Available online at www.sciencedirect.com

ScienceDirect

Procedia Engineering 70 (2014) 872 – 876

Procedia Engineering

www.elsevier.com/locate/procedia

12th International Conference on Computing and Control for the Water Industry, CCWI2013

Security checklists: a compliance alibi, or a useful tool for water network operators?

M.G. Jaatun[a]*, J. Røstum[b], S. Petersen[a], R. Ugarelli[b]

[a]SINTEF ICT, NO-7465 Trondheim, Norway
[b]SINTEF Building and Infrastructure, NO-7465 Trondheim, Norway

Abstract

Checklist Compliance is a term that has been used derisively in the information security community, implying that checklists are something used for paying lip service to security without instigating real changes to technology or processes. In this paper we argue that checklists can also be used as a practical tool to quickly establish a security baseline for water and wastewater systems.

Keywords: information security; checklists; water and wastewater networks;

1. Introduction

"SMS fra VAV" stands for Secure and Monitored Service from Oslo VAV. This is a project that aims to improve the efficiency and the security in monitoring and control of the urban water and wastewater system of Oslo VAV in order to ensure a safe service to the public without compromising the environment, and while taking cost – efficient decisions for rehabilitation planning (Ugarelli et al. 2012). Oslo VAV has in the last years faced maloperation, accidents, or system failures with impacts to environment, service and loss of reputation. As a result,

* Corresponding author. Tel.: +47 900 26 921; fax: +47 73 59 43 02
E-mail address: martin.g.jaatun@sintef.no

doi:10.1016/j.proeng.2014.02.096

Oslo VAV has a clear priority to invest in monitoring for controlling the system reliability, and in mechanisms for avoiding unwanted incidents, thus retaining the public's trust.

However, while a monitored and controlled system can be more efficient and effective than a manual one, it can on the other hand be much more vulnerable. Integrated operational management in itself is not enough if security is not guaranteed. The ICT network has become a critical infrastructure within the critical infrastructure water itself. It is important that the IT security is evaluated with respect to the following three key aspects: confidentiality, integrity and availability.

We have developed a guidance document on information security in water and wastewater network operation for the Norwegian water sector, inspired by Good Practice efforts in the Dutch drinking water sector (Luiijf 2008), and complemented with our own experience from process control networks in the Norwegian oil industry (Jaatun et al. 2009). Since technical personnel are not primarily qualified in information security, we quickly found that a simple checklist is much more likely to be used by the intended audience than a thick report. Many industry representatives opined that detailed step-by-step instructions for specific tasks such as firewall configuration would be even more useful, but this must be balanced by the realization that detailed instructions have a much shorter shelf life than general guidelines, since the former are frequently made obsolete by improvements in technology.

In this paper we will describe initial experiences with our guide and checklist, and show how the checklist can be used both to gauge the current information posture of the water organization, and to establish a security baseline for water and wastewater control system networks (Jaatun et al. 2013).

2. Background

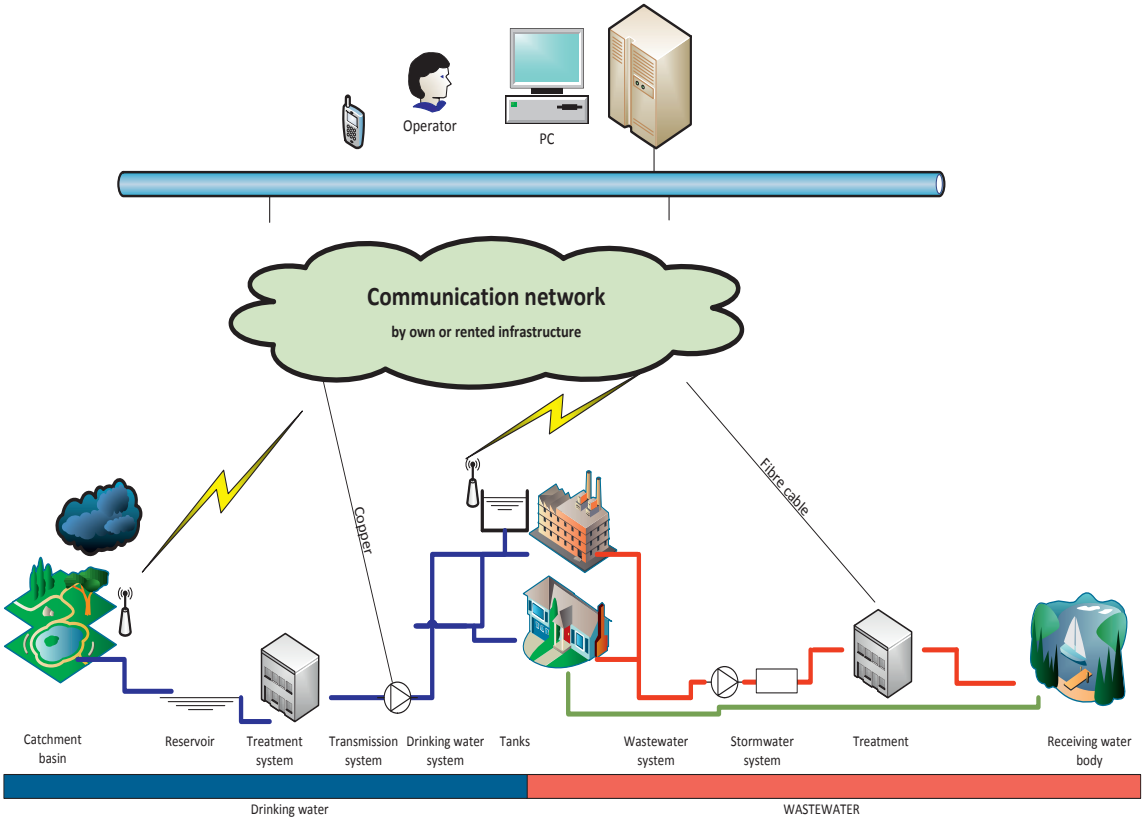

Fig. 1. Illustration of the urban water cycle with corresponding communication system

Traditionally, industrial control systems such as found in the water and wastewater sector have consisted of closed networks with no outside communication. This is rapidly changing, and recent experiments show that the attackers are aware of these developments: A researcher at Trend Micro connected a cluster of industrial control systems honeypots to the internet, and found that they were under attack in less than a day (Simonite 2013). A honeypot (Jaatun et al. 2007) is a network server which looks like it provides a normal service to an outside observer, e.g., a web server, a file server, or in this case an industrial control system. In reality, a honeypot will simulate the function it is supposed to emulate, providing plausible responses to anyone who interacts with it, but not actually performing the requested actions. The honeypot owner, on the other hand, will be provided with a full complement of interaction logs to analyze the intentions of the attackers (since a honeypot has no legitimate uses, anybody who tries to use it is by definition an attacker). A total of 39 attacks were registered during the experiment, and it is interesting to note that several of the attacks attempted to change water pressure or manipulate pumps. The fact that attackers could find the systems so quickly is not surprising, since there are dedicated search engines available to specifically locate industrial control systems connected to the internet (ICS-CERT 2011).

Modern water networks involve many process control technologies (Fig. 1), and it is increasingly important to consider information security in the water domain. The classical information security incident in process control networks is indeed the Maroochy Shire incident (Slay and Miller 2007), where a disgruntled employee misused credentials to cause a sewage spill with major environmental impact. Current reports indicate that industrial control network professionals do not currently have faith is the security of their systems (LaMonica 2013). Since all processes now are automated, an attacker could inflict major damage both to water supply and sewage treatment.

Many process control systems professionals were forced to reconsider their position that "information security breaches will not happen in our systems" when the Stuxnet malware was discovered in 2010 (Chien 2011). Allegedly developed by US and Israeli intelligence agencies, Stuxnet was specifically targeted at Iranian nuclear reactor centrifuges in order to delay the suspected Iranian nuclear weapons program. Stuxnet contained an unprecedented 4 different zero-day Windows exploits to be used against the Human-Machine Interface (HMI) which subsequently allowed it to make disastrous changes to the Programmable Logic Control units the HMI was controlling.

A testament to the vulnerability of water networks is given by Dilanian (2011), who cites a penetration testing exercise at a major US water operator in 2011. Within a day, the hired consultant was able to completely penetrate the operator's process control networks, to the extent where he was in a position to modify the amount of chemical additives at the drinking water treatment plant. Remote access to the process control network by operator employees was identified as the weak point, putting the attacker in a position to make the water for millions of subscribers undrinkable.

3. Checklist development

The checklist has initially been based on several good practice documents as mentioned above, and in particular on Luiijf (2008). This initial list has then gone through several iterations with domain and/or security experts, converging on 45 questions to be treated as recommendations (i.e., answering "yes" is better than answering "no"). To get a more fine-grained result, we also added the possibility to answer "to some extent". Finally, we added a "not applicable" option, but stipulated that a justification has to be provided if this is selected.

A snapshot of the checklist with result visualization is given in Fig. 2. The color scheme is intuitively selected, with green (yes), amber (to some extent), and red (no). The color blue has been selected for "not applicable". Water and wastewater network owners in Norway are predominantly municipalities, many of which are small and with limited resources. There is thus an important psychological element in the visualization of the result; heaping long wordy reports on the local finance committee's agenda is more likely to make the members' eyes glaze over, but a blood-red donut from a good-practice checklist may make them sit up and pay attention.

Checklist for more secure W&W process control networks

	Questions	Yes	Somewhat	No	N/A
1	Does information security in process control systems (PCS) have sufficient buy-in from upper management?	x			
2	Is there information security awareness in the entire organization?		x		
3	Does all users have individual usernames and credentials for access to PCS?		x		
4	Have all standard passwords been removed?			x	
5	Are minimum strength requirements for passwords enforced?			x	
6	Are regular password change requirements enforced?			x	
7	Is 2-factor authentication required for remote access to PCS?		x		
8	Does the organization have control over who has access to PCS, which operations they are allowed to perform, and when they have accessed the system?	x			
9	Can different access levels (read-only, modify) be specified for different users?				x
10	Are access rights audited annually to ensure that they are correct and at the right level?				x
11	Has a security risk analysis that also covers off-premise on-call scheme been performed?				x
12	Are only dedicated computers or tablets used for PCS administration?				x

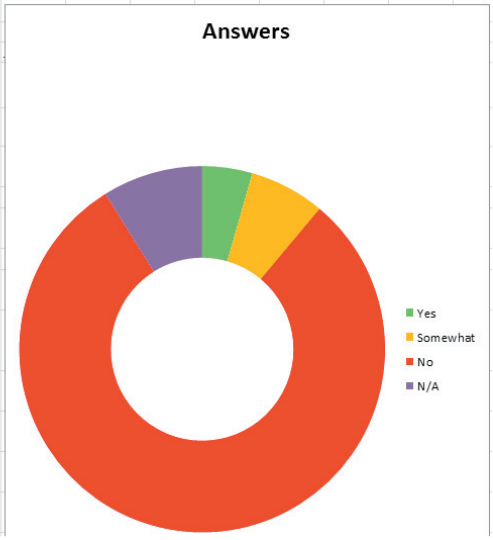

Fig. 2. Illustration of the checklist and quick results

4. Discussion and Further Work

As already mentioned, very detailed checklists have a short shelf life; Information and Communication Technologies change quickly, and step-by-step instructions for yesterday's solutions end up being more of a nuisance than a help. Thus, it is important that checklists are sponsored, and maintained on a regular basis, for instance by a relevant member organization.

While it is obviously important to ensure that process control systems in the water and wastewater sector are as secure as possible, we must acknowledge that 100% security is unattainable in any practical system. This implies that security incidents will eventually happen in any system, and it is incumbent upon system owners to prepare for when this happens.

There are several critical infrastructure sectors that share many similarities with the water and wastewater sector; from our personal experience we would like to highlight the oil and gas sector, and the electric power transmission and distribution sector. In a recent study performed by Line (2013), it is revealed that very few electricity Distribution Service Operators (DSOs) have formalized procedures for handling of ICT security incidents. Our discussions with water and wastewater sector representatives seem to indicate a similar situation in that industry, and we see this as an area for improvement. Furthermore, a sector-specific incident reporting scheme should be established; both in order for quicker dissemination of threats and specific attacks within the sector, but also to facilitate better learning from incidents (Jaatun et al. 2009). This is particularly important for smaller water network operators whose limited resources make it difficult to prioritize learning activities in isolation.

Unfortunately, information security is a never-ending process, and since the threat picture is constantly evolving, continual improvement is the only choice for an organization wishing to maintain a good security posture. Bernsmed & Tøndel (2013) argue for the use of security indicators in order to stay one step ahead of the malfeasors. We believe that many of their experiences from the oil & gas industry can be applicable to the water sector.

5. Conclusion

We have presented a checklist for use when establishing a security baseline for water network operators. By balancing generality with detailed step-by-step-instructions, we find that this checklist can offer a tangible improvement in security of particularly smaller water network operators.

Acknowledgements

This paper has reported results from the research project "Secure and Monitored Service from Oslo Water and Sewerage Works" funded by *Regionalt Forskningsfond Hovedstaden* and Oslo VAV. The checklist development was funded by Norsk Vann.

References

Bernsmed, K. and Tøndel, I. A. 2013. Forewarned is Forearmed: Indicators for Evaluating Information Security Incident Management. in "IMF 2013 - 7th International Conference on IT Security Incident Management and IT Forensics", IEEE Computer Society: 3-14.

Chien, E. 2011 "W32.Stuxnet Dossier." Security Response Blog http://www.symantec.com/connect/blogs/w32stuxnet-dossier.

Dilanian, K. 2011. Virtual war a real threat. Los Angeles Times.

ICS-CERT. 2011, May 2013. "Control System Internet Accessibility." Retrieved May, 2013, from http://ics-cert.us-cert.gov/alerts/ICS-ALERT-11-343-01.

Jaatun, M. G., Grøtan, T. O. and Line, M. B. 2009. "Secure remote access to autonomous safety systems: A good practice approach." International Journal of Autonomous and Adaptive Communications Systems 2(3).

Jaatun, M. G., Nyre, Å. A. and Sørensen, J. T. 2007. Survival by Deception. in "Computer Safety, Reliability, and Security - 26th International Conference, SAFECOMP 2007, Nuremberg, Germany, September 18-21, 2007. Proceedings". F. Saglietti and N. Oster. Nürnberg, Springer.

Jaatun, M. G., Røstum, J. and Petersen, S. 2013. Security guidelines for industrial information and control systems used for water and wastewater systems (in Norwegian). . Norsk Vann Rapport, Norsk Vann.

LaMonica, M. 2013 "Cybersecurity Risk High in Industrial Control Systems." MIT Technology Review http://www.technologyreview.com/view/511671/cybersecurity-risk-high-in-industrial-control-systems/

Line, M. B. 2013. A Case Study: Preparing for the Smart Grids - Identifying Current Practice for Information Security Incident Management in the Power Industry. in "IMF 2013 - 7th International Conference on IT Security Incident Management and IT Forensics", IEEE Computer Society: 26-32.

Luiijf, E. 2008. SCADA Security Good Practices for the Drinking Water Sector, TNO.

Simonite, T. 2013 "Honeypots Lure Industrial Hackers Into the Open." MIT Technology Review http://www.technologyreview.com/news/514216/honeypots-lure-industrial-hackers-into-the-open/.

Slay, J. and Miller, M. 2007. Lessons Learned from the Maroochy Water Breach. in "Critical Infrastructure Protection". E. Goetz and S. Shenoi, Springer Boston. 253: 73-82.

Ugarelli, R., Selseth, I., Myhre, B., Berge, S. P. and Jaatun, M. G. 2012. SMS fra VAV- First periodic progress report - Project objectives, work progress and achievements, project management, SINTEF