BUILDING MANAGEMENT SYSTEM (IN) SECURITY

HVAC building management systems are not immune from the need for computer security and defensive computing.

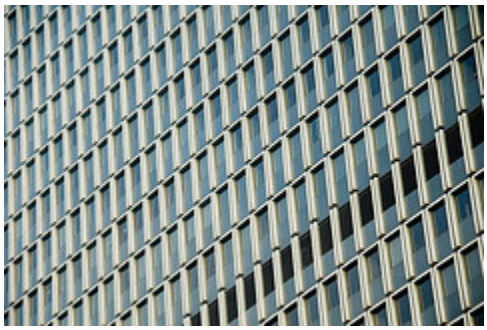
A Visible Example

In 2010, a computer virus dubbed Stuxnet was used to attack nuclear enrichment centrifuges at Iran's Natanz nuclear facility. Widely speculated to be a joint project of the US and Israeli intelligence services, the virus spread worldwide but was designed to only target specific process controllers used to control centrifuges at Iran's nuclear facility. The process controllers had a simple (and previously known) security vulnerability that allowed them to be reprogrammed by the virus to behave differently than intended–without anyone knowing. The ultimate effect was that a portion of the centrifuges were physically spun out of control causing irreparable damage. The estimated impact of this attack on Iran's nuclear program varies widely, but some reports state that the damage may have set back progress by up to 18 months. One amazing part of this story is that the equipment was not simply connected to the internet and targeted remotely–the servers were "air-gapped" for security against these exact kinds of threats. Instead, the virus was designed to piggyback on a USB thumb drive from a computer connected to the internet, to one of the secure control servers.

English: Symbolic image depicting the computer virus Stuxnet (Photo credit: Wikipedia)

The HVAC Connection

What does this have to do with HVAC and Energy Efficiency, you may ask? Well, the control systems we use to automate control of commercial buildings (aka BMS or DDC systems) are functionally equivalent (though HVAC-application-specific) versions of these industrial process control systems. And like the industrial process controllers in Iran, our building BMS servers (and laptops, smartphones, and other servers, for that matter) all have vulnerabilities in their design and programming that if discovered, can be exploited for nefarious purposes. In the past several months, a security hole was discovered in a popular BMS platform Tridium Niagara — which is used in commercial and governmental buildings worldwide. An attacker used knowledge of this vulnerability to compromise a commercial building in New Jersey–effectively gaining administrative control of a BMS system without requiring a password. No damage was done, but the breach should act as a wakeup call — that the computers controlling building HVAC systems are not immune from the computer threats that plague everyone from governments to home PC users. While no physical damage was done, if the reader is familiar with BMS systems, one could imagine many ways that disruptive actions could be taken–from the annoying and time consuming to resolve, to the possibly building-integrity-threatening.



Office building windows (Photo credit: thatguyhans)

So What Does This Mean For A Typical Building Owner?

As a building owner of a non high-profile facility, you may think that threats like these are what the big companies have to deal with, and that just by being small or unknown, nobody will be interested in tinkering with, or know where to find your possibly insecure BMS system. But it turns out that there are search engines on the internet that troll the web looking for all kinds of vulnerable systems — including HVAC controlling BMS systems and industrial process controllers. So if your system were vulnerable, it

would be trivial for someone interested in tinkering with it to discover. Granted, it is unlikely that any given system will be attacked, especially low profile targets–however it is not out of the question. The ultimate point here is that HVAC servers are not immune from the security problems that plague all computer systems–and are possibly even more at risk because they are often connected directly to the internet (not behind a hardware firewall). Like all computer systems supporting critical business operations, Owners should be taking the same precautions to protect their building automation systems. These include:

If systems will never require remote access, keep them off of the network.

If BMS systems will require remote access:

Put these systems behind a dedicated hardware firewall router, and if possible, not interconnected with the business network.

Use a router equipped with VPN (Virtual Private Network) capability for remote access. At one time expensive, routers with VPN access are now under $100 and provide a high degree of security compared to having servers with open ports sitting directly on the internet.

Like any other computer, keep software up-to-date with patches and updates. Both operating systems and BMS programs should be kept current. This is sometimes organizationally challenging because BMS servers may not fall under the umbrella of the IT department's responsibility and can be inadvertently neglected.

As with any other computer/hardware, ensure usernames and passwords are reasonably rigorous (they should be at least as rigorous as those you would use for personal banking) and that "default" passwords do not remain after the system is set up.

Source : http://buildingenergy.cx-associates.com/2013/01/building-management-system-insecurity/