RFC 2350 UNIKU-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 10 Mei 2023.

1.2. Daftar Distribusi untuk Pemberitahuan

UNIKU-CSIRT.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://csirt.uniku.ac.id/download/rfc2350.pdf (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

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

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 UNIKU-CSIRT;
Versi : 1.0;
Tanggal Publikasi : 10 Mei 2023;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Universitas Kuningan Computer Security Incident Response Team
Disingkat : UNIKU-CSIRT.

2.2. Alamat

Gedung Rektorat Lantai 2 Kampus 1 Universitas Kuningan
Jl. Cut Nyak Dhien No. 36A, Cijoho, Kec. Kuningan, Kab. Kuningan, Jawa Barat, 45513

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

(+62) 232873696

2.5. Nomor Fax

-

2.6. Telekomunikasi Lain

(+62)811 2200 850

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

csirt[at]uniku[dot]ac[dot]id

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

Bits : ECC Curve25519
ID : csirt Universitas Kuningan <csirt@uniku.ac.id>
Key Fingerprint : 2108 F282 694E 821B 4BDA C891 1422 153E DB5D F53E

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: FlowCrypt [BUILD_REPLACEABLE_VERSION] Gmail Encryption
Comment: Seamlessly send and receive encrypted email

xjMEZFNK1BYJKwYBBAHaRw8BAQdAQhQqJ7hBskxRf0ev3xDcfCELyocuziin
PTtuiKMVXdXNLmNzaXJ0IFVuaXZlcnNpdGFzIEt1bmluZ2FuIDxjc2lydEB1
bmlrdS5hYy5pZD7CrQQQFgoAPgWCZFNK1AQLCQcICZAUIhU+2131PgMVCAoE
FgACAQIZAQKbAwIeARYhBCEI8oJpToIbS9rIkRQiFT7bXfU+ACEJEBQiFT7b
XfU+FiEEIQjygmlOghtL2siRFCIVPttd9T6kfAD+LBSIAEp63JxmUqUih4sk
5Wd4t287kZ4jwKVx5VDatUAA/RdfmmWko0/RRrxYoIoOLPg3X6JDzx26zvG6
PEtjrskMzjgEZFNK1BIKKwYBBAGXVQEFAQEHQFHaxRFBKVQ09G57a6eXqtB8
zB6bjBwqN+VDpK5mp3dvAwEIB8KZBBgWCAAqBYJkU0rUCZAUIhU+2131PgKb
DBYhBCEI8oJpToIbS9rIkRQiFT7bXfU+ACEJEBQiFT7bXfU+FiEEIQjygmlO
ghtL2siRFCIVPttd9T4LggEArXOZM9AeGQfd5igLsP0xct1f7GhqUI8rvHTW
DYjNrpkBAKofmrfy97RQj1HcX2DvK32ypzp8Dh2MQ8GvTv2W8FMD
=zv9o
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://csirt.uniku.ac.id/download/uniku-csirt.asc

2.9. Anggota Tim

Ketua UNIKU-CSIRT adalah Fitra Nugraha, M.Kom. Yang termasuk anggota tim adalah Bambang Wahyudi, M.Kom; Mohammad Firdaus, S.Kom; Aji Permana, M.Kom; Jejen Riana, S.Kom; Devi Heryani, S.Kom .

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak UNIKU-CSIRT

Metode yang disarankan untuk menghubungi UNIKU-CSIRT adalah melalui *e-mail* pada alamat csirt[at]uniku[dot]ac[dot]id atau melalui nomor telepon (+62)811 2200 850 ke UNIKU-CSIRT yang siaga selama 24/7.

3. Mengenai UNIKU-CSIRT

3.1. Visi

Visi UNIKU-CSIRT adalah Terwujudnya keamanan siber pada pengelolaan Teknologi Informasi dan Komunikasi di lingkungan Universitas Kuningan.

3.2. Misi

Misi dari UNIKU-CSIRT, yaitu :

1. Membangun, mengoordinasikan, mengolaborasikan dan mengoperasionalkan pencegahan, penanggulangan dan pemulihan terhadap insiden keamanan siber di lingkungan Universitas Kuningan
2. Membangun kerjasama dalam rangka pengamanan siber terhadap layanan TI di lingkungan Universitas Kuningan.
3. Meningkatkan kapasitas sumber daya manusia terhadap ancaman keamanan siber pada aspek pencegahan, penanggulangan dan pemulihan insiden keamanan siber di lingkungan Universitas Kuningan.

3.3. Konstituen

Konstituen UNIKU-CSIRT meliputi seluruh satuan unit kerja di lingkungan Universitas Kuningan.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan UNIKU-CSIRT bersumber dari Universitas Kuningan

3.5. Otoritas

1. UNIKU-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber dilingkungan Universitas Kuningan.
2. UNIKU-CSIRT dapat berkoordinasi serta bekerjasama dengan pihak lain yang mempunyai kompetensi untuk insiden yang tidak dapat ditangani.

4. Kebijakan – Kebijakan

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

Nama-CSIRT melayani penanganan insiden siber dengan jenis berikut :

a. Web Defacement;
b. DDoS;
c. Malware;
d. Phising;
e. Pembajakan akun;
f. Akses Ilegal;
g. Spam;

Dukungan yang diberikan oleh UNIKU-CSIRT kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden. Layanan penanganan insiden berdasarkan pada laporan konstituen.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

UNIKU-CSIRT akan melakukan kerjasama dan berbagi informasi dengan CSIRT atau Organisasi yang berkepentingan dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh UNIKU-CSIRT akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, UNIIKU-CSIRT dapat menggunakan email tanpa enkripsi data dan telepon namun untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi pgp pada email.

5. Layanan

5.1. Layanan Utama

Layanan utama dari UNIKU-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini dilaksanakan oleh UNIKU-CSIRT berupa pemberian peringatan adanya insiden siber pada sistem elektronik dan informasi yang dikelola oleh masing-masing satuan kerja dilingkungan Universitas Kuningan.

5.1.2. Penanganan Insiden Siber

Layanan ini diberikan oleh UNIKU-CSIRT berupa koordinasi, analisis, rekomendasi teknis, dan bantuan kunjungan ke lokasi dalam rangka penanggulangan dan pemulihan insiden siber.

5.2. Layanan Tambahan

Layanan tambahan dari UNIKU-CSIRT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini diberikan oleh UNIKU-CSIRT berupa koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan, UNIKU-CSIRT memberikan informasi statistik terkait layanan ini. Namun, layanan ini hanya berlaku apabila syarat-syarat berikut terpenuhi:

1. Pelapor atas kerawanan adalah pemilik sistem elektronik. Jika pelapor adalah bukan pemilik sistem, maka laporan kerawanannya tidak dapat ditangani;
2. Layanan penanganan kerawanan yang dimaksud dapat juga merupakan tindak lanjut atas kegiatan Vulnerability Assessment.

5.2.2. Penanganan Artefak Digital

Layanan ini diberikan UNIKU-CSIRT berupa penanganan artefak dalam rangka pemulihan sistem elektronik terdampak ataupun dukungan investigasi.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Pemberitahuan hasil pengamatan terkait dengan ancaman baru Layanan ini diberikan oleh UNIKU-CSIRT berupa hasil dari log perangkat aktif yang digunakan oleh Universitas Kuningan.

5.2.4. Pendeteksian Serangan

Melakukan pendeteksian terhadap berbagai serangan yang terjadi dan di pantau melalui sistem deteksi dan monitoring keamanan.

5.2.5. Analisis Risiko Keamanan Siber

Layanan ini berupa identifikasi kerentanan dan penilaian risiko kerentanan yang di temukan. Selanjutnya di berikan rekomendasi yang dapat dilakukan untuk mengurangi risiko tersebut.

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Pemberian konsultasi terkait kesiapan penanggulangan dan pemulihan insiden keamanan siber.

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Sosialisasi dan pembinaan kepada seluruh unit di lingkungan Universitas Kuningan yang bertujuan untuk meningkatkan kesadaran dan kepedulian para pegawai tentang keamanan siber

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt@uniku.ac.id 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*

a. Sampai saat ini UNIKU-CSIRT hanya merespon dan menangani insiden keamanan siber yang terjadi pada perangkat kerja yang ada di lingkungan UNIKU;

b. Terkait penanganan insiden jenis malware tergantung pada ketersediaan tools yang dimiliki.