PRINCÍPIOS FUNDAMENTAIS

Referências Bibliográficas

Os conteúdos para elaboração das provas de concurso são extraídos dos documentos:

- *Segurança de Redes em Ambientes Cooperativos*, de Emilio Tissato Nakamura e Paulo Lício de Geus;
- *Criptografia e Segurança de Redes – Princípios e Práticas*, de William Stallings;
- *Segurança de Computadores – Princípios e Práticas*, de William Starllings e Lawrie Brown;
- Normas da International Organization for Standardization (ISO); e
- Conceitos básicos constantes no endereço *cert.br.*

Fatores de preocupação da Segurança da Informação

O entendimento da natureza dos ataques implica a compreensão de que falhas no projeto pode ocasionar vulnerabilidades que serão exploradas pelos atacantes. Erros de configuração também resultam em vulnerabilidades – por exemplo, uma senha não alterada de um roteador recém-comprado é um erro de configuração.

5m

Novas tecnologias implicam novas vulnerabilidades. Erros de criação de software podem ser evidenciados, o que resultam em vulnerabilidades.

Os atacantes se utilizam de combinações de técnicas e comumente cooperam entre si, trocando informações em comunidades voltadas a hackerismo. Dessa dinâmica resulta novas formas de ataques.

Do ponto de vista terminológico, segundo a literatura, *hacker* é aquele indivíduo com vasto conhecimento em relação a redes de computadores, sistemas operacionais e outros; de outro lado, *cracker* é o indivíduo com esse vasto conhecimento, cujo intuito é realizar atividades maliciosas. Apesar da definição da literatura, é comum que *cracker* seja reconhecido como *hacker*.

Aumento da conectividade é outro fator de risco, resultante do BYOD (Bring Your Own Device) e do IoT (Internet of Things). Para exemplificação, BYOD implica na situação em que aparelhos pessoais, muitas vezes desatualizados ou sem proteção adequada, são conecta-

ANOTAÇÕES

dos a aparelhos de empresas, o que pode ser uma ponte para atacantes. Já IoT implica no envio e recebimento de dados por meio da internet; a dinâmica ocorre com todos os aparelhos conectados à internet, como uma tevê, um sensor de incêndio etc. Esses equipamentos, por estarem conectados à internet, podem ser alvos de ataques.

10m

Mais um fator de risco é o aumento dos crimes digitais. Os crimes digitais ocorrem por meio de recursos computacionais. Nesse bojo, é importante as organizações estarem em conformidade com as disposições legais.

Observa-se que a Segurança da Informação é complexa, porque envolve aspectos:

- Tecnológicos;
- Humanos;
- Educacionais; e
- Técnicos.

No âmbito da Segurança da Informação, não há absoluta segurança. Sempre há um elo fraco, que é o recurso humano – o usuário. Por isso, o recurso humano precisa ser conscientizado.

Definição de Segurança da Informação

A Norma ISO 27002:2013 dispõe das diretrizes e das boas práticas da gestão da Segurança da Informação.

Ela esclarece que a Segurança da Informação é alcançada pela implementação de políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware.

Ativos Organizacionais

Ativo organizacional é aquilo que tem valor para uma organização.

Ativo é classificado em tangível (concreto) ou intangível (abstrato).

Edifício, equipamentos e pessoas são exemplos de ativos tangíveis.

Imagem, marca e informações são exemplos de ativos intangíveis.

ANOTAÇÕES

Propriedades da Segurança da Informação

Em relação aos ativos organizacionais, importa garantir certas propriedades, consideradas fundamentais para a organização. São ditas propriedades ou princípios da Segurança da Informação.

Confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade são propriedades da Segurança da Informação.

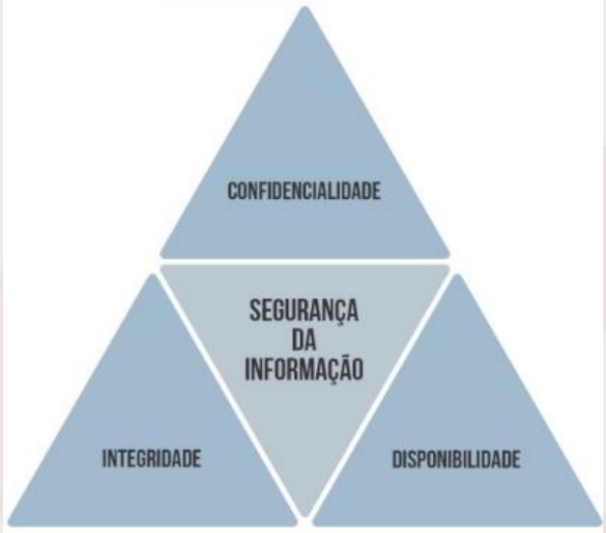
Confidencialidade é a garantia que a informação seja acessada ou manipulada apenas por entidades autorizadas (pessoas ou processos). Então, quando se busca confidencialidade, busca-se restrição.

Integridade é a garantia de que a informação seja mantida com todas as suas características originais ou modificadas somente pelas partes autorizadas. Por vezes, pensa-se que integridade está relacionada somente a não alteração da informação. Esse pensamento não é adequado: informação pode ser alterada e, ainda assim, manter-se íntegra, desde que a alteração tenha sido realizada por parte autorizada – quando é realizada por parte não autorizada, verifica-se um ataque direto à integridade da informação.

Disponibilidade é a garantia de que a informação esteja sempre disponível a quem de direito, sempre que preciso. Observa-se a restrição se junta à disponibilidade; desse modo, se um usuário não tem acesso a um determinado serviço ou sistema, em que é exemplo um serviço de Wi-Fi, ele não pode afirmar que houve um ataque à disponibilidade, porque nunca teve direito àquele serviço.

20m

Confidencialidade, integridade e disponibilidade compõem a tríade ou o triângulo da Segurança da Informação.



Triângulo da Segurança da Informação

Importa destacar a sigla em inglês para as propriedades da tríade: CIA – *Confidentiality, Integrity and Availability*. A letra "A" da sigla inglesa não diz respeito à autenticidade, mas sim à disponibilidade, cujo signo em inglês é "availability".

Mais duas propriedades merecem destaque.

Autenticidade é a garantia que a informação seja proveniente da fonte indicada.

Por fim, não repúdio ou irretratabilidade é a garantia de que o emissor não poderá negar a autoria de uma informação.

Ataques aos fluxos de informação

15m

A informação circula dentro de uma organização ou mesmo fora de uma organização. Segue um fluxo normal, em que a fonte de informação (A) envia determinada informação ao destino da informação (B).

No entanto, esse fluxo de informação pode sofrer ataques.

Quando o fluxo de informação de A para B é interceptado, tem-se um ataque direto à propriedade da confidencialidade, uma vez que somente B deveria ter acesso à informação interceptada.

Quando o fluxo de informação de A para B é interrompido, tem-se um ataque à propriedade da disponibilidade, porque o envio não foi concluído.

Quando o fluxo de informação de A para B é interceptado, modificado e enviado para B, respectivamente, verifica-se uma modificação. Nesse caso, observa-se um ataque à confidencialidade, à integridade e à autenticidade da informação.

Quando o fluxo de informação é iniciado por um terceiro, e não por A, e a informação é enviada para B, verifica-se uma fabricação, que fica configurada como um ataque à autenticidade, visto que o terceiro que envia a informação para B se passa por A.

DIRETO DO CONCURSO

1. (Ano: 2019 Banca: IADES Órgão: CRF-TO Prova: IADES - 2019 - CRF-TO - Analista de TI) Um programa de segurança deve seguir os três princípios de segurança conhecidos como CIA. Quais são esses princípios?

   a. Confidencialidade, interação e artifícios.

   b. Confidencialidade, integridade e disponibilidade.

ANOTAÇÕES

c. Montagem, infalibilidade e segurança.
d. Contenda, inatividade e arguição.
e. Concretude, inerência e disponibilidade.

COMENTÁRIO

A sigla inglesa CIA refere-se a “confidentiality”, “integrity” e “availability”. Em português, as propriedades são, respectivamente, confidencialidade, integridade e disponibilidade.

30m

2. (Ano: 2018 Banca: CESPE / CEBRASPE Órgão: CGM de João Pessoa - PB Prova: CESPE - 2018 - CGM de João Pessoa - PB - Auditor Municipal de Controle Interno - Desenvolvimento de Sistemas) Acerca de integridade, disponibilidade e confidencialidade em segurança da informação, julgue o item a seguir.
A disponibilidade pressupõe que uma informação deva estar disponível a qualquer pessoa de direito, sempre que necessário.

COMENTÁRIO

O princípio da disponibilidade implica que uma informação deve estar disponível a qualquer pessoa que esteja devidamente autorizada a acessar essa informação, sempre que desejar.

3. (Ano: 2018 Banca: CESPE / CEBRASPE Órgão: CGM de João Pessoa - PB Prova: CESPE - 2018 - CGM de João Pessoa - PB - Auditor Municipal de Controle Interno - Desenvolvimento de Sistemas) Acerca de integridade, disponibilidade e confidencialidade em segurança da informação, julgue o item a seguir.
A integridade, propriedade da segurança da informação, garante que uma informação ou um dado não seja alterado por pessoa ou processo não autorizado.

COMENTÁRIO

Integridade diz respeito à manutenção adequada da informação, de modo que a informação não seja modificada ou que seja modificada por pessoa ou processo autorizado para tanto.

ANOTAÇÕES

4. (Ano: 2021 Banca: FGV Órgão: IMBEL Prova: FGV - 2021 - IMBEL - Analista Especializado - Analista de Sistemas - Reaplicação) Segundo padrões internacionais, a Segurança da Informação distingue quatro atributos básicos que orientam a implementação de políticas e procedimentos de proteção. Assinale o atributo que não é parte desse grupo.
   a. A) Autenticidade.
   b. B) Confidencialidade.
   c. C) Disponibilidade.
   d. D) Flexibilidade.
   e. E) Integridade.

COMENTÁRIO

Dentre os atributos, merecem destaque, respectivamente, a confidenciabilidade, a integridade, a disponibilidade – que compõem a tríade – e a autenticidade.

GABARITO

1. b
2. C
3. C
4. d

ANOTAÇÕES