NOTA MAKLUMAN CSIRTNS BILANGAN 1 TAHUN 2024

31 JANUARI 2024

ISU/ANCAMAN

Makluman Aktiviti Ancaman Siber yang Menyasarkan Infrastruktur Malaysia

PENGENALAN

Cyber Security Incident Response Team Negeri Sembilan (CSIRTNS) ingin memaklumkan bahawa telah menerima notifikasi ancaman daripada National Cyber Coordination and Command Centre (NC4) berhubung ancaman serangan siber ke atas infrastruktur ICT Malaysia. NC4 telah mengenal pasti "R00TK1T ISC CyberTeam" sebagai entiti penggodam yang menyasarkan infrastruktur ICT di Malaysia melalui saluran telegram mereka pada 26 Januari 2024. Walaupun tarikh dan tempoh serangan tidak dinyatakan dengan tepat, namun dipercayai penggodam tersebut adalah sebahagian daripada pasukan pembalasan terhadap kempen siber yang berpunca daripada konflik Timur Tengah.

CSIRTNS ingin mengingatkan Pentadbir Sistem, Pentadbir Rangkaian dan warga Pentadbiran Kerajaan Negeri Sembilan supaya segera melaksanakan langkah-langkah pencegahan untuk memastikan perkhidmatan digital dan rangkaian Kerajaan terjamin pada setiap masa. Kegagalan berbuat demikian boleh mengakibatkan gangguan operasi dan menjejaskan keselamatan infrastruktur organisasi, data dan sistem penyampaian perkhidmatan kepada pelanggan.

IMPAK

Kemungkinan kebocoran maklumat termasuk maklumat pengenalan peribadi (PII) dan harta intelek (IP), kerosakan web dan gangguan perkhidmatan.

SASARAN

Semua sistem pengoperasian, pelayan web dan perkhidmatan dalam talian.

CADANGAN TINDAKAN PENGUKUHAN

Jabatan/ Agensi dinasihatkan supaya berwaspada dan mengambil tindakan berikut:

1. Memastikan aset ICT kritikal dikemas kini dengan perisian keselamatan terkini. Jika kemas kini tidak dapat dilaksanakan, sahkan bahawa aset tersebut mempunyai kawalan dan perlindungan yang mencukupi untuk mengelakkan dieksploitasi secara dalaman atau luaran.
2. Memberi kesedaran dan menghantar peringatan ancaman kepada warga Pentadbiran Kerajaan Negeri Sembilan.

3. Berwaspada dan jangan klik e-mel serta pautan yang tidak diminta dengan atau tanpa lampiran.
4. Memastikan perisian anti-virus/perisian hasad adalah terkini dan berfungsi.
5. Semak log *firewall* dan peranti keselamatan secara kerap untuk sebarang pencerobohan.
6. Semak konfigurasi *firewall* dan perkakasan keselamatan anda dengan kerap.
7. Sekat atau hadkan akses kepada semua port (cth.. 3389 untuk RDP, 5900 untuk VNC dan 22 untuk SSH) dan perkhidmatan lain yang tidak diperlukan.
8. Pastikan kata laluan akses ke sistem anda kukuh dan selamat serta mematuhi Polisi Keselamatan Siber (PKS) Pentadbiran Kerajaan Negeri Sembilan.
9. Tukar kata laluan sekiranya anda mendapati akaun anda telah dikompromi.
10. Menghadkan hak akses kepada pengguna sistem yang perlu sahaja berdasarkan peranan dan tanggungjawab.
11. Elakkan penggunaan sistem secara jarak jauh (remote access).
12. Melaksanakan sandaran data melalui salinan pendua (backup) fail/sistem yang dikenalpasti untuk mengurangkan kesan kehilangan data serta mempercepatkan proses pemulihan. Sebaik-baiknya, sandaran perlu dilakukan setiap hari pada medium yang berasingan dan disimpan di luar talian atau lokasi alternatif.
13. Jika anda mengesyaki sistem anda telah terjejas, asingkan, tetapkan semula semua pengguna dan kata laluan serta mulakan prosedur tindak balas insiden sekiranya perlu.
14. Laporkan sebarang aktiviti yang mencurigakan berlaku dalam rangkaian dan persekitaran jabatan/agensi anda kepada CSIRTNS.

RUJUKAN

https://twitter.com/DailyDarkWeb/status/1750866521079926798
https://izoologic.com/region/central-asia/r00tk1t-hacking-group-threatens-malaysia-in-its-latest-post/
https://www.nc4.gov.my/alert/65b5cbec90087b4855570ee1

MAKLUMAT LANJUT

Cyber Security Incident Response Team Negeri Sembilan (CSIRTNS)
Unit Pengurusan Teknologi Maklumat
Tingkat 3, Blok B, Wisma Negeri, 70503 Seremban, Negeri Sembilan
Tel : +606-7659890; Faks : +606-7627760
E-Mel : certn9@ns.gov.my