1. Ataque de Ransomware - WannaCry

1. **Data do Ataque:** Maio de 2017
2. **Tipo de Ataque:** Ransomware
3. **Descrição do Ataque:** O WannaCry foi um ataque de ransomware que criptografou arquivos em computadores e exigiu um pagamento em Bitcoin para desbloqueio. O ataque se espalhou rapidamente devido à exploração de uma vulnerabilidade do Windows, conhecida como EternalBlue.
4. **Vulnerabilidade Exploradas:** CVE-2017-0144. A vulnerabilidade permitia a execução remota de código em sistemas Windows não atualizados.
5. **Impactos e/ou Prejuízo:** O ataque afetou mais de 200.000 computadores em 150 países, com prejuízos estimados em bilhões de dólares, afetando hospitais, empresas e instituições governamentais.
6. **Tipo de Proteção que Poderia Ter Sido Aplicada:** Atualizações de segurança regulares e aplicação de patches críticos para corrigir vulnerabilidades conhecidas. Além disso, uma solução de backup robusta e estratégias de mitigação de ransomware poderiam ter reduzido o impacto.

2. Ataque de DDoS - Dyn (2016)

1. **Data do Ataque:** Outubro de 2016
2. **Tipo de Ataque:** Ataque de Negação de Serviço Distribuída (DDoS)
3. **Descrição do Ataque:** O ataque de DDoS contra a Dyn, uma provedora de DNS, envolveu a utilização de botnets formadas por dispositivos IoT comprometidos. O ataque congestionou os servidores de DNS da Dyn, resultando em falhas em sites populares como Twitter, Netflix e Reddit.
4. **Vulnerabilidade Exploradas:** Utilização de dispositivos IoT mal protegidos, que foram comprometidos e usados para formar uma botnet (Mirai botnet). Não havia um CVE específico para a vulnerabilidade, pois envolvia dispositivos IoT com segurança inadequada.
5. **Impactos e/ou Prejuízo:** O ataque causou interrupções significativas na disponibilidade de serviços online, afetando a funcionalidade de muitos sites e serviços, e gerou prejuízos financeiros e danos à reputação das empresas afetadas.
6. **Tipo de Proteção que Poderia Ter Sido Aplicada:** Melhoria na segurança dos dispositivos IoT, incluindo a alteração de senhas padrão e a aplicação de atualizações de firmware. Além disso, a implementação de soluções de mitigação de DDoS e a redundância de infraestrutura DNS poderiam ter ajudado a minimizar o impacto.

Esses dois ataques ilustram diferentes vetores de ameaça e a importância de medidas de segurança robustas para prevenir e mitigar o impacto de incidentes cibernéticos.