**-Atividade Integradora do Terceiro Bimestre: Etapa 06 & 07**

Nicolas Gabriel Pereira dos Santos

**Etapa 06 – Tipos de Ataque:** Sua empresa deverá conhecer os tipos de ataques hackers existentes, para que a consiga sempre manter seu sistema protegido:

* **SQL Injection**: É provavelmente um dos tipos mais eficazes de ataques contra bancos de dados, já que se vale da injeção de um código malicioso de SQL (tipo predominante na área dos bancos de dados) para manipular um sistema, obtendo controle sobre este e podendo não somente ler informações registradas, mas também as deletar e instaurar um verdadeiro caos no sistema por meio do payload (nome do malware responsável).
* Uma das contramedidas é a validação de entrada, já que ao filtrar os usuários que tem acesso ao sistema, o cenário de ataques pode ser drasticamente reduzido. Outra filtragem que deve ser realizada é a de caracteres especiais da entrada do usuário, de maneira a impedir que injete códigos no sistema. A última alternativa a ser citada é o uso de firewalls web para bloquear indivíduos suspeitos e sua entrada.
* **Phishing**: O nome desta ferramenta da engenharia social já é capaz de explicá-la, já que o pescador (usuário mal-intencionado) lança uma isca para sua presa (vítima), que é fisgada ao corresponder a investida de seu predador. O hacker que realiza esta prática normalmente constrói-se como uma figura a quem se possa confiar, e com essa persona, extrai informações sigilosas da vítima, como por exemplo senhas de cartões ou contas, identidades, endereços e outras muitas informações que podem estar atreladas a vítima. É um dos tipos de ataques cibernéticos mais utilizados, visto a falta de requisitos técnicos em sua execução.
* Pode ser combatido por meio da criação de um sistema de comunicação restrito entre usuários da rede/programa e também por meio da criação de programas de conscientização entre os responsáveis pelo banco de dados, de maneira que nenhuma informação restrita chegue aos ouvidos de alguma entidade externa possivelmente mal-intencionada.
* **Keylogger**: Keylogger já é mais complexo que a técnica mencionada anteriormente, e consiste no ato de coletar informações digitadas no teclado da vítima por meio de um malware. Por meio de variadas maneiras, incluindo práticas de engenharia social como o *phishing*, o hacker instala o keylogger na máquina que deseja utilizar para obter informações, e desta maneira, passa a registrar todas as informações que entram no computador a partir do teclado – um típico dispositivo de entrada que é necessário para quase todas as tarefas realizadas na internet. Vale pontuar que a técnica não é exclusivamente ilegítima, mas é sempre sufocante, ardilosa e violadora quando se trata de privacidade. Há além do keylogger software, o keylogger hardware, que consiste em um microdispositivo instalado no computador principal.
* Para combater esta prática, pode-se efetuar uma navegação mais inteligente na internet, sem clicar em links ou navegar/baixar conteúdo de fontes não fidedignas. Por outro lado, também deve-se proteger a estação de trabalho física e atentar-se a conexão de dispositivos usb suspeitos ou possíveis keylogger hardware.
* **Screenlogger**: Screenlogger é uma técnica irmã do Keylogger, e difere-se ao capturar não os registros do teclado, mas da tela e do cursor do mouse. A ferramenta registra os cliques dados pelo dispositivo de entrada e registra suas posições junto as informações dispostas no monitor da vítima, enviando todas as informações compiladas diretamente ao criminoso. Este tipo de ataque pode ocorrer da mesma maneira que seu correspondente ao teclado, mas é costumeiramente empregado por meio de softwares, já que não requer presença física na estação de trabalho a ser invadida.
* Assim como o Keylogger, também existem cenários legítimos, já que a técnica pode ser utilizada para por exemplo, registrar momentos importantes a partir da tela de um dispositivo. No entanto, é costumeiramente utilizada para fins maliciosos e deve-se manter cuidado contra a abertura de arquivos suspeitos ou ao navegar por sites que possam ser não confiáveis.
* **Ransomware:** O Ransomware também detém um nome autoexplicativo, e consiste no sequestro de informações armazenadas em um dispositivo. É normalmente alicerçado em estratégias de chantagem, como por exemplo na cobrança de um resgate em troca da recuperação das informações criptografadas no dispositivo. Ransomware tem histórico de afetar não somente banco de dados (que são normalmente um livro preenchido por informações pessoais) mas dispositivos do mundo inteiro.
* Alternativas de resolução para este problema são a atualização constante das versões de softwares em seu dispositivo, a criação de backups, comunicação mais restrita entre dispositivos (para evitar que estrangeiros possam realizar algum tipo de phishing seguido pelo sequestro dos dados) e evitar inserir dispositivos USB desconhecidos nas máquinas de trabalho.
* **DDoS**: O ataque DDoS é resumidamente um ataque por negação de serviço, que consiste na inundação de acessos de cunho mal-intencionado com o intuito de sobrecarregar o servidor até que não possa mais haver tráfego. É normalmente fundado na utilização de bots para derrubar algum app ou site.
* Medidas necessárias no combate a prática são a aprimoração da estrutura (como a ampliação da largura da banda) e a utilização de firewall web para filtrar os usuários ao reconhecer suas intenções por meio da ferramenta. A diversidade de servidores de acesso (secção do site) pode ser uma saída inteligente para este tipo de problema, já que não haverá concentração de informação em apenas um âmbito.

**Etapa 07 – Plano de Contenção:** Sua equipe deverá criar uma contenção, para evitar possíveis invasões ao banco de dados...

**Nosso plano de contenção consiste em:**

1. Uso de um Firewall Web para analisar e eliminar usuários com tráfego suspeito
2. Prática de filtragem contra entradas com códigos maliciosos e contra caracteres especiais que possam ser inclusos em prompts suspeitos
3. Atualização constante de drivers e softwares
4. Backup regulado e rotineiro para garantir que nenhuma informação se perca
5. Educação dos administradores do sistema para evitar que cliquem em links suspeitos, caiam em técnicas de engenharia social e garantir que possuam ciência acerca dos riscos que correm ao estabelecer contatos
6. Proteção da estação de trabalho de maneira física e digital por meio de monitoramento constante dos dispositivos e seu desempenho
7. Auditorias de segurança regulares para assegurar-se do bom funcionamento dos dispositivos na empresa
8. Criação de uma rede única para o banco de dados e a eliminação do BYOD (Bring Your Own Device) para evitar a entrada de dispositivos infectados no sistema.