THE GAME HAS CHANGED

Why Today's Security Strategy May Not Be Enough

For auto racing fans and teams, safety is a subject that is always on everyone's mind. Compared to racing 25 years ago, the game today has changed dramatically. Cars are faster, lighter, and danger to the drivers has increased. Safety features to accommodate these changes certainly cost the race team more money – but they're necessary to stay secure. Investments in safety continue, as long as the threat escalates. The same is true in business, technology and cybercrime The game has indeed changed and a business's security investment must adapt.

A failure to realize that "the game has changed" could have tragic results.

www.graycyberdefense.com

(303) 468-5515

5 Reasons The Game Has Changed

Cyber-security, much like car racing, has changed significantly over the past several years. There are five ways the cyber-security game has changed and why the current strategy, particularly for the SMBs, may not be enough.

1. The Growth of Cyber-Crime

The growth in attack volume on the SMB has grown exponentially because it's easy. SMBs (and some public sector entities as well) tend to be well behind the security curve, making the organization an easy target of cybercrime.

2. The Target of Cyber-Crime

The real target of cyber-crime is the SMB! In 2017, 70% of all known successful attacks where against small and medium businesses. And of those that were breached, 60% went out of business within 6 months.

3. The Number of Security Solutions

While firewalls, IDS/IPS, AV, etc., are critical, improper configuration and management of these tools often create more risk. Many companies might not have the resources or expertise to know what to do if those tools alert them of a problem.

4. The Lack of Expertise

The most effective way to listen to these devices is to observe their every action and their communication patterns. Because these actions and "event logs" occur several times per second, many companies turn to a Security Information and Event Management tool (SIEM) to help make sense of the vast amount of machine data being generated.

5. The Lack of Resources

Security products, to be effective, must be monitored and maintained 24/7 so that threats are detected and responded to immediately. Not an easy task for the typical SMB company that cannot afford around-the-clock security experts. Cisco agreed that "the worldwide shortage of information security professionals is at 1 million openings, even as cyber attacks and data breaches increase each year".

Better safety is going to cost more money and there's no way around it. What a Managed Services Provider sold to an SMB for protection yesterday was all that was required. A changing threat landscape has demanded a new level of vigilance and increased investment to avoid risk.

Contact us today for a no-obligation quote on our 24/7 cyber-threat monitoring program

GRAY CYBER SECURITY
CYBER SECURITY MADE SIMPLE

www.graycyberdefense.com

(303) 468-5515