**You are providing a recommendation to use input validation on a web application.**

**Answer the following question: provide a valid rational for your explanation. Provide 2 resources that support your explanation.**

**Explain how input validation is used to prevent SQL injection attacks.**

When using any web application or website, especially where fillable forms (login, survey, etc.) are present, the user is interacting with these forms client-side (in the browser), but the intent is that this information will eventually be transmitted to a server and this server will take action on a database or other application/microservice to update, retrieve, delete, or create information.

Because the information in these form fields is encapsulated in a request to the server which eventually makes a request of a database, potentially one containing other information that should not be updated, retrieved, deleted, or created in the context of the user’s session, it is important that all input into these fields is validated. “For example, an application may allow a user to select a four-digit “account ID” to perform some kind of operation. The application should assume the user is entering a SQL injection payload, and should check that the data entered by the user is exactly four digits in length, and consists only of numbers (in addition to utilizing proper query parameterization).”

Input validation can be used to prevent SQL injection attacks by checking all input server-side. One must check to make sure that the input is syntactically valid, that is the data falls within a valid range of characters expected, and that the data is sanitized (only valid characters or code are allowed). This can be done by whitelisting or blacklisting data:

*“...input validation can be either whitelisted or blacklisted, it is preferable to whitelist data. Whitelisting only passes expected data. In contrast, blacklisting relies on programmers predicting all unexpected data. As a result, programs make mistakes more easily with blacklisting.”*

*Anton, K., Bird, J., &amp; Manico, J. (n.d.). C5: Validate all inputs¶. C5: Validate All Inputs - OWASP Proactive Controls documentation. Retrieved March 18, 2022, from https://owasp-top-10-proactive-controls-2018.readthedocs.io/en/latest/c5-validate-all-inputs.html*

*Input validation. WhiteHat Security Glossary. (n.d.). Retrieved March 18, 2022, from https://www.whitehatsec.com/glossary/content/input-validation*

**For this question, an event is any observable occurrence in a computer, device, or network. An event can be anything that you may see reported in a log file. Events can be good or bad. Any event that results in a violation of or poses an imminent threat to the security policy of the company is an incident.**

**Answer the following question(s): provide valid rationale for your choices. Provide 2 resources supporting you position.**

**Would the process of incident response change if a crime was intentionally committed versus an accidental event, such as an employee who clicks a phishing email link? That is, would the process of detecting, identifying, resolving, and documenting system or network intrusions change? Why or why not?**

The response should not change based on whether it was a security incident that occurred independently of interaction with an employee or because an employee fell victim to a technical social engineering attack (the example given). Regardless of why the incident occurred, there was malicious and/or criminal intent by a third party (the threat actor). The incident should be responded to based on the severity of the threat and whether or not the incident warrants legal action.

Per the textbook, “...incident response may have legal consequences...the formal investigation will include special techniques for gathering and processing evidence for the purpose of potentially presenting that evidence in a court of law.”

In the case that you are dealing with a smaller contained security incident, “...internal teams or consultants may be all that are needed to investigate and analyze an incident.”, but in a case where legal action is being considered, the incident response should be, “...conducted under the guidance of law enforcement.”

*Oriyano, S.-P., &amp; Solomon, M. (2020). Hacker techniques, tools, and incident handling. Jones &amp; Bartlett Learning.*

**You want to install a biometric access control outside of a restricted room in your facility. You are considering using a retina pattern system and a voice recognition system.**

**Answer the following question: provide a valid rationale for your choice. Provide 2 resources supporting your position.**

**What are the top three factors that will influence your decision, and why?**

The top three factors that would influence my decision to install a retinal pattern scanner and voice recognition system are:

1. Price
2. Accuracy
3. Privacy

While the benefit may be worth it for some companies, it is important to consider the cost of implementing biometric access control. According to vizpin, “...prices for biometric access control systems range from a total of $2,500-10,000 per door”

Depending on the size of the company and the sensitivity of the assets they are protecting, it may or may not be worth the very significant investment to use biometrics over traditional lock/key security.

When considering which biometric access control implementation you want to use, you also have to consider accuracy. “Research by the National Institute of Standards and Technology (NIST) shows that iris scans are 90-99% accurate.” while voice recognition is “...90% accurate on average.”

The final factor that would influence my decision is the privacy of the users that are utilizing the biometric access control system. For a system like this to function as intended it must store a record of the biometric that it can compare each scan to; if this information cannot be properly secured it poses a serious threat to the privacy of those users.

*Access control system pricing: 2022 average cost (per door). VIZpin Smart Property Systems. (2021, May 7). Retrieved March 18, 2022, from https://vizpin.com/blog/access-control-pricing/*

*Navrup, T. (2021, May 24). What are biometrics? the Pros/cons of biometric security. Auth0. Retrieved March 18, 2022, from https://auth0.com/blog/what-are-biometrics-the-proscons-of-biometric-security/*