BIZCOMMUNITY

The inevitable convergence of physical and cybersecurity

By Sven Smit

6 Dec 2018

It may not be immediately clear as to how, but physical and cybersecurity are converging and the need for a combination of cyber and physical defences will soon, if they aren't already, become a non-negotiable addition to enterprise security systems.

Sven Smit is portfolio director at Specialised Exhibitions Montgomery

When you consider that today, we are able to remotely control virtually all of our security systems, from those that govern our data to those that protect our physical businesses, it should come as no surprise that hackers are able to do so as well.

The exponential adoption of the Internet of Things (IoT) - with more devices than ever before operating through the cloud, 22 billion by 2020 estimates IMS Research - has made it necessary for security experts to consider the correlations between physical and cybersecurity, including the shared risk factors and the shared protective measures that can be taken.

Most modern buildings, for example, include video surveillance systems, access controls, elevator systems and even digitally controlled air-conditioning lines, which can all be accessed and controlled remotely and are thereby vulnerable to security breaches.

Consider Lappeenranta, a small town in Finland, the residents of which found themselves freezing in sub-zero temperatures when attackers caused heating systems to go offline using a Distributed Denial of Service (DDoS) attack in 2017.

Another example is when two hackers took over 123 of the 187 cameras used by the Metropolitan Police Department of the District of Columbia (MPDC) for four days in early 2017. The main aim of the attack was to use police department computers to e-mail ransomware to more than 179,000 accounts. However, it also meant that the police department was unable to record video from their security cameras for several days before Donald Trump was sworn in as president.

Physical threats of a cybercriminal

When you consider the types of people we're talking about here, there is always the risk that a cybercriminal could pose a serious threat to the physical safety of the workplace. Using their way of thinking, the possibilities are endless – imagine a fire alarm with all exits locked and panicked staff, or no fire alarm at all when it's really needed.

It's best to avoid being naïve or trusting when it comes to security. When the talking fridge was invented, who'd have thought there'd be someone out there who'd want to mess with it? But they do, or they will, and the networked enablement of business functions is forcing companies to see that physical and cybersecurity must be treated in a unified manner.

The good news is that businesses are seeing how the convergence of physical and cyber security is increasing operational efficiencies, with many taking the necessary steps to protect themselves and their customers by using cybersecurity innovations to protect their physical systems.

ABOUT THE AUTHOR

Sven Smit is portfolio director at Specialised Exhibitions Montgomery