JENIS JENIS SERANGAN SIBER YANG DAPAT MENGAKIBATKAN TERJADINYA INSIDEN SIBER DI KABUPATEN MAGELANG

Oleh :
Mardiyanto Joko Wicaksono, S.Kom, MMSI

A. Pengertian System Informasi

- Sebuah data yang diubah menjadi lebih bermanfaat untuk orang yang memerlukannya dalam membantu mengambil keputusan atau dengan kata lain system informasi adalah sebuah data yang didalemnya terdapat informasi penting yang biasanya digunakan untuk mengambil keputusan oleh instansi untuk hubungannya dengan operasional.(biasanya system informasi disimpan berbasis teknologi)

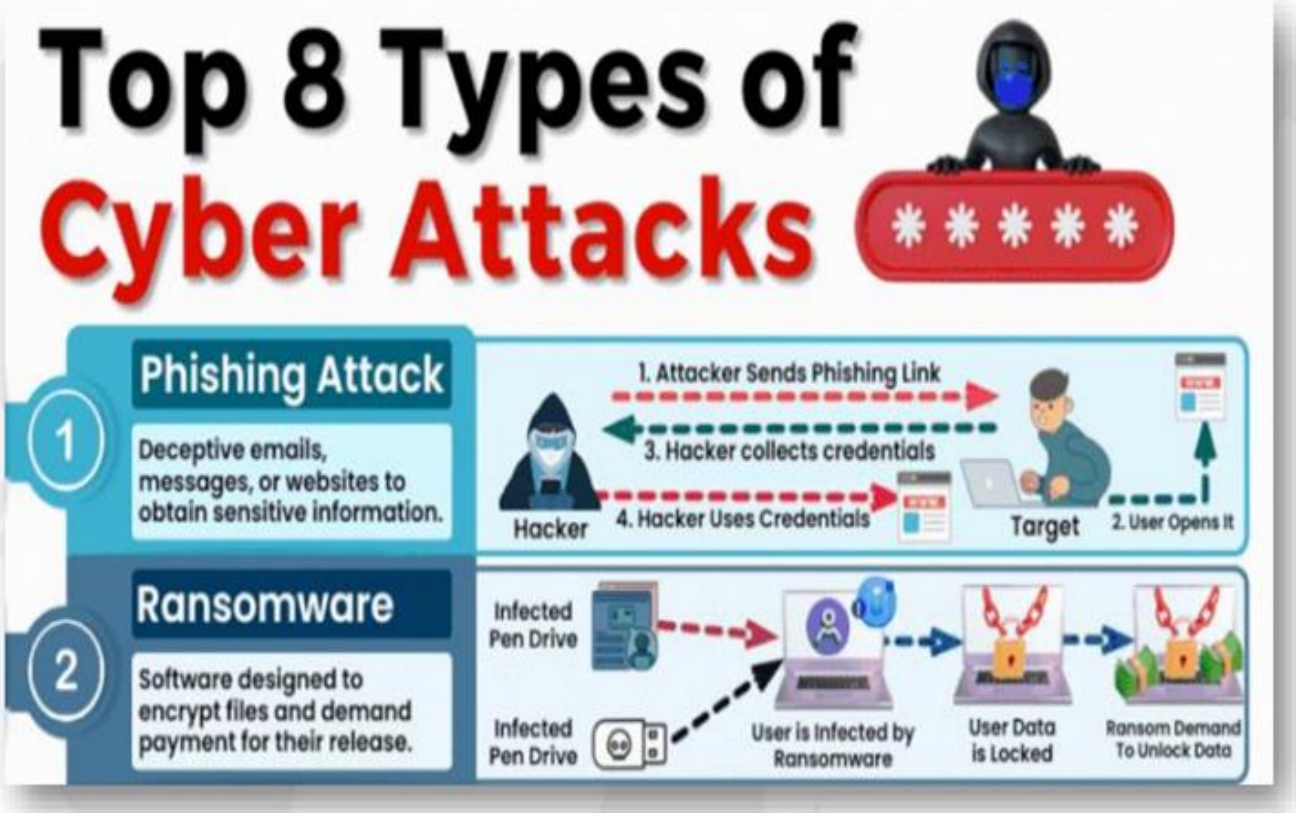
B. Mengapa perlu mengamankan system informasi ?

- Data yang disimpan dalam system informasi biasanya berbentuk eletronik dan disimpan didalamnya ,karena system infomasi dan jaringan komunikasi berhubhungan diberbagai tempat , negara dan lokasi sehingga penyalahgunaan dan kecurangan dapat terjadi , terlebih lagi jika data yang kita simpan adalah data perusahaan atau pribadi yang bersifat sangat penting ,akan bahaya jika hal tersebut terjadi.

C. Serangan siber yang biasa terjadi

- Serangan siber adalah jenis serangan yang digunakan oleh negara, individu, atau organisasi yang menargetkan sistem informasi komputer, infrastruktur, atau jaringan komputer, dan perangkat komputer pribadi dengan berbagai cara tindakan berbahaya yang biasanya mencuri, mengubah, atau menghancurkan target yang ditentukan dengan cara meretas sistem yang rentan

BAHAYA RANSOMWARE



Sumber: LetsDefend, 2024

INSIDEN RANSOMWARE DI DUNIA

1989
"AIDS Trojan" atau "PC Cyborg"
Penyebaran melalui disket di konferensi AIDS di Afrika.

2005
"PGPCoder" atau "Gpcode"
Ransomware $20, ransomware pertama yang didistribusikan secara online

2006
"Archievus"
Ransomware dengan algoritma enkripsi RSA

2011
"WinLock"
Ransomware ini mengunci akses ke mesin komputer dan mengandung foto pornografi

2013
"CryptoLocker"
RaaS, *command & control*, menghasilkan $27 juta dalam 2 bulan pertama operasi. Ransomware pertama dengan tebusan bitcoin.

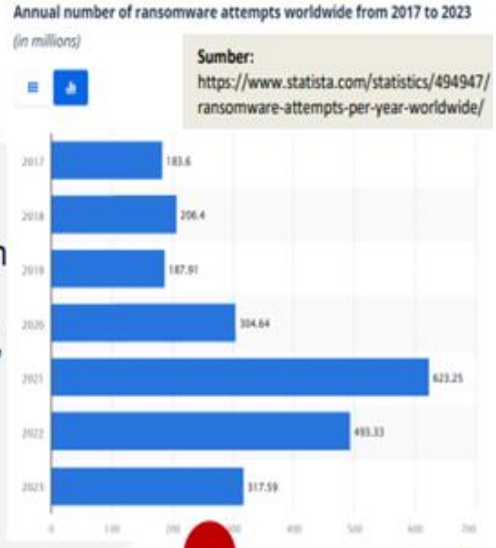
2014
"SimpleLocker"
Penyebaran melalui pesan update Adobe Flash palsu pada tablet/perangkat Android

2016
"Petya"
Serangan global pada 2017. Negara paling terdampak Ukraina (80%). Matinya sistem pemantauan radiasi Chernobyl, termasuk Kementerian, Bank, dan Sistem Kereta di Ukraina.

2017
"WannaCry"
Penyebaran pada seluruh perangkat OS Windows di seluruh dunia, termasuk Indonesia. Memanfaatkan kerentanan EternalBlue

2019
Insiden ransomware meningkat 365% dan disebut sebagai *big game hunting*. Muncul LockBit versi pertama (ransomware abcd)

2020-2021
Eksistensi Ransomware-as-a-Service (RaaS)
Penyerang tidak terlalu membutuhkan pengalaman dengan tawaran platform. Contoh: REvil (Sodinokibi), LockBit, DarkSide, Babuk Locker, Maze



2023-2024
- **LockBit** diduga menyerang BSI (Lockbit 3.0). Sepanjang 2023, terdapat 1.011.209 aktivitas ransomware, seperti LockBit, Mallox, BrianLian (Lanskap Kamsiber Indonesia, 2023).
- Lockbit 3.0 berkembang menjadi Brain Cipher Ransomware yang menyerang Pusat Data Nasional Sementara (PDNs) di Indonesia.

TOP 5 ATTACK VECTOR – INSIDEN RANSOMWARE

EKSPLOITASI
REMOTE DESKTOP PROTOCOL (T1021.001)
Miskonfigurasi pada RDP menyebabkan seseorang mengakses tanpa izin (penyusupan malware hingga lateral movement ke seluruh jaringan)

KAMPANYE PHISHING
Metode utama untuk memperoleh akses ke jaringan target. Kerentanan pada kurangnya kewaspadaan dan kesadaran pengguna

KERENTANAN PERANGKAT LUNAK
Target dengan memanfaatkan kerentanan pada perangkat lunak yang belum diperbaiki / usang

SERANGAN RANTAI PEMASOK (SUPPLY CHAIN)
Kebocoran berasal dari vendor atau pihak ketiga yang memiliki akses ke klien

TEKNIK LIVING-OFF-THE-LAND (T1218)
Memanfaatkan alat dan proses yang sah pada jaringan korban (PowerShell, aplikasi Office, dsb). Teknik yang berpotensi membuat *threat actor* tidak terdeteksi sistem keamanan. Tujuan hingga eksfiltrasi data korban

Sumber: Lanskap Keamanana Siber di Indonesia 2023

LAPORAN
KEAMANAN SIBER
BULAN JULI 2024

COMPUTER SECURITY INSIDEN RESPONSE TEAM

https://csirt.magelangkab.go.id

RINGKASAN

Analisis Aktivitas Server Menggunakan SIEM

- Total kejadian : 10.879.942
- Peringatan kritis : 472
- Autentikasi gagal : 1.113.311
- Autentikasi sukses : 8.902
- Jumlah sensor terpasang : 8 servers

Bug Hunter

- Open Redirect : 1
- Reflected Cross-Site Scripting : 6
- Sensitive data exposure : 1
- PHP Info exposure : 1
- Broken Link Hijacking : 1
- SQL Injection : 1
- Stored Cross-Site Scripting : 1

Insiden Siber

- Web Defacement : 3

Vulnerability Assessment (Penilaian Kerentanan) Websites

- Jumlah Website Dianalisa : 5
- Level Kerentanan Medium : 19
- Level Kerentanan Low : 4

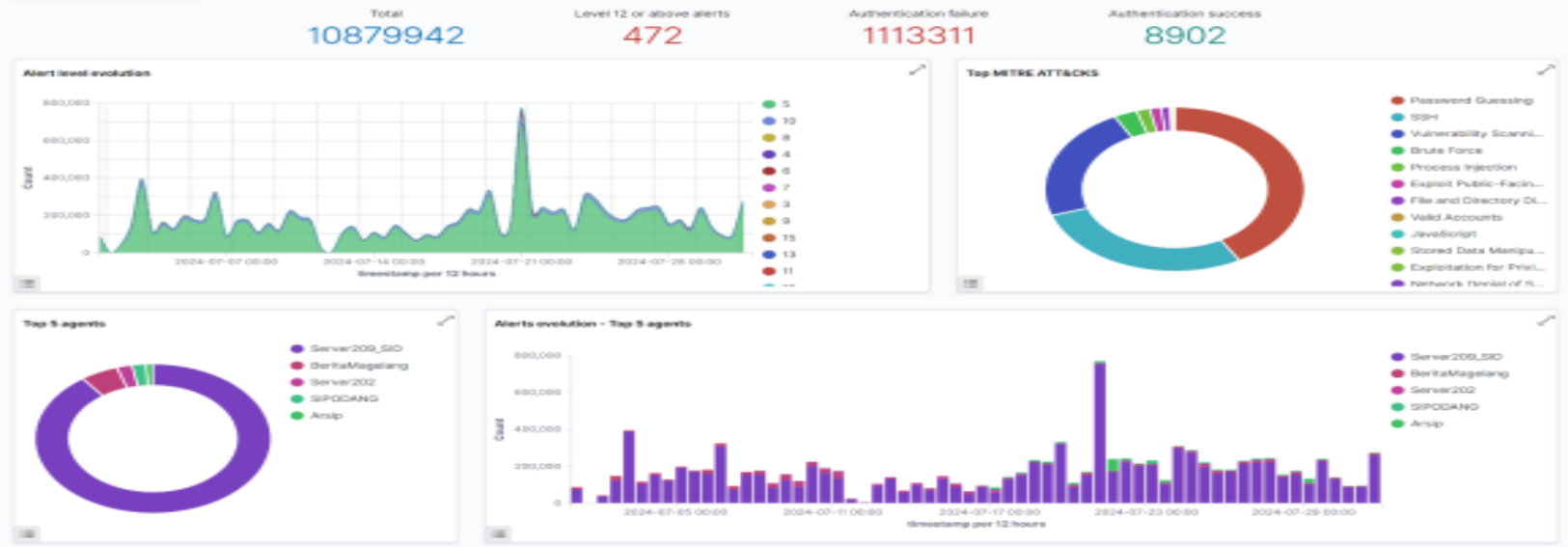
SIEM

SIEM (Security Information and Event Management) adalah sebuah solusi keamanan yang menggabungkan dua fungsi utama **Security Information Management (SIM)** Mengumpulkan, menganalisis, dan menyimpan log data dari berbagai sumber untuk keperluan audit dan kepatuhan. **Security Event Management (SEM)** Memantau dan mengelola peristiwa keamanan secara real-time untuk mendeteksi dan merespons ancaman keamanan.

SIEM memberikan pandangan menyeluruh tentang aktivitas keamanan dalam organisasi dengan mengumpulkan dan menganalisis data dari berbagai sumber seperti firewall, sistem deteksi intrusi (IDS), perangkat jaringan, server, aplikasi, dan endpoint.

Dinas Kominfo Kabupaten Magelang menggunakan Wazuh sebagai SIEM. Wazuh adalah solusi keamanan open-source gratisan yang berfungsi sebagai sistem deteksi intrusi (Intrusion Detection System - IDS) dan platform SIEM (Security Information and Event Management). Wazuh menyediakan fitur-fitur yang kuat untuk pemantauan keamanan, analisis ancaman, dan manajemen kepatuhan.

Analisis Aktivitas Server Menggunakan SIEM



Analisis Tactics

Credential Access	1112097
Lateral Movement	701331
Reconnaissance	561710
Privilege Escalation	51675
Defense Evasion	51051
Initial Access	44197
Discovery	25860
Persistence	8920
Execution	2958
Impact	2381

Analisis Techniques

T1110.001 - Password Guessing 1039812	T1021.004 - SSH 700585	T1595.002 - Vulnerability Scanning 561710	T1110 - Brute Force 72273
T1055 - Process Injection 42097	T1190 - Exploit Public-Facing App... 35278	T1083 - File and Directory Discov... 25860	T1078 - Valid Accounts 8919
T1059.007 - JavaScript 2781	T1565.001 - Stored Data Manipulati... 1771	T1068 - Exploitation for Privilege Es... 652	T1498 - Network Denial of Service 594
T1210 - Exploitation of Remote Serv... 453	T1021 - Remote Services 293	T1059 - Command and Scripting Inte... 177	T1562.001 - Disable or Modify Tools 25
T1212 - Exploitation for Credential Ac... 12	T1499 - Endpoint Denial of Service 12	T1548.003 - Sudo and Sudo Caching 6	T1485 - Data Destruction 4
T1070.004 - File Deletion 4	T1547.006 - Kernel Modules and Exte... 1		

Bug Hunter

Bug Hunter adalah seseorang yang secara aktif mencari dan melaporkan bug atau kerentanan keamanan dalam perangkat lunak, aplikasi, sistem, atau jaringan. Para bug hunter sering kali berpartisipasi dalam meningkatkan keamanan informasi. Para bug hunter menemukan dan melaporkan masalah keamanan sebelum dapat dieksploitasi oleh pihak yang tidak bertanggung jawab.

Open Redirect

Open redirect adalah kerentanan yang umum terjadi pada aplikasi web. Pada dasarnya, open redirect terjadi ketika sebuah situs web memungkinkan pengguna untuk mengubah URL yang mengarahkannya ke halaman lain tanpa memvalidasi dengan benar di mana pengalihan tersebut akan berakhir. Hal ini dapat dieksploitasi oleh penyerang untuk mengalihkan pengguna ke situs yang berbahaya atau mencurigakan.
Kerentanan Open redirect ditemukan oleh :

- Samudera Aziz Alfarisqi pada salah satu halaman website direk.magelangkab.go.id

Reflected Cross-Site Scripting

Dampak Penyerang dapat mengubah atau memanipulasi konten halaman web yang dilihat oleh pengguna, yang dapat digunakan untuk menyebarkan pesan palsu atau menipu pengguna.
Kerentanan Reflected Cross-Site Scripting ditemukan oleh:

- Rafli setyawan Winata pada website dlh.magelangkota.go.id
- Anugrah Gilang Ramadhan pada website desakajoran.magelangkota.go.id
- I Nengah Pranata Adhi Soesastyo pada website amongrasa.magelangkab.go.id
- Maskuri pada website amongrasa.magelangkab.go.id
- Faiz Ahmad Habibi pada website jdih.magelangkab.go.id/olc/Home/forum
- Indo Ahya Maulana pada website jdih.magelangkab.go.id

Sensitive data exposure

Sensitive data exposure terjadi ketika data yang seharusnya dilindungi atau tidak boleh diakses oleh pihak yang tidak berwenang, secara tidak sengaja atau sengaja terbuka kepada pihak yang tidak berhak. Jenis data sensitif yang sering menjadi target termasuk informasi pribadi seperti nomor identitas, informasi kartu kredit, data kesehatan, dan data bisnis yang sensitif.
Kerentanan Sensitive data exposure ditemukan oleh:

- Robi Subagja pada website bkppd.magelangkab.go.id

PHP info exposure

PHP info exposure merujuk pada situasi di mana informasi konfigurasi dan status sistem PHP terbuka untuk publik atau pihak yang tidak berwenang. Biasanya, ini terjadi ketika file atau halaman yang menampilkan output dari fungsi phpinfo() tidak dilindungi dengan baik atau tersedia di server web.
Kerentanan PHP info exposure ditemukan oleh:

- Anugrah Gilang Ramadhan pada website mail.simpkp.magelangkab.go.id dan sig.magelangkab.go.id

Broken Link Hijacking

Broken Link Hijacking (BLH) adalah teknik serangan di mana penyerang memanfaatkan tautan yang rusak atau tidak valid pada halaman web untuk mengambil alih atau memanfaatkan sumber daya yang terkait dengan tautan tersebut. Tautan yang rusak biasanya mengarah ke domain yang sudah tidak aktif atau tidak terdaftar lagi, sehingga memungkinkan penyerang untuk mendaftarkan domain tersebut dan menggunakannya untuk berbagai tujuan berbahaya.
Kerentanan Broken Link Hijacking ditemukan oleh

- Alessandro Christo Rumampuk pada website bkppd.magelangkab.go.id

Sql injection

SQL injection adalah jenis serangan keamanan di mana penyerang menyisipkan atau menyuntikkan kode SQL berbahaya ke dalam input yang diproses oleh aplikasi, dengan tujuan mengakses atau memanipulasi database secara tidak sah. Ini dapat terjadi ketika aplikasi web tidak memvalidasi atau membersihkan data input yang diterima dari pengguna sebelum menggunakannya dalam query SQL
Kerentanan SQL Injection ditemukan oleh:

- Isma Elan Maulani pada website absen.dishub.magelangkab.go.id

Stored Cross-Site Scripting

Stored Cross-Site Scripting (XSS) adalah jenis serangan keamanan di mana penyerang menyuntikkan skrip berbahaya ke dalam konten yang disimpan di server target. Skrip berbahaya ini kemudian dijalankan dalam konteks browser pengguna lain yang mengakses konten tersebut. Karena skrip disimpan di server, semua pengguna yang mengakses halaman atau aplikasi yang terinfeksi akan terkena dampaknya.
Kerentanan Stored Cross-Site Scripting (XSS) ditemukan oleh:

- Miftah Rizky Alamsyah pada website jdih.magelangkab.go.id

INSIDEN SIBER

Insiden siber adalah kejadian yang berdampak negatif pada keamanan sistem informasi, jaringan, atau data. Ini mencakup serangan yang disengaja seperti peretasan, malware, dan pencurian data, serta kejadian yang tidak disengaja seperti kegagalan sistem atau kesalahan manusia yang mengakibatkan kerentanan keamanan.

Web defacement adalah jenis serangan siber di mana penyerang mengubah tampilan situs web dengan cara yang tidak sah. Biasanya, penyerang mengakses server web dan mengubah halaman web, sering kali dengan memasukkan pesan, gambar, atau konten lain yang mungkin bersifat ofensif, politis, atau provokatif. Serangan ini umumnya bertujuan untuk merusak reputasi organisasi, menyampaikan pesan politis, atau sekadar menunjukkan kemampuan peretasan penyerang.

Dampak Web Defacement:

- Kerusakan Reputasi: Situs yang di-deface bisa kehilangan kredibilitas dan kepercayaan dari masyarakat.
- Penyebaran Malware: Penyerang juga bisa menyisipkan malware ke dalam halaman yang di-deface, yang kemudian dapat menginfeksi pengunjung situs.
- Kehilangan Data: Jika penyerang mencuri data pengguna, ini bisa menyebabkan pelanggaran privasi yang serius.

Website Pemerintah Kabupaten Magelang mengalami 3 kali web defacement selama bulan Juli 2024 sebagai berikut:

No	Asset	Nama Serangan	Tanggal Kejadian	Pelaku Serangan	Segment Yang Dirusak	Level Kesulitan	Analisa Dampak
1	disdukcapil.magelangkab.go.id	Web Defacement	13 Juli 2024	tentarasilihwangi@gmail.com	Menyisipkan halaman html verifikasi	Medium	Selesai
2	arsip.magelangkab.go.id	Web Defacement	18 Juli 2024	kazamaj4481@gmail.com	Menyisipkan halaman html verifikasi	Medium	Selesai
3	arsip.magelangkab.go.id	Web Defacement	20 Juli 2024	lhasta477@gmail.com	Menyisipkan halaman html verifikasi	Medium	Selesai

VULNERABILITY ASSESSMENT

Magelang Smart Service

No	Kerentanan	Level
1	Web Application Potentially Vulnerable to Clickjacking	Medium
2	HSTS Missing From HTTPS Server	Medium
3	HTTP TRACE / TRACK Methods Allowed	Medium
4	Web Server Allows Password Auto-Completion	Low

Sidering

No	Kerentanan	Level
1	CGI Generic Local File Inclusion	Medium
2	Web Application Potentially Vulnerable to Clickjacking	Medium
3	CGI Generic Cookie Injection Scripting	Medium
4	CGI Generic HTML Injections (quick test)	Medium
5	HSTS Missing From HTTPS Server (RFC 6797)	Medium
6	CGI Generic XSS (quick test)	Medium
7	HTTP TRACE / TRACK Methods Allowed	Medium
8	Web Server Allows Password Auto-Completion	Low

Sipodang

No	Kerentanan	Level
1	Web Application Potentially Vulnerable to Clickjacking	Medium
2	HSTS Missing From HTTPS Server (RFC 6797)	Medium
3	Apache Tomcat 9.0.0.M1 < 9.0.90	Medium
4	Apache Tomcat Default Files	Medium
5	Web Server Allows Password Auto-Completion	Low

Arsip

No	Kerentanan	Level
1	HSTS Missing From HTTPS Server (RFC 6797)	Medium
2	Web Server Allows Password Auto-Completion	Low

Dukcapil

No	Kerentanan	Level
1	Web Application Potentially Vulnerable to Clickjacking	Medium
2	HSTS Missing From HTTPS Server (RFC 6797)	Medium
3	HTTP TRACE / TRACK Methods Allowed	Medium
4	WordPress User Enumeration	Medium

DOKUMEN
RAHASIA

31 Mei 2024

No. 071/D21/LAP/05/2024

Pemerintah Kabupaten Magelang

Laporan Hasil ITSA

Information Technology Security Assessment

Badan Siber dan Sandi Negara

Direktorat Operasi Keamanan Siber
Deputi Bidang Operasi Keamanan Siber dan Sandi

Jl. Harsono No. 70, Pasar Minggu,
Jakarta Selatan 12550
Email: itsa@bssn.go.id

Temuan kerentanan
API Menoreh

Tampilan Sistem Elektronik

Tinjauan Umum

Deskripsi	Untuk layanan administrasi perubahan data kependudukan yang berupa pengelolaan dokumen dokumen persyaratan perubahan data
Alamat URL	https://itsa-menoreh.magelangkab.go.id
Alamat IP	103.115.104.195
Tanggal Pelaksanaan	27 Mei s/d 31 Mei 2024
Teknik Pengujian	☑ *Black-Box Testing* ☑ *Grey-Box Testing* ☐ *White-Box Testing*

Temuan kerentanan
Sistem informasi Desa

Tampilan Sistem Elektronik

Tinjauan Umum

Deskripsi	Sebagai layanan informasi desa baik kegiatan , persuratan maupun kependudukan yang pengelolaan informasinya dilakukan oleh pemerintah desa.
Alamat URL	https://itsa-sid.magelangkab.go.id/landing
Alamat IP	103.115.104.195
Tanggal Pelaksanaan	27 Mei s/d 31 Mei 2023
Teknik Pengujian	☑ *Black-Box Testing* ☑ *Grey-Box Testing* ☐ *White-Box Testing*

Temuan kerentanan
Aplikasi TTE

Tampilan Sistem Elektronik

Tinjauan Umum

Deskripsi	Layanan pemberian tandatangan elektronik
Alamat URL	itsa-tte.magelangkab.go.id
Alamat IP	103.115.104.195
Tanggal Pelaksanaan	27 Mei s/d 31 Mei 2024
Teknik Pengujian	☑ *Black-Box Testing* ☑ *Grey-Box Testing* ☐ *White-Box Testing*

Temuan kerentanan
Aplikasi Single Log On

Tampilan Sistem Elektronik

Tinjauan Umum

Deskripsi	Sebagai manajemen User untuk aplikasi MSS (Magelang Smart Service)
Alamat URL	https://itsa-slo.magelangkab.go.id/login
Alamat IP	103.115.104.195
Tanggal Pelaksanaan	27 Mei s/d 31 Mei 2024
Teknik Pengujian	☑ *Black-Box Testing* ☑ *Grey-Box Testing* ☐ *White-Box Testing*

PENJELASAN KERENTANAN

Stored XSS (Cross-Site Scripting)

Stored XSS adalah jenis serangan XSS di mana kode berbahaya disimpan di server dan kemudian dieksekusi saat pengguna yang rentan mengakses halaman yang berisi kode tersebut. Tidak seperti *Reflected XSS*, di mana kode berbahaya dikirim kembali segera dalam respon HTTP, *Stored XSS* lebih berbahaya karena efeknya lebih luas dan tahan lama.

Dampak Serangan :

1. Pengambilalihan Akun: Penyerang dapat mencuri cookies sesi pengguna, yang dapat digunakan untuk mengambil alih akun pengguna.
2. Eksekusi Perintah: Penyerang dapat menjalankan perintah berbahaya di browser korban.
3. Pencurian Data: Informasi sensitif seperti data pribadi pengguna dapat dicuri.
4. Manipulasi Tampilan Halaman: Penyerang dapat mengubah konten halaman web yang dilihat oleh pengguna.

Open Redirect

Open Redirect adalah kerentanan di mana aplikasi web mengarahkan pengguna ke URL yang dikendalikan oleh penyerang. Ini bisa digunakan untuk serangan phishing atau untuk memanipulasi pengguna agar mengunjungi situs berbahaya:

Dampak Serangan :

1. *Phishing*: Pengguna dapat diarahkan ke situs phishing yang terlihat seperti halaman login WordPress, di mana kredensial mereka bisa dicuri.
2. Eksekusi Perintah Berbahaya: Penyerang dapat mengarahkan pengguna ke situs yang menjalankan skrip berbahaya atau malware.
3. Penurunan Kepercayaan Pengguna: Pengguna yang diarahkan ke situs berbahaya mungkin kehilangan kepercayaan pada integritas situs asli.

Email Address Disclosure

Email Address Disclosure adalah kerentanan di mana alamat *email* pengguna dapat diakses oleh pihak yang tidak berwenang. Ini bisa digunakan oleh penyerang untuk *spam*, *phishing*, atau serangan lebih lanjut yang memanfaatkan informasi pribadi pengguna

Dampak Serangan :

1. *Spam*: Alamat *email* yang terungkap dapat digunakan untuk mengirim spam kepada pengguna.
2. *Phishing*: Penyerang dapat menggunakan alamat email yang terungkap untuk mengirim email phishing kepada pengguna.
3. Privasi Pengguna: Pelanggaran privasi karena informasi kontak pribadi pengguna terekspos kepada publik.

Reflected Cross-Site Scripting (XSS)

Reflected Cross-Site Scripting (XSS) adalah jenis kerentanan keamanan yang terjadi ketika data yang disediakan oleh pengguna langsung direfleksikan kembali oleh aplikasi web tanpa validasi atau penyaringan yang memadai. Ini memungkinkan penyerang untuk menyuntikkan skrip berbahaya yang dijalankan di *browser* pengguna yang tidak menaruh curiga

Dampak Serangan :

1. Pencurian Data: Penyerang dapat mencuri *cookie* sesi, token autentikasi, atau informasi sensitif lainnya.
2. Pengambilalihan Akun: Dengan mencuri token sesi, penyerang dapat mengambil alih akun pengguna.
3. Pengubahan Konten: Penyerang dapat mengubah konten halaman web yang dilihat oleh pengguna.
4. Serangan *Phishing*: Penyerang dapat mengarahkan korban ke halaman *phishing* yang terlihat seperti halaman *login* asli.

Cross-Site Request Forgery (CSRF)

Cross-Site Request Forgery (CSRF) adalah jenis kerentanan keamanan di mana penyerang memaksa pengguna yang telah terautentikasi untuk melakukan tindakan yang tidak diinginkan pada aplikasi web yang mereka autentikasi. Serangan *CSRF* mengeksploitasi kepercayaan yang dimiliki aplikasi web terhadap pengguna yang sah.

Dampak Serangan :

- Transfer Dana yang Tidak Sah: Penyerang dapat memindahkan dana dari akun pengguna.
- Perubahan Informasi: Penyerang dapat mengubah informasi akun, seperti alamat *email* atau kata sandi.
- Aksi Tidak Sah Lainnya: Penyerang dapat melakukan tindakan apa pun yang diizinkan untuk pengguna, seperti menghapus data, mengirim pesan, atau melakukan transaksi.

Content from Multipart Emails Leaked

Content from Multipart Emails Leaked adalah jenis kerentanan keamanan yang terjadi ketika konten dari *email* multipart terekspos atau bocor, memungkinkan penyerang untuk mengakses informasi sensitif yang seharusnya tidak mereka lihat.

Dampak Serangan

- Pelanggaran Privasi: Data pribadi atau sensitif pengguna dapat terekspos.
- Kebocoran Informasi Rahasia: Informasi rahasia perusahaan atau kredensial dapat bocor.
- Eksploitasi Informasi: Informasi yang bocor dapat digunakan oleh penyerang untuk melakukan serangan lebih lanjut, seperti *phishing* atau *social engineering*.

SQL Injection (SQLi)

SQL Injection (SQLi) adalah jenis kerentanan keamanan yang memungkinkan penyerang untuk menyisipkan atau "menyuntikkan" perintah *SQL* berbahaya ke dalam kueri yang dijalankan oleh basis data aplikasi. Serangan ini dapat mengakibatkan akses tidak sah ke data, pengubahan data, atau bahkan pengambilalihan kontrol penuh atas *server* basis data.

Dampak Serangan

- Pengungkapan Data: Penyerang dapat mengakses data sensitif yang seharusnya dilindungi.
- Modifikasi Data: Penyerang dapat mengubah atau menghapus data dalam basis data.
- Pengambilalihan Akun: Penyerang dapat mengakses akun pengguna lain atau meningkatkan hak akses mereka.
- Eksekusi Perintah Berbahaya: Dalam kasus yang lebih parah, penyerang dapat mengeksekusi perintah berbahaya di *server* basis data, yang dapat mengakibatkan kerusakan sistem secara keseluruhan.

Data Exposure

Data Exposure adalah jenis kerentanan keamanan di mana informasi sensitif atau rahasia secara tidak sengaja terekspos kepada pihak yang tidak berwenang. Ini bisa terjadi karena berbagai alasan, termasuk kesalahan konfigurasi, kelemahan perangkat lunak, atau kesalahan dalam proses pengembangan. Data yang terekspos dapat mencakup informasi pribadi, kredensial pengguna, data keuangan, atau informasi bisnis rahasia.

Dampak Serangan

- Pelanggaran Privasi: Informasi pribadi atau sensitif pengguna dapat terekspos, melanggar privasi mereka.
- Kehilangan Kepercayaan: Pengguna mungkin kehilangan kepercayaan pada organisasi atau layanan yang mengalami kebocoran data.
- Kerugian Finansial: Data keuangan atau bisnis yang terekspos dapat mengakibatkan kerugian finansial bagi organisasi.
- Serangan Lebih Lanjut: Data yang terekspos dapat digunakan oleh penyerang untuk melakukan serangan lebih lanjut, seperti *phishing* atau pencurian identitas.

Multiple Stored Cross-Site Scripting (XSS)

Multiple Stored Cross-Site Scripting (XSS) adalah jenis kerentanan keamanan yang terjadi ketika aplikasi web memungkinkan penyerang untuk menyuntikkan skrip berbahaya ke dalam banyak lokasi atau parameter yang berbeda, yang kemudian disimpan oleh aplikasi dan dijalankan di browser pengguna lain. Kerentanan ini lebih berbahaya dibandingkan dengan *single stored XSS* karena melibatkan banyak titik injeksi, memperbesar risiko dan dampak serangan.

Dampak Serangan

- Pencurian Data: Penyerang dapat mencuri cookie sesi, token autentikasi, atau informasi sensitif lainnya dari pengguna.
- Pengambilalihan Akun: Dengan mencuri token sesi, penyerang dapat mengambil alih akun pengguna.
- Pengubahan Konten: Penyerang dapat mengubah konten halaman web yang dilihat oleh pengguna.
- Serangan Phishing: Penyerang dapat mengarahkan korban ke halaman phishing yang terlihat seperti halaman login asli.

Unauthenticated Blind Server-Side Request Forgery (SSRF)

Unauthenticated Blind Server-Side Request Forgery (SSRF) adalah jenis kerentanan keamanan di mana penyerang dapat membuat server aplikasi mengirim permintaan *HTTP* ke lokasi yang dipilih penyerang tanpa memerlukan autentikasi. Istilah "*blind*" menunjukkan bahwa penyerang tidak menerima respons langsung dari server yang diserang, sehingga mereka tidak dapat melihat hasil permintaan secara langsung. Meskipun demikian, penyerang masih dapat menyalahgunakan kerentanan ini untuk berbagai tujuan berbahaya.

Dampak Serangan

- Pengungkapan Informasi Sensitif: Penyerang dapat mengakses informasi sensitif dari server *internal* atau layanan *cloud*.
- Pengambilalihan Akun: Penyerang dapat memperoleh kredensial atau token autentikasi yang digunakan oleh *server* untuk berkomunikasi dengan layanan lain.
- Pemindaian Jaringan Internal: Penyerang dapat memetakan layanan dan *server* yang berjalan di jaringan *internal*.
- Serangan Lanjutan: Penyerang dapat menggunakan *server* yang tereksploitasi untuk melancarkan serangan lebih lanjut, seperti *Remote Code Execution (RCE)* atau *Denial of Service (DoS)*.

Directory Traversal

Directory Traversal, atau juga dikenal sebagai *Path Traversal*, adalah jenis kerentanan keamanan yang memungkinkan penyerang untuk mengakses *file* dan direktori di luar direktori yang diizinkan oleh aplikasi web. Dengan mengeksploitasi kerentanan ini, penyerang dapat membaca, menulis, atau mengeksekusi *file* yang seharusnya tidak dapat diakses, yang dapat mengakibatkan paparan data sensitif, kerusakan sistem, atau serangan lebih lanjut.

Dampak Serangan

- Pengungkapan Data Sensitif: Penyerang dapat mengakses *file* yang berisi data sensitif seperti kredensial, konfigurasi, atau data pengguna.
- Kerusakan Sistem: Penyerang dapat menulis ke *file* sistem yang penting, merusak atau mengubah konfigurasi sistem.
- Eksekusi Kode Berbahaya: Jika penyerang dapat menulis *file* ke lokasi yang dieksekusi oleh sistem, mereka dapat menempatkan dan menjalankan kode berbahaya.

Web Application Potentially Vulnerable to Clickjacking

Server web jarak jauh tidak menyetel header respons X-Frame-Options atau header respons 'frame-ancestors' Content-Security-Policy di semua respons konten. Hal ini berpotensi mengekspos situs terhadap serangan clickjacking atau UI redress, di mana penyerang dapat mengelabui pengguna agar mengeklik area halaman yang rentan yang berbeda dari apa yang dirasakan pengguna sebagai halaman tersebut. Hal ini dapat mengakibatkan pengguna melakukan transaksi penipuan atau jahat

HSTS Missing From HTTPS Server

Server web jarak jauh tidak memberlakukan HSTS, sebagaimana didefinisikan oleh RFC 6797. HSTS adalah header respons opsional yang dapat dikonfigurasi di server untuk memerintahkan browser agar hanya berkomunikasi melalui HTTPS. Kurangnya HSTS memungkinkan serangan penurunan versi, serangan man-in-the-middle SSL-stripping, dan melemahkan perlindungan pembajakan cookie

HTTP TRACE / TRACK Methods Allowed

Server web jarak jauh mendukung metode TRACE dan/atau TRACK. TRACE dan TRACK adalah metode HTTP yang digunakan untuk men-debug koneksi server web.

Web Server Allows Password Auto-Completion

Server web jarak jauh berisi setidaknya satu bidang formulir HTML yang memiliki input bertipe 'kata sandi' yang mana 'pelengkapan otomatis' tidak disetel ke 'nonaktif'. Meskipun hal ini tidak mewakili risiko bagi server web ini, ini berarti bahwa pengguna yang menggunakan formulir yang terpengaruh mungkin memiliki kredensial yang tersimpan di browser mereka, yang pada gilirannya dapat menyebabkan hilangnya kerahasiaan jika salah satu dari mereka menggunakan host bersama atau jika mesin mereka disusupi pada suatu saat

SURAT EDARAN BADAN SIBER DAN SANDI NEGARA

BADAN SIBER DAN SANDI NEGARA
Jalan Raya Muchtar Nomor 70, Kel. Bojongsari Lama, Kec. Bojong Sari, Depok 16516
Telepon (021) 77973360, Faksimile (021) 78844104, 77973579
Website : https://bssn.go.id, *E-mail* : humas@bssn.go.id

Yth.

1. Pejabat Pengelola Teknologi Informasi dan Komunikasi di Instansi Pemerintah Pusat;
2. Pejabat Pengelola Teknologi Informasi dan Komunikasi di Instansi Pemerintah Daerah.

di
Tempat

SURAT EDARAN
NOMOR 42 TAHUN 2024
TENTANG
HIMBAUAN PENCEGAHAN DAN MITIGASI *RANSOMWARE*
PADA LAYANAN PUBLIK

A. UMUM

Ransomware merupakan salah satu insiden siber yang belakangan ini terjadi di sektor pemerintahan. Tidak hanya menimbulkan gangguan proses bisnis yang sedang berjalan dan kerugian finansial, hal ini juga dapat merusak reputasi dan kepercayaan masyarakat terhadap pemerintah. Oleh karena itu, Badan Siber dan Sandi Negara memandang perlu untuk mengeluarkan Surat Edaran ini guna menghimbau agar seluruh IPPD dapat mencegah dan mengantisipasi terjadinya insiden siber, terutama *ransomware* pada layanan publik.

B. DASAR

1. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
2. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi dan Standar dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik;
3. Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Struktur Organisasi dan Tata Kerja Badan Siber dan Sandi Negara.

PELAKSANAAN HIMBAUAN :

1. Melakukan identifikasi dan kategorisasi Sistem Elektronik
2. Melakukan dan memastikan *update* dan *patching* perangkat lunak dan sistem operasi
3. Melaksanakan prosedur *backup* dan *recovery*
4. Menggunakan *anti virus* / *anti malware* dengan versi terbaru
5. Melaporkan pelaksanaan kegiatan pengamanan kepada BSSN

TINDAK LANJUT SURAT EDARAN BSSN

Segera melakukan identifikasi Sistem Elektronik dan *updating* serta *patching* perangkat lunak yang digunakan pada layanan (meminimalkan terjadinya risiko serangan ransomware).

Tujuan

Instansi Pusat dan Instansi Pemerintah Daerah dapat mengantisipasi dan memitigasi terjadinya insiden siber, salah satunya yaitu *Ransomware*

Instansi Pusat dan Instansi Pemerintah Daerah dapat meminimalisir celah kerentanan yang dimanfaatkan untuk mengeksploitasi situs-situs layanan publik di sektor Pemerintahan

SEBERAPA BANYAK SISTEM ELEKTRONIK YANG DIMILIKI?

Sumber: LetsDefend, 2024

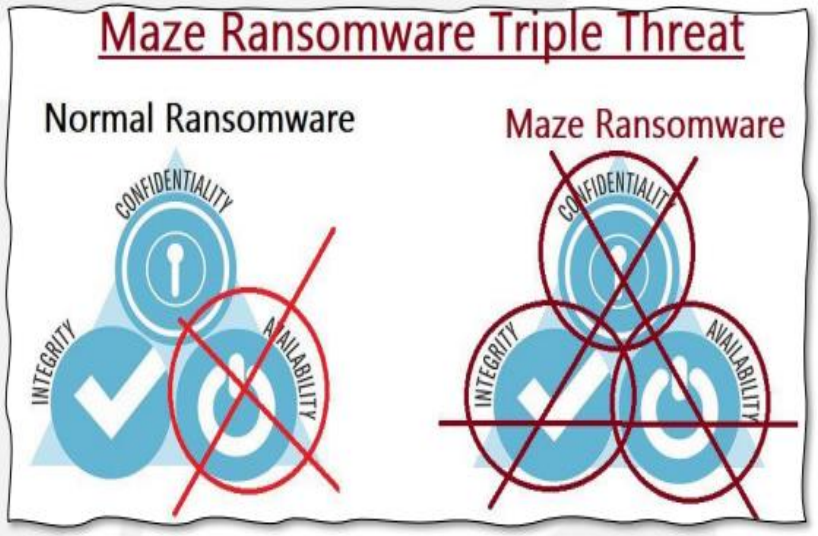
ASPEK KEAMANAN DATA DAN INFORMASI

Informasi hanya tersedia bagi yang terotorisasi saja (**C** = ***Confidentiality***/kerahasiaan).

Informasi tersedia ketika dibutuhkan (**A** = ***Availability***/ketersediaan).

Keutuhan informasi terjaga, baik ketika diproduksi, disimpan, ataupun ditransmisikan (**I** = ***Integrity***/Keutuhan)

ASPEK KEAMANAN DATA DAN INFORMASI



Contoh ancaman aspek keamanan dari Ransomware Maze

UPDATE DAN *PATCHING* PERANGKAT LUNAK DAN SISTEM OPERASI

Pembaruan Sistem dan Perangkat Lunak secara rutin dapat memitigasi risiko Ransomware

Pembaruan dapat menyediakan fitur baru, juga memperbaiki kerentanan keamanan yang dimanfaatkan *threat actor*

- Menerapkan patch secara teratur
- Menggunakan alat manajemen patch
- Menguji patch sebelum penerapan patching
- Membuat rencana pemulihan insiden siber
- Prioritaskan melakukan patching keamanan yang kritis
- Mendokumentasikan proses manajemen patch

APA SAJA YANG DILAKUKAN PATCHING?

Sistem Operasi

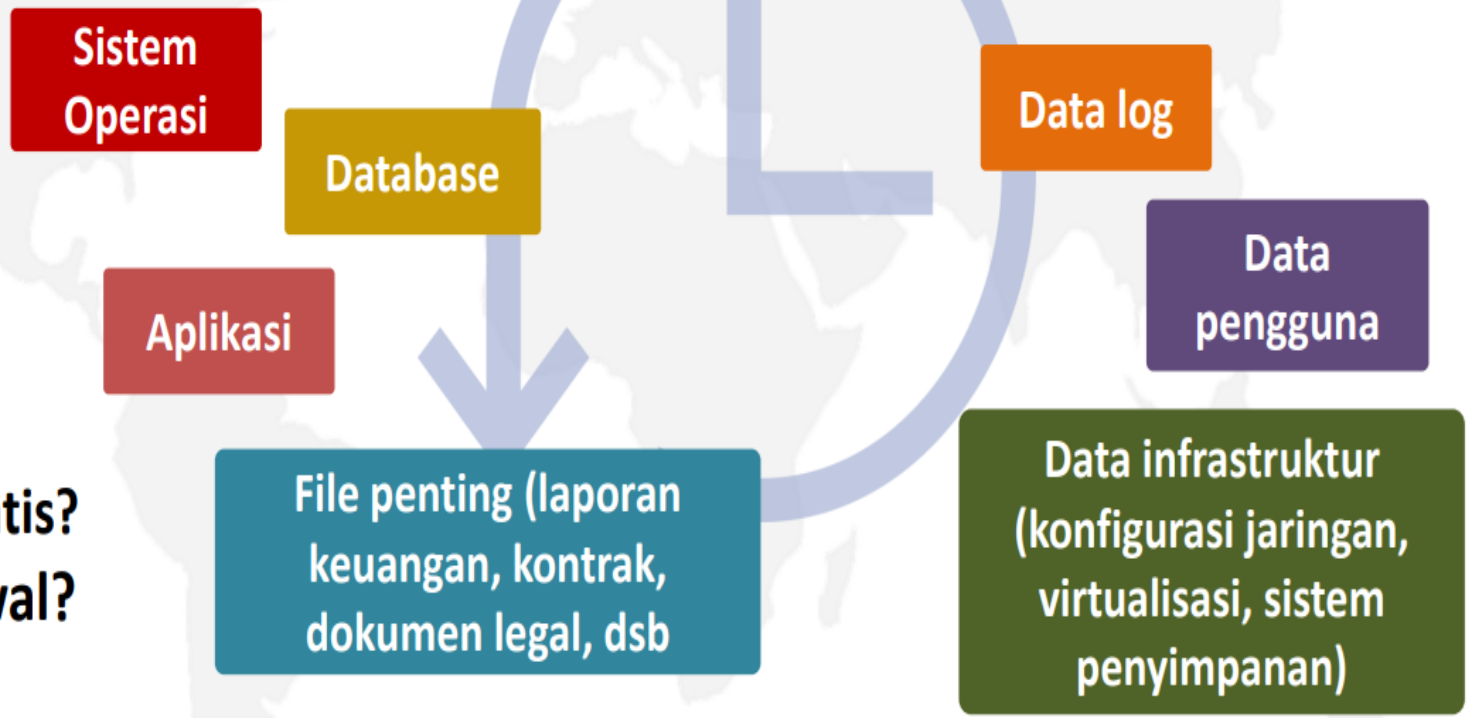
Perangkat TIK

Driver **Firmware**

Aplikasi

PENCADANGAN (BACKUP)

Apa saja data yang penting dan harus dicadangkan?



Otomatis?
Terjadwal?

PENTINGNYA PENCADANGAN (BACKUP) DATA SECARA TERATUR

Melindungi data dari kehilangan atau kerusakan (serangan malware, bencana alam)

Mempermudah pemulihan data pada saat kehilangan data (tanpa harus membayar kepada *threat actor*)

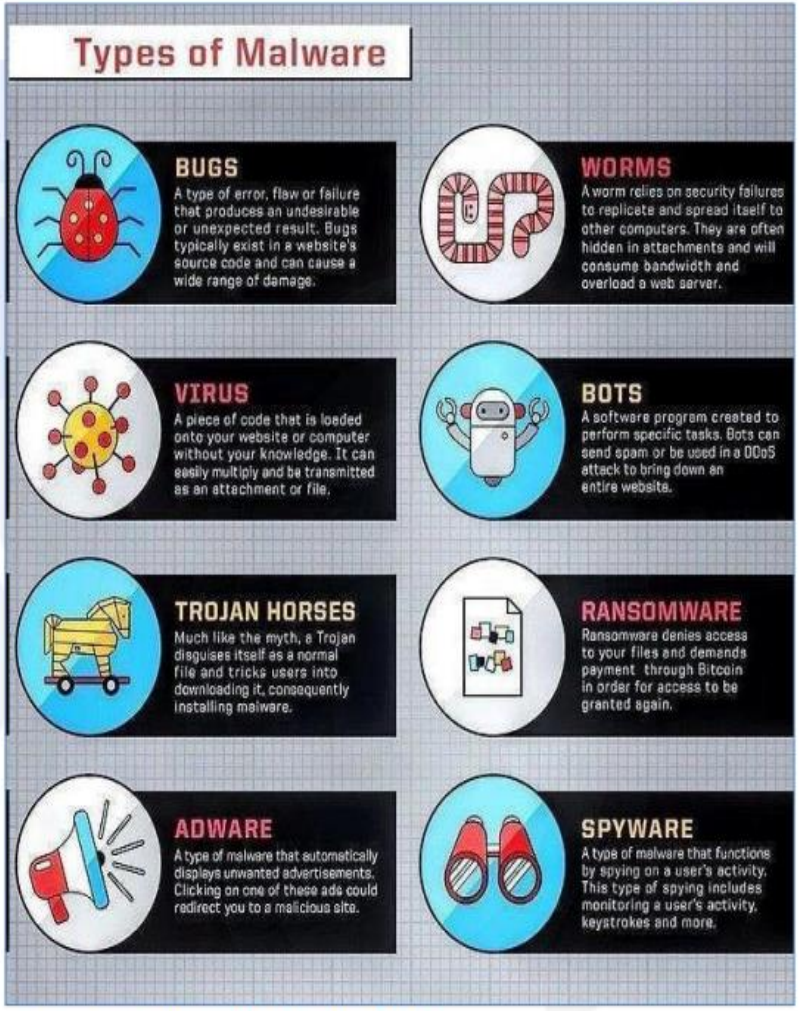
Menghemat waktu dan anggaran organisasi serta mencegah kerugian akibat kegagalan operasional

Meningkatkan ketersediaan layanan dan reputasi instansi

ANTI VIRUS DAN ANTI MALWARE

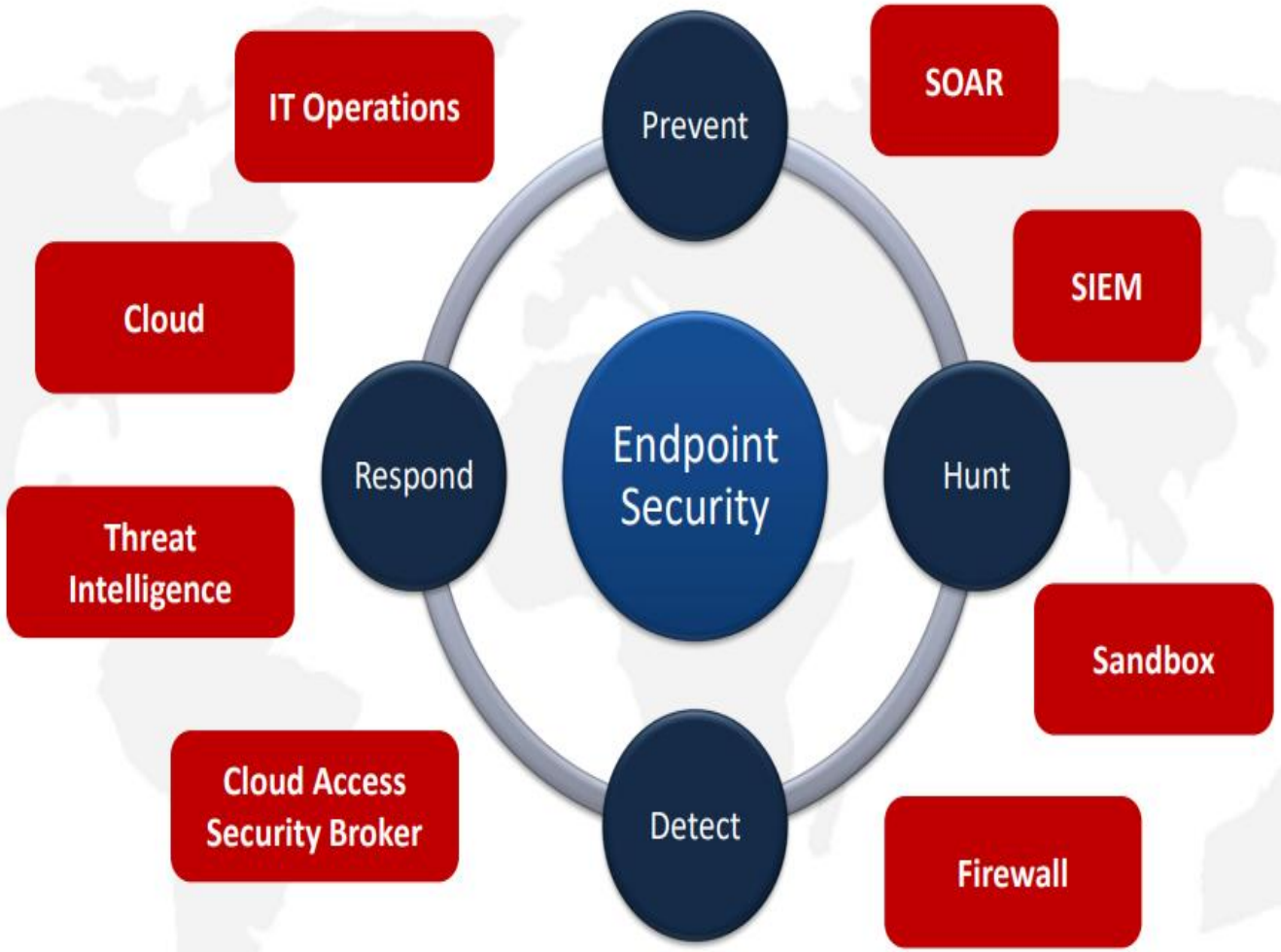
Antivirus ataupun anti-malware dapat membantu mencegah dan melindungi Ransomware yang merusak sistem

Teknologi ini perlu digabungkan dengan praktik keamanan lainnya, sebagai Upaya meningkatkan ketahanan organisasi terhadap Ransomware



Sumber: LetsDefend, 2024

ANTI VIRUS DAN ANTI MALWARE




"Ingatlah bahwa :
Kechilafan Satu
Orang Sahaja
Tjukup Sudah
Menjebabkan
Keruntuhan Negara"
(dr. Roebiono Kertopati)
TERIMA KASIH