**Ataques Cibernéticos**

**Ataque 1: Change Healthcare (EUA) — Ransomware BlackCat/ALPHV**

1. **Data do ataque:** fevereiro de 2024
2. **Tipo de ataque:** Ransonware + exfiltração de dados (“double extortion”)
3. **Descrição do ataque ou de como aconteceu:**
   * Atacantes do grupo BlackCat/ALPHV usaram credenciais comprometidas de um serviço Citrix remoto sem autenticação multifator.
   * Conseguiram acesso inicial, moveram-se lateralmente na rede, roubaram cerca de 6 TB de dados sensíveis e criptografaram sistemas críticos.
   * O ataque paralisou processos de faturamento e pagamentos no setor de saúde.
4. **Vulnerabilidade explorada:**
   * Acesso remoto sem MFA.
   * Falhas de segmentação de rede e de monitoramento interno.
5. **Impactos e/ou prejuízo:**
   * Dados de **até 190 milhões de pacientes** expostos.
   * Interrupção de serviços hospitalares, clínicas sem recebimento de pagamentos.
   * **Prejuízo estimado: bilhões de dólares**, incluindo perda de receita, custos de recuperação e impacto reputacional.
   * Pagamento de **US$22 milhões de resgate** confirmado.
6. **Tipo de Proteção que poderia ter sido aplicada para evitá-lo:**
   * Autenticação multifator em todos os acessos remotos.
   * Princípio de privilégio mínimo e segmentação de rede.
   * Monitoramento e auditoria de logs para identificar movimentações suspeitas.
   * Backups isolados e testados regularmente.
   * Treinamento e políticas rígidas de gestão de credenciais.

**Ataque 2: Kyivstar (Ucrânia) — Ataque Destrutivo à Telecom**

1. **Data do ataque:** dezembro de 2023
2. **Tipo de ataque:** Ataque destrutivo (com elementos de intrusão APT + wiper)
3. **Descrição do ataque ou de como aconteceu:**
   * Hackers do grupo Sandworm (ligados ao serviço secreto russo) comprometeram uma conta de funcionário e permaneceram meses na rede da Kyivstar.
   * Escalaram privilégios, obtiveram acesso ao Active Directory e executaram destruição em massa de servidores e infraestrutura de nuvem.
   * O ataque derrubou serviços móveis e de internet em toda a Ucrânia.
4. **Vulnerabilidade explorada:**
   * Comprometimento de credenciais de funcionário.
   * Falta de segmentação e redundância de rede crítica.
5. **Impactos e/ou prejuízo:**
   * **Mais de 24 milhões de usuários** sem serviços de telefonia e internet.
   * Sistemas de alerta aéreo e operações bancárias ficaram prejudicados.
   * **Prejuízo estimado: cerca de US$90 milhões** em recuperação e investimentos emergenciais.
   * Impacto direto na segurança pública durante a guerra.
6. **Tipo de Proteção que poderia ter sido aplicada para evitá-lo:**
   * MFA e controle rígido de acessos privilegiados.
   * Monitoramento avançado para detectar intrusões persistentes (APT).
   * Segmentação de rede e redundância em sistemas críticos.
   * Backups resilientes e planos de continuidade de operações.
   * Políticas de segurança cibernética em nível nacional para proteger infraestrutura crítica.