ADVISORY NOTE

A service to A.G. Coombs Group Clients

Protecting Your Building Management and Control System from Cyberattack

A Building Management and Control System (BMCS) connected to a company intranet or the outside world via the internet offers the benefits of remote building systems management; monitoring, issue diagnosis, and control, but can also expose a building and its systems to significant operational risks from external attacks including: destructive viruses, phishing attacks, and Trojan horse attacks.

These type of attacks can not only severely affect building system operation including life safety systems, there is the potential to affect other interconnected systems including security and access control, communications and business enterprise systems.

As BMCS's are increasingly connected to business systems, they are now targets of ransomware style Trojan horse attacks, either directly, or indirectly from a targeted attack on connected systems. A Trojan horse attack is a malicious attack where a system is infiltrated via a vulnerability in software, social media, or by system users opening infected files commonly distributed by email or USB sticks.

A popular type of ransomware is Cryptolock, which uses an encryption type method where once the virus 'payload' has been introduced into the system it will begin to encrypt and disable large amounts of data on connected storage devices, then display a ransom message with a promise to unencrypt data, for a fee. Payment is commonly requested by an anonymous transaction system like bitcoin.

Cryptolock style attacks have become quite high profile in the media due to targeting mission critical business systems in hospitals, financial institutions, and large infrastructure and service providers. Ransom payments are common due to the mission critical status of the encrypted data, even though there is no guarantee that any data will, or can be recovered.

Ransomware style attacks are also becoming increasingly prevalent and harder to detect. The payload activation in an infected system may be delayed and lay dormant for some time to prevent detection, over time it may even penetrate deeper into a connected system and make complete removal near impossible.

Robust prevention and circumvention processes are now a necessity to assure uninterrupted service and damage minimisation, these should be applied to a BMCS and include:

- Regular Onsite and offsite backups
- Replacement of system default passwords
- Critical systems isolation
- Robust authorisation and security level rules
- Up to date firmware for all IT hardware
- Up to date anti-virus
- User training to identify suspicious files and activity
- Real time alerts and monitoring, e.g. File Server Resource Manager (FSRM)
- Available redundancy systems

Ransom message from the Cryptolocker trojan

Where possible it can be advantageous to include the management of the BMCS server and workstations within the management regime for business IT systems to ensure that all hardware, software and security policies are maintained to the same level as the enterprise systems. This should be coordinated with BMCS vendor to ensure the proper support of the BMCS applications.

As BMCS's become more advanced with more critical systems under their control, and more interconnected with other systems and the internet, it is imperative that proactive measures be put in place to assure uninterrupted service. The best cybersecurity process has elements to Predict, Prevent, Detect, and Respond to these risks.

A disrupted BMCS may prevent a building from being occupied and directly affect the business bottom line.

For futher information, please contact:

Andrew Smith, Leader Building Technologies
A.G. Coombs Advisory
T: +61 3 9248 2700
E: asmith@agcoombs.com.au