Joshua Lane
IT419

Threat Assessment

This brief report covers the possible threats Taste Unlimited may face given the current infrastructures and sensitive information it has in said infrastructure. There are many different bad actors after this sensitive information or the company itself, each with their own resources, capabilities, motivations, and aversion to risk. These bad actors include: professional cybercriminals, APT (Advanced Persistent Threat), insiders (company's own employees), hacktivists, and script kiddies/individual actors.

Professional cybercriminals tend to have more resources than your average hacker. They take their time to hide their presence online/cover their tracks. We do have many Wi-Fi access points at our several locations as well as servers at HQ that need to be thoroughly secured. These more organized criminals are typically out for financial gain and will attack with ransomware. Financial losses due to ransomware for companies like Taste Unlimited are at an all-time high during COVID. They will lock up company resources, creating a denial of service due to not being able to use these company resources. They will then sell off this sensitive information (namely customer credit card information) while they have access to it.

Advanced persistent threats can include professional cybercriminals but can also include state-sponsored attacks. Increased activity from Russian/Chinese hacking teams has begun to wreak havoc on American Companies. This also includes industrial spies eavesdropping on our networks, placing deep-seated listening devices/software in important infrastructure. Groups such as these have a much larger pool of resources due to state-funding. It is hard to garner motivations of these groups, but mostly it is for garnering money/information. They sell the information on the black market for more money. State-sponsored accounts can commit IP theft

to pose as another group and create panic among Americans, essentially making Taste Unlimited collateral damage. These groups do not care about making their presence known, but it is hard to pursue legal action since they reside in a different country more often than not.

Insider threats are the company's own employees. Most of this is employees simply being negligence and incompetence, so this can be solved with regularly scheduled employee training programs to keep them fresh on current secure practices in the cyber world. Much more damage can be done by disgruntled employees who know they will be fired soon. Recently fired employees can be a problem as well if the proper precautions are not taken regarding retiring previous employee access and ID's. We allow managers to use Wi-Fi, so we need to be especially cautious with securing our wireless networks.

Another bad actor to consider is a group of hacktivists. Since we are a food company, there may be groups out there that are against harming animals and will therefore seek to put Taste Unlimited out of business. They may not have as large a resource pool as state-sponsored groups, but they have strong motivations with their own sense of justice. Highly motivated individuals can be a large threat to Taste Unlimited. They are not averse to risking everything to take this company down. They have similar capabilities to state-sponsored groups.

Script kiddies/individual actors have motivations that range from entertainment to financial gain. Script kiddies do not have a large pool of resources and use simple software programs to deny service etc. Individual actors are typically motivated by financial gain. Each has a small pool of resources and pose less of a risk than groups that are highly motivated with more resources. Simple security measures should be able to stop most of these types of bad actors.

Security measures should be in place with each of these bad actors in mind to prevent data leakage and denial of service. It is not a matter of if these attacks will happen, but when they will happen. A risk assessment regarding these bad actors should be drawn up, and backup plans for denial-of-service attacks/data loss should be completed. For more information, proceed to the next page to read in depth about these bad actors.

Joshua Lane
IT419

More Information

https://www.sentinelone.com/blog/threat-actor-basics-understanding-5-main-threat-types/

https://www.accountingtoday.com/opinion/whats-new-about-normal-3-vulnerabilities-for-accounting-and-finance-professionals-today