22 Ogos 2024
22 August 2024
P.U. (A) 220

WARTA KERAJAAN PERSEKUTUAN

FEDERAL GOVERNMENT GAZETTE

PERATURAN-PERATURAN KESELAMATAN SIBER (PEMBERITAHUAN INSIDEN KESELAMATAN SIBER) 2024

CYBER SECURITY (NOTIFICATION OF CYBER SECURITY INCIDENT) REGULATIONS 2024

DISIARKAN OLEH/
PUBLISHED BY
JABATAN PEGUAM NEGARA/
ATTORNEY GENERAL'S CHAMBERS

AKTA KESELAMATAN SIBER 2024

PERATURAN-PERATURAN KESELAMATAN SIBER (PEMBERITAHUAN INSIDEN KESELAMATAN SIBER) 2024

PADA menjalankan kuasa yang diberikan oleh seksyen 63 Akta Keselamatan Siber 2024 [*Akta 854*], Menteri membuat peraturan-peraturan yang berikut:

Nama dan permulaan kuat kuasa

1. (1) Peraturan-peraturan ini bolehlah dinamakan **Peraturan-Peraturan Keselamatan Siber (Pemberitahuan Insiden Keselamatan Siber) 2024**.

(2) Peraturan-Peraturan ini mula berkuat kuasa pada 26 Ogos 2024.

Tempoh pemberitahuan dan butiran maklumat

2. (1) Orang yang diberi kuasa bagi entiti infrastruktur maklumat kritikal negara hendaklah memberitahu dengan segera, melalui cara elektronik, mengenai suatu insiden keselamatan siber yang telah atau mungkin telah berlaku sebagaimana yang diperuntukkan di bawah seksyen 23 Akta apabila insiden keselamatan siber itu diketahui oleh entiti infrastruktur maklumat kritikal negara.

(2) Dalam masa enam jam daripada insiden keselamatan siber itu diketahui oleh entiti infrastruktur maklumat kritikal negara, orang yang diberi kuasa hendaklah mengemukakan butiran maklumat seperti yang berikut:

(a) butiran orang yang diberi kuasa;

(b) butiran entiti infrastruktur maklumat kritikal negara yang terlibat, sektor infrastruktur maklumat kritikal negara dan ketua sektor infrastruktur maklumat kritikal negara yang berkaitan dengannya; dan

(c) maklumat mengenai insiden keselamatan siber termasuk—

(i) jenis dan perihal insiden keselamatan siber;

(ii) keseriusan insiden keselamatan siber;

(iii) tarikh dan masa insiden kejadian keselamatan siber disedari; dan

(iv) kaedah penemuan insiden keselamatan siber.

(3) Dalam masa empat belas hari selepas pemberitahuan yang disebut dalam subperaturan (1), orang yang diberi kuasa hendaklah mengemukakan setakat yang boleh maklumat tambahan seperti yang berikut:

(a) butiran infrastruktur maklumat kritikal negara yang tejejas oleh insiden keselamatan siber itu;

(b) bilangan hos yang dijangka terjejas dengan insiden keselamatan siber itu;

(c) butiran pelaku ancaman keselamatan siber;

(d) artifak yang berkenaan dengan insiden keselamatan siber;

(e) maklumat mengenai apa-apa insiden yang berhubungan dengan, dan cara insiden itu yang berkaitan dengan, insiden keselamatan siber itu;

(f) butiran taktik, teknik dan tatacara insiden keselamatan siber itu;

(g) kesan insiden keselamatan siber terhadap infrastruktur maklumat kritikal negara atau mana-mana komputer atau sistem komputer yang saling bersambung; dan

(h) tindakan yang telah diambil.

(4) Orang yang diberi kuasa oleh entiti infrastruktur maklumat kritikal negara hendaklah menyediakan, dari semasa ke semasa, kemas kini lanjut mengenai insiden keselamatan siber sebagaimana yang dikehendaki oleh Ketua Eksekutif.

Cara pengemukaan maklumat

3. Pengemukaan maklumat di bawah subperaturan 2(2) dan (3) hendaklah dibuat melalui Sistem Pusat Penyelarasan dan Kawalan Siber Negara atau sekiranya berlaku gangguan pada Sistem Pusat Penyelarasan dan Kawalan Siber Negara, dengan komunikasi sebagaimana yang ditentukan oleh Ketua Eksekutif.

Dibuat 19 Ogos 2024
[MKN(S).10.600-9/2/4 Jld.9(5); PN(PU2)768]

DATO' SERI ANWAR BIN IBRAHIM
Perdana Menteri

CYBER SECURITY ACT 2024

CYBER SECURITY (NOTIFICATION OF CYBER SECURITY INCIDENT) REGULATIONS 2024

IN exercise of the powers conferred by section 63 of the Cyber Security Act 2024 [*Act 854*], the Minister makes the following regulations:

Citation and commencement

1. (1) These regulations may be cited as the **Cyber Security (Notification of Cyber Security Incident) Regulations 2024**.

(2) These Regulations come into operation on 26 August 2024.

Period of notification and particulars of information

2. (1) An authorized person of a national critical information infrastructure entity shall immediately, by electronic means, give a notification of a cyber security incident that has or might have occurred as provided under section 23 of the Act when the cyber security incident comes to the knowledge of the national critical information infrastructure entity.

(2) Within six hours from the time the cyber security incident comes to the knowledge of the national critical information infrastructure entity, the authorized person shall submit the following particulars of information:

(a) the particulars of the authorized person;

(b) the particulars of the national critical information infrastructure entity concerned, the national critical information infrastructure sector and national critical information infrastructure sector lead to which it relates; and

(c) the information on the cyber security incident including—

(i) the type and description of the cyber security incident;

(ii) the severity of the cyber security incident;

(iii) the date and time of the occurence of the cyber security incident is known; and

(iv) the method of discovery of the cyber security incident.

(3) Within fourteen days after the notification referred to in subregulation (1), the authorized person shall provide to the fullest extent practicable the following supplementary information:

(a) the particulars of the national critical information infrastructure affected by the cyber security incident;

(b) the estimated number of host affected by the cyber security incident;

(c) the particulars of the cyber security threat actor;

(d) the artifacts related to the cyber security incident;

(e) the information on any incident relating to, and the manner in which such incident relates to, the cyber security incident;

(f) the particulars of the tactics, techniques and procedures of the cyber security incident;

(g) the impact of the cyber security incident on the national critical information infrastructure or any computer or interconnected computer system; and

(h) the action taken.

(4) The authorized person of the national critical information infrastructure entity shall provide, from time to time, further updates on the cyber security incident as the Chief Executive may require.

Manner of submission of information

3. The submission of information under subregulations 2(2) and (3) shall be made through the National Cyber Coordination and Command Centre System or in the event of disruption in the National Cyber Coordination and Command Centre System, by the communication as may be determined by the Chief Executive.

Made 19 August 2024
[MKN(S).10.600-9/2/4 Jld.9(5); PN(PU2)768]

DATO' SERI ANWAR BIN IBRAHIM
Prime Minister