Muito mais do que uma senha segura

Segurança da Informação: um guia prático

Versão 1.0

Novembro / 2018

Licença

Créditos

Arte
Amanda Serikawa Balzano
Imagens: Fonte Vector Stock

Criação e Revisão
Amanda Serikawa Balzano
André Luiz Leitão de Azevedo
Bruno Oliveira Rodarte
Fernando Torres Ferreira da Silva
Leandro Silva Lemos
Luiz Felipe Meireles Mendes
Luiz Felipe Miranda Ferreira
Mônica Cristina Ferreira Crespo Souza
Paulo José Souza Demestri
Rider Carlos Fernandes Sateles
Rodrigo Costa dos Santos
Vitor Melo Arruda Leite
Wellington de Morais Gino
William Stauffer Telles

Versão 1.0
Novembro / 2018

Índice

Introdução

Este e-Book é um trabalho colaborativo idealizado para esclarecer os principais conceitos de Segurança da Informação através de uma linguagem simples e didática.

A segurança da informação tem por objetivo garantir a confiabilidade entre os processos, as tecnologias e as pessoas através dos principais pilares: a confidencialidade, integridade e disponibilidade. Alguns autores também consideram os pilares não repúdio e autenticidade.

Acreditamos que através da conscientização vamos preparar as pessoas para as situações em que estarão expostas. Queremos alinhar o pensamento humano com práticas de defesa e antecipação para que se apliquem em conformidade com as normas e políticas estabelecidas pela organização em que atua.

Esperamos que o e-book conscientize os profissionais de TI sobre a importância da Segurança da Informação nas empresas.

Boa leitura!

Capítulo 1

Espionagem

Espionagem

Há quem diga que a espionagem acabou com a Guerra Fria , porém, casos como o Edward Snowden [1] nos provam que somos constantemente espionados, sejam por empresas, governo, ou até mesmo através de engenharia social, precisamos sempre nos manter informados sobre tendências de ataques, golpes, e até mesmo sobre o que podemos ou não falar nas redes sociais.

"Offline é o novo luxo", quem hoje que possui um smartphone fica offline? Dificilmente estamos fora dessa rede, e, portanto, precisamos saber o que escrevemos, falamos, pesquisamos dentro dela. Como podemos fazer isso de forma segura?

Há grandes riscos nessas ações, uma vez que as empresas e governos que espionam, são também detentores de poder e de consideráveis técnicas para uso dessas informações, seja para adotar estratégias de marketing ou para saber sobre o pensamento político de uma população.

Logaritmos de sites de redes sociais influenciam nosso poder de compra, nossos desejos, nossas posições políticas, nossas opiniões.

[1]Eduardo Snowden Exilado na Rússia após delatar um amplo esquema de espionagem pela Agência de Segurança Nacional (NSA, na sigla em inglês), o ex-agente da CIA Edward Snowden considerou autêntica a revelação do WikiLeaks de que a agência controla secretamente celulares, PCs e até smart TVs. Segundo ele, as informações mostram que o governo teria pagado para manter um esquema de espionagem.

Espionagem

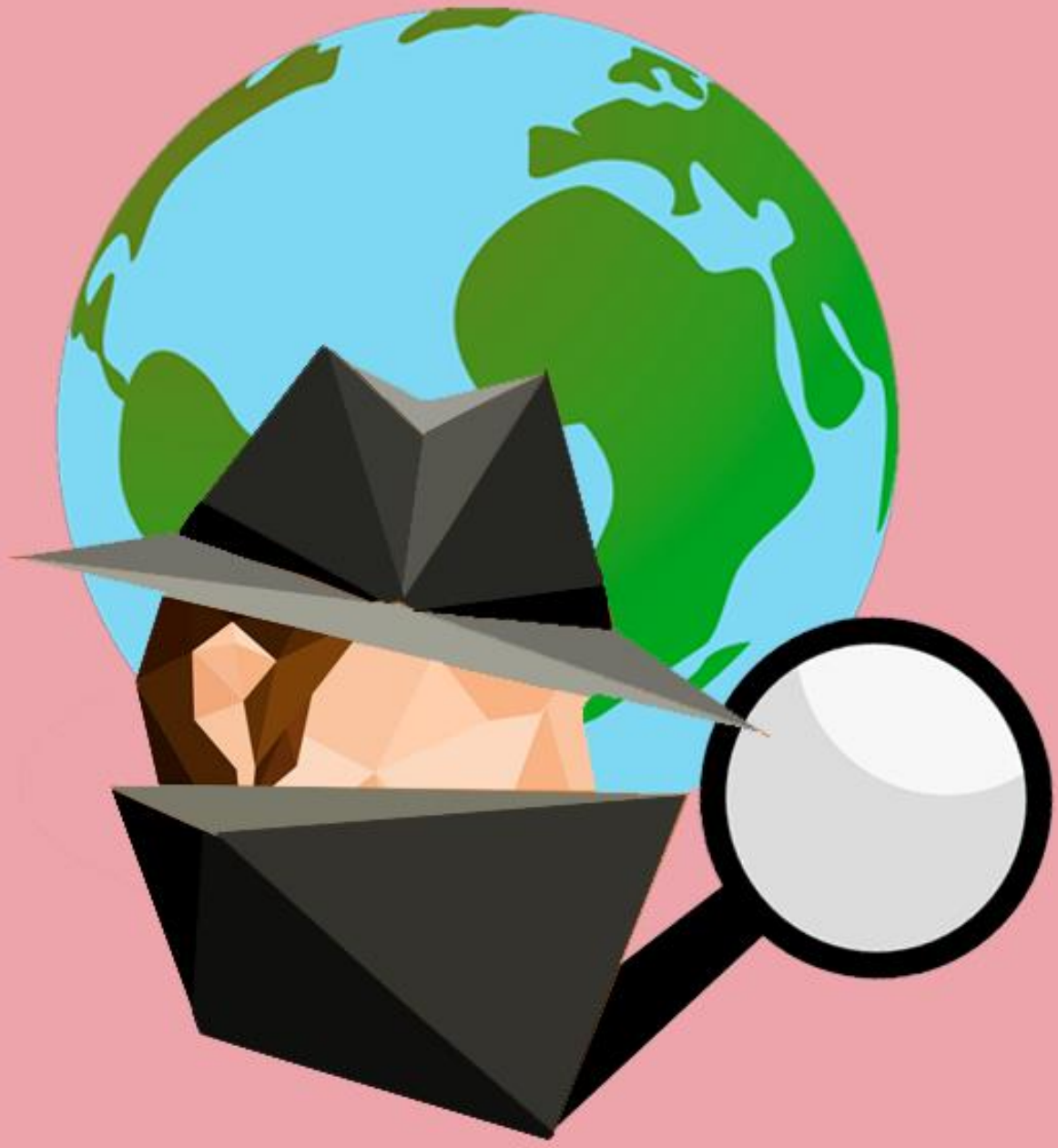
“A Operação Durkheim, deflagrada pela Polícia Federal na última semana, lançou luz mais uma vez sobre a venda indiscriminada de dados sigilosos no Brasil. A quadrilha tinha braços em variados setores e faziam parte dela policiais, funcionários de bancos e empresas telefônicas.” (HAGE, Kamila 2012).

Acima podemos verificar que aqui no Brasil não é de hoje que sabemos de caso abertos de Espionagem, não só somos espionados por outros países quanto por empresas que detém nossos dados. A nova legislação aprovada em 2018 LGPD (Lei Geral de Proteção de Dados do Brasil) vem para regulamentar como os dados serão armazenados e qual será a política sobre eles. Até ano passado o Brasil não contava com uma legislação que os regulamentasse.

“Em 31 de julho, o "Guardian" publicou nova reportagem, mostrando que um sistema de vigilância secreto conhecido como XKeyscore permite à inteligência dos EUA supervisionar "quase tudo o que um usuário típico faz na Internet". O sistema seria o de maior amplitude operado pela agência nacional de segurança americana.” (G1, 2013)

Com nossos dados disponíveis em diversos aplicativos, além de todas as permições de acesso ao nossos dispositivos que concedemos às empresas, precisamos prestar atenção cada vez mais o que estamos fazendo com nossos dados, aonde estamos colocando esses dados e se realmente precisamos informar cada detalhe da nossa vida na internet.

Precisamos saber ponderar e medir como podemos lidar com esse mundo 100% conectado sem que nos prejudiquemos tanto.



Capítulo 2

Política de Segurança da Informação

Política de Segurança da Informação

Um documento de Política de Segurança da Informação (PSI) é o conjunto de ações obrigatórias que devem ser tomadas para garantir a confidencialidade, integridade e disponibilidade da Informação. Sem uma PSI, quaisquer controles de segurança da informação seriam avulsos, sem integração ou gestão abrangente, e obviamente com um custo financeiro muito maior.

Considerando a informação como principal ativo de uma organização, não ter padrões e controles para a proteção destes ativos significa que o nível de segurança da informação nunca poderá ser mensurado, e o que não pode ser medido, não pode ser gerenciado!

Uma PSI é regulamentada pela ISO 27001, e quando bem elaborada, deve ser dividida em 2 partes distintas: o que deve ser feito (Políticas) e como deve ser feito (Procedimentos), e muitas das vezes por falta de clareza nos procedimentos, uma PSI acaba por ser mal implementada e gera uma perda significante de sua importância. Outro fator determinante e que comprova a importância de uma PSI é a necessidade de conformidade. Em certos casos em que a Alta Direção de uma organização não tenha a percepção devida de importância de uma PSI, os Órgãos Reguladores desta empresa, por força de garantia de conformidade, garantem que a PSI tenha sua importância (re)estabelecida.

Uma outra questão que não pode ser esquecida é que uma PSI também é um comprovante público de compromisso da organização com a manutenção de elevados padrões de segurança da informação, o que acaba por refletir na percepção de valor para a "marca" da empresa.

A importância de uma PSI precisa estar primeiramente clara para a Alta Direção. Se o time responsável pela criação e implementação da PSI não tiver capital político com a Alta Direção, a PSI será apenas "mais um documento".

Elaboração

Antes de começar a escrever os elementos que devem fazer parte da sua PSI, é importante que se faça um diagnóstico inicial da organização, identificando todos os ativos de Informação juntamente com possíveis ameaças ou vulnerabilidades. A partir daí, é possível especificar quais ativos de informação (pessoas, processos e tecnologias) precisam de controles específicos de segurança, baseado nos riscos aos quais estão expostos, por exemplo: Política de Senhas, Política de Backup, Política de Mesa Limpa, etc...

Vale salientar que para uma boa e eficaz PSI, o mais importante não é o quanto se escreve mas COMO se escreve. É imperioso ser o mais objetivo na construção de um documento que na prática será lido por alguém que nem sempre terá tempo ou boa vontade para "entender" o que deve fazer. Simplicidade e clareza são fundamentais para uma PSI que gere resultados consistentes.

Um outro fator tão importante quanto o anterior, é garantir que a PSI esteja alinhada com os objetivos do negócio. Não adianta criar uma PSI "imbatível" se ela engessar as operações comerciais da organização, o que pode ir de encontro as metas de crescimento financeiro da empresa. Uma PSI será tão efetiva quanto conseguir garantir o equilíbrio entre Controle x Operação. Se ao elaborar uma PSI isto não for observado, e a implementação da mesma significar tornar mais rígidos alguns processos críticos de negócio, ou mesmo tornar muito ruim a experiência do usuário, os controles previstos na PSI dificilmente serão postos em prática.

O alinhamento com o negócio precisa garantir uma boa experiência do usuário, o que consecutivamente irá garantir taxas elevadas de adesão à PSI. O profissional de Segurança da Informação precisa garantir a proteção das informações o mesmo tempo o mínimo de gargalos na operação, mantendo o equilíbrio entre a Proteção x Usabilidade.

Implementação

Tão logo a PSI seja aprovada pelo RH e demais líderes e gestores, e homologada como documento oficial da organização, é hora de cumprir e fazer cumprir os controles descritos na PSI, e é aí que começam muitos dos problemas...

Não adianta nada uma organização ter uma série de controles descritos em um documento, se estes controles não forem postos em prática; e eles não serão postos em prática se as pessoas responsáveis por tal não o fizerem.

Não adianta pensar que a PSI ficou pronta e foi disponibilizada que automaticamente as pessoas irão fazer o que lhes é devido de acordo com o documento. Para garantir que pessoas se comprometam com a PSI e cumpram suas tarefas designadas no documento, é necessário "criar consciência".

No dia-a-dia fazemos aquilo que já adotamos como rotina, e se nada for feito para que os controles de segurança passem a fazer parte da rotina diária de trabalho de um colaborador, a PSI será inócua.

Tanto profissionais de TI quanto usuários de TI terão mudanças nas suas atividades diárias oriundas da PSI, e isso precisará de reuniões, palestras, seminários de conscientização.

Como forma de medir o cumprimento da PSI, indicadores poderão ser criados e ações periódicas de verificação de cumprimento da PSI irão ajudar a definir estratégias de reforço na conscientização das áreas ou profissionais com baixa adesão à PSI.

Uma etapa quase sempre ignorada pelas organizações que implementam uma PSI, e a criação de um cronograma periódico de revisão do documento. Vivemos um momento ímpar de surgimento de tecnologias evolutivas, e uma PSI deve contemplar controles para cada nova tecnologia adotada pela organização.

Capítulo 3

Riscos

O que são riscos?

O risco é a exploração de uma ou mais vulnerabilidades, gerando um impacto negativo nos recursos afetados, na imagem na empresa, nas atividades da organização. Afetando, dessa forma, um ou mais pilares da Segurança da Informação: confidencialidade, disponibilidade, integridade e autenticidade.

É impossível uma organização prever todos os ataques. Dessa forma, é preciso analisar quais são os potenciais riscos, e estar preparado através de tecnologias atualizadas e pessoas capacitadas por meio de detecção e prevenção, procurando sempre mitigar o risco.

Algumas formas de medir os potenciais dos riscos são:

- O grau de vulnerabilidade existente;
- A probabilidade da ocorrência de um incidente de segurança (concretização de uma ameaça);
- O impacto resultante do mesmo.

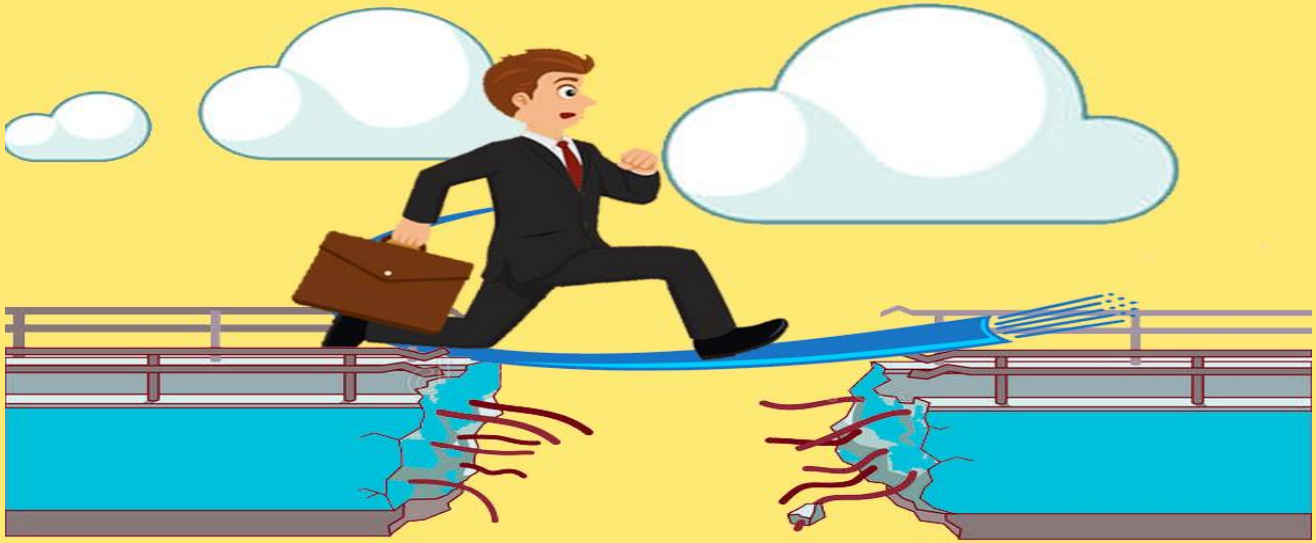
O maior problema do risco é que quando explorado pode causar danos irreparáveis à organização, sejam eles: financeiros, danos à imagem, sobre a continuidade do negócio.

De uns tempos para cá, a maneira de se fazer negócio foi totalmente alterada pelos avanços tecnológicos. E, se houve avanço, vieram com ele vários riscos e desafios. A conexão existente entre todos os nossos dispositivos e os inúmeros processos envolvidos, dificulta ainda mais esta tarefa. Diante deste cenário é necessário se proteger com novos controles além do cumprimento de exigências regulatórias.

É baseado neste aspecto que falamos sobre Controles Internos. CI, nada mais é que estabelecer medidas, procedimentos ou rotinas com o objetivo de proteger os ativos mais críticos da Organização. Infelizmente, muitas empresas não possuem políticas adequadas, matriz de riscos desenhada e implementada e muito menos processos de auditoria interna e externa. Para entendermos melhor esta definição é importante compreender o significado destes termos a seguir:

Definições

- Políticas: é a forma mais simples e completa de se conduzir uma Organização. São documentos que são estabelecidos e aprovados pela alta direção com o objetivo de se alcançar conformidade em seus processos e atividades.
- Matriz de Riscos: é a formalização e documentação de tudo o que representa prejuízo à Organização em caso de perda e/ou indisponibilidade. São riscos identificados com as devidas remediações/mitigações para causar menor impacto possível em processos críticos
- Auditoria: é uma averiguação detalhada de todas os processos críticos de uma Organização, com o objetivo de examinar se os mesmos estão de acordo com as políticas apresentadas e/ou regulamentações exigidas. Pode ser apresentada de forma Interna, quando a própria Organização averigua ela mesma e também de forma Externa, quando a Organização é auditada por uma outra empresa competente que demonstra o resultado para órgãos competentes.



Controles internos

É importante salientar que o risco envolvido sem o estabelecimento de controles pode acarretar em sérios prejuízos à Organização.

Algumas informações importantes para atuação em Controles Internos:

- Mantenha todas as políticas atualizadas e divulgadas;
- Estabeleça métodos e métricas para mensurar a efetividade dos controles;
- Tenha sempre um processo de auditoria ativo na Organização;
- Revise os processos periodicamente;
- Mantenha todas as políticas atualizadas e divulgadas;
- Estabeleça métodos e métricas para mensurar a efetividade dos controles;
- Tenha sempre um processo de auditoria ativo na Organização;
- Revise os processos periodicamente.

> "Sem políticas, matriz de riscos bem definida e um processo de auditoria, fica muito complexo de se fazer um trabalho satisfatório de monitoramento e Controles Internos.."
>
> Rodarte, Bruno

Capítulo 4

Vulnerabilidades

Vulnerabilidades

Quando falamos sobre vulnerabilidades, um dos primeiros itens que nos vem à mente são vulnerabilidades conhecidas, de sistemas, infraestrutura e quase tudo relacionado ao ambiente computacional. É basicamente um servidor que não tem o último patch de correção instalado, é o antivírus desatualizado, sistema operacional sem suporte, etc. Porém, o tema vai um pouco mais além...

Para esclarecer um pouco, vamos fazer uma ilustração e uma comparação com a construção de uma casa.

Imagine que o terreno ainda está vazio e você precisa planejar e arquitetar a sua nova casa. Você contrata o melhor arquiteto e engenheiro e estabelece uma premissa importante: uma casa segura, fortificada.

Neste projeto, arquitetos e engenheiros trabalham juntos e lhe apresentam o que há de melhor nos requisitos de segurança física para sua nova casa: fechadura de vários segredos com biometria, câmeras instaladas e configuradas para visualização remota, leitura de íris, cercas elétricas de última geração, portas blindadas, etc. O projeto fica caro, mas você acena positivamente.

Aliás, você está seguro, com tantos aparatos trabalhando em conjunto. Você aprova o projeto e conclui a construção de sua nova moradia. Casa pronta, vida nova, segurança total... porém, um detalhe importante, passou desapercebido. Um belo dia, o interfone de sua nova casa toca e uma pessoa se identifica como técnico de uma operadora de TV a cabo conhecida e diz que precisa realizar uma manutenção em seu equipamento. Como sua empregada doméstica não foi informada que esse tipo de golpe poderia acontecer, ela simplesmente aperta o botão do interfone, permitindo a entrada do falso técnico. Portas e portões se abrem e o atacante leva seus pertences, sem deixar nenhum rastro de arrombamento.

Uma vulnerabilidade é tudo aquilo que compromete a segurança de qualquer ativo ou recurso, seja ele computacional ou pessoal. Uma brecha, uma fraqueza que quando explorada pode resultar em significativos problemas à Organização e às pessoas.

Vulnerabilidades

Vale o reforço que um trabalho consciente junto às pessoas é essencial ao ambiente.

O elo mais fraco, mais vulnerável, quando tratamos de segurança da informação, ainda continua sendo as pessoas e se elas são vulneráveis, o ambiente é vulnerável, independente da tecnologia implementada.

Algumas medidas práticas para manter o ambiente menos vulnerável:

- Manter sempre seu parque computacional atualizado;
- Promova programas de conscientização de usuários, a fim de evitar ataques de engenharia social e evitar vazamento de informações;
- Faça um código com qualidade. Revise-o sempre que necessário;
- Tenha uma gestão de identidades e controle de ciclo de vida do usuário em seu ambiente. Um usuário desligado nunca deve permanecer ativo em seus acessos;
- Faça uma revisão periódica dos perfis de acesso e se possível, estabeleça o conceito de segregação de funções.

Capítulo 5

Conscientização

Conscientização e Treinamento

A segurança da informação tem por objetivo garantir a confiabilidade entre os processos, as tecnologias e os humanos, através dos principais pilares que são a confidencialidade, Integridade, disponibilidade, não repúdio e autenticidade. Para que o nível de conscientização possa se elevar segundo uma estratégia bem definida, é fundamental compreender dois princípios de aprendizagem: a conscientização e o treinamento.

Um fator determinante que chamamos de "o elo mais fraco", ainda é o fator humano, o qual precisa ser conscientizado e treinado adequadamente para entender as ameaças que os cercam, pois elas não estão presentes somente no perímetro organizacional, mas em todos os ambientes frequentados. É necessário que se esteja apto a se esquivar delas de forma consciente.

O motivo para treinar e conscientizar com frequência é devido a evolução das ameaças em passos largos. Sabemos bem que muitas dessas ameaças são intangíveis, apesar disso, a ameaça interna é a maior preocupação dos profissionais de TI, administradores de redes e/ou sistemas, que são os responsáveis pela tecnologia da informação no ambiente organizacional, ou seja, de fato são os responsáveis pela segurança das informações.

A conscientização tem como foco a segurança, objetivando através de temáticas disseminar a Segurança da Informação no ambiente organizacional, conforme os valores da estratégia citados no documento apresentado pelo Gabinete de Segurança Institucional da Presidência da República intitulado como Estratégia de Segurança da Informação e comunicações e de segurança cibernética da administração pública federal, um dos principais valores é a disseminação da cultura de SIC (Segurança da Informação e Comunicações) e de SegCiber (Segurança Cibernética): “promover o comprometimento da sociedade com os valores, visões, boas práticas, símbolos, hábitos, comportamentos e políticas, relativas à segurança da informação e comunicações e à segurança cibernética.“

A Importância da Educação

A educação é essencial para a sociedade, quando o assunto é educação em Segurança da Informação, conforme artigo redigido por Guilherme Teles para o site TI Especialistas, ao final, Teles conclui que a educação é uma maneira econômica de atingir pelo menos o mínimo de segurança.

Nelson Barbosa, especialista em segurança da Norton, diz que "A maioria dos brasileiros se sente muito confiante em relação à segurança virtual. Eles acreditam que não serão vítimas de um crime virtual e não adotam medidas proativas de segurança, mesmo sabendo que são necessárias."

Cláudio Martinelli, diretor geral da Kaspersky Lab no Brasil, afirma que as empresas precisam implementar três fatores para garantir a segurança:

- Treinamento e capacitação dos funcionários;
- Políticas de Segurança que indiquem sites que podem ou não ser acessados;
- Ferramentas que ajudem a barrar malwares.

Ainda segundo Martinelli, "é importante saber que, se não existir treinamento e politica de segurança, não adianta investir valores altos em ferramentas. E é preciso treinar funcionários além da sala de TI, pois esse é o departamento menos afetado por cibercriminosos. A minha dica é: treine urgentemente os funcionários de recursos humanos".

Convém que todos os funcionários da organização e, onde pertinente, partes externas recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.

ABNT NBR ISO/IEC 27002:2013

Na prática

Temas a serem levantados:

- Segurança da Informação;
- Mesa e Tela limpa;
- Senhas;
- Navegação na Internet;
- E-mails (Phishing, SpearPhishing, spam entre outros);
- Aplicativos de Mensageria;
- Vírus;
- Malware;
- Mecanismos;
- Normas, Padrões e Políticas de Segurança.

Boas Práticas

Este tópico apresenta boas práticas para a implementação de Programas de Conscientização em Segurança baseando-se na norma ISO/IEC 27002:2013. É responsabilidade dos diretores e/ou gestores solicitar a todos os funcionários e partes externas, como clientes, fornecedores e equipes terceirizadas que pratiquem a segurança da informação, de acordo com o estabelecido nas políticas e procedimentos da organização.

É recomendado que a direção demonstre seu apoio às políticas, procedimentos e controles e aja de forma exemplar.

Na prática

Planejamento

Deve ser desenvolvido um programa continuo e completo de conscientização e treinamento em segurança da informação. Para que seja transmitido de forma confortável aos envolvidos, os princípios, as considerações, conceitos, técnicas e as tecnologias de segurança da informação devem ser entregues de forma metódica e em um ritmo adequado.

O clico de vida da conscientização e treinamento é um processo continuo e deve ser atualizado e avaliado com frequência.

Campanhas

A campanha serve para integração das áreas, em grandes empresas são feitas através de folhetos, convites de E-mail, fatos reais, FAQ, boletim de notícias, Pôster, PowerPoint e Referencias Rápidas. Uma forma inovadora para a disseminação de dicas de segurança da informação em prédios, é a utilização de monitores de informações, conhecidos como Display de Propaganda.

Apresentações

As apresentações comumente são geradas em arquivos de apresentações do PowerPoint, mas nada impede de se utilizar outras ferramentas e formas diversificadas de apresentações.

A didática é muito importante na apresentação e uma melhor elaboração do conteúdo, existem diferentes formas que as pessoas assimilam as informações, os tipos mais comuns são os visuais, auditivos, cinestésicos e leitura/escrita. Conheça as suas principais características:

- Visuais: Interpretação de gráficos ou mapas, artigos ou qualquer coisa que mostre um processo; (Memoria fotográfica);
- Auditivos: Responder questões sobre a aula expositiva ou palestra; Provas orais; (Gravadores humanos);
- Cinestésicos: Definições, curtas questões de completar e múltipla escolha; (Mão na massa).

Muito mais do que uma senha segura

A Importância da Educação

Treinamento

Concentra-se nas habilidades de ensino, permitindo que os profissionais atuem em funções especificas.

O treinamento é importante, pois prepara os funcionários para se defenderem, se esquivarem de ameaças. Assim como nas artes marciais, o perigo invisível está a porta e não podemos ver, mas uma forma de nos anteciparmos é através do treinamento e não só aprendermos como se defender e com quais armas, mas também entender como o inimigo ataca, sua linha de pensamento e quais meios utiliza.

Conscientização

A conscientização direciona a atenção de um profissional para uma questão ou série de problemas específicos.

A Conscientização tem como objetivo principal preparar a mente das pessoas para que estejam prontas para as situações em que estarão expostas. Alinhando o pensamento humano com práticas de defesa e antecipação para que se apliquem em conformidade com as normas e políticas estabelecidas pela organização em que atua.

Questionários

Forma de avaliação do conhecimento em segurança da informação, fornecendo um relatório completo que apresenta uma análise dos resultados, possibilitando a comparação das pontuações com a média existente, além de possibilitar a visualização das explicações sobre todos os termos e tópicos de cada questão.

Disciplina

Um processo disciplinar formal deve existir para tomar ações contra funcionários que tenham cometido uma violação de segurança da informação. Assim como no mundo real onde os infratores recebem punições por suas práticas ilícitas no mundo virtual controlado também é necessário agir com severidade com objetivo de garantir a ordem.

Capítulo 6

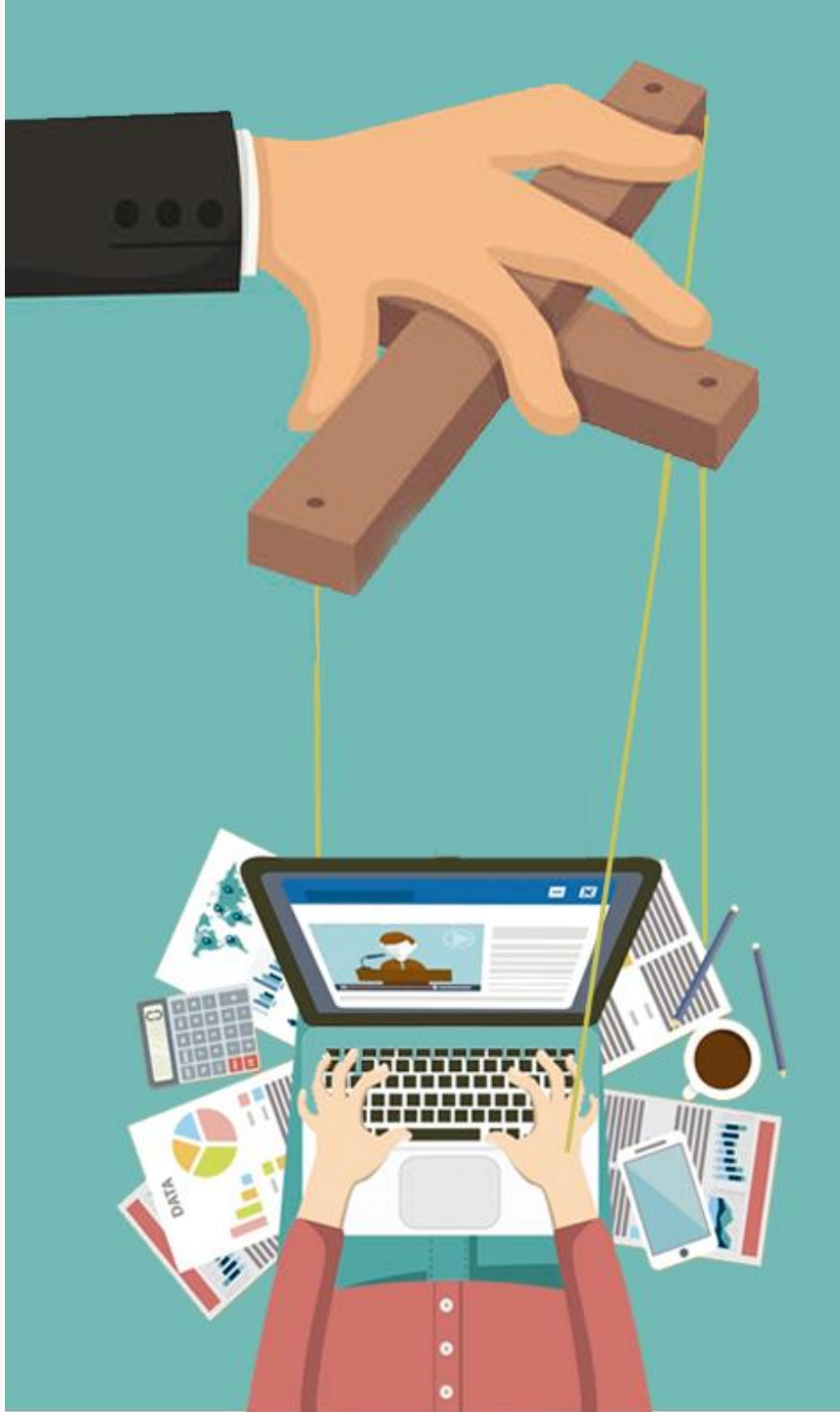
Engenharia Social

Engenharia Social

"Engenharia social é o ato de influenciar uma pessoa a tomar uma ação que pode ou não ser de seu interesse." Hadnagy (2011)

Nós praticamos engenharia social no nosso dia-a-dia com nossos parentes, filhos, cônjuges. Por exemplo, quando desconfiamos de uma informação que nosso filho nos falou, e podemos através de um colega dele realizar uma ligação para descobrir a verdade. Isso é engenharia social. Utilizar-se da manipulação psicológica com o objetivo de através da credibilidade ganhar acesso às informações confidenciais ou até mesmo espaços confidenciais.

Similarmente, no conceito que é mais difundido em Segurança da Informação, temos casos como o acima, porém com intenções realmente maliciosas. Veja uma história para que possamos exemplificar o conceito:



Engenharia Social: Sr. Roberto

Sr. Roberto Tavares é CEO de uma empresa multinacional, um profissional extremamente requisitado para reuniões. Sua secretária, Sra. Maria Julia, recém-contratada, não recebeu todos os treinamentos devidos de Segurança da Informação. Em seu segundo dia de trabalho ela atende uma ligação que acreditava ser do Sr. Roberto. O atacante, se passando pelo CEO, pede para que ela rapidamente lhe envie uma senha de acesso a uma pasta informando que está com uma emergência fora do país. Logo após, Sra. Maria Laura rapidamente aciona o departamento de TI solicitando a senha.

O suposto Sr. Roberto informou que precisava da informação em e-mail pessoal pois não conseguia acessar o e-mail corporativo de onde estava, e informou o seguinte e-mail: roberto-taveres2015@.... Na cabeça de sua secretária, tudo estava certo, o Sr. Roberto Tavares realmente estava fora do país, ele realmente não tinha respondido aos seus e-mails o que podia ser um indicativo desta emergência e o e-mail pessoal era extremamente parecido com o original. Assim, a senha foi enviada para o "e-mail pessoal".

Dias depois, para sua surpresa, ao retornar para o escritório, o Sr. Roberto Tavares teve todas as suas planilhas apagadas e todos seus arquivos substituídos por informações de como transferir dinheiro via Bitcoins para conseguir recuperar suas informações.

Ao final, a empresa estabeleceu políticas severas de conscientização dos usuários para evitar casos como este e conseguiram por conta de um backup atualizado recuperar as informações.

Tivemos na história acima um final feliz, não são todos os casos em que podemos contar com isso.

Engenharia Social: Sr. Roberto

Uma situação com essa envolve riscos muito grandes para a empresa, tais como:

1 – Disponibilidade: não conseguir acessar os arquivos.

2 – Reputação: uma empresa que tem dados vazados tem um risco muito alto de ter sua reputação extremamente prejudicada para seus fornecedores, funcionários e principalmente com os seus clientes.

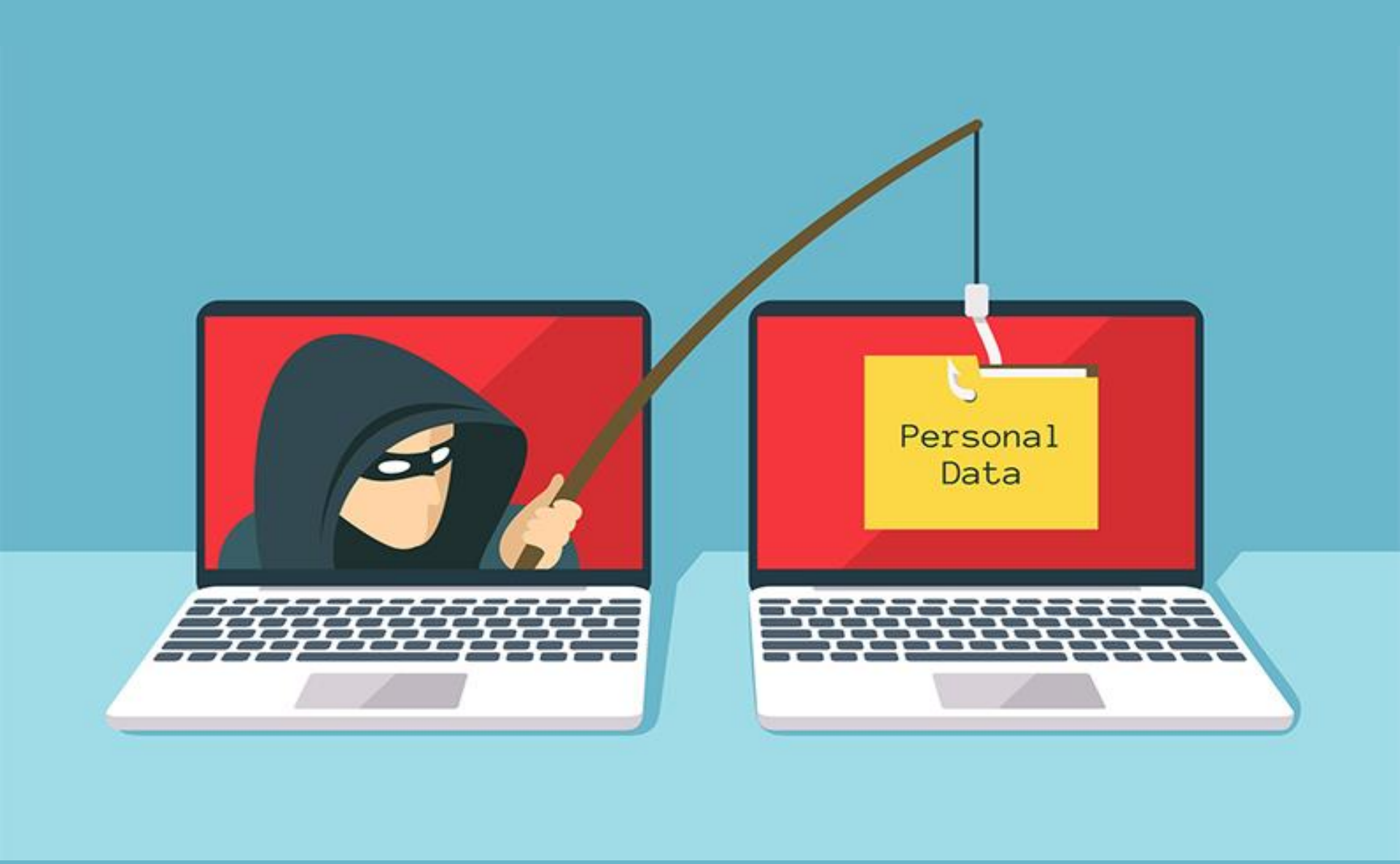
3 – Perdas financeiras: o ataque pode resultar em grandes perdas financeiras ou de recursos, pode causar danos significativos à organização, o que impede que ela cumpra algumas tarefas com clientes, e resulta em perda de interesse e até em casos mais graves envolvem a vida de pessoas.

4 – Confidencialidade: faz parte do pilar de Segurança da informação assim como a integridade e disponibilidade. Um vazamento de dados pode incorrer em processos judiciais por ferir contratos e legislações sobre confidencialidade.

Segundo relatório da Akamai em 2017, o Brasil é o segundo maior alvo de ataques na web. Sabendo disso, precisamos disseminar muito mais o conhecimento sobre Segurança da Informação.

Empresas gastam muito dinheiro nas melhores tecnologias para evitar malwares, entre outros ataques, possuem os melhores firewalls, proxys, sistemas de biometria para acesso às salas restritas. Porém, pecam no primordial: no treinamento para seus funcionários.

Portanto, cabe aos profissionais de Segurança e TI em geral alertar, orientar para que sejam feitos treinamentos e campanhas constantes de conscientização a fim de mitigar esses riscos.



Muito mais do que uma senha segura

Fonte: https://www.defcon-lab.org.
Edit: Amanda Balzano

Capítulo 7

Monitoração

Monitoração

Começamos esse capítulo fazendo uma pergunta. Há meios de responder a qualquer estímulo que ainda não foi detectado? Bem, um programa de monitoramento contínuo de segurança da informação é de difícil implementação, mas quando bem estruturado tira a sua empresa da obscuridade, trazendo às claras as ameaças e as vulnerabilidades que até então estavam encobertas. Voltando a pergunta inicial, é prudente responder que não!

O programa de monitoramento de segurança contínuo lhe trás uma consciência permanente sobre as ameaças e as vulnerabilidades e lhe fornece insumos para tomada de decisão do gerenciamento do risco organizacional. Sintetizando, lhe permite avaliar e reavaliar sua postura de segurança. Desta maneira, é possível afirmar que o monitoramento de segurança é o coração da resposta a incidente.

Partindo de um princípio: monitoração

O sucesso da monitoração de segurança está diretamente ligado aos aspectos de negócios. O capítulo 4, contexto da Organização, da ISO 27001, documento referência para construção de um sistema de gestão de segurança da informação, diz que a organização deve determinar as questões internas e externas que são relevantes para o seu propósito e que afetam sua capacidade para alcançar os resultados pretendidos do seu sistema de gestão da segurança da informação.

A ISO 27002, código de práticas para controles de segurança, diz no capítulo 0.2, requisitos de segurança da informação, que é essencial que a organização identifique os seus requisitos de segurança e descreve três fontes principais como mostra o resumo abaixo:

- Avaliação de risco organizacional: levando em conta os objetivos e estratégias globais;
- A legislação vigente: levando em consideração a regulamentação e cláusula contratual, e;
- Conjuntos particulares de princípios: considerando os requisitos e objetivos de negócio para manuseio, processamento, armazenamento.

Os dois documentos citados nesse capítulo fazem, nas entrelinhas, menção a negócio. Juntando as referências das duas ISOS é possível criar uma pequena estrutura de pensamento para iniciar qualquer processo de monitoramento de segurança: "Os seus requisitos de segurança devem estar conectados com as questões internas e externas relevantes para o propósito do seu negócio."

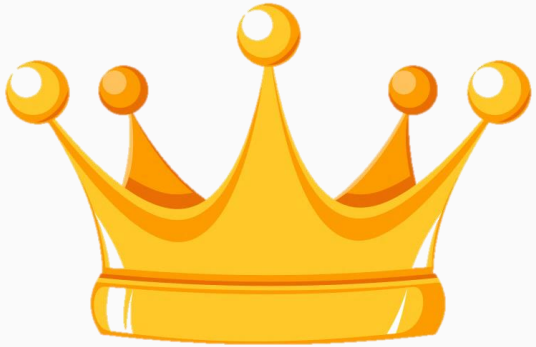
Para elucidar o raciocínio citado acima, imagine que você possui um site que ofereça produtos diversos em que os clientes realizam pedidos e você precisa identificar algum requisito de segurança associado ao tema monitoramento de segurança. Bem, você precisará implementar um processo para monitorar e agir quando for detectado uma indisponibilidade. Perceba que isso é um requisito de segurança para o seu negócio: gestão de indisponibilidade. Disponibilidade está dentro do conjunto de princípios particulares proposto pela ISO.

As Joias da Rainha

As joias da Rainha é um termo interessante que pode ser usado para construção de um processo de observação de comportamento, afinal uma Rainha desperta a atenção de muitos com o simples ato ao alçar uma coroa de sua cabeça.

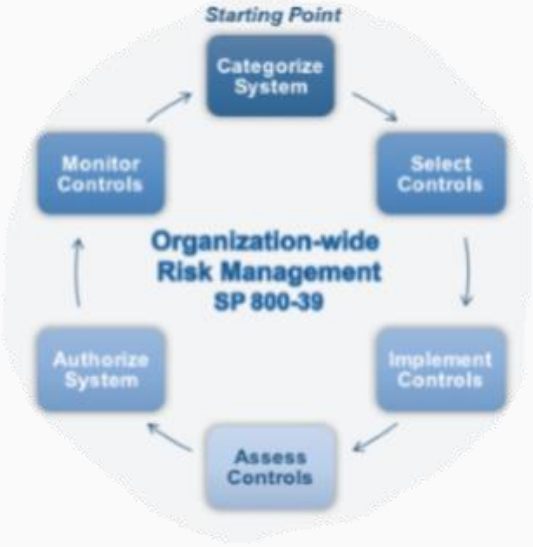
Um programa monitoramento de segurança é um processo em que os seus resultados não pode ser fruto do acaso. Pelo contrário, o monitoramento deve ser implementado para aumentar o nível de segurança de modo que traga resultado satisfatório no combate as constantes ameaças. Mas para alcançar esse nível pretendido, até pode-se monitorar todo ambiente, mas o foco deve estar direcionado a observar as joias da Rainha.

As joias da Rainha é a representação de ativos que realmente representa valor para Organização. Fazendo uma incursão no capitulo anterior, é aquilo que é relevante para o seu propósito. Como veremos em seguida.



A categorização

As organizações possuem muitos ativos, mas nem tudo representa a mesma importância, por isso faz-se necessário um processo de categorização no qual os ativos são diferenciados pelo seu valor, impacto e perdas financeiras. Esse processo facilita diferenciar o importante do essencial e, quando implementado, trás um importante insumo para o programado de monitoramento. O documento Risk-Management-Framework do Nist possui uma referência que nos auxilia nesse processo de categorização e, no que se refere ao monitoramento, sugere que ele seja a ultima etapa do processo de gerenciamento de risco.



Fonte: https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-(RMF)-Overview

Eventos de Segurança

No inicio desse capítulo foi feita uma pergunta muito apropriada para essa parte: Há meios de responder a qualquer estímulo que ainda não foi detectado? Bem, era disso que eu estava me referindo, eventos. Sem eventos, não há o que se monitorar. Há duas importantes referências que nos auxiliam a validar esse controle, a produção de eventos é muito importante para segurança.

A primeira fonte refere-se aos logs e diz que são registros de eventos ocorridos em sistemas ou redes dentro de uma organização. Esses registros são compostos de entradas e cada uma destas entradas contém informações relacionadas a um evento específico. Muitos destes registros estão relacionados com a segurança do ambiente- NIST 800-92. Em complemento temos o capítulo 12.4, Registro e Monitoramento da ISO 27002:2013, que diz que os registros de eventos estabelecem o fundamento para os sistemas de monitoramento automatizados, os quais são capazes de gerar relatórios consolidados e alertas na segurança do sistema. Fechado!

Não há muito mais o que dizer, somente ratificar que o monitoramento é um controle de segurança que depende da produção de eventos, que é um outro controle de segurança. A produção de eventos lhe habilitar a identificar os estímulos que você precisa identificar e alertar. A equipe de resposta a incidente de segurança terá um recurso de valor para mitigação rápida de um ataque.

Modelo de Monitoração

O modelo de segurança organizacional é uma estrutura composta por camadas. Uma camada fornece suporte para camada de cima e proteção para camada de baixo. Por exemplo, um NAC (Network Access control), controla quem tem permissão de acessar a rede fazendo o controle de camada 2, MAC, de modo que se a ferramenta não liberar, uma estação nem consegue autenticar no domínio, camada 7, aplicação. Isto é, a estação é bloqueada antes de interagir com o servidor e ao menos consegue validar se um usuário legítimo. Por sua vez, um Firewall de rede, já possuem regras que permitem o tráfego entre a estação e os servidores, sendo assim, o processo de identificação, validação e autenticação do usuário acontece porque o controle de rede permite a comunicação entre a estação e o servidor.

O Firewall de rede analisa e controla tráfego e não se preocupa se a estação conectada no Switch já foi identificada/legitimada porque o NAC já lhe oferece esse suporte. Por sua vez, se o controle físico falhar e alguém conectar uma máquina em uma porta vaga de Switch, a mesma não ingressará na rede porque não foi autorizada pelo NAC. Bem, isso é um exemplo de camada que fornece suporte para camada de cima e proteção para camada de baixo e essa é uma estratégia de segurança utilizada em larga escala.

Procurei construir um raciocínio técnico para elucidar como um modelo pode trazer benefícios para a monitoração de segurança. A adoção de uma modelo lhe ajuda a eliminar boa parte da sua própria responsabilidade, pois você está seguindo uma referência técnica de alto nível e não apenas suas convicções, o modelo também lhe auxilia a identificar e corrigir falhas no processo em questão. A implementação de um programa de monitoramento de segurança contínuo eficaz, também requer uma modelo estratégico capaz de nos assessorar para construção de controles focados na essência do negócio. Esse modelo precisa ser capaz de prover uma assistência no âmbito gerencial e não técnico. O NIST 800-137 é uma excelente fonte para trilharmos uma estratégica para o emprego de um monitoramento conectado ao negócio. O documento reúne informações completas para se estabelecer um programa de monitoramento de segurança e serão abordadas as três camadas proposta pela referência.

A três camadas são respectivamente Organizacional, Processo de Negócio e Sistema de Informação. A primeira camada encontra-se à alta direção que Governa a Companhia como um todo, desta camada saem às políticas, gerenciamento de risco, estratégias etc. A camada Processo de Negócios é a engrenagem que fatia os principais processos e distribui as funções em diversas outras áreas. E a camada Sistema de Informações é responsável por receber, processar, manipular, armazenar e transferir informações. Cada uma dessas camadas tem questões de segurança que precisa ser monitoradas, validadas e reportadas. Esse modelo estabelece conexões importantes entre si e facilidade a criação de um programa de monitoramento com foco no que realmente interessa.

Processo

Ao se compreender as conexões entre as camadas e identificar os gatilhos do que precisa ser observado, identificado e reportado, é preciso definir o escopo para que o programa de monitoramento traga resultados eficazes. O NIST 800-137 também oferece esse recurso em 6 itens que resumidamente serão abordados a seguir.

1. Definir: Definição de uma estratégia de tolerância ao risco com uma clara visão das vulnerabilidades;
2. Estabelecer: Estabelecer métricas e avaliação frequente dos controles;
3. Implementar: Implementar coletas relacionadas a segurança do ambiente necessárias para as métricas;
4. Analisar: Analisar os dados coletados e reportar os resultados;
5. Responder: Responder as vulnerabilidades encontradas com controles técnicos;
6. Atualiza e revisar: Revisar e atualizar o programa do monitoramento para a constante aderência a estratégia.

Ferramenta

Security Information and Event Management (SIEM), é uma ferramenta capaz de concentrar e correlacionar eventos de segurança de diversos dispositivos como, por exemplo, Antivírus, Filtro de Conteúdo Web, Firewall, IPS, Active Directory etc. Por exemplo, temos um indício de comprometimento de credencial se um usuário que autenticou na rede, não passou pela catraca e não possui acesso a VPN. Outro exemplo é se um usuário normal tem seu privilégio escalado para Domain Admin a ferramenta é capaz de observar e lhe alertar. Caso, uma regra de firewall que protege um ativo crítico foi alterada às três horas da manha, fora do intervalo especificado e sem rodar o processo de gestão de mudança, a ferramenta é capaz de observar e enviar um alerta sobre esse incidente de segurança com detalhes sobre o incidente. Para terminar, um cliente de Antivírus foi desabilitado de um servidor crítico, a ferramenta poderá observar esse comportamento e enviar alertas.

Sobre a VPN, o SIEM é capaz de automatizar o cruzamento dessas três informações e lhe entregar um indicador de comprometimento para ser investigado. Os exemplos restantes demonstra a potencialidade da ferramenta, mas sem nenhum tipo de correlacionamento técnico, mas baseado e contexto, critério e regras.

O requisito para esse processo é que os eventos estejam sendo produzidas pelas aplicações e enviados ao SIEM, que concentrará os eventos brutos, normalizará para o padrão CEF (Common Event Format). Além de todo motor de correlacionamento, identificação e alertas, a ferramenta permite-nos observar os eventos de segurança olhando para um único ponto, eliminando o tempo gasto na coleta de informações.

Existem no mercado diversas ferramentas que se baseia no conceito SIEM. Caso não tenha condições de adquiri uma ferramenta de mercado, existem ferramentas Open Source que pode lhe ajudar lhe iniciar nesse programa sem investimentos dispendiosos.

Considerações: Monitoramento

Gaste um tempo planejando esse programa de monitoramento, não inverta as três camadas proposta pelo NIST, pois iniciando o processo pela camada de Sistema de Informações, dificilmente será capaz de alcançar os objetivos de negócios. Lembre-se que vem de cima os insumos para as camadas inferiores e, seguindo essas camadas, será possível trilhar o caminho para o gerenciamento do risco. Pode-se dizer que sem está conectado ao negócio, o programa será pouco vital e muito trivial. Defina também o escopo, o que serão coletados, as métricas, sabendo que a segurança deve abranger a empresa como um todo, mas o foco deverá ser nas joias da rainha.

Um programa de monitoramento contínuo de segurança lhe permite avaliar o comportamento da situação em tempo real, identificar os gaps de segurança e propor ações para implementar controles em conjuntos com as áreas responsáveis. Os controles são partes importantes do escopo do monitoramento, visto que uma coisa é a implementação de controles, porém a outra e validar sua permanência contínua. Controle de identidade, Antivírus, Firewall etc. devem ser observados no processo da monitoração de segurança.

Defina um limite aceitável para que determinados eventos aconteçam, afinal cinco erros de autenticação do mesmo usuário não quer dizer nada, mas se todos os dias, no mesmo horário, esse comportamento ocorrer, já pode indicar alguma coisa. Seguindo o exemplo de autenticação, esse tipo de controles podem ser desmembrados em limites diferentes, tipo em 5 erros em cinco segundo, 20 erros e 10 segundos e correlacionado entre si.

Por fim, o motor de correlacionamento de uma ferramenta de SIEM é muito escalável, mas a aplicação precisa ser customizada para observar aquilo que é importante. Não tente adivinhar o que é importante garimpando logs, deixe essa atividade para a equipe de resposta a incidente, visto que, se um incidente ocorreu e não foi possível detectar é porque a ferramenta não foi programada para observar esse estimulo. Deixa que o relatório do CSIRT tragam as informações sobre os modus operandi e então coloque uma nova inteligência na ferramenta. Faça incursões nas áreas, agende reunião para demonstrar o propósito do programa, envolva a alta administração.

Capítulo 8

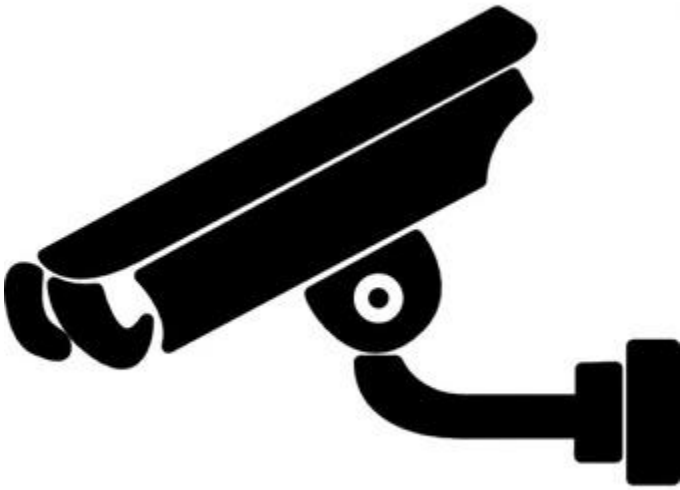
Segurança Física e do Ambiente

Segurança Física

A Segurança Física cuida da proteção dos ativos valiosos da organização. Seu escopo é extremamente abrangente, englobando todas as instalações físicas, internas e externas. Além disso, cuida da proteção de ativos importantes que estejam sendo transportados, como, por exemplo, as mídias de backup.

Ativos que devem ser protegidos:

- Data Center
- Computadores
- Mídias de backup
- Arquivos de documentos em papel
- Antenas de Comunicação
- Central Telefônica



Segurança Física

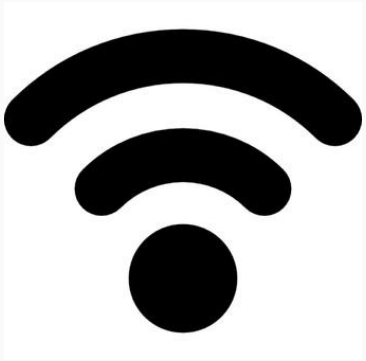
As dependências da empresa e o espaço físico onde se encontram os servidores e mídias de backups e documentos devem ser protegidos por controles físicos:

- Criar controle de acesso físico, identificação dos funcionários, terceiros e visitantes, preferencialmente com uso de crachás, catracas e portas de acesso por ambiente ou andar da companhia.
- Criar, preferencialmente, controle nominal de quem entrou e saiu do ambiente, seja acompanhado ou não por um funcionário.
- Utilizar mecanismos de controle de acesso físico em salas e áreas de acesso restrito (fechaduras eletrônicas, câmeras de vídeo, alarmes, CFTV, etc).
- Criar controles de condições ambientais adequados, tais como ar-condicionado e medidor de umidade temperatura para o CPD, ou espaço físico equivalente onde se encontram os servidores e mídias de backups, devem possuir.
- Criar controles contra falhas elétricas e falta de energia, preferencialmente suportados por no-break e geradores de energia, de acordo com as necessidades do negócio, para os principais equipamentos que suportam serviços críticos da companhia.
- Criar regras para portar equipamento pessoais dentro da empresa, como notebooks e aparelhos celulares, bem como controle na transferência de equipamentos dentro da empresa.
- Restringir, quando necessário, que funcionários e visitantes registre imagens e fotografias dos ambientes da empresa.
- Restringir uso e entrada de alimentos, líquidos e cigarros em ambientes da empresa.

Capítulo 9

Redes sem fio

Redes sem fio



As redes sem fio estão cada vez mais presentes no cotidiano das empresas, principalmente pela facilidade e comodidade. As pessoas conseguem acessar a rede corporativa de qualquer ponto com uma alta gama de dispositivos. Porém, como qualquer outra tecnologia existem pontos negativos, principalmente no que se diz respeito a segurança da informação.

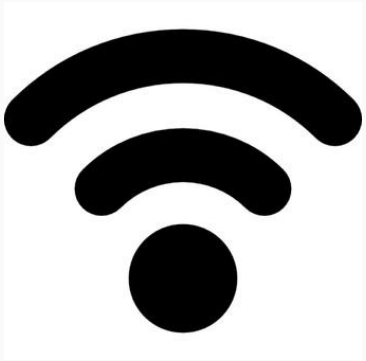
Um dos principais aspectos é a facilidade de se conectar em alguma rede disponível, porém o grande problema é que "qualquer" pessoa pode ter acesso a esta rede, sendo obstruída apenas por uma senha para conseguir a conexão à rede em questão, por isso é necessário um cuidado maior para com esse tipo de conexão. Algumas práticas são simples de serem efetuadas e garantem uma maior proteção para sua rede WI-FI, seja ela corporativa ou residencial.

A seguir será demonstrando em alguns tópicos procedimentos que podem ser feitos para deixar a sua rede wireless mais segura e evitar possíveis ataques ou acessos indevidos.

Escolha uma senha forte para acesso de sua rede wireless.

Hoje em dia já é um clichê requisitar que os sistemas de informação sejam protegidos com senhas fortes (caracteres especiais, números, letras maiúsculas e minúsculas), mas ainda há diversos casos de acessos indevidos, por conta de senhas fracas (ex: 1234567890). Esse tipo de procedimento dificulta não só a tentativa de ataques propriamente ditos, mas também o simples fato de uma pessoa qualquer conseguir "adivinhar" a senha em questão da rede.

Redes sem fio: cuidados



Evitar compartilhamento de senhas entre setores.

Vemos em muitas empresas o compartilhamento de senhas entre os setores, já que um setor pode ter acesso a algumas aplicações que outros não (ex: rede social) e isso pode acarretar em diversos problemas de segurança, já que uma pessoa de um departamento distinto ao seu poderá acessar recursos e informações que poderão não lhe ser concedidas, podendo agir de má fé ou coisa parecida.

Não conecte qualquer dispositivo a rede sem fio.

Com a facilidade da conexão é possível conectar diversos tipos de dispositivos (smartphone, tabeles, notebooks, etc...), mas há o risco de inserir os dispositivos dos quais não são verificados pelo setor de TI, pois tais equipamentos geralmente são usados em outras redes, em casa e para acessar outros conteúdos, sejam redes sociais, sites de filmes, download de arquivos etc... e como consequência existe o grande risco desses equipamentos serem infectados por algum tipo de malware trazendo consigo perigo para a rede da organização se conectado a rede da mesma . Por isso é de extrema importância antes de conectar algum dispositivo novo ou que foi conectado em outra rede levar para o setor de TI para que o dispositivo possa ser checado e como consequência ser liberado para uso dentro da empresa.

Capítulo 10

Backups

Backups

Diariamente, seja usando os nossos smartphones ou computadores pessoais, temos a tendência de armazenar uma grande quantidade de arquivos, como imagens, músicas, documentos e vídeos. É bem verdade que não damos muita importância em fazer a cópia deles, mas basta algo de errado acontecer que quase de imediato iremos com o susto de perde-los, ver o quanto eles possuem valor para nós.

Imagina perder as fotos de uma das melhores viagens que você fez com sua família para fora do país!?... Ou 2 dias antes da entrega do seu TCC, o bendito não abre... Ou perder os milhares de contatos da sua agenda do celular!?. Essas são algumas das diversas situações que provavelmente você já passou ou pode passar algum dia.

Você não vai querer perder seus dados, não é mesmo? Portanto, para evitar perdê-los, desde já adote uma postura preventiva, faça cópias de segurança dos seus arquivos.

Como você pode perder seus arquivos?

Existem diversas situações em que você pode perder seus arquivos. São elas:

- Os seus dispositivos serem invadidos, infectados e em seguida os arquivos serem apagados ou criptografados;
- Os seus dispositivos apresentarem problemas e como consequência corromper seus arquivos;
- Por falta de atenção os arquivos serem apagados acidentalmente;
- Os seus dispositivos serem perdidos ou roubados.

Backups: onde armazenar?

Onde armazenar os backups?

As cópias de segurança podem ser armazenadas localmente, no próprio computador, smartphone, tablet, remotamente, em mídias off-line como CDs, DVDs, pen drives, HDs externos ou ainda on-line utilizando serviços em nuvem.

Para armazenar backups em nuvem, você dependerá da velocidade da rede. Quanto maior o volume de dados a serem enviados mais tempo será necessário para salvar os arquivos, tornando inviável em alguns casos este tipo de backup. Os serviços de armazenamento em nuvem como Dropbox, Google Drive, entre outros, não são considerados serviços de backup, mesmo que sejam utilizados para este fim. Então quer dizer que os arquivos que estão na minha conta do Dropbox não são backups em nuvem?

Um simples arquivo importante enviado para seu e-mail, pode ser considerado um backup em nuvem, de forma simples, mas prática. Os serviços de armazenamento em nuvem, salvam os seus arquivos fora do seu computador, notebook, celular ou tablet. Mas não é possível guardar versões. Por exemplo, você tem instalado o aplicativo do Dropbox, sua conta está configurada e o sincronismo dos arquivos está ativo. Se você fizer alguma alteração no arquivo no seu computador, automaticamente, após o aplicativo sincronizar, o arquivo em nuvem também será atualizado.

Já um sistema de backup em nuvem, faz o controle de versões dos arquivos. Por exemplo, você contrata um serviço de backup em nuvem e configura para que todos os dias às 20h o backup seja realizado e enviado para o servidor automaticamente. É possível definir que a cada vez que a tarefa for executada será criado um novo arquivo no servidor em nuvem, assim no final de um mês você terá 30 cópias de segurança do mesmo arquivo.

Backups: como armazenar?

Como armazenar os backups?

Tão importante quanto fazer o backup é guardar as cópias de segurança em local seguro. Não adianta ter vários backups armazenados localmente no mesmo disco. Em caso de falha do disco se perde os arquivos originais e as cópias de segurança.

Obviamente, não existe uma regra que diz qual combinação é a melhor, vai depender dos seus recursos e suas necessidades, mas um modelo interessante a ser seguido é a regra "3-2-1.

Essa regra, portanto, define que você terá pelo menos 3 cópias dos dados (a original e 2 backups); irá armazenar aos backups em 2 tipos de mídias diferentes e terá uma cópia remota ou off-line . Seguindo esta regra, você poderá criar várias combinações de locais de armazenamento:

- Os arquivos originais, uma cópia num pen drive (off-line) e uma cópia na nuvem (remota).
- Os arquivos originais, uma cópia em outra partição do HD e uma cópia em outro computador.
- Os arquivos originais, uma cópia em DVD e uma cópia num servidor na mesma rede.

As mídias off-line sempre deverão ser desconectadas do equipamento após a conclusão do backup. Imagine que você sempre faz o backup no pen drive, mas o deixa conectado no notebook. Caso ocorra uma falha elétrica e danifique seu notebook, grandes são as chances do pen drive ser danificado e você perder todos os seus dados.

Tenha sempre atenção onde guarda as mídias off-line, pois por serem portáteis podem ser facilmente perdidas. Muito cuidado ao descartar mídias, pois existem programas que podem recuperar os arquivos mesmo após a mídia ser formatada. O ideal é que a mídia seja destruída ou incinerada.

Ao contratar um serviço de backup em nuvem fique atento as seguintes questões:

- O fornecedor tem boa reputação e é bom?
- O serviço está sempre disponível?
- Qual o tempo que os arquivos são mantidos? Esse tempo atende as suas necessidades?
- O fornecedor oferece a possibilidade de criptografar os dados antes de enviá-los para a nuvem?

Backups: como manter?

Mantenho os backups por quanto tempo?

Claro que existem arquivos que você sempre vai querer manter a salvo, mas existem aqueles que podem perder a validade, se tornarem obsoletos ou perdem a sua importância. Como um trabalho do ensino médio que você fez na época, mas que estando na faculdade agora, ele talvez não tenha mais a importância de antes.

Desta maneira, mantenha seus backups pelo tempo que eles continuarem tendo valor para você ou e claro, se não tiver problemas de espaço para armazená-los.

Validando e testando o backup

Você quer evitar surpresas não é mesmo!? Não vai querer executar o backup quando necessário e ele estar corrompido não é!?. Sendo assim, é muito válido ao gerar os backups, validá-los e testá-los. Verifique se as cópias geradas possuem as mesmas características, como por exemplo, o mesmo tamanho e data de criação e claro abrindo as cópias para verificar se possuem o mesmo conteúdo. Senão, de nada vai adiantar ter cópias que não sejam idênticas a original.

Capítulo 11

Resposta a incidentes

Resposta a incidente

Todos os dias são desenvolvidas diversas ferramentas e são lançados muitos produtos tanto para internet quanto para uso "off-line". Por isso é cada vez mais difícil manter a segurança da informação nas organizações, violações de dados e ataques cibernéticos são coisas que a maioria das empresas já aceitam como possibilidade e com base nisso está cada vez mais difundido o conceito de que as estratégias de segurança da informação das empresas precisam ter várias camadas. Neste momento vamos falar sobre o Plano de Resposta a Incidentes, camada que vem sendo cada vez mais inserida pelas organizações em suas estratégias.

O Plano de Resposta a Incidentes tem como objetivo ser uma forma organizada de solucionar ou gerenciar um incidente de segurança limitando danos causados, minimizando os custos de recuperação e reduzindo tempo de tratamento, ou seja, é um planejamento para que todos os envolvidos na resposta saibam "o que fazer", "como fazer" "e quando fazer" durante um incidente.

Um Plano de Resposta a Incidentes depende de cada organização, porém o SANS Institute descreve 6 etapas básicas que, se seguidas, garantem a eficácia da resposta a um incidente:

Resposta a incidente

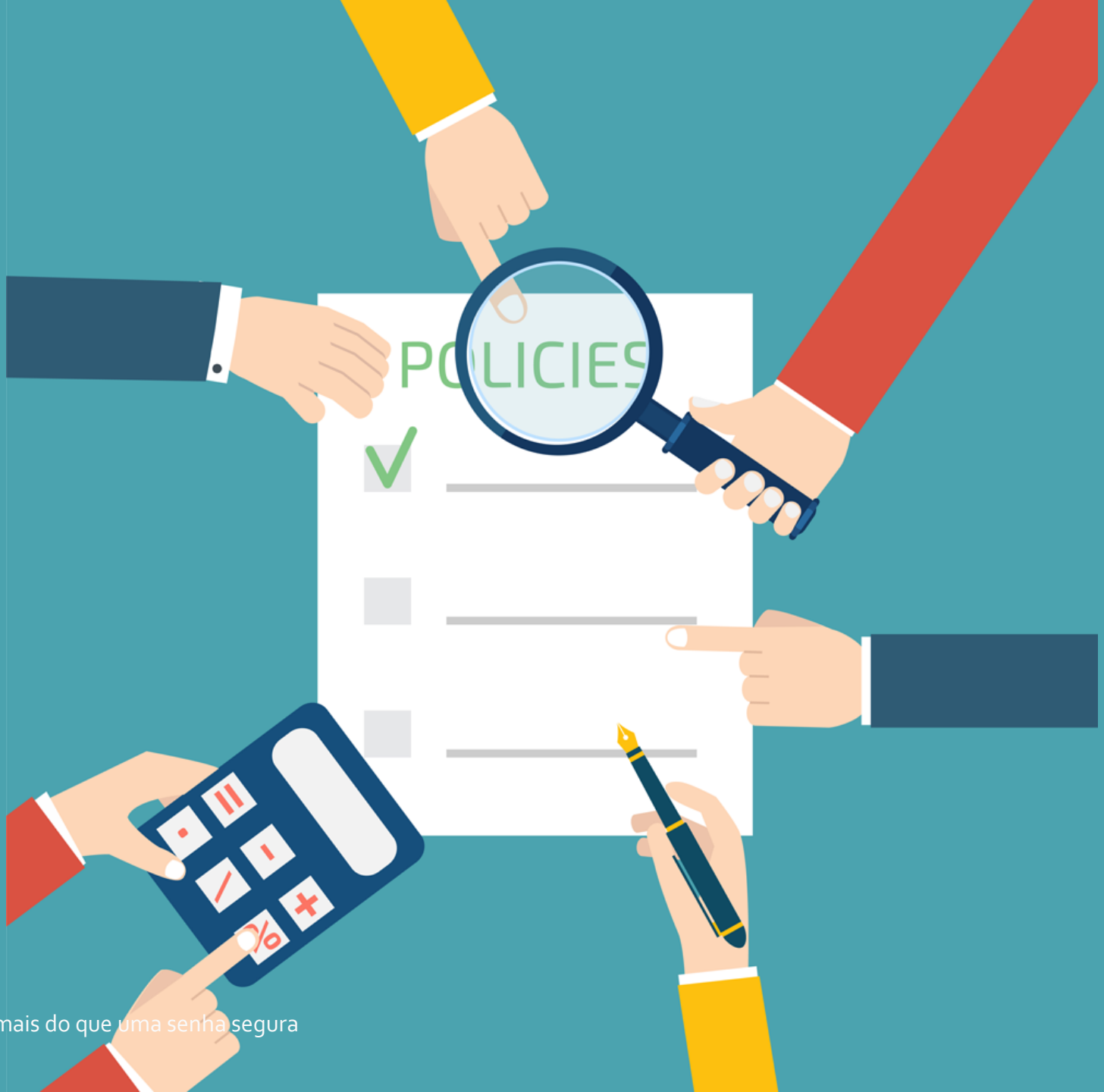
Preparação: Nesta etapa todos os procedimentos e políticas devem ser conhecidas e testadas pelos profissionais envolvidos no tratamento, e as ferramentas devem ser bem difundidos para que a corporação consiga responder a qualquer incidente potencial e reduzir tempo de indisponibilidade, recuperação e custos;

Detecção e Identificação: Que tipo de incidente ocorreu? Perda de dados? Ataque de rede? É preciso determinar seu tipo e sua gravidade para que seja possível seguir na respondendo ao incidente conforme a política e procedimentos definidos pela corporação. Saber o impacto gerado pelo incidente também é importante para decidir a forma e prioridade de tratamento;

Contenção: A contenção é uma etapa crítica, pois se resume a reduzir o impacto que pode ocorrer durante um incidente. Dentre as formas de contenção existem: Isolar a área infectada para facilitar análise, bloquear um trafego de rede malicioso, cortar acesso de um usuário mal intencionado à rede e etc... A comunicação aqui também é muito importante, certifique-se de que as pessoas que foram comunicadas do incidente são pessoas envolvidas e que tem participação no Plano de Resposta a Incidentes;

Remediação: Nesta etapa são resolvidos os problemas, remoção de códigos maliciosos e qualquer ameaça que possa manter o incidente, os logs são analisados em busca da causa raiz, é analisado se é necessário backup ou se existem vulnerabilidades que causaram o incidente;

Recuperação: Aqui são feitas as recuperações dos sistemas afetados, a validação se tudo voltou a funcionar normalmente (politicas, procedimentos, sistemas, processos...). Nesta fase o monitoramento continuo é muito importante, pois garante que o problema de fato foi resolvido.


POLICIES

Resposta a incidente

Lições Aprendidas: deve ser feito um relatório de tudo o que ocorreu, todas as medidas de correção tomadas, pontos que podem ser melhorados para que o incidente não ocorra novamente. Este relatório é importante para os casos em que a prevenção de um mesmo incidente só ocorrerá em casos mudança cultural ou em processos de áreas externas à área que tratou o incidente. É muito importante que esse relatório seja divulgado para pessoas certas e que podem dar suporte técnico, gerencial ou político para as mudanças que serão feitas.

Essas são recomendações que, se seguidas, podem minimizar custos de um incidente ou até mesmo prevenir que os mesmos ocorram. É importante ressaltar que todos devem ter conhecimento do plano e o mesmo precisa ser de fácil acesso para que existam testes e manutenções afim de trazer melhorias para o mesmo, porém não podemos falar de Plano de Resposta a Incidentes de Segurança não falar da equipe que é ponto focal para lidar com eles na organização. Essa equipe é o Grupo de Resposta a Incidentes de Segurança em Computadores (em inglês CSIRT Computer Security Incident Response Team), mas como ter uma equipe dessas na organização?

Antes de tudo é importante ressaltar que os CSIRT's são únicos, ou seja, por mais que existam recomendações de como cria-los cada um terá a "cara" da sua organização. Vamos citar aqui algumas boas práticas que segundo o CERT.br e a Microsoft, quando seguidas, ajudam na criação de um CSIRT.

Primeiramente o que é o CSIRT? É um grupo responsável por analisar e responder atividades relacionadas a incidentes de segurança em computadores, sua atuação visa controle, tratamento, redução no impacto e nos custos de um incidente. Eles podem atender organizações, comunidades específicas e até grupos maiores como países.

CSIRT’s

Existem basicamente dois tipos de CSIRT's:

Grupo Formal: Este tem como principal função a resposta a incidentes, sem mudança de foco para outra atividade. Neste modelo a equipe tem profissionais dedicados a funções específicas relacionadas apenas a tratamento dos incidentes;

Grupo Adhoc: Este é criado apenas no momento em que há possibilidade ou um incidente ocorre. Geralmente é composto por profissionais de TI de diversas áreas de atuação sendo coordenados por um Líder de Resposta a Incidentes. Este modelo tem boa eficácia para pequenas e médias empresas, pois como não há necessidade de profissionais dedicados e o custo fica reduzido;

OBS: A terceirização dos serviços de resposta a incidentes também é uma opção quando a organização possui poucos em sua equipe de TI ou quando a alta demanda não permite que os mesmos se dediquem a tratar incidentes.

CSIRT's também podem ter tamanhos diferentes e servir a objetivos e comunidades diferentes e podem ser:

CSIRT's Internos: Estes servem a organizações específicas;

CSIRT's Nacionais: Estes proveem serviços de resposta a incidentes para um país;

Centros de Coordenação: Estes coordenam ações de resposta entre diversos CSIRT's;

Centros de Análise: Estes agrupam dados de várias fontes para identificar padrões de atividade e tendências;

Grupos de Empresas Fornecedoras: São as empresas que fornecem serviços de resposta a incidentes a outras corporações.

CSIRT’s

A relação entre um Plano de Resposta a Incidentes de Segurança e um CSIRT é grande apesar de o primeiro não estar sempre relacionado a incidentes em computadores, CSIRT’s podem compor um SIRT (Security Incident Response Team) por exemplo e serem treinados para tratar qualquer tipo de incidente. Suas atividades podem ser reativas ou proativas, não existe uma padronização para suas funções, porém elas precisam se basear nos interesses de sua comunidade ou organização, sua atuação pode ser no desenvolvimento de um software visando correção de vulnerabilidades antes de ser utilizado em ambiente de produção ou pode ser na contenção de um malware que está se propagando através da rede corporativa, basta que seu escopo seja claro e bem definido. Abaixo vamos citar alguns pontos que, segundo o CERT.BR e Microsoft, são importantes sobre os CSIRT's.

CSIRT's não tem definição hierárquica padrão, ou seja, na organização podem estar dentro da área de Segurança da Informação, dentro da equipe de TI ou até mesmo fazer parte do Plano de Continuidade da empresa. Cada organização definirá seu local na hierarquia;

CSIRT's precisam ter na equipe ou estar em constante contato com diversos profissionais de equipes diferentes da empresa ex: relações públicas, departamento jurídico, recursos humanos, gerência e outros. Esses contatos são para que as ações tomadas pelo CSIRT tenham respaldo e não interfiram negativamente na organização;

Considere que o CSIRT precisa de treinamento para que seja capaz de tratar os incidentes como: de políticas, da organização e dos sistemas utilizados. O CERT.br também ministra cursos do CERT/CC pelo Brasil para formação de CSIRT's vale a pena conferir;

CSIRT's

Ao final do tratamento de cada incidente é importante que seja feita uma avaliação de como foi a resposta. Discutir com a equipe tudo o que foi realizado com êxito e as falhas que ocorreram, pois na maioria das vezes encontrará processos ou alguns pontos que precisam ser mudados para tratamento de incidentes futuros. A busca de pontos fracos na resposta ajuda a melhorar a atuação do CSIRT e o Plano de Resposta.

Diante do que vimos a construção de um CSIRT aliado a um bom Plano de Resposta a Incidentes de Segurança é essencial para a organização, isso não impede e nem acaba com possiblidades de ataques ou incidentes, porém fornece um controle que reduz consideravelmente os riscos e custos no caso de um incidente. Lembre-se que parece não fazer diferença, mas aceitar um risco dentro de uma organização e saber seu custo em casos de exploração não é o mesmo que não conhecê-lo.

Capítulo 12

Recomendações aos profissionais de TI

Recomendações

O ideal é que a segurança da rede fosse projetada logo após o plano de negócios ter sido concluído e antes de qualquer tecnologia seja adquirida. Mas sabemos que isso é utopia, infelizmente, nos deparamos com tudo em funcionamento. E este é o grande desafio. Por onde começar?

Identifique os riscos

Para projetar uma rede segura, deve-se primeiramente identificar as ameaças, que podem vir de dentro e ou fora da rede. Os riscos associados à segurança da rede incluem ações acidentais e intencionais. Por isso é importante manter-se atualizado sobre os meios de ataques ou vulnerabilidades.

Conheça a sua Rede

Faça um inventário de todos os ativos da empresa, mapeando a rede física e lógica. Assim poderá identificar o que ajudará a proteger o fluxo de informação para a criação de zonas dentro da rede. Estabeleça diferentes níveis de segurança. Defina o tipo de informação que deve ser protegida.

Avalie os riscos

Depois de avaliar e priorizar os riscos para sua rede, você pode avaliar suas opções para enfrenta-los e terá uma solução mais clara para resolver seus problemas de segurança. Comece com as soluções que não requerem custos, depois avalie seu orçamento disponível e procure a melhor ferramenta para lhe ajudar.

Recomendações

Segurança em Camadas

A proteção em camadas combina várias medidas de segurança para dar proteção a diferentes tipos e fontes de ameaças. Existem modelos diferentes de segurança em camadas, escolha um que se adeque ao seu ambiente e implante.

Crie uma política de segurança

Uma vez que você identificou todas as ameaças à sua rede e você começa a escrever informações sobre como implementar e proteger essas áreas em sua rede, você desenvolverá uma política de segurança.

Analise a situação

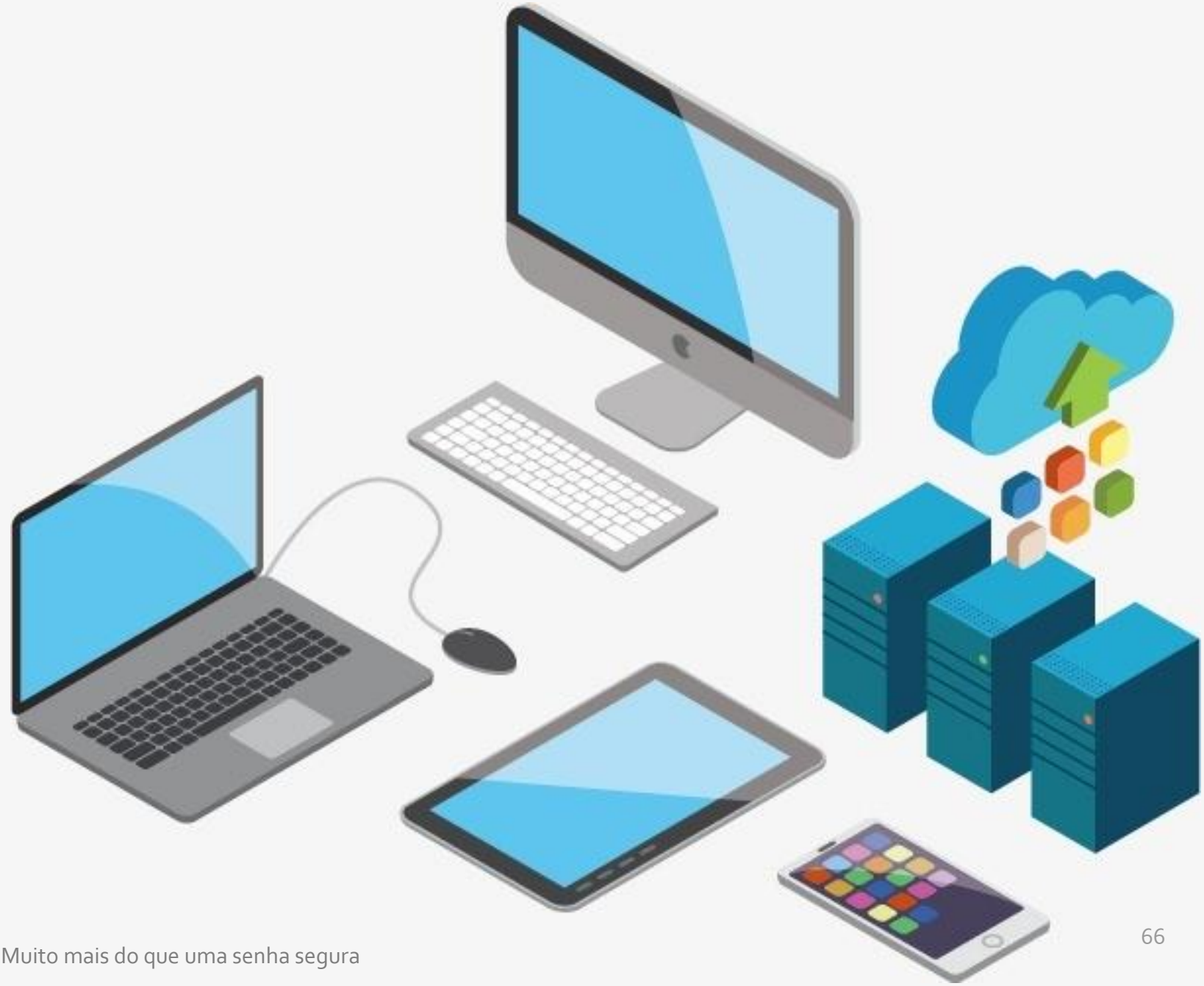
Comece com uma auditoria da tecnologia existente. Aproveite o tempo para criar um inventário de todos os servidores, desktops, equipamentos de rede, políticas existentes, comportamento do usuário e assim por diante.

Entenda e defina a funcionalidade necessária para o sistema

Qual serviço é necessário? Quem pode acessar um serviço?

Determine os métodos para garantir a funcionalidade do sistema

O que você pode fazer para evitar que alguém use o sistema?



Recomendações

Implemente medidas de segurança

Sua política de segurança não terá efeito se os usuários e administradores não conhecerem as medidas.

Teste as medidas - Realize uma auditoria de segurança. Isso irá ajudá-lo a encontrar falhas ou cenários que o time de segurança possa ter perdido.

Backup

Não importa o tamanho de sua empresa, ter backup significa “poder dormir tranquilo". Hoje há diversos meios de realizar este procedimento. Escolha o que melhor se adequar a sua empresa, mais lembre-se "quem tem um, não tem nenhum".

Treinamento / Conscientização

“O elo mais fraco é sempre o usuário, então o funcionário muitas vezes acaba sendo a porta de entrada”, diz Fábio Picoli, country manager da empresa de segurança da informação japonesa Trend Micro.

Por esses motivos, a conscientização dos funcionários se torna cada vez mais essencial como parte da estratégia das empresas, então mãos à obra: elabore treinamentos, faça simulações, compartilhe com o usuário...

Recomendações

Plano de Resposta

Mas se algo acontecer, você está preparado? Então elabore um plano de resposta a incidentes.

- Mapeie todas as soluções que a empresa possui, bem como ter definido os responsáveis pelo processo de resposta de cada área da companhia;
- Identificado o incidente, qualificar a abrangência e o impacto nos negócios;
- Fazer a contenção, isolando o incidente para que ele não se propague por toda a empresa;
- Erradicar o problema, aplicando as correções levantadas e monitorando para se ter o resultado esperado;
- Recuperação, que vai restabelecer o ambiente afetado;
- Realizar o histórico das ocorrências do incidente, assim como documentar todos os processos de resposta que erradicaram o incidente, o que vai criar um material para a empresa estar preparada para ataques que possam ocorrer no futuro.

Recomendações

Mantenha-se atualizado

Por fim, mantenha-se atualizado. Com o impulso de possibilidades no setor de tecnologia da informação, o setor se reinventa e a cada dia surge um novo risco. Manter-se atualizado é necessário. Acompanhe blogs especializados e canais de tecnologia e participe de grupos de whatsapp, telegrama e facebook.

Gerencie e Monitore

Com a alta complexidade que as redes corporativas apresentam hoje, é necessário realizar um acompanhamento proativo, visando a garantir a manutenção do acesso e a segurança da informação. Existem hoje no mercado inúmeras soluções como Zabixx, Opemon, Nagios, etc, para auxiliar sua empresa na realização de um monitoramento de rede eficaz. Além do acompanhamento dos relatórios do antivírus e firewall. Alguns dos sinais de comprometimento da rede que podem ser facilmente identificados são: dificuldade de acesso, lentidão, redução de desempenho de alguns sistemas e processos etc.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para controles de segurança da informação. 2 ed. Rio de Janeiro: ABNT, 2013. 99p.

GAZOLA, André. INFOGRÁFICO: QUAL SEU ESTILO DE APRENDIZAGEM?. Disponível em: <https://www.lendo.org/infografico-estilo-aprendizagem-visual-auditivo-cinestesico/>. Acesso em: 29 nov. 2017.

AFRIKA TECNOLOGIA E NEGÓCIO, Redação. Importância da educação em segurança da informação. Disponível em: <http://www.afrikatec.com.br/educacao-em-seguranca-da-informacao/>. Acesso em: 29 nov. 2017.

TELES, Guilherme. Por que a educação em segurança da informação é importante. Disponível em: <https://www.tiespecialistas.com.br/2011/12/por-que-a-educacao-em-seguranca-da-informacao-e-importante/>. Acesso em: 12 dez. 2017.

Brasil. Presidência da República. Gabinete de Segurança Institucional. Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018: versão 1.0 / Gabinete de Segurança Institucional, Secretaria-Executiva, Departamento de Segurança da Informação e Comunicações. – Brasília: Presidência da República, 2015.

EMPRESAS devem ficar atentas ao fator humano. Disponível em: <http://itsa-brasil.com.br/hotsite/noticias/empresas-devem-ficar-atentas-ao-fator-humano/>. Acesso em: 12 dez. 2017.

Referências

ENTANDA A IMPORTANCIA DO BACKUP PARA EMPRESAS Disponível em https://gdsolutions.com.br/seguranca-da-informacao/entenda-a-importancia-do-backup-para-empresas/ Acesso em março, 2018.

COMO SE MANTER ATUALIZADO NA AREA DE TI Disponível em https://gaea.com.br/afinal-como-se-manter-atualizado-na-area-de-ti/ Acesso em fevereiro, 2018.

TREINAR FUNCIONARIOS E TAO ESSENCIAL QUANTO OS ANTIVIRUS Disponível em http://www.phishx.io/treinar-funcionarios-e-tao-essencial-quanto-os-antivirus Acesso em março, 2018.

CARTILHA CERT Disponível em https://cartilha.cert.br/ Acesso em fevereiro, 2018.

6 MEDIDAS PARA UM PLANO DE RESPOSTA A INCIDENTES https://www.itforum365.com.br/seguranca/6-medidas-para-um-plano-de-resposta-a-incidentes-de-seguranca Acesso em março, 2018.

SEGURANÇA EM CAMADAS POR QUE FUNCIONA http://blog.infomach.com.br/seguranca-em-camadas-por-que-funciona/ Acesso em abril, 2018.

Referências

VOCÊ SABE O QUE SÃO CAMADAS DE SEGURANÇA Disponível em http://www.administradores.com.br/noticias/tecnologia/ti-voce-sabe-o-que-sao-camadas-de-seguranca/84439 Acesso em abril, 2018

QUAL IMPORTANCIA DO MONITORAMENTO DE REDE Disponível em http://introduceti.com.br/blog/qual-a-importancia-do-monitoramento-de-rede/ Acesso em junho, 2018

IMPORTANCIA MONITORAMENTO DE TI Disponível em https://www.s3curity.com.br/importancia-monitoramento-de-ti/ Acesso em março, 2018

Christopher Hadnagy (29 November 2010). Social Engineering: The Art of Human Hacking. John Wiley & Sons.

STATE OF THE INTERNET Disponível em https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q1-2017-state-of-the-internet-security-report.pdf Acesso em fevereiro, 2018.

O MERCADO BILIONARIO DA ESPIONAGEM NO BRASIL https://veja.abril.com.br/brasil/o-mercado-bilionario-da-espionagem-no-brasil/ Acesso em março, 2018.