RFC 2350 CSIRT-ITECH

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 29 Desember 2024.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan mengenai pembaharuan dokumen.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://csirt.i-tech.ac.id/CSIRT-ITECH-RFC2350.pdf (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

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

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 CSIRT-ITECH;
Versi : 1.0;
Tanggal Publikasi : 29 Desember 2024;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Computer Security Incident Response Team Sekolah Tinggi Teknologi Informasi NIIT (I-Tech)
Disingkat : CSIRT-ITECH

2.2. Alamat

Jl. Asem Dua No.22, RT.11/RW.5, Cipete Sel., Kec. Cilandak, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12410

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

(021) 7515870

2.5. Nomor Fax

(021) 7691108

2.6. Telekomunikasi Lain

WA Resmi STTI NIIT 0897-0127001

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

csirt[at]i-tech[dot]ac[dot]id

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

Bits : 4096
ID : 0xB069B976
Key Fingerprint : 46F8 D112 D440 36F0 062D 638E EDD6 A78B B069 B976

Blok PGP Public Key Misalnya :

-----BEGIN PGP PUBLIC KEY BLOCK-----
mQINBGdvhVIBEADhXCqbaaUvpZ29utSqxZFBJqP7C/fMVQqw+QpDMvfh4ML05
GZEFtrwuxqmh7Z4CFSf6/GCu7J3fr3due6q/4aWFKU3Ekvbxs0R3+Ks0s8EV7umb
R8Bq8T5EvdgzNH2Yvng+WCPbui/nOZ3TFOfQyL0XHsrrLzcspi7K8fBDQizAlAOLA
7Xe2ThsX/sHoE4Z64PG2bfFt7dqK2kedQ122RaVqMGOh1T812eOxe1VdQ4B6yze
fsSPTpGVC84bLX9WObfBv2fF6eUj10s+8OsSv2q/vHWTZmH+ITuoqYKFvVx5xajt
Ux/Scu56eNpacDZ/7tsQTO32YeWVkRpLH5FJJXMZhUQyZr3o6ojeQFVTbe0n6XV
CiTP7hIUIErFdjNLsy5DvMuuRg+cW/kZvgWF4bxNXth+wxcksEXtHRnkPGyj6qMr3c
zS7jtbROn04Q4rpJNNTw8norsE7WQVxSmdadbbH54OjamFk6Lvxby/hTK9LnSqrd
gNwy/jdsDrUXVu9p60IEoAaiH2jcdFiMlE8I0ZV4zVZEUfFFAT6iPwUDwI2WZ72DDv
6TbnB+kPZXqQYd/fIrrsuABuwQlRZy9ChHWT45xjeW5SIo4GIL266PuTll9a0Cjj1oz
d7DJpHiUmq13x0XhomQnCBHgQAaf5ynjIu/MTbLgU/04mF0NQvcxffQARAQAB
tDpDU0lSVCBJLVRlY2ggKENTSVJUIFNUVEkgTklJVCBJLVRlY2gpIDxjc2lydEBp
LXRlY2guYWMuaWQ+iQJRBBMBCAA7FiEERvjREtRANvAGLWOO7dani7BpuXYF
AmdvhVICGwMFCwkIBwICIgIGFQoJCAsCBBYCAwECHgcCF4AACgkQ7dani7Bpu
XbiMQ/9Fze6OtLpTcD51xGCqHvb8OJXzRZqU8yD/uAxxyT5rmt0wxICzNmnxvvs9t
zFfP5tA1MURZrbRpe3ECImxNTR/uEVUNsZi94jWZxFrLOi08/Tt04ReQM6HeFA8lf
NEuD3k9eJ2rmuKhhQzaNz1k2ZK8Dkdsgzom6vcQweJH9XUQUbAD9aAmr0qESia
dN5UKwmXqhomMpprrpucmQBR1rRdqFo+OWB+PEri44MwtwWxwMPNkZpyoIAz
XzEDxHKQtH00x83lHiVxk2Wplz7Vn8WI5q56iBbD16Ov74nByV5NAZqiHdPNChq2
Ewq2JF0vtwAynhr8pdt/sA2+VeCrgZvnyck0WFaUoeBC68DemF3Z4/WX7s4bLV0fO
kNFTu8yUyaFvvA38rlzbpvMjzzi2nf7Vm0UO+1g/nTZYeRgSxAMVqkj7UGE4h2IY5x
o0x/QY0qh5Ng+EMSwjf+nd0UK8mEI3R0M2lX7QkCYwG7QXL5LjBuT8MIysvjth6S
PQ437Mttw7XyTJfkuG0qq9cR5iSvuEDb5FzvitVjLteInGISlmanAFDPkoOw0Irmlb11
F7TQ3L3Tz5urDiyraD9ZcedC+VhGEp1g56Z0OskTt+PXuPK8ttpkrpeHP/zjIMfbI1bV
gIGssmRVmgMT24C9g7D7jvVJBpLPLgZEd4z5cdevuR25Ag0EZ2+FUgEQAMcWQ
gqaW/KKZRmXJFYO6VJxet6rm9pWc0CbWnsC69jKxGW7oMSZ5wOMAPHWAnA
yDkQq6NmsgYW+EUFt6BxvUpTDU3uYiNd9YgaagLfgFs690AVnGMZB+tGnOPgQ

sJPhE8RDxqJM90TWMeKMpdvqj3qfTqMMtAuzeaikXZRQTlazT9vUtmzRMOMtbF
BZ8AhR6jUbukzruNYHtdVdGBbdq8l0zwXGHqLZrf2q1cfQMMHysuS/zMf6laZGluF
wQOG+0SCFSoDZuBozQaO5OIy4nT+w2XOqi3BvOTLKVYIXSHwth6KIilpwCByZ
m8Sy79Q+1mkctkz45p0qxQkFPpt8zU32LXkSYWQGf3LvpqNDImfg97CaMid+/BEz
sbzpMoqtufH3Bo140QH+ViBa9FIxkWtctgS3vKsw543ij1HchJ3gLInsqiLajV0TQDSK
mmIBCFENLCi28tdJLwCxX+G+ArMHHh612nHsJ3Pe/wAuiU6V97N6it0P/HbCt0Kej
/GLu4p6rhCIdBoy77CNxpyJtjFa6QRBQelEgYNlFR4++8Bc7rnHAaWRZX7Jzj+hGU
SgXWBTezmYy0cAIzzH6apDG521KCNY3sJOzrlXl+u8vtIZw7D7gBf302Dc1+pN0Z
z+fGSPoTmemoXnef2gZrp22aevzDNnuNF9q7TSOWsqFfEbABEBAAGJAjYEGAEI
ACAWIQRG+NES1EA28AYtY47t1qeLsGm5dgUCZ2+FUgIbDAAKCRDt1qeLsGm5
div7EACSs1/iJ+yOFiOnJh/nfWyJAtCRUQpRA3xMYDSdMyjdWlywU4NaSt13Qo8ve
t5byafQxelrzVu/drJtraQXi87EULFzjkIDHgyHZMpRCBpAI5anrjBOQ6lQFPqsbHBqK
5VvtCnYfrWvEvygeoF+F9g6m1TBfr7fVS8uQq2dN33MMVGjrs1e0gTrL/blPq1Qjnsa
TKqh5KxvqTd0il1QWI2kRLnOrNwjFOw/KTeMJb8z4uIrkCJdDV1vb/DJvr/G9Ki+hnh
6DlJrzN4hlzf86oY2xERNpRRFfbIT7EhdTnQv61E+1lmUSVLPrJm+UGUtr5EDoZkS
AYnjbgV4GZ9MHAurLIZlwjfnxsUA6ZT5jmYdwFOdOtsRJPMQvXTh5qigzjk78wiWC
40CJTzzQn6WRJfruwnRcnOuTSkeasBiUbXn3/6jlS3HnhqHrUx/RmehE5rKePpSnO
gX38jHn5GceJ3y9piieAI5LzsGvds23KjvR/MMP0pNc0yxF+ZaKVD7AjLgS3FjC5O/
4pau5AL5wGWDVeL6swnh4jfSOS1eIHbcekprV6oOdzwmVN5V0dwIC890XBGy+O
pyLc9jaEmk9oqtnje+TkazY6OTEXDXWtFppcY+S5P1TvAkGvwrCCk3AnJhsOlRbd
LVMm3ejq6vTsyPJkbBOU3dwBovEVAklJeVsA==
=Snv8
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://csirt.i-tech.ac.id/publickey.asc

2.9. Anggota Tim

Ketua CSIRT-ITECH adalah Kepala Bagian Layanan Teknologi Informasi dengan anggota tim terdiri dari Kepala Program Studi Teknik Informatika, Dosen dan Staff Layanan IT Sekolah Tinggi Teknologi Informasi NIIT.

2.10. Informasi/Data lain

Tidak ada

2.11. Catatan-catatan pada Kontak CSIRT-ITECH

Metode yang disarankan untuk menghubungi CSIRT-ITECH adalah melalui *e-mail* pada alamat csirt[at]i-tech[dot]ac[dot]id atau melalui WA Resmi STTI NIIT 0897-0127001 pada hari kerja Senin-Sabtu jam 08.30 - 16.30 WIB.

3. Mengenai CSIRT-ITECH

3.1. Visi

Visi CSIRT-ITECH adalah terwujudnya ketahanan siber yang handal dan profesional di lingkungan Sekolah Tinggi Teknologi Informasi NIIT (I-Tech)

3.2. Misi

Misi dari CSIRT-ITECH, yaitu :

a. Menyediakan respons yang cepat dan efektif terhadap insiden keamanan siber untuk melindungi aset informasi, menjaga integritas data, dan memastikan kelangsungan operasional di STTI NIIT
b. Mengimplementasikan langkah-langkah pencegahan yang proaktif untuk mengurangi kemungkinan terjadinya insiden keamanan.
c. Menyediakan pelatihan dan sumber daya untuk meningkatkan kesadaran keamanan siber di kalangan staf, mahasiswa, dan pemangku kepentingan lainnya.

3.3. Konstituen

Konstituen CSIRT-ITECH adalah seluruh civitas akademika di lingkungan Sekolah Tinggi Teknologi Informasi NIIT (I-Tech)

3.4. Sponsorship dan/atau Afiliasi

Pendanaan CSIRT-ITECH bersumber dari Sekolah Tinggi Teknologi Informasi NIIT (I-Tech)

3.5. Otoritas

Memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber pada lingkungan Sekolah Tinggi Teknologi Informasi NIIT (I-Tech).

4. Kebijakan – Kebijakan

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

CSIRT-ITECH melayani penanganan insiden siber dengan jenis berikut :

a. Web defacement
b. DoS / DDoS
c. Malware
d. Phising
e. Pembajakan akun UK Petra
f. Akses ilegal
g. Spam

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

CSIRT-ITECH kan melakukan kerja sama dan berbagi informasi dengan CSIRT dari Kementerian dan atau Lembaga lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh CSIRT-ITECH akan dirahasiakan

4.3. Komunikasi dan Autentikasi

Komunikasi dan Autentikasi untuk komunikasi biasa CSIRT-ITECH dapat

menggunakan alamat e-mail tanpa enkripsi data (e-mail konvensional) dan telepon.

Komunikasi terkait laporan insiden dan pertukaran informasi ancaman insiden lainnya dapat menggunakan saluran komunikasi yang disediakan (e-mail dan whatsapp) yang telah terenkripsi atau dilengkapi dengan kata sandi.

5. Layanan

5.1. Layanan Utama

Layanan utama dari CSIRT-ITECH yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini bertujuan untuk memberikan informasi dan peringatan kepada organisasi atau individu mengenai potensi ancaman dan kerentanan yang dapat mempengaruhi keamanan sistem informasi mereka. Pemberian peringatan ini mencakup beberapa aspek, antara lain:

- **Monitoring Ancaman:** CSIRT-ITECH secara aktif memantau perkembangan ancaman siber, termasuk malware, serangan phishing, dan kerentanan perangkat lunak. Informasi ini dikumpulkan dari berbagai sumber, termasuk laporan keamanan, komunitas siber, dan penelitian.
- **Pemberitahuan Dini:** Setelah mengidentifikasi ancaman yang relevan, CSIRT-ITECH akan mengeluarkan peringatan dini kepada pihak-pihak yang berpotensi terpengaruh. Peringatan ini dapat berupa buletin, email, atau notifikasi melalui platform tertentu.
- **Rekomendasi Tindakan:** Selain memberikan informasi tentang ancaman, layanan ini juga mencakup rekomendasi tindakan yang dapat diambil oleh organisasi untuk melindungi diri mereka. Ini bisa termasuk pembaruan perangkat lunak, penguatan kebijakan keamanan, atau pelatihan bagi karyawan.
- **Edukasi dan Kesadaran:** CSIRT-ITECH juga berperan dalam meningkatkan kesadaran tentang keamanan siber melalui seminar, workshop, dan materi edukasi lainnya, sehingga organisasi dapat lebih siap menghadapi ancaman yang ada.

5.1.2. Penanganan Insiden Siber

Layanan penanganan insiden siber berfokus pada respons dan pemulihan dari insiden keamanan yang telah terjadi. Proses ini melibatkan beberapa langkah penting, antara lain:

- **Deteksi Insiden:** CSIRT-ITECH membantu organisasi dalam mendeteksi insiden keamanan siber melalui analisis log, pemantauan sistem, dan penggunaan alat deteksi intrusi. Deteksi yang cepat sangat penting untuk meminimalkan dampak dari insiden.
- **Respons Insiden:** Setelah insiden terdeteksi, tim CSIRT-ITECH akan segera merespons dengan melakukan analisis untuk menentukan sifat dan

skala insiden. Ini termasuk mengidentifikasi sumber serangan, jenis data yang terpengaruh, dan potensi kerugian.

- **Mitigasi dan Pemulihan:** Tim akan mengambil langkah-langkah untuk mengurangi dampak insiden, seperti memutuskan akses ke sistem yang terpengaruh, menghapus malware, dan memperbaiki kerentanan. Setelah mitigasi, fokus beralih ke pemulihan sistem agar dapat beroperasi kembali dengan aman.
- **Pascainsiden:** Setelah insiden ditangani, CSIRT-ITECH melakukan evaluasi untuk memahami penyebab insiden dan mengidentifikasi langkah-langkah pencegahan yang dapat diambil di masa depan. Ini termasuk pembaruan kebijakan keamanan, pelatihan tambahan untuk staf, dan peningkatan infrastruktur keamanan.
- **Laporan dan Dokumentasi:** Layanan ini juga mencakup penyusunan laporan insiden yang mendetail, yang dapat digunakan untuk analisis lebih lanjut dan sebagai referensi untuk perbaikan di masa mendatang.

5.2. Layanan Tambahan

Layanan tambahan dari CSIRT-ITECH yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini berfokus pada identifikasi, analisis, dan mitigasi kerawanan yang ada dalam sistem elektronik, termasuk perangkat keras dan perangkat lunak. Proses ini meliputi:

- **Identifikasi Kerawanan:** Melakukan pemindaian dan analisis untuk menemukan kerentanan dalam sistem yang dapat dieksploitasi oleh penyerang.
- **Penyusunan Rencana Mitigasi:** Mengembangkan strategi untuk mengatasi kerawanan yang teridentifikasi, termasuk pembaruan perangkat lunak, penguatan konfigurasi, dan penerapan kontrol keamanan tambahan.
- **Uji Coba dan Validasi:** Melakukan pengujian untuk memastikan bahwa langkah-langkah mitigasi yang diambil efektif dalam mengurangi risiko.

5.2.2. Penanganan Artefak Digital

Layanan ini berkaitan dengan pengelolaan dan analisis artefak digital yang dihasilkan selama insiden siber atau aktivitas mencurigakan. Ini mencakup:

- **Pengumpulan Artefak:** Mengumpulkan data dan bukti digital dari sistem yang terpengaruh, seperti log, file, dan jejak aktivitas pengguna.
- **Analisis Forensik:** Melakukan analisis forensik untuk memahami bagaimana insiden terjadi, termasuk metode yang digunakan oleh penyerang dan dampak yang ditimbulkan.
- **Dokumentasi dan Pelaporan:** Menyusun laporan yang mendetail mengenai temuan analisis untuk digunakan dalam proses hukum atau untuk perbaikan keamanan di masa depan.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini bertujuan untuk memberikan informasi terkini mengenai potensi ancaman yang dapat mempengaruhi organisasi. Proses ini meliputi:

- **Monitoring Ancaman:** Memantau berbagai sumber informasi untuk mengidentifikasi ancaman baru yang muncul, termasuk tren serangan dan teknik yang digunakan oleh penyerang.
- **Pemberitahuan kepada Klien:** Menginformasikan klien tentang potensi ancaman yang relevan, termasuk rekomendasi untuk mitigasi.
- **Edukasi dan Kesadaran:** Memberikan informasi tambahan untuk meningkatkan kesadaran tentang ancaman yang ada dan cara melindungi diri.

5.2.4. Pendeteksian Serangan

Layanan ini berfokus pada identifikasi serangan yang sedang berlangsung atau yang telah terjadi. Ini mencakup:

- **Penggunaan Alat Deteksi:** Mengimplementasikan sistem deteksi intrusi (IDS) dan alat pemantauan lainnya untuk mendeteksi aktivitas mencurigakan dalam jaringan.
- **Analisis Log:** Menganalisis log sistem dan jaringan untuk menemukan pola yang menunjukkan adanya serangan.
- **Respons Cepat:** Mengambil tindakan segera untuk mengatasi serangan yang terdeteksi, termasuk isolasi sistem yang terpengaruh dan pemberitahuan kepada tim keamanan.

5.2.5. Analisis Risiko Keamanan Siber

Layanan ini bertujuan untuk mengevaluasi risiko yang dihadapi oleh organisasi terkait keamanan siber. Proses ini meliputi:

- **Identifikasi Aset dan Ancaman:** Mengidentifikasi aset penting yang perlu dilindungi dan ancaman yang dapat mempengaruhi aset tersebut.
- **Penilaian Kerentanan:** Menganalisis kerentanan yang ada dalam sistem dan infrastruktur organisasi.
- **Evaluasi Risiko:** Menghitung tingkat risiko berdasarkan kemungkinan terjadinya ancaman dan dampaknya terhadap organisasi, serta memberikan rekomendasi untuk mitigasi.

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Layanan ini memberikan dukungan kepada organisasi dalam mempersiapkan diri untuk menghadapi insiden siber. Ini mencakup:

- **Penilaian Kesiapan:** Melakukan evaluasi terhadap kebijakan, prosedur, dan infrastruktur yang ada untuk menangani insiden siber.
- **Pengembangan Rencana Respons Insiden:** Membantu organisasi dalam menyusun rencana respons insiden yang efektif, termasuk peran dan tanggung jawab tim.
- **Pelatihan dan Simulasi:** Menyediakan pelatihan dan simulasi untuk meningkatkan keterampilan tim dalam menangani insiden siber.

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Layanan ini bertujuan untuk meningkatkan kesadaran dan kepedulian terhadap keamanan siber di dalam organisasi. Ini mencakup:

- **Program Edukasi:** Mengembangkan program pelatihan untuk karyawan mengenai praktik terbaik keamanan siber, termasuk pengenalan terhadap ancaman dan cara melindungi informasi.
- **Kampanye Kesadaran:** Melaksanakan kampanye untuk meningkatkan kesadaran tentang pentingnya keamanan siber di seluruh organisasi.
- **Evaluasi dan Umpan Balik:** Mengukur efektivitas program kesadaran dan melakukan penyesuaian berdasarkan umpan balik dari peserta.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt[at]i-tech[dot]ac[dot]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*

Penanganan insiden tergantung dari ketersediaan sumber aya yang dimiliki oleh Sekolah Tinggi Teknologi Informasi NIIT (I-Tech).