EINPRESSWIRE

Cybersecurity issues and challenges for SME in 2022

DOMINICAN REPUBLIC, November 2, 2022 /EINPresswire.com/ -- Small and medium enterprises operate under a stringent budget with most of the resources delegated to work on activities that add more value to the operational aspects of the business. In pursuit of the main business objectives, SMEs tend to neglect some of the key points of data integrity that can jeopardize the overall functioning of their businesses. Therefore, it is imperative that SMEs focus on making their business secure and identify areas that can hamper the implementation of a robust network infrastructure. Let's take a look at some of the issues that SMEs face due to the lack of implementation of network security and also shed light on the possible implications on the functioning of SMEs.

Issues Faced by SMEs Due to the Lack of Implementation of a Secure Network Infrastructure

The objective of small enterprises is to generate revenue with limited funds hence the main emphasis is to streamline the business activities. SMEs often tend to ignore the security aspect of their businesses as a result risk losing important data and operational functionality. According to the IBM-Ponemon Institute "Cost of a Data Breach 2021" report, the average cost of enterprise data breach stands 17 years high at US$4.24 million. Let's examine some of the main reasons why data breaches and cyberattacks happen to SMEs. Another report by Check Point Research shows that in 2021, a 50% increase was observed in overall attacks per week on corporate networks as compared to 2020.

Reasons for the Lack of Cybersecurity and Cyberattacks

Low Budget – Enterprises tend to allocate most of their budgets to ongoing projects and focus on spending more on business ventures that generate revenue for the company. This leads to a lack of funding for network and IT infrastructure that ensures the protection of IT assets from any external cyberattacks. According to a report by Untangle, 30% of SMEs invest less than $1000 in IT security, this shows a lack of funding for cybersecurity measures.

Cost of Cybersecurity and IT Infrastructure – IT infrastructure needed for data security in general costs much more than the allocated budgets for SMEs. Cybersecurity measures get neglected as SMEs do not prioritize security as a fundamental component of day-to-day business operations.

Lack of Resources and Training –. Small enterprises in general have more resources allocated to the main business functions such as project execution, marketing, finance, etc. IT department of SMEs consists of very minimal personnel, additionally, the resources are also not trained well and lack knowledge of the latest cybersecurity threats. A report by Fortinet indicates that the cybersecurity skills gap has contributed to at least 80% of data breaches. This shows that SMEs do not have a comprehensive strategy to overcome cybersecurity threats and also lack training resources.

Common Cyberattacks and their Implications on SMEs

The lack of prioritization of cybersecurity can result in a compromise of the IT infrastructure of an enterprise. Hackers can exploit the vulnerabilities in an organization using different techniques. These attacks can jeopardize the operational activities of any small organization and can even result in the closure of business. According to research by the National Cybersecurity Alliance, almost 60% of SMBs go out of business within six of a cyberattack. The following illustrates some of the common attacks carried out by hackers.

Phishing – These attacks involve sending files such as emails and texts by impersonating the organization's employee or the company itself.

Malware – A malware attack is also one of the common attacks that hackers employ to steal enterprise data. Malware is loaded into an email or text which upon opening executes a code that can extract the data from the enterprise and can also damage the functioning of IT equipment.

DDoS –Distributed Denial of Service (DDoS) attacks are performed by sending excessive amounts of traffic to a website, server, or network of an enterprise.

Ransomware – Hackers tend to take control of key operational components of an enterprise and steal valuable data to blackmail businesses.

How to Overcome Cybersecurity Challenges Faced by SMEs
- Develop proper budgeting plans for IT networking infrastructure and cybersecurity
- Certified Training for IT Staff
- Use Best Security Practices (MFA, Disaster Recovery Plans and Security Policies)

Esmil Contreras Hidalgo
Ibex Networks
email us here

we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.