UAS

KEAMANAN INFORMASI

Disusun oleh:

RICKY PRASOJO UTOMO H

1310651081

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2015

Informasi
Tata Kelola Keamanan dan
Manajemen Risiko

Analisis Risiko

Semua profesional keamanan informasi menilai risiko: kita melakukannya begitu sering sehingga menjadi sifat kedua. Analisis Risiko akurat adalah keterampilan penting untuk keamanan informasi
profesional. Kita harus menahan diri untuk standar yang lebih tinggi ketika menilai risiko. kami
keputusan risiko akan menentukan yang pengamanan kita menyebarkan untuk melindungi aset dan
jumlah uang dan sumber daya yang kami habiskan melakukannya. Keputusan yang buruk akan menghasilkan
di buang uang atau, bahkan lebih buruk, data dikompromikan.

Assets

Aset adalah sumber daya berharga Anda mencoba untuk melindungi. Aset dapat data, sistem,
orang, bangunan, properti, dan sebagainya. Nilai atau kekritisan aset akan dic-tate apa pengamanan Anda menyebarkan.

Ancaman dan Kerentanan

Ancaman adalah segala sesuatu yang berpotensi dapat menyebabkan kerusakan pada aset. ancaman termasuk
gempa bumi, listrik padam, atau cacing berbasis jaringan.
Kerentanan adalah sebuah kelemahan yang memungkinkan ancaman untuk menyebabkan kerusakan. contoh
kerentanan (pencocokan ancaman kami sebelumnya) yang bangunan yang tidak dibangun untuk dengan-
berdiri gempa bumi, pusat data tanpa daya cadangan yang tepat, atau Microsoft Win
dows sistem XP yang belum ditambal dalam beberapa tahun.

Annualized Loss Expectancy

Perhitungan memungkinkan Anda untuk menentukan
biaya tahunan kerugian akibat risiko. Setelah dihitung, ALE memungkinkan Anda untuk membuat
keputusan untuk mengurangi risiko.
Bagian ini akan menggunakan contoh resiko karena laptop tidak terenkripsi hilang atau dicuri.
Asumsikan perusahaan Anda memiliki 1.000 laptop yang berisi pribadi diidentifikasi masi
mation (PII). Anda adalah petugas keamanan, dan Anda khawatir tentang risiko
paparan dari PII karena hilang atau dicuri laptop. Anda ingin membeli dan menyebarkan
solusi enkripsi laptop.

Paparan Factor

Faktor Exposure (EF) adalah persentase nilai aset yang hilang akibat insiden.
Dalam kasus laptop dicuri dengan tidak terenkripsi PII, Faktor Exposure adalah 100%: yang
laptop dan semua data hilang.

Tingkat tahunan Terjadinya

Tingkat Tahunan Kejadian (ARO) adalah jumlah kerugian Anda menderita per tahun.
Melihat melalui peristiwa masa lalu, Anda menemukan bahwa Anda telah menderita 11 hilang atau dicuri
laptop per tahun rata-rata. ARO Anda adalah 11.

Biaya Total Kepemilikan

Total Cost of Ownership (TCO) adalah total biaya dari perlindungan yang meringankan. TCO
menggabungkan biaya dimuka (sering biaya modal satu kali) ditambah biaya tahunan main-
tenance, termasuk staf jam, biaya pemeliharaan penjual, langganan software, dll
Biaya-biaya yang berkelanjutan biasanya dianggap biaya operasional.

Anggaran dan metrik

Ketika dikombinasikan dengan Analisis Risiko, Total Cost of Ownership dan Imbal
Perhitungan investasi faktor dalam penganggaran yang tepat. Beberapa organisasi memiliki
posisi iri dana keamanan informasi yang cukup, namun mereka sering
dikompromikan. Mengapa? Jawabannya adalah biasanya karena mereka dikurangi risiko yang salah.
Mereka menghabiskan uang mana mungkin belum perlu dan mengabaikan risiko yang lebih besar.
Terlepas dari ukuran staf atau anggaran, semua organisasi dapat mengambil jumlah terbatas masi

proyek keamanan mation. Jika mereka memilih tidak bijaksana, keamanan informasi dapat menderita.
Metrik dapat sangat membantu proses penganggaran keamanan informasi. mereka membantu
menggambarkan risiko yang berpotensi mahal dan menunjukkan efektivitas (dan potensi
penghematan biaya) kontrol yang ada. Mereka juga dapat membantu juara penyebab masi
keamanan mation.

Pilihan Risiko
Setelah kami telah dinilai risiko, kita harus memutuskan apa yang harus dilakukan. Pilihan termasuk menerima
risiko, mengurangi atau menghilangkan risiko, mentransfer risiko, dan menghindari risiko.

Menerima Risiko
Beberapa risksmay diterima: dalam beberapa kasus, lebih murah untuk meninggalkan aset yang tidak dilindungi
karena risiko tertentu, daripada membuat usaha (dan menghabiskan uang) yang diperlukan untuk
melindunginya. Hal ini tidak bisa menjadi keputusan yang bodoh: risiko harus dipertimbangkan, dan semua
Pilihan harus dipertimbangkan sebelum menerima risiko.

Kriteria Penerimaan Risiko
Risiko rendah kemungkinan / rendah-konsekuensi adalah kandidat untuk penerimaan risiko. tinggi dan
risiko ekstrim tidak dapat diterima. Ada kasus, seperti data yang dilindungi oleh undang-undang atau
peraturan atau risiko bagi kehidupan manusia atau keamanan, di mana menerima risiko bukanlah pilihan.

Mengurangi Risiko
Mengurangi riskmeans menurunkan risiko ke tingkat yang dapat diterima. Enkripsi laptop
contoh yang diberikan dalam Bagian "Annualized Loss Expectancy" adalah contoh dari mitigasi
risiko. Risiko hilang PII karena laptop dicuri wasmitigated dengan mengenkripsi data pada
laptop. Risikonya belum dihilangkan seluruhnya: enkripsi lemah atau terkena
sandi bisa mengekspos PII, tapi risiko telah berkurang ke tingkat yang dapat diterima.
Dalam beberapa kasus, adalah mungkin untuk menghapus risiko secara keseluruhan: ini disebut menghilangkan
risiko.

Mentransfer Risiko

Mentransfer risiko adalah "model asuransi." Kebanyakan orang tidak menganggap resiko kebakaran
ke rumah mereka: mereka membayar perusahaan asuransi untuk menganggap bahwa risiko bagi mereka. itu
perusahaan asuransi yang ahli dalam Analisis Risiko: membeli risiko bisnis mereka.

Penghindaran Risiko

Sebuah Analisis Risiko menyeluruh harus diselesaikan sebelum mengambil sebuah proyek baru.
Jika Analisis Risiko menemukan risiko tinggi atau ekstrim yang tidak dapat dengan mudah diatasi,
menghindari risiko (dan proyek) dapat menjadi pilihan terbaik.

Analisis Risiko Kualitatif dan Kuantitatif

Analisis Risiko Kuantitatif dan Kualitatif dua metode untuk menganalisis risiko.
Analisis Risiko Kuantitatif menggunakan metrik keras, seperti dolar. Risiko kualitatif Analisis menggunakan nilai perkiraan sederhana. Kuantitatif lebih objektif; kualitatif
lebih subjektif. Analisis Risiko Hybrid menggabungkan dua: menggunakan kuantitatif
analisis untuk risiko yang mungkin mudah dinyatakan dalam nomor keras, seperti uang,
dan kualitatif untuk sisanya.
Menghitung Harapan Loss Annualized (ALE) adalah contoh kuantitatif
tive Analisis Risiko. The Matrix Analisis Risiko (ditunjukkan sebelumnya pada Tabel 3.1) isan
contoh Analisis Risiko Kualitatif.

Proses Manajemen Risiko

US National Institute of Standar dan Techn
Publikasi Khusus 800-30, Manajemen Risiko Panduan fo
Sistem (lihat http://csrc.nist.gov/publications/nistpubs/8
panduan menjelaskan proses Analisis Risiko 9-langkah:
1. Sistem Karakterisasi
2. Ancaman Identifikasi
3. Kerentanan Identifikasi
Analisis 4. Kontrol
Penentuan 5. Kemungkinan
6. Analisa Dampak

KEAMANAN INFORMASI TATA

Keamanan Informasi Pemerintahan adalah keamanan informasi di tingkat organisasi:
manajemen senior, kebijakan, proses, dan staf. Itu juga merupakan primer organisasi
Sebagian Besar disediakan oleh kepemimpinan senior, yang diperlukan untuk informasi yang berhasil
program keamanan.

Kebijakan Keamanan dan Dokumen Terkait

Dokumen seperti kebijakan dan prosedur adalah bagian yang diperlukan dari setiap sukses
program keamanan informasi. Dokumen-dokumen ini harus didasarkan pada realitas: mereka
tidak dokumen idealis yang duduk di rak-rak mengumpulkan debu. Mereka harus mencerminkan
dunia nyata dan memberikan bimbingan pada benar (dan kadang-kadang diperlukan) cara
melakukan hal-hal.

Policy

Kebijakan yang arahan manajemen tingkat tinggi. Kebijakan adalah wajib: jika Anda tidak
setuju dengan kebijakan pelecehan seksual perusahaan Anda, misalnya, Anda tidak memiliki
pilihan untuk tidak mengikutinya.

Komponen Kebijakan Program

Semua kebijakan harus mengandung komponen-komponen dasar:

- Tujuan
- Lingkup
- Tanggung Jawab
- Kepatuhan

Tujuan menggambarkan kebutuhan untuk kebijakan, biasanya untuk melindungi kerahasiaan,
integritas, dan ketersediaan data yang dilindungi.

Lingkup menjelaskan apa sistem, orang, fasilitas, dan organisasi yang tertutup
oleh kebijakan. Setiap entitas terkait yang tidak dalam lingkup harus didokumentasikan untuk
menghindari kebingungan.

Tanggung jawab termasuk tanggung jawab staf keamanan informasi, kebijakan dan tim manajemen, serta tanggung jawab semua anggota organisasi.

Kepatuhan menggambarkan dua isu terkait: bagaimana menilai efektivitas
kebijakan (seberapa baik mereka bekerja) dan apa yang terjadi ketika kebijakan dilanggar(sanksi). Semua kebijakan harus memiliki "gigi": kebijakan yang melarang mengakses eksplisit
konten melalui Internet tidak berguna jika tidak ada konsekuensi untuk melakukannya.

Prosedur

Prosedur adalah langkah-demi-langkah panduan untuk menyelesaikan tugas. Mereka tingkat rendah dan
spesifik. Seperti kebijakan, prosedur wajib.

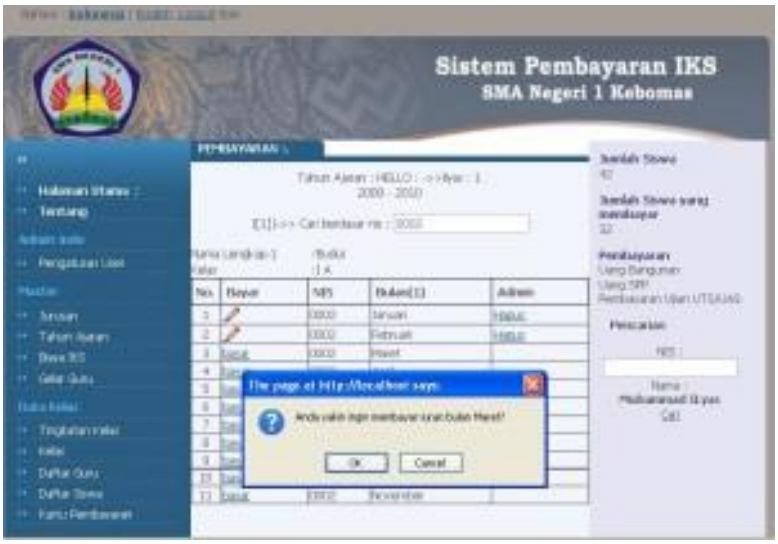
Berikut ini adalah contoh prosedur sederhana untuk membuat user baru:

1. Menerima formulir permintaan baru-pengguna dan memverifikasi kelengkapan.
2. Pastikan bahwa manajer pengguna telah menandatangani formulir.
3. Pastikan bahwa pengguna telah membaca dan setuju dengan kebijakan keamanan akun pengguna.
4. Klasifikasikan peran pengguna dengan mengikuti prosedur peran-tugas NX-103.
5. Pastikan bahwa pengguna telah memilih "kata rahasia," seperti gadis ibu mereka nama, dan masukkan ke dalam profil akun help desk.
6. Buat account dan menetapkan peran yang tepat.
7. Menetapkan kata rahasia sebagai password awal dan mengatur "Angkatan pengguna untuk mengubah
password pada login berikutnya untuk 'Benar'. "
8. E-surat dokumen Akun Baru ke pengguna dan manajer mereka.

Langkah-langkah dari prosedur ini adalah wajib. Administrator keamanan tidak memiliki
pilihan untuk melewatkan langkah 1, misalnya, membuat akun tanpa formulir.

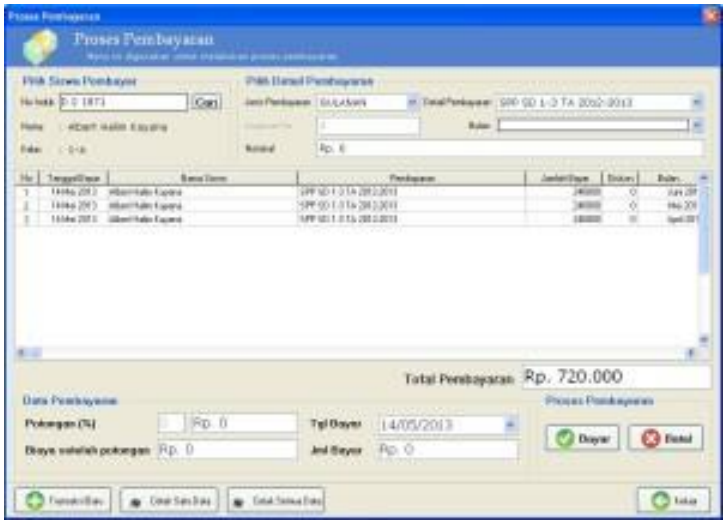
2.

Dengan kecanggihan teknologi masa kini, kita semua bisa memanfaatkan kecanggihan teknologi tersebut untuk sebuah aplikasi pembayaran SPP sekolah. Aplikasi ini memang berguna untuk mengatur laporan data keuangan sekolah dengan mudah. Pemanfaatan software ini membantu setiap pihak sekolah dalam melakukan pengelolaan dan pengaturan keuangan sekolah dengan otomatis melalui teknik komputerisasi. Melalui aplikasi software inilah kita juga bisa mengkalkulasikan keuangan secara otomatis tanpa lagi memerlukan perhitungan secara manual.



Jika kita memanfaatkan aplikasi PHP untuk pembayaran SPP ini, maka Anda bisa lebih efisien dalam menghemat waktu saat akan merekap keuangan atau tutup buku. Aplikasi PHP juga bisa dimanfaatkan untuk berbagai tingkatan sekolah, mulai dari SD, SMP, SMA, MTS, dan lain sebagainya. Seperti pada umumnya, pihak sekolah melakukan perekapan atau pengelolaan keuangan secara manual, melalui buku keuangan biasa. Namun, hal ini tentunya membuat waktu Anda lebih banyak dan lebih sibuk.

Dengan penggunaan program aplikasi php ini, Anda tak perlu lagi melakukan pembukuan manual. Cukup dengan menginput data-data keuangan secara online apabila memungkinkan. Sehingga Anda hanya perlu mengolah data keuangan dengan baik dan melakukan kalkulasi di internet. Ada beberapa *Gambar Contoh Aplikasi Php Sistem Informasi Pembayaran SPP* yang bisa kita jumpai saat ini. Ada banyak kelebihan menggunakan aplikasi pembayaran SPP sekolah, antara lain:



1. Anda tak perlu melakukan rekapan data keuangan secara manual dari awal. Karena menggunakan software atau aplikasi pembayaran SPP bisa membuat sebuah rekapan laporan yang otomatis. Sehingga Anda cukup melakukan input data saja. Dengan begitulah, Anda juga bisa lebih cepat mengerjakan laporan keuangan dan lebih menghemat waktu.
2. Pekerjaan dengan menggunakan aplikasi ini juga lebih praktis dan simpel. Dengan desain yang simpel, membuat Anda juga lebih mudah mengerjakannya.

3. Menggunakan software aplikasi pembayaran SPP tentu memberikan kemudahan pekerjaan untuk Anda.