Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

COVID-19: Remote Access to Operational Technology Environments

MAY 2020

Introduction

This cyber security advice is for critical infrastructure providers who are deploying business continuity plans for Operational Technology Environments (OTE)/Industrial Control Systems (ICS) during the COVID-19 pandemic.

This guidance is specifically for people working in an OTE. For general COVID-19 contingency planning advice, see ***Cyber security is essential when preparing for COVID-19***[1].

For COVID-19 cyber security threats, see ***Threat Update: COVID-19 Malicious Cyber Activity***[2].

Context

Many critical infrastructure providers are moving to remote working arrangements in line with social distancing guidelines.

Modifying cyber security defences to the OTE is not a decision you should take lightly. Physical worksites such as control rooms and operations floors provide inherent security benefits by restricting physical and cyber access to the OTE. Corporate information technology provides an additional defensive layer.

An increase in remote working significantly increases opportunities for adversaries to gain unauthorised access to systems and may cause real world physical harm. Critical infrastructure providers need to balance the risks and opportunities of moving staff offsite and document those considerations for senior managers to make informed risk-based decisions on sustaining business continuity.

Consider this guidance along with your established change management policies and procedures.

General remote access guidance

Endpoint management

Minimise trust in endpoints that connect to your remote access solution, such as home networks and devices. The more your solution trusts the endpoint, the more controls you will need to mitigate those risks. Ideally, you should supply and configure a work laptop and network connection (such as separate mobile wireless hotspots) to remote workers to connect to the OTE. This circumvents the need to use home computing and networks all together.

[1] https://www.cyber.gov.au/news/cyber-security-essential-when-preparing-covid-19
[2] https://www.cyber.gov.au/threats/threat-update-covid-19-malicious-cyber-activity

If your organisation does supply mobile communications, a mobile hotspot is preferable to a device that requires additional drivers, like USB dongles. Ensure all communications are encrypted and that Virtual Private Network split tunnelling is disabled[3]. Insist that remote workers avoid activities like web browsing on devices that access the OTE.

Encourage remote workers to improve their home cyber security. However, as you have little control over endpoints, it is reasonable practice to assume that endpoints are compromised, and user credentials can be stolen. Take steps to minimise the impact and harm that compromised credentials can cause:

- Use a limited privileged account for remote access[4]. Adversaries target remote access credentials in order to gain an initial foothold.
- Use unique passphrases for every system within your environment. This limits the reach that a compromised passphrase has in your organisation.
- Use multi-factor authentication (MFA) [5], particularly to protect your remote access solution and privileged accounts or sensitive information.

Ensure that remote workers lock remote sessions when not in use, and do not share devices with other members of their household. If other members of the household can see work screens, it may be a breach of organisational policy and ***The Privacy Act 1988***[6]. Confirm that remote workers have a private physical space for working with sensitive information.

Given the assumption that your OTE personnel have technical knowledge, suggest they use an isolated Virtual Local Area Network if the home network has such capability. For example, most home networks have a 'guest wireless network' which is often left unused. This Virtual Local Area Network can be used to segregate devices from the rest of the household's internet traffic.

Corporate systems

On the corporate side, prioritise remote access system patches. An adversary will attempt to compromise your system as soon as they discover a vulnerability. Prepare for an increase in malicious email[7] and Denial of Service attacks[8] and consider restricting geolocations or source Internet Protocol addresses, noting that this would have a limited effectiveness against a persistent adversary.

Implement remote vulnerability scanning to know which essential services may be exposed to adversaries. Centralise and monitor remote access logs for anomalies, preferably in real time[9].

Finally, keep records of all changes for when business-as-usual operations resume, particularly changes to remote access services. Follow the remote access advice in the ***Australian Government Information Security Manual*** (ISM)[10] and brief key employees of the additional risks inherent in implementing remote access arrangements.

[3] https://www.cyber.gov.au/publications/using-virtual-private-networks
[4] https://www.cyber.gov.au/publications/restricting-administrative-privileges
[5] https://www.cyber.gov.au/publications/implementing-multi-factor-authentication
[6] https://oaic.gov.au/privacy/the-privacy-act
[7] https://www.cyber.gov.au/publications/malicious-email-mitigation-strategies
[8] https://www.cyber.gov.au/publications/preparing-for-and-responding-to-denial-of-service-attacks
[9] https://www.cyber.gov.au/ism/guidelines-for-system-monitoring
[10] https://www.cyber.gov.au/ism/australian-government-information-security-manual

Remote access in Operational Technology Environments

Minimise overall exposure

Consider whether alternate physical sites (like control rooms) would provide sufficient business continuity before permitting remote access working arrangements. A secondary (or tertiary) control room with dedicated communication links to the OTE may offer better (cyber and physical) security.

Personnel requirements

OTE, telecommunications and cyber security specialists are a scarce resource, so ensure your organisation has a human resource plan to manage the increase in workload. Seconding additional personnel during the COVID-19 pandemic may be a practical measure to manage the increased workload.

OTE personnel may have to compete with corporate personnel for network bandwidth when accessing the OTE. In this case, attempts to gain OTE access may receive a denial of service during a critical time, such as when people's safety is at risk. Ideally, OTE personnel requiring access to the OTE should have a separate logical path than corporate personnel who need access to the corporate environment. If a dedicated path is unavailable, prioritise the remote access sessions OTE personnel will use.

Change management

Document all proposed changes and develop a run-sheet to record both planned and unplanned configuration changes, deployment, and rollback decision points.

Backup your device configurations before making changes to interfaces between corporate and the OTE to ensure you can return to business-as-usual operations.

Actively maintain a detailed logical diagram of the network while the business continuity plan is in effect. This allows clear understanding of all remote access pathways and easy removal of paths added to temporarily supplement access to the OTE during business continuity.

Develop a rapid disconnection plan for 24-hour deployment, disconnecting remote access if malicious activity is identified. Incorporate your rapid disconnection plan into incident response planning, and capture communications channels, reporting requirements, and physical and/or logical isolation of the OTE.

Maintain vision of vulnerability alerts[11] and advisories[12] affecting OTE/ICS. Patch vulnerable systems where possible.

Communications

Establish and routinely test formal lines of communication between teams (such as between the change management team, Cyber Security Operation Centre, and the real-time control room) to ensure the resilience of your communications pathways.

[11] https://www.us-cert.gov/ics/alerts
[12] https://www.us-cert.gov/ics/advisories

Jump hosts

You should configure a minimum of two jumps for remote access to an OTE.

Preferably, the first jump should be from a device supplied and controlled by your organisation, with a Virtual Private Network connection. If using personal devices, use corporate Virtual Desktop Infrastructure.

The jump should go to a jump host in a demilitarised zone outside the OTE.

The second jump then moves to the second jump host within the OTE.

Each remote worker should have a unique account, strong passphrase[13] and individual MFA for each jump. This means it will take a minimum of two unique account names, two unique passphrases and two MFA tokens to reach the OTE:

- Each jump host should be bound to a separate security domain and configured using the principle of least privilege[14].
- Suspend or disconnect idle jump host sessions after 15 minutes.
- Disable remote desktop copy/paste functionality and drive redirections into the OTE to reduce risks of sensitive information disclosure and malicious file transfers[15].
- Download patches such as binaries or scripts onsite, on corporate systems and verify each file's authenticity. Then initiate the transfer from within the OTE. Do not allow patches into the OTE via remote access.

For more information see: ***Essential Eight Explained***[16], ***Essential Eight in Linux Environments***[17], ***Guidelines for System Hardening***[18] and ***Guidelines for System Management***[19] within the ISM, and ***Fundamentals of Cross Domain Solutions***[20].

Monitoring and auditing

Increase automated monitoring and auditing of account logins, login failures, deviations from baseline traffic and anomalous network access.

Produce daily reports that identify abnormal logins (behaviour that is unusual – for example someone who is not on a nightshift logs in at midnight). Ensure you have the audit trail you need to support incident response and protective monitoring.

Automate potentially hostile abnormalities with priority notifications (such as an email or SMS) to your security operations team. Limit notification fatigue by restricting numbers to only those that require urgent investigation, and write targeted, specific and context-appropriate messages.

Consider full packet capture on key data choke points both inside the OTE and at the boundary. As the OTE network traffic is often unencrypted, it is difficult for an adversary to remain hidden in a full packet capture.

Engage an independent party to 'blue-team' your remote access solution. Given the possible impact on physical systems, any penetration testing will typically stop at the OTE boundary.

---

[13] https://www.cyber.gov.au/news/get-smarter-with-passwords
[14] https://www.cyber.gov.au/publications/restricting-administrative-privileges
[15] https://www.cyber.gov.au/publications/hardening-microsoft-windows-10-version-1709-workstations
[16] https://www.cyber.gov.au/publications/essential-eight-explained
[17] https://www.cyber.gov.au/publications/essential-eight-in-linux-environments
[18] https://www.cyber.gov.au/ism/guidelines-for-system-hardening
[19] https://www.cyber.gov.au/ism/guidelines-for-system-management
[20] https://www.cyber.gov.au/publications/fundamentals-of-cross-domain-solutions

Embrace continual improvement

When you return to business-as-usual operations, remove measures that temporarily increased risks.

As you revert your network to a known secure state, update your baseline documentation and incorporate any changes that enhanced your cyber security.

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. It can be found at https://www.cyber.gov.au/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents.

For further information on this topic, see the following publications:

- the Australian Government's ***Remote Access: A Tool to Support Business Continuity Planning***[21]
- the US Department of Homeland Security's ***Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies***[22].

Contact details

Organisations or individuals with questions regarding this advice can email asd.assist@defence.gov.au or call 1300 CYBER1 (1300 292 371).

[21] https://www.tisn.gov.au/Documents/CSG%20Remote%20Access%20-%20A%20Tool%20to%20Support%20Business%20Continuity%20-%20PDF%20ed.pdf
[22] https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf