Cyber Security Update

Presented to WA Electricity Consultative Forum

By Tim Daly, GM, Cyber Security

4 May 2022

Agenda

- Recent cyber incidents affecting energy market participants in the Australia
- Urgently adopting an enhanced cyber security posture
- Security of Critical Infrastructure Act Reforms (SLACI and SLACIP)
- Australian Energy Sector Cyber Incident Response Plan
- GridEx VI

Recent cyber incidents affecting participants in the NEM

SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe | 2022 CISO Forum | ICS Cyber Security Conference | Contact

Malware & Threats | Cybercrime | Mobile & Wireless | Risk & Compliance | Security Architecture | Security Strategy | ICS/OT | IoT Security

Home › Cybercrime

Ransomware Operators Leak Data Stolen From Wind Turbine Giant Vestas

By Eduard Kovacs on December 09, 2021

Share | Tweet | Recommend 0 | RSS

Cybercriminals have made public the data stolen recently from Danish wind turbine giant Vestas Wind Systems, and the company confirmed the leak on Wednesday.

Vestas became aware of the breach on November 19 and it immediately started shutting down IT systems. The company confirmed in late November that it had been hit by ransomware and that the breach resulted in internal files getting compromised.

The firm said the incident did not impact wind turbine operations and nearly all systems had been restored by late November.

Google™ Custom Search | Search

GET THE DAILY BRIEFING

BRIEFING

Business Email Address | SUBSCRIBE

itnews

NEWS | GOVERNMENT | SECURITY | RESOURCES | PODCAST | STATE OF IT | DIGITAL NATION | BENCHMARK AWARDS | LOG IN | SUBSCRIBE

CS Energy ransomware attack claimed by Russian-speaking criminals

By Joseph Menn
Dec 9 2021
11:44AM

1 Comment

Conti group names utility on its website.

One of the most prolific Russian-speaking ransomware gangs has claimed credit for a late November attack on Australian electricity utility CS Energy. The claim was made after multiple media reports attributed the breach at CS Energy, which is owned by the Queensland state in northeast Australia,...

Urgently adopting an enhanced cyber security posture

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Home / News, threats and hazards / Archive

CISC News

Contains news and media resources, speeches, links to social media and subscription services.

17 MAR 2022

UPDATE: 16 March 2022 – Version 9 of ACSCs Technical Advisory: Australian organisations should urgently adopt an enhanced cyber security posture.

Related articles

15 MAR 2022
Cyber Security Incident Reporting

10 MAR 2022
UPDATE: 09 March 2022 - Technical Advisory: Australian organisations should urgently adopt an enhanced cyber security posture

07 MAR 2022
Cyber and Infrastructure

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Report

Search

Contact us Portal login

Individuals & families | Small & medium businesses | Organisations & Critical Infrastructure | Government | Learn

Australian organisations encouraged to urgently adopt an enhanced cyber security posture

Home > About the ACSC > View all content > View all alerts > Australian organisations encouraged to urgently adopt an enhanced cyber security posture

Australian organisations are encouraged to urgently adopt an enhanced cyber security position. Organisations should act now and follow ACSC's advice to improve their cyber security resilience in light of the heightened threat environment.

Alert status: HIGH

Background / What has happened?

There has been a historical pattern of cyber attacks against Ukraine that have had international consequences. Malicious cyber activity could impact Australian organisations through unintended disruption or uncontained malicious cyber activities.

While the ACSC is not aware of any current or specific threats to Australian organisations, adopting an enhanced cyber security posture and increased monitoring for threats will help to reduce the impacts to Australian organisations.

Mitigation / How do I stay secure?

Content written for

- Individuals & families
- Small & medium businesses
- Organisations & critical infrastructure
- Government

View all content

First published: 23 Feb 2022
Last updated: 23 Feb 2022

Security of Critical Infrastructure Act Reforms SLACI (aka Bill 1 – now law) and SLACIP (Bill2 - before parliament)

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Bill One – Security Legislation Amendment (Critical Infrastructure) Act 2021

- The Security Legislation Amendment (Critical Infrastructure) Act 2021 commenced in December
- The Department has concluded consultation with industry on the proposed 'turning on' of Positive Security Obligations
  - Register of Critical Infrastructure Assets
  - Notification of Cyber Security Incidents
- The Minister may seek to make the Rules

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

OFFICIAL

Risk Management Program Rules

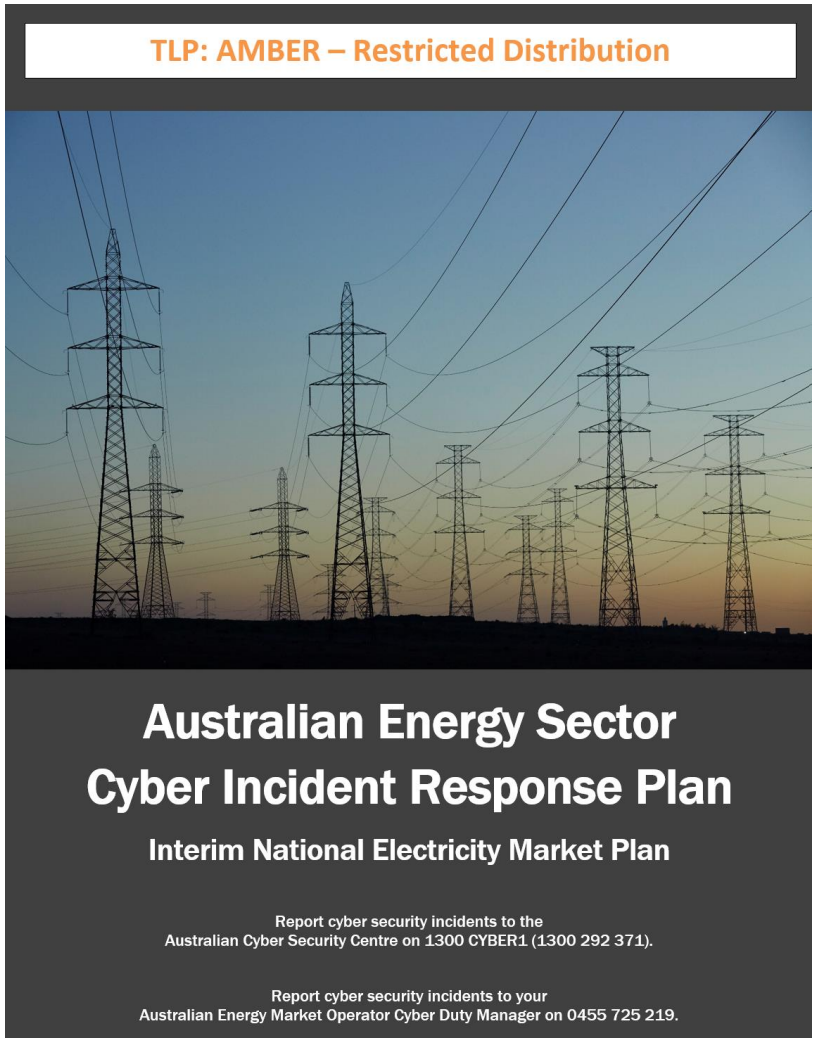
26 November 2021

Contents

Context Statement 2
Data Hosting Certification 5
Definition of Material Risk 6
Rule 1 – Cyber and information security hazards 7
Rule 2 – Personnel hazards 8
Rule 3 –Supply chain hazards 9
Rule 4 – Physical and natural hazards 10
Attachment A – AusCheck explanatory information 11

DRAFT

Australian Energy Sector Cyber Incident Response Plan



Date	Milestone	Summary
March 18 2022	Launch of Stage 1 Interim NEM Version (Version 1.0) Issued for Review and Comment	Target stakeholders: • NEMEMF Members • NEM TNSP CISOs • ACSC • Jurisdictional Cyber Agencies
	Interim NEM Version (Version 1.0) issued to NEMEMF for Endorsement	Revised AESCIRP Version 1.1 will be issued for endorsement through NEMEMF
April 1 2022	Interim NEM Version (Version 1.0) published	Document will be approved by AEMO CISO and issued to stage 1 stakeholders as TLP AMBER.
	Rewrite for Stage 2 of implementation.	The document will be reviewed internally by AEMO in preparation for Stage 2
April 14 2022	Launch of Stage 2 Extension to Generators, DNSPs and Gentailers in the NEM. Version 1.1 issued for review and comment	Target Stakeholders: • NEM DNSP CISOs and Emergency Teams • Generator CISOs and Emergency Teams • Gentailer CISOs and Emergency Teams
	Rewrite for Stage 3 implementation	Revised AESCIRP Version 1.2 will be issued for endorsement through NEMEMF
From June (Dependent on feedback to-date)	Launch of Stage 3 Extension into WA and NT	Target Stakeholders • AEMO (SWIS) • NWIS (Horizon) • NT Power & Water
	Rewrite for Stage 4 implementation	Revised AESCIRP Version 1.3 will be issued for endorsement through NEMEMF and the other relevant jurisdictional fora

Australian Government
Department of Industry, Science, Energy and Resources

GridEx VI

gridex.com.au

AEMO

About the exercise

TLP AMBER

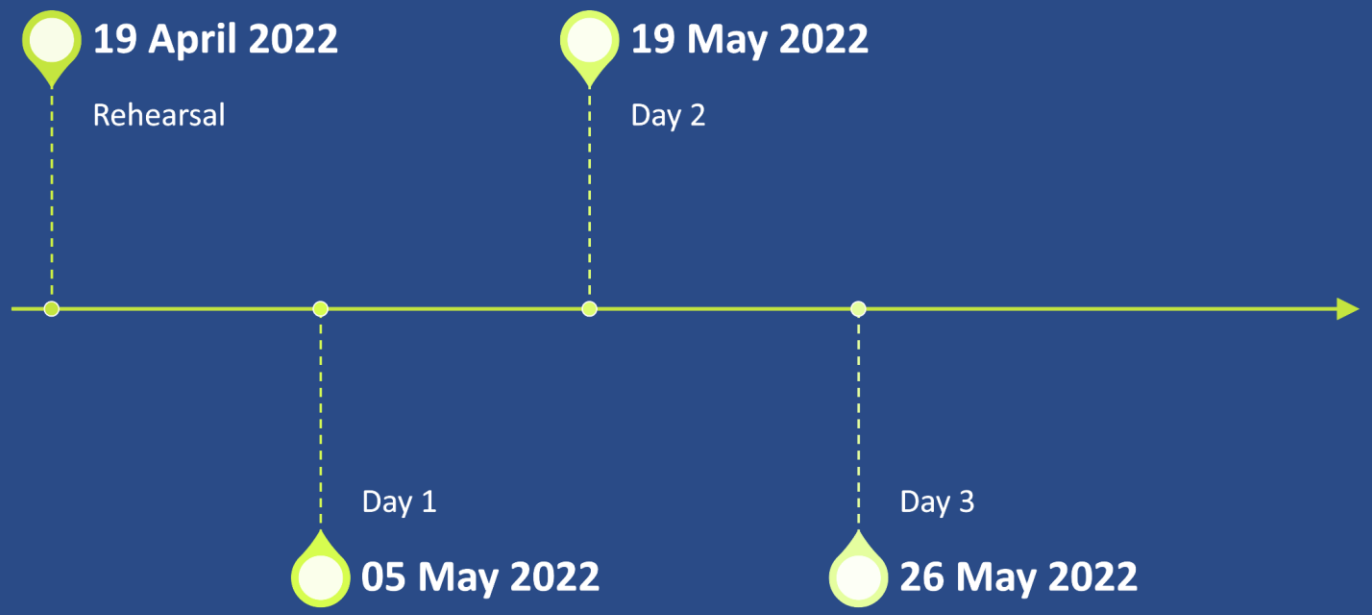
- Department of Industry, Science, Energy and Resources (DISER)
- National energy sector cyber exercise - 3 days in May 22
- NOT linked to US GridEx VI in 2021
- Build familiarity across collaborative response partners
- Functionally test and practice response, coordination, & communications arrangements

One rehearsal and three exercise days

TLP AMBER

One rehearsal and three exercise days

TLP AMBER



Questions and feedback