reportadas todos os dias. Hoje a Segurança dos Sistemas de informação é considerado um quesito primordial e, é de extrema importância, a nossa conscientização e cautela, para evitarmos grandes danos e prejuízos às organizações. O presente artigo, busca abordar de forma generalizada a importância da Segurança nos Sistemas de Informação, dando ênfase no ambiente organizacional e nos tipos de usuários de sistemas que estão cada vez mais influenciados pelos prazeres e armadilhas existentes no mundo virtual.

Palavras-chave: Sistemas de Informação, Segurança, Dados, Cibernéticos.

ABSTRACT:
Currently, in the face of the expansion of the Internet, thousands of vulnerabilities are reported every day. Today, Information Systems Security is considered a key issue, and our awareness and caution are of the utmost importance in order to avoid great damages and losses to organizations. This article seeks to cover the importance of Security in Information Systems, with emphasis on the organizational environment and the types of system users that are increasingly influenced by the pleasures and pitfalls of the virtual world.

Keywords: Information Systems, Security, Data, Cybernetics.

---

[1] Graduando em Sistemas de Informação da Universidade de Araraquara-UNIARA. E-mail: faabyrod@gmail.com

[2] Orientador. Mestre da Universidade de Araraquar-UNIARA. E-mail: mttorres@uniara.com.br

[3] Coordenadora. Doutora da Universidade de Araraquara-UNIARA. E-mail: florian@uniara.com.br

1 INTRODUÇÃO

Discorrer sobre segurança da informação é de extrema importância no mundo globalizado em que vivemos, uma vez que tudo gira em torno da informação. Alertar empresas e usuários sobre os perigos constantes que se encontram no mundo virtual e lhe dar dicas de como se proteger de eventuais danos e/ou prejuízos futuros, com certeza, é de suma importância e contribui para diminuir os crimes virtuais.

Atualmente, as empresas são totalmente dependentes de Sistemas de Informação, o que significa que, se esses sistemas sofrerem qualquer tipo de falha, de alguma forma suas atividades rotineiras de trabalho serão afetadas e algum prejuízo será tomado. Sendo assim, para minimizar essas ocorrências de perdas de dados devido a falhas, indisponibilidades ou mesmo punições legais devido ao uso impróprio dos sistemas, é de extrema importância que estes, utilizados pelas organizações, possuam políticas de segurança e cumpram com os requisitos definidos pela própria organização, baseados em seus objetivos de negócio. Lembrando que, isso é válido não só para sistemas já existentes, mas também para aqueles que estejam sendo adquiridos ou desenvolvidos.

Pensando nos sistemas já existentes, é necessário verificar se os mesmos estão de acordo com os requisitos da política de segurança da informação e, em caso de não conformidade, recomenda-se que se implante controles de sistemas de segurança

adicionais ou mesmo, a substituição dos sistemas atuais por sistemas que possuam tecnologias inovadoras.

Essa decisão de adquirir ou não um novo sistema de segurança, cabe ao responsável, no qual o mesmo deve averiguar se o novo produto está ou não dentro dos requisitos legais da segurança da organização.Portanto, deve existir dentro da empresa/ organização um processo para que o responsável possa verificar se os produtos estão ou não de acordo com os requisitos necessários, para realizar ou não a aquisição desses novos sistemas de informação.

Agora, se tratando de sistemas desenvolvidos internamente, é conveniente que seja adotado, desde o início do projeto, um sistema de segurança que esteja de acordo com os requisitos organizacionais, pois além de ser muito menos custoso, é muito mais eficaz do que adicionar controles de segurança em um projeto que se encontra em estado avançado.

Todo Sistema de Informação contém falhas, as quais mais cedo ou mais tarde acabam sendo descobertas por hackers, usuários ou pelo próprio fabricante. Essas falhas geram diversas vulnerabilidades, principalmente quando fazem parte de sistemas amplamente utilizados, onde acabam sendo disponibilizadas na Internet, se tornando disponíveis para o acesso de qualquer pessoa, que poderá utilizá-las tanto para fazer o bem quanto para fazer o mal.

Pensando diminuir a possibilidade de comprometimento da segurança das informações organizacionais, devido a esse quadro, convém primeiramente que seja feito um inventário completo e, que o mesmo seja sempre atualizado, dos ativos de informação(fabricantes, versões, usuários internos).

Identificadas essas vulnerabilidades, passa-se a ter uma noção do quão exposta está a organização a vulnerabilidades técnicas, que devem ser minimizadas e/ou eliminadas por meio da implantação dos Sistemas de Segurança de Informação, desde que estejam de acordo com os requisitos necessários de sua organização. Convém ainda, a execução

de testes para ter-se a certeza de que os problemas realmente foram solucionados. E, para fins de auditoria, todo esse processo deve ser documentado e arquivado.

Com a evolução permanente das ameaças, conhecer e gerenciar bem os riscos de segurança cibernética se tornou uma das maiores preocupações dos líderes de empresas e governos. As organizações estão agindo, de forma que, cada vez mais, adotam tecnologias inovadoras, como a segurança cibernética baseada em nuvem, a segurança analítica e a autenticação avançada para reduzir riscos e melhorar seus programas de segurança.

2 SEGURANÇA DA INFORMAÇÃO

Segurança da Informação significa proteger seus dados e sistemas de informação de acessos e uso não autorizados, divulgação, modificação, leitura, gravação, inspeção e destruição. O Conceito de segurança da informação está relacionado a confidencialidade, integridade e disponibilidade da informação. Já o conceito de segurança de processamento está ligado a disponibilidade e operação da infraestrutura computacional. Esses conceitos são complementares e asseguram a proteção e a disponibilidade das informações das organizações. O impacto de perda de dados ou até mesmo violação de informações para uma empresa é enorme e pode, em alguns casos, levá-la a falência. Existem casos reais de empresas que tiveram seus sistemas invadidos por hackers e que sofreram quedas no valor de suas ações nas bolsas de valores. A questão de segurança da informação cresce muito em importância com o uso do comércio eletrônico e das redes sociais. (FAGUNDES)

As diretrizes para a segurança dos sistemas de informação, definidas pelo OCDE(Organisation for Economic Co-operation and Development), propôs nove princípios geralmente aceitos: consciência e responsabilidade; resposta; ética; democracia; avaliação de risco; design e implantação de segurança; gestao da segurança e reavaliação. (FAGUNDES)

A Segurança da Informação se refere à proteção de determinados dados, com a intenção de proteger e preservar seus respectivos valores para uma determinada organização ou indivíduo.

Podemos dizer que informação é todo conteúdo ou dado valioso para uma organização, que consiste em qualquer conteúdo com capacidade de armazenamento ou transferência, que serve a determinado propósito e que é de utilidade do ser humano. Atualmente a informação digital é um dos principais produtos de nossa era e necessita ser protegida. A segurança de determinadas informações podem ser afetadas por vários fatores, como os comportamentais e do próprio usuário, pelo ambiente/infraestrutura em que ela se encontra armazenada e através de pessoas que tem o objetivo de agir de má fé(roubar, destruir ou modificar essas informações). (KERDNA).

Segurança da Informação está relacionada com a proteção de um conjuto de dados, no sentido de preservar o valor que possuem para uma organização. Atualmente o conceito de Segurança da Informação está padronizado pela norma ISO/IEC 17799:2005, influenciada pelo padrão inglês(British Stantard) BS 7799. A série de normas ISO/IEC 27000 foram reservadas para tratar de padrões de Segurança da Informação, incluindo a complementação ao trabalho original do padrão inglês. A ISO/IEC 27002:2005 continua sendo considerada formalmente como 17799:2005 para fins históricos.

A segurança se refere a proteção existente sobre dados de uma determinada empresa ou pessoa, isto é, aplica-se tanto à informações corporativas quanto pessoais. E pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição. (Ferreira)

3 PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

- Confidencialidade

A informação só deverá ser acessada pelas pessoas que possuam devida autorização e que estejam ligadas diretamente com a empresa. O sistema deve

possuir travas de segurança para que as pessoas que não possuam autorização, não consigam acessar as devidas informações.

- Confiabilidade

É demonstrar ao usuário/cliente a fidelidade e a boa qualidade da informação com a qual ele estará trabalhando.

- Integridade

É a garantia de que a informação estará protegida e completa, da maneira como foi arquivada. Evitando quaisquer problemas, como alterações indevidas ou de má fé.

- Disponibilidade

É ter a certeza de que a informação sempre estará disponível e acessível em qualquer hora e lugar que o usuário autorizado precisar acessá-las.

- Autenticidade

É saber através de registros apropriados quem teve acesso a tais informações, quem realizou alterações/exclusões e acima de tudo, se possui autorização do responsável em todas essas execuções.

De forma que os usuários vejam que a segurança dessas informações estão sendo tratadas com devido cuidado e responsabilidade, para que dessa forma, todos sejam beneficiados, sendo eles, gestores/colaboradores, assim como os clientes.

- Não Repúdio

Visa garantir que o autor não negue ter criado ou assinado algum documento ou arquivo.

Estabelecer um programa de Segurança da Informação em uma organização deve sempre passar por ações que levem a esses princípios. Tal modelo deve estar acompanhado por um sistema de gestão de Segurança da Informação, no qual

precisa ser planejado e organizado, implementado, mantido e monitorado. (Oliveira, 2016).

Figura 1- Modelo dos Princípios da Segurança da Informação.
Fonte: Bertola, 2013.

4 MELHORES PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO

A segurança da Informação possui diversas práticas, onde fazendo uma análise descobrimos quais são as melhores práticas a serem utilizadas em sua empresa. Lembrando que, essas práticas podem ir do básico ao sofisticado, ou seja, existem as práticas mais comuns, conhecidas por todo o mercado e as mais sofisticadas que só quem é especialista na área de segurança, as conhece e aplica. Sendo elas:

- Detectar vulnerabilidade de hardware e software

Esses equipamento de TI estão sempre passando por evolução tecnológica e portanto, precisam sempre ser atualizados, não perdendo sua qualidade e eficácia. Ou seja, não podendo se basear apenas pelo custo, mas sim por sua qualidade e todos seus aspectos técnicos. (POSITIVO, 2017).

A defasagem e a falta de qualidade tecnológica torna extremamente vulnerável o sistema de segurança de qualquer empresa, gerando muitas consequências, tais como: ineficiência operacional, insatisfação dos clientes, ineficácia do processo decisório, perda de competitividade com o mercado, etc.

Esses softwares estão sempre sujeitos a falhas técnicas, de configurações de segurança e mal uso. Devido a todas essas questões é necessário que sejam adotadas práticas de segurança para cada elemento da infraestrutura de TI: os softwares, computadores, servidores, a rede, dentre outros. Também é necessário providenciar treinamentos e atualização de conhecimento para toda a equipe de TI, seus colaboradores e usuários que utilizam desses recursos tecnológicos. Não sendo menos importante, a detecção, de forma ágil, em notar as vulnerabilidades dos equipamentos(hardware e software), para assim, tomar decisões imediatas. (POSITIVO, 2017).

- Cópias de Segurança

Cópia de segurança ou o tão conhecido backup, é um mecanismo fundamental para garantir a disponibilidade da informação, caso as bases de dados onde essas informações estão armazenadas sejam danificadas ou até mesmo roubadas.

Esse backup deve conter pelo menos duas ou mais cópias armazenadas em locais distintos e seguros fora do prédio de sua empresa. Podem ser armazenados tanto em dispositivoso físicos, como servidores de backup, pendrive, HD externo, ou mesmo, em nuvem. Sendo mais importante ressaltar que haja sempre mais de uma cópia segura armazenada em local distinto. (POSITIVO, 2017).

A partir dessas cópias de segurança, podemos recuperar em tempo hábil, informações que foram perdidas acidentalmente ou mesmo devido a consequências naturais(enchentes, incêndio, etc) ou até mesmo por sabotagens e roubo de informações.

Um dos casos que é válido lembrar é o das empresas que funcionavam no Word Trade Center, na ocasião do atentado de 11 de setembro de 2001, que tinham boas práticas de manutenção de backup e todas sobreviveram a este terrível atentado, voltando a funcionar normalmente em poucos dias. (POSITIVO, 2017).

- Redundância de Sistemas

É importante sempre garantir que a organização possua alta disponibilidade de informações com a garantia de possuir redundância de sistema, ou seja, a empresa deve dispor de infraestrutura replicada, sendo ela, física ou virtualizada.

Se ocorrer de um servidor ou mesmo outro equipamento de TI(roteador, nobreak, etc) falhar, seu substituto deve entrar imediatamente em ação, permitindo que suas operações continuem, de forma, as vezes, até imperceptível.

- Eficácia no controle de acesso

Existem mecanismos físicos e lógicos destes controles de acesso a informação e as vezes até mesmo, uma combinação dos dois. Estes mecanismos podem ser físicos: sala de infraestrurtura de TI com acesso restrito e com sistemas de câmeras de monitoramento.

Outra forma de restrição de acesso é utilizar o uso de travas em portas, que serão acionadas somente por senha. Já os principais mecanismos lógicos, são:

1.Firewall

Sendo ele, um mecanismo de tráfego de dados entre os computadores de uma rede Interna e destes com outras redes externas. Ele trabalha utilizando

protocolos de segurança(TCP/IP, IPSec, HTTP, etc) que garantem a eficaz comunicação entre as duas pontas, visando sempre proteger e impedir intrusões.

2. Assinatura Digital

É uma forma segura de identificação do usuário que possui validade legal aos documentos digitais, assegurando a autenticidade do emissor daquela informação.

3. Biometria

Os acessos as informações só são permitidos para a pessoa autorizada, levando em consideração suas características físicas (impressão digital, voz, padrões da íris do olho, etc).

Outra jogada importantíssima do controle de acesso é o uso de equipamentos próprios dos colaboradores para a operação de sistemas e aplicativos empresariais de forma remota.

Porém, como a empresa não possui controle sobre as configurações de segurança destes dispositivos particulares, é necessário que ela sempre reforce os mecanismos de validação de autenticidade dos usuários e as barreiras contra os famosos ataques cibernéticos.

- Política de Segurança da Informação

Se trata de um documento que estabelece diretrizes comportamentais para os membros da organização, no qual atinge as regras de uso dos recursos de tecnologia da informação.

Estas regras são utilizadas para impedir invasões e ataques cibernéticos, no qual podem resultar em fraudes ou mesmo em vazamento de informações, evitar a entrada de vírus na rede ou roubo de dados e também garantir a confidencialidade, confiabilidade, integridade, autencidade e disponibilidade das informações.

Vale ressaltar que esta política deve ser desenvolvida de forma participativa com a equipe de TI e seus colaboradores, de forma que seja aprovado pela alta direçao da empresa. É indispensável também, que o texto desta política seja, prático e objetivo, de forma que facilite e estimule a leitura, tornando o processo de divulgação de treinamento das pessoas mais leve e eficaz.

- Decisão pela estrutura de nuvem pública/ privada/ híbrida

Atualmente uma das formas mais avançadas e eficazes de garantir a segurança da informação é a decisão pela utilização de uma estrutura de computação em nuvem. Essa estrutura possui tres categorias distintas: nuvem pública, privada ou híbrida.

1. Nuvem pública
   Nesta categoria, toda a infraestrutura de TI, sua manutenção, seus mecanismos de segurança e sua atualização são de responsabilidade do provedor do serviço. Sua instalação geralmente é rápida e seus recursos são escalonáveis, de acordo com o perfil da empresa.

2. Nuvem privada
   A nuvem privada é prioridade da empresa e costuma ficar instalada em sua área física, onde requer de infraestrutura de hardware, software, segurança e pessoal adequado para o gerenciamento.

3. Nuvem Híbrida
   É a combinação dos dois tipos citados anteriormente, ou seja, parte dos dados são disponibilizados na nuvem privada e outra parte fica na nuvem pública. Os que exigem sigilo ficam na parte privada e os que não são confidenciais na parte pública.

Os 3 tipos de nuvem respeitam os altos padrões de segurança da informação, basta apenas avaliar qual o mais adequado para as necessidades de sua organização.

A computação em nuvem viabilizou serviços como IaaS(Infraestrutura como Serviço), PaaS(Plataforma como Serviço) e SaaS(Software como serviço). Essas novas modalidades, permitem terceirizar importantes serviços de tecnologia da informação, reduzindo custos, assegurando agilidade e atualização permanente, elevando o nível de segurança de hardware e software. (POSITIVO, 2017).

- Gestão de Risco Apropriada

Os principais riscos à Segurança da Informação estão relacionados à alguns itens, como:

1. Falta de Orientação

   O desconhecimento de técnicas de proteção e não saber como operar equipamentos, sistemas e aplicativos, coloca em risco a segurança da informação. Por isso, é de suma importância, sempre promover treinamentos, atualizando o conhecimento e os recursos de TI dos usuários e da equipe de TI.

   Dependendo do porte da empresa, seja ela média ou grande, vale a pena pensar em desenvolver profissionais C-Level em TI, que possam ampliar os horizontes tecnológicos da empresa, tornando a área de TI muito mais alinhada a estratégia empresarial.

2. Erros de procedimentos internos

   Procedimentos de gestão da segurança da informação mal estruturados ou desatualizados podem acarretar em vulnerabilidade ou até mesmo em perda de dados. E estas vulnerabilidades podem se manifestar nos softwares, hardwares e até mesmo através do despreparo das pessoas envolvidas.

3. Negligência

   O não cumprimento com a política de segurança da informação ou com os processos internos de TI, por mero descuido, podem acarretar em prejuízos financeiros, de imagem ou materiais.

   Devido a isso, é de extrema importância a realização de campanhas de conscientização, para redobrar os cuidados e ficar sempre alerta a ataques

cibernéticos, especialmente em e-mails, sites e arquivos maliciosos, que podem ocasionar em propagação de vírus, malwares e outros na rede de informática.

4. Malícia

   Devemos conhecer as principais fontes de riscos para podermos mapear os diversos cenários que podem gerar ameaças à segurança da informação e tornar possível o desenvolvimento de boas práticas de gestão de risco. Importante ressaltar também a importância de possuir mecanismos que detectem instrusões, pois ações mal-intencionadas podem vir de colaboradores insatisfeitos e até mesmo de pessoas externas, que tornam a segurança da informação instável.

- Regras de Negócio bem definidas

As regras de negócios são indispensáveis para a configuração de permissões de acesso em softwares, hardwares e redes lógicas. Essas regras tem a necessidade de serem melhoradas continuamente, sempre agregando mecanismos físicos e lógicos atualizados, assim como novas práticas comportamentais que contribuam para diminuir os riscos à segurança da informação.

Portanto, as informações críticas devem ser identificadas e as regras de negócio referentes ao acesso, manutenção(inclusão, alteração e exclusão) e tempo de guarda devem ser estabelecidas de forma criteriosa, para garantir a total segurança dos dados.

- Cultura da organização

A terceira plataforma de TI combinou tecnologias sociais, computação em nuvem, dispositivos móveis(smartphones, tablets, etc) e tecnologias de análise de dados(business intelligence e big data) para assim promover a conectividade permanente e gerar informação em tempo real sobre o comportamento dos consumidores.

Esse movimento todo fez com que as metodologias de gestao da segurança da informação ganhassem uma nova dinâmica de readequação e ajustes constantes,

para bloquear as novas rotas de ataques cibernéticos as bases de dados das organizações.

Tudo isso impacta diretamente na cultura organizacional, a qual necessita se adequar a essa transformação digital, atualizando seus processos internos, sem se descuidar da segurança.

- Contratos de Confidencialidade

Muitas vezes, devido a realizações de suas atividades, colaboradores internos de uma organização e até mesmo os terceirizados, precisam ter acesso a informações sigilosas, que devem ser resguardadas.

A melhor e mais segura forma de preservar a segurança dessas informações, é fazer com que todas as pessoas que conheçam e acessem essas informações, assinem um contrato de confidencialidade. Lembrando que, é importante que este contrato seja redigido considerando os requisitos legais aplicáveis a organização e eventuais acordos deste gênero que estejam de comum acordo com clientes, fornecedores, prestadores de serviços e parceiros de negócios.

- Gestão de Continuidade de negócios(GCN)

A gestão de continuidade de negócios é uma prática que visa estabelecer planos de ação de emergência para respostas ágeis a eventos adversos(desastres naturais, explosões, incêndios, atentados, falhas nos sistemas ou nos equipamentos, etc).

Esses planos de ação devem permitir minimizar ou até mesmo evitar impactos negativos que possam ser causados, tais como: paralisações na produção e/ou prestação de serviço, perdas financeiras e danos a imagem ou credibilidade do negócio.

A GCN nada mais é do que uma ferramenta de ação preventiva que deve priorizar a tomada de ações para os processos, produtos ou serviços de TI.

- Benchmarking

O benchmarking é um importante instrumento de gestão que compara os produtos, serviços, processos e práticas empresariais próprios de uma organização ou com os de terceiros.

Muitas idéias surgem de análises de situações das empresas de ramos diferentes de atividade e que podem ser replicadas, em casos de sucesso, ou evitadas, em caso de insucesso em sua organização.

Lembrando que o benchmarking não foca somente em situações de sucesso do mercado empresarial para gerar conhecimento, mas também em lições obtidas em experiências ruins que são divulgadas. Conhecer esses casos de insucesso de gestão de segurança serve como base para não cometer os mesmo erros e evitar possíveis prejuízos.

Vamos relembrar alguns casos que viraram manchetes em jornais:

1. eBay

   Em maio de 2014 a base de dados do eBay sofreu a violação das senhas de 112 milhões de pessoas, que foram obrigadas a trocá-las e ocasionou a perda de dados pessoais ali armazenados. Foram preservadas apenas as informações financeiras.
2. Snapchat

   O Snapchat passou por maus momentos em janeiro e outubro de 2014. No primeiro evento de ataque cibernético, foram vazados os dados pessoais de 4,6 milhões de usuários. O que gerou um pedido de desculpas por parte da empresa e a promessa de melhorias nos mecanismos de segurança.

   Já o segundo evento, resultou de falhas de segurança em um parceiro de negócios do Snapchat, que estava responsável por armazenar imagens compartilhadas pelo APP, o que possibilitou a divulgação indevida de 13GB de fotos dos usuarios na WEB.
3. Kickstarter

   A Kikckstarter foi vítima da quebra de segurança dos dados pessoais e senhas de 6 milhões de usuários cadastrados, também no ano de 2014. A reação

rápida da empresa conseguiu evitar a perda de dados dos cartões do clientes, mas os impactos nao deixaram de ser imensos.

4. Nasdaq

   Nem mesmo o sistema de segurança da Nasdaq, considerado um dos mais robustos do mercado, ficou imune a intrusão, alteração e roubo de 160 milhões de registros, no ano de 2013, gerando altos prejuízos financeiros.

5. Heartland Payment Systems Inc.

   Em 2009 um malware infectou o datacenter da Heartland, importante operadora de cartões de crédito norte-americana e permitiu o acesso de hackers a 100 milhões de registros, causando perdas milionárias de recursos financeiros e de inúmeros clientes.

Devido a esses eventos desagradáveis, devemos estar sempre alertas e com os radares da equipe ligados para a percepção de riscos internos e externos, que podem abalar o moral dos colaboradores e dos clientes de uma organização e que, em alguns casos, podem até decretar o fim de uma empresa. (POSITIVO, 2017).

Portanto, essas 12 melhores práticas de segurança da informação que vimos aqui, poderá ser utilizada por sua empresa para evitar qualquer tipo de instrusão, roubo, fraude, alteração e até mesmo exclusões indevidas de informações. Desta maneira, serão prevenidas perdas de milhares de clientes, assim como o repasse indesejado de estratégias de negócios para empresas concorrentes.

As atualizações tecnológicas ao mesmo tempo que produzem novos recursos para proteção da informação, também abrem espaços que podem ser aproveitados por pessoas mal-intencionadas para realizar ataques cibenérticos. Devido a isso, é necessário que sempre estejamos atentos aos casos de violação de segurança da informação para que, a partir destes casos, determinemos novas práticas de proteção, tanto na área das máquinas e aplicativos, quanto nas ações das pessoas.

Outro ponto importante quando o assunto é segurança, é a adoção de critérios rigorosos para a seleção e monitoramento da segurança da informação nos parceiros de negócios da area de TI. Além disso, também é preciso garantir a segurança

jurídica das relações de trabalho e de parceria, por meio da aplicação de contratos de confidencialidade.

Por fim, vimos que a segurança da informação possui muitas facetas, sendo elas:

1. Tecnológicas
2. Jurídicas
3. Humanas
4. Físicas
5. Virtuais.

Todas elas devem ser alvos de medidas que contribuam para melhorar a gestão de segurança da informação.

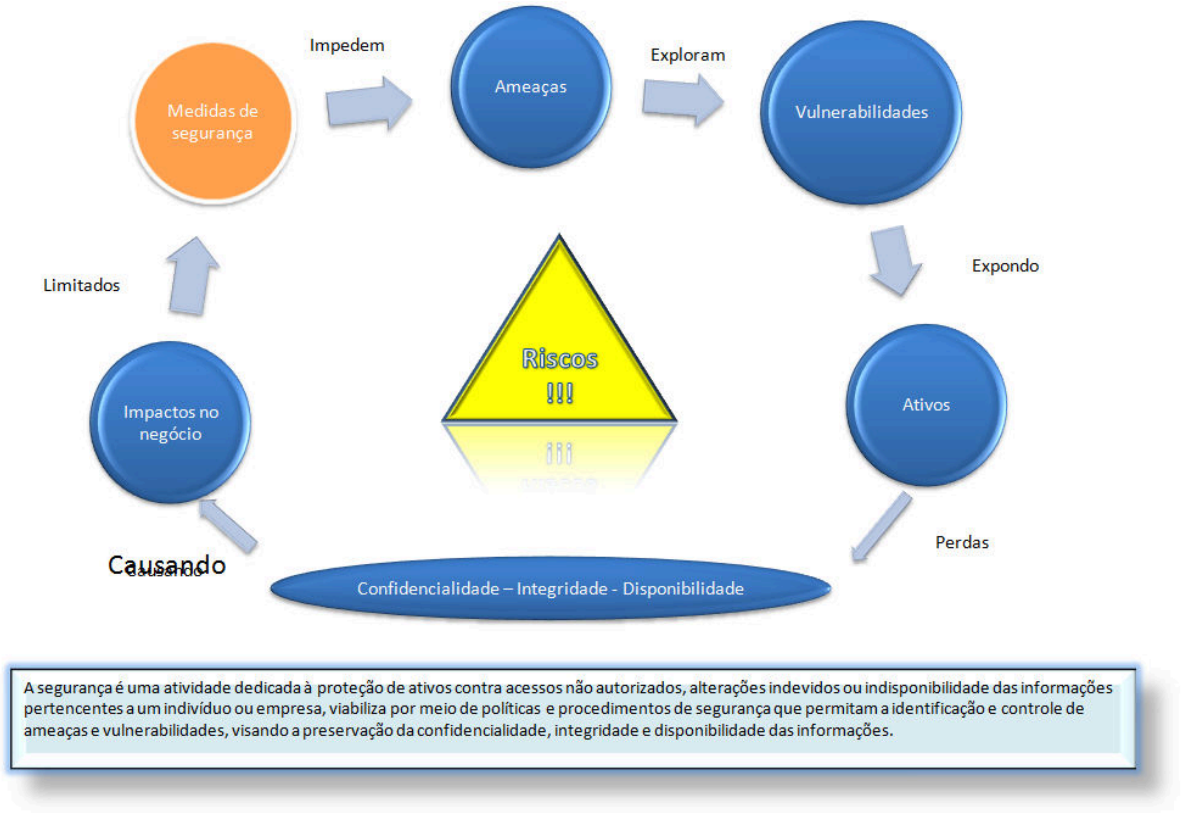

Figura 2- Ciclo da Segurança da Informação.

Fonte: Araújo, 2010.

5 MAIORES RISCOS

O ano de 2017 foi marcado por diversos acontecimentos no mundo da Segurança da Informação. Tivemos o enfático 12 de maio e os ataques de Ransomware com WannaCrypt, onde milhares de empresas e organizações do mundo todo foram afetadas, além de vários outros ataques a nível mundial.

Esses acontecimentos só nos mostram o quanto o mundo corporativo está vulnerável em relação à Segurança da Informação e reafirmam a enorme

necessidade de invetimentos em prevenção contra ataques virtuais e proteção de dados corporativos.

Essa sequência de ataques só ressalta que o mercado também deve considerar o crescimento do cibercrime, em especial em forma de Ransomware, que, devido a utilização de criptomoedas para movimentações financeiras, dificulta o rastreio e identificação dos criminosos.

É claro que, com todos esses incidentes de segurança e prejuízos que foram causados, muitas lições foram aprendidas e a principal delas é que nenhuma empresa está 100% protegida, já que as formas de ataques mudam constantemente e as vulnerabilidades estão em diversos pontos, como por exemplo, nos próprios usuários. Outra lição que se pode tirar com tudo isso, é sobre a importância da segurança da informação e a necessidade de proteção desses dados, independente se estamos falando de uma organização de pequeno ou grande porte, pois as duas podem ter prejuízos enormes ou até mesmo deixar de operar, sem acesso aos dados e sistemas de seu negócio.

Se engana quem pensa que 2017 foi um ano terrível em matéria de quebras de segurança de dados, pois o Forúm de Segurança da Informação(ISF), um organismo global e independente de segurança de informação focado em ciber-segurança e gestão de riscos de informação, prevê um aumento significativo no número e impacto das violações de dados, devido a cinco ameaças principais que as organizações irão enfrentar no ano de 2018.

“A abrangência e o ritmo das ameaças à segurança da informação estão a prejudicar a reputação das organizações de maior confiança da actualidade”(DURBIN).

“Em 2018 vamos ver as ameaças a tornar-se mais sofisticadas, personalizadas aos pontos fracos de cada um e transformando-se para contornar as defesas que já foram implantadas”(DURBIN).

A ISF também prevê que os clientes insatisfeitos vão pressionar os governos a introduzir legislação de proteção de dados mais rígida.

Abaixo estão as 5 ameaças que as organizações poderão enfrentar em 2018:

- **Crime as Service(CaaS) terá mais ferramentas e serviços**

  No ano de 2017, o ISF havia previsto um salto quântico com organizações criminosas a desenvolver hierarquias complexas, parcerias e colaborações em tudo semelhantes à organização do setor privado.

  Durbin, diretor do ISF considera que a previsão se concretizou, pois uma vez que, em 2017 se regirou um enorme incremento no ciber-crime, em particular do crime-como-um-serviço. A ISF prevê que a tendência continue em 2018 e com maior variedade de organizações criminosas em novos mercados e distribuídas por todo o mundo.

  Em 2018, através do CaaS, os ciber-criminosos aspirantes, sem necessitar de muitos conhecimentos técnicos, poderão comprar ferramentas e serviços que lhes permitam realizar ataques que de outra forma nao seriam capazes de empreender.

  O criptoware será atualmente a mais popular categoria de malware. Anteriormente, a utilização do ransomware por parte dos criminosos dependia de uma cruel forma de confiança, onde, depois de bloquear o computador, a vítima pagaria o resgate e o ciber-criminoso o desbloqueava.

  Durbin acredita na chegada de ciber-criminosos aspirantes e que devido a isso, essa confiança que antes tinham, irá sumir. Até as vítimas que pagam o resgate poderão nao ter acesso a chave para desbloquear seus dados. Ele acredita que os ciber-criminosos estão tornando-se mais sofisticados na utilização de engenharia social e mesmo os alvos geralmente sendo indivíduos e não empresas, esses ataques representam uma enorme ameaça as organizações.

- **Internet das Coisas adiciona perigos**

  As organizações estão adotando cada vez mais dispositivos das Coisas(IoT), mas a maioria desses dispositivos nao está seguro desde sua concepção(“security by design”). Além disso, a ISF alerta que haverá uma crescente falta de transparência no ecossistema de IoT, com termos e condições muito vagas que permitem às organizações utilizar dados pessoais de modos que os clientes nao gostariam.

  Será de grande preocupação para as organizações saberem que informações estão saindo de suas redes ou que dados podem ser captados e transmitidos secretamente por dispositivos como smartphones e televisões inteligentes. Quando essas violações começarem a ocorrer ou as violações de transparência forem reveladas, as organizações estarão sujeitas a serem responsabilizadas.

- **Cadeia de abastecimento: O elo mais fraco na gestão de risco**

  A ISF chama atenção há anos para as questões de vulnerabilidade da cadeia de abastecimento. A organização afirma que existe um vasto conjunto de dados valiosos e sensíveis que é frequentemente partilhado com seus fornecedores. Sendo que, quando essa informação é compartilhada, o controle direto é perdido, ou seja, isso significa um grande risco de se comprometer a confidencialidade, integridade ou a disponibilidade de informação.

  Esse ano, as organizações terão de se concentrar e focar nos pontos mais fracos de suas cadeias de abastecimento e embora nem todas as quebras de segurança possam ser prevenidas com antecedência, as empresas e os fornecedores terão de ser ágeis em identificar quaisquer vulnerabilidade.

  Durbin recomenda que sejam adotados processos de grande impacto e reproduzíveis com garantias proporcionais aos riscos enfrentados. As organizações devem também incorporar gestão de riscos de informações na cadeia de abastecimento nos processos de gestão de contratos e fornecedores existentes.

"Todos nós temos cadeia de abastecimento. O desafio que enfrentamos é saber como está a nossa informação em cada fase do ciclo de vida? Como protegemos a integridade dessa informação enquanto é partilhada?"(DURBIN).

- **Regulamentação irá somar-se a complexidade da gestão de ativos críticos**

A regulamentação vai acrescentar complexidade e o Regulamento Geral de Proteção de Dados(RGPD) estará em vigor agora em Maio de 2018, acrescentando uma nova camada de complexidade à gestao de ativos críticos. O ISF assinala que os recursos adicionais necessários para abordar as obrigações da RGPD são suscetíveis de aumentar os custos de conformidade e de gestão de dados e ainda de desviar a atenção e o investimento de outras tarefas.

- **Riscos do desalinhamento com as expectativas da administração**

De acordo com a ISF, o desalinhamento entre as expectativas da administração e a realidade da capacidade da função de segurança da informação em entregar os resultados, será uma grande ameaça.

> *A administração, em regra, nao percebe. Compreendem que estão a trabalhar no ciber-espaço, mas o que não entendem, em muitos casos, é a real implicação disso. Eles acham que o CISO(Chief Information Security Officer) tem tudo sob controle. Em muitos casos, a administração ainda nao sabe as pergutas certas a fazer. E o CISO ainda não sabe como falar com a administração ou com os responsáveis pelo negócio sobre o assunto(DURBIN).*

A ISF acredita que a administração espera que os orçamentos de segurança da informação mais elevados, dos últimos anos, tenha habilitado o CISO e a função de segurança da informação a produzir resultados imediados, porém uma organização totalmente segura é um objetivo inalcançável.

E mesmo que as organizações tenham capacidade e competência para realizar melhorias à Segurança da Informação, muitas administrações não compreendem que isso leva tempo e esse desalinhamento significa que quando ocorrer um

incidente importante, ele nao terá apenas impacto na organização, mas sim, é provável que tenha impacto na reputação da administração, tanto coletiva como individual.

Um bom CISO precisa ser um vendedor e um consultor. Não se pode apenas possuir as duas habilidades, ou seja, eu posso ser o melhor consultor do mundo, porém se não consigo vender minhas idéias, estas não vão chegar à sala da administração.

6 CONCLUSÃO

Neste artigo foram apresentados os príncipios e a importância da Segurança da Informação dentro das empresas/organizações.

Após pesquisa e dados coletados, foram apresentados a importância da Segurança da Informação, seus princípios e as práticas a serem aplicadas. Também foram apresentados as ameaças predominantes, o que conclui-se que nos dias de hoje é de suma importância que as organizações possuam sistemas de Segurança da Informação para proteção de seus dados.

Estamos em tempos em que os ciber-ataques estão evoluindo cada vez mais e por menor que seja, sempre causam prejuízos enormes aquelas empresas que estão despreparadas. Portanto, com esse estudo, reafirmo a importância da proteção dos dados de uma empresa, proporcionando maior segurança à seus usuários e colaboradores.

REFERÊNCIAS

ALFREDO SANTOS. **Quem Mexeu no meu Sistema?** Primeira Edição, Editora: Brasport, 2008

AMEAÇAS E ATAQUES CIBERNÉTICOS. Disponível em: < http://web.unifoa.edu.br/cadernos/edicao/05/11.pdf> Acesso em: 07 Abr.

AMEAÇAS E RISCOS. Disponível em: < https://www.computerworld.com.pt/2017/11/20/cinco-ameacas-a-seguranca-de-informacao-que-vao-dominar-2018/> Acesso em: 07 Abr.

CABRAL,CARLOS / CAPRINO,WILLIAN. **Trilha Em Segurança da Informação - Caminhos e Ideias Para A Proteção de Dados.** Primeira Edição, Editora: Brasport, 2015.

IMPLEMENTAÇÃO DA SEGURANÇA DA INFORMAÇÃO. Disponível em: < http://www.techoje.com.br/site/techoje/categoria/detalhe_artigo/221> Acesso em: 17 Mar.

KIM,DAVID / SOLOMON,MICHAEL G. **Fundamentos de Segurança de Sistemas de Informação**. Primeira Edição, Editora: LTC, 2014.

PRINCÍPIOS E PRÁTICAS DA SEGURANÇA DA INFORMAÇÃO. Disponível em: < https://www.meupositivo.com.br/panoramapositivo/seguranca-da-informacao/> Acesso em: 19 Mar.

REQUISITOS DE SEGURANÇA. Disponível em: < http://marceljm.com/seguranca-da-informacao/seguranca-em-sistemas-de-informacao/> Acesso em: 20 Fev.

RISCOS. Disponível em: <https://www.sienge.com.br/blog/seguranca-da-informacao-em-empresas-riscos-e-como-se-proteger/> Acesso em: 05 Abr.

RISCOS. Disponível em: <https://www.profissionaisti.com.br/2018/02/tendencias-em-seguranca-da-informacao-para-2018-e-como-ficar-protegido/> Acesso em: 20 Abr.

SEGURANÇA CIBERNÉTICA. Disponível em: < https://www.pwc.com.br/pt/publicacoes/servicos/assets/consultoria-negocios/2016/tl-gsiss16-pt.pdf> Acesso em: 15 Mar.

SEGURANÇA DA INFORMAÇÃO. Disponível em: < http://efagundes.com/artigos/seguranca-da-informacao/> Acesso em : 10 Fev.

SEGURANÇA DA INFORMAÇÃO. Disponível em: < http://seguranca-da-informacao.info/> Acesso em: 12 Fev.

SEGURANÇA DA INFORMAÇÃO. Disponível em: < http://www.apinfo2.com/apinfo/informacao/artigo81.cfm> Acesso em:12 Fev.