Genesis Grant

CTEC 345-002

Who are the threat actors? What type of threat actors are they? Include a description and explanation for the threat actors.

What protection(s) has been compromised? Explain your response.

How might Penetration Testing benefit the organizations in the articles? Outline all of the steps performed in pen testing and account for vulnerabilities.

**Article: “Ransom gang claims attack on Prince George County school district”**

1. In this article the **threat actors** are the Rhysida group. Although there is not much information about the group, as they are relatively new, they seem to operate as **Black hat hackers**, with the **intent/motivation** to make profit from the information they gained through **data exfiltration**. Rhysida is a cyber ransomware group who are also notable for attacking Prospect Medical Holdings thus causing them to shut down multiple facilities and prolong services and patients.
2. Primarily the confidentiality of the stolen information was compromised. Confidentiality is supposed to ensure that only authorized users can access information and divert adversaries, though the **hacker** group was able to bypass and gain access to a variety of confidential information.
3. Penetration testing would have/will benefit the PGCPS by allowing them to see beforehand what vulnerabilities they may have overlooked and possibly come up with defenses prior to the attack. As well as protecting not only employee information, but students and parents.
   1. Planning
   2. Phase 1 Reconnaissance
      1. **Footprint/** get more outside information on the entity. Possibly use **passive reconnaissance**, especially because it is a school system and a variety of information is **open source intelligence** already. Including school emails, employee names, departments, telephone numbers, etc.
   3. Phase 2 Penetration
      1. Utilize **blue teaming/red teaming** to find potential adversarial vectors, then find best blue team defenses in order to protect system.
      2. Possible utilize NIST Cybersecurity Framework/NIST Risk Management Framework to fully analyze and focus on certain attacks/defenses that may potentially cause the most harm/risks.
      3. **Threathunt:** Search for overlooked threat actors. Possibly even **insider threats**, because of such a large school district.

**Article: “Data of 300K+ Standard Insurance customers exposed in MOVEit-related NTT DATA attack”**

1. In this article the threat actor is Cl0p, a ransomware group. They are also Black hat hackers, but their personal gain is not described though they inflicted malicious damage. Through a **data breach**, they have gained large amounts of social security numbers, names and personal information of over 300,000+ people close to the Standard Insurance company. This could be in part inflicted by **unsecure protocols** (protocols that did not accurately secure the system), unsecure **system integrations** (sometimes when entrusting **third party** vendors to hold data they may not have the same appliances and software as the company and when integrating work arounds, they can lead to vulnerabilities), **insider threats**, etc.
2. In this instance, the confidentiality protections of the customers were compromised. Social security numbers, names, etc. were exposed and thus could potentially also hurt the company(s) involved reputation leading to loss of public trust and ultimately **financial loss**.
3. Penetration testing would have/will be beneficial for the NTT Data Americas company as they could also potentially limit any other possible **attack vectors** and secure further information.
   1. Planning
   2. Phase 1 Reconnaissance
      1. Footprint/getting outside information. Possibly utilize **active reconnaissance** as this is a larger corporation and have more users, so adversaries may want to find data by looking to delve into the actual company databases.
   3. Phase 2 Penetration
      1. Utilize blue teaming/red teaming to find potential adversarial vectors, then find best blue team defenses in order to protect system.
      2. Possible utilize **NIST Cybersecurity Framework/NIST Risk Management Framework** to fully analyze and focus on certain attacks/defenses that may potentially cause the most harm/risks.