News

A Focus on Emerging Threats: Cybersecurity Awareness Month

In 2022, cybercrime is ever-increasing, and the number of attacks and bad actors continues to increase exponentially. As soon as we've learned to eliminate a threat, perpetrators are creating new ways to breach networks. It can feel like a never-ending cycle.

And it is no surprise because successful attacks on Medibank, the Colonial Pipeline, and SolarWinds demonstrate the significant need for cybersecurity efforts that act differently than traditional practices. A holistic approach must be defined and expanded to cover applications and workloads during runtime wherever they may reside to protect our enterprise systems better. This is the only way to ensure that the correct code and processes can execute and nothing else, regardless of the threat environment.

Cybercrime's threat to individuals and organizations leaves them feeling anxious, thinking about the possibilities that can take place without appropriate security practices or solutions. In response to this increasing threat, we as an industry must commit to being as proactive as possible by educating, training, and staying updated on security-leading practices.

As you can imagine, our cybersecurity strategies have undergone immense changes over the years, and significant strides have been made by security teams across the globe. Since its introduction in October 2003,Cybersecurity Awareness Month(CSAM) has brought greater awareness to this global issue. Leaders and employees have been more aware of their role in mitigating threats, while ISOs and CISOs worldwide are now developing greater Security Education Training and Awareness (SETA) programs. The bottom line is that security knowledge should be focused on awareness for all, training employees with key roles, and educating cybersecurity specialists. SETA programs are not a one size fits all, and many now include phishing exercises, tabletop security incidents rehearsal, and simulated attacks with Red and Blue teams.

The theme of this year's CSAM campaign is “*See Yourself in Cyber, "* demonstrating that while cybersecurity might seem complex, it is all about teamwork. ACRE recognizes that all members of an organization play a role in defending our organization's data, assets, and employees. We also all play a part in protecting personal data in our day-to-day life.

Currently, employees need to keep a mindset of security in all tasks that they complete, whether cyber or physical. Supporting this initiative is our SETA program, which is designed to promote cybersecurity awareness. Additionally, our team has developed other campaigns to enhance our employee's overall security knowledge through workshops, assessments, and security incident scenario rehearsal to help reduce our security risks.

Regarding our security solutions, ACRE strives to balance our security strategy with our core product pillars of identifying, protecting, detecting, responding, and recovering. Adhering to cybersecurity best practices, we actively train our specialists to be conscious of security and data protection in every step of the product lifecycle from the initial concept through retirement.

In a world where ever-evolving technology produces incredible innovations, it raises threats more than ever before. We believe that one factor contributing to this is the risk of complacency. Any organization that believes it is doing enough or becomes too negligent in security strategies could be heading down a dangerous path. Organizations must stay engaged and vigilant and remain dedicated to keeping their employees, suppliers, and customers informed. After all, security is and will always be a team effort.