eSecurity

Treinamentos em Segurança da Informação

O que temos para hoje?

Conceitos:

- ✓ A necessidade da Segurança
  - ✓ Confidencialidade
  - ✓ Integridade
  - ✓ Autenticidade
  - ✓ Não Repúdio ou Irretratabilidade
  - ✓ Disponibilidade
- ✓ O mercado de trabalho
- ✓ Certificações
- ✓ Certificações em Segurança
  - ✓ Certificações de apoio
  - ✓ Certificações técnicas

Conhecendo o Nmap

A necessidade da Segurança

Informação compreende qualquer conteúdo que possa ser armazenado ou transferido de algum modo, servindo a determinado propósito e sendo de utilidade ao ser humano.

Trata-se de tudo aquilo que permite a aquisição de conhecimento.

Nesse sentido, a informação digital é um dos principais, senão o mais importante, produto da era atual.

Ela pode ser manipulada e visualizada de diversas maneiras. Assim, à medida que a informação digital circula pelos mais variados ambientes, percorrendo diversos fluxos de trabalho, ela pode ser armazenada para os mais variados fins, possibilitando ela ser lida, modificada ou até mesmo apagada.

Fonte: Wikipedia

A necessidade da Segurança

É de extrema importância que as empresas invistam em segurança, não apenas as empresas grandes e médias, mas todas.

Porém, esse deve não deve ser aplicado apenas às empresas, mas também a qualquer pessoa que esteja online ou não, visto que, todos obtemos informações, sejam elas aparentemente insignificantes para outros ou não.

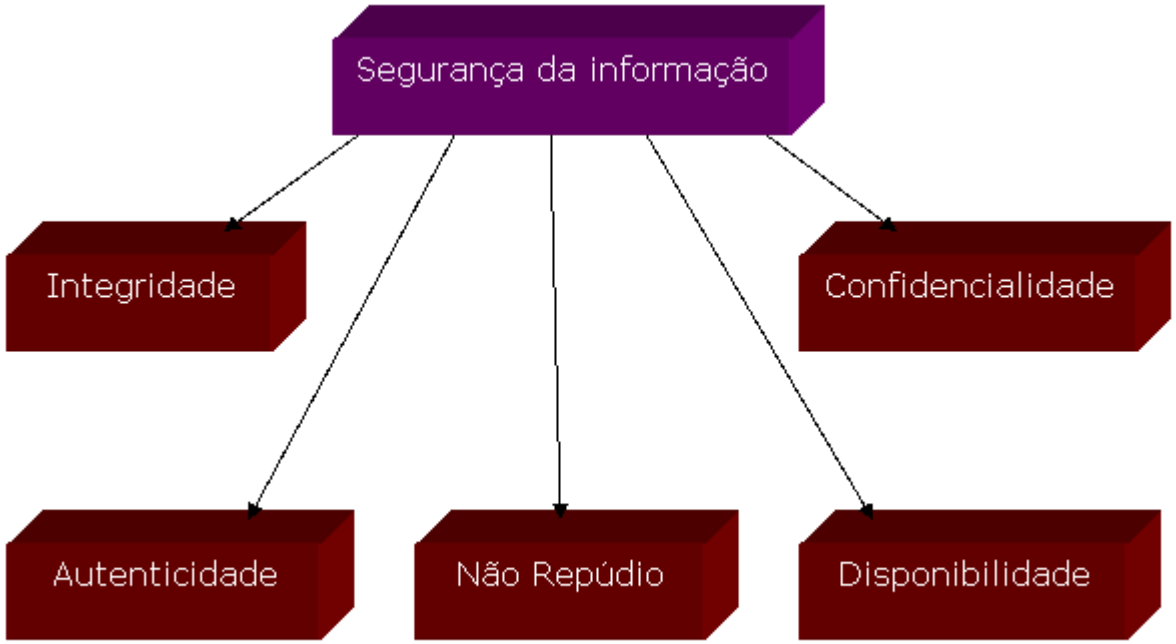
Vamos pensar em alguns exemplos:

- Dados do seu smartphone
- Nome, CPF, RG, PIS e afins
- Horários rotineiros
- Lugares frequentados
- Desejos (Utilizado por sistemas de marketing na internet)

A necessidade da Segurança

Quando falamos de empresas, as necessidades são maiores. As informações podem não apenas ser roubadas por concorrentes, mas também por funcionários, até mesmo aqueles de confiança.

Não podemos focar apenas em roubo de dados, mas, a Segurança da Informação, está envolvida em 5 pilares, que falaremos ainda nesta aula.



Confidencialidade

Confidencialidade:
Propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.
Fonte: Wiki

Sabemos que sempre há nas empresas por onde passamos a falta de controle de acessos, seja ela em redes, aplicações ou arquivos.

É importante ter um controle de acesso bem afinado para que a confidencialidade esteja em conformidade, e não podemos deixar de esquecer, quanto mais complexo o sistema ou rede versus número.

Integridade

Integridade:
Propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento,manutenção e destruição).
Fonte: Wiki

É importante sabermos que em qualquer ataque, sempre há falta de integridade, seja ela na transmissão de dados ou na manipulação de aplicações.

Não é uma tarefa fácil manter a integridade em um ambiente informático e pior fica, quando esse ambiente possui muitos dispositivos.

Autenticidade

Autenticidade:
Propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo.
Fonte: Wiki

Podemos dizer que e-mails como SPAM não são de fato autênticos, afinal, não vem da fonte ao qual deveria.

Na área de Segurança da Informação, a autenticidade é algo crítico, sem ela, ou sem o controle dela, não podemos saber se determinada informação é confiável ou maliciosa.

Disponibilidade

Disponibilidade:
Propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.
Fonte: Wiki

A disponibilidade deve andar junto com a confidencialidade, ou seja, a informação deve estar disponível, porém, apenas para as pessoas que estão autorizadas a acessar determinada informação.

Muitos não agregam a propriedade Disponibilidade com Segurança da Informação, e de nada adianta termos um sistema altamente seguro se ele não está disponível.

Existem ataques que exploram apenas este tipo de vulnerabilidade, porém, existem casos que não vale a pena o investimento.

Não repúdio ou irretratabilidade

Não repúdio ou irretratabilidade:
Propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita.
Fonte: Wiki

Podemos chamar soluções de não repúdio como assinaturas digitais, em muitos casos, essas assinaturas garantem que uma transação foi realizada por determinado indivíduo e não outro.

Decorrente deste tipo de controle, crackers tentam a todo tempo se mascarar para não serem identificados, sendo assim, não se responsabilizando pelos atos cometidos, que na sua maioria, de forma ilegal.

O mercado de trabalho

O mercado de trabalho

O mercado de trabalho:
No Brasil, Segurança da Informação é um assunto que está em alta, porém, culturalmente ainda vemos um descaso quando entramos nesse assunto.

São poucas as empresas que se preocupam com isso, além de instituições financeiras e grandes lojas virtuais, as demais empresas só começam a se preparar para ataques quando já são atacadas.

Essa cultura é típica do Brasileiro, que possui o hábito de achar que nada irá acontecer com ele, apenas com os outros, ou que sua empresa não possui nenhum dado valioso para hackers.

Precisamos, nós de TI, começar a nos aprofundar nessa área, partindo dos desenvolvedores e Administradores de Sistemas.

O mercado de trabalho

No mercado de trabalho, existem pouquíssimos profissionais de Segurança com capacidade suficiente para controlar e mitigar a maioria dos ataques, sejam eles internos e externos.

Os cursos de formação acadêmica, como pós graduação, não possuem conteúdos suficientes para formar um profissional em Segurança da Informação com conhecimento técnico no mercado.

Por outro lado, existem os profissionais que visam o ganho financeiro, que por sua vez, não se interessam na área técnica e exploram a Segurança da Informação voltada em auditorias, controles e políticas. Esses profissionais são mais remunerados, por possuírem cargos de nível gerencial. Eles são tão importantes quanto os de nível técnico.

Decorrente disto, são raríssimos os profissionais que possuem ambos conhecimentos, políticas e técnicas, e existem empresas que pagam muito bem para profissionais como estes.

O mercado de trabalho

Quando temos em uma empresa profissionais apenas com conhecimentos técnicos, temos problemas de gestão e controle, por outro lado, quando encontramos profissionais apenas teóricos, temos falhas de segurança.

O profissional ideal é aquele que se enquadra nas necessidades da empresa, que entende e respeita suas políticas e trabalha incessantemente para que estas, por sua vez, estejam em constante melhoria.

Não há política ou técnica que não possa ser melhorada, assim como não há profissional que não pode ser lapidado e melhorado para que haja sempre o entendimento mútuo entre empregador x empregado.

Certificações

Certificações

Existem certificações para todos os gostos, gêneros e áreas, porém, também existe a grande polêmica entre o conhecimento prático e técnico dos certificados.

A certificação de fato é sempre um diferencial quando há competição no mercado de trabalho, então, é importante possuí-las, mas, mais importante que as certificações é o conhecimento embarcado.

Iremos debater sobre esse assunto tão polêmico e conhecer os atalhos para conquistar algumas certificações importantes e entender como elas podem te ajudar nesse mercado.

Primeiro vamos conhecer as principais certificações úteis na área de SegInfo.

Certificações

Certificações que não são de Segurança, mas são muito solicitadas nas principais vagas de SegInfo:

ITIL (Information Technology Infrastructure Library)
É um conjunto de boas práticas para serem aplicadas na infraestrutura, operação e manutenção de serviços de tecnologia da informação (TI).
O modelo ITIL busca promover a gestão com foco no cliente e na qualidade dos serviços de tecnologia da informação (TI). O ITIL lida com estruturas de processos para a gestão de uma organização de TI apresentando um conjunto abrangente de processos e procedimentos gerenciais, organizados em disciplinas, com os quais uma organização pode fazer sua gestão tática e operacional em vista de alcançar o alinhamento estratégico com os negócios.
Esta certificação não expira.

Cobit (Control Objectives for Information and related Technology)
É um guia de boas práticas apresentado como framework, teste dirigido para a gestão de tecnologia de informação (TI).1 Mantido pelo ISACA (Information Systems Audit and Control Association), possui uma série de recursos que podem servir como um modelo de referência para gestão da TI, incluindo um sumário executivo, um framework, objetivos de controle, mapas de auditoria, ferramentas para a sua implementação e principalmente, um guia com técnicas de gerenciamento. Esta certificação não expira.

Certificações

Certificações de Infra, que todo profissional de SegInfo precisa conhecer:

LPI (Linux Professional Institute)

É uma organização sem fins lucrativos, constituída em 1999 pela comunidade Linux e desenvolve de forma acessível um programa de certificação em sistemas GNU/Linux reconhecido internacionalmente por empresas, empregadores e profissionais de TI.
A principal vantagem da LPI sobre outras certificações Linux é a neutralidade de distribuição, pois as provas do LPI são baseadas no Linux Standard Base, um conjunto de normas que mantém a compatibilidade entre as diferentes versões e distribuições do sistema operacional. A certificação LPI é, portanto, independente de distribuição. A certificação LPI expira a cada 5 anos, sendo assim, necessário refazer a avaliação.

CCNA (Cisco Certified Network Associate)

Embora este seja apenas o primeiro passo na certificação da carreira Cisco, o CCNA (Cisco Certified Network Associate) é um exame difícil, se comparado a outras certificações como Microsoft. A recente inclusão de perguntas práticas tornou-o ainda mais desafiador. Sua primeira tentativa em se tornar certificado pela Cisco exige muito estudo e muita confiança naquilo que você já conhece sobre redes. Quando estiver pronto para testar as suas habilidades, pôr em prática o que conhece sobre os tópicos avaliados e se preparar para o dia do exame.
Existe também, após a aprovação do CCNA, o CCNA Security ao qual é focado em Segurança em Redes. A certificação expira a cada 3 anos.

Certificações

Certificações de Desenvolvimento, que todo desenvolvedor precisa conhecer:

CSSLP (Certified Secure Software Lifecycle Professional)

É a maior e mais abrangente coleção de melhores práticas, políticas e procedimentos para garantir níveis de segurança adequados em todas as fases do ciclo de desenvolvimento de software, independentemente da tecnologia utilizada. Do conceito e planejamento a operações e manutençãoe, finalmente, à eliminação, ela estabelece padrões e práticas recomendadas do setor para a integração de segurança em cada fase. Esta certificação não expira

Certificações

Certificações de Segurança de Redes, excelentes para profissionais de infra:

CompTIA Security+

É uma certificação profissional que envolve tópicos em segurança de computadores tais como criptografia e controle de acesso. Foi criada e mantida pela Associação das Indústrias de Tecnologia da Computação dos Estados Unidos (CompTIA). Esta certificação expira a cada 3 anos.

ECSA – EC-Council Security Analyst

É uma certificação de formação avançada de hacking ético, que complementa o Certified Ethical Hacker, CEH, explorando a fase analítica de hacking ético. Enquanto a certificação Certified Ethical Hacker expõe o aluno a ferramentas e tecnologias de hacking, o curso Certified Security Analyst leva um passo adiante, explorando como analisar o resultado dessas ferramentas e tecnologias. Através de rede inovadores Teste de Invasão métodos e técnicas de formação, esta caneta de teste de segurança do computador certificação ajuda os alunos a realizar as avaliações intensivas necessárias para efetivamente identificar e mitigar os riscos para a segurança da informação da infra-estrutura.
Esta certificação expira em 3 anos

Certificações

Certificações de Auditoria e Conformidade, excelente para gestores:

ISO 27001

A norma ISO 27001 é o padrão e a referência Internacional para a gestão da Segurança da informação, assim como a ISO 9001 é a referência Internacional para a certificação de gestão em Qualidade.
Ao longo dos anos, milhares de profissionais contribuíram com o seu know-how e experiência para o estabelecimento de um Standard estável e maduro, mas que certamente continuará a evoluir ao longo dos tempos.
Esta certificação não expira.

CISA – Certified Information Systems Auditor

A certificação CISA já foi conquistada por mais de 60.000 profissionais desde seu lançamento em 1978. É uma certificação reconhecida mundialmente para profissionais de controle, auditoria e de segurança. Ser certificado CISA mostra sua experiência em auditoria, habilidades e conhecimento, além de demonstrar que você é um profissional capaz de gerir as vulnerabilidades, assegurar conformidade e estabelecer controles dentro da empresa.
Esta certificação não expira

Certificações

Certificações técnicas em Segurança da Informação:

CEH - Certified Ethical Hacker

É uma certificação independente de fabricante, o que é uma vantagem haja vista a variedade de técnicas e ferramentas de vários fabricantes que os criminosos utilizam para invasão.
A certificação proporciona um amplo conhecimento e prática real sobre as mais atuais ferramentas e técnicas de ataque e devesa virtual, permitindo atuar profissionalmente diante da ameaça.
Esta certificação expira em 3 anos.

LPT – Licensed Penetration Tester

A certificação EC-Council Certified Security Analyst (ECSA) complementa a certificação Certified Ethical Hacker (CEH) explorando a fase analítica do hacking ético. Enquanto CEH apresenta ao aluno tecnologias e ferramentas, ECSA vai um passo adiante, ao explorar como analisar os resultados destas. O profissional sendo certificado CEH e ECSA, estará apto a se certificar na certificação máxima da EC-Council na área de Auditoria Teste de Invasão, a Licensed Penetration Tester - LPT.
Esta certificação não expira.
Essa certificação expira em 3 anos

Certificações

Certificações técnicas em Segurança da Informação:

CPTE - Certified Penetration Testing Expert

Esta certificação é onde o candidato vai é testado em um cenário em que ele precisa desenvolver seus próprios exploits para violar a segurança. Este exame irá tornar candidato um desenvolvedor de ferramentas de segurança. O exame de laboratório não se limita a lacunas do sistema operacional Windows, também usamos mais recente Cisco IOS.
O laboratório é projetado para lidar com ameaças cibernéticas do mundo real e para atender às necessidades de uma organização de segurança em um curto espaço de tempo.
Esta certificação expira em 3 anos.

Certificações

Certificações em gestão em Segurança da Informação:

CISSP - Certified Information Systems Security Professional

É um certificado para profissionais de Segurança da Informação que tem o maior número de profissionais certificados e é a única presente em mais de 130 países. Ideal para quem busca visibilidade, carreira internacional e crescimento profissional.

O CISSP é um dos mais valorizados certificados do mercado por abranger um conteúdo neutro, comprovando que os profissionais certificados, independente da tecnologia, tem uma compreensão ampla da área de Segurança da Informação e maestria em gerenciar uma equipe nos problemas enfrentados no dia a dia.

Ser membro de uma das maiores e mais reconhecidas instituições de Segurança da Informação traz benefícios que só ela pode oferecer, como descontos em conferências em todo mundo e oportunidade de networking com outros profissionais da área.

Além, é claro, de passar na prova, para se certificar, o candidato deve atender aos seguintes pré-requisitos:

- Concordar e assinar o Código de Ética do $(ISC)^2$;
- Ter, no mínimo, três anos de experiência profissional em alguns dos 10 domínios de conhecimento em segurança da informação testados pela prova de certificação;
- Ser indicado por outro CISSP, empregador ou outra fonte digna de confiança;

Esta certificação não expira

Excelente site de referência: http://www.seginfo.com.br/principais-certificacoes-na-area-de-seguranca-da-informacao/#2-todas-certificacoes-dsic

Chega por hoje

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Fanpage: www.facebook.com/academiahacker