Your Own Security Cameras Could Be Used Against You

How to Make Sure Your Business Isn't Vulnerable to a Cyber Attack

It's hard to believe, but the very same security cameras you chose to protect your business may actually present an enormous threat to your operations. That's because hackers are increasingly gaining access to these cameras — by using generic passwords programmed by the manufacturer — and using them as a launch pad to attack businesses via website outages, data breaches and other costly business disruptions.

According to Nik Gagvani, General Manager of Kastle's Video Solutions, the potential damage that cyber-attacks can do to a business and its continuity should not be underestimated. Of course, one of the biggest dangers is that your data could be compromised, lost, or destroyed, requiring significant time and money to restore. Another potential implication: You could be infected by ransomware — a type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them. An attack could even be used to compromise your physical security system, leaving your property without protection.

So, how can you be confident that your cameras — and ultimately your business — aren't vulnerable to an attack?

First and Foremost, If You Have KastleVideo Cameras, You Don't Have to Worry.

Unlike other cameras, Kastle's cameras are designed to be cyber-secure, and therefore do not use passwords for each camera. Instead, Kastle's managed video services use encrypted communications to lock down network access to cameras. And that's not all. "Our team is constantly monitoring cyber security and updating our cameras to ensure all information remains secure," Gagvani said.

For businesses that don't use Kastle security cameras, an obvious first step in making sure your business is protected is to change the passwords supplied by the cameras' manufacturer. However, Gagvani said this isn't always effective, especially if you choose the same passwords for multiple cameras, forget to change them frequently, and don't store them in a safe place — leaving your business vulnerable to an attack.

Fortunately, there's a more secure solution: Kastle can install a gateway device, which takes control over the existing cameras, locks their passwords and acts as a barrier to any harmful information making it way through the cameras into your system.

For organizations that use other security cameras, Kastle would like to offer a complimentary, no-obligation assessment to ensure that the cameras being used are safe. Kastle's video experts will share with you best practices that can help you take the right steps to protect yourself from the growing number and sophistication of hacker attacks.

For more information, contact your Kastle Account Manager, email **info@kastle.com** or visit **www.kastle.com**.