SPOTLIGHT ON DATA CENTRE SECURITY

PHYSICAL PERIMETER SECURITY STRATEGIES FOR DATA PROTECTION

SOUTHWEST MICROWAVE

MicroPoint™ II pinpoints intrusion attempts to within 1m, simplifying incident detection and assessment for long perimeters.

As cyber security threats escalate in complexity and as global privacy regulations expand, businesses are under significant pressure to ensure the protection of data and as importantly, the infrastructure that supports reliable housing and storage of this digital information.

While there is much attention dedicated to securing the network perimeter, of equal importance is a focus on fortification of the physical perimeter of a data centre, given that this is the first line of defense against unauthorized site access. The convergence of information security and physical security in a comprehensive data centre security framework ensures successful mitigation of risk to these critical assets.

PROTECTING THE OUTER PERIMETER

Physical perimeter security aims to Deter, Detect and Delay an unauthorized intruder so that security personnel have sufficient time to Assess and Respond to an attack with appropriate protocols. In a data centre environment, crash-rated or anti-scale fencing, strategically installed to physically prevent entry by bad actors serves as an appropriate deterrent and delay mechanism. Even with these barriers in place, fortifying the perimeter against unauthorized access calls for multiple detection technologies, or layering, to provide an additional level of protection against breach. The incorporation of a fence-mounted sensor to detect cut-or-climb attempts, coupled with CCTV cameras for visual assessment capability and tracking of intruder movement, enables security personnel to take immediate, defensive action before an intruder has the opportunity to reach the protected asset.

While any fence detection sensor is designed to alarm on an attempt to scale or penetrate fence fabric, several performance metrics separate today's 'intelligent' sensors from more traditional technologies.

"In evaluating a fence detection solution for a data centre environment, a system's ability to discriminate between intrusion attacks and environmental disturbances is of utmost importance," explains Maira Zanrosso, Director of Sales for Arizona-based perimeter security systems producer Southwest Microwave.

High nuisance alarm rates can desensitize system operators, which in turn can increase risk of breach. To address this challenge, Southwest Microwave developed the INTREPID™ MicroPoint™ II fence detection system, an advanced smart sensor currently in use at data centres worldwide that identifies intrusion attempts to within 1m and seamlessly integrates with camera presets to provide precise, immediate assessment of disturbances.

"MicroPoint™ II relies on patented technology that discriminates between legitimate fence attacks and distributed disturbances, such as strong wind, heavy rain or vibration from vehicles, trains or aircraft. Our data centre clients are able to avoid nuisance alarms that these environmental conditions would have triggered in other sensors."

Maira Zanrosso
Director of Sales, Southwest Microwave

MicroPoint™ II employs a proprietary Sensitivity Leveling™ process that enables the system to optimize detection sensitivity in 1 meter increments or 'cells' along the cable by accounting for variations in fence fabric or tension. This provides data centre clients, typically relying on fences that span extensive perimeters, with uniform detection across the entire protected fence line.

To filter out the environmental disturbances that typically trigger nuisance alarms in traditional fence sensors, MicroPoint™ II has the unique ability to differentiate between 'Point Impacts' - legitimate intrusion attempts that affect a small number of cells - and 'Distributed Disturbances' - such as strong wind, heavy rain or vibration from vehicles, trains or aircraft - which affect a longer linear distance. Where harsh climatic conditions are an issue, nuisance alarm reduction capabilities become key.

"We recommend that Users verify that any fence sensor they are considering offers advanced calibration capabilities and configuration settings to successfully filter out harmless environmental activity without the need for weather stations or other sensitivity-reduction tools that sacrifice detection performance," says Zanrosso.

MAXIMIZING DETECTION PROBABILITY & ADAPTABILITY

Just as nuisance alarm prevention must be top of mind, so must be achieving the highest probability of detection, given the significant ramifications of data compromise.

Zanrosso stresses that it is critical for the User to take the time to consult with their Provider partner to ensure that adequate testing has been done to ensure good compatibility between the fence detection system being considered and the fencing on which it will be deployed.

"Rigid, crash-rated, anti-scale fencing typically deployed in data centre environments handles vibrations differently than a more flexible chain link or welded mesh material. As such, a sensor will register a climbing intruder attack completely differently," she says.

The goal is to ensure that the fence detection system being evaluated can successfully identify these attacks, regardless of fence characteristics. This may mean using a different mounting configuration on a rigid fence versus one made of steel mesh.

For data centre clients, Zanrosso also urges that attention be paid to a detection system's ability to adapt to changes in a site's perimeter configuration. She recommends choosing an intelligent sensor with modular design, software-based detection zone assignment and seamless integration with a User's alarm monitoring and control system to simplify system reconfiguration or the addition of new hardware if fencing must be moved or extended to accommodate facility growth.

PROTECTING CRITICAL INNER ELEMENTS

Because servers and critical systems are vulnerable to attack from both unauthorized intruders and internal personnel, Zanrosso explains that the concept of layering should also be applied to a data centre's critical inner elements. Along with 24/7 audited door access control and local and remote surveillance, installing fence detection systems on server room wire mesh panels and colocation cage access doors, walls and flooring adds reinforcement to these vulnerable entry points.

Since data centres are expected to deliver uninterrupted service, access to redundant network, cooling and power systems should also be well-controlled not only with network protection, but with physical safeguards. Zanrosso suggests that Users work with Provider partners to conduct performance trials on proposed sensors to validate that they can successfully filter out the distributed vibrations caused by generators or other systems that can trigger nuisance alarms.

Zanrosso also stresses the importance of selecting a sensor that offers authorized individuals the ability to easily disarm portions of the cable temporarily in system software to accommodate routine building or server maintenance.

KEY IMPLEMENTATION CONSIDERATIONS

Along with the critical considerations outlined for evaluating Provider partners, Zanrosso reinforces the importance of appointing Systems Integrator partners with proven experience deploying the selected physical security technologies to ensure a seamless implementation. She encourages Users to verify that these partners possess the relevant technical certifications for any perimeter security solutions they are installing in the data centre environment to assure smooth and timely implementation, reduce rework requirements and optimize system performance.

"Successful physical perimeter protection for data centres combines intelligent technologies that address industry security specifications while also considering a User's unique risk profile and site characteristics," Zanrosso explains.

"We suggest that Users carefully identify solutions and partners based on their ability to help achieve a fortified physical perimeter that complements and enhances their network perimeter protection strategy, and that best protects against financial and reputational risks."

Southwest Microwave has been a trusted global supplier of intrusion detection technologies since 1971. Learn more about reliable perimeter security solutions for data centre protection at ***www.southwestmicrowave.com.***

SOUTHWEST MICROWAVE

USA (CORPORATE HEADQUARTERS): *Southwest Microwave, Inc., Arizona, USA | Telephone +1 (480) 783-0201*

EUROPEAN OFFICES: *Southwest Microwave Ltd., Worcestershire, UK | Telephone +44 1386 75 15 11*