GAC119 - REO 3: Análises de notícias envolvendo ataques e/ou problemas de segurança por falta de uso de técnicas de programação segura

Mateus Carvalho Gonçalves - 201810245
Pedro Antônio de Souza - 201810557

ANÁLISE 1

- **Notícia**

  Site do Ministério da Saúde sofre ataque hacker durante madrugada e sai do ar

- **URL**

  https://www.cnnbrasil.com.br/nacional/site-do-ministerio-da-saude-sofre-ataque-hacker-durante-madrugada-e-sai-do-ar

- **Análise**

  A notícia relata o sequestro e bloqueio dos dados de servidores do Ministério da Saúde. Todos os portais vinculados ao ministério, como o "ConecteSUS" e o "Portal Covid", também foram afetados pelo incidente. Este foi um ataque de Negação de Serviços (DoS - Denial of Service) por meio de um ransomware. Uma técnica simples que o sistema deveria implementar para evitar esse tipo de ataque é ter um serviço de backup frequente, além de armazenar os dados com redundância em diferentes servidores independentes. Como ransomwares são softwares maliciosos e precisam penetrar na máquina para agir, a validação das entradas no servidor poderia barrar ou pelo menos dificultar a entrada do software no sistema. Outras práticas que poderiam ser implementadas são: manter softwares e aplicativos do servidor sempre atualizados; desenvolver políticas de permissões e restrições de acesso a determinados recursos do servidor (como ACLs, por exemplo); e contar com ferramentas de segurança sempre atualizadas para prevenir movimentações maliciosas.

ANÁLISE 2

- **Notícia**

  Falhas de segurança na Atlassian permitiam roubar contas com um clique

- **URL**

  https://canaltech.com.br/seguranca/falhas-de-seguranca-na-atlassian-permitiam-roubar-contas-com-um-clique-188206/

- **Análise**

  A notícia expõe falhas encontradas pela empresa de segurança Check Point Research (CPR) nos sistemas desenvolvidos pela Atlassian, como o Jira e o Confluence. Essas falhas permitiam que um atacante se apoderasse de contas associadas aos sistemas com apenas um clique, já que os problemas encontrados possibilitavam a execução de ataques XSS, CSRF e de fixação de sessão. Portanto, para mitigar os riscos de um ataque XSS, é importante que os dados sempre sejam validados e sanitizados para que o sistema não execute códigos maliciosos injetados nas interfaces de entrada. Em relação à mitigação de ataques CSRF, é fundamental garantir a autenticidade de requisições. Para isso, pode-se utilizar certificados SSL, exigir tokens de sessão ou, até mesmo, utilizar o atributo SameSite na criação de cookies. Por fim, para o problema da fixação de sessão, pode-se aplicar um tempo limite de duração da sessão e/ou dos dados de autenticação. Por exemplo, pode-se atribuir um tempo de validade para senhas e solicitar que o usuário a altere no momento do vencimento.

ANÁLISE 3

- **Notícia**

  SanDisk sofre falha de segurança com brecha para invasões e roubo de dados

- **URL**

  https://canaltech.com.br/seguranca/sandisk-sofre-falha-de-seguranca-com-brecha-para-invasoes-e-roubo-de-dados-204044/

- **Análise**

  A notícia descreve a vulnerabilidade que permitia a descoberta de senhas do programa SanDisk PrivateAccess através de aplicação de força bruta. Esse programa é utilizado em dispositivos de armazenamento USB da SanDisk com o objetivo de criptografar os dados guardados tornando-os acessíveis com a utilização de senhas geradas aleatoriamente. Como o texto informa, a criptografia era feita utilizando uma função de derivação de chave fraca, e esse problema foi mitigado através da utilização de criptografia utilizando derivação de chaves mais potentes. Porém, pode-se perceber que o programa não oferecia nenhum bloqueio contra múltiplas tentativas de autenticação fracassadas, já que permitia a realização de um ataque de força bruta. Dessa forma, a implementação de um bloqueio temporário após um certo limite de tentativas fracassadas se torna uma solução adicional à essa vulnerabilidade, uma vez que para realizar um ataque de força bruta levaria muito mais tempo.

ANÁLISE 4

- **Notícia**

  Log4J Vulnerability

- **URL**

  https://blog.gft.com/br/2021/12/23/log4j-vulnerability/

- **Análise**

  A matéria tem como objetivo explicar a vulnerabilidade do framework Apache Log4J 2.x encontrada em dezembro de 2021. A vulnerabilidade ganhou proporções gigantescas pela difusão do uso do software e por ser considerada uma das mais graves já descobertas. Conhecida como Apache Log4j Remote Code Execution (ou CVE-2021-44228), possui a marca de severidade mais alta - 10 em 10. Ela permite que o invasor execute um código arbitrário ao injetar dados em uma mensagem de log. Nesse caso, ressalta-se a importância de práticas de programação seguras como a validação de entradas e saídas, bem como a sanitização delas. Neste acontecimento especificamente, também, é sabido que a versão que possui a vulnerabilidade é antiga, por isso, existe a necessidade de manter as aplicações sempre atualizadas.

ANÁLISE 5

- **Notícia**

  O ataque de hackers a maior oleoduto dos EUA que fez governo declarar estado de emergência

- **URL**

  https://www.bbc.com/portuguese/internacional-57055618

- **Análise**

  O artigo noticia um ataque a um dos maiores oleodutos dos EUA, da empresa Colonial. Os crackers roubaram mais de 100GB de informações, além de desconectar totalmente as redes da instalação, o que configura como um ataque de Negação de Serviço (DoS, Denial of Service). James Chappell, cofundador e diretor de inovação da Digital Shadows (empresa de segurança cibernética), acredita que a DarkSide obteve detalhes de login de programas de acesso remoto, como TeamViewer e Microsoft Remote Desktop. As principais técnicas que podem ser aplicadas nesse caso é orientar (ou obrigar, caso possível) que os funcionários utilizem senhas fortes, que combinem em pelo menos 12 caracteres letras maiúsculas e minúsculas, números e caracteres especiais. Além disso, o uso de VPNs corporativas é uma prática interessante para casos de necessidade de acesso remoto em sistemas críticos.