1 - Resposta

Cibersegurança é a prática que protege computadores e servidores, dispositivos móveis, sistemas eletrônicos, redes e dados contra ataques maliciosos. Também é chamada de segurança da tecnologia da informação ou segurança de informações eletrônicas. O termo é aplicável a uma variedade de contextos, desde negócios até computação móvel, e pode ser dividido em algumas categorias comuns.

Segurança de rede é a prática de proteger uma rede de computadores contra intrusos, sejam eles invasores direcionados ou malware oportunista.

Segurança de aplicativos foca em manter o software e os dispositivos livres de ameaças. Um aplicativo comprometido pode fornecer acesso aos dados que pretende proteger. O sucesso da segurança começa na fase de projeto, bem antes de um programa ou dispositivo ser implantado.

Segurança de informações protege a integridade e a privacidade dos dados, tanto no armazenamento como em trânsito.

Segurança operacional inclui os processos e decisões para tratamento e proteção dos arquivos com dados. As permissões que os usuários têm ao acessar uma rede e os procedimentos que determinam como e onde os dados podem ser armazenados ou compartilhados se enquadram nesta categoria.

Recuperação de desastres e continuidade dos negócios definem como uma organização responde a um incidente de cibersegurança ou qualquer outro evento que cause a perda de operações ou dados. As políticas de recuperação de desastres ditam como a organização restaura suas operações e informações para retornar à mesma capacidade operacional de antes do evento. A continuidade dos negócios é o plano ao qual a organização recorre ao tentar operar sem determinados recursos.

Educação do usuário final aborda o fator de cibersegurança mais imprevisível: as pessoas. Qualquer pessoa pode introduzir acidentalmente um vírus em um sistema seguro se deixar de seguir as práticas recomendadas de segurança. Ensinar os usuários a excluir anexos suspeitos de e-mail,
não conectar unidades USB não identificadas e várias outras lições importantes é vital para a segurança de qualquer organização.

2 - Resposta

1. Disable SSH Password Login:
O uso direto de senhas repassadas de forma simples diretamente aos servidor vem se tornando uma prática amplamente desencorajada, tanto porque já existem maneiras muito mais seguras de realizar esta autenticação quanto porque quando esta opção no contexto do protocolo SSH automaticamente ativa a comunicação por clear text o que é altamente não recomendado do ponto de vista de segurança.

2. Disable Direct root SSH Login:
É mais vantajoso utilizar, assim como utilizado geralmente em distros do Linux para End Users, não utilizar o acesso de root diretamente, e ao inves disso configurar um usuário com acesso padrão e depois acessá-lo com contexto sudo (se possível utilize-de da configuração de alias) pois assim teremos maior controle dos acessos repassados a possíveis atacantes, além de inserir uma camada extra de proteção até para possíveiserros ou confusões do próprio programador.

3. Change Default SSH Port:
Trocar a porta padrão de comunicação é uma atitude recomendada em vários ambientes da comunicação via internet pois ela diminui significativamente os riscos de ataques mais simples (mais igualmente perigosos) feitos por atacantes que não conhecem qual a porta utilizada e buscam prefencialmente a porta padrão.

4. Disable IPv6 for SSH:
Apesar de o IPv6 ser uma tecnologia em crescimento e com grandes chances de se tornar uma necessidade, do ponto de vista da segurança ele representa um grupo e funcionalidades muito maior do que o IPv4, porém na maior parte das vezes essas funcionalidades não estão sendo utilizadas pelo desenvolvedor do sistema, servindo apenas para abrir o leque de ferramentas de possíveis atacantes

5.Setup a Basic Firewall:
O autor chama atenção especialmente para uma escolha consiente de qual o sistema de Firewall será utilizado pois muitas das vezes desenvolvedores utilizam firewalls altamente potentes de em ambientes q a sua função será simplesmente fechar as portas inutilizadas, gerando gastos desnecessários, ou pior ainda gerando uma falsa sensação de segurança:

6. Unattended Server Auto Upgrade
Auto Upgrade é uma funcionalidade essencial em sistemas de usuário final, pois permite manter o user protegido de novas tipos de ataques, virús e entre outros; porém essa realidade não se estende aos servidores, isso porque muitas vezes os serviços programados não conseguem se adaptar as mudanças tão facilmete quanto os usuários finais e dependem de características específicas dos sistemas utilizados ficando a mercê de bugs e vulnerabilidades quando estas atualizações acontecem.

3 - Resposta

a) A melhor maneira de salvar os dados de forma a proteger tanto a informação do usuário quanto a segurança do sistema seria passar sua senha por uma engine de IDs universais, exemplos clássicos destes modelos são: UUID e GUID.

b) Criptográfia de chave simétrica é caracterizada pelo uso de uma função que encripta (ou decripta) os dados em uma nova sequência encriptada (ou decripta) utilizando uma mesma chave, embora os tipos de implementação possam ser os mais variados podendo gerar resultados de mesmo tamanho, tamanho variados, resultados que se repetem de acordo com a entrada e entre outros.
podendo ser visto de forma simplificada como: tome um modelo M de entrada E e saida S logo:
$S = M(E) <=> E = M(S)$

c) De forma resumida podemos dizer que um sistema está preocupado com a transmição de uma mensagem isto é que os dados possam ser transmitidos de forma segura entre dois interlocutores, sem serem lidos por interceptadores intermediários, isso gera uma necessidade primária aos sistemas de criptográfia que os dados vistos pelos interlocutores originais sejam exatamente
iguais. Por outro lado os sistemas de HASH estão preocupados com a geraçãod de uma impressão digital do arquivo, desta forma os dados gerados por um HASH embora possam ser comparados (isso não garante a igualdade perfeita entre dois arquivos aleatórios embora em ambientes especificos seja muito improvável que o arquivos não seja o mesmo), não é possivel reconstruir um arquivo base a partir de ser HASH.

d) A “Threat Model” é um procedimento para otimizar a segurança do aplicativo, sistema ou processo de negócios, identificando objetivos e vulnerabilidades e, em seguida, definindo contramedidas para prevenir ou mitigar os efeitos das ameaças ao sistema.
Um modelo de ameaça é essencialmente uma representação estruturada de todas as informações que afetam a segurança de um aplicativo.
Em essência, é uma visão do aplicativo e de seu ambiente por meio de lentes de segurança. A modelagem de ameaças é um processo de captura, organização e análise de todas essas informações. A modelagem de ameaças permite a tomada de decisões informadas sobre o risco de
segurança do aplicativo. Além de produzir um modelo, os esforços típicos de modelagem de ameaças também produzem uma lista priorizada de melhorias de segurança para o conceito, requisitos, design ou implementação.

e) Secure Boot Configuration é um novo recurso que ajuda o computador a resistir a ataques e a infecções por malware. Quando o seu computador foi fabricado, a UEFI criou uma lista de chaves que identificam hardware, firmware e código de carregamento de sistema operacional confiáveis. Também foi criada uma lista de chaves que identificam malware conhecido.
Quando Secure Boot é ativado, o computador bloqueia ameaças em potencial antes que elas possam atacar ou infectar o computador. Por exemplo, a opção Secure Boot pode impedir que seu computador inicie CDs ou DVDs ilegalmente copiados que poderiam danificar o computador. Secure Boot não bloqueia discos de recuperação ou discos de Windows válidos.

f) A criptografia é um elemento fundamental da segurança de dados. É a forma mais simples e mais importante de garantir que as informações do sistema de um computador não sejam roubadas e lidas por alguém que deseja usá-las para fins maliciosos. A criptografia envolve a conversão de texto simples legível por humanos em texto incompreensível, o que é conhecido como texto cifrado. Essencialmente, isso significa pegar dados legíveis e transformá-los de forma que pareçam aleatórios. A criptografia envolve o uso de uma chave criptográfica, um conjunto de valores matemáticos com os quais tanto o remetente quanto o destinatário concordam.

O destinatário usa a chave para descriptografar os dados, transformando-os de volta em texto simples legível. Quanto mais complexa for a chave criptográfica, mais segura será a criptografia, pois é menos provável que terceiros a descritografem por meio de ataques de força bruta (ou seja, tentar números aleatórios até que a combinação correta seja adivinhada).
A criptografia também é usada para proteger senhas. Os métodos de criptografia de senha codificam a sua senha de forma que ela fique ilegível por hackers.

4 - Resposta

A) Uma das principais características do bitcoin é seu sistema distribuido (que não depende de um certificador principal), a base por trás deste sistema é o uso de um sistema específico (e custoso) de criação de HASHs os quais são guardados na famigerada Blockchain, a grande sacada por tras do Bitcoin é permitir que estas operações altamente custosas de geração de HASH possas ser feitas por qualquer e ofereçer grandes quantias pelo resultado assim alcançando a grande popularidade da moeda.

B) A implementação do protocolo TSL criptografa o tráfego de internet. É por isso que quando é realizado o acesso de algum site na web e possui um cadeado e o https na barra de endereços podemos confirmar que o protocolo TSL/SSL está sendo utilizado.
O método TSL se difere na criptografia assimétrica pois ele utiliza a criptografia, de forma mais fácil, no começo da comunicação entre o cliente e o servidor

C) Os certificados digitais são considerados documentos eletrônicos que correspondem a cada pessoa, contendo mensagens, assinaturas e verificações de identidades de forma criptografadas para tornar essas informações mais segura para o cliente que utiliza o servidor.
O comitê que faz a gestão do ICP-Brasil é responsável por estabelecer os critérios e políticas para regulamentar a emissão desses certificados. O Sistema ICP-Brasil, denominada de Infraestrutura de Chaves Públicas Brasileira, é uma forma de dividir de forma hierárquica viabilizando a geração/emissão dos certificados digitais para identificação virtual do cidadão. Para que o sistema funcione de forma correta, são necessárias várias técnicas e procedimentos feitos para aguentar um sistema criptográfico com base nos certificados digitais.