Navegação do teste

1 2 3 4 5 6

Terminar revisão

Iniciada	quinta, 22 de abril de 2021 às 18:35
Estado	Terminada
Terminada em	quinta, 22 de abril de 2021 às 20:03
Tempo gasto	1 hora 28 minutos

Pergunta 1
Respondida
Nota: 1,00
Marcar pergunta

Questão 1 / Question 1 (10%) (max. 15 linhas)
Explique o é um verme (worm), como se propaga e como se pode proteger. Sustente as suas afirmações com exemplos concretos deste malware.

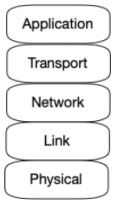
Explain what is a worm, how does it spread and how can we protect from it. Include real world examples that sustain your statements.

Um verme (worm) é um programa do tipo malware (de intenções geralmente maliciosas).
Tem a função de se propagar, replicando-se de computador para computador. A propagação pode ser feita fisicamente ou virtualmente, isto é.
- Na propagação física, o worm pode espalhar-se, por exemplo, usando dispositivos USB considerando que o mesmo está programado para quebrar alguma falha de segurança do dispositivo host.
- Enquanto que, na propagação virtual, este infeta outros hosts criando cadeias automatizadas usando serviços na rede (local ou externa), como por exemplo, documentos e emails.
Uma das maneiras como nos podemos proteger, que abrange os dois métodos, é a utilização de um programa anti-malware e o mesmo esteja atualizado. Uma técnica para proteger o equipamento fisicamente, é proibir o uso de dispositivos USB não autorizados. Um exemplo real é o worm Stuxnet que propagava por USB e tinha como alvo uma base no Irão que continha uranio. Outra técnica, esta para proteger virtualmente, é não abrir documentos de fontes não fedignas. Um exemplo real é a worm ILOVEYOU (Love Bug), que infetou milhões de computadores ao espalhar um email com um ficheiro mailicioso.

Pergunta 2
Respondida
Nota: 1,00
Marcar pergunta

Questão 2 / Question 2 (15%) (max. 40 linhas)
Considere as camadas do protocolo TCP/IP. Para cada uma delas identifique, em termos de segurança informática, o seguinte:
1) 2 possíveis fragilidades
2) 2 possíveis ataques informáticos
3) 2 possíveis contra-medidas para proteger

Consider the TCP/IP protocol layers. For each of that layers identify, in terms of informatics security, the following:



APPLICATION
- Um possível ataque é o DoS (Denial of Service), um ataque que se baseia na injeção de informação a mais

TRANSPORT
- Um possível ataque é o 'Port Scanning'

Pergunta 3
Respondida
Nota: 1,00
Marcar pergunta

Questão 3 / Question 3 (25%) (max. 40 linhas)
Explique o que é o ciclo PDCA e em que medida é usado no âmbito do ISO 27000. Desenvolva de forma a abranger o enquadramento deste ciclo no âmbito do referido standard, sustentando as suas afirmações com exemplos concretos.

Explain what is the PDCA cycle and how it is used in the ISO 27000 standard. Explain how does this cycle fits into the standard with real examples that will sustain your statements.

O ciclo PDCA (plan-do-check-act) é um método de gestão de quatro passos. Este é usado para continuamente controlar e melhorar processos e produtos.
No caso do standard ISO 27000 com o ciclo PDCA, este baseia-se em quatro fases, sendo estas repetidas até que uma solução seja desenvolvida que cumpra os critérios atuais.
Na primeira (PLAN), é estabelecer, caso não exista, um SGSI (Sistema de Gestão de Segurança da Informação) com base na motivação e âmbito a aplicar à organização. Para de seguida, definir políticas de segurança e abordagens de análise/avaliação de riscos para a organização e assim conseguir identificar, bem como analisar/avaliar os mesmos. Após a análise e identificação de riscos, será necessário também identificar e avaliar opções para os tratar, bem como definir objetivos de controlo para esse tratamento. Sendo que, desta maneira, todo o planeamento fica realizado, para que se possa avançar para a fase seguinte.
A segunda fase (DO), trata de formular e implementar um plano de tratamento de riscos (PTR), implementando todos os controlos selecionados na primeira etapa. Assim definindo como será feita a medição da eficácia desses mesmos controlos. Por fim, implementando procedimentos e controlos capazes de permitir a deteção imediata de eventos de segurança e resposta a incidentes, ambos específicos à informação presente da organização. Desta maneira, os empregados (staff) fica prevenidos com as medidas especificadas, para minimizar (sendo impossível impossibilitar) futuras falhas.
A terceira fase (CHECK), é responsável por estabelecer procedimentos de monitorização crítica. As análises (monitorizações), estão apontadas à eficácia do SGSI para verificar se os requisitos de segurança da informação foram cumpridos. Assim, será possível analisar essas monitorizações para confirmar se estão dentro dos níveis de risco aceitáveis. Para que, caso apareçam anomalias/irregularidades, sejam mais facilmente detetadas por auditorias internas do SGSI em intervalos planeados (ou até mesmo auditorias de certificação). E em casos "positivos", estes sejam registados, visto a ação/evento em questão poderá ter tido impacto no desempenho do SGSI.
E por fim, caso o ciclo não repita, temos a quarta fase (ACT), que serve para implementar melhorias identificadas no SGSI. Bem como executar ações preventivas adequadas, juntamente com a comunicação de melhorias aos membros apropriados. Para que se possa assegurar que as melhorias atinjam os objetivos pretendidos.

Pergunta 4
Respondida
Nota: 1,00
Marcar pergunta

Questão 4 / Question 4 (10%) (max. 15 linhas)
Explique o que é um ataque por reconhecimento e em que medida ele pode ser um perigo para a nossa organização. Em que medida este ataque se relaciona com um ataque por acesso?

Explain what is an reconnaissance attack and why is it a problem for our organization. How does it relates to the access attack?

Um ataque por reconhecimento, é um método de recolha de informação, na maior parte dos casos, geral. Mais especificamente, é um dos primeiros métodos que se deve usar em ataques, por ser muito abrangente.
Este tipo de ataque é um perigo para a nossa organização visto ter a possibilidade de descobrir potenciais falhas de segurança que o atacante desconheça, ou que sejam comuns. Visto abranger ambas as camadas físicas e virtuais de segurança (por exemplo, vigilância presencial e ataques de 'social engineering' que equivalem às duas camadas respetivamente).
Este ataque é semelhante ao ataque por acesso, visto que o de reconhecimento, após a recolha inicial de informação, pode usar a mesma para realizar um ataque por acesso (aceder a uma conta de utilizador local), ou até mesmo, para recolher mais informação (usando-a para chantagear elementos da nossa organização).

Pergunta 5
Não respondida
Nota: 1,00
Marcar pergunta

Questão 5 / Question 5 (15%) (max. 15 linhas)
Explique o que contemplam os atributos de segurança confidencialidade e não repúdio. Identifique 2 exemplos concretos para cada um dos atributos, clarificando os problemas, como podem ser explorados e como se podem proteger.

Explain what is it about the attributes confidentiality and no repudiation. Identify, for each one, 2 real world examples, their problems, how they can be explored by malicious attckers and how can we tackle them.

Pergunta 6
Respondida
Nota: 1,00
Marcar pergunta

Questão 6 / Question 6 (25%) (max. 40 linhas)
Explique o que é a catalogação AVOIDIT, em que medida é importante para a segurança informática e de que forma pode ser implementada na nossa organização. Sustente as suas afirmações com exemplos concretos.

Explain what is the AVOIDIT catalog, why is it important for the informatics security and how can it be implemented in our organization. Integrate in our statements real world examples that sustain your affirmations.

A catalogação AVOIDIT é uma técnica de identificação e defesa contra ciber ataques, constituída por diferentes categorias para mais rapidamente atribuir o termo correto ao ataque e identificar futuros eventos do mesmo.
Esta medida é importante para a segurança informática visto facilitar a deteção de ataques já registados e assim habilitar o começo de medidas de contra-ataque/preventivas.
Esta catalogação pode ser implementada na nossa organização inicialmente, pela recolha de informação de ataques passados (dentro e fora da empresa) e previamente atualizada a partir de relatórios de ataques que tenham acontecido recentemente.
Desta forma, será possível treinar o 'staff' seguindo o ciclo PDCA, bem como re-configurar quaisquer equipamentos/serviços de modo a prevenir e proteger contra futuros ataques.

Terminar revisão

« PREVIOUS ACTIVITY
Enunciado Trabalho Prático / Assignment description

Ir para...

Obter a Aplicação móvel