SECURITY CONTROL OPERATION CENTER

Curitiba, 15/01/2019 – CNPJ 20.962.496/0001-91 – IDC 2112 – REG: 05/06/2014
Registro Contrato e termos de uso de dados e exclusividade

Os termos de segurança da informação, compartilhamento de dados, servidores de uso ou disponibilidade de qualquer serviço relacionado a nuvem dedicada, uma vulnerabilidade é uma fragilidade encontrada em um ativo ou em um controle e que pode ser explorada por uma ou mais ameaças, o que torna um risco de segurança. Uma forma de proteger as informações é através da identificação de análise proativa, avaliação, priorização e correção das deficiências identificadas nos ativos.

Esta atividade é conhecida como Vulnerability Assessment e visa encontrar as fragilidades nas plataformas de software ou hardware para resolver as falhas, antes que elas possam gerar um impacto negativo causando todo um cenário de instabilidades de níveis financeiros ou sistemáticos de reputação.

Etapas para a avaliação de Vulnerabilidades Também conhecida como análise de vulnerabilidades, consiste em uma análise ou avaliação, pois, além de cobrir a fase de análise, envolve também uma avaliação das fragilidades identificadas, utilizando diferentes critérios que permitem qualificar e quantificar seu impacto causador.

Em geral, vulnerabilidades podem ser encontradas em sistemas ou por falhas humanas devido ao desconhecimento, pois os mesmos podem conter falhas de segurança conhecidas e desconhecidas como configurações padrão ou resultado de erros de configuração para quaisquer aspectos da tratativa que é tratado ou não observado da qualidade da segurança.

Para resolver esses problemas, é possível aplicar diferentes métodos para realizar a avaliação de falhas na infraestrutura de uma empresa, programação ou situação.

Em geral, são consideradas as seguintes atividades: Obter a aprovação para a avaliação de vulnerabilidades Como as atividades relacionadas com a identificação de vulnerabilidades podem ser classificadas como intrusivas pelas ferramentas de segurança que são instaladas dentro da infraestrutura do centro de dados e diretamente ligado ao servidor de hospedagem dos dados arquivos, é necessário ter a aprovação do scanner, agendar a atividade e notificar as partes interessadas, ou seja, aquelas que podem afetar ou ser afetadas por essa atividade ocorrida no ato de uma simples migração ou até mesmo uma proteção de análise antes de qualquer envio de dados para o servidor como medida de pró atividade.

Gerar um inventário de ativos Nosso protocolo de Segurança e prática de gerenciamento de segurança consiste na análise de risco e verificação dos arquivos dispostos pelo cliente ou desenvolvedor com a geração bilheteira sobre a possível manutenção de um inventário de ativos associados às informações e sistemas, usados para processar, armazenar ou transmitir essas informações.

Quando a lista estiver disponível e laudo técnico entregue ao cliente sobre a tratativa, os ativos nos quais a avaliação será realizada devem ser informados com tudo em na medida de informações e proteções que o usuário cliente poderá aplicar para esta correção de dados e manter ativa o conceito de medidas de proteção para qualquer aspectos de

correção. Em geral, os testes devem se concentrar nos elementos críticos, relacionados aos processos mais importantes. Definir o escopo da avaliação Derivado da geração do inventário e da seleção dos objetivos, a nossa avaliação é executada de duas maneiras: interna e externa.

Do ponto de vista interno, a varredura é realizada a partir da infraestrutura do servidor, com acesso aos recursos de forma direta ao código fonte ou estrutura disponível para o cliente. A avaliação externa envolve lidar com a proteção de perímetro na rede de acesso e adotar a posição que a vulnerabilidade teria em busca de alguma porta para a entrada. Coletar informações, identificar e avaliar vulnerabilidades Página 2 de 5 A avaliação é feita manualmente e automatizada através das nossas ferramentas, para obter informações relevantes sobre vulnerabilidades nos sistemas considerados.

Após a identificação dos pontos fracos e a obtenção das informações a eles relacionadas, é necessário realizar um processo de avaliação que permita conhecer seu impacto. Para isso, é usamos um sistema de pontuação em conjunto com um nível de softwares de bordas e do núcleo de Firewall escam.

É importante mencionar que as nossas ferramentas especializadas permitem automatizar as atividades e gerar nossos logs garantindo assim mais segurança nas informações e métricas de dados com saldo positivo em análise dos mesmos. Gerar um relatório de resultados Com base nos resultados da avaliação, geramos um relatório interno que permita conhecer o estado de segurança nos sistemas com base nas descobertas.

Neste processo, mostramos os resultados através da priorização de vulnerabilidades, com o objetivo de, primeiramente, abordar as fragilidades de maior impacto sobre os ativos e informar as ações necessárias. Gerar um plano de remediação Como última atividade associada à avaliação de vulnerabilidades, é necessário desenvolver e executar um plano de remediação que permita corrigir as falhas identificadas e avaliadas, de acordo com os resultados da priorização. Em geral, a correção dessas falhas está relacionada à aplicação de atualizações ou patches de segurança que estão sempre disponíveis e isso garante que as correções de segurança já identificadas foram ajustadas corrigidas para evitar danos maiores. Razões para realizar uma avaliação de vulnerabilidade A exploração de vulnerabilidades tornou-se a principal preocupação da nossa empresa em questões de segurança, seguida por outros incidentes como infecção por Malware, fraudes, ataques de phishing ou negação de serviço (DoS). Portanto, a avaliação torna-se relevante para evitar os incidentes relacionados à exploração dos mesmos e como meio de aplicação de um elemento da chamada segurança ofensiva, através dos scanner de vulnerabilidades e já fazem parte de nosso núcleo de segurança interna que são responsáveis por clientes de redes maiores como Governo do Estado.

O que faz a análise de vulnerabilidade Análises de vulnerabilidade identificam, quantificam e priorizam o que há de mais frágil nos seus sistemas, a fim de tornar sua segurança mais robusta. Embora sejam tradicionalmente executadas em ambientes de TI, elas não se limitam a essa aplicação e englobam vários níveis de ações que muitos ainda desconhecem ou passam desapercebidos por muitos.

É possível fazer uma análise de vulnerabilidade em sistemas local host como Desktop de conexões ou de comunicação via endereçamento URL apenas como exemplo. Além disso, tanto os pequenos quanto os grandes negócios podem se beneficiar dela com as

ferramentas que analisam o tráfego ou as que iniciam escaneamento em tempore reais quais ligadas. Uma análise de vulnerabilidade é diferente de um teste de penetração porque seus objetivos são distintos.

Enquanto o teste explora táticas específicas de invasão, a análise identifica todas as brechas existentes em um sistema. Em geral, análises de vulnerabilidade são divididas em três etapas. Conheça-as melhor a seguir. Avaliação de risco A primeira etapa em qualquer análise de vulnerabilidade é avaliar os riscos.

Para isso, é preciso, acima de tudo, entender e identificar como um negócio funciona. Nenhuma análise de vulnerabilidades será idêntica a outra porque cada uma delas tem um contexto diferente. Nessa importante fase, o ideal é colaborar com tantos membros da equipe quanto possível para entender os processos e as infraestruturas fundamentais para a empresa.

Só assim é possível começar a analisar os dados e as aplicações que sustentam as operações. Durante a avaliação de risco, localizamos e classificamos os ativos da organização. Esse processo envolve relacionar servidores, estações de trabalho, dispositivos móveis e todos os tipos de mídias que podem ser alvos de ataques. Página 3 de 5 Classificamos quanto ao tipo de informação que carregam. utilizamos uma escala de 1 a 5 na qual:

1 – Diz respeito às informações públicas sobre a companhia e como protegê-las.
2 – São os dados internos, que não são confidenciais e como protegê-las.
3 – Dados e informações sensíveis, como utilizar e proteger.
4 – Estes são os dados que não podem ser vistos nem mesmo por todos.
5 – Englobam todas as informações confidenciais ou repasses.

Avaliação de vulnerabilidades Passando para a etapa de avaliação de vulnerabilidades, nossa equipe criará um modelo das principais ameaças a seus ativos e, para isso, podemos utilizar métodos tradicionais, como endurecimento das aplicações por vários meios. O método elaborado como Endurecimento tem esse nome porque cada uma de suas iniciais corresponde a uma ameaça: Spoofing of identity (roubo de identidade ou falsificação); Tampering with data (violação ou adulteração de dados); Repudiation of transaction (divulgação não autorizada de informação); Information disclosure (ataques de negação de serviço); Denial of service Elevation of privilege (elevação de privilégio). human failure (falha humana) A partir das ações, criamos os meios e medidas com todos os ativos do negócio e a categoria Security de ameaça que ele pode sofrer e como proteger.

E, sempre que possível, deve averiguar a probabilidade de um ataque ocorrer, utilizando uma escala de 0-10 para após procedimentos. É comum escanear um sistema por vulnerabilidades para encontrar os dados relevantes para essa etapa. Tratamento do risco A última etapa da análise de vulnerabilidade é sempre o tratamento do risco. Nesse momento, devemos fazer o possível para mitigar as vulnerabilidades detectadas. Sabendo exatamente qual a porcentagem dos sistemas que está sob risco e identificando a importância de cada um deles, é possível enumerar as ameaças que devem ser endereçadas primeiro.

Se há vulnerabilidades nos controles existentes, por exemplo, elas devem ser corrigidas o quanto antes. A chave aqui é entender como o tipo de risco que o negócio corre pode ser evitado e quais são as ferramentas mais eficazes para isso. Uma análise de vulnerabilidade pode ajudar o negócio a evitar problemas no futuro. Manter-se informado sobre questões de segurança é também um passo importante.

Assine a newsletter da Alerta Security e esteja sempre por dentro das novidades da área, assinalando no ato de um pedido ou editando sua conta em Perfil. Causas e origens das Vulnerabilidades As falhas conhecidas e presentes podem ser causadas por: ERROS DE PROGRAMAÇÃO/DESENVOLVIMENTO: Grande parte das vulnerabilidades surge do erro de programação, por exemplo, quando usadas por SMS como WP/Wordpress, temas desatualizados, plugins desatualizados, vários temas na pasta sem o uso ou necessidade, temas NULLED craqueados da internet, estes com códigos de ofuscação, base64 etc. Outro erro também comum, é a possibilidade de inserção de códigos de consulta MySQL, brecha considerada dentre as mais graves em nível mundial; ou o mau gerenciamento de credenciais como senhas de níveis 0 total falta de proteção no sms.

MÁ CONFIGURAÇÃO
Aplicativos de segurança, como o firewall WAF internos, devem ser corretamente configurados, ou podem ser brechas para ataques maliciosos. Infraestrutura de acesso também precária e muitas vezes doméstica, implementada em um ambiente corporativo com um gerenciamento descuidado de partes.

FALHA HUMANA
Execução de arquivos maliciosos manualmente. Hábitos ruins dos usuários e experimentar coisas. Página 4 de 5 Quais os objetivos da Análise de Vulnerabilidades? Assim como em todos os processos de gestão e repressão a ataques, existem diversos objetivos.

A fim de simplificar a análise, com base nos conceitos aplicados pela Módulo Security Corp. Seguem alguns dos principais objetivos galgados que aplicamos para a Análise de Vulnerabilidades: Identificar e tratar falhas de softwares que possam comprometer seu desempenho, funcionalidade e segurança; Providenciar uma nova solução de segurança como, por exemplo, o uso de um bom antivírus em seu local ou no servidor, com possibilidade de update constante e implementação de sistemas de detecção e prevenção de intrusão; Alterar as configurações de softwares a fim de torná-los mais eficientes e menos suscetíveis a ataques; Utilizar mecanismos para bloquear ataques automatizados Ransonwares, Trojans, Malware, Worms, Bots, entre outros); Implementar a melhoria constante do controle de segurança no servidor do cliente e auxiliar em requisitos básicos desktops locais estes munidos de ações que podem ser consideradas como porta de entrada. Documentar os níveis de segurança atingidos para fins de auditoria e compliance com leis, regulamentações e políticas.

Técnicas e ferramentas utilizadas Em muitas situações, nossos profissionais utilizam de técnicas chamadas de Baseline Reporting, que o auxilia a identificar o que está acontecendo na sua rede ou companhia quando não existem ameaças, ou seja, quando nenhum agente está explorando, intencionalmente ou não, alguma falha ou vulnerabilidade no ambiente.

Este comportamento é utilizado quando há a suspeita de algum evento e precisa compará-lo ao funcionamento normal de suas atividades. Contudo, tanto o ambiente quanto as

operações de sua empresa se modificam naturalmente, de forma que se deve garantir que a Linha de Base seja atualizada frequentemente e seguir rigorosamente os termos de uso. O processo de Análise de Vulnerabilidade é suportado por diversas Ferramentas de Análise, capazes de auxiliar o nesta identificação. Dentre estas, podemos citar: PORT SCANNER: Um Port Scanner varre as portas de serviço TCP/IP de cada host analisado na rede, identificando quais destas portas estão abertas ou expostas; PROTOCOL ANALYZER: Analisadores de Protocolo, ou Sniffers são ferramentas capazes de visualizar o tráfego de rede, capturando pacotes trafegados e permitindo a análise de seu conteúdo.

VULNERABILITY ESCÂNERES
São ferramentas inteligentes capazes de escanear o sistema, analisando serviços, versões de software, sistemas operacionais, bancos de dados e outros elementos no ambiente, identificando versões desatualizadas, patches de correção não aplicados, má configuração e outros detalhes que possam expor a Corporação às ameaças.

HONEYPOTS/HONEYNETS
"Potes de Mel" e "Redes de Mel", têm esse nome porque são utilizados para atrair ameaças que normalmente seriam direcionadas para o ambiente real de produção. Tratam-se de implementações de software complexas, que "sentam" no ambiente e tentam se parecer com sistemas em produções vulneráveis, no intuito de atrair atacantes, a fim de conhecer e identificar as técnicas utilizadas por estes, para melhorar os processos de mitigação de ataques. Proteja-se! Proteja todos os hosts de uma rede com soluções de segurança.

Mantenha habilitada as funcionalidades de proteção para navegação na internet. Softwares e serviços devem estar sempre atualizados e com os últimos pacotes de segurança instalados.

Configure todas as soluções de proteção para que se mantenham ativas e bloqueando ameaças. Não abra links de fontes duvidosas, tenha cautela ao baixar/acessar qualquer tipo de arquivo na internet.

FORO DE ELEIÇÃO 307
As partes elegem o foro da cidade de Curitiba para dirimir todas as dúvidas ou litígios resultantes da execução do presente.

HOSTCURITBA – HOSPEDAGEM DE SITES.
CNPJ: 20.962.496/0001-91

Para o esclarecimento de possíveis dúvidas em relação à terminologia técnica utilizada na internet que possa ser relevante para a interpretação do presente contrato prevalecerão as definições constantes do glossário existente nos sites:
Provedora: https://www.hostcuritiba.net.br
Institucional: https://www.hostcuritiba.com.br

HOSTCURITIBA – Hospedagem Security Central do Cliente (41) 3014-8891
Curitiba, 15 de Janeiro 2020.