REQUEST FOR COMMAND (RFC) 2350 KBI-CSIRT

1. Informasi Mengenai Dokumen

Dokumen ini berisi deskripsi KBI-CSIRT berdasarkan RFC 2350, yaitu informasi dasar mengenai KBI-CSIRT, menjelaskan tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi KBI-CSIRT.

1.1. Tanggal Update Terakhir

Versi 1.0 diterbitkan pada tanggal 21 Agustus 2024.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan pembaharuan dokumen.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada:
https://www.ptkbi.com/cfind/source/files/rfc2350-kbi-csirt.pdf

1.4. Keaslian Dokumen

Dokumen ini ditandatangani secara fisik oleh Direktur Utama PT Kliring Berjangka Indonesia. Berkenaan dengan keaslian dokumen dapat dilihat lebih lanjut pada Subbab 2.8.

1.5. Identifikasi Dokumen

Dokumen memiliki atribut yaitu:

Judul	: RFC 2350 KBI-CISRT
Versi	: 1.0
Tanggal Publikasi	: 21 Agustus 2024
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Tim Respon Insiden Keamanan Komputer (*Computer Security Incident Response Team*) PT Kliring Berjangka Indonesia.

2.2. Alamat

Menara Danareksa Lantai 6
Jl. Medan Merdeka Selatan No. 14 Jakarta Pusat 10110

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

(021) 35280000 ext. 285 / 103

2.5. Nomor Fax

(021) 35282000

2.6. Telekomunikasi Lain

Tidak ada

2.7. Alamat Surat Elektronik (E-mail)

csirt@ptkbi.com

2.8. Kunci Publik {Public Key) dan Informasi/ Data Enkripsi lain

-----BEGIN PGP PUBLIC KEY BLOCK-----

xsBNBGbGqL4BCADphLBVJsq/SVssQcU0lYM3mFg1qH//8I3YVY90GQqvg7uLau+I
4/yuizEtlHsEo0IWpGufALA78YCDhU4PFsy4WWOac1s8GlzIUjvirFJIqv/e0ZB+
LQkTStUy5K5pkNmQVMAyztkTFk50/IXoJUTdoarKaauKH1Av3zUUkWhFPhKidNuj
zRtT3+CUxP95vYO+hiUbUiMqEdAtTXgGwEYcnlnItqK4a0q+L+5CUym35v469H9N
EfqwU4iKuRsteHh0He3fX7LiJG167edoTsIW8iaJQFYn/fBApTgFSKjN8jQlt4Me
Y0olyIJ0++gC0wyaJENVbh9Gmr74j2aigFV/ABEBAAHNMURpdmlzaSBUZWtub2xv
Z2kgSW5mb3JtYXNpIFBUIEtCSSA8ZHRpQHB0a2JpLmNvbT7CwHoEEwEKACQFAmbG
qL4CGy8DCwkHAxUKCAIeAQIXgAMWAgECGQEFCQAAAAAACgkQ4cAwixNw68UzXwf
9
GuvdCZZfP6X0WVpkELFdsFtbS1Ti1zLILFB5qI+pQCglWHySvGKVo2fWUOCADm0i
cdOShl5xPkEObJlUoj59yj2q6TbBb3vFjH/WAR19kbpP3OYbdeeWLvMspnnhHpvT
EqYq9R+meUtgKl1S+hdjzzJnkUFlsE+XU70zumgyaTo0TmUkS/X8p44AisHyIfuQ
APyC8ngEiepH2YikJpBXZ2+6HMVonBYJbIrMusgBzad/GEaSYehcvC2QvdWrIlfd
3ipTKY68JbVqWMT640Le6tKoHsdrTlgysNFRXp1tIUgD2HC5TYHyQ+EN2EtEO3Da
FO2BBtLbDupzzLlW/uu+js7ATQRmxqi+AQgA7fLELrKxuxDJC/pjeyOCY6OtAmgZ
ROW3TbH0oPrwMunHzl/xD+aI+jyWi7JEDL0+1nuIKYfIJSa/1wHwd9BGVaEwUZ9y
gFNg2m7Zyh6dcpS8H9MeHybXRLt1KgD+wzoM/8118zmUpGkmNb0HTw6DLa1mpJyb
ae1Zx+cqL+zDFBwlCCPUo69wnoUewQknU5+jHmDDYaWvQlfFFuur0JWYaESW2ffM
mVn1lU5VUq2shhB+auit7NY+uJZfB0i7KY4IfXLeZy032Yw+K0gOpZYxYxRVEQf5
Ft4ZN8W9eClyhcTA4+9r43xE/idesFfEfng5lERlAxM+2Lo8UgBNeFs7FQARAQAB
wsGEBBgBCgAPBQJmxqi+BQkAAAAAAhsuASkJEOHAMIsTcOvFwF0gBBkBCgAGBQJm
xqi+AAoJEFgHH0q6/YIbsyYH/Rh2yFgShzR6bzoQMa/x/fJOjxIhrXBxzzlhU4kc
N/RQeaTcUGZ83gzL+yke9F/Kvac8NNZFq9yZDwLEjZgCMwQ+9dWKK9Z91YvTkL0C
oPGulthfehSH/V6eiBoxTYZBaC3/FibNhEj9HA/JbNANjhDvLAgmSniQmHg1lWS+
DEJkyoEJMpbHjoYoZjnwIwGMr82eF8K4kWmWkpT/n4/QhB6JtPYgGXPK4qR5LcVn
HQAvdq1vyRDJaGM0i5zGNzsrhD5hyNvDrhBN9uiFXOUm50p3+lZpSbWT5L6yK4us
I8mb/GL+upkIZpZWMd65w6xI0PJvuX4ZuUSE9u9739sf1SyczQgAh2pKyHHk49bf
L6NS9pRtLmLZkHTPghaqEiKsg22m2DWFMpVCug+KcbEJx06zivexoVvoXwxoXpXK
ntj+1THzzwhIIdY6pCCqFk0K3kc46+f8MZhyRWuzJqRWo/8yiP0NymDIds/MhWZA
c6/vqTpEgKKekFetjZ50Sx2r3G2SDgXZLsurIuje6j/y/qB7t6/6lwXb8wLiJmC0
mQNgb6E2RWHYfveG7eHOWcH3k9WKPkri1TqvMu6hrmxV1z2Uejw1FDmT+MCDNx
pH
WbHMTo3XajrYrwlYprhcBcsHr2kBLxeSq/c8RBnKL2bD9Zs3ZBt3XvPMboID7mnB
dAoMg2QUO87ATQRmxqi+AQgAqpYANV1mwvC29NVbKdnSYL4H6P9YV5lrjwXFxWm
P
n+g0ADITHYWNkJKNWAlxzUFJm1VObUnf8cCDyeoUfMAT1DN2xFliHB2PMZdzOo0P
ylBA14DuxG9YkYIch/rY8u2rf7D1Rg91SPxjANvirL70OY+eYFQ6DekP9xHWG7Sj
9kxq1jdKAd2X+w7VyOTU/HsvgXp+auWWnWQyw2GSVncJvFHoBAjhs4Nl7NudsCQ8
NHuYx7JOao3isSSDL32Huo2OLMSr0qlqmdzXKJ9jJMMs6PsnCfZuWwUTTk81YD4B
77QePHgLKxzJoWeOCta4Kvvf0vb5z3aoSXWyL9k4mHiJ/wARAQABwsGEBBgBCgAP
BQJmxqi+BQkAAAAAAhsuASkJEOHAMIsTcOvFwF0gBBkBCgAGBQJmxqi+AAoJEIJ+
F1vAmbv0gRwH/222n9iFQmnjI+XW22cysWXebTRTHInzSHDu7El+39KPGSLMF5DL
9CTZjku/zw3v82gxRDSgiibo8xQqJ/8xuVdbQrmz4cGpiGzWcNUVViuHLat3obg6
3fnmwex1/P5C9UCvz5NfHz+tp61UGPjgY7fmxiV9U8l+gfPbGlG3o0/Gygll1M8e

FHhiX/utgrjncV9UZOqdqEstJbLB1tlDGqDOhD/i1mkIem5Miv9GmAEHRS9of08X
72lpOrKa4cZ3ES0RJzy+auAbwTSNqV3DUDfwgPug0LOmBameqfDTCD+sUNRb7Jcn
F6SdKvzHZ0++ly1ljpFk8Hf35WSyBJ3yfhnuUAf/T68ewccP9etKxZyLomP7nhK5
4VFcKtobWguwmKPTuHdCTqzzbP1Fw4XWlVZ3y7lT7bTodHVb7pyRw6AqlO4lXBfO
1tT/Jz+YbOZf/K/xPtsfjWs3hAv2C64zSQF1vANKe41OY9CnXNZLpOQc7qd+0V5q
0hhILbAMWcYcuDVijrFvdyy5PV//ZFtPbaisGrQx7On+A6tguN2ZHodgKcLJNZD0
cSg4O4k4uVhlT/XkFjhGZGagvMdKnMksDDG8oSDeg91OdBZpxIQTYC5NuM91QgM0
ktBAlhHvyUTzpVmn3TECdEjAbfVEQAGU7/FNv3vDzer63Y0NA4eO0Gnf3xRVbg==
=6im2
-----END PGP PUBLIC KEY BLOCK-----

2.9. Anggota Tim

Ketua KBI-CSIRT dijabat oleh Kepala Divisi Teknologi Informasi PT Kliring Berjangka Indonesia. Yang termasuk anggota tim adalah seluruh pegawai pada Divisi Teknologi Informasi.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak KBI-CSIRT

Metode yang disarankan untuk menghubungi KBI-CSIRT adalah melalui e-mail pada alamat csirt@ptkbi.com atau melalui nomor telepon (021) 35280000 ext. 285 / 103 yang siaga selama 24/7 (khususnya melalui email).

3. Mengenai KBI-CSIRT

3.1. Visi

Terwujudnya pengelolaan sistem keamanan informasi dengan baik dan aman di Lingkungan PT Kliring Berjangka Indonesia untuk melindungi aset informasi yang dimiliki oleh PT Kliring Berjangka Indonesia.

3.2. Misi

Misi dari KBI-CSIRT, yaitu:

a. Mengoordinasikan penanganan insiden keamanan informasi di PT Kliring Berjangka Indonesia.
b. Meningkatkan kesadaran keamanan informasi pada seluruh unit kerja yang menjadi konstituen KBI-CSIRT.
c. Menyediakan dan mengoptimalkan sumber daya keamanan informasi melalui proses pembelajaran dan peningkatan kualitas yang berkelanjutan.

3.3. Konstituen

Konstituen KBI-CSIRT meliputi pengguna sistem elektronik di lingkungan PT Kliring Berjangka Indonesia.

3.4. Sponsorship dan/atau Afiliasi

Seluruh pendanaan KBI-CSIRT bersumber dari Anggaran *Cyber Security* PT Kliring Berjangka Indonesia.

3.5. Otoritas

KBI-CSIRT melakukan koordinasi penanganan insiden keamanan siber atas permintaan konstituen dan memberikan bantuan teknis untuk keluhan atas insiden keamanan informasi di Internal PT Kliring Berjangka Indonesia, bekerja sama dengan para pihak yang terlibat dalam insiden keamanan informasi terkait, dan melakukan koordinasi

dengan pihak BSSN selaku Gov-CSIRT atau pihak lain untuk insiden yang tidak dapat ditangani.

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/Level Dukungan

KBI-CSIRT melayani penanganan insiden siber dengan jenis berikut:

a. Malware;
b. Web Defacement;
c. DDOS;
b. Phising;
c. Advanced Persistent Threats (APT).

Dukungan yang diberikan oleh KBI-CSIRT kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden.

4.2. Kerja sama

a. Kerja sama antar instansi dapat dilaksanakan dengan tujuan untuk saling berbagi sumber daya pengetahuan, keterampilan dan informasi mengenai keamanan siber/informasi.
b. Kerja sama antar instansi dilakukan dengan tetap memperhatikan kebijakan, sistem prosedur dan perlindungan kepentingan PT Kliring Berjangka Indonesia.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa KBI-CSIRT dapat menggunakan alamat e-mail tanpa enkripsi data (e-mail konvensional) dan telepon. Namun, untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi PGP pada e-mail.

5. Layanan

5.1. Layanan Utama

Layanan utama dari KBI-CSIRT yaitu:

1. Pemberian Peringatan Terkait Keamanan Siber
    a. Memastikan kebenaran insiden dan pelapor;
    b. Menilai dampak dan prioritas insiden.
2. Penanganan Insiden Siber
    a. Mengoordinasikan insiden dengan konstituen;
    b. Menentukan kemungkinan penyebab insiden;
    b. Memberikan rekomendasi penanggulangan berdasarkan panduan/SOP yang dimiliki kepada konstituen;
    c. Mengoordinasikan insiden dengan Gov-CSIRT atau pihak lain yang terkait.

5.2. Layanan Tambahan

Layanan tambahan dari KBI-CSIRT yaitu pembangunan kesadaran dan kepedulian terhadap keamanan siber melalui berbagai kegiatan meliputi Sosialisasi, Workshops Bimbingan Teknis, *Drill Test,* dan *Forum Grup Discussion* (FGD) terkait Keamanan Siber.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt@ptkbi.com dengan melampirkan sekurang-kurangnya:

a. Foto/scan kartu identitas;
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan;

c. Atau sesuai dengan ketentuan lain yang berlaku.

7. Disclaimer

Terkait penanganan jenis *malware* tergantung pada ketersediaan *tools* dan kompentensi yang dimiliki.