Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Remote access to operational technology environments

First published: May 2020
Last updated: March 2023

Introduction

Many critical infrastructure providers are moving to support remote working arrangements. In doing so, modifying cybersecurity defences for operational technology environments (OTE) is not a decision that should be taken 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 malicious actors 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.

General remote access guidance

Endpoint management

Minimise trust in endpoints that connect to remote access solutions, such as home networks and devices. The more a solution trusts the endpoint, the more controls will be needed to mitigate those risks. Ideally, supply and configure a work device and network connection (such as a separate mobile wireless hotspot) for remote workers to connect to the OTE. This circumvents the need to use home computing and networks altogether.

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

Encourage remote workers to improve their home cybersecurity. However, as there is often little control over endpoints, it is a 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 by:

- using a limited privileged account for remote access
- using unique passphrases for every system within the environment
- using multi-factor authentication (MFA), particularly to protect the 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*. Confirm that remote workers have a private physical space for working with sensitive information.

Given the assumption that remote workers have technical knowledge, suggest they use an isolated Virtual Local Area Network if the home network has such a 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 work devices and their traffic from the rest of the household's internet traffic.

Corporate systems

On the corporate side, prioritise remote access system patches. Malicious actors will attempt to compromise a system as soon as they discover a vulnerability. Prepare for an increase in malicious email and denial-of-service attacks and consider restricting geolocations or source Internet Protocol addresses, noting that this would have a limited effectiveness against persistent malicious actors.

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

Finally, follow the remote access advice in the Australian Signals Directorate's *Information security manual* (ISM) and brief key employees on the additional risks inherent in implementing remote access arrangements.

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 security.

Personnel requirements

OTE personnel working remotely 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 peoples' safety is at risk. Ideally, OTE personnel requiring access to the OTE should have a separate logical path from 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 for the OTE.

Backup device configurations before making changes to interfaces between the corporate environment and the OTE to ensure configurations can be rolled back if needed to return to business-as-usual operations following a failed change attempt.

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 a rapid disconnection plan into cybersecurity incident response planning, and capture communications channels, reporting requirements, and physical or logical isolation of the OTE.

Maintain vision of vulnerability alerts and advisories affecting the OTE. Patch vulnerable systems where possible as soon as possible.

Communications

Establish and routinely test formal lines of communication between teams (such as between the change management team, security operations centre and the real-time control room) to ensure the resilience of communications pathways.

Jump hosts

Configure a minimum of two jumps for remote access to the OTE. Preferably, the first jump should be from a device supplied and controlled by the organisation, with a Virtual Private Network connection. If using personal devices, use corporate Virtual Desktop Infrastructure. The first 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 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. In addition:

- each jump host should be bound to a separate security domain and configured using the principle of least privilege
- idle jump host sessions should be suspended or disconnected after 15 minutes
- remote desktop copy/paste functionality and drive redirections into the OTE should be disabled
- patches, such as binaries or scripts, should be downloaded onsite using corporate systems and verified for authenticity
- patches should be transferred from within the OTE, do not allow patches into the OTE via remote access.

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 (e.g. someone who is not on a nightshift logging in at midnight) and ensure there is an audit trail to support monitoring and response activities.

Automate altering of abnormalities with priority notifications (such as an email or SMS) to security operations teams. Limit notification fatigue by restricting altering 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 malicious actors to remain hidden in a full packet capture.

Engage an independent party to assess the security of the remote access solution. Given the possible impact on physical systems, any penetration testing will typically stop at the OTE boundary.

Further information

The *Information security manual* is a cybersecurity framework that organisations can apply to protect their systems and data from cyberthreats. The advice in the *Strategies to mitigate cybersecurity incidents*, along with its Essential Eight, complements this framework.

Further information on this topic in the Australian Government's *Remote Access: A Tool to Support Business Continuity Planning* and the United States Department of Homeland Security's *Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies* publications.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate