



Dinas Komunikasi Informatika
Statistik dan Persandian Kota
Semarang



Sosialisasi Keamanan Informasi

Semarang, 21-24 Oktober 2024

Pendahuluan

Perkembangan teknologi saat ini yang meliputi Big Data dan Artifisial Inteligence memberikan dampak luar biasa bagi umat manusia. Saat ini data menjadi "New Gold" yang perlu mendapat perhatian bagaimana pemanfaatannya, risikonya, serta keamanannya.

Perubahan paradigma tersebut membuat keamanan informasi menjadi perhatian utama di era digital ini, di mana teknologi dan internet memainkan peran penting dalam kehidupan sehari-hari. Perkembangan pesat teknologi informasi berbasis Big data dan Artificial Inteligence telah membawa perubahan signifikan terhadap cara informasi dihasilkan, disimpan, dan disebarluaskan.

keamanan informasi menjadi aspek penting yang harus diperhatikan oleh organisasi maupun individu. Tanpa langkah-langkah keamanan yang memadai, risiko terjadinya kebocoran data, pencurian identitas, sabotase, dan serangan siber lainnya akan semakin meningkat



Prinsip Utama Keamanan Informasi

Kerahasiaan (Confidentiality)

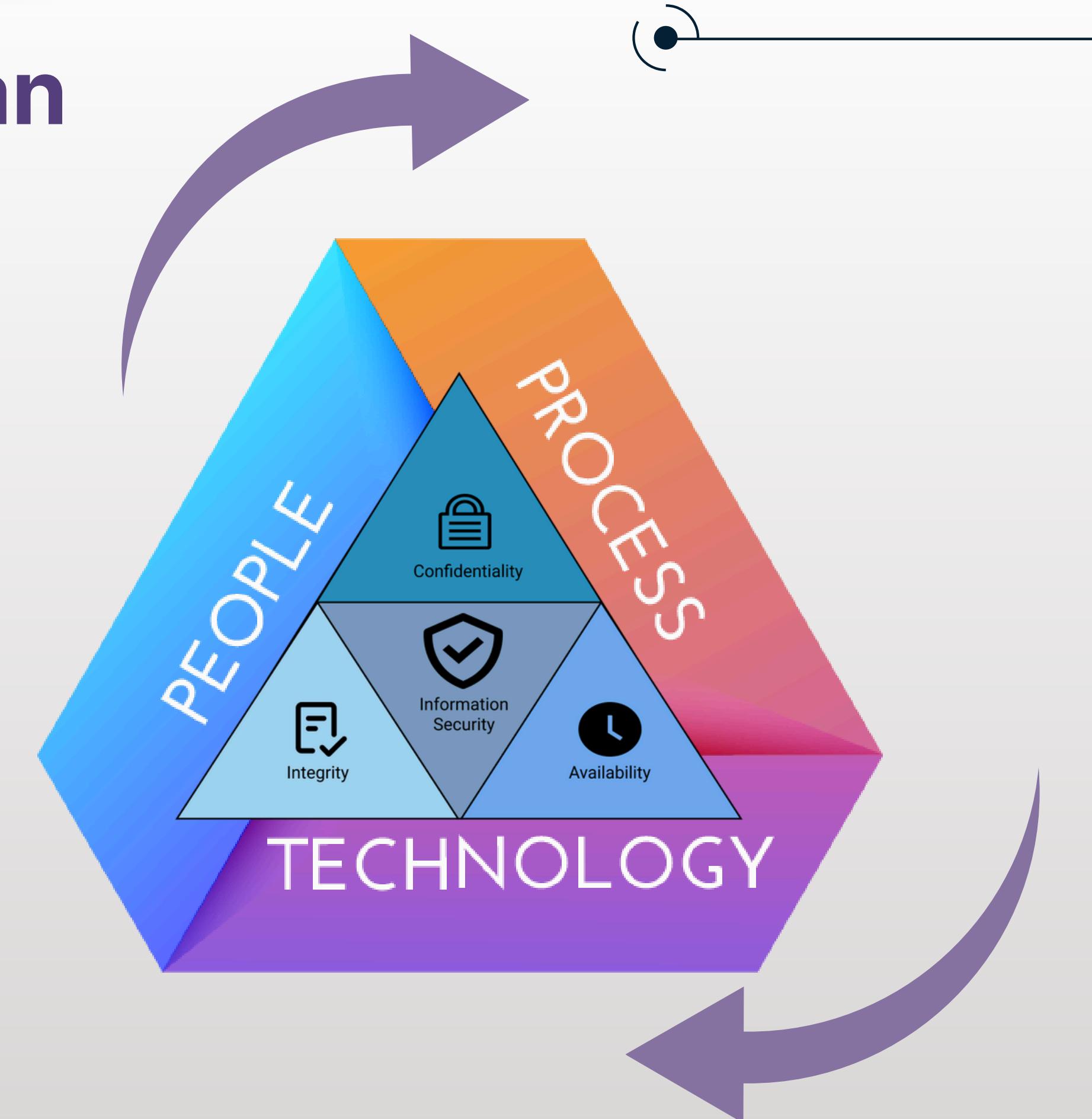
Kemampuan akses dan modifikasi informasi diberikan hanya kepada pihak yang berwenang untuk tujuan yang jelas.

Integritas (Integrity)

Informasi yang digunakan pengguna bisa dipercaya kebenarannya merefleksikan realitas sebenarnya, terutama informasi strategis.

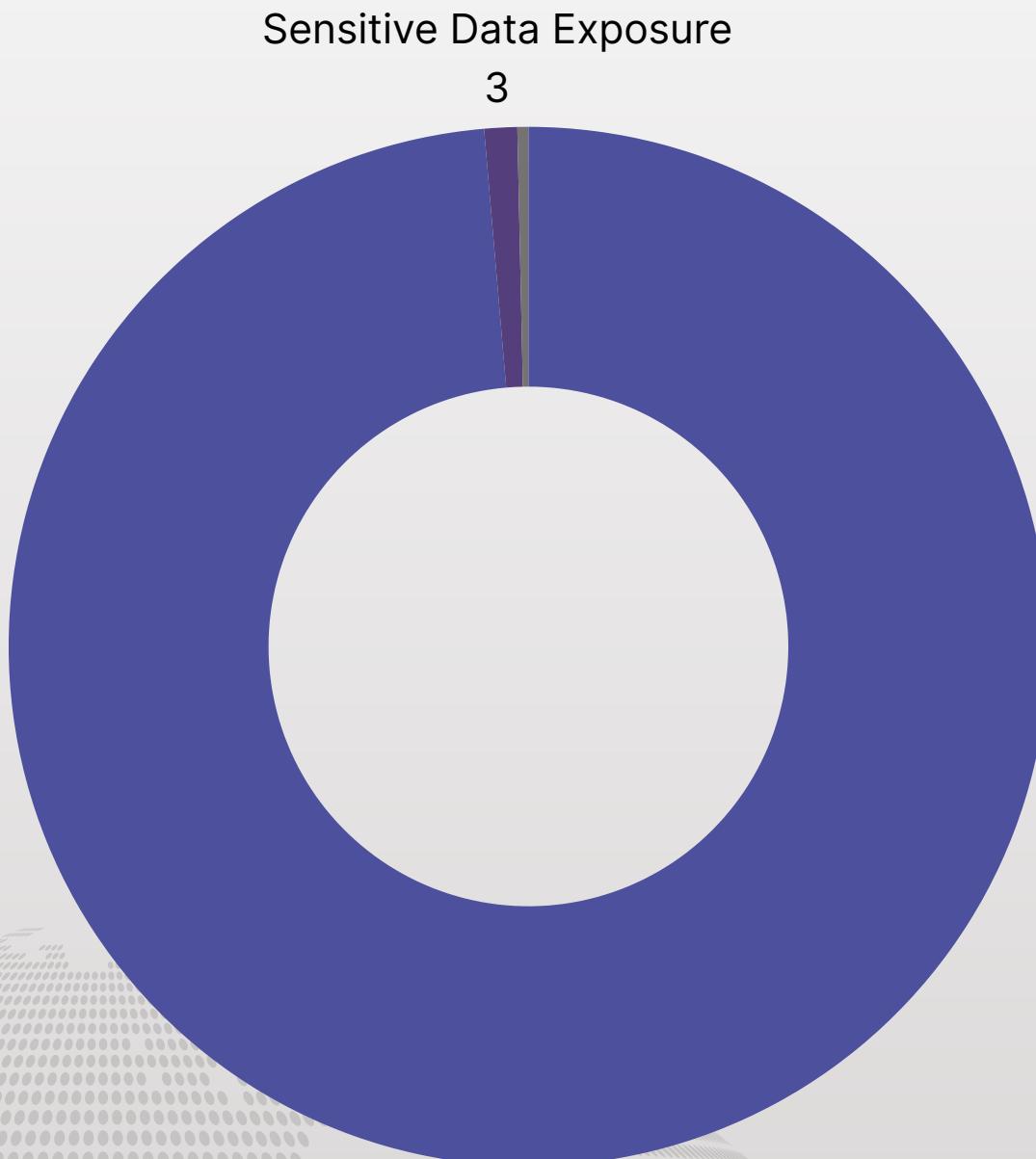
Ketersediaan (Availability)

Informasi tersedia untuk mendukung organisasi dalam rentang waktu yang disepakati bersama dan sesuai dengan peraturan yang ada sesuai tujuan organisasi



Insiden Keamanan Informasi

Insiden Keamanan Informasi di Pemkot Semarang Periode Januari - September 2024



Total Insiden Keamanan Informasi

294 Insiden

290

Penambahan Halaman
Slot Gacor

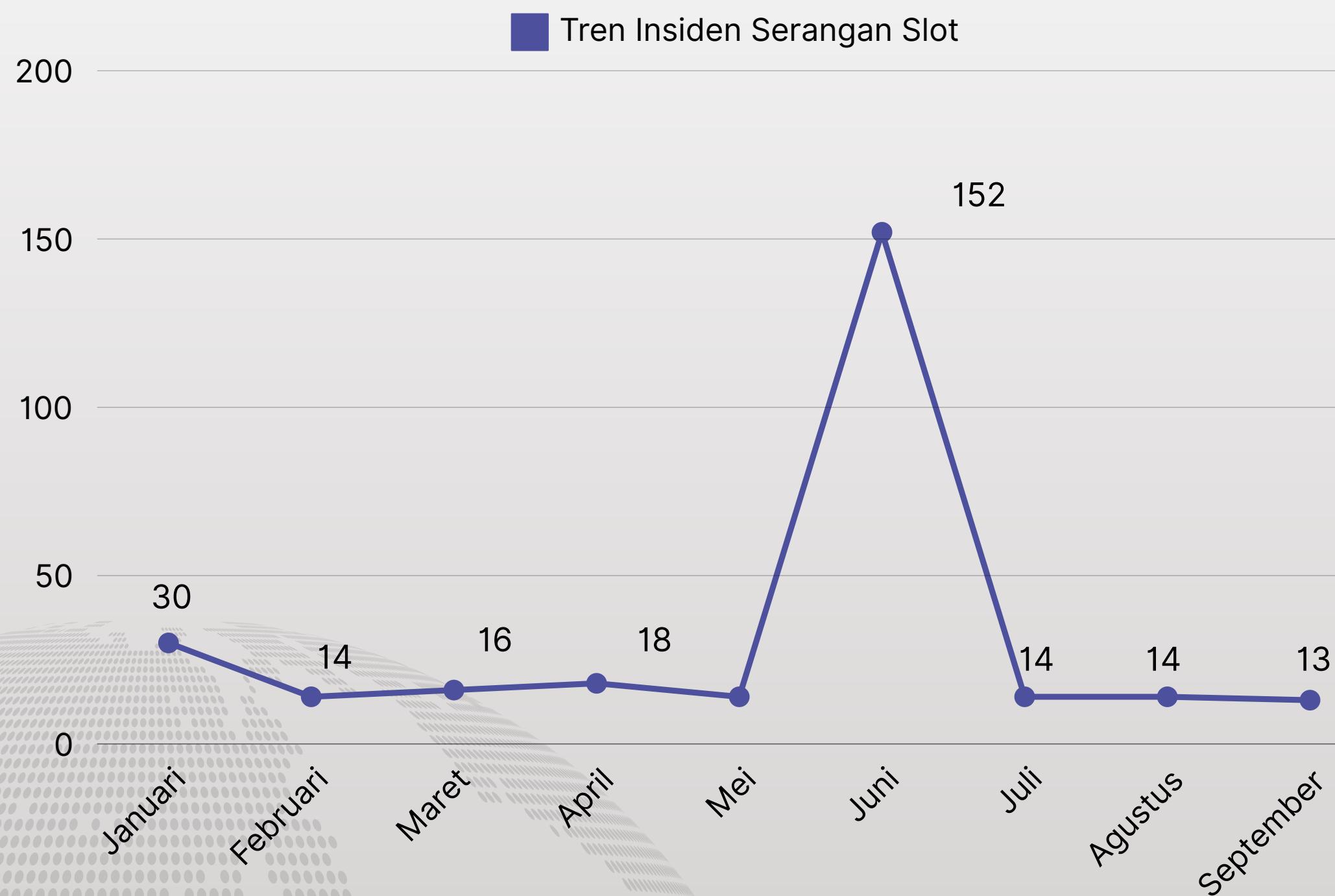
3

Sensitive Data
Exposure

1

Defacement

Tren Insiden Keamanan Informasi di Kota Semarang



Rekap Insiden Keamanan Website pada Pemerintah Kota Periode Januari 2024 s/d September 2024

Jumlah Serangan Slot Gacor di Website Pemkot Semarang



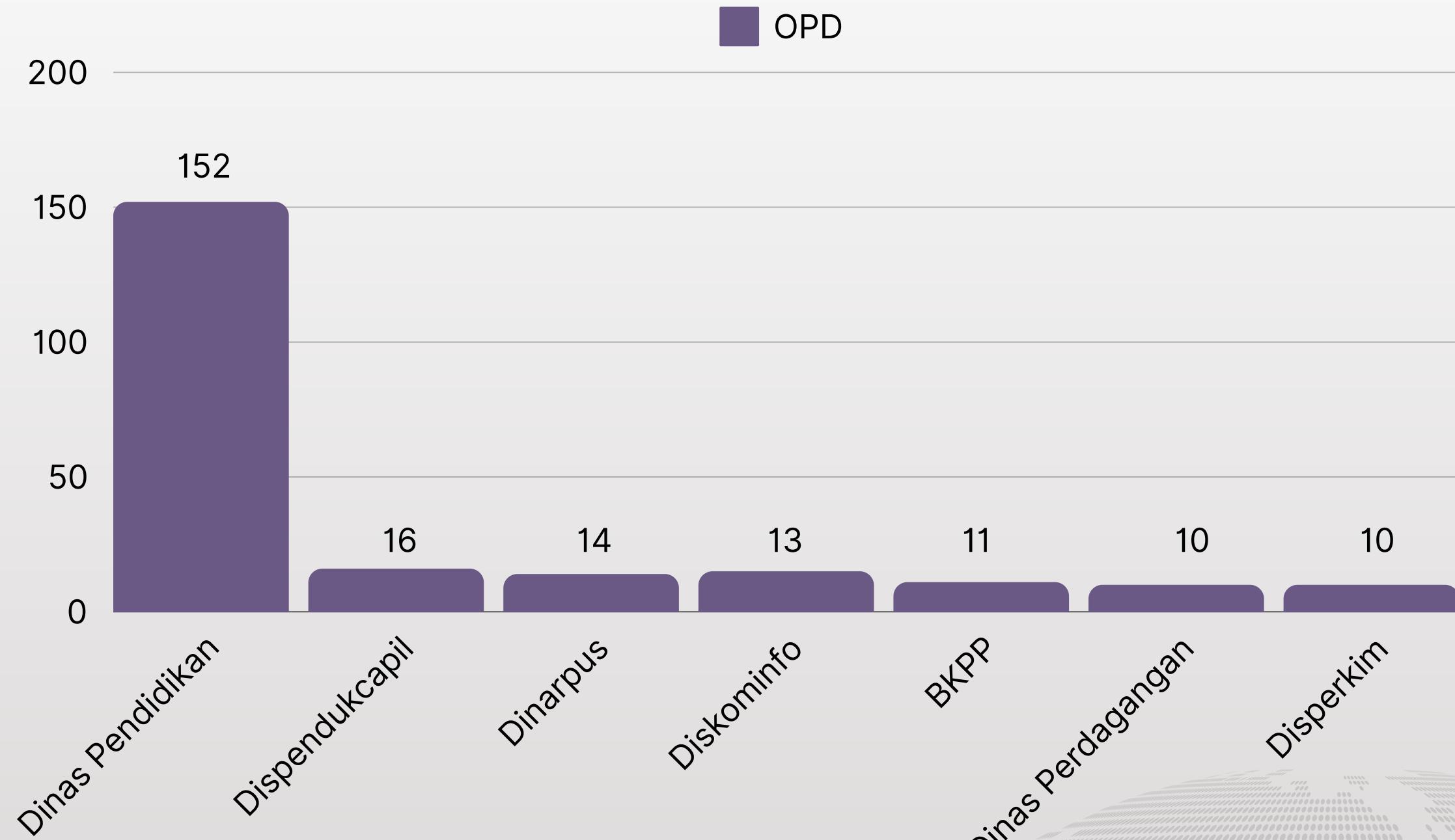
Serangan Insiden Keamanan Informasi pada website milik Pemerintah di Kota Semarang.

Terjadi anomali serangan pada Bulan Juni sebanyak 152 Insiden yang sebagian besar menyasar pada website Sekolah karena bertepatan dengan Penerimaan Peserta Didik Baru (PPDB)

Rekap Data Serangan Slot Gacor pada Website Pemerintah Kota Semarang Periode Januari - September 2024

Top 7 OPD yang terdampak serangan slot gacor.
Serangan menyerang pada website-website Dinas yang sering diakses oleh masyarakat

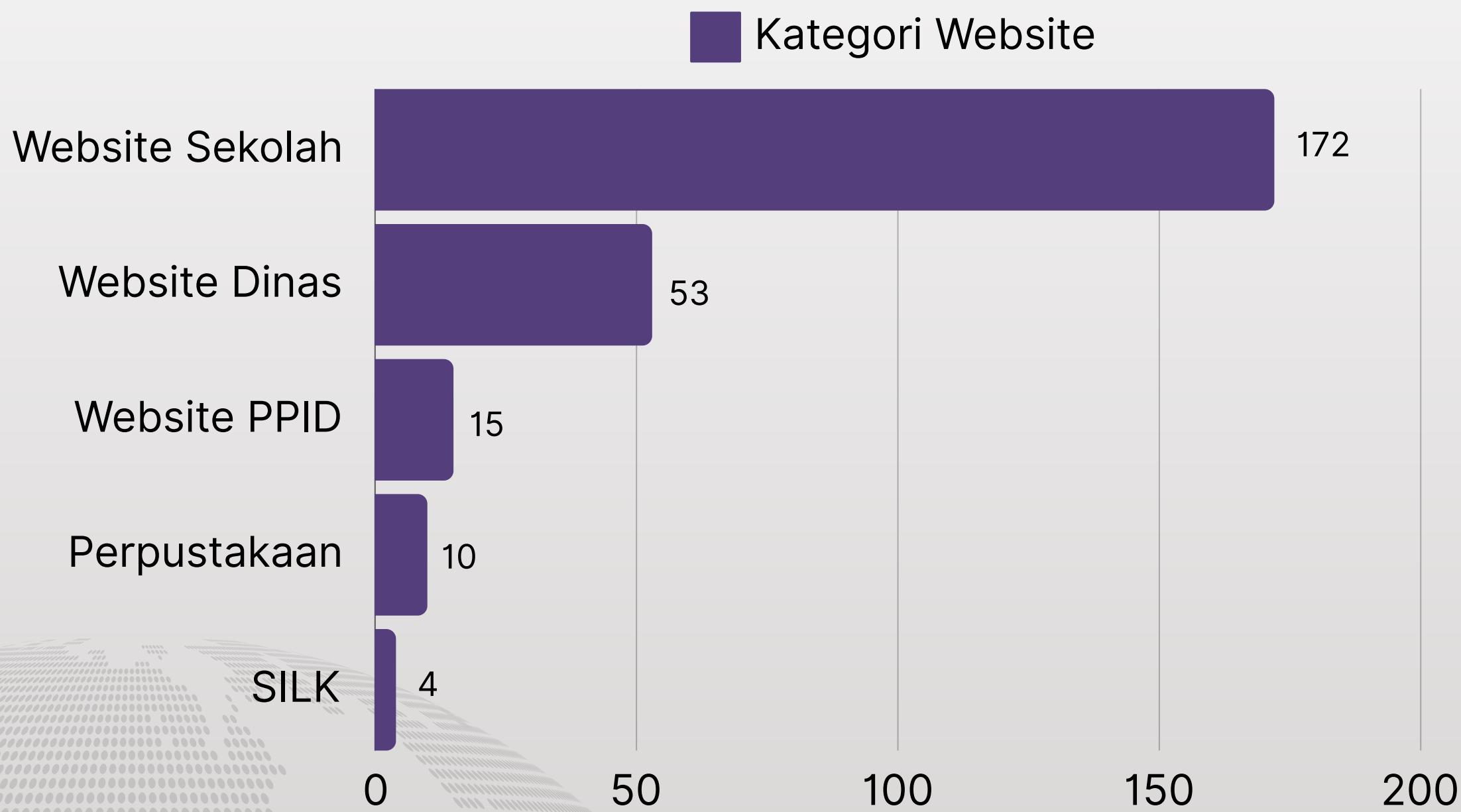
Top 7 OPD Terdampak



Rekap Data Insiden Keamanan Informasi pada Website Pemerintah Kota Semarang Periode Januari - September 2024

Top 5 Kategori Website yang terjadi insiden keamanan informasi
Website Sekolah menjadi sasaran paling utama dikarenakan banyaknya akses menuju website tersebut

Top 5 Kategori Website



Contoh Insiden Keamanan Informasi pada Website Pemerintah Kota Semarang

The image displays four separate browser windows showing different web pages:

- Lazada Marketplace:** A listing for "GRAND JACKPOT SLOTS" with a price of Rp.50.000. The listing includes a link: "JAYATOGEL 🎰 Link Login Resmi Situs Slot Gacor Anti Rungkad Server Dubai".
- ANTARA News:** An article titled "Mbokslot > Situs Gacor Mbokslot Terpercaya Mudah Maxwin Server Gacor Dan Terpercaya Gampang Di Akses Hari Ini". The date is 03 Agustus 2024 04:50 WIB.
- Scatter Hitam ! Agen Slot Gacor Online Terlengkap:** A screenshot of a website with a blue header and a green footer. The main text on the page reads: "Scatter Hitam ! Agen Slot Gacor Online Terlengkap Modal Receh Bisa WD Ratusan Juta Tahun 2024 — SCATTER HITAM".
- Scatter Hitam ! Agen Slot Gacor Online Terlengkap:** A screenshot of a website with a blue header and a green footer. The main text on the page reads: "Scatter Hitam ! Agen Slot Gacor Online Terlengkap Modal Receh Bisa WD Ratusan Juta Tahun 2024 — SCATTER HITAM".

A decorative graphic of a globe is visible on the left side of the collage.

Penyebab Masuknya Halaman dan Link Judi Online pada Website Pemerintah

Aplikasi yang rentan

Celah Keamanan
Celah keamanan dalam kode atau sistem manajemen konten (CMS) dapat dimanfaatkan oleh penyerang menyisipkan skrip berbahaya yang menampilkan iklan judi online

Akun Website yang telah dicuri

Password Lemah
Penggunaan password yang mudah ditebak atau penggunaan ulang password yang sama di banyak platform dapat membuat website lebih rentan dan mudah untuk dicuri

Penyusupan Backdoor

Infeksi File Backdoor
Setelah berhasil mendapatkan akses, penyerang sering kali menanamkan backdoor atau malware di dalam website, memungkinkan mereka menyisipkan iklan judi secara berkelanjutan bahkan setelah masalah pertama diperbaiki.

Aplikasi yang rentan

Celah Keamanan Aplikasi seperti :

- 1.Fitur upload yang tidak disanitasi tipe file dengan benar
- 2.Fasilitas Demo Aplikasi yang masih berjalan padahal tidak digunakan
- 3.SQL injection

jQuery File Upload Demo

Basic Plus UI version

File Upload widget with multiple file selection, drag&drop support, progress bars, validation and preview images, audio and video for jQuery. Supports cross-domain, chunked and resumable file uploads and client-side image resizing. Works with any server-side platform (PHP, Python, Ruby on Rails, Java, Node.js, Go etc.) that supports standard HTML form file uploads.

+ Add files... Start upload Cancel upload Delete

Demo Notes

- The maximum file size for uploads in this demo is **999 KB** (default file size is unlimited).
- Only image files (**JPG, GIF, PNG**) are allowed in this demo (by default there is no file type restriction).
- Uploaded files will be deleted automatically after **5 minutes or less** (demo files are stored in memory).
- You can **drag & drop** files from your desktop on this webpage (see [Browser support](#)).
- Please refer to the [project website](#) and [documentation](#) for more information.

Nama

No Phone / HP

Sumur

Kecamatan

Contact Person

Pesan

Gambar

Choose File No file chosen

Semua kolom harus diisi

Kirim

Kodeguru *

Enter Kodeguru

Password *

Enter Password

Should contain 6 Characters minimum Capital Letter Number Symbol

Confirm Password *

Enter Confirm Password

Nama *

Enter Nama

Tempatlahir *

Enter Tempatlahir

Tanggallahir *

Enter Tanggallahir

Alamat *

Enter Alamat

Email *

Enter Email

Nohp *

Enter Nohp

Photo *

Choose files or drag and drop files to upload

Nip *

Enter Nip

User Role Id *

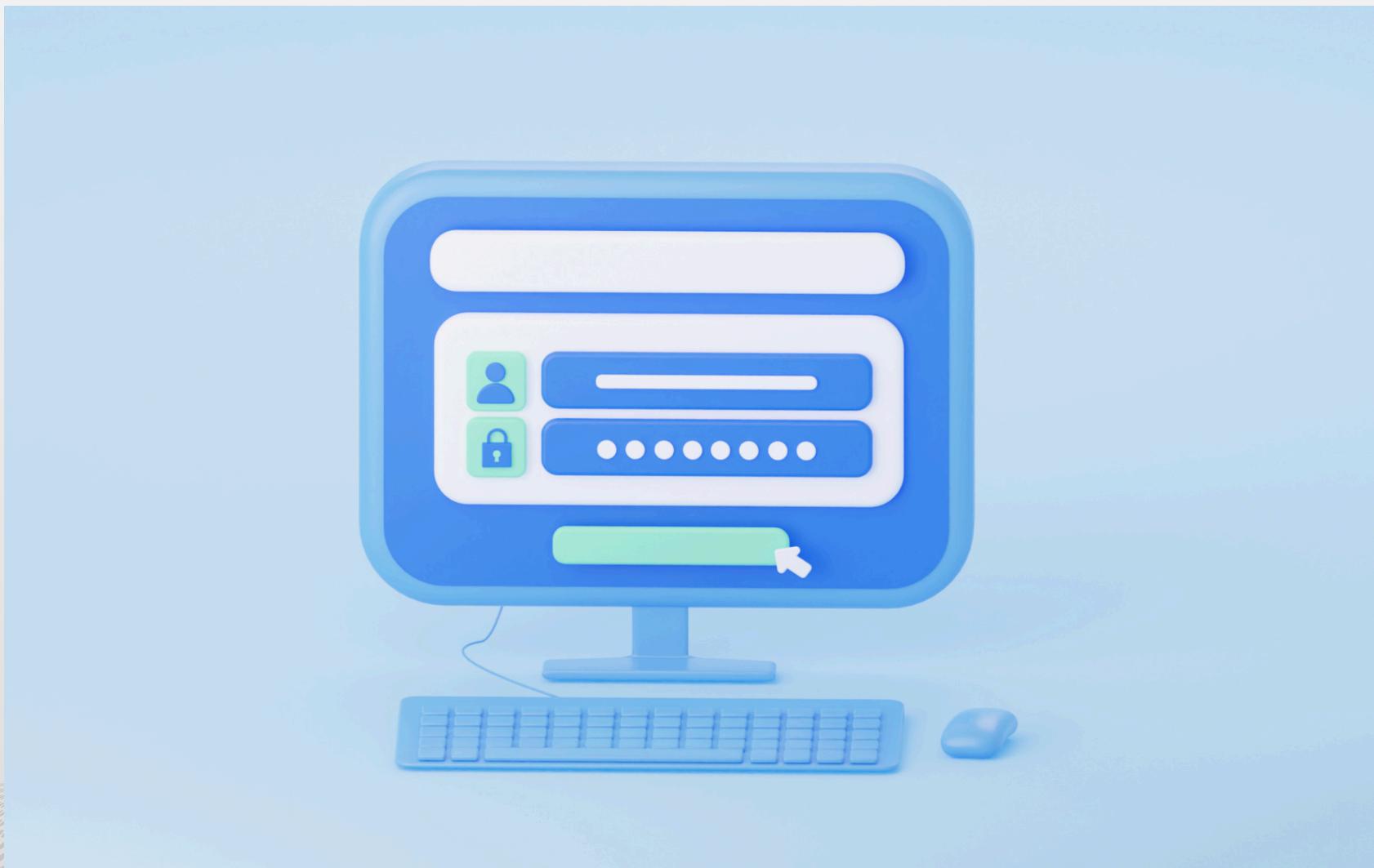
Select a value ...

Submit

*gambar hanya sebagai ilustrasi (tidak menggambarkan kondisi yang sebenarnya)



Akun website yang telah dicuri

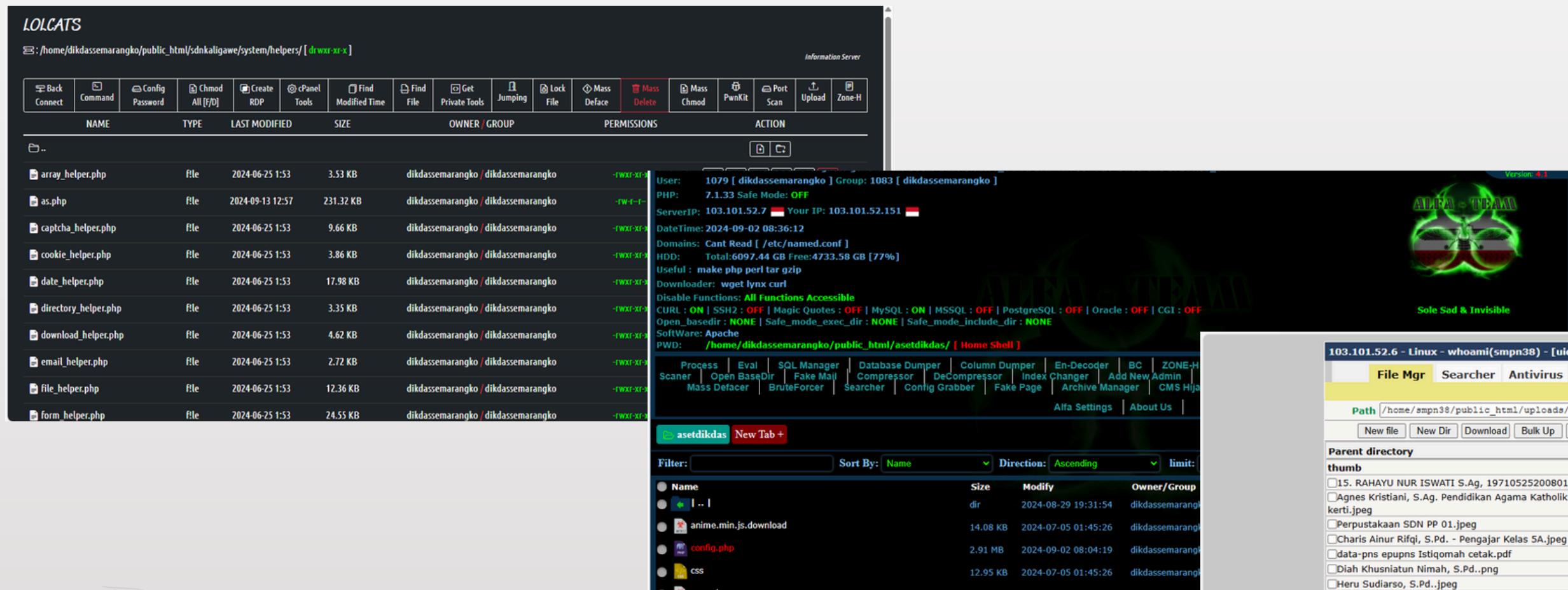


Penyebab akun website mudah dicuri

1. Password yang lemah dan mudah ditebak
2. Password tidak sesuai dengan Standar password
(<https://smg.city/standarpassword>)
3. Menyimpan password pada tulisan atau di browser
4. Menyerahkan akun kepada pihak lain

Penyusupan Backdoor

Setelah berhasil mendapatkan akses, penyerang sering kali menanamkan backdoor atau malware di dalam website, memungkinkan mereka menyisipkan iklan judi secara berkelanjutan bahkan setelah masalah pertama diperbaiki.



LOLCATS

:/home/dikdassemarangko/public_html/sdnkaligawe/system/helpers/ [drwxr-x]

Information Server

NAME TYPE LAST MODIFIED SIZE OWNER / GROUP PERMISSIONS ACTION

array_helper.php file 2024-06-25 1:53 3.53 KB dikdassemarangko /dikdassemarangko -rwxr-xr-x

as.php file 2024-09-13 12:57 231.32 KB dikdassemarangko /dikdassemarangko -rw-r--r--

captcha_helper.php file 2024-06-25 1:53 9.66 KB dikdassemarangko /dikdassemarangko -rwxr-xr-x

cookie_helper.php file 2024-06-25 1:53 3.86 KB dikdassemarangko /dikdassemarangko -rwxr-xr-x

date_helper.php file 2024-06-25 1:53 17.98 KB dikdassemarangko /dikdassemarangko -rwxr-xr-x

directory_helper.php file 2024-06-25 1:53 3.35 KB dikdassemarangko /dikdassemarangko -rwxr-xr-x

download_helper.php file 2024-06-25 1:53 4.62 KB dikdassemarangko /dikdassemarangko -rwxr-xr-x

email_helper.php file 2024-06-25 1:53 2.72 KB dikdassemarangko /dikdassemarangko -rwxr-xr-x

file_helper.php file 2024-06-25 1:53 12.36 KB dikdassemarangko /dikdassemarangko -rwxr-xr-x

form_helper.php file 2024-06-25 1:53 24.55 KB dikdassemarangko /dikdassemarangko -rwxr-xr-x

User: 1079 [dikdassemarangko] Group: 1083 [dikdassemarangko]
PHP: 7.1.33 Safe Mode: OFF
ServerIP: 103.101.52.7 Your IP: 103.101.52.151
DateTime: 2024-09-02 08:36:12
Domains: Cant Read [/etc/hostname]
HDD: Total:6097.44 GB Free:4733.58 GB [77%]
Useful: make php perl tar gzip
Downloader: wget lynx curl
Disable Functions: All Functions Accessible
CURL : ON | SSH2 : OFF | Magic Quotes : OFF | MySQL : ON | MSSQL : OFF | PostgreSQL : OFF | Oracle : OFF | CGI : OFF
Open_basedir : NONE | Safe_mode_exec_dir : NONE | Safe_mode_include_dir : NONE
SoftWare: Apache
PWD: /home/dikdassemarangko/public_html/asetdkdas/ [Home Shell]

Version: 4.1

ALFA - TEAM

Sole Sad & Invisible

103.101.52.6 - Linux - whoami(smpn38) - [uid(1027) gid(1030)] - [PostgreSQL]

File Mgr Searcher Antivirus Mass htcs Lock File Back Cnct Exec CMD Exec SQL System

[Wopp Phy0186 bisa ?]

Path /home/smpn38/public_html/uploads/gallery/media/ Go Root dir Current dir ---Special Dir---

New file New Dir Download Bulk Up Choose File No file chosen Upload Renamed to

Parent directory	Action	Perm	Creation time	Last Changed	Size
thumb	Del Ren	0755	2024-04-25 03:31:54	2024-04-25 03:31:54	-
15. RAHAYU NUR ISWATI S.Ag, 197105252008012013.jpg	View Ren	0644	2022-05-23 06:48:01	2021-06-09 03:28:14	1.69 M
Agnes Kristiani, S.Ag. Pendidikan Agama Katholik dan Budi Pe	View Ren	0755	2022-05-23 06:48:01	2021-06-09 03:28:14	43.31 K
kerti.jpeg	View Ren	0644	2022-05-23 06:48:01	2021-06-09 03:28:14	102.04 K
Perpustakaan SDN PP 01.jpeg	View Ren	0755	2022-05-23 06:48:01	2021-06-09 03:28:14	22.30 K
Charis Alinur Rifqi, S.Pd. - Pengajar Kelas 5A.jpeg	View Ren	0644	2022-05-23 06:48:01	2021-06-09 03:28:14	38.71 K
data-pns epupns Istiqomah cetak.pdf	View Ren	0755	2022-05-23 06:48:01	2021-06-09 03:28:14	2.34 M
Diah Khusniyatun Nimah, S.Pd..png	View Ren	0644	2022-05-23 06:48:01	2021-06-09 03:28:14	109.35 K
Heru Sudiarso, S.Pd..jpeg	View Ren	0755	2022-05-23 06:48:01	2021-06-09 03:28:14	232.86 K
Dyah Sri Rahayu, S.Pd..jpg	View Ren	0644	2022-05-23 06:48:01	2021-06-09 03:28:14	245.21 K
Foto KS-ok.jpg	View Ren	0755	2022-05-23 06:48:01	2021-06-09 03:28:14	190.90 K
Juminten, S.Pd..PNG	View Ren	0644	2022-05-23 06:48:01	2021-06-09 03:28:14	1.65 M
IMG20210426081150.jpg	View Ren	0755	2022-05-23 06:48:01	2021-06-09 03:28:14	12.75 K
Juminten, S.Pd..jpg	View Ren	0644	2022-05-23 06:48:01	2021-06-09 03:28:14	1.65 M
IMG20210426081517.jpg	View Ren	0755	2022-05-23 06:48:01	2021-06-09 03:28:14	168.93 K
Siti Kholisoh, S.Pd..jpeg	View Ren	0644	2022-05-23 06:48:01	2021-06-09 03:28:14	1.57 M
IMG20210427083522(1).jpg	View Ren	0755	2022-05-23 06:48:01	2021-06-09 03:28:14	145.81 K
Twitibbon HUT Kota Semarang.jpeg	View Ren	0644	2022-05-23 06:48:01	2021-06-09 03:28:14	1.89 M
IMG20210427083830.jpg	View Ren	0755	2022-05-23 06:48:01	2021-06-09 03:28:14	163.18 K
Twitibbon Hari Lahir Pancasila.jpeg	View Ren	0644	2022-05-23 06:48:01	2021-06-09 03:28:14	371.96 K
Image_ProactiveClinics.png	View Ren	0755	2022-05-23 06:48:01	2021-06-09 03:28:14	107.15 K
Halaman SDN PP 01.jpeg	View Ren	0644	2022-05-23 06:48:01	2021-06-09 03:28:14	21.12 K
Tetinomah S.Drl Densstar Kelse GR inan	View Ren	0755	2022-05-23 06:48:01	2021-06-09 03:28:14	-

Mengapa Website Pemerintah Dipilih untuk disusupi Slot Gacor?

Terlepas dari faktor teknis terhadap celah keamanan website, berikut adalah alasan mengapa website milik Pemerintah dipilih untuk menumpang dan disusupi halaman slot gacor

Kepercayaan Publik yang Tinggi

Website pemerintah umumnya memiliki reputasi baik dan dipercaya oleh masyarakat. Penyerang memanfaatkan kepercayaan ini untuk menampilkan konten yang biasanya dihindari oleh mesin pencari atau pemblokiran otomatis. Dengan menumpang di website resmi, iklan judi bisa lolos dari filter keamanan pengguna.

Lalu Lintas Tinggi

Website pemerintah sering kali memiliki banyak pengunjung, baik untuk mencari informasi, mengakses layanan, atau mengurus administrasi. Dengan menanam iklan judi di situs yang ramai, penyerang dapat menjangkau lebih banyak orang dan meningkatkan peluang konversi ke situs judi mereka.

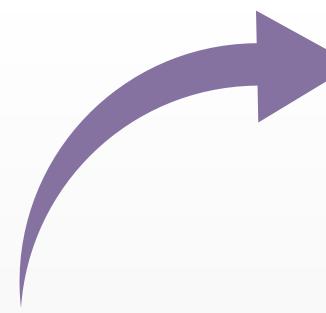


Peringkat Mesin Pencari

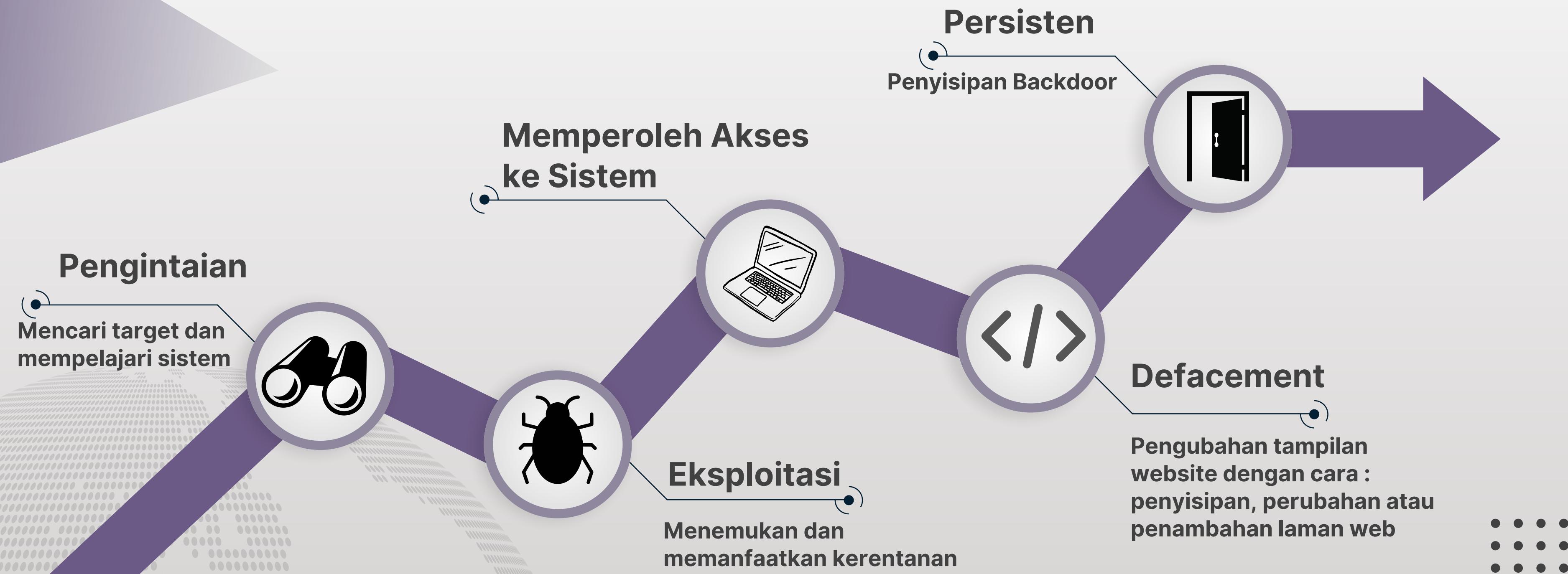
Dengan menyisipkan tautan atau konten judi online di website pemerintah, penyerang mencoba meningkatkan peringkat SEO (Search Engine Optimization) dari situs judi mereka. Mesin pencari sering kali menganggap tautan dari website pemerintah sebagai tautan berkualitas tinggi, yang meningkatkan otoritas situs judi dalam hasil pencarian.

Sulitnya Terdeteksi

Website pemerintah cenderung tidak sering diawasi dengan ketat, terutama jika tidak ada tim keamanan siber yang memantau secara rutin. Hal ini memungkinkan konten berbahaya tetap ada di situs tersebut lebih lama sebelum terdeteksi dan dihapus.



Langkah-langkah Serangan Judi Online



Penanggulangan Insiden Keamanan Informasi di website Pemkot Semarang



Melakukan verifikasi Insiden siber kepada pemilik/pengelola website

Melakukan suspend website untuk mencegah pengunjung mengakses konten yang berbahaya dan dapat mencegah penyerang melakukan perubahan lebih lanjut saat melakukan perbaikan serta agar insiden yang terjadi tidak meluas

Melakukan analisa terhadap pola serangan untuk menemukan sumber serangan.

Penghapusan file / halaman yang terkena serangan slot gacor serta melakukan penghapusan file yang terindikasi sebagai backdoor / malware

Melakukan pemulihan website termasuk mengganti username dan password serta memonitor website secara berkala untuk mendeteksi aktivitas mencurigakan lebih awal



Informasi Tentang Keamanan Siber di Kota Semarang

Semarang Kota – Computer Security Incident Response Team (SemarangKota-CSIRT), merupakan CSIRT sektor Pemerintah Daerah Kota Semarang yang dibentuk pada tahun 2021 guna mendukung penerapan kebijakan Sistem Manajemen Keamanan Informasi (SMKI) Pemkot Semarang. Semarang Kota CSIRT merupakan wadah koordinasi antar unit dan atau stakeholder di lingkungan Pemerintah Kota Semarang terkait dengan keamanan informasi.



<https://csirt.semarangkota.go.id/>
Website yang berisi tentang informasi terkini terkait dengan keamanan siber

Peran OPD dalam Keamanan Informasi

Perwali No 28 Tahun 2021 tentang SMKI

Pasal 7

Semua Perangkat Daerah terkait, memiliki tanggung jawab dalam pengamanan sistem informasi melalui kooordinasi dengan perangkat daerah yang menyelenggarakan tugas dan fungsi di bidang teknologi informasi dan komunikasi.

Kebijakan Umum Sistem Manajemen Keamanan Informasi dalam Lampiran Perwali No 28 Tahun 2021 tentang SMKI

B. KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI

1. RUANG LINGKUP KEAMANAN INFORMASI

Keamanan informasi merupakan tanggung jawab dari semua pihak yang terkait pada Pemerintah Kota Semarang meliputi seluruh pemangku kepentingan (stakeholder) internal dan eksternal di lingkungan Kota Semarang.

Kanal Pelaporan Insiden Siber Kota Semarang

Semarang Kota – Computer Security Incident Response Team (SemarangKota-CSIRT), merupakan CSIRT sektor Pemerintah Daerah Kota Semarang yang dibentuk pada tahun 2021 guna mendukung penerapan kebijakan Sistem Manajemen Keamanan Informasi (SMKI) Pemkot Semarang. Semarang Kota CSIRT merupakan wadah koordinasi antar unit dan atau stakeholder di lingkungan Pemerintah Kota Semarang terkait dengan keamanan informasi.



email : csirt@semarangkota.go.id

Computer Security Incident Response Team, disingkat CSIRT Pemkot Semarang merupakan CSIRT sektor Pemerintah Daerah.

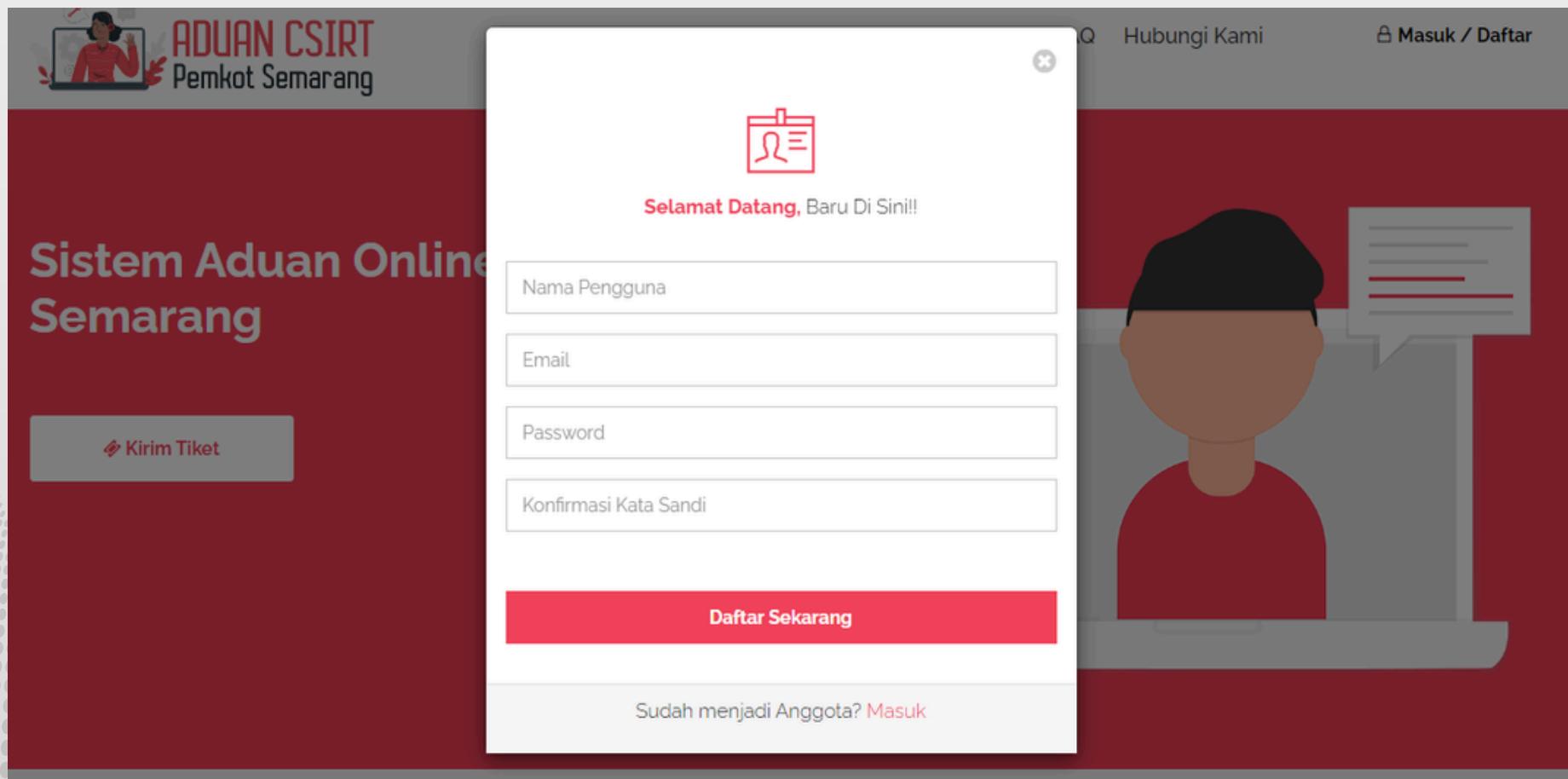


<https://aduan.csirt.semarangkota.go.id/>

Kanal Aduan untuk melaporkan insiden siber dan kerentanan website Pemerintah Kota Semarang

Alur Pelaporan Insiden Siber

1. Membuat akun di aduan.csirt.semarangkota.go.id
2. Membuat tiket aduan siber
3. Mendeskripsikan dengan jelas kronologi temuan insiden siber beserta bukti dukungnya



Sistem Aduan Online
Semarang

Kirim Tiket

Selamat Datang, Baru Di Sini!!

Nama Pengguna

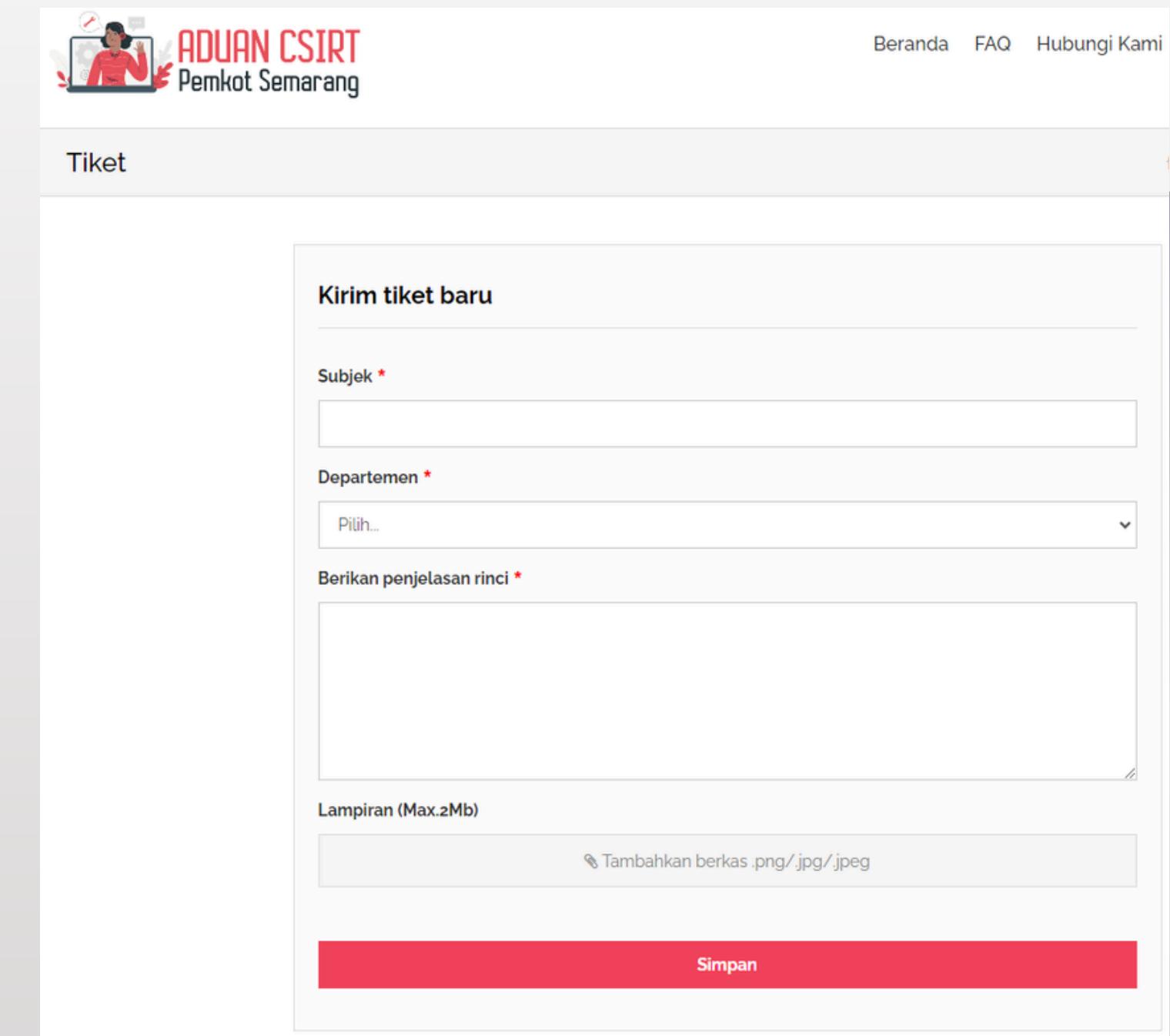
Email

Password

Konfirmasi Kata Sandi

Daftar Sekarang

Sudah menjadi Anggota? Masuk



ADUAN CSIRT
Pemkot Semarang

Beranda FAQ Hubungi Kami

Tiket

Kirim tiket baru

Subjek *

Departemen *

Berikan penjelasan rinci *

Lampiran (Max.2Mb)

Tambahkan berkas .png/.jpg/.jpeg

Simpan

Tips agar terhindar dari serangan Slot Gacor

1. Melakukan update sistem : Operating Sistem, Security Patch, plugin, dll.
2. Pergunakan password yang kuat dan unik mengacu pada Standar Password (<https://smg.city/standarpassword>)
3. Pembiasaan kebersihan layar dan meja kerja mengacu pada Standar Kebersihan Layar dan Meja Kerja
(<https://smg.city/standarkebersihanlayardanmeja>)
4. Pembatasan akses login hanya untuk pihak-pihak yang berkepentingan (Least Privilege)
5. Melakukan peningkatan keamanan aplikasi (Input Sanitization)
6. Melakukan pemindaian kerentanan keamanan secara rutin
7. Meningkatkan literasi keamanan informasi melalui csirt.semarangkota.go.id
8. Berkoordinasi dengan Dinas Komunikasi, Informatika, Statistik dan Persandian Kota Semarang

Terima Kasih

“Ingatlah, Bahwa Kechilafan Satu
Orang Sahaja Tjukup Sudah
Menjebabkan Keruntuhan Negara”

DR. ROEBIONO KERTOPATI

Bapak Persandian Indonesia



diskominfo.semarangkota.go.id



Pemuda 148, Sekayu, Semarang
Tengah, Kota Semarang