ACSC releases guidance for critical infrastructure providers to help reduce risk of cyber attack during COVID-19 pandemic

Sources: www.cyber.gov.au

Date: 27 May 2020

Abstract:

The Australian Cyber Security Centre (ACSC) has produced advice to help critical infrastructure providers protect themselves from cyber attack as key staff work remotely during the COVID-19 pandemic.

Critical infrastructure facilities such as power and water distribution networks, as well as transport and communication grids, are potential targets for malicious cyber adversaries in Australia and elsewhere.

The guidelines come as the ACSC continues to see attempts to compromise Australia's critical infrastructure during the pandemic. The challenge of keeping businesses running while allowing access to sensitive operational technology assets by staff working remotely – staff who would normally be locate in control rooms or worksite protected by effective cyber and physical security barriers – poses considerable risks that malicious actors are actively seeking to exploit.

The ACSC advice provides guidance on technical controls that organisations can use to respond to challenges associated with COVID-19, as well as to support operations and staff working remotely, some for the first time.

The guidance outlines general cyber security practices for remote working, as well as specific advice for infrastructure operations including:

- consideration of a secondary or tertiary operations control room that may offer better security controls than home or remote access;
- using the key technical control of two communications 'jumps' to reach the operations environment, combined with unique accounts, passphrases, and multi-factor authentication;
- maintaining a detailed logical diagram of the operations network; and
- having a rapid disconnect plan that can be deployed quickly at any time if malicious activity is identified.

The ACSC guidelines are available here.

The ACSC media release can be found here.

LexisNexis | About LexisNexis | Privacy Policy | Terms & Conditions | Copyright © 2020 LexisNexis