6 REASONS WHY CYBER CRIME IS INCREASING – AND WHAT YOU CAN DO ABOUT IT

If you're like most people, you probably lock the doors of your home or apartment when you're not there. It's easy to do, is a cultural norm, and reduces the chance of having a criminal break in. It's a standard practice that leaves you less vulnerable to intruders. Now, take that same thought and apply it to protecting the enterprise. As digital business increases, there are greater opportunities and higher payoffs for cybercrime, and enterprises need to take precautions to reduce vulnerabilities that can lead to breaches. They simply can't afford to leave the door open or even delay closing it.

Here are six reasons to be concerned, and guidance on what you can do to protect your business.

Attack of the Zombie Servers and Other Alarming Facts

1. The cost of data breaches continues to rise and has increased 29% to an average of $4 million per incident.
2. In 2015, mobile devices had less than a 1% infection rate, so they were considered safe. Now, more than three-fifths of IT security professionals report that it is either certain or likely their organization suffered a breach because of mobile devices.
3. Cybercriminals have embedded malware into legitimate applications and they're targeting poorly secured Wi-fi spots, stealing passwords, and more in their quest to steal information.
4. Attackers like to exploit unauthorized products with weak security controls in the corporate

cloud.
5. Zombie servers that are left unattended or are not updated offer additional ways to access networks.
6. Known vulnerabilities are not patched in time – a study has found that it takes an average of 193 days before a patch gets applied to fix a problem, even though the patch is available. That's an easy place for exploiters to get in and do their damage.

Roadblocks to Protecting the Enterprise

Meanwhile, companies have to deal with these and other threats but are challenged because the organizations responsible for addressing them – Security and Operations – have different and conflicting roles and priorities. Security does the scans for vulnerabilities but it's up to Operations to do the patching. Meanwhile, Operations is focused on uptime and availability so patching can get deprioritized and delayed.

All too often, security and operations teams don't have enough visibility into each other's plans and activities and this situation adds to a disconnect between the two groups, which is known as the SecOps Gap. Failure to close that gap can leave a business open to breaches, lead to a loss of revenue, increase costs, and damage a company's brand. It can also result in the failure to meet regulatory requirements and big fines. But it doesn't have to be that way. You can address this challenge and close the SecOps gap.

Take Control with SecOps solutions

SecOps solutions can help companies reduce the unknown risk of blind spots and enhance collaboration between these two organizations with automation. They can help Security and Operations find, prioritize, and fix vulnerabilities with an actionable view of threat information based on risk.

Get more details about the SecOps challenge and how BMC automation closes the gap and protects organizations by automating compliance, getting the right information to the right people at the right time, and automating remediation.