Katelynn Johnson

Taste Unlimited security plan recommendations

**Likely Cyber Attacks Based on Network:**

 Bad actors (or hackers) will most likely target this network for user data or theft. Taste Unlimited stores company and user information at their headquarters. The company information that is stored and would likely to be targeted is the companies accounting and banking information. A bad actor would target this information and attempt to find a way to steal this information for a monetary value. There are a few ways a bad actor would attempt to steal this information. They could “sniff” the traffic to try and steal bank transfers over the internet to acquire bank account numbers. They could try and gather username/password combinations from sniffing the traffic also as a means to gain access to the company’s banking account. The bad actors could make a website that looks extremely similar to that of the actual company banking website. If a store manager were to input their username/password banking combination into this website the bad actor would have this information.

 A bad actor could target the user data rather than the company’s data. The user data would be of value to the bad actors because of the monetary value that comes with this information. The bad actors can attempt to steal this information by targeting the database where this information is stored directly for Taste Unlimited customer who have a user account. This account would be used to place orders online and the user has the option to save credit card information to their account for the ease of repeated transactions. The attack to target a database is more sophisticated because there is a lot of layers of security that a bad actor would have to go through in order to be able to reach the database. A way that a bad actor would try and access the database would be to send an SQL injection to the database. If successful, the bad actor will gain access to the user stored data in the database to include credit card information. An easier attack would be to steal user credentials but sniffing traffic or duping the user. The bad actor could sniff the traffic and wait until a user tries to log into their account. By doing this, a bad actor could try and do a man-in-the-middle attack where the bad actor sits in the middle of the user and the database and watches all the traffic. The bad actor could then steal username and password combinations for the user if the traffic is not encrypted. The bad actor could create a false website that looks very similar to that of the user log in page. The bad actor could then steal a user’s credentials if they use the fake website to access their account.

The bad actor could target the credit card transactions directly. Bad actors would do this by targeting the traffic that is passed when trying to “authorize” each credit card transaction. When a credit card is swiped at a store during checkout, this information needs to be verified as legitimate information. This verifying traffic is what the bad actor would target to steal the credit card information.

**How To Prevent From Likely Cyber Attacks:**

 To prevent from the attacks above I recommend the following methods:

1. Require all user account as well as company account to have strong password. A “strong” password is categorized as one that is at least 12 characters in length, and it has at least 1 uppercase, 1 lowercase, 1 number, and 1 special character in it. The passwords are required to be changed every 90 days and the user is not allowed to have a similar password as their previous password (ie they cannot change their password from $unSh1neSUnd@Y to $unSh1neSUnd@YY).
2. To protect against bad actors accessing the database, protection against SQL injections is required. This is done by not allowing the website to “talk” to the database directly. Meaning, the sql queries are not sent directly to the database from user input. This can be done by reading website code and taking the appropriate steps to make sure the code does not allow for users to submit SQL queries directly.
3. Make sure that user account information is stored securely. The easiest way this can be done is to make sure passwords and not stored in plain text in the database. Make sure to hash the user password.
4. Make sure all traffic is encrypted. This is done by purchasing a certificate from a credible Certificate Authority. This will allow for your websites to use HTTPS. You can use a “self-signed” certificate but this is not credible. Using HTTPS over HTTP is very important. This is because HTTP sends all traffic in clear text, allowing for information to be stolen easily if “sniffed”.
5. The use of firewalls are important. These rules can be set up to only allow company bank information to be accessed from certain IP’s. Meaning that a manger cannot login to the company bank account from just anywhere. A firewall rule can be set up to where only internal IP addresses are allowed to go to the company banking IP address and vice versa. This would prevent an outside IP addresses from accessing the company’s banking information.
	* This same type of rule can be set up to make sure only internal IP addresses are communication with headquarters to access company information. On the other hand, all external traffic where users would be logging in from would be set to access only Taste’s websites.
	* A rule can be set up to where no external IP can access the databases directly.
	* A firewall would be set up at each of the stores to only allow traffic to and from headquarters.

**Recovery and Incident Response if an Attack Occurs:**

No matter how many security precautions are taken, there is still always a chance that a security breach will happen. Because of this, it is important to take preparation steps beforehand and to have a plan for recovery.

* **In Preparation:**

**Backups**

To “prepare” yourself for an attack it is important to “save” your information. This means regular back-ups for your network are needed. This is important because if servers were compromised, corrupted, or stolen by encryption, we need a way to be able to recover them.

Before deciding on a backup schedule, it is important to decide and prioritize what needs to be backed-up. This is because there will be a budget for backups. Backups cost money because of the medium used for back-ups which can either be magnetic tape (recommended) or optical disk. Prioritizing what needs to be backed up is done with a few factors.

* First, decide what is most important to the company (this is also most likely what is most desirable to bad actors).
* Second, decide what is regularly changing as in what servers have constant data going to and from them.
* Third, decide what cannot be “down” or unavailable for a long time in order for the company to continue normal business.

 With these recommendations, it should be easier to prioritize what gets back-up more often. With a prioritized list, now a backups schedule can be decided on. It is recommended that higher priority backups are done a few times a week while lower items on the list can be done weekly. Make sure backups are stored in a location that is secure! A backup of a server is just the same of importance as the running server. Make sure backups are labeled properly. This is important in the recovery process.

**Intrusion Detection System/ Intrusion Prevention System**

IDS/IPS’s are a great tool to have on your side in detecting suspicious activities. These systems can be host based or network based. These systems alert when there is suspicious activity based on what it is configured to look for. Network traffic happens at the speed in the thousand’s per second. This is much faster than any human can handle in real time. The IDS/IPS allows for real time monitoring of all this traffic. Do not forget these systems only look for an alert for traffic when it matches a pattern rule. Therefore, these systems are only as good as the rules that are configured for them. These systems are a great starting point when looking for suspicious traffic on the network but they are not absolute. Meaning, this should not be the only measure used to gage on how “secure” the network is.

* **Response:**

If a breach does occur. It is important to figure out how the breach happened first before conducting any recovery steps. This is so steps can be taken to make sure this same type of breach does not occur again in the future. This would be covered by a cyber forensics team. In order for a forensics team to do their job, information must be gathered, and systems preserved at their current states. This should be done a quickly but as accurately as possible so the recovery process can begin. The recovery process would include fixing what caused the cyber breach, and then bringing all systems back up to operating states.