2022

RFC 2350 CSIRT Blibli.com

Version 2.0
September 2022
Klasifikasi: Public
CSIRT Blibli.com, CSIRT Di PT Global Digital Niaga

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 2.0, yang menggantikan dokumen versi sebelumnya(v.1.0) yang terbit pada tanggal 7 Mei 2021. Dokumen v.2.0 dipublikasikan pada 30 September 2022.

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://github.com/bliblidotcom/CSIRT-RFC2350/blob/main/Blibli-RFC2350.txt

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.com. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5. Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Title	:	RFC2350
Version	:	2.0
Document Date	:	30 September 2022
Expiration	:	This document is valid until superseded by a later version

2. Informasi Data/Kontak

2.1. Nama Tim

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

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, Indonesia (GMT+7)

2.4. Nomor Telepon

+62-21-50881370

2.5. Nomor Fax

N/A

2.6. Telekomunikasi Lain

N/A

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.

Bits : ECC with ed25519 curve
Key ID : 6C1B FF5F 9288 EF68
Key Fingerprint : 521D 5789 07E8 29FF 58EF 9E69 6C1B FF5F 9288 EF68
Blok PGP Public Key :

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

mDMEYLh8hBYJKwYBBAHaRw8BAQdAWWuz90wSsQ4U0tVWudzo8ncBbIXyTiTwPtK0
T58gbia0W0NTSVJUIEJsaWJsaS5jb20gKEN5YmVyc2VjdXJpdHkgSW5jaWRlbnQg
UmVzcG9uc2UgVGVhbSBCbGlibGkuY29tKSA8Y3NpcnRAZ2RuLWNvbW1lcmNlLmNv
bT6IlAQTFgoAPBYhBFIdV4kH6Cn/WO+eaWwb/1+SiO9oBQJguHyEAhsDBQsJCAcC
AyICAQYVCgkICwIEFgIDAQIeBwIXgAAKCRBsG/9fkojvaB1+APwLQlLbUz6Dxc7x
p1QFUZKdJAl7VkrtF9PvEF6thA2lcwEAomyXpd6OrP/wyDc3O6E5JYX8TfyedMXD
+npdLtZrYwK4OARguHyEEgorBgEEAZdVAQUBAQdA4K/iBUjmPc3Tp0YV78OuLkPA
2NsSG9Zzf+nIxI7x2iQDAQgHiHgEGBYKACAWIQRSHVeJB+gp/1jvnmlsG/9fkojv
aAUCYLh8hAIbDAAKCRBsG/9fkojvaB23AP4nc1AaBwwIRvfCxXYGSM2fVRlFR2tX
clsRYkEotFHxkgEApQoXBRo2wolOh0P+EYPVF3Dn9sHbYZ26+3x3s3CBXwk=
=vhQT
-----END PGP PUBLIC KEY BLOCK-----
```

File PGP *key* ini tersedia pada :
https://github.com/bliblidotcom/CSIRT-RFC2350/blob/main/CSIRT-Blibli.pub

2.9. Anggota Tim

Ketua CSIRT Blibli.com adalah Rendra Perdana Satria, yang dibantu oleh tim yang terdiri dari 40 anggota staf.

2.10. Informasi/Data lain

N/A

2.11. Catatan-catatan pada Kontak CSIRT Blibli.com

Metode yang disarankan untuk menghubungi CSIRT Blibli.com adalah melalui *e-mail* pada alamat csirt@gdn-commerce.com atau melalui nomor telepon +62-21-50881370 yang siaga selama 24 H.

3. Mengenai CSIRT Blibli.com

3.1. Visi & Misi

3.1.1. Visi

Meningkatkan pengalaman perdagangan digital melalui peningkatan keamanan siber

3.1.2. Misi

Misi dari CSIRT Blibli.com, yaitu :

1. Memberikan pelayanan teknologi yang bertujuan terbentuknya ketahanan dan kehandalan siber yang menunjang tujuan bisnis
2. Memberikan edukasi dan kesadaran siber pada karyawan serta pihak lain yang terkait dengan tujuan meningkatkan ketahanan siber
3. Memberikan informasi temuan kerentanan, potensi serangan serta informasi tentang intelijen siber lainnya yang bertujuan agar terbentuknya ekosistem ketahanan siber

3.2. Konstituen

Konstituen CSIRT Blibli.com meliputi :

1. PT Global Digital Niaga
2. PT Global Kassa Sejahtera
3. PT Digital Otomotif Indonesia

3.3. Sponsorship dan/atau Afiliasi

Pendanaan CSIRT Blibli.com bersumber secara swasta

3.4. Otoritas

1. Menentukan asesmen tingkat keamanan informasi pada proses bisnis yang sedang atau yang akan berlangsung
2. Melakukan asesmen 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

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/Level Dukungan

CSIRT Blibli.com melayani penanganan insiden siber dengan jenis berikut :

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

☐ Layanan tambahan
- X Penanganan kerawanan sistem elektronik
- X Penanganan artefak digital
- X Pemberitahuan hasil pengamatan potensi ancaman
- X Pendeteksian serangan
- X Analisis risiko keamanan siber
- X Konsultasi terkait kesiapan penanganan insiden siber
- X Pembangunan kesadaran dan kepedulian terhadap keamanan siber

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

4.3. Komunikasi dan Autentikasi

Untuk komunikasi bersifat biasa ke CSIRT Blibli.com 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.com yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini akan dilaksanakan oleh CSIRT Blibli.com 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.com - Proactive Activities)

Layanan tambahan dari CSIRT Blibli.com 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 :

1. Pelaporan kerawanan yang bersifat sewaktu oleh pemilik/penyelenggara sistem elektronik milik konstituen

2. 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.com terhadap aset digital milik konstituen.

5.2.4. Pendeteksian Serangan

Layanan ini diberikan apabila CSIRT Blibli.com 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-process-technology* 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

a) CSIRT blibli.com melaksanakan kegiatan respon insiden dengan menerapkan prinsip kerahasiaan sebagai prinsip kerja, pembagian informasi ke para pihak akan dilakukan dengan menerapkan prinsip *need-to-know*

b) CSIRT blibli.com menyediakan layanan konsultasi dengan lingkup terbatas dengan tujuan ketahanan siber bersama dengan usaha semaksimal mungkin, kami tidak dapat menjamin hasil akhir secara pasti dari pekerjaan yang tercantum pada daftar layanan

c) Kami tidak bertanggung jawab atas kebenaran dan/atau kecepatan dari laporan terkait diseminasi informasi ancaman

d) CSIRT blibli.com hanya menyediakan sarana komunikasi melalui kanal yang tercantum pada RFC2350, kami tidak bertanggung jawab atas komunikasi yang mengatasnamakan CSIRT Blibli.com melalui kanal lain

rendra.satria@gdn-commerce.com
2022.10.06 10:44:47 +07'00'