

KS.16. Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer

By Ganesh V

September 16, 2025



Time for establishing AML
Digital Intelligence
Departments in Financial
Institutions

Internet-connected technology, also known as the Internet of Things (IoT), is now part of daily life, with smart assistants like Siri and Alexa to cars, watches, toasters, fridges, thermostats, lights, and the list goes on and on.

But of much greater concern, enterprises are unable to secure each and every device on their network, giving cybercriminals hold on their network hostage with just one insecure device.

Since IoT is a double-edged sword, it has the potential to severely disrupt other organisations, or the Internet itself.

Hackers exploited a vulnerability in the thermostat to get a foothold in the network. Once there, they managed to access the high-roller database of gamblers and "then pulled it back across the network, out the thermostat, and up to the cloud."

The adoption of IoT technology raises concerns over new and more imaginative cybersecurity threats, and this incident is a compelling reminder that the IoT devices are vulnerable to being hacked or compromised.

"There's a lot of internet of things devices, everything from thermostats, refrigeration systems, HVAC [air conditioning] systems, trade operations systems, to people who bring in their Alexa devices into the offices," . "There's just a lot of IoT. It expands the attack surface and most of this isn't covered by traditional defences."

Manufacturers of IoT devices majorly focus on performance and usability of IoT devices but ignore security measures and encryption mechanisms, which is why they are routinely being hacked.

Therefore, people can hardly do anything to protect themselves against these kinds of threats, until IoT device manufacturers timely secure and patch every security flaws or loopholes that might be present in their devices.

The best way you can protect is to connect only necessary devices to the network and place them behind a firewall.

Also, keep your operating systems and software up-to-date, make use of a good security product that protects all your devices within the network, and most importantly, educate yourself about IoT products.

Lessons for a digitalized trade finance ecosystem?? I leave it to you to ponder....

Source : Cybersecurity and Cybercrime investigators...