Cybersecurity and BEMS

What is Cybersecurity?

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.

Why is Cybersecurity Important?

The report "Trends in cyberattacks, exploits and Malware, 2023 Global Threat Roundup Report" by Forescout Research documents that more than 420 million cyberattacks worldwide were made between January and December 2023. This equates to more than 13 attacks per second and represents a 30% increase over 2022.

Examples

- **Barcelona**: A cyberattack shut down a hospital's labs and pharmacies, surgeries were cancelled, and sensitive information was uploaded to the dark web, with a €4.5M ransom demand.
- **Ireland**: 180 houses lost water for two days due to a cyberattack targeting water pumps.
- Iran: Centrifuges in a nuclear power plant were permanently decreased by 30% efficiency due to hackers accessing through PLCs.
- **Finland**: A DDoS attack on a selection of buildings turned off the heating in freezing temperatures.
- **Saudi Arabia**: An oil & gas plant's safety control system was hacked through their Schneider Controllers.
- **USA**: in 2023 Johnson Controls spent $27M on cyberattack ransoms and penalties.

Austria: Hotel guests were locked inside their rooms because the hackers targeted the booking system and demanded a Bitcoin ransom.

What has this to do with BEMS?

The report also provides a breakdown of the types of vulnerabilities that were exploited and shows that 3% of these attacks were achieved through building automation systems. That equates to 13 million cyberattacks were carried out using building controls in 2023.

Why are BEMS systems so vulnerable to Cyberattack?

System Vulnerabilities

Legacy Systems
Many buildings use outdated BEMS that were not designed with modern cybersecurity threats in mind.

Default Configurations
Systems often run with default passwords and configurations, making them easy targets for attackers.

Network Security

Insecure Communication Protocols
Data transmitted between BEMS components and to/from external networks can be intercepted if not properly encrypted.

Unauthorised Access
Inadequate access controls can lead to unauthorised access to the BEMS, allowing attackers to manipulate energy systems.

Integration with Other Systems

IoT Integration
As BEMS integrates with other systems and IoT devices, the attack surface expands. Each connected device can be a potential entry point for cyberattacks.

Third-Party Services
Dependence on third-party cloud services for data storage and analytics can introduce additional vulnerabilities.

Physical Security

Access to Hardware
Physical access to BEMS hardware can lead to tampering or sabotage.

Insider Threats
Employees or contractors with malicious intent can exploit their access to the system.

sse
Energy Solutions

Best Practices for Securing BEMS

Regular Updates and Patch Management

- Ensure that all BEMS components are regularly updated with the latest security patches.

Strong Authentication and Access Controls

- Implement multi-factor authentication (MFA) for accessing the BEMS.
- Install a password management tool so that when employees leave, their access can be removed.
- Define and enforce strict access control policies.

Network Security Measures

- Use firewalls, intrusion detection/prevention systems (IDS/IPS), and virtual private networks (VPNs) to protect BEMS communications.
- Segment the network to isolate BEMS from other IT infrastructure.

Encryption

- Encrypt data at rest and in transit to prevent unauthorised access and data breaches.

Incident Response Planning

- Develop and regularly update an incident response plan to quickly address any cybersecurity incidents.
- Conduct regular drills and training sessions for staff.

Vulnerability Management

Perform regular vulnerability assessments and penetration testing to identify and mitigate potential security weaknesses.

Physical Security

- Secure BEMS hardware in locked and monitored locations.
- Implement security measures such as CCTV and access control systems.

User Training and Awareness

- Educate employees and contractors about the importance of cybersecurity and best practices for maintaining security.

Conclusion

Cybersecurity is essential for the safe and reliable operation of Building Energy Management Systems. As BEMS become more interconnected with other systems and devices, the complexity and potential for security vulnerabilities increase.

By implementing robust cybersecurity measures and staying vigilant, organisations can protect their BEMS from threats and ensure the continued efficiency and security of their energy management operations.

Talk to SSE about strengthening the security of your building systems

For a better world of energy

To find out more about how SSE Energy Solutions can help your organisation, get in touch today

info@sseenergyoptimisation.co.uk | 0345 072 9529 | SSEEnergySolutions.co.uk

SSE Energy Solutions is a trading name of TESGL Limited which is part of the SSE Group. The Registered Office of TESGL Limited is Ocean Court, Caspian Road, Atlantic Street, Altrincham, WA14 5HH. Registered in England & Wales No. 084 62158