SMEs cybersecurity risks

Cybersecurity risks are always prevalent in any system or network. developing even the most simplistic applications would require some sort of protection from cyber attackers or hackers who are constantly trying to infiltrate your software to gain means of unnecessary access, in other words, unethical hacking. Similarly, small businesses are placed as a jackpot for hackers due to a variety of reasons, for instance, lack of resources to protect their systems, untrained staff due to newly formed company and lack of protective measures that can lead to massive damage to a firm’s reputation and also risks people’s sensitive data protection against cyber-attacks. However, not only the company is to be blamed for cybersecurity risks but also the people it.

**Threats**

* **Internal attacks:** the attacks could be launched internally where employees could have access to unwanted data or higher privileged access, which are competent enough to cause a tremendous amount of damage to SMEs. To mitigate this issue, firms need to identify authorized accounts of those who have higher privileged access to internal systems. Account activity needs to be tracked and tools to detect malicious activity before any damage has been dealt with
* **Lack of knowledge**: employees lacking cybersecurity knowledge creates a higher risk for SMEs to counter cyber-attacks since they aren’t aware of cybersecurity strategies, policies and types of attacks that can astray them from falling under the trap. For instance, an employee with lacking skills can be convinced into providing his credentials to an attacker

**DDoS attacks:**

* SMEs can face massive amounts of web traffic that can slow down their business operation to a great extent. It can also cost SMEs huge bandwidth charges since DDOS attacks eat up a considerable amount of bandwidth and cost businesses by the hour
* **SQL injection:** not implementing many security barriers can leave SMEs vulnerable to cyber-attacks, making their data transparent to attackers. SQL injections are some of the most common forms of cyber-attacks that alter the database behind any web application. Malicious SQL statements are passed on to databases that misbehave in contrast with its original functionality, sony( april 2011), personal data of 77 million users, network vulnerability
* Malware, target example In December 2013, abnormal bank movements , installed malware in cash registers to read credit card information

**Prevention against cyber attacks**

* Privileged access to accounts to mitigate internal attacks within the organization
* Use multiple authentication techniques or in other words, two-factor authentication. For instance, when logging into any system would require fingerprint ID and password before accessing the system or other security measures such as facial recognition that uniquely identifies yourself
* Backing up data regularly since SMEs are more vulnerable to cyber attacks