**Alan Diek da Silva Guimarães**

**Segurança Cibernética - Entrega de Exercício**

**a) Quais tipos de ataques foram utilizados em cada caso?**

**American Express**

Tipo de ataque: Na American Express ocorreu vazamento de dados devido a uma violação de segurança e embora o tipo exato não tenha sido explicitado, casos assim geralmente envolvem acessos não autorizados, muitas vezes por phishing ou ataques a credenciais.

**Tesla**  
Tipo de ataque: Na Tesla ocorrei uma ameaça interna, onde funcionários vazaram dados pessoais, onde as informações foram comprometidas por pessoas com acesso autorizado.

**Cisco**  
Tipo de ataque: Na Cisco ouve sequestro de dados. Um grupo de hackers utilizou técnicas de ransomware, sequestrando dados e exigindo um resgate para não os divulgar.

**Sony**  
Tipo de ataque: Na Sony ouve uma invasão e roubo de dados. Os hackers conseguiram invadir o sistema da Sony, provavelmente utilizando técnicas de malware e exploits, para roubar informações de usuários.

### **b) Quais medidas poderiam ser aplicadas para a prevenção de tais ataques em cada caso?**

**American Express**

Medidas preventivas: Pode ser implementação de autenticação de dois fatores para dificultar acessos não autorizados. Educação e conscientização dos usuários para identificar e evitar phishing.

**Tesla**

Medidas preventivas: Pode se aplicar políticas de acesso rigorosas, limitando o que cada funcionário pode acessar com base em sua função, monitoramento constante dos funcionários e auditorias internas para identificar possíveis vazamentos.

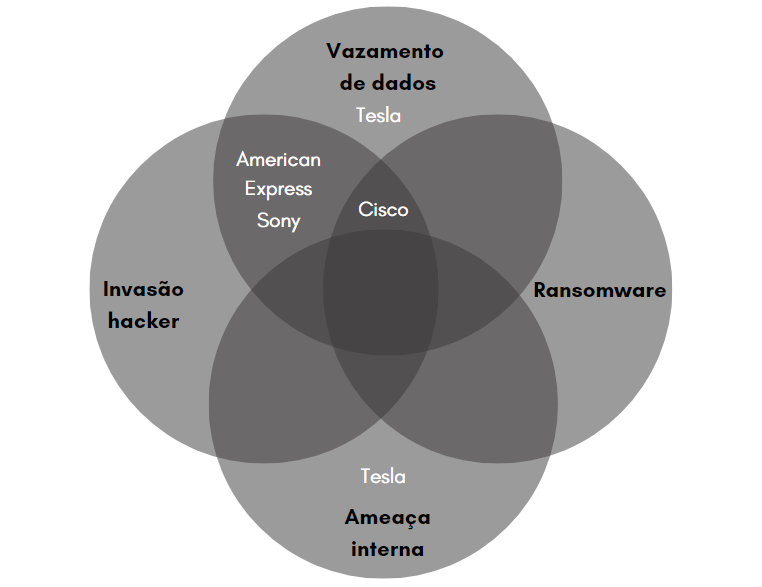
**Cisco**

Medidas preventivas: Efetuar o backup regular de dados e um plano de resposta a incidentes, para minimizar os impactos de um ransomware. Também podem ser utilizadas de ferramentas de detecção de intrusão e firewalls para impedir que hackers comprometam os sistemas.

**Sony**

Medidas preventivas: Efetuar atualização constante dos sistemas e softwares para evitar que vulnerabilidades conhecidas sejam exploradas. Pentests regulares para identificar falhas de segurança antes que os hackers obtenham conhecimento delas.

### **c) Faça um Diagrama de Venn para relacionar os ataques que os casos descritos têm em comum.**



### **d) Aplicação de medidas de prevenção na empresa**

Várias das medidas acima podem ser aplicadas basicamente em qualquer empresa. Por exemplo:

Educação dos funcionários, treinando os sobre os riscos de phishing e engenharia social, que é fundamental em qualquer organização.

Implementar a autenticação de dois fatores, com essa camada extra de segurança para todos os sistemas críticos, protegendo informações sensíveis.

Realizar auditorias periódicas nos sistemas e monitorar atividades suspeitas para identificar e prevenir ataques internos.

Efetuar backups regulares dos dados, o que é essencial para proteger a empresa contra ransmware.

Essas práticas ajudam a reduzir as vulnerabilidades e a preparar a empresa para lidar com ameaças cibernéticas comuns.