Small Business. Big IT Problems.

BriteStar Protects Small Business from Cyber Attacks

Large companies are not the only ones susceptible to cyberattacks. The 2018 Verizon Data Breach Investigations Report reveals that 58% of all data breach victims are small businesses. Many of these attacks happen by chance due to the increasing popularity in the "spray-and-pray" attack method. Since these attacks are random, any business that is not sufficiently protected can be negatively impacted.

Most small to medium sized organizations have limitations that restrict its ability to build and/or maintain a mature, experienced IT department required in today's environment. The lack of an advanced IT strategy leaves the organization most susceptible to random attacks and will sustain significant business loses.

Enter BriteStar, Brite's premier managed service offering. BriteStar helps companies protect and manage its IT infrastructure through a superior combination of people, process and technology. Built off industry-leading IT best practices, BriteStar increases uptime, reduces break/fix issues and offloads day-to-day IT tasks, all at a fixed monthly cost. With BriteStar, businesses can offload the tactical efforts and focus on strategic projects that propel the business forward.

"Brite focuses on providing secure, stable and scalable IT environments to all of our customers, no matter the organization size. After nearly 20 years in the enterprise security space, we realized that small and medium sized businesses are faced with many of the same problems and threats that large organizations face. BriteStar was created out of the need for both affordable and premium IT support," stated David D'Agostino, Brite's Vice President of Operations.

A Small Company's Struggle

Lupton Associates undertook the everyday burden of managing its IT infrastructure. The company of 20, like many companies of similar size, was not able to dedicate the necessary resources to properly manage and secure the IT infrastructure. The information manager was responsible for all IT duties, along with marketing, the support of new business development. As a result, disruptions would take the entire infrastructure down for days while the company reactively scrambled to find a solution.

The organization's information manager said, "As a one man show, there is just no way for me to keep up. Network administration wasn't my strong suit. I have a limited IT background, and I am a "hack my way through problems" kind of person. That does not work in today's world. There are just too many threats and too many ways for disaster to happen. It really does bring your business to a screeching halt when you are interconnected like we are."

After recognizing the struggle to manage the day-to-day IT needs the company made the decision to offload tactical daily tasks to a managed service provider. “We always had someone in the role of network administrator, but nobody was really qualified for that position. But I think that it makes perfect sense for our organization,” said the information manager. “Frankly, a lot of times, I just didn’t have answers.”

The company chose Brite as its managed service provider and were onboarded just in time.

BriteStar in Action

The investment in a managed serviced provider was quickly validated. Though multiple zero-day security prevention tools were put in place, an end user clicked on a malicious email sent in a “spray and pray” attack and started a chain reaction. The company suffered an attack that could have caused the network to crash if it wasn’t for BriteStar.

A hacker silently infiltrated the network. The malicious attacker changed all administrator passwords, prohibiting users from logging onto the system. With command and control, the attacker was preparing to use the company’s environment to launch attacks on others.

Luckily for this BriteStar customer, while the prevention didn’t stop the attack, one of the many detection tools alerted Brite of the dramatic changes in the environment. Brite’s in-house Network and Operations Center received the alert and responded within 15 minutes of detection. The team immediately began an investigation to evaluate the legitimacy of the threat. Once the team validated the threat, it notified the customer of the incident and began remediation.

“BriteStar uses a suite of technologies to protect our customers from all kinds of attacks. Understanding prevention is never 100%, we have designed our technology stack to detect anomalies and allow us to restore the parts or the entire environment almost immediately,” said D’Agostino. “We managed to resolve this incident within 45 minutes of being notified with only 15 minutes of downtime.”

Brite’s unique combination of both proactive and reactive methods ensures that the customer is covered, no matter what happens.

“From our side, we switched to the backup environment and we really lost no time during that morning, which is huge,” said the information manager. “I’m completely and utterly thankful that we contracted with Brite. It’s been a great relationship for us.”