**Ransomware Case Study Knowledge Check**

**Question 1**

**Describe the ransomware attack against the City of Atlanta in the United States.**

* **Describe the attack vector.**
* **Describe what City departments and functions were impacted?**
* **Did the City know they had vulnerabilities?**
* **Did they attempt to address them?**
* **Describe what the City of Atlanta have done to prevent the attack or minimize its consequences.**
* **Describe what the City of Atlanta has done since the attack to improve its security posture?**
* **Describe the ransom demanded, what was paid and what the overall costs were to the city.**

**Attack Vector:**

The SamSam ransomware was the attack vector utilized in the City of Atlanta ransomware incident. To obtain unauthorized access, the attackers may have used phishing attacks or unpatched systems to take advantage of weaknesses in the city's network.

**Affected City agencies and services:**

The ransomware assault had a significant negative impact on several city agencies and services. There were disruptions to vital departments and systems, such as the court system, public safety agencies, and utilities services. Essential files were the focus of the attackers, who encrypted them and demanded a payment to unlock them.

**Awareness of Vulnerabilities:**

It's unclear from the text whether the city knew of any specific weaknesses that allowed for the attack, but it's not uncommon for organisations to struggle to keep their security procedures up to date, which can lead to vulnerabilities.

**Attempts to Resolve Vulnerabilities:**

It appears from reports that the City of Atlanta encountered difficulties in quickly resolving vulnerabilities. It's possible that outdated software and a deficiency in strong cybersecurity defences let the ransomware attack succeed.

**Actions Made to Prevent and Reduce Repercussions:**

In the wake of the attack, the City of Atlanta implemented measures to reduce repercussions and avoid such situations in the future. This involved making investments in network security measures, improving cybersecurity, and patching systems with known vulnerabilities.

**Enhancements to Post-Attack Security:**

Following the attack, the City of Atlanta took steps to strengthen its overall security stance. This probably included investing in employee cybersecurity training, improving incident response capabilities, and carrying out extensive security evaluations.

**Ransom Demanded, Payment, and Overall Costs:**

To obtain the decryption key for the encrypted files, the attackers sought a ransom in the amount of roughly $51,000 in Bitcoin. The city, however, refused to comply with the extortion demand and instead decided to repair the compromised systems and restore services in place of paying the ransom. The anticipated total expenses of the event to the City of Atlanta were substantially greater, amounting to millions of dollars for cybersecurity enhancements, system upgrades, and recovery.

In conclusion, a disruptive ransomware attack affected vital services for the City of Atlanta. The incident forced the city to make investments in strengthening its cybersecurity, fix its weaknesses, and implement defences against such incidents in the future. The choice to forgo paying the ransom was made as part of an endeavour to strengthen the city's cybersecurity defences and deter ransomware payments.