CESS (Journal of Computer Engineering System and Science) **p-ISSN :2502-7131**
Vol. 5 No. 2 Juli 2020 **e-ISSN :2502-714x**

PENGUKURAN TINGKAT KESADARAN KEAMANAN INFORMASI BERDASARKAN *BEHAVIOR DAN OFFENCE SCALE*

Senie Destya

Fakultas Ilmu Komputer, Universitas AMIKOM Yogyakarta
Jl. Ring Roud Utara, Condong Catur, Depok, Sleman, Yogyakarta
seniedestya@amikom.ac.id

Abstrak—**Keamanan komputer menjadi topik yang sangat penting di tengah pertumbuhan sistem informasi saat ini, *cyber attact* perlu diantisipasi perusahaan melalui keamanan hardware dan peningkatan pengetahuan pengguna sistem dalam lingkup perusahaan. Urgensi peningkatan pemahaman *user,* memerlukan *assesment* awal terkait tingkat *awarness* keamanan komputer informasi pengguna. Hal ini yang mendasari penelitian ini untuk mengukur tingkat kesadaran keamanan informasi di kalangan mahasiswa. Hasil dari penelitian ini diharapkan dapat membantu proses pengambilan keputusan pengembangan sistem kedepan dan melakukan peningkatan kapasitas pengetahuan user terhadap keamanan informasi. Metode yang digunakan dalam penelitian ini adalah kuantitatif melalui kuisioner yang terdiri dari RBS (*Risky Behavior Scale), CBS (Conservative Behavior Scale), dan EOS (Exposure to Offence Scale)* dengan skala Tabulasi, Hasil penelitian ini menunjukkan bahwa RBS dan CBS menunjukkan nilai yang tinggi, sedangkan *EOS* memperoleh nilai yang rendah. Peneliti selanjutnya dapat mengukur lebih lanjut ke tingkat struktural dosen dan karyawan AMIKOM dengan menggunakan variable yang berbeda untuk mendapatkan hasil yang lebih signifikan.**

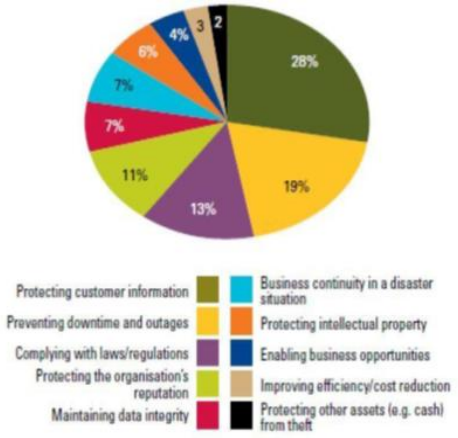
Kata Kunci **: keamanan informasi, *RBS, CBS, EOS***

Abstract— ***Computer security is a very important topic in the midst of the growth of information systems at this time, cyber attact needs to be anticipated by companies through hardware security and increased knowledge of system users within the company. The urgency of increasing user understanding, requires initial assessment related to the level of awareness of the user's computer information security. This is what underlies this research to measure the level of information security awareness among students. The results of this study are expected to help the decision making process of developing the system in the future and to increase the capacity of the user's knowledge of information security. The method used in this study is quantitative through a questionnaire consisting of RBS (Risky Behavior Scale), CBS (Conservative Behavior Scale), and EOS (Exposure to Offence Scale) with a tabulation scale. The results of this study indicate that the RBS and CBS show significant values high, while EOS gets a low value. The researcher can then measure further to the structural level of AMIKOM's lecturers and employees by using different variables to get more significant results.***

Keywords— **information security, RBS, CBS, EOS**

I. PENDAHULUAN

Keamanan informasi pada sebuah organisasi menjadi kajian yang sedang banyak dibahas di era industry 4.0 ini. Salah satu organisasi yang terdampak adalah organisasi pendidikan, khususnya di tingkat perguruan tinggi. Hal ini diperkuat dengan maraknya program pembelajaran online School From Home (SFH) di masa pandemi. Kesadaran civitas akademik tentang keamanan data masih minim. Selain itu keamanan system informasi di kampus juga belum terorganisir dengan baik. Kelemahan dalam proses monitoring dan pemulihan ketika terjadi bencana adalah isu yang paling krusial saat ini. Isu ini diperkuat dengan data dari laporan Info Security Europe tentang 10 faktor pemicu pelanggaran keamanan informasi 2010 terhadap 539 perusahaan. Kesepuluh faktor tersebut diidentifikasikan pada Gambar 1.



Gbr. 1 Diagram komposisi faktor keamanan informasi

Dari gambar 1 dapat dilihat bahwa faktor kepatuhan hukum, penjagaan data pengguna, dan proses integrase data menjadi tiga prioritas utama dalam factor keamanan informasi. Adapun factor lain tidak memiliki prosentase sebesar tiga factor tersebut.

Cybercrime yang terjadi saat ini memiliki tiga model yang sering terjadi, pertama adalah penyerangan terhadap lini jaringan. Kedua adalah serangan terhadap hardware dan software. Model yang terakhir adalah penyerangan terhadap user. Dari ketiga model tersebut, serangan ketiga adalah model yang paling mudah dilakukan oleh hacker, hal ini dikarenakan kurangnya pengetahuan end user terhadap keamanan data. Kelalaian dan kurangnya ketelitian user dalam memberikan informasi menjadi celah utama terjadinya *cybercrime* pada data sebuah organisasi.

Beberapa kelemahan user yang disebutkan di atas membuat hacker menjadi lebih memilih model ini untuk digunakan dalam proses pencurian data. Hal ini dilakukan karena serangan langsung ke lini jaringan atau hardware jauh lebih susah dibandingkan dengan serangan kepada user. Hal ini kemudian menginspirasi peneliti untuk mengukur tingkat kesadaran keamanan pada civitas akademik kampus guna menghindari kerugian cybercrime pada perusahaan.

II. LANDASAN TEORI

A. Konsep Keamanan Informasi

Chan dan Mubarak (2011) menyebutkan beberapa konsep keamanan informasi sebagai berikut:

1) *Phishing:* Cara hacker yang secara umum dilakukan adalah dengan mencuri identitas pengguna dengan meniru email atau website perusahaan. Modus ini sangat mudah dilakukan, dan sering terjadi akibat kurang telitinya karyawan dalam mengakses informasi. Untuk itu, pentingnya sosialisasi bagi karyawan perusahaan untuk memahami konsep dan bahaya dari konsep pencurian data ini.
2) *Spam*: Model pengiriman email yang tidak diinginkan kepada user merupakan metode umum kedua yang sering digunakan oleh Hacker. Email spam merupakan media distribusi virus dan trojan untuk mengakses system komputer dan mencuri data pengguna. Selain itu, spam sering kali berisi link kepada website phishing yang telah dibahas sebelumnya. Kesadaran individu dalam menyikapi konsep spam adalah cara preventif paling baik untuk menghindari jenis serangan ini.
3) *Social Engineering:* Konsep penyerangan ke tiga adalah dengan memanipulasi psikologis pengguna. Konsep non-teknis ini mendorong user untuk memberikan informasi penting kepada hacker. Dengan cara ini penyerang dapat memperoleh data rahasia untuk masuk ke system perusahaan. Pencegahan ini dapat diatasi dengan perusahaan dengan membuat aturan terkait keamanan dan privasi.

B. Kesadaran Keamanan Informasi

Pengetahuan di sekolah adalah elemen utama dalam mengedukasi user tentang kesadaran keamanan. Hal itu dikarenakan bidang ilmu kesadaran keamanan sangat berhubungan erat dengan factor manusia dalam keamanan asset informasi. Pejabat di Innovation Center merupakan penanggungjawab utama dalam proses pengadaan bimbingan teknis terkait kesadaran keamanan kepada karyawan, selain itu divisi ini juga memiliki kewajiban dalam mempersiapkan penerapan elemen keamanan di dalam system informasi perusahaan.

Selain control keamanan teknis, control procedural dan administrasi di tingkat manajemen juga menjadi cara utama dalam menghindari serangan kepada user (Papagiannakis, Pijl, & Visser, 2011). Peranan karyawan, manajer, dan personal IT dalam menggunakan system perusahaan adalah kunci sukses dalam mengamankan data penting perusahaan.

C. Pengukuran Kesadaran Keamanan Informasi

Krugger & Kearney pada tahun 2006 memperkenalkan purwarupa pengukuran Security awareness yang dilakukan pada perusahaan tambang. Metode yang digunakan untuk proses pengukuran menggunakan tiga komponen utama, yaitu: Behaviour, cognition, dan affect. Ketiga komponen ini diadopsi dari ilmu psikologi tentang bagaimana kecenderungan seseorang dalam melakukan suatu pekerjaan yang menguntungkan atau tidak. Ketiga komponen tersebut kemudian dijadikan landasan untuk mengembangkan tiga dimensi ekuivalen sebagai berikut: Sikap, Pengetahuan, dan perilaku. Pengukuran ketiga dimensi ini dilakukan dengan mengajukan kuesioner yang mencakup lima bidang. Bidang pertama adalah Ketaatan karyawan pada regulasi perusahaan, kedua adalah kesadaran dalam menjaga kerahasiaan password. Bidang ketiga adalah bijaksana dalam menggunakan email perusahaan, dan bidang ke empat adalah kewaspadaan terhadap penggunaan perangkat seluler. Adapun bidang terakhir adalah pelaporan insiden keamanan informasi.

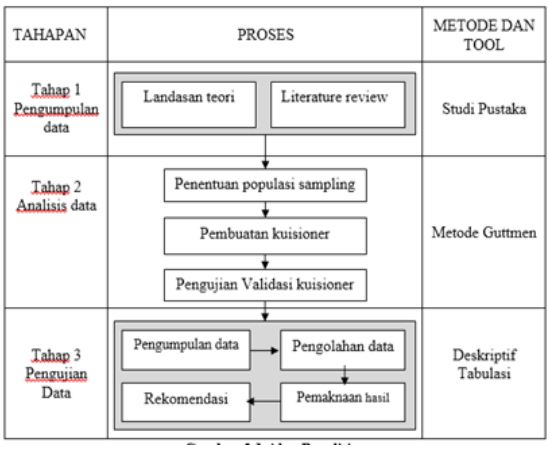
Penelitian yang dilakukan oleh Kruger kemudian dikembangkan oleh Chan & Mubarak di tahun 2011. Penelitian yang berjudul "Information Security Awareness Levels of TAFE South Australia Employees" berfokus pada pengukuran pengetahuan dan behaviour pengguna terhadap poin-poin keamanan informasi. Area yang digunakan mengadopsi dari penelitian Kruger, dengan memodifikasi beberapa model pertanyaan. Adapun cara yang digunakan adalah dengan menganalisis hasil jawaban responden dari kuesioner yang diberikan.

III. METODOLOGI PENELITIAN

Tujuan penelitian ini adalah melakukan pengukuran tingkat kesadaran keamanan informasi untuk digunakan di lingkungan Universitas Amikom Yogyakarta. Metode yang digunakan yaitu deskriptif kuantitatif. Untuk mengetahui tingkat kesadaran keamanan informasi, maka diperlukan penentuan populasi sampling dengan cara membuat klaster profil pengguna sistem informasi di lingkungan Universitas Amikom Yogyakarta khususnya pada mahasiswa S1 Teknik Komputer.

Jumlah mahasiswa S1 Tekkom (Teknik Komputer) yang diambil sebagai sample adalah 30 orang. Pengambilan data dipilih berdasarkan konsentrasi perkuliahan yaitu cyber security dan mata kuliah keamanan dasar. Penelitian dimulai dengan proses pengumpulan data yang diambil dari populasi dengan teknik purposive sampling. Data yang didapatkan dari sample kemudian dianalisis secara deskriptif kuantitatif, dengan metode analisis tabulasi silang (*crosstabs*).

Proses alur penelitian menjelaskan alur proses pada penelitian ini, yang dilakukan dalam tiga tahap dalam proses pengerjaannya. Untuk lebih jelasnya dapat dilihat pada gambar 2.



Gbr. 2 Alur penelitian

Pada gambar 2 menjelaskan proses alur penelitian, tahap 1 pengumpulan data yang proses pengerjaannya mengumpulkan landasan teori dan literature review yang menggunakan metode studi pustaka yaitu RBS (*Risky Behavior Scale), CBS (Conservative Behavior Scale), dan EOS (Exposure to Offence Scale)*. Pada tahap 2 melakukan analisis data dengan melakukan proses pengolahan data secara bertahap, mulai dari menentukan populasi sampling, lanjut proses pembuatan kuisioner menggunakan metode model Guttmen. Kuisioner yang sudah dibuat kemudian diuji validasi. Tahap 3 pengujian data, pada tahap pengujian melakukan proses pengumpulan data, pengolahan data, pemaknaan hasil dan rekomendasi yang menggunakan model deskriprif dan tabulasi.

Pada proses pengumpulan data, peneliti menggunakan purposive sampling untuk perhitungan datanya. Penggunaan purposive sampling berdasarkan pertimbangan mendalam oleh peneliti, bahwa sampel benar-benar telah mewakili karakter populasi (Yunus, 2016). Populasi dalam penelitian ini adalah seluruh civitas akademi Universitas AMIKOM yang berinteraksi langsung dengan sistem informasi. Sampel yang diambil adalah mahasiswa di prodi Teknik Komputer yang berjumlah 30 orang. Teknik pengumpulan data dilakukan dalam bentuk pengisian kuesioner. Pertanyaan tertulis yang diberikan kepada stakeholder berisi pengetahuan tentang tingkat kesadaran keamanan pada sistem informasi. Pengumpulan data dilakukan dengan menggunakan alat ukur berupa lembaran kuesioner berskala Guttman, data yang diperoleh berupa data interval atau rasio dikotomi (dua alternatif) yaitu “Ya” dan “Tidak” sehingga dengan demikian memiliki jawaban yang tegas atas permasalahan yang sedang diteliti.

Variabel penelitian yang digunakan dalam penelitian ini yaitu (1) sikap, (2) pengetahuan, (3) Perilaku. Parameter yang digunakan untuk analisis yaitu jabatan, usia, jenis kelamin, dan bidang keilmuan. Usia digunakan untuk menganalisis tingkat pemahaman mahasiswa terhadap pengetahuan dan upaya tentang kedasaran keamanan informasi. Jurusan/prodi digunakan sebagai indikator tingkat pengetahuan dan upaya tentang kedasaran keamanan informasi. Hasil penilaian digunakan untuk mengetahui tingkat pemahaman pengetahuan dan upaya tentang kedasaran keamanan informasi.

Pada peneltian ini, untuk mengukur keberhasilan penelitian menggunakan instrumen kuesioner atau angket untuk memperoleh hasil informasi yang relevan dan untuk memperoleh tingkat keandalan (*reliability*) dan keabsahan (*validity)* setinggi mungkin. Peneliti menggunakan kuesioner dengan skala Guttman. Peneliti menggunakan skala guttman dilakukan bila ingin mendapatkan jawaban yang tegas (konsisten) terhadap suatu permasalahan yang ditanyakan.

Skala Guttman disebut juga skala *scalogram* yang sangat baik untuk menyakinkan hasil penelitian mengenai kesatuan dimensi dan sikap atau sifat yang teliti. Adapun skoring perhitungan responden dalam skala Guttman adalah sebagai berikut :

Tabel I
Skor perhitungan

Alternatif Jawaban	Skor Alternatif Jawaban	
	Positif	Negatif
Ya	1	0
Tidak	0	1

Jawaban dari responden dapat dibuat skor “satu” untuk angka tertinggi dan “nol” untuk angka terendah, peneliti menetapkan kategori untuk setiap pernyataan positif, yaitu Ya= 1 dan Tidak = 0, sedangkan kategori untuk pernyataan negatif, yaitu Ya= 0 dan Tidak =1.

IV. HASIL DAN PEMBAHASAN

Setelah didapatkan data hasil dari kuesioner, peneliti melakukan tabulasi pada tabel guttman dengan menyusun item menurut ukuran skor jawaban "Ya" tertinggi sampai dengan yang paling rendah. Dari data yang diperoleh hasil angket dipindahkan ke tabel distribusi frekuensi :

Tabel II
Model RBS (*Risky Behavior Scale*)

Item pertanyaan	Jawaban Ya	Jawaban Tidak
P1	30	0
P2	30	0
P3	24	6
P4	20	10
P5	26	4
P6	12	18
Total	142	38

Tabel III
Model CBS (*Conservative Behavior Scale*)

Item pertanyaan	Jawaban Ya	Jawaban Tidak
P1	29	1
P2	23	7
P3	12	18
P4	24	6
P5	22	8
Total	110	40

Tabel IV
Model EOS (*Exposure Offense Scale*)

Item pertanyaan	Jawaban Ya	Jawaban Tidak
P1	7	23
P2	3	27
P3	5	25
P4	8	22
Total	23	97

Setelah mendapatkan hasil data dari kuesioner, peneliti melakukan tabulasi pada tabel Guttman dengan mengubah ke tabel distribusi frekuensi seperti tabel diatas. Karena pada penelitian ini menggunakan skala guttman untuk hasil uji kuesionernya maka untuk memperoleh tingkat validitas kuesioner, maka peneliti menggunakan koefisien Reprodusibilitas dan koefisien Skalabilitas. Adapun rumus yang digunakan adalah :

Koefisien Reprodusibilitas (*Kr*)

$$Kr = 1 - \frac{e}{n}$$

Keterangan :
Kr = koefisien Reprodusibilitas
e = jumlah kesalahan
n = jumlah pertanyaan dikali jumlah responden

Koefisien Skalabilitas

$$Ks = 1 - \frac{e}{c\,(n - Tn)}$$

Keterangan :
Ks = koefisien Skalabilitas
e = jumlah kesalahan
k = jumlah kesalahan yang diharapkan = c(n-Tn) dimana c adalah kemungkinan mendapatkan jawaban yang benar. Karena jawaban adalah "Ya" dan "Tidak"
maka c = 0,5
n = jumlah pertanyaan
x = jumlah responden
Tn = jumlah pilihan jawaban
(Usman Rianse dan Abdi,2008:157)

A. Kuesioner Model RBS (Risky Behavior Scale)

Dari hasil kuesioner menggunakan model RBS, ada 6 pertanyaan yang harus dijawab oleh responden, dengan jumlah responden 30 orang. Total pilihan jawaban yang tersedia untuk responden adalah 6 dikalikan 30 = 180. Error yang terjadi adalah 38 seperti terlihat pada tabel II. Untuk mengukur derajat ketepatan alat ukur hasil dari data kuesioner menggunakan koefisien Reprodusibilitas dengan Rumus :

$$Kr = 1 - \frac{e}{n}$$
$$= 1 - \frac{38}{180}$$
$$= 1 - 0{,}21$$
$$= 0{,}79$$

Skala nilai *Kr* > 0,71 dianggap baik, karena nilai dari hasil perhitungan 0,79 maka koefisien Reprodusibilitas untuk hasil uji dianggap hampir memenuhi.
Koefisien Skalabilitas (*Ks*)

$$Ks = 1 - \frac{e}{c\,(n - Tn)}$$
$$= 1 - \frac{38}{0{,}5(180-142)}$$
$$= 1 - \frac{38}{0{,}5(38)}$$
$$= 1 - \frac{38}{19}$$
$$= 1 - 0{,}5$$
$$= 0{,}5$$

Dalam penghitungan *Ks* > 41 dianggap cukup, karena hasil nilai dari perhitungan 0,5 sehingga disimpulkan bahwa skala bernilai cukup baik. Hasil dari menggunakan model pertanyaan RBS (*Risky Behavior Scale*), hampir semua responden menggunakan sistem informasi dalam kesehariaannya dan tahu akan resiko penggunaan sistem informasi tersebut.

B. Kuesioner Model CBS (Conservative Behavior Scale)

Dari hasil kuesioner menggunakan model CBS, ada 5 pertanyaan yang harus dijawab oleh responden,

dengan jumlah responden 30 orang. Total pilihan jawaban yang tersedia untuk responden adalah 5 dikalikan 30 = 150. Eror yang terjadi adalah 40 seperti terlihat pada tabel 3.6. Untuk mengukur derajat ketepatan alat ukur hasil dari data kuesioner menggunakan koefisien Reprodusibilitas dengan Rumus :

$$Kr = 1 - \frac{e}{n}$$
$$= 1 - \frac{40}{150}$$
$$= 1 - 0{,}26$$
$$= 0{,}74$$

Skala nilai *Kr* > 0,71 dianggap baik, karena nilai dari hasil perhitungan 0,74 maka koefisien Reprodusibilitas untuk hasil uji dianggap hampir memenuhi.

Koefisien Skalabilitas (*Ks*)

$$Ks = 1 - \frac{e}{c\,(n - Tn)}$$
$$= 1 - \frac{40}{0{,}5(150-110)}$$
$$= 1 - \frac{40}{0{,}5(40)}$$
$$= 1 - \frac{40}{20}$$
$$= 1 - 0{,}5$$
$$= 0{,}5$$

Dalam penghitungan *Ks* > 41 dianggap cukup, karena hasil nilai dari perhitungan 0,5 sehingga disimpulkan bahwa skala bernilai cukup baik. Hasil dari menggunakan model pertanyaan Model CBS (*Conservative Behavior Scale*) responden cukup berhati-hati saat menggunakan teknologi atau sistem informasi dalam kehidupan sehari – hari.

C. Kuesioner Model EOS (Exposure Offense Scale)

Dari hasil kuesioner menggunakan model CBS, ada 4 pertanyaan yang harus dijawab oleh responden, dengan jumlah responden 30 orang. Total pilihan jawaban yang tersedia untuk responden adalah 4 dikalikan 30 = 120. Eror yang terjadi adalah 23 seperti terlihat pada tabel 3.7. Untuk mengukur derajat ketepatan alat ukur hasil dari data kuesioner menggunakan koefisien Reprodusibilitas dengan Rumus :

$$Kr = 1 - \frac{e}{n}$$
$$= 1 - \frac{23}{120}$$
$$= 1 - 0{,}19$$
$$= 0{,}81$$

Skala nilai *Kr* > 0,71 dianggap sangatbaik, karena nilai dari hasil perhitungan 0,81 maka koefisien Reprodusibilitas untuk hasil uji dianggap hampir memenuhi.

Koefisien Skalabilitas (*Ks*)

$$Ks = 1 - \frac{e}{c\,(n - Tn)}$$
$$= 1 - \frac{23}{0{,}5(120-97)}$$
$$= 1 - \frac{23}{0{,}5(23)}$$
$$= 1 - \frac{23}{11{,}5}$$
$$= 1 - 2$$
$$= 1$$

Dalam penghitungan *Ks* > 0,91 dianggap sangat baik, karena hasil nilai dari perhitungan 1 sehingga disimpulkan bahwa skala bernilai sangat baik untuk digunakan dalam survei. Hasil dari menggunakan model pertanyaan Model EOS (*Exposure Offense Scale*) responden tahu dampak terkena insiden keamanan cyber karena perilaku sendiri.

V. PENUTUP

Hasil dari penelitian ini menunjukkan bahwa mahasiswa prodi tekkom memiliki tingkat kesadaran keamanan informasi yang baik dan mengetahui dampak yang terjadi apabila menggunakan teknologi informasi atau sistem informasi.

Saran untuk peneliti selanjutnya adalah responden tidak hanya di kalangan mahasiswa saja tetapi juga dikalangan dosen dan karyawan di lingkungan Universitas AMIKOM Yogyakarta, untuk mengetahui seberapa besar tingkat kesadaran keamanan informasinya.

REFERENSI

[1] Amin Mukhlis (2014). Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (MCDA). Jurnal Penelitian dan Pengembangan Komunikasi dan Informatika Vol. 5 No. 1

[2] Chan, H., & Mubarak, S. (2011). Information Security Awareness Level of TAFE South Australia Employees.

[3] Global, S. (2008). Security Awareness: measuring Attitudes, Knowledge and Behavior. SAI Global

[4] Krugger, H. A., & Kearney, W. D. (2006). A Prototype for assessing information security awareness. Computer & Security, 289 – 296.

[5] Papagiannakis, K., Pijl, G. v., & Visser, A. d. (2011). An Overview of the current level of Securty Awareness in Greek Companies. Erasmus University of Rottersam.

[6] Schlienger, T., & Teufel, S. (2003). Information Securty Culture – From Analysis to Change. South African Computer Journal, 638-646.

[7] Steve Hawkins David C. Yen David C. Chou, (2000),"Awareness and challenges of Internet security", Information.

[8] Jumiati, Santi Indarjani, Dwi Destrya Sofiana.2011. Pembinaan Kesadaran Keamanan Informasi di Lingkungan Sekolah Tinggi Sandi Negara Berdasarkan Standar National Institute of Sandardand Technology (NIST SP 800-100). Institut Teknologi Bandung