

Security Trends & The Importance of Security Operations

Onno W. Purbo
onno@indo.net.id
onno@itts.ac.id
[@onnowpurbo](https://www.onnowpurbo.com)

Objectives

- Menjelaskan tren ancaman siber terkini
- Menunjukkan pentingnya Security Operations (SecOps)
- Mendukung transformasi digital yang aman & berkelanjutan



pdns.jebol



TEMPO.CO

<https://www.tempo.co> > politik > k... · Translate this page

Kronologi Pusat Data Nasional Jebol hingga Desakan ...

30 Jun 2024 — TEMPO.CO, Jakarta - **Serangan siber berupa ransomware pada Pusat Data Nasional Sementara 2 atau PDNS2** menyebabkan lumpuhnya server beberapa ...



Kompas.com

<https://nasional.kompas.com> > read · Translate this page

Pusat Data Nasional Jebol: Menkominfo Mundur atau ...

28 Jun 2024 — Artinya, jebolnya Pusat Data Nasional tersebut bukan karena kelemahan teknologi, tetapi pada kelalaian pegawai atau staf. Terbukti, kelalaian ...



Kompasiana.com

<https://www.kompasiana.com> > Vox Pop

PDNS Jebol, Kedaulatan Data Digital Terancam Hacker ...

28 Jun 2024 — Pusat Data Nasional Sementara (**PDNS**) mengalami serangan Ransomware pada hari Kamis, 20 Juni 2024.



kumparan

<https://kumparan.com> > pdns-jebo... · Translate this page

PDNS Jebol: Krisis Kepemimpinan yang Memicu Dampak



BSI bobol



Bank BSI Pasca Serangan Siber: Mengungkap Potensi ...

Namun, pada tanggal 14 Mei 2023, fakta baru terungkap bahwa **gangguan layanan BSI sebenarnya disebabkan oleh serangan ransomware** dari sekelompok hacker.



BBC

<https://www.bbc.com > articles> · [Translate this page](#)

BSI diduga kena serangan siber, pengamat sebut sistem ...

16 May 2023 — Menurut Pratama, ada indikasi gangguan di **BSI** adalah akibat serangan peretas alias hacker karena sistem mengalami mati total selama beberapa ...

Videos :



Hacker Lockbit Klaim Retas Sistem Bank BSI

YouTube · METRO TV
14 May 2023



Diduga Dihack, Server Bank BSI Down

YouTube · METRO TV
11 May 2023



Indicator

Keyword

Enter Keyword

Search

Global Breach

Schedule



ata Breach

Stealer Logs

Government Monitoring

Company Breach Monitoring

Ransomware Activity Monitoring

Darkweb Link Preview

Immediately

History

Scheduled

6/20

Onno W Purbo

Keyword : indonesia

Searched at 19 May 2025, 09:34

Export



Leak Title

Bad Actor

Detection Date (UTC+7)

Source URL

#

[INDONESIA] DATABASE MAHKAMAHAGUNG.GO.ID

XSVSHACKER

18 May 2025, 21:54

Not supported to FREE version

[INDONESIA] MPPDIGITAL.JABARPROV.GO.ID

gesss

18 May 2025, 21:49

Not supported to FREE version

Phone & Doxed For Indonesia Government Has Been...

Naisya

14 May 2025, 10:29

Not supported to FREE version

[INDONESIA] DISPERAKIM.JATENGPROV.GO.ID

gesss

11 May 2025, 12:30

Not supported to FREE version

[INDONESIA] LOGS ADMIN BPKSDM.MOJOKERTOKOTA.GO.ID

gesss

10 May 2025, 10:25

Not supported to FREE version

[INDONESIA] LOGS ADMIN KAPAL.DEPHUB.GO.ID

gesss

10 May 2025, 10:25

Not supported to FREE version

[ID] Indonesia Full Citizens - dukcapil.kemendagri.go.id 337.2M

DATABASE

14 Apr 2025, 15:24

Not supported to FREE version

magelangkota.go.id - Indonesian

System

14 Apr 2025, 15:23

Not supported to FREE version

Transformasi Digital dan Risiko Baru

- Digitalisasi = peluang + permukaan serangan makin luas
- Teknologi seperti AI, cloud, IoT tingkatkan efisiensi tapi juga risiko
- Keamanan = fondasi suksesnya digitalisasi

Ledakan Ancaman Siber

- 411.000 malware baru per hari (SAFEnet, 2024)
- Ransomware naik 37%
- Deepfake & AI untuk serangan manipulatif
- Target utama: data, sistem, dan trust

Biaya Serangan dan Regulasi

- Kerugian data breach global: \$4.45 juta (IBM, 2023)
- Regulasi: GDPR, UU PDP
- Ketidakpatuhan =
 - rusak reputasi
 - denda (Rp 50M + Sita)

KETENTUAN PIDANA

Pasal 67

- (1) Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).
- (2) Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).
- (3) Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

pidana dan pembayaran ganti kerugian.

Pasal 70

- (1) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 67 dan Pasal 68 dilakukan oleh Korporasi, pidana dapat dijatuhkan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan/atau Korporasi.
- (2) Pidana yang dapat dijatuhkan terhadap Korporasi hanya pidana denda.
- (3) Pidana denda yang dijatuhkan kepada Korporasi paling banyak 10 (sepuluh) kali dari maksimal pidana denda yang diancamkan.
- (4) Selain dijatuhi pidana denda sebagaimana dimaksud pada ayat (2), Korporasi dapat dijatuhi pidana tambahan berupa:
 - a. perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil dari tindak pidana;
 - b. pembekuan seluruh atau sebagian usaha Korporasi;
 - c. pelarangan permanen melakukan perbuatan tertentu;

Tren Teknologi Keamanan

Zero Trust Architecture	Verifikasi Setiap Akses
Security Orchestration, Automation, and Response (SOAR)	Otomatisasi deteksi & respons
Artificial Intelligence (AI)	Prediksi ancaman, vulnerability analysis
Machine Learning (ML)	Deteksi ancaman, ransomware
Secure Access Service Edge (SASE)	SD-WAN + network security services
Cloud Access Security Broker (CASB)	Perantara pengguna dan layanan cloud (Google Workspace, Microsoft 365, Salesforce).

Security Operations = Pilar Utama

- SecOps = perlindungan operasional menyeluruh
- Cegah downtime
- Lindungi data pelanggan & aset
- Sediakan ekosistem aman untuk inovasi

Komponen Kunci SecOps

- SIEM: pemantauan & korelasi real-time
- Incident Response: prosedur penanganan insiden
- Kolaborasi tim: IT, security, operasional

Manfaat Strategis SecOps

- Efisiensi: respons lebih cepat
- Kepatuhan: hindari sanksi
- Kepercayaan pelanggan naik:
 - keamanan = reputasi

Strategi Membangun SecOps Modern

- Adopsi Artificial Intelligence (AI) & Machine Learning (ML)
- Adopsi Extended Detection and Response (XDR)
 - Evolusi dari Endpoint Detection and Response (EDR) dan Security Information & Event Management (SIEM)
- Terapkan Zero Trust Architecture
- Training rutin
 - 82% insiden akibat human error (Verizon, 2024)

Kemitraan & Kolaborasi

- Bekerja dengan Managed Security Service Provider (MSSP)
 - penyedia layanan keamanan siber profesional yang mengelola, memonitor, dan merespons ancaman keamanan TI atas nama perusahaan atau organisasi secara 24/7.
- Berbagi intelijen antar industri
- Bangun ekosistem keamanan kolaboratif

Risk Based Approach

- Fokus pada aset digital kritis
- Penilaian risiko berkala
- Prioritas keamanan selaras bisnis

BUKU PEGANGAN PENANGANAN

INSIDEN SIBER

"Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum."

"Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum." "Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum."

"Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum."



PENERBIT ANDI®

Penerbit Andi

Jl. Beo 38-40 Yogyakarta
Telp. (0274) 561881 Ext. 103
08112926116
andipenerbitan@gmail.com
@penerbitandi

Info Buku Baru dan Pemasaran, klik www.andipublisher.com

COMPUTING & INTERNET

ISBN 978-623-7230-XX-X
ISBN 978-623-7230-XX-X (PDF)



Harga Pulau Jawa Rp000.000



PENERBIT ANDI®

BUKU PEGANGAN PENANGANAN
INSIDEN SIBER

BUKU PEGANGAN PENANGANAN

INSIDEN SIBER



Onno W. Purbo | Jimmy Alberto | Hafizhan Irawan
Bagus Gede Arta Perdana | Aolia Ikhwanudin | Muhamad Yusuf
Agianto Syamhalim | Tubagus Toifur | Ibnu Mas'ud
Dimaz Arno Prasetyo | Tubagus Asep Nurdin

DINAS KOMINFO TANGERANG SELATAN
INSTITUT TEKNOLOGI TANGERANG SELATAN

Kesimpulan

- Transformasi digital butuh keamanan
- SecOps = kunci inovasi & kepercayaan
- Tanpa keamanan, digitalisasi bisa gagal

Call for Action

-  Evaluasi postur keamanan saat ini
-  Investasi di SOC, SIEM, SOAR
-  Mulai Zero Trust
-  Edukasi tim secara terus-menerus