Atividade 3

Tema: Ataques Cibernéticos

1: O ataque hacker ao STJ (Superior Tribunal de Justiça)

Ocorreu em novembro de 2020 e foi um dos maiores incidentes de cibersegurança envolvendo uma instituição pública no Brasil. O ataque paralisou completamente as atividades do tribunal por vários dias e teve um grande impacto no funcionamento da Justiça Federal.

Como ocorreu o ataque:

O ataque ao STJ foi realizado utilizando um **ransomware**, um tipo de malware que criptografa dados e sistemas, exigindo um resgate em troca de sua liberação. O sistema de TI do STJ foi comprometido, resultando no bloqueio do acesso a processos, documentos e sistemas essenciais. Todos os dados armazenados nos servidores da instituição foram afetados, incluindo informações sigilosas e processos jurídicos em andamento.

As técnicas ultizadas:

- **Ransomware**: O malware criptografou os dados dos servidores, tornando-os inacessíveis.
- **Exploração de vulnerabilidades**: Embora detalhes específicos da vulnerabilidade explorada não tenham sido divulgados amplamente, é provável que os

atacantes tenham explorado falhas em servidores ou sistemas desatualizados do tribunal.

- **Impacto nos backups**: Uma das principais dificuldades foi a falta de um backup imediato disponível para restaurar rapidamente os sistemas. Isso aumentou a gravidade da situação, prolongando a recuperação dos sistemas.

Consequências:

- **Paralisação das atividades**: O STJ ficou totalmente offline por vários dias, afetando julgamentos e processos em andamento.
- **Intervenção da Polícia Federal**: Após o incidente, a Polícia Federal e a equipe de TI do governo foram chamadas para investigar e mitigar o impacto do ataque.
- **Melhorias na segurança**: O incidente expôs fragilidades na segurança cibernética da instituição, levando a uma revisão e aprimoramento das medidas de proteção e controle dos sistemas judiciais.

Esse ataque foi um alerta importante sobre a necessidade de reforçar a cibersegurança em instituições públicas e privadas, principalmente em órgãos que lidam com informações sensíveis e críticas para o funcionamento do país.

2: Insomniac Games

Como ocorreu e quando ocorreu o ataque:
O ataque ocorreu a mais de 9 meses, O grupo hacker Rhysida vazou 1,3 milhões de arquivos da Insomniac Games, desenvolvedora de jogos responsável por títulos como Spider-Man e o icônico Spyro the Dragon. Os criminosos pediram US$ 2 milhões (aproximadamente R$ 9,7 milhões) em resgate para não divulgar os arquivos. A maior parte dos dados vazados, 1,6 TB de documentos, são do jogo Wolverine, com lançamento previsto para setembro de 2025

Tipo de ataque: A desenvolvedora Insomniac Games é de propriedade da Sony, sendo uma subsidiária da PlayStation Studios. Na semana passada, a Sony comunicou que estava investigando um possível caso de ransomware na Insomniac. Em setembro, a empresa japonesa passou por outra situação do tipo, quando o grupo Ransomed.vc invadiu o sistema da companhia.

As técnicas ultizadas(Fora o ransomware o resto são palpites):

Ransomware: O malware criptografou os dados dos servidores, tornando-os inacessíveis.
Remote exploit: Um tipo de exploit que permite a um atacante comprometer um sistema remotamente, sem

necessidade de acesso físico ao dispositivo. Eles exploram vulnerabilidades na rede ou nos protocolos de comunicação.

Client-side exploit: Explora vulnerabilidades no software cliente, como navegadores da web ou aplicativos, geralmente usando sites maliciosos ou arquivos comprometidos para executar códigos não autorizados.

Consequências:

Redefinições de jogabilidade, mudança de conteúdo e design de história de personagens

Os arquivos de Wolverine que foram divulgados são documentos sobre o level design, personagens e capturas de tela de dentro do jogo. Pelo que se sabe até agora, não há vídeos da gameplay.

Os documentos vazados revelam ainda o acordo entre Sony e Marvel para o lançamento de três jogos do X-Men. O primeiro é Wolverine, os outros ainda não estão decididos — e seu lançamento deve acontecer em 2029 e 2033. O orçamento para cada jogo é de US$ 120 milhões (R$ 582 milhões).

Os hackers também publicaram documentos internos do RH e capturas de tela de conversas do Slack da Insomniac. Até

mesmo dados pessoais de Yuri Lowenthal, dublador do Peter Parker nos jogos Spider-Man, foram vazados.
O grupo Rhysida, de acordo com investigações, surgiu em 2021. Na época, foi conhecido como Gold Victor. A nacionalidade do grupo é desconhecida, com suspeitas caindo sobre a Rússia ou um conjunto de membros deste país com hackers da Bielorrússia e Cazaquistão.

Tipo de proteção:

Para a proteção contra ransomware, tanto no stj quanto na insomniac, eles poderiam ter optado pelo seguinte método

1. Backup Regular e Seguros

- **Backup frequente**: Mantenha backups atualizados de todos os dados críticos. Isso garante que, mesmo que os dados sejam criptografados por um ransomware, você poderá restaurá-los sem pagar o resgate.
- **Backup offline**: Tenha pelo menos um backup fora da rede (offline) ou em locais não acessíveis diretamente, como armazenamento em nuvem, para evitar que o ransomware comprometa também os backups.

2. Atualizações e Patches

- **Manter sistemas atualizados**: Aplicar todas as atualizações de segurança e patches fornecidos pelos

fabricantes de software é crucial, especialmente para corrigir vulnerabilidades conhecidas que os ransomware exploram.

3. Antivírus e Antimalware

- **Ferramentas de segurança**: Utilize software de antivírus e antimalware confiáveis que incluam proteção contra ransomware. Estas ferramentas podem identificar e bloquear ameaças antes que causem danos.
- **Análise proativa**: Use soluções que monitorem o comportamento de arquivos e detectem atividades suspeitas relacionadas a ransomware.

4. Segurança de E-mails

- **Filtro de spam**: E-mails são a principal porta de entrada para ransomware via phishing. Utilize filtros de spam eficientes para bloquear anexos e links suspeitos.
- **Anexos e links maliciosos**: Oriente os funcionários a nunca abrir anexos de e-mails ou clicar em links de remetentes desconhecidos.

5. Autenticação Multifator (MFA)

- **MFA**: Implementar autenticação multifator (MFA) para acessos críticos dificulta a exploração de credenciais roubadas por ransomware.

Agora na parte da insomniac que foi usado mais de uma técnica como o possível exploit, a forma séria essa:

1. Atualizações e Patches Regulares

- **Aplicar patches de segurança**: Mantenha todos os sistemas, aplicativos e dispositivos atualizados com os últimos patches de segurança. Isso corrige vulnerabilidades conhecidas que podem ser exploradas.
- **Gerenciamento de patches automatizado**: Utilize ferramentas que automatizam o processo de verificação e aplicação de patches para garantir que nenhum sistema fique desatualizado.

2. Ferramentas de Detecção e Prevenção de Intrusão (IDS/IPS)

- **IDS/IPS**: Sistemas de Detecção de Intrusão (IDS) e Sistemas de Prevenção de Intrusão (IPS) monitoram o tráfego de rede em busca de padrões de ataque e tentativas de exploração. Enquanto o IDS alerta sobre possíveis ataques, o IPS pode bloquear automaticamente atividades suspeitas.

3. Segurança de Aplicações (Hardening)

- **Configuração segura de software**: Reduza a superfície de ataque de servidores e aplicativos desabilitando serviços e funcionalidades desnecessárias.

- **Controle de exceções**: Implemente o manuseio adequado de entradas e erros nas aplicações para evitar vulnerabilidades, como *buffer overflows*.

4. Uso de Firewalls

- **Firewalls de próxima geração (NGFW)**: Utilize firewalls que oferecem inspeção profunda de pacotes (DPI), análise de comportamento e detecção de ameaças em tempo real. Eles ajudam a bloquear tráfego malicioso e impedir a exploração de vulnerabilidades.

5. Autenticação Multifator (MFA)

- **Implementação de MFA**: A autenticação multifator adiciona uma camada extra de segurança, dificultando o uso de credenciais roubadas em exploits que visam ganho de acesso não autorizado.