Building Management Systems: the cyber security blind spot

White Paper
Introduction

Building, Energy and Facilities Management Systems (BEFMS, or BMS) allow increased energy efficiency, comfort and in many cases improved physical security. They integrate and simplify control of heating, air conditioning, lighting, CCTV, lifts, access controls and perimeter security. The data generated from these allows continued improvement of building management.

But as these systems bring greater benefit, such as centralised control and monitoring, more and more are being connected to corporate IT networks, wireless networks and directly to the internet and any connected device has the potential to be hacked. These devices control systems critical to the functioning of business and government, so hackers who successfully gain access could do huge amounts of damage.

Much of the problem relates to how these systems are designed, installed, operated and maintained. This tends to be by individuals who are experienced in installation or facilities management, but lack awareness of security threats and so do not employ adequate security controls and risk mitigation measures.

This whitepaper outlines why such BMS are at risk, where the vulnerabilities lie and how to mitigate the risk.

A short history of control system vulnerabilities

BMS are essentially a subset of Industrial Control Systems (ICS), which are widely used in critical industries such as power generation and transmission, as well as manufacturing, to ensure systems such as nuclear reactors and production lines operate correctly.

ICS are generally made highly secure (unless designed a significant time ago) as compromise could be disastrous. Nevertheless, even in these secure environments, vulnerabilities have been exploited.

- It is believed that one of the earliest cases of sabotage of ICS dates back to 1982 when the CIA triggered an explosion in a Siberian gas pipeline.
- The allegedly state sponsored Stuxnet virus reportedly destroyed 20% of Iran’s nuclear centrifuges by attacking their control systems even though they were air-gapped from the internet and wider networks.
- In 2014, a steel mill in Germany suffered serious physical damage when hackers managed to mount a successful spear phishing campaign against the system operators.

As ICS are used in developing BMS in less secure environments, they pose serious risks to the businesses they are intended to protect. We have already seen both ‘proof of concept’ and real-life attacks on BMS including:

- Jesus Molina took control of lighting, shading and HVAC systems in a luxury hotel in Shenzen, China, via the iPad in his room.
- The Tridium Niagara vulnerability was shown to allow control of locks, lifts and CCTV cameras of organisations using that BMS system.
- The US ICS-CERT monitor newsletter reported that the BMS of a New Jersey manufacturing company had been hacked in 2012.
- One of the indirect consequences of poor security around BMS made the headlines in November 2013 when 40 million customers of US retailer Target had their payment card details exposed when authentication information to their network was stolen from a HVAC subcontractor.

Consequences of Compromise

Potentially vulnerable BMS are now prevalent in many buildings and offices, including hospitals, airports, sports stadiums and government departments. The environments of these organisations are therefore vulnerable to outside control; control that has the potential to impact external and internal communications, computer networks, building access, lighting and heating. Downtime on every single one of these systems has a direct link to the wellbeing of people, the commercial performance of businesses, and the corporate reputation of organisations, institutions and entire industries.

Would a hospital with no lighting be able to treat patients? Could an airport function without communications for a single hour let alone a whole day? How would a business operate if its staff could not access its building? Such attacks, even if quickly resolved, could cause untold damage in fragile systems that rely on continued operation, such as electricity generators, casinos, hospitals or stock exchanges, to name a few. Organisations would cease to function and potentially collapse, taking down their reputation as well as severely inhibiting their commercial performance.

There are multiple reasons behind such attacks:

- Activist groups wanting to break up organisations they take issue with
- Terrorists wanting to disrupt national functions, for example transport or government operations
- Nation states wanting to harm organisations they consider a competitive risk or a threat to their security
- Companies wishing to sabotage competitors
- Aggrieved former employees wanting revenge
- ‘The bored teenager’ testing their hacking skills

If these actors gained control of BMS, the damage that can be done is highly significant:

<table>
<thead>
<tr>
<th>System</th>
<th>Impact of Compromise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management System/ Dashboard</td>
<td>• Lockout genuine users from system</td>
</tr>
</tbody>
</table>
| Lighting                      | • Deactivation of lights may cause safety and productivity issues including public panic and inability to conduct business as usual  
• Flickering of lights could cause health issues 
• Increased situational awareness for criminals by activating lighting remotely  
• Reduces situational awareness for guards/ CCTV operator by deactivating lighting remotely |
| Access Control                | • Remote release of secure doors resulting in unauthorised access  
• Deactivation of door release to inconvenience users/force use of green break glass  
• Deactivation of authorised users  
• Addition of unauthorised users  
• Erasure of access logs to cover criminal activity |
| HVAC                          | • Deactivation of cooling to cause plant/ ICT equipment to overheat/shutdown/malfunction  
• Activation of heating to cause plant/ ICT equipment to overheat/shutdown/malfunction  
• Deactivation of cooling/heating making normal working difficult or sometimes impossible |
| CCTV                          | • Increased situational awareness for intruder to be able to see guard locations and blind-spots  
• Ability to turn cameras away from criminal activity  
• Ability for intruder to erase footage  
• Ability to capture sensitive information such as passwords, sensitive business details or private activity that could cause embarrassment if made public |
| Lifts                         | • Denial of service  
• Override lift access control |
| Tenant Billing                | • Tenant’s under or overcharged for utility usage, affecting profitability or alienating customers |
| Building Information Modelling and CAD | • Criminals have a greater awareness of where key systems are located and how they are connected and powered |
| Building/ Perimeter Intruder Detection System | • Deactivation of system allowing unauthorised access  
• Creating false alarms for distraction  
• Erasure of event records to hide criminal activity |
| Fire Detection                | • Cause panic and disruption by activating alarm or risk lives by deactivating it (Note: We assume that fire detection would not be under the control of the BMS to comply with standards therefore vulnerabilities should be limited, but this may change in future) |
Specific Attack Vectors

Many BMS were developed at a time when the main concern was increasing operational efficiency, with cyber security being a minor concern.

Current systems are still largely manufactured by companies with a heritage in developing efficient building management systems, not companies with experience of cyber security. Flaws are likely to exist which leave them vulnerable to hackers. Furthermore, BMS run critical business infrastructure meaning they often cannot simply be taken down and/or upgraded. Even updating and patching software and firmware is difficult.

Those involved in installing and managing BMS tend not to have security expertise. As such new systems are often plugged straight into networks or connected to wireless networks without adequate security. They may be accessible through public Wi-Fi or even physically accessed. Default passwords are often left in place.

For this reason, a modern day attacker can access multiple attack vectors that are generally controlled in other more security conscious industries such as defence and energy.

The table below provides information about various attack vectors in relation to BMS security and the high-level controls needed in each case to mitigate those specific vectors.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of Protocol Security</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
<td></td>
<td>•</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>Erosion of Isolation</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>Convenience over Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>Weak Audit Trails</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>•</td>
<td></td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Vendor Backdoors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>Interconnection (IOT)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>Human Error</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>Unpatched Systems</td>
<td>•</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>Malware</td>
<td>•</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>Adoption of Common Technologies and Standards</td>
<td>•</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>Lack of Physical Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>•</td>
<td></td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>Default, weak or no security controls</td>
<td>•</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>•</td>
</tr>
</tbody>
</table>
Summary and Key Recommendations

Given the range of consequences for a compromised BMS and the current lack of security, we recommend organisations take a range of proactive measures to mitigate the risk of such an attack.

Prior to installation

- Prior to procurement, plan system design with secure architecture, understanding where systems are connected and how they are isolated from other systems
- The procurement and installation process should be verified by independent specialists, corporate security departments and Information Assurance (IA) specialists as appropriate
- Installation and maintenance contractors are certified to ISO 27001 or equivalent
- Facilities Managers are trained in relevant security issues, or security is transferred to the IT domain, employing IT security specialists
- Certified specialists are involved in the procurement and installation process, whether trained internally, recruited or bought in as consultants. Certifications covering this area include: Global Industrial Cyber Security Professional (GICSP); ISO 27001 Lead Implementer, and ISO 27001 Lead Auditor and the CESG Certified Professional (CCP)
- There is the provision of appropriate local override designed in from the outset
- Hardware access is physically secure and tamper alarms are prevalent especially in public/semi-public areas
- Critical systems such as a fire detection and control systems are air gapped from ICT networks

For companies with BMS already in place:

- BMS across the business should undergo a health check by certified Cyber Security professionals to ensure the system does not have the vulnerabilities outlined above
- All passwords are changed from default to secure passwords
- Installation and maintenance contractors are certified to ISO 27001 or equivalent
- Systems are regularly penetration tested by specialists certified to the standards mentioned to ensure that the security posture is maintained
- Those with full control of the BMS are limited to a small trusted pool of users
- Duties of those monitoring the BMS are appropriately separated
- If users with BMS access leave the company, remove them from the system immediately

Wider industry recommendations

- All BMS are designed by, or with consultation from, independent and certified security specialists
- Establish industry wide certification scheme to demonstrate BMS meets minimum security requirements
- Develop independent training programmes for buildings and facilities managers and BMS installers that cover security and/or integrate security into existing training programmes

Written by Andrew Kelly, security consultant in the QinetiQ Cyber Consulting team.

For more information contact: cyberteam@QinetiQ.com