CPNI
Centre for the Protection
of National Infrastructure

ADOPTING A SECURITY-MINDED APPROACH TO BUILDING MANAGEMENT SYSTEMS

An introductory guide for Built Asset Owners and Facilities Managers

March 2017

Disclaimer
Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation or favour by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential, and including but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using the information contained in this document or its references. You should make your own judgment as regards use of this document and seek independent professional advice on your particular circumstances.

Introduction

A Building Management System (BMS) is an automated control system that is installed to manage internal environmental conditions, support critical infrastructure and monitor critical systems. Additionally, they are often employed for energy metering to provide analysis and financial billing of utilities consumption.

Within the business and public sector arenas the inclusion of BMS has been commonplace for decades and is the accepted 'norm' of any new building design or existing building refurbishment.

While the list of potential uses is almost endless, they most commonly manage:

- environmental control – heating, ventilation and air-conditioning (HVAC)
- lighting – control of lighting schemes, often in public areas
- energy monitoring – real time energy metering, automatic monitoring &targeting (AM&T) billing
- critical system monitoring & alarm notification – flood & leak detection, electrical power monitoring, potable water monitoring
- back-up electrical power alarm notification – generators, uninterruptible power supplies (UPS)
- computer data suite environmental control

Why is the security and resilience of building management systems an issue?

The technology employed by most BMS and 3rd party systems is converging with that commonly found in an enterprise's corporate network, with nearly all now employing IP (Internet Protocol) networks to communicate, both internally and with the outside world. In addition, many make use of commercial-off-the-shelf IT products, software and operating systems as key system components.

As building management systems have historically been disparate and employed specialist hardware and communications protocols, these developments greatly increase their overall cost effectiveness. Further, the IP network structure is quite straightforward to manage and may be integrated with a client's own in-house network, generating potential cost savings.

However, these benefits create a number of vulnerabilities:

Unauthorised access via unprotected network points

The security of many building management systems is based on the use of password controlled access to workstations and the presumption that only authorised devices will be permitted access to the BMS networks.

The connection of unauthorised equipment, including end user devices (laptops, tablet devices and IT-based test equipment), and/or wireless access points to unprotected network points within the BMS can allow normal security measures to be bypassed.

As well as each piece of automation equipment being a potential access point to all other pieces of equipment on the network, it could also be a means to gain entry to the client's much larger IT systems.

Unauthorised access via remote connectivity

Many building management and control systems have the ability to be remotely monitored via the internet. This is often undertaken using a dedicated 3G/4G Router that would allow a manufacturer or service provider to remotely interrogate the system, fault diagnose and sometimes reset or restart the system, without the need to visit or enter the client's building. However, such connectivity can be attacked with the aim of gaining access to the system, and potentially to gain remote access to the much wider network of equipment or client's enterprise IT.

Malicious Software

The internet is awash with malicious software (malware) that can function in a largely undetected way. This software is designed for a variety of purposes, including: to enable unauthorised access to systems by exploiting known software vulnerabilities; to allow unauthorised manipulation, corruption and sabotage of systems; or to enable the unauthorised collection and exfiltration of corporate data.

All automated systems have to be engineered, commissioned and maintained by specialists. Such specialists undertake these duties with proprietary software running on PCs and laptops which they may bring to site. If such a device contains malware it may infect or exploit the client's systems as soon as it is connected to the BMS IP network.

The Human Factor

Individuals with nefarious intent could position themselves in employment with providers of automated equipment for building management systems, or with the maintenance and facilities management contractors who support and run the BMS, with the sole intention of gaining unauthorised access to a client's IP network or to instigate a disruption of physical service (DOPS) incident.

A DOPS threat is one that targets the physical real-world equipment that supports, or could compromise, the critical systems (including the BMS) that are essential to the business operations and/or the environment used by an organisation. Without these systems operating correctly, it may not be possible to retain people within buildings or the site, maintain essential communications and computer equipment, or to continue operating. In manufacturing, this type of threat could halt production, ruin items being produced, or damage raw materials or stock.

Risk mitigation – adopting a security-minded approach

The approach detailed below will not only help you recover from a system security breach but will provide greater overall resilience to your organisation.

1. **Identify which systems and processes are essential to: your organisation; the health and safety of its personnel and third parties; and/or the services it provides.**

   These may include cooling, water supplies, electrical power, lighting or environmental conditions. The process must include identification of those secondary systems which support the primary systems.

2. **Question and examine the physical and technological state of each of the identified systems to establish its serviceability and longevity.**

   This process should include establishing the age and type of working life the system and its components have had, with a comparison to the product's expected working life. This assessment should take into account the availability of support and planned service end-of-life for software components, including the operating system(s).

   The relevant maintenance team/contractors should be contacted to determine how they would respond to a failure event and the likely response time, and the availability of spares.

   Many manufacturers make or configure specialist equipment to order and do not keep equipment on the shelf. Lead times can vary significantly from 1-2 working weeks to months, particularly if key components are at or close to their end of life. If it is identified that there are several key components to the business-critical elements of your system, it may be worth having a stock of spare items to allow your business to recover much faster.

3. **Ensure both the organisation and its automated systems or BMS specialist have up-to-date copies of the BMS software safely stored on site.**

   This software should include back-ups of the operating software, patches and up-to-date configurations from each device (if available) as this will be needed to restore failed items.

4. **Examine the security measures around each of the identified systems.**

   While it is easy to concentrate on remote attacks on the various automated systems, it should be kept in mind that the simplest way to interfere with a system is by physically interacting with it, potentially through centralised control panels, power supplies and connectivity to critical components.

   Centralised control panels support several, if not all, the systems. Usually, as a result of current design specifications and standards, they have an array of manual user switches installed upon the fascia for each pump, fan or other electro-mechanical process. These switches allow the user to override the automated control process by selecting either 'Hand' (manual 24/7 operation), 'Auto' (fully automatic control) or 'Off'.

   By law, any electro-mechanical device that is installed has to have local electrical power isolation in the form of a suitable power switch local to it.

   Anyone with access to either control panels or the items they control could have an immediate and disruptive affect upon system operation that could take hours to locate. These components should therefore be sited so that access can be controlled, e.g. in a locked equipment room or cabinet.

   If operatives can gain access to these control panels then they can also access the controllers and their networks. The opportunities to add a 'device' to an existing IP network are numerous if access is not properly controlled. This could lead to unauthorised local and/or remote access, and, if the automation systems have been linked to the client's network infrastructure, access to the enterprise's network.

5. **Put in place a process with regard to engineers or technicians who come to site to work on the automated systems.**

   It is advised that relevant staff are able to answer the following questions prior to an engineer or technician accessing any system:

   - Is the engineer or technician known? Are they the usual operative?
   - Why is the operative on site – was the visit requested or planned?
   - Should they be accessing the automation system?
   - What software changes, if any, are they making?
   - What hardware changes, if any, are being made and why?
   - What equipment, if any, have they brought onto site and will it be connected to the BMS or site network(s)?

   Systems such as permit-to-work should be an absolute minimum and should ring fence ALL elements of the system from the basement plant room to the roof cooling units and all that is in between. You are gaining little if you have excellent protection around your server room but have not stopped someone from accessing and simply turning off the associated roof air-conditioning units. The effect is equally disruptive.

   Where the engineer or technician is bringing any equipment onto site which will be connected to the automation or any associated communications and networking infrastructure (including storage media, laptops, tablet devices and other IT-based test equipment), it is prudent to have measures in place to check for malware prior to allowing such connections to be made.

6. **Implement appropriate and proportionate physical protection of systems.**

   Physical protection measures that should be considered include:

   - Physical redesign of the network structure of the supporting IP network to separate systems identified as being of value or business-critical.
   - Employing System Transparent Air-Gap technology to maintain essential communication between a secure System Automation network and existing IP network in a secure manner.
   - Provision of organisation-owned laptop computers, complete with relevant automated systems proprietary software, for the install and service engineers when they come to site. This allows the laptops to be maintained under the organisation's own IT security policy and policed at all times.
   - Employing an N+1 strategy (main system plus adequate back-up) on systems that are most critical so that there are no single points of failure.
   - Regular maintenance and testing of all equipment and practices to ensure operational effectiveness.

7. **Testing and exercising as part of resilience and business continuity planning.**

   In order to ensure that there is an effective response to any incident affecting a BMS, regular testing and exercising should be undertaken. Depending on the nature of the business, the BMS in place, and its criticality to safety and business operations, this testing should include:

   - Periodic testing of incident response plans for security incidents which, where relevant, may include liaison with specialist stakeholders, e.g. penetration testers (physical and cyber), digital forensic response teams, law enforcement, etc.
   - Periodic table top exercises to confirm the on-going validity and effectiveness of business continuity and disaster recovery plans.
   - Annual testing of business continuity plans involving use of alternative facilities, sites or accommodation.
   - Routine testing of alarm and monitoring systems to ensure sensors, actuators and warning systems are fully functional.
   - Periodic testing of back-up or stand-by equipment and systems to verify that the cut-over/start-up works as planned. This should include testing of any uninterruptible power supply and back-up generators to ensure smooth transition off, and back onto, the public electricity supply in the event of loss of supply.
   - Occasional testing of a complete or extensive loss of systems for the site or building to ensure that all business-critical systems can be restored to operational use in a safe, orderly and secure manner.

Future designs

Much of what has been covered above refers to legacy systems that are already installed and operational. However, new systems are being designed all the time. The mandatory inclusion of appropriate security measures at this stage is easier, can be more comprehensive and is much more cost effective than redesigning the system to address vulnerabilities at a later date.

When considering a new system installation or even a refit of current systems, it is advised that the answers to the following questions are established:

- What areas of the organisation are business critical?
- What is the reliability and longevity of the equipment required to be?
- Do the automated systems or BMS designers have the appropriate design experience and skill set to produce a system of this level?
- What procedures are in place to safeguard the system design information?
- Have system designers of all associated disciplines (mechanical, electrical, automation & monitoring) been consulted to ensure N+1 or fault tolerant redundancy (enabling a system to continue operating properly in the event of the failure of, or one or more faults within, some of its components) has been built in?
- Is it intended that any rare or unique equipment types will be used which would lead to prolonged procurement times and limited support facilities?
- Are suitable system transparent air gap solutions being used where critical primary systems are required to communicate with the less important secondary systems?
- Has remote connectivity (3G/4G router, phone dialler, etc.) been included in the design to the new system that could present a backdoor weakness?
- Have suitable system maintenance and response measures been put into place while the newly installed system is within its 12-month warranty period? (historically, new systems are rarely maintained in this period)

- Have the security procedures been reviewed by the relevant personnel to ensure the correct level of managed access exists around the new systems?

Resilience – a by-product of vigilance

Systems can fail due to completely benign reasons, such as component failure or accidental damage. Employing the defensive steps detailed above, in particular the use of N+1 or fault-tolerant approaches to critical systems, will not only to help to make systems far more secure, but will also assist in protecting against such failures having a catastrophic effect to your organisation.

While it cannot be guaranteed that failures within systems will not occur, a good system design will help to ensure that the organisation remains operational on back-up systems/components while corrective action is taken, affording time to source the correct components and to undertake repairs in a methodical and non-rushed manner.

Additionally, security measures placed around critical systems will prevent works on secondary systems having an accidental knock-on effect on critical elements.

The elevated levels of monitoring of critical systems recommended by this document should also, if correctly implemented, provide facilities for notifying key personnel as soon as an issue has occurred, decreasing response and repair times.

Further Information

Good practice guidance on Industry Control System (ICS) security, covering many of the issues set out in this document in more detail, is available in *Security for Industrial Control Systems (SICS) Framework*, CPNI/CESG, available at www.ncsc.gov.uk.

ICS is used as a generic term to cover all industrial control, process control, distributed control system (DCS), supervisory control and data acquisition (SCADA), industrial automation and related safety systems.