Securi.ly: How A Startup Can Fortify Its Cybersecurity

November 19, 2021

November 19, 2021 - PRESSADVANTAGE -
Boca Raton, FL based Securi.ly has published a new blog on their website that aims to help startups & scale-ups improve their cybersecurity. While some may believe that this refers exclusively to online threats, the company clarifies that any network can be compromised under the right conditions, even those that have no connection to the internet at large. Businesses are welcome to read Internet Security: Cybersecurity to learn how they can reduce their vulnerabilities via a few simple steps.

As the post points out, organizations lose an estimated $100 billion every year to cybercrimes in the US alone. It is in a business? best interests to be proactive here because cyberattacks can have devastating and far-reaching consequences, in some cases harming the business? reputation with customers (such as by exposing personal data) in addition to targeting its finances.

The first step involves taking a look at the layout of the business? network and its various aspects. This includes what software is used, what type and how many devices are connected to it (and exposed to the internet), what sort of data is collected and even what sections of it each employee has access to. This is necessary in order to gain an overview of its potential vulnerabilities. An IT team can then use this information to create Internet security and data backups to prevent all systems from being stolen or hacked.

It is also important to remember that cybersecurity is nothing short of a team effort. Hackers and other parties may target individuals, corporations and government agencies from a variety of directions, and a single weak link can be enough to leave the business completely vulnerable. While it is not unheard of for a company?s firewall to be breached via hacking, it is often easier to exploit the people involved with a system when looking for vulnerabilities. This is known as social engineering, and Securi.ly states that this is why cybersafety protocols should be a basic part of every employee?s training (even when they may not have direct access to critical systems).

This training may include the following: how to build and preserve strong passwords, utilize a password

manager, recognize phishing attempts (usually via email) and what steps to take once a possible attack has been identified (such as when a suspicious attachment or email is received). While this training should be mandatory for all employees, those whose responsibilities cover company finances and other types of delicate information should be aware of every preventative measure they should take to protect this data. The startup cybersecurity expert adds that their team is familiar with such protocols and can help businesses get their employees up to speed in a prompt fashion.

Securi.ly adds that password managers can make it both more secure and more convenient for employees to refresh their passwords as often as necessary (as well as share them with trusted coworkers when required). The company explains that passwords should be updated every 30, 60 or 90 days, with the shortest interval being reserved for passwords that protect more critical systems.

Furthermore, this training should be accompanied by computers with software that is always up to date. The easiest way to ensure this is to make it mandatory for every computer to be able to receive software updates, and updates should be pushed out as soon as new vulnerabilities, malware and so on are discovered and fixed.

Securi.ly?s final piece of advice is to begin putting all of these security measures into practice immediately. An attack can happen at any time, and the sooner every employee is familiar with the best safety practices (avoiding suspicious emails or links, reporting glitches and so on), the better the business? cybersecurity will be.

Those who wish to bolster their business? defenses are welcome to contact Securi.ly for a comprehensive assessment of its infrastructure and software cybersecurity. Once potential vulnerabilities are identified, the company will also design a practical roadmap that the business can use to improve their cybersecurity. As part of their services, Securi.ly will also continue to monitor the business? operations in order to ensure it is always as secure as possible.

Orit Benzaquen of Securi.ly is available to respond to any further inquiries. Businesses may also read the company?s blog for more information on staying secure in the digital age. They are rapidly growing their business and accepting new clients.

###

For more information about Securi.ly, contact the company here:Securi.lyOrit Benzaquen310-402-8473oritbenzaquen@securi.lyBoca Raton, Florida

Securi.ly

Be Security Compliant using the most cost-effective and straightforward method, our Innovative proprietary system will take you to ISO 27001, SOC2, CMMC, or HIPAA compliant effortlessly!

Website: https://securi.ly/

Email: oritbenzaquen@securi.ly

Phone: 310-402-8473