RFC 2350 MIL-CSIRT TNI

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 20 Desember 2021.

1.2. Daftar Distribusi untuk Pemberitahuan

Pemberitahuan update dikirim ke milis .Permintaan berlangganan daftar ini dikirim ke piket@satsiber-tni.mil.id dengan isi pesan yang memuat permintaan bergabung dengan menyebutkan nama, asal satker dan nomer telpon yang dapat dihubungi.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada Satuan Pemulihan Satsiber TNI.

1.4. Keaslian Dokumen

Kedua dokumen telah ditanda tangani dengan PGP *Key* milik Mil-CSIRT TNI. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 Mil-CSIRT TNI;
Versi : 1.0;
Tanggal Publikasi : 20/12/2021;

2. Informasi Data/Kontak

2.1. Nama Tim

Military Computer Emergency Response Team Satsiber TNI
Disingkat : Mil-CSIRT TNI.

2.2. Alamat

Mabes TNI Cilangkap, Jakarta Timur.

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

a. +62 812-1214-1379 (Whatsapp Piket)
b. (021) 84590703

2.5. Nomor Fax

(021) 84590703

2.6. Telekomunikasi Lain

Tidak ada.

2.7. Alamat Surat Elektronik (*E-mail*)

piket@satsiber-tni.mil.id

2.8. Komunikasi dan Autentikasi

Untuk komunikasi yang aman, berikut adalah PGP key Satsiber TNI:
Blok PGP Public Key :
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: BCPG C# v1.6.1.0

mQENBGHALr0BCADHKlwHIJ1nZWhBd7I5eigXsLAmg61WyveuQ3/rU6kbh4+n2A
LvouqwN47n6ZX5FYu6HMIyHxaRaKy/lwnyTUGATXbuFiy7LAakJvtAPTa30fdybwP
T5O+UXS5VGvisdefoZTatjGgzGbZOxt9Nru3eCbb2KpiETrMKmP+EmsEjLxgueCyo
faqOPZkGe8AxkmbeCDOVDeRfTDz1HdMyKdlOtOb4ycfadVy/yEg0tVfafe9mcmMz
MbtC9chHUhjnugEIVFEG6bhpRVRSszKVk9zQTooep8BKqrO0iKrGxEdWIRb7szgg
O7y8CFys1+RBrBNF5AiPCS21SMzGDLFa63wNABEBAAG0E2Rpb25haW0zMEB
nbWFpbC5jb22JARwEEAECAAYFAmHALr0ACgkQMAxcQo48f9Wu1gf+IQDvzbsU
gHVGl/RMRkTKBaq/RnT7ducHpCAcnolOu8L+ZhkBkNkHrpJN5pLeX5yn3M2XKN7
SrpliyZRCPYOhQ12f4dV9Jk1te8Q2HL6blcO7GEhGzezXTmJiZEe+jr3gX8Z94ggz/i
2NbftYBvUccmIj3vS+QulPJW6fqM0SpoK7d7H3ufK9oFe29X6quXAWXCi0TXEB37
LbzRfm08pu0QgffaIbajwaE+ESE/sd30ZY0EfNS0grgH2/21b3WlflFIcAdVWLppRTIj
CtNoGx45ES9wAKTX7kbKU9YvU1IGwjywiFSVDOR1vfJZ9KQY1kH6AJTUV/j+n40
YGCGqDEZw==
=k5jd
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini dibuat melalui :
https://www.igolder.com/pgp/generate-key/

2.9. Anggota Tim

Ketua Mil-CSIRT TNI adalah Mayor Lek Teuku Rizliansyah. Yang termasuk anggota tim adalah sebutkan nama tim:

a. Mayor Lek Achmad Bayu Setiawan
b. Kapten Arh Erith Cannabid
c. Lettu Laut (E) Agung S Ch Lages
d. Lettu Laut (Kh) Ahmad Wahyudi

e. Serka Iqbal Widagdo
f. Serka Martinus Wahyu Permadi

2.10. Catatan-catatan pada Kontak Mil-CSIRT TNI

Metode yang disarankan untuk menghubungi Mil-CSIRT TNI adalah melalui *e-mail* pada alamat piket@satsiber-tni.mil.id atau melalui nomor *Whatsapp* piket jaga di nomor +62 812-1214-1379 siaga selama 24/7.

3. Mengenai Gov-CSIRT

3.1. Visi

Visi Mil-CSIRT TNI adalah untuk meningkatkan *awareness* keamanan Siber di jajaran u.o Mabes TNI.

3.2. Misi

Misi dari Mil-CSIRT TNI, yaitu :

a. Menangani insiden siber,
b. Mekanisme untuk mencegah penyebarluasan insiden (isolasi insiden),
c. Mengidentifikasi tingkat keparahan yang ditimbulkan,
d. Menghilangkan sumber penyebab insiden,
e. Memulihkan sistem beserta data yang terdampak, dan
f. Evaluasi pembelajaran untuk mencegah insiden serupa terulang di kemudian hari.

3.3. Konstituen

Konstituen Mil-CSIRT TNI meliputi :

- Satsiber TNI
- Satkomlek TNI
- Paspampres
- BAIS TNI
- Sesko TNI
- Pusinfomar TNI
- Pusinfolahta TNI
- Kohanudnas
- Pusdalops TNI
- Puspen TNI
- Kodiklat TNI
- Kogabwilhan I
- Kogabwilhan II
- Kogabwilhan III
- STT Natuna
- Staf Umum TNI
- Itjen TNI
- Sahli Panglima TNI
- Srenum TNI
- Sintel TNI
- Sops TNI
- Spers TNI
- Slog TNI
- Ster TNI
- Skomlek TNI
- Akademi TNI
- Koopsus TNI
- Babinkum TNI
- Puskes TNI
- Puspom TNI
- Otjen TNI
- Puslemasmil
- Babek TNI
- Pusbintal TNI
- Pusku TNI
- Pusjarah TNI
- Puskersin TNI
- PMPP TNI
- Pusjianstra TNI
- Pusjaspermildas TNI
- Satkomlek TNI
- Setum TNI
- Denma Mabes TNI

3.4. Otoritas

Mil-CSIRT TNI tidak memiliki otoritas secara operasional terhadap konstituensinya dalam jajaran U.O Mabes TNI, melainkan hanya menginformasikan

berbagai keluhan atas insiden jaringan, serta bergantung sepenuhnya pada kerjasama dengan para-pihak yang terlibat dalam insiden jaringan terkait.

Mil-CSIRT TNI mengharapkan untuk dapat bekerja sama dengan para sys-admin dan user/pengguna berbagai organisasi termasuk tim Mil-CSIRT masing-masing matra (TNI AD, TNI AL, dan TNI AU), serta sedapat mungkin, menghindari hubungan yang otoriter.

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/*Level* Dukungan

Mil-CSIRT TNI melayani penanganan insiden siber dengan jenis berikut :

a. *Web Defacement*
b. *Malware/Ransomware*
c. *DDoS* (*Distributed Denied of Service*)
d. *SQL Injection*
e. *Phishing*
f. *Data Breached*

Tim Mil-CSIRT akan menganalisa dan melalukan *penetration testing* ulang setelah dilakukan proses *patching* atau *hardening*.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

Mil-CSIRT TNI bekerja sama dengan seluruh Mil-CSIRT masing-masing matra, yaitu TNI AD, TNI AL, dan TNI AU. Mil-CSIRT TNI bertanggung jawab penuh terhadap asset/inventaris server di bawah jajaran U.O Mabes TNI dan siap diperbantukan untuk penanganan insiden siber di masing-masing matra.
Untuk informasi-informasi yang bersifat sensitif/rahasia tidak akan dipublikasikan

5. Layanan

5.1. Layanan Utama

Mil-CSIRT TNI akan membantu *sysadmin* dalam menangani aspek-aspek teknis dan organisasi dari insiden. Khususnya, tim akan memberikan bantuna atau saran pada aspek-aspek menejemen insiden berikut ini:

5.1.1. Triage Insiden

Menginvestigasi apakah benar-benar sebuah insiden terjadi Menentukan luasnya insiden

5.1.2. Koordinasi Insiden

a. Menentukan penyebab awal dari insiden (pemanfaatan kepekaan/kelemahan).
b. Memfasilitasi kontak dengan pihak lain yang mungkin terlibat.

c. Memfasilitasi kontak dengan tim Keamanan Mil-CSIRT lainnya dan/atau sesuai Undang-undang resmi yang sesuai, bila perlu.
d. Membuat laporan untuk tim Mil-CSIRT yang lain.
e. Menyusun pemberitahuan/pengumuman kepada para user/pengguna, bila diperlukan.

5.1.3. Resolusi Insiden

a. Menghilangkan kelemahan, dilakukan oleh pihak yang dilaporkan.
b. Mengamankan sistem dari efek-efek insiden, dilakukan oleh pihak yang dilaporkan.
c. Mengevaluasi apakah tindakan tertentu memungkinkan untuk memperoleh hasil-hasil yang sebanding dengan biaya dan resikonya, khususnya tindakan-tindakan yang ditujukan pada suatu tuntutan atau tindakan disipliner: mengumpulkan bukti nyata, observasi akan satu insiden yang sedang terjadi, menyeting jebakan untuk para penyusup, dan lain-lain. Dilakukan oleh penegak hukum atau pihak terkait lainnya sesuai peraturan Perundangan yang berlaku.
d. Mil-CSIRT TNI akan mengumpulkan statistik mengenai insiden yang terjadi dalam atau yang melibatkan komunitas CSIRT, dan akan menotifikasi komunitasnya seperlunya untuk membantu melindungi dari serangan-serangan yang dikenal.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke alamat email piket@satsiber-tni.mil.id dengan melampirkan sekurang-kurangnya :

a. Foto/*scan* KTA yang mengadukan
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan
c. Log file
d. Nomor telepon yang dapat dihubungi