Semana 22 - Aula 1

Tópico Principal da Aula: Gestão de Riscos e Resposta a Incidentes de Segurança

Subtítulo/Tema Específico: Introdução à Gestão de Riscos de Incidentes de Segurança

Código da aula: [SIS]ANO1C2B3S22A1

Objetivos da Aula:

- Compreender como ocorre a gestão de riscos de incidentes de segurança.
- Conhecer técnicas de computação e gerenciar dados para soluções em nuvem, parametrizar aplicações e dimensioná-las de acordo com as necessidades do negócio.
- Identificar e analisar problemas.
- Agir com curiosidade na resolução de problemas técnicos.

Recursos Adicionais (Sugestão, pode ser adaptado):

- Caderno para anotações;
- Acesso ao laboratório de informática e/ou internet.

Exposição do Conteúdo:

Referência do Slide: Slide 06 - 73% dos ataques de ransomware no Brasil foram bem-sucedidos

- **Definição:** Ransomware é um tipo de software malicioso que criptografa os arquivos da vítima, tornando-os inacessíveis, e exige um pagamento (resgate) para restaurar o acesso aos dados. Este slide destaca a alta taxa de sucesso dos ataques de ransomware no Brasil, com 73% sendo bem-sucedidos, e aponta o setor financeiro como um dos mais visados. Trojans são um mecanismo comum para a distribuição de ransomware.
- **Aprofundamento/Complemento (se necessário):** Ransomware não apenas bloqueia o acesso aos dados, mas muitas vezes também ameaça divulgar informações confidenciais se o resgate não for pago. As consequências de um ataque de ransomware vão além da perda de dados, incluindo interrupção das operações de negócios, danos à reputação e custos significativos de recuperação. Muitos ataques de ransomware se iniciam por e-mails de phishing, nos quais os funcionários são enganados a clicar em links maliciosos ou baixar anexos infectados, como ilustrado pelo caso de um hospital que teve seus sistemas paralisados após um ataque de ransomware via phishing.
- **Exemplo Prático:** Uma rede hospitalar é paralisada após um funcionário abrir um e-mail de phishing com um link malicioso, resultando na criptografia de seus sistemas. Isso força o hospital a cancelar consultas e redirecionar pacientes, com os atacantes exigindo um resgate em criptomoedas para a liberação dos arquivos.

Referência do Slide: Slide 09 - Gestão de riscos diante de incidentes de segurança [12]

- **Definição:** A gestão de riscos diante de incidentes de segurança é um processo estruturado para identificar, avaliar, mitigar e monitorar os riscos associados a incidentes de segurança da informação. É fundamental para proteger os ativos de uma organização e garantir a continuidade dos negócios. [13]
- **Aprofundamento/Complemento (se necessário):** A gestão de riscos não é um evento único, mas um ciclo contínuo que se adapta às mudanças no cenário de ameaças e vulnerabilidades. Envolve a implementação de controles de segurança para reduzir a probabilidade de incidentes e o desenvolvimento de planos de resposta para gerenciar incidentes quando eles ocorrem.
- **Exemplo Prático:** Uma empresa realiza uma avaliação de seus sistemas para identificar possíveis falhas de segurança (vulnerabilidades) e as ameaças que podem explorá-las. Com base nessa análise, ela implementa um firewall, sistemas de detecção de intrusão e políticas de acesso rigorosas para mitigar os riscos de acesso não autorizado e perda de dados.

Referência do Slide: Slide 10 - Etapas da gestão de riscos: Identificação de riscos [14]

- **Definição:** A identificação de riscos envolve a listagem dos ativos de informação críticos da organização (dados, sistemas, redes, infraestrutura) e a análise das ameaças potenciais e vulnerabilidades associadas a esses ativos. [15]
- **Aprofundamento/Complemento (se necessário):** Um ativo de informação pode ser qualquer coisa de valor para a organização, como bancos de dados de clientes, propriedade intelectual, servidores de rede ou softwares específicos. Ameaças são eventos ou circunstâncias que podem causar danos, como ataques de malware ou desastres naturais. Vulnerabilidades são fraquezas nos sistemas ou processos que podem ser exploradas por ameaças.
- **Exemplo Prático:** Uma empresa de e-commerce identifica seu banco de dados de clientes como um ativo crítico. A ameaça é o roubo de dados, e a vulnerabilidade pode ser um software desatualizado no servidor do banco de dados.

Referência do Slide: Slide 10 - Etapas da gestão de riscos: Avaliação de riscos

- **Definição:** A avaliação de riscos estima o potencial impacto de incidentes de segurança (interrupção de operações, perda financeira, danos à reputação) e determina a probabilidade de sua ocorrência, com base nas ameaças e medidas de controle existentes.
- **Aprofundamento/Complemento (se necessário):** O impacto pode ser quantificado em termos financeiros (custos de recuperação, multas) ou qualitativos (perda de confiança dos clientes). A probabilidade é a chance de uma ameaça explorar uma vulnerabilidade. A matriz de risco (probabilidade x impacto) é uma ferramenta comum para visualizar e priorizar os riscos.

- **Exemplo Prático:** Após identificar o risco de um ataque de ransomware, uma empresa avalia que o impacto seria alto (paralisação total das operações e perda financeira significativa) e a probabilidade média, devido à falta de backups regulares e um sistema de e-mail vulnerável a phishing.

Referência do Slide: Slide 10 - Etapas da gestão de riscos: Mitigação de riscos

- **Definição:** A mitigação de riscos envolve o desenvolvimento e implementação de controles de segurança (controles de acesso, sistemas de detecção de intrusão, criptografia) e a criação de um plano de resposta a incidentes para gerenciar eficazmente os eventos de segurança.
- **Aprofundamento/Complemento (se necessário):** Controles de segurança podem ser técnicos (criptografia, firewalls), administrativos (políticas de segurança, treinamento de funcionários) ou físicos (controle de acesso a data centers). Um plano de resposta a incidentes detalha os passos a serem seguidos desde a detecção até a recuperação de um incidente.
- **Exemplo Prático:** Para mitigar o risco de vazamento de dados, uma empresa implementa criptografia em todos os dados sensíveis, adota autenticação multifator para acesso a sistemas críticos e estabelece um plano de resposta que inclui a equipe responsável, os passos para conter um incidente e a comunicação com as partes interessadas.

Referência do Slide: Slide 10 - Etapas da gestão de riscos: Monitoramento e revisão

- **Definição:** O monitoramento contínuo dos riscos e a revisão periódica das estratégias de segurança são cruciais para garantir que as medidas de proteção permaneçam eficazes diante de novas ameaças.
- **Aprofundamento/Complemento (se necessário):** Isso inclui a análise de logs de segurança, testes de penetração, auditorias regulares e a atualização de políticas e procedimentos com base nas lições aprendidas de incidentes anteriores. A tecnologia e as ameaças evoluem constantemente, o que exige uma postura de segurança adaptativa.
- **Exemplo Prático:** Uma equipe de segurança da informação monitora o tráfego de rede em tempo real para detectar atividades incomuns. Mensalmente, eles realizam testes de vulnerabilidade em seus sistemas e, anualmente, revisam suas políticas de segurança para incorporar novas tecnologias e frameworks de segurança.

Semana 22 - Aula 2

Tópico Principal da Aula: Gestão de Riscos e Resposta a Incidentes de Segurança

Subtítulo/Tema Específico: Resposta a Incidentes de Segurança: Análise e Avaliação, Classificação e Priorização

Código da aula: [SIS]ANO1C2B3S22A2

Objetivos da Aula:

- Compreender como ocorre a gestão de riscos de incidentes de segurança.

- Conhecer técnicas de computação e gerenciar dados para soluções em nuvem, parametrizar aplicações e dimensioná-las de acordo com as necessidades do negócio.
- Identificar e analisar problemas.
- Agir com curiosidade na resolução de problemas técnicos.

Recursos Adicionais (Sugestão, pode ser adaptado):

- Caderno para anotações;
- Acesso ao laboratório de informática e/ou internet.

Exposição do Conteúdo:

Referência do Slide: Slide 06 - Conheça o ataque de ransomware à Colonial Pipeline

- **Definição:** Este slide apresenta o ataque de ransomware sofrido pela Colonial Pipeline em maio de 2021, que paralisou suas operações e teve um grande impacto no fornecimento de combustíveis. A empresa pagou um resgate para recuperar seus dados.
- **Aprofundamento/Complemento (se necessário):** O ataque à Colonial Pipeline é um exemplo notório de como o ransomware pode impactar infraestruturas críticas, resultando em consequências econômicas e sociais significativas. A decisão de pagar o resgate é sempre complexa, pois embora possa restaurar o acesso aos dados, também pode encorajar futuros ataques. O incidente ressalta a importância de planos robustos de resposta a incidentes e resiliência cibernética.
- **Exemplo Prático:** Uma empresa de energia tem seus sistemas de controle industrial comprometidos por um ataque de ransomware, resultando na interrupção do fornecimento de energia para uma região. A equipe de segurança deve então avaliar a gravidade, investigar como ocorreu, e decidir sobre a melhor estratégia de recuperação, que pode ou não incluir o pagamento de resgate.

Referência do Slide: Slide 09 - Resposta a incidentes de segurança

- **Definição:** Resposta a incidentes de segurança é uma abordagem estruturada e coordenada para gerenciar e mitigar incidentes de segurança em uma organização. Uma resposta eficaz é crucial para minimizar danos, restaurar a operacionalidade normal e prevenir futuras ocorrências.
- **Aprofundamento/Complemento (se necessário):** A resposta a incidentes vai além da simples remediação técnica. Ela envolve comunicação estratégica, aspectos legais, e a coordenação de múltiplas equipes (TI, segurança, jurídico, comunicação, gestão). O objetivo final é não apenas "apagar o fogo", mas também aprender com o incidente para fortalecer as defesas futuras.
- **Exemplo Prático:** Após a detecção de uma intrusão em sua rede, uma equipe de resposta a incidentes ativa seu plano predefinido, que inclui isolar os sistemas afetados, analisar o malware, notificar as autoridades competentes e iniciar a restauração dos dados a partir de backups seguros.

Referência do Slide: Slide 10 - Resposta a incidentes de segurança: Análise e avaliação

- **Definição:** Esta etapa envolve a investigação preliminar para avaliar a natureza, gravidade e impacto do incidente, além da coleta de evidências digitais e registros para apoiar a análise.
- **Aprofundamento/Complemento (se necessário):** A investigação deve ser meticulosa para entender a causa raiz, o escopo da violação e os sistemas afetados. A coleta de evidências digitais (logs de servidor, imagens de disco, tráfego de rede) é crucial para uma análise forense, que pode ser usada para identificar os atacantes e fortalecer defesas futuras. A integridade das evidências é fundamental para possíveis ações legais.
- **Exemplo Prático:** Um sistema de detecção de intrusões alerta sobre uma atividade incomum. A equipe de resposta inicia uma investigação, coletando logs do firewall, registros de acesso ao servidor e uma imagem forense do disco rígido do sistema comprometido para determinar como o ataque ocorreu e quais dados foram acessados.

Referência do Slide: Slide 11 - Resposta a incidentes de segurança: Classificação e priorização

- **Definição:** A classificação envolve categorizar o incidente com base em sua gravidade, tipo de ameaça, impacto potencial e urgência de resposta. A priorização define as ações a serem tomadas, focando na mitigação de riscos, restauração da operacionalidade e proteção de ativos críticos.
- **Aprofundamento/Complemento (se necessário):** Incidentes podem ser classificados como "alto", "médio" ou "baixo" em termos de gravidade do impacto. Tipos comuns de incidentes incluem malware, acesso não autorizado, phishing, DDoS e violação de dados. A urgência de resposta pode ser imediata, urgente ou regular. A complexidade e a escala do incidente também influenciam a classificação, com incidentes complexos exigindo maior coordenação.
- **Exemplo Prático:** Uma empresa detecta um ataque de DDoS (Negação de Serviço Distribuída). Eles classificam o incidente como de alta gravidade devido à interrupção total do serviço e priorizam a mitigação imediata para restaurar a disponibilidade, enquanto um incidente de phishing de baixo volume pode ter uma prioridade mais baixa e uma resposta regular.

Semana 22 - Aula 3

Tópico Principal da Aula: Gestão de Riscos e Resposta a Incidentes de Segurança

Subtítulo/Tema Específico: Resposta a Incidentes de Segurança: Contenção, Recuperação, Comunicação e Revisão

Código da aula: [SIS]ANO1C2B3S22A3

Objetivos da Aula:

- Compreender como ocorre a gestão de riscos de incidentes de segurança.

- Conhecer técnicas de computação e gerenciar dados para soluções em nuvem, parametrizar aplicações e dimensioná-las de acordo com as necessidades do negócio.
- Identificar e analisar problemas.
- Agir com curiosidade na resolução de problemas técnicos.

Recursos Adicionais (Sugestão, pode ser adaptado):

- Caderno para anotações;
- Acesso ao laboratório de informática e/ou internet.

Exposição do Conteúdo:

Referência do Slide: Slide 06 - Ponto de partida: Incidente de segurança da Equifax (2017)

- **Definição:** Em setembro de 2017, a Equifax, uma grande agência de crédito dos EUA, sofreu uma violação de dados que expôs informações pessoais de mais de 145 milhões de pessoas.
- **Aprofundamento/Complemento (se necessário):** Este caso é um marco na história da cibersegurança devido à sua escala e ao tipo de dados comprometidos (informações financeiras e pessoais altamente sensíveis). A resposta inadequada inicial da Equifax, incluindo atrasos na notificação e problemas com o site de verificação, agravou o impacto na confiança dos clientes e resultou em grandes multas e ações legais.
- **Exemplo Prático:** A violação da Equifax serve como um exemplo claro da necessidade de uma resposta a incidentes rápida e transparente, com um plano de comunicação claro e eficaz, para mitigar o dano à reputação e as ramificações legais e financeiras.

Referência do Slide: Slide 07 - Resposta a incidentes de segurança

- **Definição:** Esta aula aprofunda a compreensão da resposta a incidentes de segurança, abordando ações como contenção e neutralização, recuperação e restauração, comunicação e coordenação, e revisão e atualização de políticas e procedimentos.
- **Aprofundamento/Complemento (se necessário):** A resposta a incidentes é um processo crítico que visa minimizar o impacto de um evento de segurança, restaurar as operações normais e fortalecer as defesas contra futuros ataques. Cada uma das fases mencionadas é vital para uma resposta eficaz e para a resiliência contínua de uma organização.
- **Exemplo Prático:** Uma empresa, ao detectar um ataque em andamento, inicia imediatamente a fase de contenção, isolando as máquinas infectadas. Em seguida, na fase de recuperação, eles restauram os sistemas a partir de backups limpos. A comunicação transparente com os clientes e a revisão das políticas de segurança para evitar reincidências são passos cruciais que se seguem.

Referência do Slide: Slide 14 - Resposta a incidentes de segurança: Contenção e neutralização

- **Definição:** A contenção envolve o isolamento dos sistemas comprometidos para evitar a propagação do incidente. A neutralização foca em medidas para neutralizar as ameaças identificadas, como remoção de malware, correção de vulnerabilidades e interrupção de atividades maliciosas.
- **Aprofundamento/Complemento (se necessário):** A contenção rápida é essencial para limitar o dano. Isso pode incluir desconectar sistemas da rede, desativar contas de usuários comprometidas ou bloquear endereços IP maliciosos no firewall. A neutralização garante que a ameaça não persista após a contenção.
- **Exemplo Prático:** Após um ataque de ransomware, a equipe de TI isola os servidores infectados da rede para impedir que o malware se espalhe para outros sistemas. Em seguida, eles utilizam ferramentas antivírus e de remoção de malware para limpar os sistemas e aplicar patches de segurança para corrigir a vulnerabilidade que foi explorada.

Referência do Slide: Slide 17 - Resposta a incidentes de segurança: Comunicação e coordenação

- **Definição:** Esta fase enfatiza a comunicação transparente e regular com todas as partes interessadas (administração, clientes, reguladores, equipes internas) e a coordenação eficaz dos esforços de resposta entre TI, segurança, comunicações e equipes jurídicas.
- **Aprofundamento/Complemento (se necessário):** A comunicação é vital para manter a confiança e cumprir com obrigações regulatórias (como a LGPD no Brasil). A coordenação garante que todas as ações sejam alinhadas e que não haja esforços duplicados ou conflitos. Um plano de comunicação pré-definido, com modelos de mensagens, é altamente recomendado.
- **Exemplo Prático:** Após uma violação de dados, a empresa emite um comunicado público informando os clientes sobre o incidente, as medidas tomadas e as ações que eles podem realizar para se protegerem. Internamente, o CISO (Chief Information Security Officer) coordena reuniões diárias com as equipes de TI, jurídico e relações públicas para garantir que todas as ações e comunicações estejam alinhadas.
-

Referência do Slide: Slide 19 - Análise pós-incidente e Revisão e atualização de políticas e procedimentos

- **Definição:** A análise pós-incidente avalia a eficácia da resposta, identifica áreas de melhoria e desenvolve recomendações para prevenir incidentes futuros. A revisão e atualização de políticas, procedimentos e controles de segurança são baseadas nas lições aprendidas dessa análise.
- **Aprofundamento/Complemento (se necessário):** Esta fase é crucial para a melhoria contínua da postura de segurança da organização. Ela envolve documentar o incidente, conduzir uma "autópsia" para entender o que deu errado e o que deu certo, e implementar mudanças para evitar que o mesmo tipo de incidente ocorra novamente.

- **Exemplo Prático:** Após um incidente de segurança, a equipe realiza uma reunião de "lições aprendidas", onde analisam o tempo de detecção, o tempo de resposta, a eficácia das ferramentas e a comunicação. Com base nisso, eles decidem implementar um novo treinamento de conscientização para funcionários e revisar a política de backup para incluir backups imutáveis.

Referência do Slide: Slide 22 - Vídeo Como evitar ataques DDoS?

Definição: O slide faz referência a um vídeo sobre como evitar ataques de Negação de Serviço Distribuída (DDoS), que visam tornar um sistema ou serviço indisponível sobrecarregando-o com solicitações. ataque de DDoS ao Google em 2020 é citado como um exemplo real.

- **Aprofundamento/Complemento (se necessário):** Ataques DDoS são uma das ameaças mais comuns à disponibilidade de serviços online. Eles podem ser realizados por botnets (redes de computadores comprometidos) e têm como objetivo sobrecarregar servidores, redes ou aplicações para que usuários legítimos não consigam acessá-los. Estratégias de mitigação incluem balanceamento de carga, filtragem de tráfego e serviços de proteção DDoS.
- **Exemplo Prático:** Uma plataforma de e-commerce sofre um ataque DDoS durante a Black Friday, que sobrecarrega seus servidores e impede que os clientes acessem o site. A equipe de TI, em resposta, ativa um serviço de proteção DDoS que filtra o tráfego malicioso e direciona apenas as requisições legítimas para os servidores, restaurando a disponibilidade do site.