Teaching Security Lesson 1: The Security Mindset

Assignment: Interpreting the Cybersecurity News

Example Responses

Read your assigned article and answer the questions below.

- Be sure to include details of the article in your answers, and cite any information you quote directly from the article.
- Your answers should be understandable to any individual who has read the article. The reader should not need to have taken classes in computer science.
- Including ideas from the rest of this lesson (such as the threat modeling card deck) will help strengthen your answers to the questions.

Article/Incident: *LabCorp breach article from Krebs on Security*

1. What aspects of this incident illustrate the importance of cybersecurity?

Example answer: *When companies like LabCorp hire third parties to provide services, and they share customer or patient information, they need to be sure that the third party has security measures in place that will keep the data from getting hacked. LabCorp has a responsibility to their patients to maintain the security of the patient data because it could be misused, but they also need to be paid for their services, and maybe it is more efficient to go to a collection agency like AMCA when customers have overdue bills.*

This balance is at the core of cybersecurity—providing needed access to data while protecting it against people who might misuse it—and everything is a trade-off. In this case, the third party had a vulnerability that was left exposed for several months, and that means that a large number of people were affected.

Learning objectives: 1 (what is cybersecurity), 2 (why cybersecurity is important), 3 (unique challenges)

2. What exactly happened in this incident?
   - What did the attackers do?
   - How did they do it? What vulnerabilities did they exploit? (If known.)

Example answer: *LabCorp had hired AMCA to collect unpaid medical bills, and a hacker was able to retrieve the billing information ("first and last name, date of birth, address, phone, date of service, provider, and balance information") of about 7.7 million customers from AMCA. The article also states that about 200,000 people who tried to pay their debt also had their bank account or credit card numbers exposed. According to the article, data had been exposed from August 1, 2018 until March 30, 2019.*

The article doesn't say for sure where the vulnerability was except that it was AMCA (not LabCorp) that got hacked, but it says there was another breach with patient data from Quest Diagnostics where there was a problem with AMCA's payment web page. It does say the vulnerability wasn't detected for a long time, so the attackers likely had a very long time to breach the system. This is an example of something we learned from the threat modeling activities: attackers often have more time to devote to figuring out how to breach a system than a company spends looking for vulnerabilities.

Learning objectives: 2 (why cybersecurity is important), 3 (unique challenges), 5 (predict threats and impacts)

3. Why was this system targeted? What did the attackers stand to gain?

Example answer: *This system may have been targeted partially because the company is known for being merciless about collecting on debts, and so the attackers probably thought they would have the most accurate and up-to-date contact information for the customers. This information could be enough for an attacker to open credit cards under the victims' names, and purchase goods or services that would then become the debts of the victims whose information was exposed in the breach.*

We also saw in the examples from the threat card deck that the hackers could sell the information to someone else who wanted to use it that way. These are examples of being motivated by monetary gain.

Learning objectives: 3 (unique challenges), 4 (threat modeling process), 5 (predict threats and impacts)

4. Who was impacted by this incident? How were they impacted? (If the attack was unsuccessful, who *could have been* impacted and how?)

Example answer: *Every customer of LabCorp who was behind in payment for their medical testing, as well as possibly other customers of LabCorp whose information was provided to the third party collector. According to the article, the list of victims still has not been provided to LabCorp, but they are going to work to notify all the individuals affected.*

Their identities could be used by the hackers to buy goods and services in the victims' names and put them in even more debt. From the threat modeling activity, this is definitely a threat to the victims' financial wellbeing.

The company AMCA will also be impacted if LabCorp decides they will no longer continue to do business with AMCA. The other medical lab company in the article, Quest, already said they won't, and other companies may stop using them too because their reputation is damaged. This means that groups of employees of AMCA will probably lose their jobs, which is a threat to their financial wellbeing and their emotional wellbeing.

Learning objectives: 4 (threat modeling process), 5 (predict threats and impacts)