RnD10-1326

KESEDARAN TEKNIK KEJURUTERAAN SOSIAL DI NUKLEAR MALAYSIA

Mohd Dzul Aiman bin Aslan*, Mohamad Safuan bin Sulaiman, Dr Abdul Muin bin Abdul Rahman
Malaysian Nuclear Agency
Bangi, 43000 Kajang, Selangor Darul Ehsan, Malaysia
***e-mail: dzulaiman@nuclearmalaysia.gov.my**

MY1204139

Abstract:

Kejuruteraan sosial atau 'social engineering' ialah salah satu seni untuk memanipulasikan seseorang untuk melakukan sesuatu dan mendedahkan maklumat rahsia, bukan dengan memecah masuk menggunakan teknik tertentu secara teknikal, dan ia lebih kepada perilakuhelah.[1] Ia juga adalah salah satu teknik godam yang dikategorikan sebagai godaman manusia (people hacking)[2]. Kertas kerja ini akan membincangkan bagaimana kejuruteraan sosial dilakukan untuk memperoleh maklumat iaitu nama dan katalaluan bagi pekerja di Nuklear Malaysia menggunakan medium email. Ia bertujuan bagi menguji tahap kesedaran pekerja berkenaan kejuruteraan sosial disamping mengkaji bagaimana prosedur kebiasaan daripada kumpulan pekerja yang berbeza semasa insiden serangan siber tersebut. Terdapat beberapa warga yang terkena dengan serangan tersebut dan satu perkara yang tidak dijangka berlaku membolehkan lebih banyak maklumat tambahan berjaya diperoleh.

Keyword: security, social engineering, hacking, phishing, email, laman web

PENDAHULUAN

Kejuruteraan sosial atau lebih dikenali dengan Social Engineering ialah satu seni memanipulasikan seseorang untuk memperoleh maklumat rahsia demi mencapai sesuatu objektif. Ia termasuk dalam beberapa kaedah hacking, namun ia tidak menggunakan teknik-teknik seperti cracking, dan sebagainya. Kejuruteraan sosial ini lebih kepada sesuatu yang berunsur helah yang membolehkan sesuatu maklumat itu diperoleh secara lembut dan tidak terlalu ekstrim[1].

Terdapat pelbagai kaedah dan teknik-teknik dalam kejuruteraan sosial, antaranya ialah; phishing, dumpster diving, impersonation, dan lain-lain lagi[7] . Tiga kaedah dipilih dalam ujian tersebut iaitu email, phishing dan impersonation. Email bermaksud ia adalah medium untuk berkomunikasi dengan mangsa tanpa berdepan dalam mengumpul maklumat. Phishing pula bermaksud satu laman web yang dicipta sama seperti laman web yang sebenar yang bertujuan untuk menipu mangsa dalam mendedahkan katanama dan katalaluan yang digunakan. Impersonation bermaksud teknik tersebut seolah-olah menyamar sebagai seseorang yang mempunyai authority bagi mendapatkan kepercayaan mangsa.

Objektif kejuruteraan sosial ini merangkumi pengukuran tahap kesedaran bagi warga Nuklear Malaysia berkenaan serangan kejuruteraan sosial dan juga untuk mengkaji semula prosedur standard daripada kumpulan yang berbeza semasa insiden serangan kejuruteraan sosial tersebut. Impak kepada warga Nuklear Malaysia ialah kesedaran mengenai teknik tersebut dan cara mengatasinya disamping SOP yang akan diperkemaskan lagi.

METHODOLOGI

Situasi berikut dipenuhi semasa menjalankan ujian tersebut. Objektif penggodam ialah memperoleh maklumat berkenaan rahsia Nuklear Malaysia (NM) seperti apa-apa tender berkaitan NM, apa-apa peluang pekerjaan, dan juga apa-apa maklumat rahsia kerajaan berkenaan nuklear. Oleh sebab itu, beberapa cara telah didraf dan cuma satu cara difikirkan efektif; menyamar dan memperoleh 'credential' iaitu katanama dan katalaluan staf NM melalui email. Email merupakan médium komunikasi penting dalam segala hal pada masa kini. Ia adalah cubaan yang dipertimbangkan sebagai berbaloi.

Dengan anggapan penggodam tahu berkenaan klien email Nuklear Malaysia daripada cakap mulut staf-staf seperti rakan serumah, bekas rakan sepejabat, bekas rakan sekolah dan sebagainya., serangan dilakukan daripada luar Nuklear Malaysia.

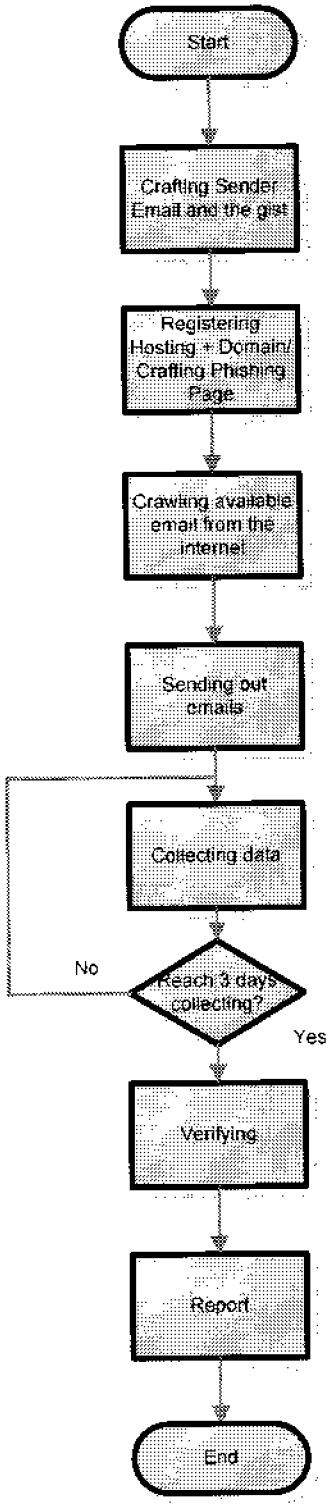
Methodology si penggodam sebelum melakukan phishing ialah melakukan beberapa persiapan seperti email dan laman web phishing[6]. Phishing ialah tindakan yang dilakukan dengan menghantar email yang palsu kepada penerima, dan email tersebut mimic seseorang yang sebenar dalam usaha menipu pengguna tersebut mendedahkan maklumat rahsia. Untuk email, penggodam mendaftar satu email palsu daripada servis email percuma seperti Google. Email palsu tersebut mestilah email yang menunjukkan identiti sebagai seseorang yang sah; maka email admin-request@gmail.com telah dipilih. Walau bagaimanapun, Gmail mempunyai konfigurasi keselamatannya tersendiri, maka email tersebut tidak dapat didaftarkan. Namun begitu, si penggodam masih boleh menwujudkan email tersebut dengan menyamar sebagai admin-request@gmail.com menggunakan teknik relay email, dan ia dilakukan menggunakan port email terbuka iaitu SMTP.com.

Selepas itu, kandungan email phishing dikarang supaya memberikan kebolehan mempengaruhi pembaca mempercayai kandungan email. Tujuannya adalah sebagai medium menarik mangsa ke laman web palsu yang direka khas seakan-akan laman web sebenar. Maka di dalam email tersebut disertakan capaian ke laman web itu dengan anggapan bahawa mangsa akan mempercayai kandungan email tersebut dan mengklik capaiannya.

Bagi laman web phishing pula, langkah pertama penggodam ialah mendaftar domain dan juga menggunakan hosting yang mempunyai kebolehan ASP atau PHP[5] untuk penggunaan pangkalan data seperti mysql untuk menyimpan maklumat. Dalam kes ini, penggodam mendaftar domain seakan-akan Nuclear Malaysia iaitu: **mywindowsxp.info** dan mendaftar hostingnya sendiri. Kemudian penggodam mereka satu subdomain yang seakan-akan email NM iaitu **mail.nuclearmalaysia.gov.mywindowsxp.info.** Hal ini adalah supaya mangsa yang lalai dan tidak prihatin terhadap laman web ini akan meletakkan login credential mereka tanpa syak wasangka. Di

dalam laman phishing tersebut, penggodam meletakkan laman yang sama dengan laman web untuk web-based email NM iaitu **mail.nuclearmalaysia.gov.my** .

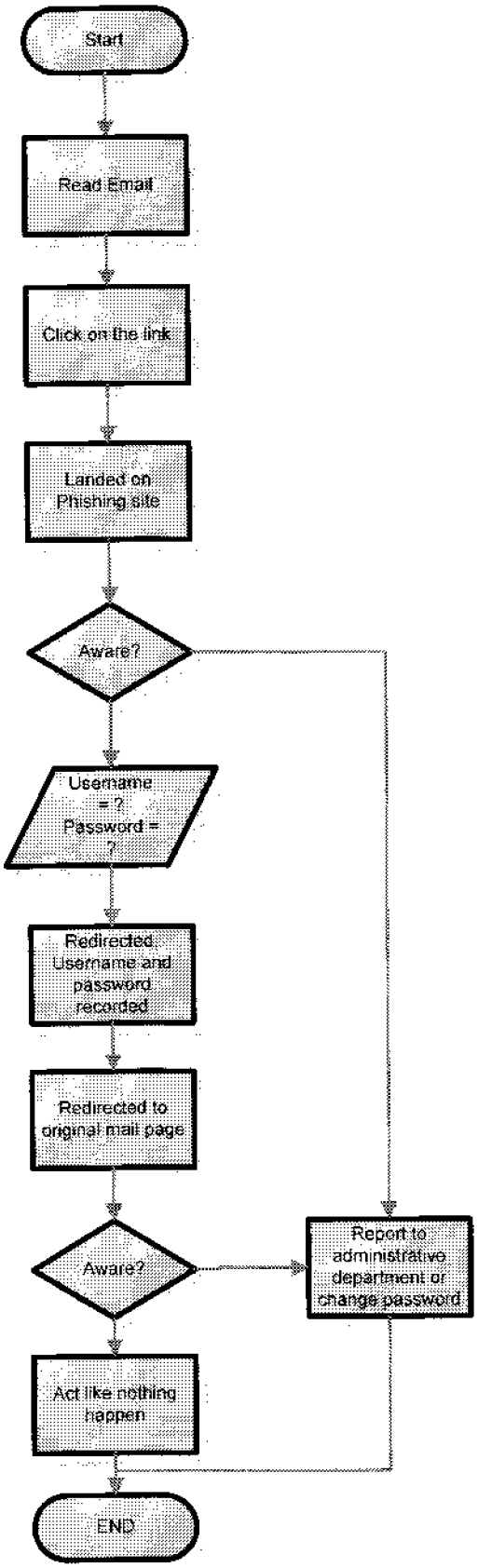
Apa yang laman phishing ini akan lakukan ialah setiap kali mangsa memasukkan katanama dan katalaluan untuk email mereka, ia akan dihantar kepada satu laman web yang akan memasukkan maklumat tersebut ke dalam pengkalan data si penggodam. Kemudian, ia akan meredirect laman tersebut kepada laman web sebenar. Hal ini adalah supaya mangsa yang tidak perasan atau keliru dengan hal tersebut akan membuka laman email seperti biasa kerana menyangkakan terdapatnya masalah email.



Rajah atas: Carta alir phishing dilakukan

Langkah seterusnya ialah menghantar email kepada mangsa. Disebabkan penggodam tidak mengetahui email-email mangsa, penggodam melakukan carian di enjin carian terkemuka, Google. Terdapat satu laman NM yang mempunyai beberapa maklumat email yang dikehendaki yang mempunyai 55 senarai email staf NM.

Sebelum menghantar email tersebut, semua proses daripada penghantaran email kepada memasuki laman web serta merekodkan data telah diuji terlebih dahulu dengan senarai email ujian oleh penggodam. Setelah berjaya, dengan menggunakan senarai email yang terdapat di dalam laman web tersebut, penggodam menghantar email yang telah dikarang tersebut kepada mangsa dan menunggu sehingga umpan mengena.



Tindakan pengguna yang difikirkan.

Keputusan Ujian

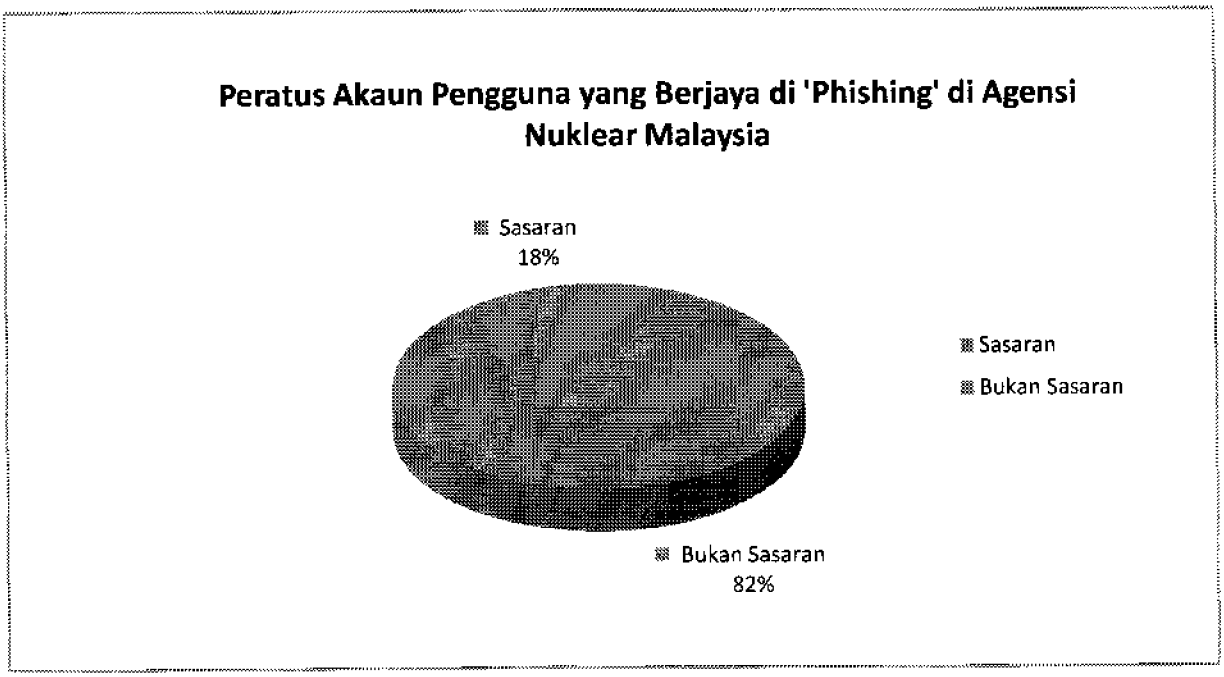
Berdasarkan jadual x.x, Dari 55 akaun pengguna yang disasarkan untuk phishing, hanya 9 akaun sahaja berjaya di 'phishing'. Walaubagaimanapun, sebanyak 41 akaun yang bukan disasarkan turut berjaya diperolehi dari serangan phishing tersebut.

Jadual x.x : Jumlah Akaun Pengguna yang Berjaya di 'Phishing' di Agensi Nuklear Malaysia

Jenis Senarai Pengguna	Jumlah
Sasaran	9
Bukan Sasaran	41
Jumlah	**50**

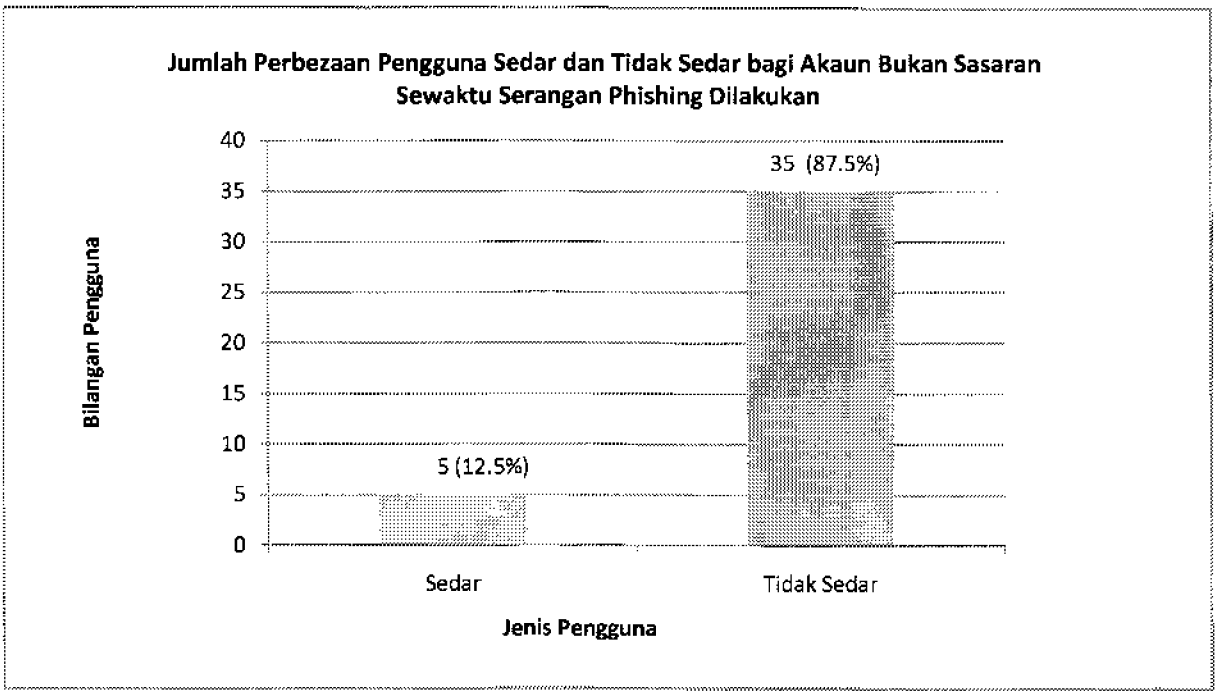
Jadual x.x menyenaraikan jumlah akaun yang berjaya di phishing berdasarkan akaun pengguna dengan memberi nama akaun pengguna (username) dan katalaluan (password). Akaun **Sasaran** adalah senarai pengguna yang disasarkan oleh penggodam (hacker) yang diperolehi dari laman web tertentu melalui enjin carian awam di Internet. Manakala akaun **Bukan Sasaran** pula adalah akaun pengguna yang bukan dalam senarai yang disasarkan penggodam tetapi memberi respon kepada email phishing yang dirancang penggodam.

Berdasarkan Graf x.x, 82% hasil dari aktiviti ini adalah bukan dari senarai akaun yang disasarkan manakala hanya 18% adalah yang disasarkan.



Graf x.x, menunjukkan akaun pengguna yang bukan sasaran memberi respon tertinggi berbanding akaun yang disasarkan. Fenomena ini sepatutnya tidak seharusnya berlaku kerana hanya akaun yang disasarkan sahaja sepatutnya menerima mesej phishing.

Daripada 82% akaun yang tidak disasarkan, didapati 5 akaun (12.5%) akaun dari pengguna yang sedar bahawa mereka sedang ditipu melalui kaedah kejuruteraan sosial iaitu phishing dengan memberi respon maklumat akaun mereka yang palsu. Sebaliknya, sebanyak 35 akaun (87.5%) memberikan maklumat sebenar akaun mereka yang boleh membantu penggodam menceroboh ke dalam sistem komputer agensi.



Graf x.x : Jumlah Akaun Pengguna yang berjaya di 'Phishing'

Merujuk kepada Graf x.x, dalam kumpulan pengguna **tidak sedar**, dijumpai satu akaun yang menyertakan domain **NTSERVER1** beserta nama akaun pengguna (username). Pendedahan domain ini juga dapat membantu penggodam untuk menjelajah jauh ke dalam sistem di agensi Nuklear.

Perbincangan

Berdasarkan keputusan ujian, tahap kesedaran tentang pentingnya mengetahui dan memahami secara asas teknik kejuruteraan sosial agak memuaskan. Hal ini adalah kerana hanya 9 (16%) daripada 56 akaun yang disasarkan berjaya diperolehi dari ujian ini. Walaubagaimanapun, fenomena 41 akaun yang tidak disasarkan iaitu bersamaan 82% dari jumlah akaun yang diperolehi dari ujian tersebut perlu dikaji dan dibincangkan dengan lebih mendalam.

Terdapat banyak kemungkinan terjadinya fenomena ini. Antara lainya, kemungkinan wujudnya virus spam yang menghantar pesanan phishing bagi pihak akaun pengguna yang disasarkan. Selain itu, terdapat juga kemungkinan mangsa ujian ini meminta rakan yang lain juga membuat seperti yang diperlukan mesej phishing tersebut.

Ada juga kemungkinan fenomena ini boleh berlaku kerana disebabkan mesej dari pentadbir sistem telah disalahertikan oleh pengguna. Buktinya, satu siasatan melalui telefon terhadap pengguna yang tidak disasarkan penggodam mendapati mesej dari pentadbir agak mengelirukan.

Jika dilihat pada graf x.x, walaupun kadar akaun pengguna yang tidak disasarkan penggodam lebih besar, namun masih terdapat dikalangan mereka iaitu sebanyak 5 akaun (12.5%) yang sedar akan serangan phishing tersebut.

KESIMPULAN

Berdasarkan kajian tersebut, dapat disimpulkan bahawa kesedaran berkenaan teknik kejuruteraan sosial masih terkawal dan perlu dipertingkatkan dari semasa ke semasa. Hal ini adalah supaya rahsia di Nuklear Malaysia dapat dilindungi daripada orang-orang yang tidak berkenaan. Selain itu juga Standard of Prosedur dan cara untuk memaklumkan kepada orang ramai jika perkara tersebut berlaku juga perlu diperhalusi supaya tidak terdapat pihak yang salah faham akan hal tersebut.

Saranan

Selepas menjalankan kajian tersebut terdapat beberapa saranan yang perlu diberi perhatian oleh semua peringkat dalam Nuklear Malaysia (NM). Yang pertama ialah seluruh warga NM mestilah sentiasa berhati-hati semasa membaca email dan sentiasa timbulkan syak sambil mengesahkan sesuatu maklumat sebelum mengambil tindakan.

Selain itu, pastikan alamat laman web yang dilawati adalah laman web yang sebenar iaitu dalam kes ini, http://mail.nuclearmalaysia.gov.my. Seterusnya, pihak admin Nuklear Malaysia mestilah berhati-hati ketika mahu memberitahu seluruh warga kerana jika link yang hidup disertakan kembali, ia akan menimbulkan kekeliruan. Warga Nuklear Malaysia yang kurang faham akan turut memasukkan katanama dan kata laluan ke dalam laman web phishing tersebut.

Jika kes ini berlaku sekali lagi, warga Nuklear Malaysia telah pun sedar dan berhati-hati. Mereka dinasihatkan supaya melaporkan kepada pihak berwajib seperti IT Administrator dan tidak memberikan credential kepada laman web tersebut.

Kajian Masa Depan

Untuk kajian masa hadapan, adalah disarankan supaya teknik phishing ini diuji semula. Hal ini adalah supaya dapat diketahui tahap keberkesan ujian ini dan kesedaran Warga Nuklear Malaysia boleh diukur. Selain itu Prosedur Standard (SOP) berkenaan laporan insiden juga boleh diperbaiki supaya lebih mantap lagi. Adalah juga disarankan supaya pelbagai lagi teknik kejuruteraan sosial diuji dalam Nuklear Malaysia supaya pensijilan ISO27001:2005 dapat dipenuhi.

RUJUKAN

[1] http://en.wikipedia.org/wiki/Social_engineering_%28security%29

[2] Social Engineering: The Art of Human Hacking

[3] Hacking For Dummies By Kevin Beaver, Stuart McClure

[4] No tech hacking: a guide to social engineering, dumpster diving, and shoulder surfing By Johnny Long, Kevin David Mitnick

[5] Phishing exposed By Lance James

[6] Cyber Security Tip ST04-014, National Cyber Alert System, http://www.us-cert.gov/cas/tips/ST04-014.html

[7] compass Security – Social Engineering Test Case, Ivan Buetler