PRESS RELEASE

30/04/2015

Cyber-security: a journey, not a destination

Cyber-security has been a hot topic since the Stuxnet incident of a few years ago. Previously it was thought that securing the "top end" of an organisation was an adequate solution but this incident and others like it completely changed the security landscape and highlighted vulnerabilities in the de-facto automation architecture that previously had not been considered. Chris Evans, Marketing & Operations Group Manager at Mitsubishi Electric Europe B.V. Automation Systems Division, explains:

It shifted the problem to the automation domain, which had often operated under the radar and outside the remit of IT. Engineers suddenly started to reconsider their cyber-security arrangements. It was realised that many people may want to bring a plant to its knees, for political or commercial reasons, because they hold what they see as a legitimate grievance or simply to see what will happen.

Scenarios were imagined where drinking water became contaminated or supply interrupted, power plants shut down, or road, rail and air traffic management compromised. In the industrial world it was realised that control systems were potentially vulnerable, often due to out of date or poorly maintained operating systems and CD drives or USB ports that had not been locked down. It did not take a lot of imagination to work out that the more critical a control system, the more likely a target it would be to cyber-attack and the more damage that could be done.

Cyber-security is an arms race of escalating capabilities, so 'defenders' of vulnerable assets must see it as a journey rather than a destination, constantly reassessing the situation and implementing new defences whenever necessary. This is against the background of developing technologies and requirements that mean control systems are always becoming bigger, more complex, more distributed and increasingly open.

Most larger control systems have many points with potential for unauthorised access. Therefore layers of protection must be built into the system both at a network, hardware and software level. For instance, future PLCs (programmable logic controllers) will include multiple embedded features such as hardware security keys and multi-layer password structures.

Each PLC will be capable of hardware security key authentication to prevent programs from being opened or edited on unapproved personal computers that have not been "bound" to the security key. Furthermore, programs will be written so that they cannot be executed by PLCs which do not have a registered security key. Thus the integrity of embedded technologies and intellectual property will be protected from compromise. Additionally, an IP filter can be used to register the IP addresses of devices approved to access each PLC. Thus unauthorised access, whether for operational reasons, hacking or implantation of malware, will become much more difficult.

Whilst end users will want maximum security; they will also continue to insist on simplicity of operation. Some of these automation security measures, all of which are optional, could be argued to complicate operations and that is why a holistic view of security needs to be taken, considering all aspects of the operation. It may be that in some areas, some measures can be relaxed for the sake of continued operations and this is fine provided that the risk has been assessed and counter measures are implemented elsewhere to elevate the threat. As with everything related to cyber security, the consideration has to be probability and risk and security and operational systems should be designed around these important criteria.

It is probably an unchangeable aspect of the human condition that some people will always seek unauthorised access to control systems. Therefore control engineers must build security measures into their products and systems - and recognise that these are surmountable hurdles rather than impregnable barriers, so must be constantly renewed and redeveloped.

About Mitsubishi Electric

With over 90 years of experience in providing reliable, high-quality products to both corporate clients and general consumers all over the world, Mitsubishi Electric Corporation is a recognized world leader in the manufacture, marketing and sales of electrical and electronic equipment used in information processing and communications, space development and satellite communications, consumer electronics, industrial technology, as well as in products for the energy sector, water and waste water, transportation and building equipment.

With around 124.000 employees the company recorded consolidated group sales of 39.3 billion US Dollar* in the fiscal year ended March 31, 2014.

Our sales offices, research & development centres and manufacturing plants are located in over 30 countries.

Mitsubishi Electric Europe, Industrial Automation – UK Branch is located in Hatfield, United Kingdom. It is a part of the European Factory Automation Business Group based in Ratingen, Germany which in turn is part of Mitsubishi Electric Europe B.V., a wholly owned subsidiary of Mitsubishi Electric Corporation, Japan.

The role of Industrial Automation – UK Branch is to manage sales, service and support across its network of local branches and distributors throughout United Kingdom.

*Exchange rate 103 Yen = 1 US Dollar, Stand 31.3.2014 (Source: Tokyo Foreign Exchange Market)

Further Information:

Website: gb3a.mitsubishielectric.com
Website: www.mitsubishielectric.com
Email: automation@meuk.mee.com
Facebook: www.facebook.com/MEUKAutomation
Twitter: twitter.com/MEUKAutomation
YouTube:youtube.com/user/MitsubishiFAEU

Editor Contact
DMA Europa Ltd: Bob Dobson
Tel: +44 (0)1798 861677
Web: www.dmaeuropa.com

Email: bob@bobdobson.com

Reader Contact
Mitsubishi Electric Europe B.V. Automation Systems Division: Chris Evans, Marketing & Operations Group Manager
Tel: +44 (0) 1707 288769
Fax: +44 (0) 1707 278695
Web: gb3a.mitsubishielectric.com
Email: automation@meuk.mee.com