Smart Buildings: The Latest Vector For Cyberattacks

Smart Buildings in Smart Cities are supposed to create a ‘safe and healthy environment’ for their occupants’ but careless security holes are drawing hackers like bees to honey. Instead of fixing the flaws, experts recommend defensive AI systems. TN Editor

As one of the top trends in 2019, smart city tech is sweeping the enterprise. Digitizing buildings is a major trend currently, however, this trend comes with a new security issues, according to Frost & Sullivan’s IT/OT Security Convergence for Building Technologies report.

The market for information technology (IT)/operation technology (OT) security services in smart buildings is predicted to hit $897 million by 2022, reaching a record compound annual growth rate of 37%, the report found.

A smart building uses technology to create a safe and healthy environment for its occupants. It typically uses IT-aided intelligence, smart sensors and controls for real-time dissemination of operational information for predictive analytics and diagnostics to help manage the building and maintain it at optimal levels.

Systems in a smart building are typically connected to an onsite management system or an offsite cloud-based management system. These are known as building automation systems (BAS).

Smart buildings are essential to smart cities, but as the number of such buildings increase, so does the security risk.

Smart building cyber attacks can occur in a number of ways, from phishing emails to an advanced persistent threat (APT), said Swetha Krishnamoorthi, industry analyst at Frost & Sullivan.

“For instance, in 2016, to take the German steel mill, cyber adversaries used phishing emails to gain access to the software network,” Krishnamoorthi said. “They gained access to the enterprise network and eventually penetrated the production management software. Once they got into the software, they gained access to the plant’s control system, and they destroyed all the human machine interaction points. Once that was destroyed, they manipulated the blast furnace systems and caused significant operational damage.”

Smart building technology is in its early stages of growth and adoption, leaving consumers unaware of the vast amount of security threats associated with the new tech, Krishnamoorthi said.

“The number of connected devices to an enterprise network is increasing phenomenally, as are the growing number of data breaches. Every single day, millions and millions of customer records, and employee records are being stolen,” Krishnamoorthi said. “The concern for brand reputation and impact on production environments is quite high, and increased awareness on including an IT/OT security to protect smart building equipment is rising.”

Read full story here…