GARIS PANDUAN

Pengurusan Insiden Keselamatan Siber

Versi 1.0

Universiti Sains Malaysia

Pusat Pengetahuan, Komunikasi dan Teknologi
Universiti Sains Malaysia

ppkt.usm.my

KANDUNGAN

DOKUMEN RUJUKAN:

1. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan bertarikh 1 Oktober 2000

2. Malaysian Public Sector Management of Information & Communications Technology Security Handbook (MyMIS) bertarikh 15 Jan 2002

3. Surat Arahan Ketua Pengarah MAMPU - Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam bertarikh 24 Nov 2010

4. Surat Arahan Ketua Pengarah MAMPU - Panduan Keperluan dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC27001:2007 dalam Sektor Awam bertarikh 24 Nov 2010

5. Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian Government Computer Emergency Response Team (GCERT) oleh NACSA bertarikh 28 Januari 2019

6. Surat Pemakluman Pengurusan Maklumat Pegawai Keselamatan ICT (ICTSO) Sektor Awam bertarikh 28 Februari 2019

7. Surat Pemakluman Kaedah Pelaksanaan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 6 April 2022

8. Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022

9. Surat Pekeliling Am Bilangan 3 Tahun 2024 - Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024

10. Surat Pekeliling Am Bilangan 4 Tahun 2024 - Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam bertarikh 21 Mac 2024

11. Standard ISO/IEC 27001:2022 information security, cybersecurity and privacy protection, information security management systems requirement

TUJUAN

Garis panduan ini bertujuan menjelaskan tatacara pengurusan dan pengendalian insiden keselamatan siber bagi Universiti Sains Malaysia (USM) seperti yang berikut:

i. Mengenal pasti tahap keutamaan tindakan terhadap insiden keselamatan siber supaya satu pendekatan yang seragam dan proaktif dapat dilaksanakan secara berkesan.

ii. Menetapkan penubuhan, fungsi, tanggungjawab, dan struktur Pasukan Tindak Balas lnsiden Keselamatan Siber *[(Cyber Security Incident Response Team,* (CSIRT)] USM.

iii. Menggariskan bidang tugas dan tanggungjawab ICTSO, CSIRT USM dan Pusat Penyelarasan dan Kawalan Siber Negara *[National Cyber Coordination and Command Centre,* (NC4)] dalam pengurusan dan pengendalian insiden keselamatan siber bagi sektor awam.

iv. Menerangkan proses kerja pelaporan insiden dan Prosedur Operasi Standard [(*Standard Operating Procedure,* (SOP)] pengendalian insiden.

TAFSIRAN

Bagi tujuan garis panduan ini, terma di bawah ditafsirkan seperti yang berikut:

i. **"Ancaman siber"** ialah ancaman yang berpunca daripada Internet atau rangkaian menggunakan laluan komunikasi data yang memberi kesan terhadap kerahsiaan, integriti dan ketersediaan sistem maklumat dari dalam sesebuah organisasi mahupun dari jarak jauh, serta penyebaran maklumat melalui medium siber yang bertentangan dengan undang-undang negara dan berupaya menggugat keselamatan negara.

ii. **“CSIRT USM”** ialah pasukan tindak balas insiden keselamatan siber yang merangkumi kesemua kampus USM.

iii. **“Infrastruktur Maklumat Kritikal Negara” (Critical National Information Infrastructure, CNII)** merujuk kepada sistem kritikal yang merangkumi aset maklumat (elektronik), rangkaian, fungsi, proses, kemudahan, dan perkhidmatan dalam persekitaran teknologi maklumat dan komunikasi (Information and Communications Technology, ICT) yang penting kepada negara di mana sebarang gangguan atau kemusnahan ke atasnya boleh memberi impak kepada pertahanan dan keselamatan negara, kestabilan ekonomi negara, imej negara, keupayaan Kerajaan untuk berfungsi, kesihatan, dan keselamatan awam serta privasi individu.

iv. **"Insiden keselamatan siber"** ialah kejadian siber yang tidak diingini apabila berlakunya kehilangan kerahsiaan maklumat, gangguan terhadap integriti data atau sistem, atau gangguan yang menyebabkan kegagalan dalam memperoleh maklumat daripada sistem komputer dan kemungkinan berlakunya kesalahan pelanggaran peraturan keselamatan maklumat, dasar-dasar tertentu atau amalan piawai keselamatan siber.

v. **"Krisis Siber Negara"** ialah suatu keadaan di mana insiden keselamatan siber melebihi tahap yang ditetapkan sehingga menjejaskan kerahsiaan, integriti, dan ketersediaan agensi sektor awam terutamanya agensi **CNII** dan memberi impak terhadap pertahanan dan keselamatan negara, kestabilan ekonomi negara, imej negara, keupayaan Kerajaan untuk berfungsi, kesihatan dan keselamatan awam serta privasi individu.

vi. **"Prosedur Tindak Balas, Komunikasi dan Penyelarasan Pengurusan Krisis Siber Negara"** ialah proses pengurusan insiden dan langkah-langkah yang perlu diambil oleh pihak yang berkaitan dalam Pengurusan Krisis Siber Negara.

vii. **"Pengurusan Krisis Siber Negara"** ialah satu pendekatan sistematik bagi pencegahan, persediaan, tindak balas, dan pemulihan daripada insiden keselamatan siber terhadap CNII.

JENIS-JENIS INSIDEN KESELAMATAN SIBER

Jenis-jenis insiden keselamatan siber adalah seperti yang berikut:

i. **Penafian Perkhidmatan *(Denial of Service,* DoS) atau Penafian Perkhidmatan Teragih *(Distributed Denial of Service,* DDoS).** Serangan DoS atau DDoS merupakan serangan terhadap sistem atau rangkaian komputer yang menyebabkan ketidakupayaan sistem atau rangkaian tersebut untuk memberikan perkhidmatan kepada pengguna.

ii. **Pencerobohan *(Intrusion).*** Pencerobohan merujuk kepada capaian tanpa kebenaran/tidak sah yang berjaya menembusi sistem atau rangkaian. lnsiden ini boleh mengakibatkan akaun pentadbir sistem diambil alih, laman web diceroboh, kerosakan pada sistem, data atau konfigurasi sistem dipinda dan/atau pemasangan kod hasad seperti *backdoor* atau *trojan.*

iii. **Jangkitan Perisian Hasad *(Malicious Software, Malware).*** Perisian hasad adalah perisian yang direka untuk memasuki sistem komputer tanpa kebenaran dan berpotensi membahayakan mesin atau rangkaian.

iv. **Pengehosan Perisian Hasad *(Malware Hosting)*** Pengehosan perisian hasad merujuk kepada keadaan di mana perisian hasad berada di dalam pelayan atau komputer pengguna secara tidak sah; seterusnya dijadikan sebagai sumber untuk dimuat turun atau diakses oleh siri serangan perisian hasad yang lain.

v. **Parcubaan Pencerobohan *(Intrusion Attempt)*** Percubaan dengan hasrat untuk menceroboh atau mengambil alih sistem secara tidak sah melalui aktiviti imbasan *port* rangkaian, akses sistem secara *brute force* atau mengenal pasti kerentanan sistem.

vi. **Potensi Serangan *(Potential Attack).*** Potensi serangan adalah ancaman yang berkemungkinan berlaku akibat daripada kerentanan yang terdapat pada sistem/rangkaian atau kelemahan pada proses kerja sesebuah agensi. Serangan ini boleh memusnah, mendedah, meminda, melumpuh, mencuri atau mendapatkan akses yang tidak sah bagi tujuan menggunakan aset yang tidak dibenarkan. Serangan ini dikenal pasti berdasarkan maklumat risikan atau hasil pemantauan terhadap agensi.

TAHAP KEUTAMAAN TINDAKAN TERHADAP INSIDEN KESELAMATAN SIBER

Tindakan terhadap insiden keselamatan siber yang berlaku hendaklah dibuat berasaskan kepada keseriusan sesuatu insiden. Tahap keutamaan tindakan terhadap insiden keselamatan siber akan ditentukan seperti yang berikut:

i. **Keutamaan 1** - insiden keselamatan siber yang memberi impak tinggi terhadap pertahanan dan keselamatan negara, kestabilan ekonomi negara, imej negara, keupayaan Kerajaan untuk berfungsi, kesihatan dan keselamatan awam serta privasi individu.

ii. **Keutamaan 2** - insiden keselamatan siber yang tidak memberi impak seperti mana yang dinyatakan dalam Keutamaan 1.

1.1 Sekiranya berstatus Keutamaan 1, USM hendaklah melaporkan insiden kepada NC4 bagi tujuan penyelarasan dan memaklumkan kepada Kementerian Pendidikan Tinggi (KPT) dalam tempoh 24 jam selepas insiden dikesan serta mengaktifkan Pelan Kesinambungan Perkhidmatan (Business Continuity Plan, BCP) dan Pelan Pemulihan Bencana (Disaster Recovery Plan, DRP) sekiranya perlu.

Bagi Keutamaan 2, USM hendaklah melaksanakan pengendalian insiden secara kendiri dan seterusnya memaklumkan kepada NC4 dan KPT setelah proses pengendalian insiden dan pemulihan pada peringkat USM selesai.

PENUBUHAN CSIRT USM

Sebagai langkah mengukuhkan pengurusan dan pengendalian keselamatan siber USM serta memastikan insiden ditangani dengan berkesan, USM:

i. Menubuhkan CSIRT bagi menangani insiden keselamatan siber. CSIRT USM bertindak sebagai *first level support* kepada NC4 dalam mengendali insiden keselamatan siber, mengawasi dan memberi khidmat nasihat berkaitan keselamatan siber kepada PTJ USM.

ii. bertanggungjawab melaporkan insiden keselamatan siber kepada Ketua Pegawai Digital (Chief Digital Officer, CDO).

TANGGUNGJAWAB CSIRT USM

Tanggungjawab CSIRT USM meliputi semua bidang tugas pengurusan dan pengendalian insiden keselamatan siber seperti yang berikut:

i. Memantau, mengesan insiden, menerima, dan mengesahkan aduan insiden keselamatan siber, seterusnya mengenal pasti jenis insiden serta menilai impak insiden keselamatan siber.

ii. Merekod dan menjalankan siasatan awal terhadap insiden yang diterima.

iii. Melaksanakan pengurusan dan pengendalian insiden keselamatan siber serta mengambil tindakan awal pemulihan.

iv. Menjalankan penilaian untuk memastikan tahap keselamatan siber dan mengambil tindakan pemulihan serta pengukuhan keselamatan siber supaya insiden baharu dapat dielakkan.

v. Melaporkan insiden keselamatan siber kepada KPT dan NC4.

vi. Menasihat semua PTJ mengambil tindakan pemulihan dan pengukuhan.

vii. Menyebarkan makluman/amaran berkaitan insiden kepada semua PTJ USM.

viii. Memastikan fail log disimpan sekurang-kurangnya enam bulan di tempat yang selamat.

Apabila berlakunya insiden keselamatan siber, ICTSO USM hendaklah menggerakkan ahli CSIRT USM untuk mengambil tindakan seperti yang berikut:

i. Mengurus dan mengambil tindakan terhadap insiden yang berlaku sehingga keadaan pulih.

ii. Mengaktifkan BCP dan/atau DRP jika perlu.

iii. Melapor dan memaklumkan insiden keselamatan siber kepada NC4 serta KPT.

iv. Menentukan sama ada insiden ini perlu dilaporkan kepada agensi penguatkuasaan undang-undang.

MEKANISME PELAPORAN INSIDEN

Carta Aliran Proses Kerja Pelaporan lnsiden Keselamatan Siber CSIRT USM dijelaskan dalam **Lampiran A.**