Diskominfo Kalbar ungkap jumlah percobaan serangan siber 165.607 kali

Sumber Gambar:// kalbar.antaranews.com/

Isi Berita:

Pontianak (ANTARA) - Kepala Bidang Persandian dan Statistik Diskominfo Kalbar, Maria Wijayanti mengungkapkan berdasarkan data dari Honeynet Badan Siber dan Sandi Negara menunjukkan bahwa jumlah percobaan serangan siber di Kalimantan Barat mencapai 165.607 kali dari tanggal 1 Januari 2024 hingga 05 Mei 2024.

"Hal ini tentu menjadi peringatan bagi semua pihak, khususnya setiap OPD dan instansi yang ada di Kalimantan Barat akan pentingnya menjaga keamanan informasi di lingkungan kerjanya masing-masing," kata Maria di Pontianak, Minggu.

Maria mengatakan, untuk menanggapi insiden tersebut, Dinas Komunikasi dan Informatika Provinsi Kalimantan Barat telah membentuk Kalbarprov-CSIRT sebagai tim tanggap insiden siber.

Beberapa langkah telah diambil oleh tim ini, termasuk pemantauan dan identifikasi terhadap situs web dan aplikasi yang terkait dengan judi online, serta analisis dan penangguhan layanan pada aplikasi yang terdampak insiden judi online hingga sistem dinyatakan aman kembali.

Selain itu pihaknya juga telah menggelar Literasi Budaya Keamanan Siber dengan tema "Lesson Learn dan Mitigasi Pasca Insiden Web Defacement" yang diikuti sejumlah pihak terkait dengan keamanan siber, untuk meningkatkan keamanan informasi pada instansi yang mereka tangani.

Maria Wijayanti selaku Kepala Bidang Persandian dan Statistik Diskominfo Kalbar mengatakan kegiatan ini sangat penting mengingat insiden baru-baru ini terkait dengan web defacement yang terjadi di lingkungan pemerintah Provinsi Kalimantan Barat.

"Kegiatan literasi ini diharapkan dapat menjadi sarana pembelajaran bagi semua peserta, sehingga mereka dapat lebih memahami langkah-langkah yang perlu dilakukan untuk mencegah dan meningkatkan literasi keamanan informasi di Kalimantan Barat," kata Maria.

Sumber Berita :

1. https://kalbar.antaranews.com/berita/578202/diskominfo-kalbar-ungkap-jumlah-percobaan-serangan-siber-165607-kali
2. https://www.suarakalbar.co.id/2024/05/serangan-siber-menggempur-kalbar-165-607-percobaan-serangan-tercatat-sejak-januari/

Catatan Berita :

Peraturan Presiden (PERPRES) Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, terdapat pengaturan sebagai berikut:

1. **Pasal 1 angka 1, menyatakan bahwa:**

   Keamanan Siber adalah upaya adaptif dan inovatif untuk melindungi seluruh lapisan ruang siber, termasuk aset informasi yang ada di dalamnya, dari ancaman dan serangan siber, baik yang bersifat teknis maupun sosial.

2. **Pasal 1 angka 2, menyatakan bahwa:**
   Strategi Keamanan Siber Nasional adalah arah kebijakan nasional dalam menggunakan seluruh sumber daya siber nasional untuk mewujudkan Keamanan Siber guna mempertahankan dan memajukan kepentingan nasional.

3. **Pasal 1 angka 3, menyatakan bahwa:**
   Insiden Siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam berjalannya sistem elektronik.

4. **Pasal 1 angka 1, menyatakan bahwa:**
   Krisis Siber adalah situasi kedaruratan akibat dari Insiden Siber pada tingkat nasional yang berdampak terhadap keselamatan, keutuhan, dan kedaulatan negara.

5. **Pasal 1 angka 1, menyatakan bahwa:**
   Manajemen Krisis Siber adalah tata kelola penggunaan sumber daya dan langkah penanganan secara efektif yang dilakukan sebelum, saat, dan setelah terjadinya Krisis Siber.

6. **Pasal 3, menyatakan bahwa:**
   Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber merupakan acuan bagi Instansi Penyelenggara Negara dan Pemangku Kepentingan untuk mewujudkan kekuatan dan kapabilitas siber dalam rangka mencapai stabilitas Keamanan Siber.

7. **Pasal 4, menyatakan bahwa:**
   Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber bertujuan:
   a. *mewujudkan Keamanan Siber;*
   b. *melindungi ekosistem perekonomian digital nasional;*
   c. *meningkatkan kekuatan dan kapabilitas Keamanan Siber yang andal dan berdaya tangkal; dan*
   d. *mengutamakan kepentingan nasional dan mendukung terciptanya ruang siber global yang terbuka, aman, stabil, dan bertanggung jawab.*

8. **Pasal 5, menyatakan bahwa:**
   Strategi Keamanan Siber Nasional terdiri atas:
   a. *fokus area; dan*
   b. *rencana aksi nasional Keamanan Siber.*

9. **Pasal 6, menyatakan bahwa:**
   Fokus area Strategi Keamanan Siber Nasional sebagaimana dimaksud dalam Pasal 5 huruf a terdiri atas:
   a. *tata kelola;*
   b. *manajemen risiko;*
   c. *kesiapsiagaan dan ketahanan;*
   d. *penguatan pelindungan infrastruktur informasi vital;*
   e. *kemandirian kriptografi nasional;*
   f. *peningkatan kapabilitas, kapasitas, dan kualitas;*
   g. *kebijakan Keamanan Siber; dan*
   h. *kerja sama internasional.*

10. **Pasal 15, menyatakan bahwa:**
    a. *Ayat (1), Rencana aksi nasional Keamanan Siber sebagaimana dimaksud dalam Pasal 5 huruf b merupakan rencana aksi tingkat nasional yang berisi upaya terencana dan terukur untuk menjabarkan dan mengimplementasikan fokus area Strategi Keamanan Siber Nasional.*
    b. *Ayat (2), Rencana aksi nasional Keamanan Siber disusun untuk jangka waktu 5 (lima) tahun.*
    c. *Ayat (3), Rencana aksi nasional Keamanan Siber sebagaimana dimaksud pada ayat (1) dapat ditinjau sewaktu-waktu.*
    d. *Ayat (4), Rencana aksi nasional Keamanan Siber sebagaimana dimaksud pada ayat (1) memperhatikan:*
       1) *rencana pembangunan nasional;*
       2) *perkembangan ilmu pengetahuan dan teknologi; dan*
       3) *perkembangan lingkungan strategis.*
    e. *Ayat (5), Rencana aksi nasional Keamanan Siber sebagaimana dimaksud pada ayat (1) paling sedikit memuat:*
       1) *kegiatan;*
       2) *indikator keberhasilan;*
       3) *waktu pelaksanaan; dan*
       4) *penanggung jawab.*

f. *Ayat (6), Rencana aksi nasional Keamanan Siber sebagaimana dimaksud pada ayat (1) disusun oleh Badan dengan mengikutsertakan kementerian/lembaga terkait.*
g. *Ayat (7), Ketentuan lebih lanjut mengenai rencana aksi nasional Keamanan Siber sebagaimana dimaksud pada ayat (l) diatur dengan Peraturan Badan.*

11. Pasal 17, menyatakan bahwa:

a. *Ayat (1), Penyelenggaraan Manajemen Krisis Siber meliputi:*
   1) *sebelum Krisis Siber;*
   2) *saat terjadi Krisis Siber; dan*
   3) *setelah Krisis Siber.*
b. *Ayat (2), Penyelenggaraan Manajemen Krisis Siber sebagaimana dimaksud pada ayat (1) dikoordinasikan oleh Badan dengan mengikutsertakan PSE.*

12. Pasal 20, menyatakan bahwa:

Penyelenggaraan Manajemen Krisis Siber sebelum Krisis Siber sebagaimana dimaksud dalam Pasal 17 huruf a diselenggarakan paling sedikit melalui:

a. *tanggap Insiden Siber;*
b. *peringatan dini Krisis Siber; dan*
c. *penetapan status Krisis Siber.*

13. Pasal 24, menyatakan bahwa:

Penyelenggaraan Manajemen Krisis Siber saat terjadi Krisis Siber sebagaimana dimaksud dalam Pasal 17 huruf b paling sedikit meliputi:

a. *penanggulangan Krisis Siber;*
b. *pemulihan Krisis Siber;*
c. *pelaporan penanganan Krisis Siber; dan*
d. *pengakhiran status Krisis Siber.*

14. Pasal 29, menyatakan bahwa:

a. *Ayat (1), Penyelenggaraan Manajemen Krisis Siber setelah Krisis Siber sebagaimana dimaksud dalam Pasal 17 ayat (1) huruf c diselenggarakan paling sedikit meliputi:*
   1) *penghitungan perkiraan nilai kerusakan dan kerugian akibat Krisis Siber;*
   2) *penghitungan perkiraan biaya pemulihan akibat Krisis Siber; dan*
   3) *evaluasi penanganan Krisis Siber.*
b. *Ayat (2), Penyelenggaraan setelah Krisis Siber sebagaimana dimaksud pada ayat (1) dikoordinasikan oleh Badan dengan mengikutsertakan PSE.*

15. Pasal 34, menyatakan bahwa:

Pendanaan penyelenggaraan Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber bersumber dari:

a. *Anggaran Pendapatan dan Belanja Negara;*
b. *anggaran pendapatan dan belanja daerah; dan*
c. *sumber lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan.*