REPORT FOR ACTION

Toronto Water SCADA System Security – Results of 2021 Follow-up of Previous Audit Recommendations

Date: October 20, 2021
To: Audit Committee
From: Auditor General
Wards: All

SUMMARY

In 2019, the Auditor General became aware of attacks on critical water systems in the U.S. and other jurisdictions. In addition, there were a number of alerts issued by the U.S. Department of Homeland Security (DHS), the U.S. Federal Bureau of Investigation (FBI), the Canadian Centre for Cyber Security, and other agencies.

These alerts included attacks and ransomware campaigns by foreign states, including an alert in March 2018 from the DHS and the FBI about a multi-stage intrusion campaign by Russian government cyber actors who targeted small commercial facilities' networks. The attackers staged malware, conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, the cyber actors conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems (ICS)[1].

The Auditor General became particularly concerned when she learned of a threat published by the U.S. Attorney General Cyber Digital Task Force describing that:

> "Iranian hackers… gained access to the Supervisory Control and Data Acquisition ("SCADA") system of a dam in New York, allowing him to obtain information regarding the dam's status and operation. Had the system not been under maintenance at the time, **the hacker would have been able to control the dam's sluice gate**[2]."

The Auditor General's concern was that if hackers could gain access and remotely move the doors on a dam, they could possibly also do other damage like manipulating chemicals in a water system.

After considering the increased risks, the increased number of alerts and the importance of cybersecurity at our own critical systems, the Auditor General fast-tracked

[1] https://us-cert.cisa.gov/ncas/alerts/TA18-074A
[2] https://www.justice.gov/archives/ag/page/file/1076696/download

an audit of the Toronto Water SCADA network in November 2019. The Auditor General had just completed a cybersecurity assessment of the City's overall IT infrastructure.

The audit of Toronto Water's SCADA system was the Office's first audit of the City's critical infrastructure Operational Technology (OT) systems. The objectives of the audit were to assess the adequacy of controls in place to address potential threats to the SCADA network, systems and applications. The results were tabled at the February 10, 2020 Audit Committee through a confidential report.

Following the initial audit, there were increased attacks on water facilities and other critical infrastructure systems. Those attacks are becoming more sophisticated and focused.

Recent Cybersecurity Incidents on Water Facilities/SCADA Systems:

1. Compromise of U.S. Water Treatment Facility

An alert from the U.S. Cybersecurity and Infrastructure Security Agency warned water system operators that there was a remote attack where the attacker tried to change the chemicals in the water supply. According to the Agency:

> "On February 5, 2021, unidentified cyber actors obtained unauthorized access to the supervisory control and data acquisition (SCADA) system at a U.S. drinking water treatment facility.
>
> The unidentified actors used the SCADA system's software to increase the amount of sodium hydroxide, also known as lye, a caustic chemical, as part of the water treatment process.
>
> Water treatment plant personnel immediately noticed the change in dosing amounts and corrected the issue before the SCADA system's software detected the manipulation and alarmed due to the unauthorized change… The cyber actors likely accessed the system by exploiting cybersecurity weaknesses, including poor password security, and an outdated operating system. Early information indicates it is possible that a desktop sharing software, such as TeamViewer, may have been used to gain unauthorized access to the system, although this cannot be confirmed…."[3]

2. Ransomware Attack on SCADA Systems at three Water Facilities in U.S.

The October 14, 2021, alert from the above-referenced U.S. government agencies describes recent ransomware attacks that impacted industrial control systems (ICS) at water facilities[4]:

[3] Compromise of U.S. Water Treatment Facility | CISA
[4] Ongoing Cyber Threats to U.S. Water and Wastewater Systems | CISA

- In the first incident, cybercriminals used unknown ransomware to target a water facility in Nevada in March 2021. The malware affected SCADA and backup systems.
- In the second incident, hackers deployed the ZuCaNo ransomware, which made its way onto a wastewater SCADA computer in Maine in July 2021. The treatment system was run manually until the SCADA computer was restored using local control and more frequent operator rounds.
- In the third incident, threat actors deployed a piece of ransomware named Ghost on the systems of a water plant in California in August 2021. The ransomware was discovered roughly a month after the initial breach, after the organization noticed three SCADA servers displaying a ransomware message.[5]

Following up on Toronto Water's progress

The Auditor General regularly reviews the implementation status of recommendations and reports the results to City Council through the Audit Committee. This follow-up review assessed Toronto Water's progress towards addressing issues and recommendations raised in the February 2020 report[6] so that the SCADA network, systems and applications remain protected.

To verify the implementation of audit recommendations, we undertook significant work to re-test the physical security at selected water facilities, network security and user access management of the SCADA network, systems and applications to identify any remaining gaps.

Testing Results – Progress made by Toronto Water

The initial audit was timely, and based on our testing, we found that Toronto Water has implemented many recommendations and made substantial progress in many areas. The following are some key areas where the Auditor General found significant progress:

- Physical security at water facilities and IT equipment
- Implementation of technical fixes related to cybersecurity
- Discontinuation of outdated systems and devices
- Staff training and awareness

The results of the testing will be provided to City Council through the Audit Committee in a separate confidential report.

Of note, we noticed a culture shift at Toronto Water in the level of awareness and importance of staying vigilant for cybersecurity risks. Going forward, however, cybersecurity risks will continue to evolve and change. Toronto Water needs to finish implementing the recommendations and directly monitor for and address any new security risks.

[5] Ransomware Hit SCADA Systems at 3 Water Facilities in U.S. | SecurityWeek.Com
[6] https://www.toronto.ca/legdocs/mmis/2020/au/bgrd/backgroundfile-145342.pdf

RECOMMENDATIONS

The Auditor General recommends that:

1. City Council receive this report for information.

FINANCIAL IMPACT

Implementing the cybersecurity audit recommendations will strengthen cybersecurity controls at the City. The extent of costs and resources needed to implement the recommendations is not determinable at this time. The investment needed to improve controls to manage and respond to cyber threats offsets the potentially significant costs that could result from security breaches, which could include data recovery/cleanup, financial loss, reputational damage, fines or litigation.

DECISION HISTORY

The follow-up of outstanding recommendations is required by Government Auditing Standards. The process is important as it helps to ensure that management has taken appropriate actions to implement the recommendations from previous audit reports.

This follow-up review is part of the Auditor General's Annual Work Plan. The Auditor General's Work Plan can be found at:

https://www.toronto.ca/legdocs/mmis/2020/au/bgrd/backgroundfile-158178.pdf

COMMENTS

As discussed in the above sections, cyber attackers are focusing more and more on critical infrastructure and systems to try to gain unlawful access to confidential data or to disrupt operations for malicious purposes.

Water IT infrastructure and SCADA systems are targeted because they use operational technology, where outdated systems and devices are still in use. These outdated systems and devices are easy to hack.

Critical Infrastructure and SCADA Systems

Critical Infrastructure definition, according to Public Safety Canada:

> "*Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. …Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence*[7]*."*

SCADA Systems: Supervisory Control and Data Acquisition (SCADA) systems are used in a variety of critical applications and industries including energy, utilities, transportation and water. This is a computer system used to monitor and analyze real-time data, and control both local and geographically dispersed industrial processes.

The Canadian Cyber Security Centre describes how ICS and SCADA systems are vulnerable if the appropriate cybersecurity protections are not in place:

> *"As part of the drive for modernization and efficiency, critical infrastructure providers are continuing to automate their processes and connect IT and OT devices to the Internet. While connecting OT, such as ICS and SCADA devices, to the Internet provides several advantages — for example, remote management — it can also expose critical infrastructure to cyber threat activity* [8]*".*

Toronto Water's SCADA System

The Toronto Water Division is responsible for treating, transmitting and storing drinkable water for all industrial, commercial and household water users in the City of Toronto and parts of York Region. It also treats wastewater from the City of Toronto and parts of Peel Region.

The SCADA system controls highly critical infrastructure equipment and processes that impact Toronto residents, businesses, industries and the environment.

Cybersecurity threats will continue to increase

While Toronto Water is doing a much better job, cyberattacks will likely continue to increase in frequency and sophistication. Toronto Water needs to continue to expedite the implementation of recommendations and stay on top of any new risks and risk advisories. While Toronto Water should continue to work in partnership with the Office of the Chief Information Security Officer (CISO) and the Technology Services Division, it needs to remain the driving force behind ensuring its systems are safe. Clear governance and accountability agreements would be helpful to ensure all players are aware of the responsibilities they must fulfil.

---

[7] https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx

[8] https://cyber.gc.ca/en/guidance/increasing-cyber-threat-exposure

Conclusion

During this follow-up review, we found that Toronto Water has made significant progress in implementing a number of recommendations. Management actions to date have demonstrated Toronto Water's commitment to cybersecurity, and most importantly, there is a culture shift evident as it is moving forward to proactively address cyber threats. With the recent cybersecurity advisories, Toronto Water needs to continue to expedite implementation of recommendations as fast as possible and stay on top of any new risks and risk advisories.

As discussed in the Executive Summary, the implementation work by the Division and the Auditor General's review is ongoing. The results of our review will be provided to Council through the November 2, 2021 Audit Committee in a separate confidential report.

Our follow-up report does not constitute a performance audit conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS). However, we believe that we have performed sufficient work to validate management's assertions on the implementation of recommendations.

We express our appreciation for the co-operation and assistance we received from management and staff of the Toronto Water Division.

CONTACT

Syed Ali, Audit Director, IT and Strategy, Auditor General's Office
Tel: (416) 392-8438, E-mail: Syed.Ali@toronto.ca

Suzanna Chan, Audit Manager, Auditor General's Office
Tel: (416) 392-8033, E-mail: Suzanna.Chan@toronto.ca

SIGNATURE

Beverly Romeo-Beehler
Auditor General