Studi Kasus dan Simulasi Penanganan Insiden Siber

2 November 2026

Tujuan Pembelajaran

Mengidentifikasi tindakan yang perlu diprioritaskan saat terjadi insiden siber

Menentukan langkah penanganan, pelaporan, dan eskalasi yang tepat

Menentukan keputusan berdasarkan perkembangan insiden dan dampaknya terhadap layanan publik



Fokus: Pengambilan keputusan, penentuan prioritas penanganan, serta koordinasi dan eskalasi insiden siber

Kanal Pelaporan dan Prosedur Eskalasi Insiden Siber

01 · Pelaporan Insiden

Laporkan insiden melalui kanal resmi CSIRT dan mekanisme pelaporan yg berlaku di instansi

02 · Informasi yang Disampaikan

Kronologi dan waktu kejadian, sistem terdampak, indikasi insiden, tindakan awal, serta bukti yang tersedia

03 · Koordinasi dan Eskalasi

Koordinasikan penanganan dengan CSIRT dan teruskan kepada pihak yang berwenang sesuai tingkat keparahan dan dampak insiden

04 · Penanganan dan tindak Lanjut

Lakukan penanganan sesuai prosedur, catat perkembangan kejadian, dan evaluasi hasil penanganan

!! **Laporkan insiden sesegara mungkin. Investigasi tidak harus selesai sebelum laporan awal disampaikan** !!

Kanal Pelaporan dan Prosedur Eskalasi Insiden Siber

01 · Pelaporan Insiden

Laporkan insiden melalui kanal resmi CSIRT dan mekanisme pelaporan yg berlaku di instansi

02 · Informasi yang Disampaikan

Kronologi dan waktu kejadian, sistem terdampak, indikasi insiden, tindakan awal, serta bukti yang tersedia

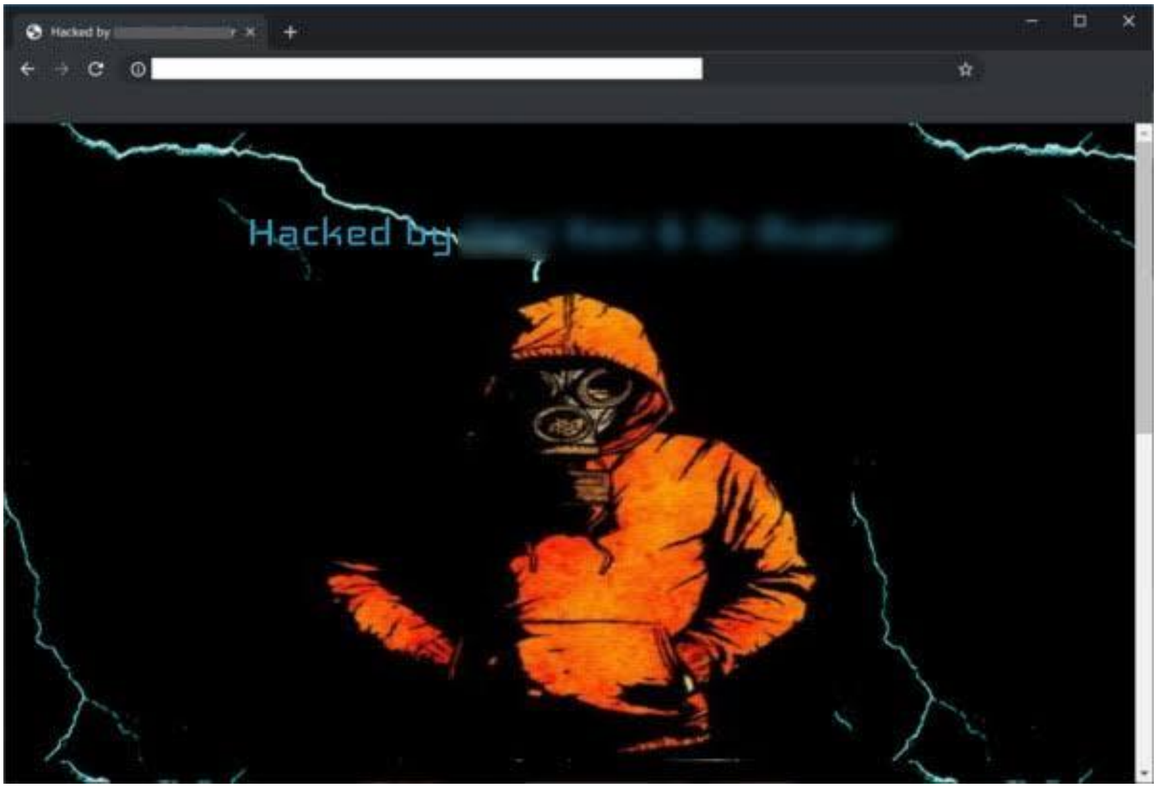
03 · Eskalasi Insiden

Koordinasikan dengan CSIRT dan pihak berwenang sesuai tingkat keparahan, dampak, dan kewenangan

04 · Penanganan dan tindak Lanjut

Lakukan penanganan, dokumentasikan perkembangan, dan evaluasi hasil perbaikan sesuai prosedur yang berlaku

!! **Laporkan insiden sesegara mungkin. Investigasi tidak harus selesai sebelum laporan awal disampaikan** !!

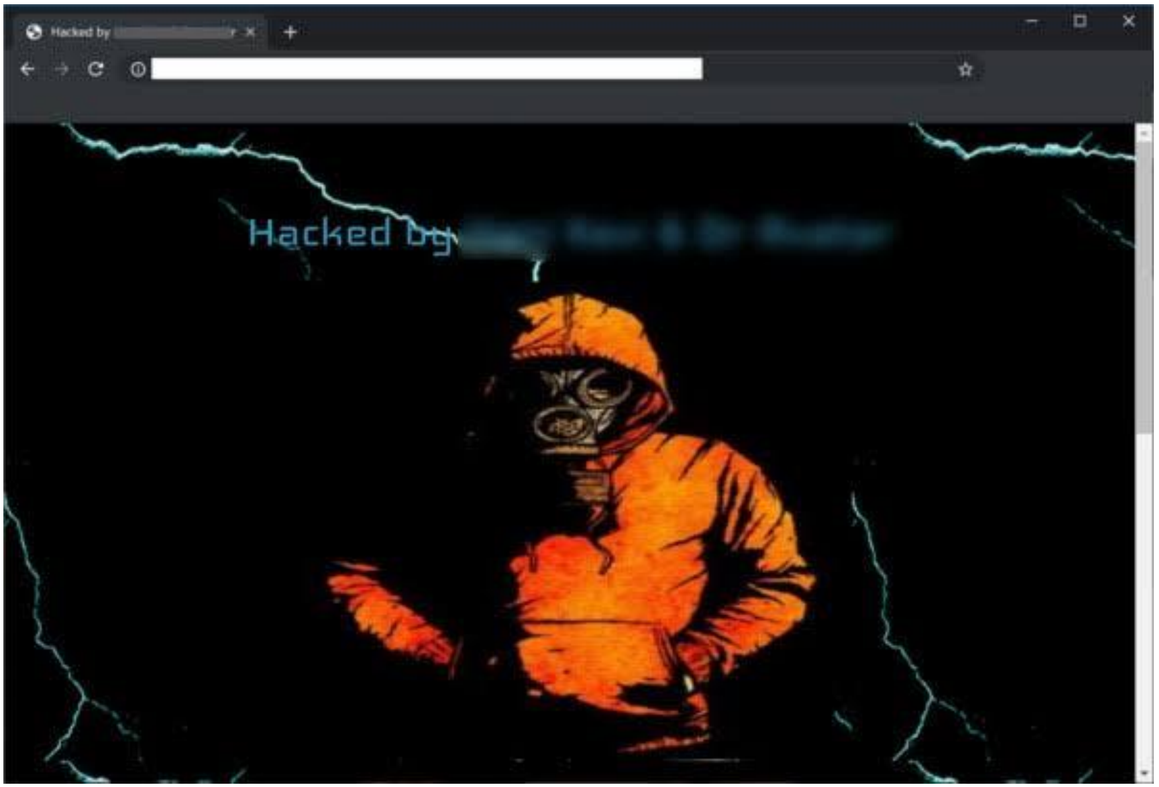


Petugas pengelola website pemerintah daerah menemukan bahwa tampilan website resmi berubah dan menampilkan pesan yang tidak semestinya. Website masih dapat diakses oleh masyarakat

Studi Kasus 1 • Web Defacement

Apa yang perlu dilakukan terlebih dahulu setelah mengetahui kejadian tersebut?

- Apa yang perlu dipastikan sebelum mengambil tindakan?
- Siapa yang perlu diberi laporan atau diajak berkoordinasi?
- Bukti apa yang perlu diamankan?
- Apakah website harus langsung dimatikan? apa pertimbangannya?

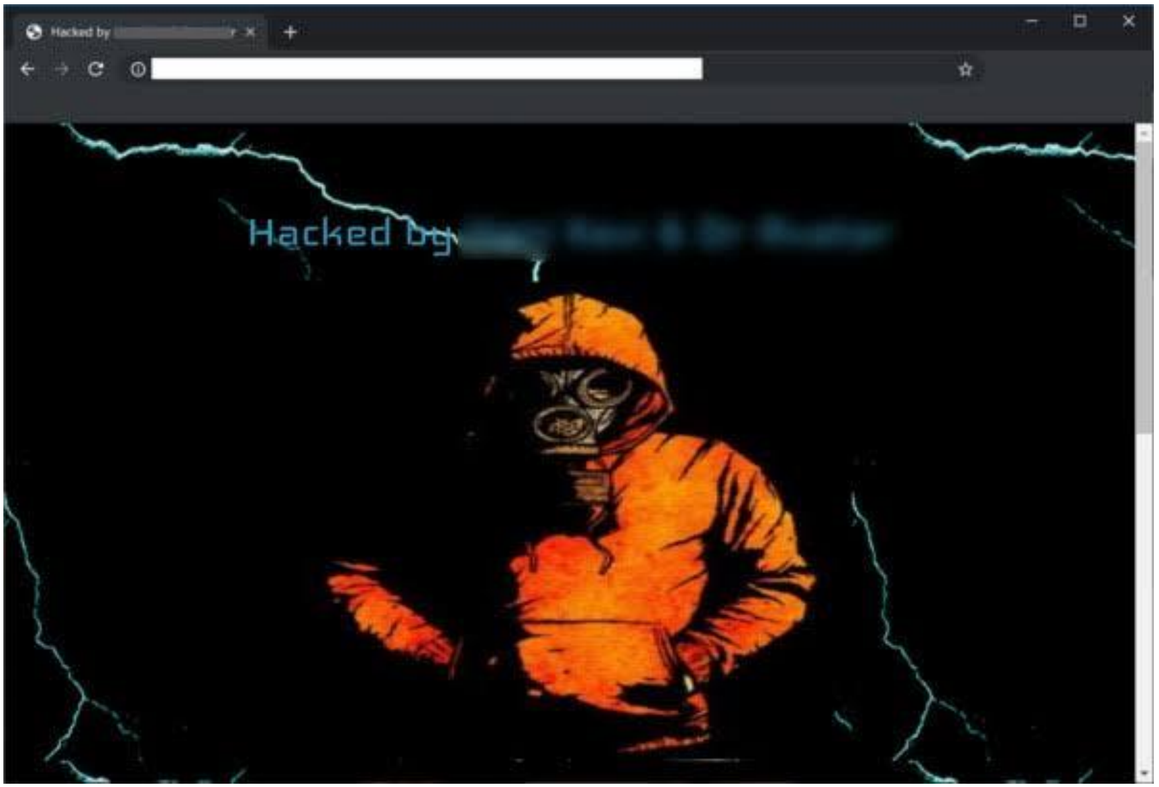


Setelah tampilan website diperbaiki, beberapa menit kemudian tampilan tersebut kembali berubah. Website masih dapat diakses oleh masyarakat

Perkembangan Kasus 1

- **Defacement Berulang**

Apakah memperbaiki tampilan website berarti insiden sudah selesai? Apa yang perlu dilakukan berikutnya



Website memuat informasi layanan publik yang dibutuhkan masyarakat. Jika website dimatikan, masyarakat dapat kesulitan mengakses informasi. Namun, jika tetap dijalankan, risiko keamanan mungkin masih ada

Dilema Keputusan • Keamanan vs. Layanan Publik

Apakah website perlu dipisahkan sementara dari sistem lain atau dimatikan? Bagaimana mempertimbangkan keamanan dan kebutuhan masyarakat?

Rangkuman Kasus 1 : Web Defacement

Website kembali normal bukan berarti insiden selesai

Penanganan harus disertai koordinasi dan penyimpanan bukti

Keamanan dan layanan publik harus dipertimbangkan bersama



Studi Kasus 2 • Dugaan Kebocoran Data

Apa yang perlu dilakukan ketika menemukan dugaan kebocoran data tersebut?

Dugaan Data di Pegawai Tersebar di Media Sosial

Petugas pemerintah daerah menemukan unggahan di media sosial yang diduga memuat data pegawai, seperti nama, jabatan, dan informasi pribadi lainnya. Belum diketahui apakah data tersebut benar berasal dari sistem pemerintah daerah

- Bagaimana memastikan apakah informasi tersebut benar?
- Bukti apa yang perlu diamankan?
- Kepada siapa dugaan insiden perlu dilaporkan?
- Apa yang harus dihindari agar penyebaran data tidak semakin luas?



Data Diduga Semakin Meluas Penyebarannya

Unggahan yang diduga memuat data pegawai mulai dibagikan oleh sejumlah akun lain. Namun, keaslian data dan sumber awal penyebarannya masih belum terkonfirmasi

Perkembangan Kasus 2

- **Unggahan Semakin Meluas**

Bagaimana memastikan kebenaran informasi dan menangani kejadian ini tanpa membuat data pribadi tersebar lebih luas?



Sumber Kebocoran Belum Teridentifikasi

Data yang beredar berpotensi merupakan data pribadi, tetapi belum ditemukan bukti yang memastikan bahwa berasal dari sistem pemerintah daerah

Dilema Keputusan • Melapor atau Menunggu Verifikasi?

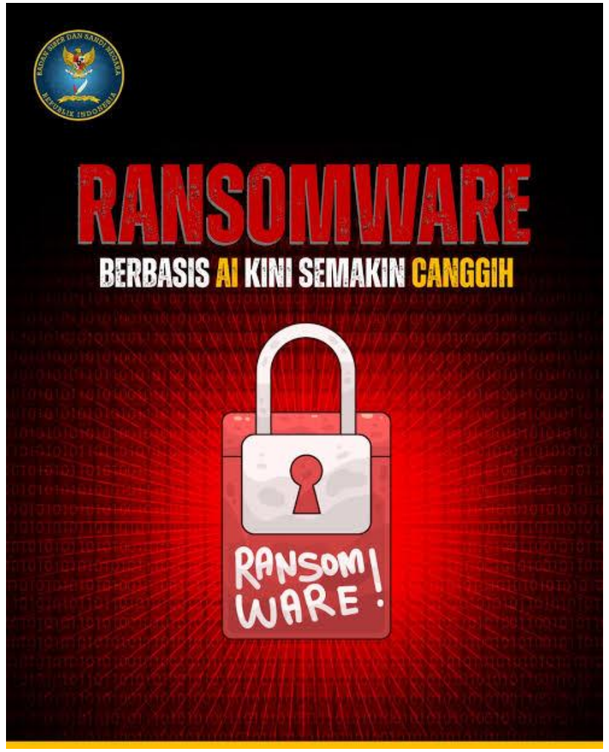
Apakah laporan harus menunggu sampai semua informasi terverifikasi? Apa yang dapat dilakukan sementara asal data belum diketahui?

Rangkuman Kasus 2 : Dugaan Kebocoran Data

Laporkan indikasi insiden tanpa menunggu semua informasi terverifikasi

Simpan bukti tanpa memperluas penyebaran data pribadi

Pastikan asal dan cakupan kebocoran melalui koordinasi

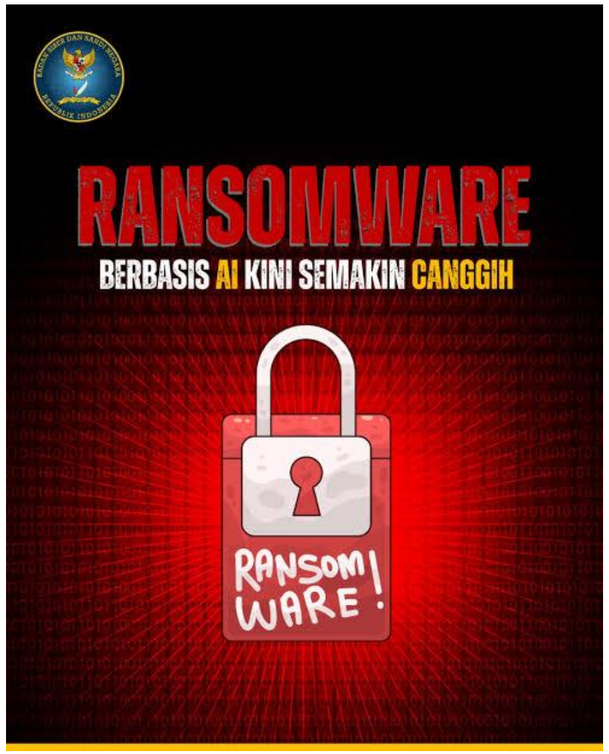


Sejumlah komputer di lingkungan pemerintah daerah menampilkan pesan yang meminta tebusan. Beberapa berkas tidak dapat dibuka, sehingga pekerjaan pada komputer tersebut terganggu

Studi Kasus 3 • Serangan Ransomware

Apa yang harus diprioritaskan saat terjadi serangan ransomware?

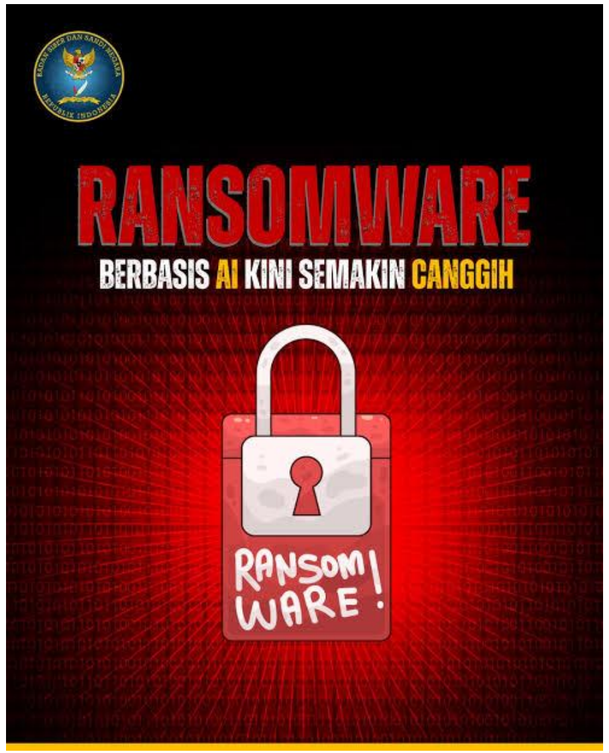
- Apa yang harus dilakukan untuk mencegah penyebaran serangan?
- Siapa yang perlu segera diberi laporan?
- Bukti apa yang perlu dikumpulkan?
- Apakah komputer yang terdampak perlu dimatikan?



Studi Kasus 3 • Gangguan Meluas

Unit kerja lain melaporkan gangguan serupa. Beberapa berkas tidak dapat dibuka, sehingga serangan diduga telah menyebar ke komputer lain

Bagaimana perkembangan ini memengaruhi langkah penanganan insiden?



Instansi memiliki cadangan data (backup) untuk memulihkan sistem. Namun, belum dipastikan apakah cadangan tersebut aman dari serangan ransomware.

Dilema Keputusan • Pemulihan Data

Apa yang perlu dipastikan sebelum instansi memulihkan data dari backup yang tersedia?

Rangkuman Kasus 3 : Ransomware

Batasi penyebaran dan identifikasi sistem yang terdampak

Laporkan insiden, koordinasikan penanganan, dan simpan bukti

Pastikan backup aman sebelum pemulihan sistem