

[INFO] Antisipasi Serangan Cyber Atas Isu Kenaikan BBM terhadap Website/Aplikasi Milik Kemenkeu

2022-09-05 - Agent 175 - General

Yth. 1. Para Kepala Kanwil Ditjen Perbendaharaan

2. Para Kepala KPPN

di Seluruh Indonesia

Untuk antisipasi serangan cyber krn isu Kenaikan BBM terhadap website/aplikasi milik Kemenkeu dan agar tidak terjadi anomali cyber security (deface, leak data, dll), sejak Sabtu sore, Pusintek selaku Pengelola Infra DC/DRC Kemenkeu sudah melakukan tindakan antisipasi, sbb :

1. Meningkatkan level severity website utama Kemenkeu dan Unit Eselon/Non Eselon ke level HIGH pada perangkat keamanan (WAF).
2. Menambahkan website lain kedalam pemantauan perangkat WAF.
3. Melakukan pengecekan halamana website secara berkala oleh petugas shift.
4. Melakukan pemantauan pada website atau forum hacker.
5. Berkoordinasikan dengan CSIRT Gov BSSN.

Mohon perkenan untuk mengingatkan Pengelola dan Pemilik Website masing-masing lingkup Ditjen Perbendaharaan, untuk melakukan langkah-langkah dan tindakan sbg mitigasi terkait isu, antara lain :

1. Melakukan pengecekan halamanan website dan log akses.
2. Melakukan pengecekan patching software pendukung aplikasi website, dan melakukan upgrade mengurangi celah keamanan dari bug software pendukung.
3. Segera melakukan hardening penutupan celah keamanan hasil VA kami.
4. Melakukan monitoring terhadap aktifitas akses halaman admin pengelola website, apabila memungkinkan menurunkan akses halaman admin website ke Intranet.
5. Melakukan reset password terhadap akun pengelola website.

Sebagai info tambahan, berdasarkan hasil investigasi kami, trending berita Kenaikan BBM di Google dan Twitter adalah :

1. Kemenkeu
2. Kemenhub
3. Pertamina
4. KemenESDM

Demikian kami sampaikan. Atas perhatian dan kerja sama Bapak/Ibu kami ucapkan terima kasih.