Sosialisasi Proteksi Keamanan Website Pemerintah

BANDUNG, 30 JULI 2019

Firdaus Kifli S.ST. M.AP.
Kepala Subdirektorat. PIIKN III

BADAN SIBER DAN SANDI NEGARA

PROFESIONAL INTEGRITAS ADAPTABILITAS TEKNOLOGI TEPERCAYA

OUTLINE

1. BADAN SIBER DAN SANDI NEGARA (BSSN)
2. DATA INSIDEN SIBER
3. STATISTIK KERENTANAN
4. LANDASAN PENERAPAN KEAMANAN SPBE
5. WEB APPLICATION SECURITY
6. REKOMENDASI

KEAMANAN SIBER BERDASARKAN PERPRES 53 TAHUN 2017

POLA KOORDINASI BSSN

Internet/Communication Provider

TELKOMSEL, XL, Telkom Indonesia, indosat ooredoo, AXIS, 3 (Tri), lintasarta

Security Operation Centre (SOC)

- Gov. SOC
- Private. SOC
- Critical Infrastructure SOC
- Commerce SOC
- Community (Honeynet Ind, OWASP Ind)

Information sharing & situational awareness

Research & Development, Professional Certification Agency

BPPT, ITB, ISACA, ITS, (ISC)², EC-Council

Monitoring security events in network access point

Building cybersecurity regulation & legislation

International Cybersecurity Agency

FIRST, enisa, CyberSecurity Malaysia, NICT, ITU

Threat Intelligence, Diplomacy

International Cooperation

BADAN SIBER DAN SANDI NEGARA — BSSN

Building cybersecurity culture & capacity

Public Trust & Incident Response

Association

ATSI Asosiasi Penyelenggara Telekomunikasi Seluruh Indonesia, id Pandi, APJII, APJATEL Asosiasi Penyelenggara Jaringan Telekomunikasi, Federasi Teknologi Informasi Indonesia (FTII)

Fighting against Cybercrime & Law Enforcement

Defence operation & Join Task Force

Cyber Security Incident Response Readiness

Cyber Defence Agency

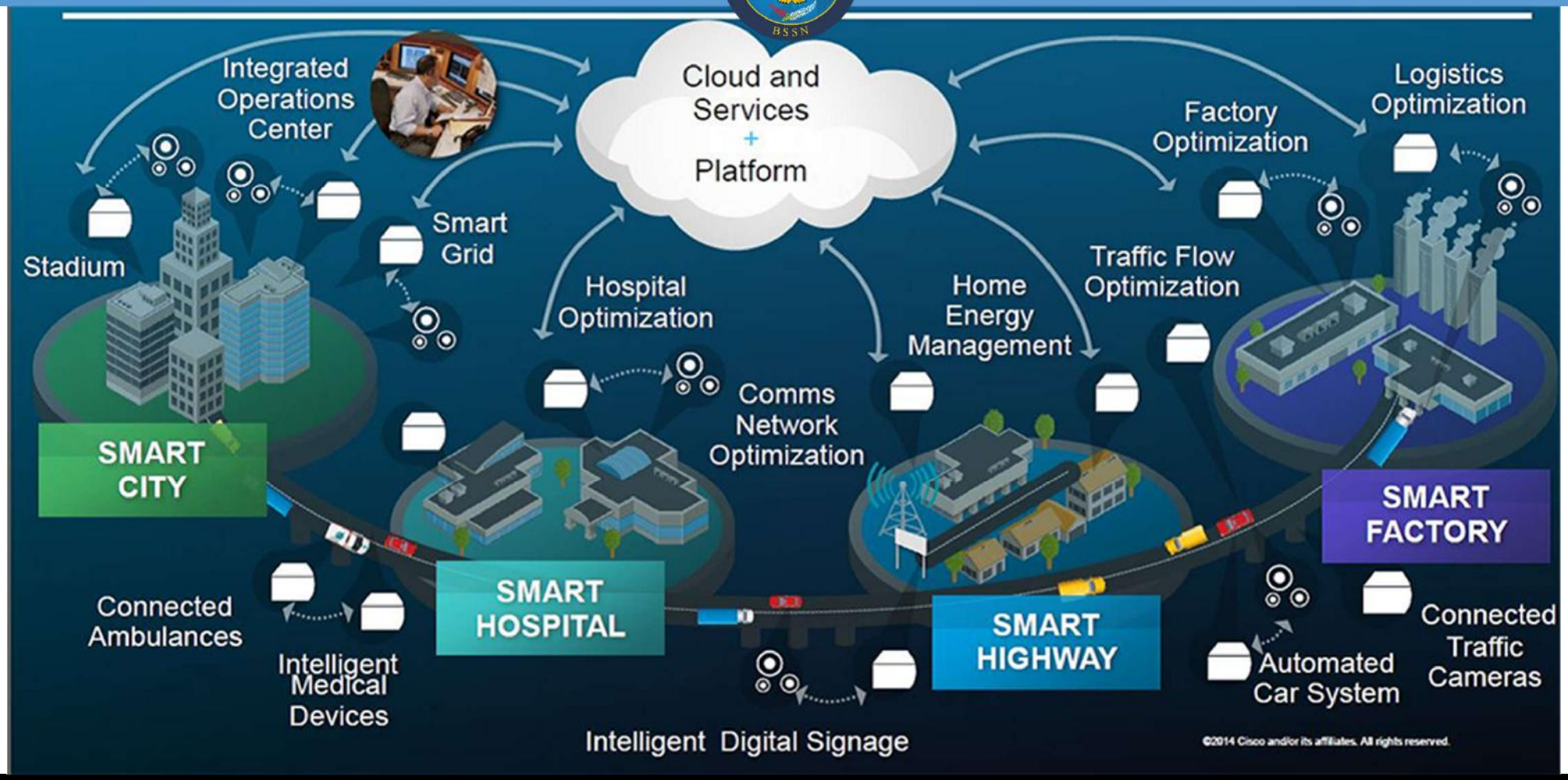
Badan Intelijen Negara Republik Indonesia, Kementerian Pertahanan Republik Indonesia

Computer Emergency Response Team (CERT)

- Gov. CSIRT
- Private CSIRT
- Community CSIRT
- Critical Infrastructure CSIRT
- Academic CSIRT

PROFESIONAL INTEGRITAS ADAPTABILITAS TEKNOLOGI TEPERCAYA

IoT Business and Society



DATA INSIDEN SIBER

AMERICAN MEDICAL COLLECTION AGENCY (AMCA) DATA BREACH

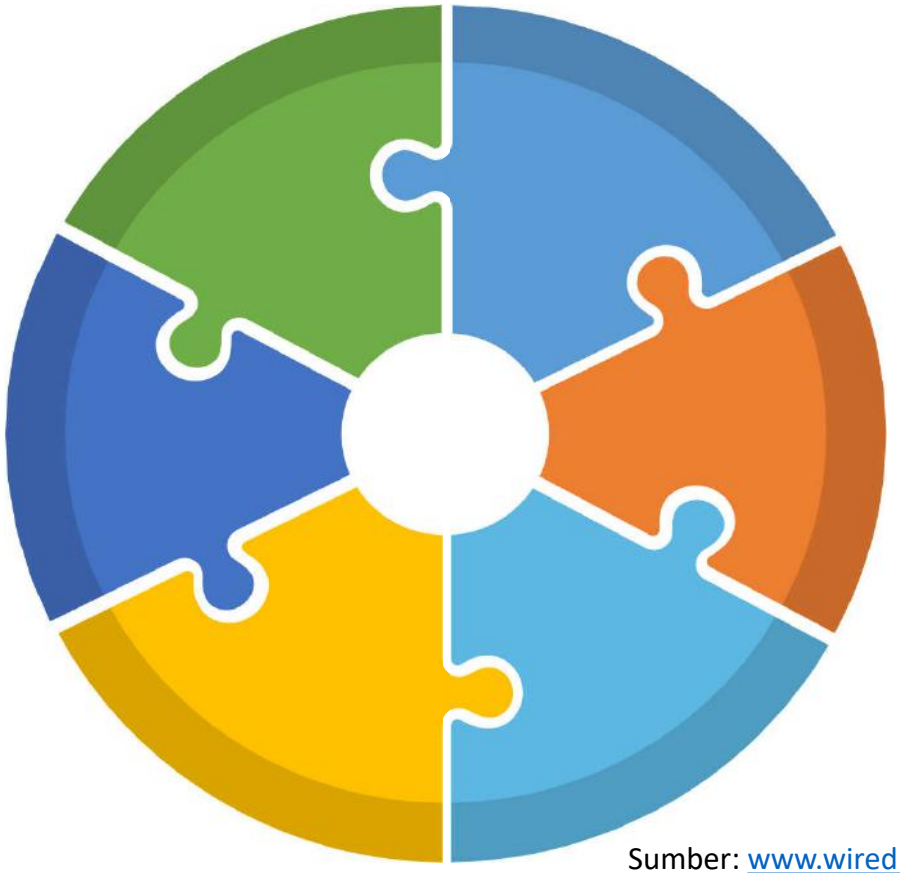
Sebanyak 7,7 Juta data pelanggan bocor dari database AMCA pada Bulan Juni 2019. data tersebut berisi biodata pasien, nomor asuransi kesehatan, dan saldo jatuh tempo dari asuransi milik pasien.

FIRST AMERICAN

First American, sebuah perusahaan properti besar di Amerika menampilkan informasi Jutaan pelanggannya di Halaman Website mereka Informasi yang ditampilkan berisi bioadata pelanggan, nomor jaminan sosial, akun bank, dan dokumen pajak. Kejadian tersebut ditemukan pada Bulan Mei oleh Jurnalis Keamanan Informasi Brian Krebs.

CYBERWAR PLAN AGAINTS IRAN

Dampak dari serangan terhadap dua kapal tanker milik US, Presiden Trump menuding Iran menjadi dalang penyerangan tersebut. Alih-alih melakukan serangan fisik, Presiden Trump menyetujui untuk melakukan serangan siber kepada fasilitas nuklir milik Iran



US CUSTOM & BORDER PROTECTION (CBP) CONTRACTOR DATA BREACHES

Pada Bulan Mei, *Hacker* mempublish 100,000 data *passport* milik penumpang yang mereka dapat dari Kontraktor yang bekerja sama dengan Bea dan Cukai Amerika Serikat bernama Perceptics. Kebocoran data ini menjadi pukulan bagi Amerika, karena kenapa data yang sifatnya terbatas dapat disimpan oleh Kontraktor

RANSOMWARE-LOCKERGOGA

Ransomware LockerGoga mengincar data-data di sektor industri dan manufaktur. LockerGoga mengganggu sistem otomatisasi Industri dan mengakibatkan berhentinya produksi.

SUPPLY CHAIN ATTACKS

Pada Bulan Maret Kaspersky melaporkan adanya celah kerawanan pada system live update komputer ASUS. Akibatnya hacker dapat menyusupkan malware pada celah tersebut dan mengancam jutaan pengguna ASUS. System live update adalah layanan purna jual dari ASUS untuk melakukan update driver perangkat (patching) secara online.

Sumber: www.wired.com/Biggest-Cybersecurity-Crises-2019-Sofar/

STATISTIK KERENTANAN

46%
Website Memiliki Tingkat Kerentanan **HIGH**

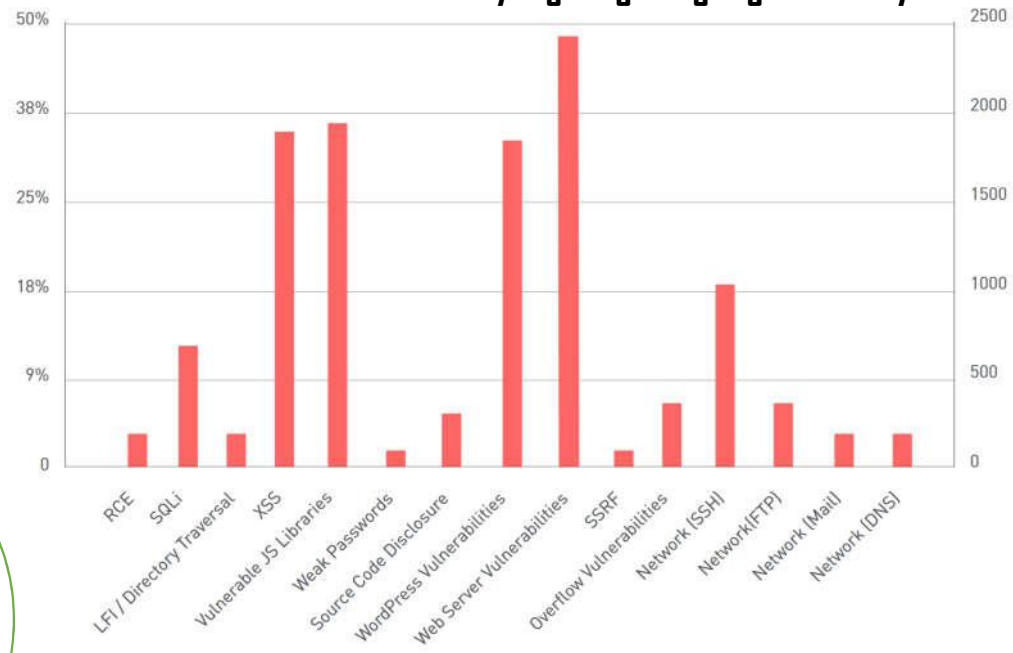
9%
Network Memiliki Tingkat Kerentanan **HIGH**

87%
Website Memiliki Tingkat Kerentanan **MEDIUM**

30%
Aplikasi Web rentan Terhadap Serangan XSS

Sumber: 2019 edition of the Acunetix Web Application Vulnerability Report

Distribusi Jenis Kerentanan yang tergolong High Severity



This year's report contains the results and analysis of vulnerabilities detected over the previous 12 months, across 10,000 scan targets

Open Web Application Security Project (OWASP)

OWASP:2017 TOP 10 APPLICATION SECURITY RISK

A1 Injection

Aplikasi tidak melakukan validasi, filter, atau sanitasi terhadap data yang diinputkan

A2 Broken Authentication

Aplikasi mengijinkan serangan *brute force,* penerapan pengamanan kredensial yang lemah

A3 Sensitive Data Exposure

Tidak menerapkan pengamanan perlindungan data dengan baik

A4 XML External Entities

Tidak dialkukannya Sanitasi / validasi terhadap XML yang di unggah oleh pengguna

A5 Broken Access Control

Access control yang tidak di terapkan dengan baik memungkinkan penyerang untuk melewati proses autorisasi

A6 Security Misconfiguration

Tidak dilakukan hardening keamanan yang sesuai, menggunakan setting default

A7 Cross Site Scripting

menginjinkan user untuk menambahkan kode custom ke sebuah path URL, atau form input

A8 Insecure Deserialization

Penyerang dapat memodifikasi logika aplikasi atau dapat mencapai *remote code execution*

A9 Using Components With Known Vulnerabilities

Menggunakan komponen sepert library, plugin, framework, dll yang memiliki kerentanan dan diketahui oleh publik

A10 Insufficient Logging and Monitoring

Tidak menerapkan logging dan Monitoring

STATISTIK KERENTANAN

TOTAL LAPORAN

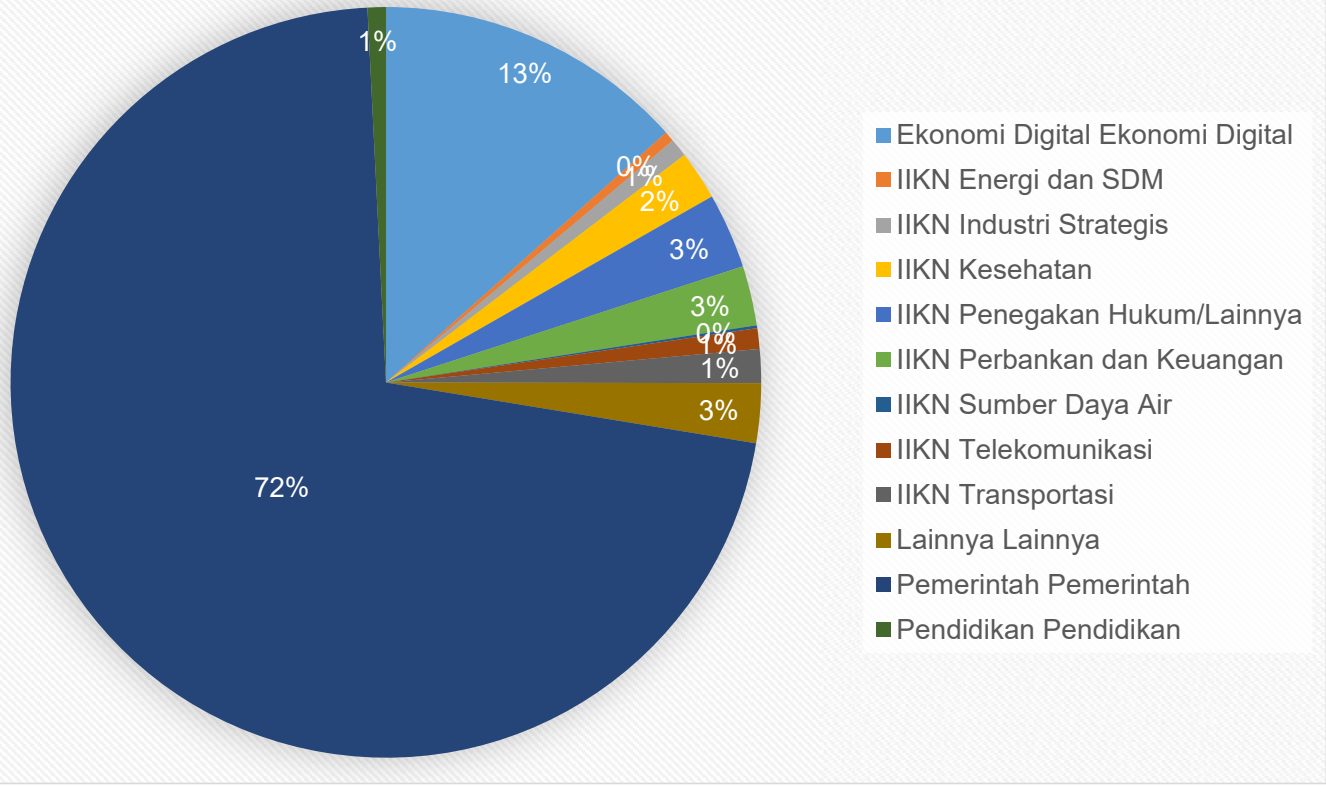
895 LAPORAN

#1	PEMERINTAH
#2	EKONOMI DIGITAL
#3	IIKN

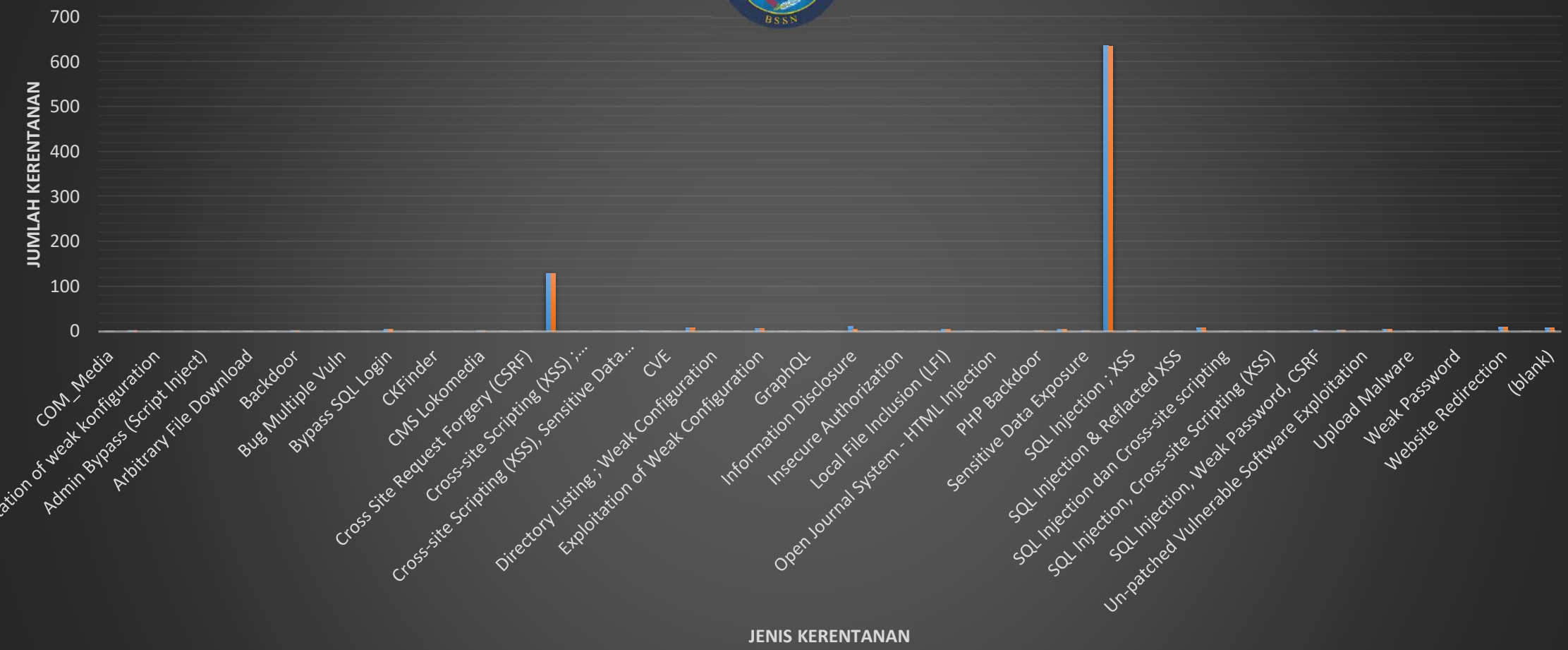
17 LAPORAN

13 BESTATUS PELAJAR

LAPORAN VVDP 1 JANUARI – 29 APRIL 2019



REKAPITULASI KERENTANAN SEKTOR IIKN , EKODIG DAN PEMERINTAH



PROFESIONAL INTEGRITAS ADAPTABILITAS TEKNOLOGI TEPERCAYA

LANDASAN PENERAPAN KEAMANAN SPBE

Perpres Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik (SPBE)

✓ **Pasal 2**

1) SPBE dilaksanakan dengan prinsip:
   a. efektivitas;
   b. keterpaduan;
   c. kesinambungan;
   d. efisiensi;
   e. akuntabilitas;
   f. interoperabilitas;dan
   g. Keamanan

8) Keamanan sebagaimana dimaksud pada ayat (1)huruf g **merupakan kerahasiaan, keutuhan,ketersediaan, keaslian, dan kenirsangkalan (nonrepudiation)** sumber daya yang mendukung SPBE.

✓ **Pasal 40**

1) Keamanan SPBE mencakup penjaminan **kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (nonrepudiation)** sumber daya terkait data dan **informasi, Infrastruktur SPBE, dan Aplikasi SPBE**.

✓ **Pasal 41**

1) Setiap Instansi **Pusat dan Pemerintah Daerah** harus menerapkan Keamanan SPBE.
2) Dalam menerapkan Keamanan SPBE dan menyelesaikan permasalahan Keamanan SPBE,pimpinan Instansi Pusat dan kepala daerah dapat melakukan konsultasi dan / atau koordinasi dengan kepala lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.
3) Penerapan Keamanan SPBE harus memenuhi standar teknis dan prosedur Keamanan SPBE

Apa itu Web Application Security?

Tidak dalam Ruang Lingkup Network Security

- ✓ Mengamankan “costum code / kode sumber” yang membuat Aplikasi web berjalan
- ✓ Mengamankan library dan depedensi
- ✓ Mengamankan Backend System
- ✓ Mengamankan Web dan *application server*

Pada Umumnya Network Security Tidak berfokus pada HTTP Traffic

- ✓ Firewalls, SSL, Intrusion Detection Systems, Operating System Hardening, Database Hardening

? Definisi

- ✓ Sekumpulan proses, protokol, dan perangkat yang bekerjasama untuk memastikan keamanan Aplikasi website dari gangguan ancaman, kegagalan, dan kebocoran data.

YOUR CODE IS PART OF YOUR SECURITY PERIMETER

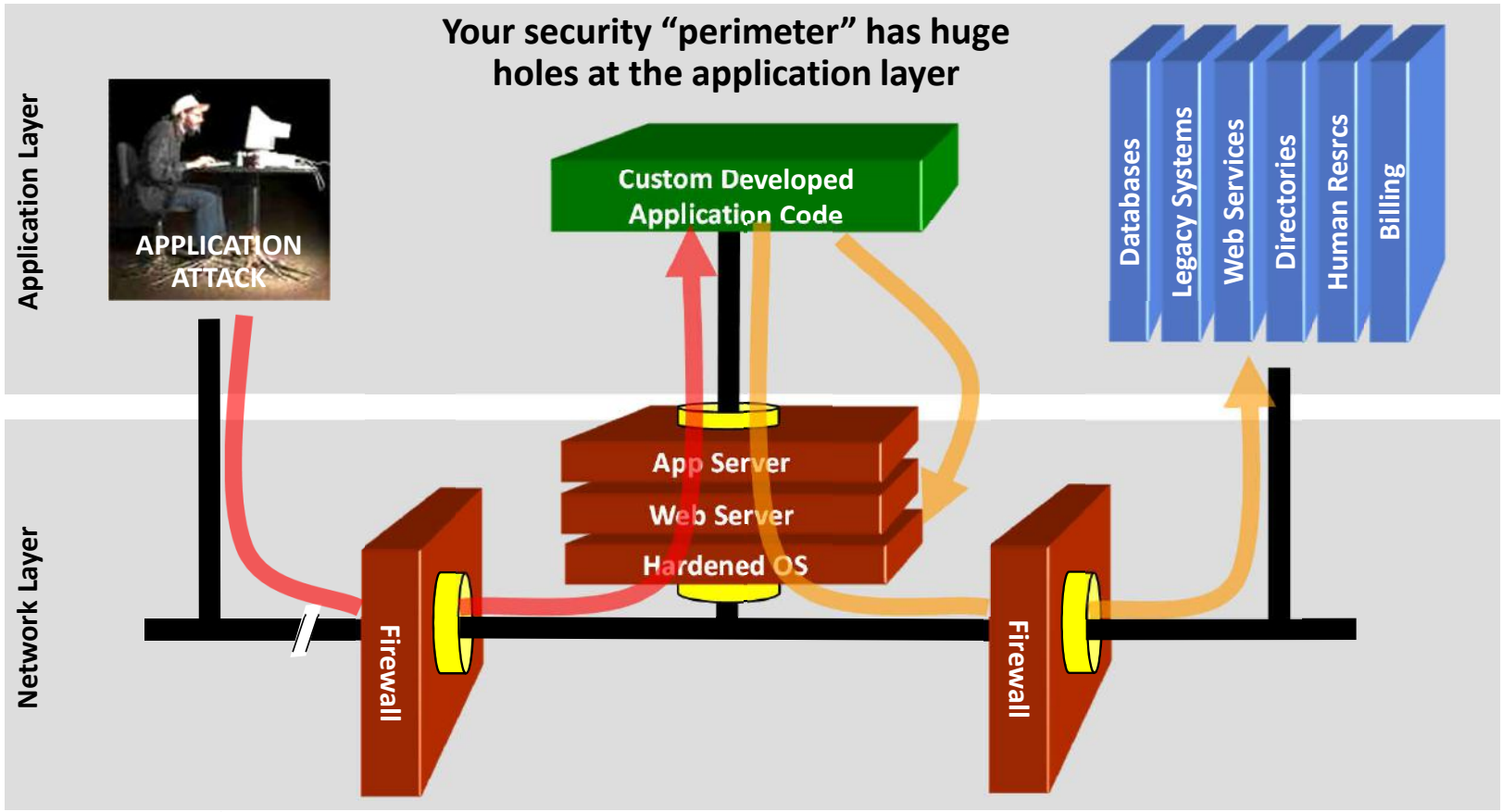


Image source: OWASP's Ten Most Critical Web Application Security Vulnerabilities

You can't use network layer protection (firewall, SSL, IDS, hardening) to stop or detect application layer attacks

.
.
.
.
.
.
.

WEB APPLICATION FIREWALL (WAF) (dapat membantu)

Dampak yang ditimbulkan oleh serangan hacking pada suatu organisasi:

1. Kerugian finansial
2. Pencurian data –data sensitive / *data breach*
3. Berpengaruh buruk pada reputasi dan persepsi organisasi
4. Mengurangi kepercayaan *customer* / *stakeholder*

Langkah yang dapat dilakukan untuk memastikan keamanan Aplikasi web

1. Melakukan Risk AssesSment
2. Meningkatkan security awarness
3. Menyusun dan Mengimplementasikan langkah untuk menanggulangi input data (berbahaya) yang dimasukan oleh pengguna
4. Menerapkan mekanisme perlindungan yang sesuai untuk Data sensitive
5. Mengimplementasikan DevSecOps
6. Melakukan Vulnerability Assesment dan Pentest secara berkala
7. Memanfaatkan perangkat keamanan pendukung seperti WAF, dan lain -lain
8. **Continous Monitoring**

CONTINOUS MONITORING (SOC)

Real-time Monitoring

- Foundation for any security operation
- Visibility across environment & stack
- Real-time correlation to detect known threats

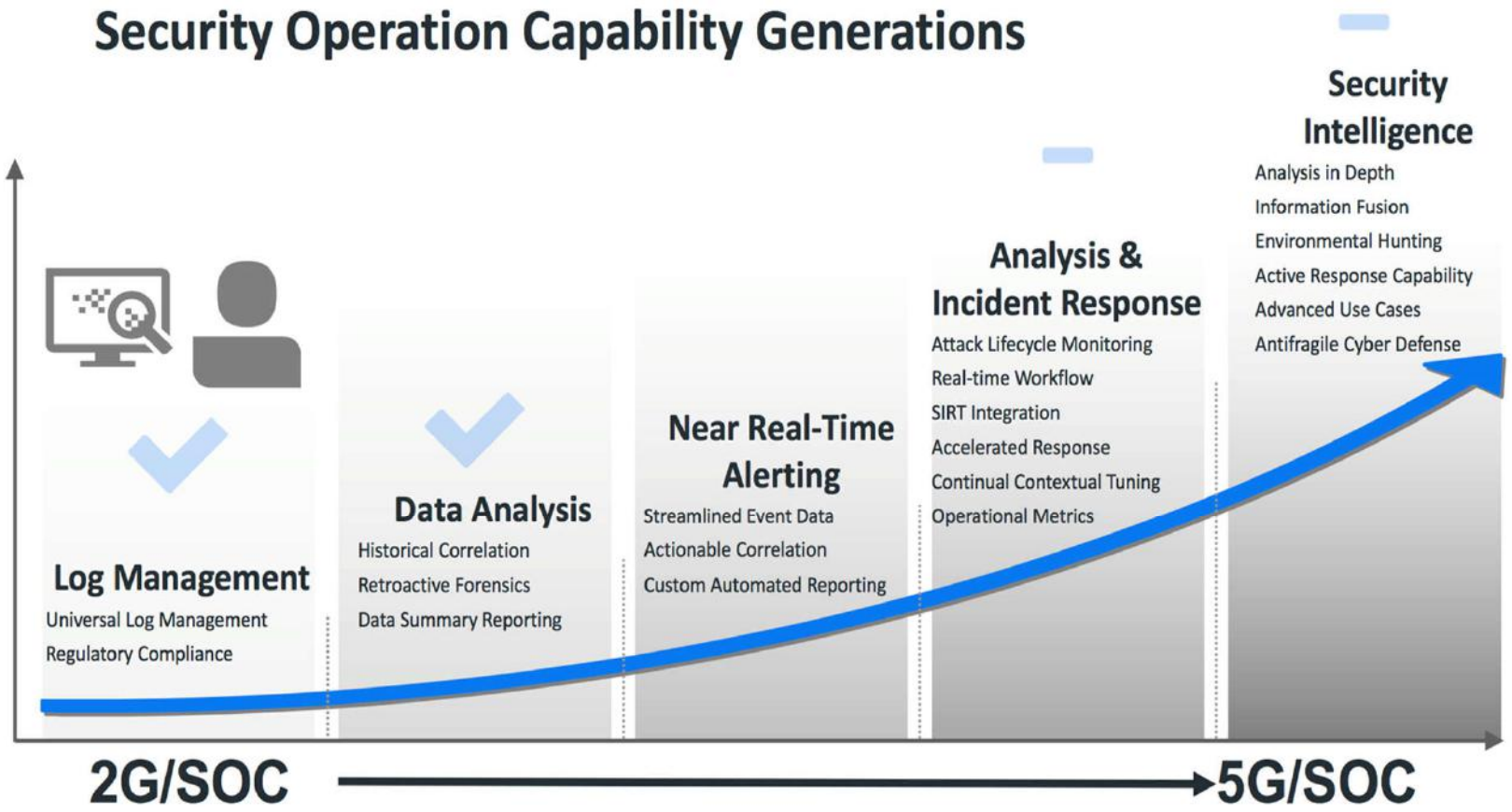
Investigation

- Investigation via workbench and interactive dashboards that allow search, data exploration and entity profiling
- Understand abnormal activity and assess blast radius of attack

Hunt

- Hunting via behavioral analysis, machine learning and graph visualization to traverse relationships and derive new insights
- Ability to discover the unknown threats through pattern discovery and anomaly detection

CONTINOUS MONITORING (SOC)



REKOMENDASI PENERAPAN KEAMANAN SPBE

- ✓ **Komitmen Top Mangement / Pimpinan Organisasi** terkait keamanan informasi, sistem informasi.
- ✓ **Menerapkan Pola Kerja / Budaya Kerja** yang mengedepankan keamanan khususnya keamanan Informasi baik mulai dari proses pembuatan, transmisi, penyimpanan informasi (berlaku juga untuk proses pembangunan Aplikasi).
- ✓ **Membuat Tata Kelola** pengelolaan informasi dan sistem informasi yang mengedepankan keamanan, dan **menjalankannya.**
- ✓ Membangun **Security Awarness SDM**.
- ✓ **Menyusun dan menerapkan SOP** yang jelas dalam pengelolaan sistem informasi.
- ✓ **Melakukan Audit / Assessement** Teknologi Informasi dan Komunikasi, secara berkala.
- ✓ **Menerapkan kontrol perlindungan** yang sesuai pada seluruh sistem khususnya sistem yang mengelola dan atau menyimpan data sensitive.

REKOMENDASI TEKNIS

- Asumsikan seluruh input dari user *malicious*
- Lakukan Validasi terhadap data apapun – inspect what is expected, and reject anything unexpected.
- Hanya menerima dan memproses “Known Good” characters.
- Pastikan input di validasi di sisi server.
- Mengimplementasikan prinsip Least Privilege
- Lakukan validasi akses kontrol untuk memeriksa apakah pengguna diizinkan untuk melakukan suatu aksi / request
- Terapkan seluruh kebutuhan akses kontrol dan web application security policy.
- Pastikan kegagalan pada Aplikasi memerapkan prosedur yang aman (Error handling)
- Gunakan halaman error yang bersifat umum untuk seluruh exception jika terjadi kegagalan, hindari menampilan data sensitive pada pesan error, seperti error SQL dll.
- Pastikan bahwa seluruh perangkat lunak up to date termasuk didalamnya depedensi seperti library, plugin, framework dll
- Batasi Akses terhadap halaman interface / dashboard administrator dengan menggunakan kontrol akses tertentu seperti pembatasan IP dll.
- Non aktifkan / Ganti default password
- Non aktifkan segala sesuatu yang tidak dibutuhkan oleh layanan (seperti: ports, accounts, services, pages, privileges, frameworks, add-ons).

“Kechilafan Satu Orang Sahaja Tjukup Sudah Menjebabkan Keruntuhan Negara”

Mayjen TNI Dr. Roebiono Kertopati
(1914 - 1984)
Bapak Persandian Republik Indonesia

BADAN SIBER DAN SANDI NEGARA