Prosedur Pengendalian Standard

Pembekuan dan Pengaktifan Akaun Identiti Yang Digodam

Versi: 2.0

Disediakan Oleh:

Khairil Anwar Jusoh
Unit Keselamatan ICT
Pusat Pengetahuan, Komunikasi & Teknologi
Universiti Sains Malaysia

Sejarah Perubahan Dokumen

Tarikh	Versi	Editor	Status
14 Februari 2018	2.0	Khairil Anwar Jusoh	Kelulusan JKPO
19 November 2017	1.2	Khairil Anwar Jusoh	
12 Oktober 2015	1.1	Khairil Anwar Jusoh	
19 November 2012	1.0	Mashithah bt Md Hasim	

1.0 Tujuan dan Skop

Dokumen ini bertujuan menjelaskan tatacara tindakan yang akan dilaksanakan ke atas akaun identiti USM yang didapati digodam oleh pihak luar. Akaun identiti USM ini dibekalkan kepada semua kakitangan USM untuk urusan rasmi.

Kesan godaman akaun identiti akan menyebabkan kebanyakan emel dari Universiti Sains Malaysia tidak diterima oleh pelbagai pihak termasuk Yahoo, AOL, Comcast dan beberapa organisasi-organisasi yang lain. Emel USM juga akan disenaraihitamkan pada peringkat antarabangsa oleh SORBS-SPAM. Ini menyebabkan emel-emel dari pengguna lain dilengahkan (delayed) atau luput tanpa dapat dihantar kepada penerima.

Justeru itu, satu tindakan perlaksaanaan yang tegas perlu diambil untuk memastikan akaun identiti yang digodam dibekukan secepat mungkin bagi mengelakkan penghantaran emel spam secara pukal berleluasa dalam masa yang singkat. Pengguna yang mendedahkan maklumat akaun kepada pihak luar yang menyebabkan akaun emel mereka digodam juga harus diberikan penalti untuk memastikan mereka sedar betapa kritikalnya kesan kecuaian mereka kepada Universiti Sains Malaysia.

Bil.	Proses Kerja	Pegawai Pelaksana
1.	Medium penerimaan dan pengesanan akaun yang digodam: 1. Terima emel amaran dari pihak Microsoft berkaitan akaun emel yang sedang menghantar emel spam 2. Pemantuan corak emel pada peranti anti spam 2. Pengguna mengadu berkenaan akaun mereka 3. Pengguna lain membuat aduan penerimaan spam dari akaun dalaman	Unit Keselamatan ICT
2.	Semak akaun emel dan corak emel untuk pengesahan sama ada akaun telah digodam	Unit Keselamatan ICT

3.	Bekukan, tagkan dengan tanda ACCOUNT HACKED dan tukar kata laluan akaun yang digodam tersebut pada Active Directory dan maklumkan melalui emel kepada: 1. ServisDesk (servisdesk@usm.my) 2. Pengarah PPKT, 3. Penolong Pendaftar PPKT 4. Timbalan Pengarah Info PPKT, 5. Ketua UEPD 6. Ketua Seksyen Komunikasi Bersepadu 7. Ketua Seksyen Pengurusan Aset & Sokongan Teknikal 8. Ketua Unit Sokongan Teknikal 9. Bagi akaun di kampus selain Kampus Induk, makluman akan dikeluarkan kepada Penyelaras, Setiausaha PPKT dan Servisdesk PPKT Kampus cawagan.	Unit Keselamatan ICT
4.	Hapuskan emel pada senarai belum hantar (Queue) pada pelayan Exchange.	UEPD
5.	Maklumkan melalui emel kepada pemilik akaun melalui: 1. Ketua Jabatan pemilik akaun 2. Setiausaha Jabatan pemilik akaun 3. Penolong Pendaftar Jabatan pemilik akaun 4. *Cadangan SMS kepada pemilik akaun Kandungan emel perlu menyatakan akaun identiti pemilik akaun telah digodam dan halangan dari mencapai perkhidmatan yang menggunakan “Single Sign On” dan meminta pemilik akaun menyediakan Surat Tunjuk Sebab melalui Ketua Jabatan pemilik akaun dan menyerahkannya kepada ke Pejabat Pengarah PPKT) *Cadangan untuk nyatakan senarai perkhidmatan.	Pejabat Pengarah (staf yang membuat emel hebahan)
6.	Pemakluman lanjutan kes-kes khas: 1. Sekiranya kes berulang, salinan pemberitahuan kepada Naib Canselor 2. Sekiranya akaun identiti Ketua Jabatan yang digodam, makluman kepada Naib Canselor	Pej. Pengarah (staf yang membuat emel hebahan)

7.	Akaun diaktifkan dan katalaluan ditetapkan semula dalam masa 24 jam setelah menerima Surat Tunjuk Sebab daripada pemilik akaun dengan kelulusan oleh Pengarah PPKT: Maklumkan sama kepada senarai di bawah: 1. ServisDesk (servisdesk@usm.my) 2. Pengarah PPKT, 3. Penolong Pendaftar PPKT 4. Timbalan Pengarah Info PPKT, 5. Ketua UEPD 6. Ketua Seksyen Komunikasi Bersepadu 7. Ketua Seksyen Pengurusan Aset & Sokongan Teknikal 8. Ketua Unit Sokongan Teknikal 9. Bagi akaun di kampus selain Kampus Induk, makluman akan dikeluarkan kepada Penyelaras, Setiausaha PPKT dan Servisdesk PPKT Kampus cawagan.	Unit Keselamatan ICT
8.	Makluman kepada pemilik akaun melalui medium telefon/emel alternatif berkaitan akaun telah diaktifkan semula beserta langkah-langkah yang perlu diambil: 1. Pemilik akaun perlu menukar kata laluan melalui portal https://self.usm.my	Unit Keselamatan ICT