RFC 2350 CSIRT Blibli

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi *3.0,* yang menggantikan dokumen versi sebelumnya*(v.2.0)* yang terbit pada 30 September 2022 yang menggantikan versi *1.0* yang terbit pada tanggal 7 Mei 2021.
Dokumen *v.3.0* dipublikasikan pada 1 Desember 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 portal berikut:
https://github.com/CSIRT-BLIBLI/CSIRT-Blibli--RFC-2350/new/main

1.4. Keaslian Dokumen

Dokumen asli terdapat 3 jenis, berbahasa Indonesia, berbahasa Inggris, dan file txt berbahasa Indonesia. Ketiga dokumen telah ditanda tangani dengan PGP *Key* milik CSIRT Blibli. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	:	RFC2350
Versi	:	3.0
Tanggal Publikasi	:	1 Desember 2024
Kadaluarsa	:	Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Kepanjangan dari	:	Cyber Security Incident Response Team - Blibli
Disingkat	:	CSIRT Blibli

2.2. Alamat

Gedung Sarana Jaya Lt. 2 Jl Budi Kemuliaan 1 No. 1, Gambir, Jakarta Pusat, DKI Jakarta, Indonesia, 10110

2.3. Zona Waktu

Jakarta (GMT +07:00)

2.4. Nomor Telepon

+62-21-50881370

2.5. Nomor Fax

Tidak ada

2.6. Telekomunikasi Lain

Tidak ada

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

Csirt@gdn-commerce.com

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

Kami menggunakan PGP untuk pertukaran informasi (pemberitahuan, pelaporan insiden, dll.) dengan rekan, mitra, dan konstituen.

Key ID : dee236a05415bc86

Key Fingerprint : 27AD1B137D8CA1A686F87711DEE236A05415BC86

PGP Public Key:

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

mDMEZ0Uv8xYJKwYBBAHaRw8BAQdAfgi3PzelcdxVJEEZ4fOx9JRD7sAT+PtCviMb
FxT4/460HkNTSVJUIDxjc2lydEBnZG4tY29tbWVyY2UuY29tPoiZBBMWCgBBAhsD
BQsJCAcCAiICBhUKCQgLAgQWAgMBAh4HAheAFiEEJ60bE32MoaaG+HcR3uI2oFQV
vIYFAme1aVkFCS9kWWAACgkQ3uI2oFQVvIbhvwD/Qxg/MBwUzRawhoZfNFtw6ANG
5m7lAa9XhAMq6cL3Qw0A/0nk7hAOl3yrWz379d8smaA1QtBehmOEZQNaMAWwHzgO
uDgEZ0Uv8xIKKwYBBAGXVQEFAQEHQN8kcZXTDvOuk3hUP0hswO8N3SFs3NxwFfOd
dzhIipJMAwEIB4h+BBgWCgAmAhsMFiEEJ60bE32MoaaG+HcR3uI2oFQVvIYFAme1
aWQFCS9kWWsACgkQ3uI2oFQVvIY8tgD/fCui8zlaUZ6BcCaLwsKIWIAd2QPcI+2r
PnfkUazWBSkBAOBIw0UeaLqn5jcO1Dd2hn9vTV8VQaXoVfVz+qkFytUL
=KUIf
-----END PGP PUBLIC KEY BLOCK-----
```

File PGP *key* ini tersedia pada portal Perusahaan

2.9. Anggota Tim

Ketua CSIRT Blibli adalah Coordinator Computer Security Incident yang ditunjuk. Untuk anggota tim CSIRT terdiri dari personnel yang berada pada Unit Information Security di Blibli.

2.10. Informasi/Data lain

Tidak ada

2.11. Catatan-catatan pada Kontak CSIRT Blibli

Metode yang disarankan untuk menghubungi CSIRT Blibli adalah melalui *e-mail* pada alamat csirt@gdn-commerce.com atau melalui nomor telepon +62-2150881370.

3. Mengenai CSIRT Blibli

3.1. Visi

Meningkatkan pengalaman perdagangan digital melalui peningkatan keamanan siber.

3.2. Misi

Misi dari CSIRT Blibli, yaitu :

a. Memberikan pelayanan teknologi yang bertujuan terbentuknya ketahanan dan kehandalan siber yang menunjang tujuan bisnis

b. Memberikan edukasi dan kesadaran siber pada karyawan serta pihak lain yang terkait dengan tujuan meningkatkan ketahanan siber

c. Memberikan informasi temuan kerentanan, potensi serangan serta informasi tentang intelijen siber lainnya yang bertujuan agar terbentuknya ekosistem ketahanan siber

3.3. Konstituen

Konstituen CSIRT Blibli meliputi seluruh pengguna teknologi informasi di lingkungan Perusahaan.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan CSIRT Blibli bersumber dari anggaran perusahaan.

3.5. Otoritas

1. Menentukan penilaian tingkat keamanan informasi pada proses bisnis yang sedang atau yang akan berlangsung
2. Melakukan penilaian tingkat keamanan sistem informasi yang dibuat secara sendiri (in-house), atau disewa/dibeli ke pihak ketiga
3. Melakukan pengawasan serta intervensi aktif terhadap operasional sistem informasi dalam rangka pemenuhan ketahanan dan keandalan siber yang menunjang tujuan bisnis
4. Merencanakan, membuat dan mengoperasikan rancang bangun mekanisme pertahanan berlapis siber (*cyber defense-in-depth*)
5. Melaksanakan program kesadaran keamanan siber bersama stakeholder terkait

6. Memiliki otoritas penuh untuk melaksanakan koordinasi dan intervensi internal dan eksternal, akses terhadap data dan sistem dalam hal penanganan insiden siber
7. Berwenang untuk melakukan pengelolaan insiden keamanan TI secara proaktif dan reaktif.

4. Kebijakan – Kebijakan

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

CSIRT Blibli melayani penanganan insiden siber di Perusahaan dengan jenis berikut:

- Layanan utama
  - Pemberian peringatan terkait keamanan siber
  - Penanganan insiden siber

- Layanan tambahan
  - Penanganan kerawanan sistem elektronik
  - Penanganan artefak digital
  - Pemberitahuan hasil pengamatan potensi ancaman
  - Pendeteksian serangan
  - Analisis risiko keamanan siber
  - Konsultasi terkait kesiapan penanganan insiden siber
  - Pembangunan kesadaran dan kepedulian terhadap keamanan siber Penanganan insiden tertentu yang belum termasuk dalam daftar di atas.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

CSIRT Blibli akan melakukan kerjasama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh CSIRT Blibli akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi bersifat biasa ke CSIRT Blibli dapat menggunakan e-mail tanpa enkripsi data khusus (e-mail konvensional) dan telepon. Namun, untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi PGP/RSA pada e-mail atau lampiran email.

5. Layanan

5.1. Layanan Utama

Layanan utama dari CSIRT Blibli yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini akan dilaksanakan oleh CSIRT Blibli yang berupa peringatan akan adanya ancaman siber kepada pemilik/penyelenggara sistem elektronik.

5.1.2. Penanganan Insiden Siber

Layanan penanganan insiden siber mencakup siklus penuh penanganan insiden. Penanganan dapat dilaksanakan dengan on-site secara langsung atau pemberian saran penanganan untuk ditindaklanjuti.

5.2. Layanan Tambahan (ikut IETF CSIRT Blibli - Proactive Activities) Layanan tambahan dari CSIRT Blibli yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

- Layanan ini berupa koordinasi, analisis dan rekomendasi teknis dalam rangka penguatan aspek kendali keamanan *(security control)* baik dalam lingkup teknis ataupun non-teknis (*Policy/Governance)*.
- Secara umum penanganan ini dibagi menjadi :
    - Pelaporan kerawanan yang bersifat sewaktu oleh pemilik/penyelenggara sistem elektronik milik konstituen
    - Layanan penanganan kerawanan sebagai tindak lanjut dari kegiatan audit atau *vulnerability assessment*

5.2.2. Penanganan Artefak Digital

Layanan penanganan artefak digital dilakukan dalam rangka menjaga sebaik mungkin proses *chain-of-custody* yang mungkin diperlukan dalam rangka penyidikan oleh penegak hukum atau sebagai sarana investigasi teknis insiden.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini diberikan dari hasil pengamatan oleh fungsi intelijen siber milik CSIRT Blibli terhadap aset digital milik konstituen.

5.2.4. Pendeteksian Serangan

Layanan ini diberikan apabila CSIRT Blibli memiliki visibilitas atas sistem keamanan yang diterapkan oleh konstituen, serangan pada konstituen akan dikorelasikan untuk memperkuat postur secara keseluruhan

5.2.5. Analisis Risiko Keamanan Siber

Layanan ini diberikan dengan tujuan sebagai fungsi perkiraan terhadap *attack surface* milik konstituen, layanan ini diberikan secara berkala sesuai dengan periode audit kepatuhan

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Layanan konsultasi ini diberikan dalam rangka membantu para konstituen agar memiliki kesiapan yang cukup dalam menghadapi insiden siber

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Layanan ini diberikan kepada konstituen dalam rangka membangun *people-processtechnology* untuk menunjang program edukasi kesadaran keamanan informasi yang berkelanjutan

6. Pelaporan Insiden

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

a. Informasi: Nama Lengkap, Jabatan, No HP dan Konstituen asal
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan
c. Bukti atau informasi lain sesuai dengan kebutuhan penanganan insiden atau ketentuan yang berlaku

7. *Disclaimer*

Tidak ada