IPBeja

INSTITUTO POLITÉCNICO DE BEJA

Fundamentos de Segurança Informática

Trabalho Individual

Gonçalo Amaro – 17440

11 de Dezembro, 2022

Lista de Abreviaturas

APT Advanced Persistent Threats
IEC International Electrotechnical Commission
IOA Indicadores de Ataque
IOC Indicadores de Comprometimento
ISO International Organization for Standardization
IT Informations Technologies
NIST National Institute of Standards and Technology
TI Tecnologias de Informação

Conteúdo

Introdução

1.1 Introdução ao trabalho

Este trabalho tem como objetivo a pesquisa e sintetização do tópico de "Fundamentos de Cibersegurança", que está inserido no módulo de "Fundamentos de Cibersegurança" do curso de "Engenharia de Segurança Informática" do Instituto Politécnico de Beja.

Em suma, este consiste na resolução de um conjunto de exercícios de pesquisa e sintetização de conteúdos enquadrados nas perguntas inseridas no documento de enunciado.

Perguntas do Grupo 1

2.1 Pesquise, enumere e argumente sobre "Vetores de Ataque" no âmbito da Cibersegurança.

Os vetores de ataque são um conceito crítico na segurança cibernética porque fornecem uma maneira de os invasores obterem acesso a um sistema de computador ou rede. Existem muitos tipos diferentes de vetores de ataque que os invasores podem usar, e entender essas ameaças é essencial para que as organizações se protejam contra elas.

Um tipo comum de vetor de ataque é um ataque de *phishing*. Em um ataque de *phishing*, o invasor envia um e-mail ou outra mensagem que parece ser de uma fonte legítima, como um banco ou outra empresa conhecida. A mensagem geralmente inclui um link ou anexo no qual o usuário é incentivado a clicar. Se o usuário cair no golpe e clicar no link ou abrir o anexo, ele pode ser levado a um site falso que parece real, mas na verdade é controlado pelo invasor. O usuário pode ser solicitado a inserir informações confidenciais (como credenciais de login) no site falso, que o invasor pode usar para obter acesso às contas do usuário.

Outro tipo de vetor de ataque é o malware. Malware é um software projetado especificamente para danificar ou interromper um sistema de computador. Existem muitos tipos diferentes de malware, incluindo vírus, worms e ransomware. O malware pode ser distribuído por meio de uma variedade de vetores de ataque, incluindo anexos de e-mail, sites maliciosos e unidades USB infetadas. Depois que o malware é instalado no sistema, ele pode executar uma ampla variedade de ações, como excluir arquivos, roubar informações confidenciais ou assumir o controle do sistema.

Ataques de engenharia social são outro tipo comum de vetor de ataque. Em um ataque de engenharia social, o invasor usa manipulação psicológica para induzir o usuário a divulgar informações confidenciais ou realizar uma determinada ação. Isso pode incluir táticas como fingir ser um representante de atendimento ao cliente de uma empresa conhecida ou ligar para o usuário e alegar ser do banco. O invasor pode usar várias táticas para tentar ganhar a confiança do usuário, como fornecer informações convincentes ou criar um senso de urgência. Uma vez que o usuário foi induzido a fornecer ao invasor informações confidenciais, o invasor pode usar essas informações para obter acesso às contas ou sistemas do usuário.

***Exploits* são outro tipo de vetor de ataque que os invasores podem usar.** Um *exploit* é um pedaço de software ou código que tira proveito de uma vulnerabilidade em um sistema (como software sem patch) para obter acesso não autorizado. Por exemplo, se um sistema tiver uma vulnerabilidade conhecida que permite que um invasor obtenha acesso sem uma senha, um invasor pode usar um *exploit* para tirar proveito dessa vulnerabilidade e obter acesso ao sistema.

Por fim, o acesso físico é outro tipo de vetor de ataque que os invasores podem usar. Em um ataque de acesso físico, o invasor obtém acesso físico a um computador ou rede para contornar as medidas de segurança e obter acesso ao sistema. Por exemplo, um invasor pode roubar um laptop do escritório de um funcionário ou obter acesso a uma sala de servidores fingindo ser um funcionário da manutenção. Uma vez que o invasor tenha acesso físico ao sistema, ele pode usá-lo para obter acesso à rede e roubar informações confidenciais.

2.1.1 Pesquise, enumere e argumente sobre "Vulnerabilidades" no âmbito da Cibersegurança.

Vulnerabilidades de segurança cibernética referem-se a pontos fracos ou falhas em sistemas de computador, redes ou software que podem ser explorados por invasores para obter acesso não autorizado ou realizar atividades maliciosas. Existem vários tipos de vulnerabilidades que podem existir em um sistema de segurança cibernética, incluindo:

- **Vulnerabilidades de software:** são falhas ou pontos fracos em programas de software que podem ser explorados por invasores para obter acesso a um sistema ou realizar atividades maliciosas. Exemplos de vulnerabilidades de software incluem estouros de buffer, falhas de injeção de SQL e brechas de segurança não corrigidas.
- **Vulnerabilidades de hardware:** são falhas ou pontos fracos em dispositivos de hardware, como roteadores, servidores e outros dispositivos de rede, que podem ser explorados por invasores para obter acesso a um sistema ou rede. Exemplos de vulnerabilidades de hardware incluem senhas fracas ou padrão, pontos de acesso físicos não seguros e protocolos de segurança inadequados.
- **Vulnerabilidades de rede:** são falhas ou fraquezas em uma rede que podem ser exploradas por invasores para obter acesso a um sistema ou rede. Exemplos de vulnerabilidades de rede incluem redes sem fio não seguras, configurações de rede mal configuradas e protocolos inseguros.
- **Vulnerabilidades humanas:** são vulnerabilidades que surgem das ações ou comportamentos dos indivíduos dentro de uma organização. Exemplos de vulnerabilidades humanas incluem senhas fracas, manuseio descuidado de informações confidenciais e cair em golpes de phishing.

É importante identificar e lidar com essas vulnerabilidades para proteger contra ataques cibernéticos e manter a segurança dos sistemas de computador, redes e software. Ao implementar fortes medidas de segurança, corrigir e atualizar regularmente o software e fornecer treinamento e educação aos usuários, as organizações podem reduzir sua exposição a vulnerabilidades de segurança cibernética e se proteger contra possíveis ataques.

2.2 Apresente o Projeto ATT&CK do Mitre; qual a sua relevância no âmbito da Cibersegurança e do Combate ao Cibercrime, relativamente aos Grupos de atacantes de eu forma este Projeto pretende contribuir para a identificação dos atacantes: escolha ainda um Grupo enunciado e apresente-o, justifique a escolha desse Grupo.

O projeto *Adversarial Tactics, Techniques, and Common Knowledge* (ATT&CK) da MITRE Corporation é uma estrutura abrangente para entender as táticas, técnicas e procedimentos (TTPs) usados por adversários em ataques cibernéticos. Desenvolvido pela organização sem fins lucrativos MITRE, que opera centros de pesquisa e desenvolvimento para o governo dos EUA, o projeto ATT&CK é uma base de conhecimento disponível publicamente que fornece informações detalhadas sobre as táticas e técnicas usadas por diferentes grupos adversários.

O projeto ATT&CK é relevante para a segurança cibernética porque fornece uma linguagem comum e uma compreensão das diferentes maneiras pelas quais os invasores podem operar, o que pode ajudar as organizações a se defenderem desses ataques. Ao fornecer informações detalhadas sobre as táticas e técnicas utilizadas por diferentes grupos adversários, o projeto ATT&CK permite que as organizações entendam melhor a ameaça específica que estão enfrentando e melhorem suas defesas contra esses ataques.

Uma das principais características do projeto ATT&CK é seu foco em diferentes grupos de invasores, conhecidos como "grupos adversários". Esses grupos são definidos com base nas táticas e técnicas que eles usam em seus ataques e fornecem uma maneira para as organizações entenderem a ameaça específica que estão enfrentando. Por exemplo, o APT1, também conhecido como *"Comment Crew"*, é um grupo de hackers patrocinado pelo estado Chinês que está ativo desde pelo menos 2006. Esse grupo é conhecido por usar uma ampla gama de táticas, incluindo *spearphishing*, malware e rede exploração, para realizar espionagem cibernética e roubo de propriedade intelectual.

Outro grupo que está incluído no projeto ATT&CK é o APT29, também conhecido como *"The Dukes"* ou *"Cozy Bear"*. Acredita-se que esse grupo esteja associado a atividades de espionagem cibernética patrocinadas pelo estado Russo e esteja ativo desde pelo menos 2008. O APT29 é conhecido por usar ferramentas e técnicas sofisticadas, incluindo ferramentas de hacking personalizadas e malware, para comprometer seus alvos.

A escolha sobre esses dois grupos para o exemplo dá-se ao facto que são grupos suportados e patrocinados por Estados, o que aumenta o meu fascínio pessoal sobre as suas ações e torna a sua ameaça mais perigosa e mais difícil de combater, visto que os Estados têm recursos financeiros e humanos para desenvolver e implementar estratégias de ataque ultra sofisticadas e complexas como também garantir a sua proteção e anonimato. Torna-se difícil para as organizações privadas e governamentais combaterem esses grupos.

Além de fornecer informações sobre grupos adversários, o projeto ATT&CK também inclui descrições detalhadas das táticas e técnicas que esses grupos utilizam em seus ataques. Por exemplo, o projeto inclui informações sobre táticas como *spearphishing* e malware, bem como técnicas como exploração de rede e quebra de senha. Ao fornecer essas informações detalhadas, o projeto ATT&CK permite que as organizações entendam melhor as táticas e técnicas específicas que diferentes grupos adversários usam e desenvolvam defesas eficazes contra esses ataques.

No geral, o projeto MITRE ATT&CK é um recurso valioso para organizações que buscam melhorar suas defesas contra ataques cibernéticos. Ao fornecer informações detalhadas sobre táticas, técnicas e procedimentos usados por diferentes grupos adversários, o projeto ATT&CK permite que as organizações entendam melhor as ameaças específicas que enfrentam e desenvolvam defesas eficazes contra esses ataques.

Perguntas do Grupo 2

3.1 Tendo em conta o "tempo tríbulo" (perceber o passado, para planear o presente e projetar o futuro) como se relaciona esse tempo com a análise de risco e como pode esta ser enriquecida?

O "tempo da tribulação" que você mencionou não é um termo normalmente usado no campo da segurança cibernética. No contexto da análise de risco, é importante considerar o passado para identificar ameaças e vulnerabilidades potenciais e usar essas informações para planear e mitigar riscos potenciais no presente e no futuro. Isso pode ser enriquecido com a realização de avaliações de risco completas e regulares, mantendo-se atualizado com os últimos desenvolvimentos e melhores práticas no campo da segurança cibernética e implementando medidas de segurança eficazes para proteger contra ameaças potenciais.

A frase "compreender o passado, planear o presente e projetar o futuro" está relacionada à análise de risco em segurança cibernética na medida em que enfatiza a importância de considerar o passado para informar a tomada de decisões no presente e no futuro. No contexto da segurança cibernética, observar incidentes e tendências de segurança anteriores pode ajudar as organizações a entender os tipos de ameaças que podem enfrentar e pode informar seu planeamento e tomada de decisão sobre a implementação de medidas de segurança para proteção contra essas ameaças.

Por exemplo, se uma organização sofreu uma violação de dados no passado, ela pode analisar a causa dessa violação e tomar medidas para evitar que incidentes semelhantes ocorram no futuro. Isso pode envolver a implementação de novas medidas de segurança, como senhas mais fortes ou autenticação de dois fatores, ou a atualização de seus protocolos de segurança para melhor proteção contra possíveis ameaças. Ao entender o passado e usar essas informações para informar seu planeamento presente e futuro, as organizações podem se proteger melhor contra possíveis ameaças e melhorar sua postura geral de segurança.

A análise de risco é um componente crítico da segurança cibernética eficaz, pois envolve a identificação e avaliação de possíveis ameaças e vulnerabilidades e a adoção de medidas para mitigar ou eliminar esses riscos. O objetivo da análise de risco é garantir a segurança e a integridade dos sistemas e dados de uma organização e proteger contra ameaças potenciais, como ataques cibernéticos, violações de dados e outros incidentes de segurança.

Para realizar uma análise de risco completa, é importante considerar o passado, o presente e o futuro. Isso significa observar os incidentes de segurança anteriores e suas causas, bem como as tendências e desenvolvimentos atuais no campo da segurança cibernética. Ao fazer isso, as organizações podem entender melhor os tipos de ameaças que podem enfrentar e podem tomar medidas para prevenir ou mitigar esses riscos.

Um aspeto fundamental da análise de risco é a identificação de vulnerabilidades potenciais. Isso pode incluir pontos fracos na infraestrutura de segurança de uma organização, como software desatualizado ou senhas fracas, bem como possíveis lacunas em protocolos ou políticas de segurança. Ao identificar essas vulnerabilidades, as organizações podem tomar medidas para resolvê-las e melhorar sua postura geral de segurança.

Uma vez identificadas as vulnerabilidades potenciais, é importante avaliar o impacto potencial dessas vulnerabilidades. Isso pode envolver a análise da probabilidade de uma ameaça em potencial, bem como as possíveis consequências se essa ameaça se materializar. Ao compreender o impacto potencial de uma ameaça, as organizações podem priorizar seus esforços e recursos para se concentrar nos riscos mais críticos.

Uma vez que os riscos tenham sido identificados e avaliados, as organizações podem tomar medidas para mitigar ou eliminar esses riscos. Isso pode envolver a implementação de novas medidas de segurança, como firewalls ou sistemas de deteção de intrusão, ou a atualização de políticas e protocolos de segurança

existentes. Também pode envolver o treinamento de funcionários sobre as melhores práticas de segurança cibernética, como a importância de senhas fortes e a necessidade de estar atento a possíveis golpes de phishing.

Em conclusão, a análise de risco é um componente crítico da segurança cibernética eficaz e envolve considerar o passado, o presente e o futuro para identificar e mitigar riscos potenciais. Ao realizar avaliações de risco completas e regulares, mantendo-se atualizado com os últimos desenvolvimentos no campo e implementando medidas de segurança eficazes, as organizações podem se proteger contra ameaças potenciais e manter a segurança e a integridade de seus sistemas e dados.

3.2 Atualmente, na actual da ISO 27002. quantos são e quais são, os pilares da Segurança da Informação?

O padrão **ISO/IEC 27002** é um padrão internacional amplamente reconhecido que fornece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar o gestão de segurança da informação em uma organização. Faz parte da família de normas **ISO/IEC 27000**, que é uma série de normas que fornecem diretrizes, melhores práticas e princípios gerais para o gestão da segurança da informação.

Foi publicado pela primeira vez em 1995 como ISO/IEC 17799, e foi revisado e renomeado como **ISO/IEC 27002** em 2013. O padrão é baseado no Código de Prática para Gestão de Segurança da Informação, desenvolvido pela Organização Internacional de Normalização (ISO) e Comissão Eletrotécnica Internacional (IEC).

Este fornece uma estrutura para as organizações usarem ao desenvolver e implementar políticas e controles de segurança da informação. O padrão é baseado no princípio de que a segurança da informação deve ser integrada ao gestão geral de uma organização, em vez de ser tratada como uma preocupação separada.

Está dividido em duas secções principais. A primeira secção fornece uma visão geral do gestão de segurança da informação e os princípios que devem ser seguidos ao implementar controles de segurança da informação. A segunda secção fornece uma descrição detalhada dos dez pilares da estrutura **ISO/IEC 27002**, que são projetados para fornecer uma abordagem abrangente para o gestão da segurança da informação.

É apenas um dos vários padrões que fazem parte da família **ISO/IEC 27000**. A família de padrões **ISO/IEC 27000** fornece diretrizes, melhores práticas e princípios gerais para o gestão de segurança da informação. Alguns dos outros padrões da família **ISO/IEC 27000** incluem:

- **ISO/IEC 27001:** Esta norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI).
- **ISO/IEC 27003:** Esta norma fornece orientação sobre a implementação de um SGSI baseado na **ISO/IEC 27001**.
- **ISO/IEC 27004:** Esta norma fornece diretrizes para a medição e avaliação da eficácia de um SGSI.
- **ISO/IEC 27005:** Esta norma fornece orientação sobre o gestão de riscos de segurança da informação com base na **ISO/IEC 27001**.
- **ISO/IEC 27006:** Esta norma especifica os requisitos para organizações que fornecem certificação de ISMSs com base na **ISO/IEC 27001**.
- **ISO/IEC 27007:** Esta norma fornece diretrizes para auditoria de sistemas de gestão de segurança da informação.
- **ISO/IEC 27008:** Esta norma fornece diretrizes para a implementação de controles de segurança da informação em serviços de terceiros de processamento de informações.
- **ISO/IEC 27010:** Este padrão fornece orientação sobre a coordenação da segurança da informação em organizações que possuem vários ISMSs.

Esses padrões são projetados para ajudar as organizações a implementar sistemas eficazes de gestão de segurança da informação e para fornecer uma estrutura e terminologia comuns para o gestão de segurança da informação. Juntos, os padrões da família **ISO/IEC 27000** fornecem uma abordagem abrangente para gerir a segurança da informação e são amplamente utilizados por organizações em todo o mundo.

Este padrão, **ISO/IEC 27002**, contrasta o padrão **ISO/IEC 27001**, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI). O padrão **ISO/IEC 27002** fornece orientação sobre como implementar controles de segurança da informação em uma organização e é uma estrutura amplamente utilizada para estabelecer, implementar, manter e melhorar continuamente a gestão de segurança da informação dentro de uma organização. A norma fornece um conjunto de diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização.

A norma é dividida em três grupos principais: **áreas, princípios e pilares.**

As **áreas** do padrão **ISO 27002** abrangem as principais áreas de preocupação com a segurança da informação, incluindo segurança humana, segurança física e segurança lógica (também conhecida como segurança cibernética).

A segurança humana abrange medidas para proteger os indivíduos dentro de uma organização de possíveis ameaças à sua segurança, como assédio, intimidação ou outras formas de abuso.

A segurança física envolve medidas para proteger os ativos físicos de uma organização, como seus prédios, equipamentos e data centers, contra possíveis ameaças. A segurança física pode ser dividida em medidas ativas e passivas. Medidas ativas são aquelas que protegem ativamente contra ameaças, como guardas de segurança e câmaras de vigilância. Medidas passivas são aquelas que protegem contra ameaças sem fazê-lo ativamente, como fechaduras e cercas.

A segurança lógica, também conhecida como segurança cibernética, abrange medidas para proteger as informações e os sistemas de uma organização contra possíveis ameaças. Isso inclui medidas como *firewalls*, criptografia e políticas de senha segura.

Os **princípios** do padrão **ISO 27002** são as diretrizes subjacentes para estabelecer e manter a segurança da informação dentro de uma organização. Existem quatro princípios principais: confidencialidade, disponibilidade, integridade e não-repúdio.

Confidencialidade refere-se à proteção de informações confidenciais contra divulgação não autorizada. Isso significa que apenas indivíduos autorizados devem ter acesso a informações confidenciais e que as informações devem ser mantidas em segredo, a menos que haja um motivo legítimo para compartilhá-las.

Disponibilidade refere-se à capacidade de indivíduos autorizados de acessar informações e sistemas quando necessário. Isso significa que as informações e os sistemas devem estar disponíveis e funcionando o tempo todo, a menos que haja um motivo legítimo para sua indisponibilidade.

Integridade refere-se à precisão e integridade das informações. Isso significa que as informações devem ser precisas, completas e atualizadas em todos os momentos, e que quaisquer alterações nas informações devem ser feitas de maneira controlada e autorizada.

O não-repúdio refere-se à capacidade de provar que uma determinada ação foi realizada por um indivíduo específico. Isso é importante nos casos em que a autenticidade de uma ação, como enviar um e-mail ou fazer uma transação financeira, precisa ser verificada. A perícia digital desempenha um papel no não repúdio, ajudando a identificar o indivíduo responsável por uma determinada ação.

Os **pilares** da norma **ISO 27002** são os quatro principais componentes de um sistema eficaz de gestão de segurança da informação. Esses pilares são tecnologia, pessoas, segurança física e organização.

Tecnologia refere-se às ferramentas e sistemas usados para proteger as informações e os sistemas de uma organização contra ameaças potenciais. Isso inclui hardware e software, como firewalls, sistemas de deteção de intrusão e algoritmos de criptografia.

As pessoas referem-se aos indivíduos dentro de uma organização que são responsáveis pela implementação e manutenção da segurança da informação. Isso inclui funcionários, contratados e provedores de serviços de terceiros que têm acesso a informações ou sistemas confidenciais.

A segurança física refere-se às medidas em vigor para proteger os ativos físicos de uma organização, conforme discutido acima. Isso inclui medidas ativas e passivas, como guardas de segurança e fechaduras.

Organização refere-se aos procedimentos e processos em vigor para garantir que a segurança da informação seja efetivamente gerida dentro de uma organização. Isso inclui políticas, padrões e diretrizes para segurança da informação, bem como as funções, responsabilidades e treinamento dos indivíduos envolvidos na segurança da informação.

3.3 Cada Pilar da Segurança da Informação tem um conjunto de subprincípios; enuncie os mesmos.

A norma **ISO 27002** divide a segurança da informação em quatro pilares principais: tecnologia, pessoas, segurança física e organização. Cada pilar possui um conjunto de subprincípios que fornecem diretrizes mais específicas para implementar e manter a segurança da informação dentro de uma organização.

O pilar de tecnologia inclui os seguintes subprincípios:

- **Política de segurança:** uma organização deve ter uma política de segurança por escrito que defina sua abordagem à segurança da informação e que seja revisada e atualizada regularmente.
- **Arquitetura de segurança:** uma organização deve ter uma arquitetura de segurança que defina os controles técnicos e as medidas implementadas para proteger suas informações e sistemas.
- **Gestão de ativos:** Convém que uma organização mantenha um registro de seus ativos, incluindo informações e sistemas, e deve revisar e atualizar regularmente o registo.
- **Controle de acesso:** uma organização deve ter controles de acesso para garantir que apenas pessoas autorizadas tenham acesso a informações e sistemas confidenciais.
- **Criptografia:** uma organização deve usar criptografia para proteger informações confidenciais, como encriptar dados em repouso e em trânsito.
- **Desenvolvimento e manutenção do sistema:** Uma organização deve ter processos em vigor para desenvolver e manter seus sistemas de informação, incluindo práticas de codificação segura e patches e atualizações regulares.
- **Gestão de vulnerabilidade técnica:** Uma organização deve ter processos em vigor para identificar, avaliar e mitigar vulnerabilidades técnicas em seus sistemas de informação.

O pilar de pessoas inclui os seguintes subprincípios:

- **Consciencialização e treinamento de segurança:** Convém que uma organização forneça conscienciali-zação e treinamento de segurança a seus funcionários, contratados e outros indivíduos com acesso a informações e sistemas confidenciais.
- **Segurança do pessoal:** Convém que uma organização tenha processos em vigor para verificar a identidade e os antecedentes de indivíduos com acesso a informações e sistemas confidenciais.
- **Gestão de incidentes de segurança:** Uma organização deve ter processos para detetar, responder e recuperar de incidentes de segurança.
- **Gestão de continuidade de negócios:** uma organização deve ter planos para manter as operações de negócios no caso de um desastre ou outra interrupção.

O pilar de segurança física inclui os seguintes subprincípios:

- **Política de segurança física:** uma organização deve ter uma política de segurança física por escrito que defina sua abordagem para proteger seus ativos físicos e que seja revisada e atualizada regularmente.
- **Perímetro de segurança física:** Uma organização deve ter um perímetro de segurança física que defina os limites de sua área protegida e que seja protegida por medidas apropriadas, como cercas, portões e guardas de segurança.
- **Controle de acesso físico:** Convém que uma organização tenha processos para controlar o acesso a suas instalações e ativos físicos, como por meio do uso de cartões de acesso e crachás de segurança.
- **Segurança física dos ativos:** uma organização deve ter medidas para proteger seus ativos físicos de ameaças potenciais, como fechaduras, alarmes e câmaras de vigilância.

O pilar da organização inclui os seguintes subprincípios:

- **Conformidade legal:** uma organização deve cumprir todas as leis e regulamentos relevantes relacionados à segurança da informação.
- **Avaliação e gestão de riscos:** uma organização deve avaliar regularmente seus riscos relacionados à segurança da informação e deve ter processos em vigor para gerir e mitigar esses riscos.
- **Relacionamento com fornecedores:** Convém que uma organização tenha processos para gerir seus relacionamentos com fornecedores e outros provedores de serviços de terceiros, incluindo a avaliação de suas práticas de segurança da informação.
- **Objetivos de segurança da informação:** Uma organização deve ter objetivos específicos, mensuráveis, atingíveis, relevantes e com prazos (SMART) relacionados à segurança da informação e deve monitorizar e relatar seu progresso para atingir esses objetivos.
- **Auditoria interna:** Uma organização deve ter uma função de auditoria interna que revise e avalie regularmente suas práticas de segurança da informação e faça recomendações para melhorias.
- **Revisão administrativa:** Uma organização deve ter um processo de revisão administrativa para garantir que seu sistema de gestão de segurança da informação seja eficaz e alinhado com as metas e objetivos gerais da organização.

3.4 Num incidente de Cibersegurança, em que medida os 'IOCs' e os 'IOAs' podem ser salvaguardados por uma intervenção digital forense? Havendo dois tipos de intervenção habituais (em linha e fora de linha) quais são os indicadores tipicamente recolhidos por um e por outro tipo de intervenção?

Em um incidente de segurança cibernética, indicadores de comprometimento (IOCs) e indicadores de ataque (IOAs) podem ser protegidos até certo ponto por meio de intervenção digital forense. A intervenção digital forense refere-se ao uso de técnicas forenses digitais para coletar, preservar e analisar evidências digitais após um incidente de segurança cibernética.

Existem dois tipos de intervenção digital forense: online e offline. A intervenção forense online envolve conduzir a investigação forense enquanto os sistemas afetados ainda estão online e conectados à rede. Isso permite que o investigador colete dados ao vivo e potencialmente interrompa o ataque em andamento. No entanto, também acarreta o risco de adulteração ou alteração das provas.

A intervenção forense offline envolve a condução da investigação forense depois que os sistemas afetados foram colocados offline e desconectados da rede. Isso permite que o investigador colete um conjunto de evidências mais completo e preciso, pois os sistemas não estão mais sendo atacados ativamente. No entanto, isso também significa que a investigação pode não ser capaz de interromper o ataque ou evitar mais danos.

Tanto na intervenção forense online quanto offline, o investigador geralmente coleta uma ampla gama de indicadores para ajudar a identificar a causa do incidente e as partes responsáveis. Isso pode incluir IOCs, como amostras de malware ou logs de tráfego de rede, bem como IOAs, como tentativas suspeitas de login ou exfiltração de dados.

Os indicadores específicos coletados durante uma intervenção digital forense dependerão do incidente específico e das ferramentas e técnicas utilizadas pelo investigador. Em geral, a intervenção forense online pode se concentrar na coleta de dados ao vivo, como tráfego de rede e logs do sistema, enquanto a intervenção forense offline pode se concentrar na coleta de artefactos dos sistemas afetados, como arquivos e chaves de registo.

No geral, a intervenção digital forense pode ajudar a proteger IOCs e IOAs, coletando e preservando evidências do incidente, que podem ser usadas para identificar a causa e as partes responsáveis. No entanto, a eficácia da intervenção dependerá do incidente específico, das habilidades e experiência do investigador e da disponibilidade de ferramentas e técnicas apropriadas.

3.4.1 Como estão relacionados os princípios da segurança da informação com a intervenção digital forense?

A intervenção digital forense está relacionada a dois dos quatro princípios da segurança da informação: integridade e não repúdio.

O princípio da integridade refere-se à precisão e integridade das informações. No contexto da intervenção digital forense, isto significa que as provas recolhidas durante a investigação devem ser precisas e completas, e que quaisquer alterações ou alterações às provas devem ser efetuadas de forma controlada e autorizada.

O princípio do não repúdio refere-se à capacidade de provar que uma determinada ação foi realizada por um indivíduo específico. No contexto da intervenção digital forense, isto significa que as provas recolhidas durante a investigação devem ser suficientes para identificar os responsáveis e provar o seu envolvimento no incidente.

Assim, seguindo os princípios de integridade e não repúdio, a intervenção forense digital pode ajudar a garantir que as evidências coletadas durante a investigação sejam precisas e completas, e que possam ser usadas para identificar os responsáveis e responsabilizá-los por seus atos.

3.5 Como desenharia e implementaria, de forma sucinta, mas fundamentada, uma ação de sensibilização numa entidade privada, tendo em conta os crimes (incidentes de Cibersegurança) que mais ocorrem na Europa?

Para desenhar e implementar uma campanha de sensibilização eficaz numa entidade privada, existem vários passos fundamentais que devem ser seguidos:

Identifique os incidentes de segurança cibernética mais comuns que ocorrem na Europa. Isso pode ser feito analisando relatórios e estudos sobre tendências de segurança cibernética na Europa, bem como consultando especialistas do setor e profissionais de segurança cibernética. Alguns dos tipos mais comuns de incidentes de segurança cibernética na Europa incluem ataques de phishing, infeções por malware e violações de dados.

Desenvolva uma campanha personalizada que aborde os riscos e vulnerabilidades específicos enfrentados pela organização. Isso deve ser feito em colaboração com o departamento de TI e a equipe de segurança cibernética da organização, que podem fornecer insights e conhecimentos valiosos sobre os desafios de segurança exclusivos da organização. A campanha deve ser projetada para educar e envolver os funcionários sobre a importância da segurança cibernética e fornecer a eles o conhecimento e as habilidades necessárias para proteger a si mesmos e à organização contra ataques.

Implemente a campanha usando uma variedade de atividades de consciencialização. A campanha pode incluir uma variedade de atividades de consciencialização, como:

- Fornecer treinamento e educação regulares aos funcionários sobre a importância da segurança cibernética e como proteger a si mesmos e à organização contra ataques.
- Partilhando exemplos de incidentes de segurança cibernética da vida real e as medidas tomadas para evitá-los.
- Destacando as possíveis consequências de não levar a segurança cibernética a sério, como perdas financeiras, danos à reputação e responsabilidades legais.
- Incentivar os funcionários a relatar quaisquer atividades suspeitas ou possíveis ameaças ao departamento de TI da organização ou à equipe de segurança cibernética.
- Além disso, eu me certificaria de monitorizar e avaliar regularmente a eficácia da campanha e fazer os ajustes necessários. Isso pode incluir a pesquisa de funcionários para avaliar sua compreensão da segurança cibernética e sua capacidade de identificar e prevenir ataques, bem como rastrear o número e os tipos de incidentes que ocorrem dentro da organização.

Monitorizar e avaliar a eficácia da campanha. Isso deve ser feito regularmente para garantir que a campanha esteja atingindo as metas e os objetivos pretendidos. Isso pode incluir a pesquisa de funcionários para avaliar sua compreensão da segurança cibernética e sua capacidade de identificar e prevenir ataques, bem como rastrear o número e os tipos de incidentes que ocorrem dentro da organização.

Além das etapas que mencionei anteriormente, existem várias outras considerações importantes ao projetar e implementar uma campanha de consciencialização em uma entidade privada:

Desenvolva uma mensagem clara e convincente que transmita a importância da segurança cibernética e motive os funcionários a agir. Esta mensagem deve ser simples, fácil de entender e relevante para a organização e seus funcionários. Também deve destacar as possíveis consequências de não levar a segurança cibernética a sério e fornecer etapas claras e acionáveis que os funcionários podem adotar para proteger a si mesmos e à organização.

Faça uso de canais de comunicação envolventes e eficazes para alcançar os funcionários. Isso pode incluir e-mail, midia social, boletins informativos, pósteres e outros materiais visuais. É importante escolher os canais de comunicação com maior probabilidade de alcançar e envolver os funcionários e usar uma combinação de canais para alcançar funcionários em diferentes locais, departamentos e cargos.

Incentive os funcionários a se apropriarem de sua própria segurança cibernética. Isso pode ser feito fornecendo treinamento e educação regulares sobre tópicos de segurança cibernética, bem como incentivando os funcionários a relatar quaisquer atividades suspeitas ou ameaças potenciais ao departamento de TI ou à equipe de segurança cibernética da organização. Ao capacitar os funcionários a assumir um papel ativo na proteção da organização contra ataques cibernéticos, as organizações podem construir uma postura de segurança mais forte e resiliente.

Envolva os líderes seniores e a gerência na campanha de consciencialização. Isso é importante porque os líderes e gerentes seniores podem desempenhar um papel crítico na consciencialização e compreensão da segurança cibernética em toda a organização. Ao envolvê-los na campanha e no planeamento e implementação de atividades de consciencialização, as organizações podem garantir que a segurança cibernética seja uma prioridade em todos os níveis da organização.

No geral, uma campanha de consciencialização eficaz pode ajudar a reduzir significativamente o risco de incidentes de segurança cibernética em uma entidade privada. Ao fornecer aos funcionários o conhecimento e as habilidades de que precisam para proteger a si mesmos e à organização contra ataques, as organizações podem melhorar sua postura geral de segurança e reduzir o impacto potencial de um ataque cibernético.

Conclusão

Em conclusão, a pesquisa e análise neste artigo mostraram que existem inúmeros vetores de ataque no âmbito da segurança cibernética. Esses vetores de ataque incluem técnicas como phishing, malware e engenharia social, que podem ser usadas por invasores para obter acesso a um sistema ou rede. O Projeto ATT&CK da Mitre é uma estrutura abrangente que visa identificar e classificar esses vetores de ataque e fornecer orientação sobre como se defender deles. O projeto é relevante no contexto da cibersegurança e do combate ao cibercrime porque ajuda as organizações a entender as táticas, técnicas e procedimentos utilizados por diferentes grupos de invasores.

Um grupo de invasores de particular interesse é o grupo APT *(Advanced Persistent Threat)*. Esse grupo é conhecido por sua capacidade de conduzir ataques furtivos e contínuos a um alvo, geralmente com o objetivo de extrair dados confidenciais. A escolha deste grupo justificou-se porque os ataques APT são muitas vezes difíceis de detetar e podem causar danos significativos a uma organização. Os exemplos de enitidades APT usados foram os grupos APT1 e APT29, que são conhecidos por seus ataques contra organizações governamentais e empresas privadas, com suporte e promoção de governos estrangeiros. A análise dos vetores de ataque e das técnicas de defesa do grupo APT1 e APT29 ajudou a identificar as principais táticas, técnicas e procedimentos utilizados por esses grupos e a fornecer orientação sobre como se defender deles.

Em termos de tempo de tribulação e análise de risco, é importante considerar o passado, o presente e o futuro ao avaliar a probabilidade e o impacto de possíveis incidentes de segurança. Ao entender as tendências e padrões de ataques anteriores, as organizações podem planear e se preparar melhor para possíveis ameaças futuras. Isso pode ajudar a enriquecer o processo de análise de risco e melhorar a postura geral de segurança de uma organização.

A versão atual da **ISO/IEC 27002** (2022) identifica quatro pilares da segurança de informação: Tecnologia, pessoas, segurança física e Organização. Cada pilar tem um conjunto de subprincípios que fornecem orientação sobre como implementar medidas de segurança eficazes nessa área.

Em um incidente de segurança cibernética, indicadores de comprometimento (IOCs) e indicadores de ataque (IOAs) podem ser fontes valiosas de informações para intervenções forenses digitais. Esses indicadores podem ajudar os investigadores a determinar o escopo e a gravidade de um ataque e identificar possíveis culpados. O tipo de indicadores coletados durante uma intervenção dependerá se a intervenção é realizada online ou offline. As intervenções online podem coletar indicadores relacionados ao tráfego de rede e logs do sistema, enquanto as intervenções offline podem coletar indicadores de dispositivos físicos e midia.

Para desenhar e implementar uma ação de sensibilização eficaz numa entidade privada, é importante ter em consideração os tipos de incidentes de cibersegurança mais comuns na Europa. Isso pode incluir incidentes como ataques de phishing e ataques de ransomware, que têm aumentado nos últimos anos. A ação deve ter como objetivo educar os funcionários sobre essas ameaças e fornecer a eles o conhecimento e as ferramentas necessárias para proteger a si mesmos e à organização de tais ataques.

No geral, este documento fornece uma visão abrangente dos principais tópicos relacionados à segurança cibernética e à luta contra o crime cibernético. A pesquisa e a análise apresentadas neste documento podem ajudar as organizações a entender melhor e se defender contra os vários vetores de ataque que representam uma ameaça a seus sistemas e redes. Ao adotar uma abordagem pro-ativa e holística à segurança, as organizações podem melhorar sua resiliência a ameaças cibernéticas e proteger seus ativos e informações valiosos.

Bibliografia

[1] Association for Computing Machinery, *ACM Code of Ethics*, Accessed on December 11, 2022, 2017. URL: https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct.

[2] IT Governance USA, *ISO 27001 vs. 27002: What's the Difference?* Accessed on December 11, 2022, 2022. URL: https://www.itgovernanceusa.com/blog/iso-27001-vs-27002-whats-the-difference/.

[3] International Organization for Standardization, *ISO/IEC 27002 Summary*, Accessed on December 11, 2022, 2013. URL: https://www.iso.org/isoiec-27002-information-security.html.

[4] National Institute of Standards and Technology, *NIST Cybersecurity Framework Overview*, Accessed on December 11, 2022, 2014. URL: https://www.nist.gov/cybersecurity-framework/overview.

[5] Open Web Application Security Project, *OWASP Top 10 2017*, Accessed on December 11, 2022, 2017. URL: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project.