Nama : Rifko Satrio Rahmadani
Email : ikosatriorahmadani@gmail.com
Pekerjaan : Mahasiswa
Nama Instansi/Sekolah : Politeknik Negeri Bandung

Challenge Pengolaan Risiko dalam Keamanan Informasi

I. Pendahuluan

Pada tugas ini, saya berperan sebagai Kepala Keamanan Informasi di sebuah perusahaan e-commerce bernama TokoShop. Sebagai bagian dari pengelolaan keamanan informasi, saya menyusun daftar risiko, lengkap dengan analisa dampak, frekuensi, dan strategi.

Analisis dilakukan menggunakan pendekatan kualitatif, yaitu memberi penilaian sederhana berdasarkan kemungkinan terjadi dan seberapa besar dampaknya bagi organisasi.

II. File & Tools yang digunakan

- Laptop dengan sistem operasi Windows
- Microsoft Excel
- File Daftar Resiko

III. Katergori Resiko

- Keamanan Data
- Keamanan Aplikasi
- Keamanan Jaringan
- Keamanan People
- Keamanan Fisik
- Kriptografi
- Akses Kontrol

IV. Tabel Daftar Risiko

Identifikasi Resiko		Analisa Resiko Qualitatif			Rencana Penanganan		
Kategori	Resiko	Dampak	frequensi	Resiko	Strategi	Tindakan	Metode Kontrol
Keamanan Data	Password admin toko disimpan di catatan HP dan berpotensi dibaca orang	0,20	0,70	0,14	Mengurangi	Gunakan password manager dan aktifkan auto-lock	Kebijakan penggunaan password + MFA
Keamanan Data	Backup data tidak terjadwal dan sering lupa dilakukan	0,40	0,30	0,12	Mengurangi	Buat sistem backup otomatis mingguan	Backup & recovery plan
Keamanan Aplikasi	Form login tidak menggunakan captcha sehingga mudah bruteforce	0,20	0,50	0,10	Mengurangi	Tambahkan CAPTCHA	Rate limiting + captcha
Keamanan Aplikasi	Update aplikasi web jarang dilakukan sehingga ada bug yang tidak diperbaiki	0,40	0,50	0,20	Mengurangi	Jadwalkan update bulanan untuk sistem	Patch management
Keamanan Jaringan	Router WiFi kantor/sekolah masih pakai password default	0,20	0,70	0,14	Mengurangi	Ganti password & aktifkan WPA3	Network Access Control (NAC)
Keamanan People	Karyawan mudah tertipu email palsu (phishing)	0,40	0,70	0,28	Mengurangi	Pelatihan edukasi keamanan tiap 3 bulan	Awareness training & simulasi phishing
Keamanan Fisik	Laptop karyawan sering ditinggal tanpa dikunci	0,20	0,70	0,14	Mengurangi	Aktifkan auto-lock 5 menit	Kebijakan workstation security
Keamanan Fisik	Ruang server tidak terkunci dan bebas dimasuki siapa saja	0,40	0,30	0,12	Menghindari	Pasang kunci & akses kartu	Physical access control
Kriptografi	Website tidak memaksa pengguna menggunakan HTTPS (masih bisa HTTP)	0,20	0,30	0,06	Mengurangi	Redirect otomatis HTTP → HTTPS	SSL/TLS enforcement
Akses Kontrol	Akun mantan karyawan tidak segera dinonaktifkan	0,40	0,50	0,20	Mengurangi	Buat SOP disable akun saat offboarding	IAM (Identity Access Management)

V. Analisa Risiko Berbasis Kualitatif

Dari hasil penilaian, sebagian besar risiko muncul karena kebiasaan user yang kurang aman, konfigurasi sistem yang belum disiplin, dan beberapa kontrol dasar yang belum diterapkan. Risiko yang nilai-nya paling tinggi ada pada phishing, password WiFi default, dan karyawan yang sering tinggalkan laptop tanpa dikunci, karena frekuensi kejadiannya tinggi dan berdampak langsung ke keamanan akun.

Risiko lain seperti form login tanpa CAPTCHA, aplikasi jarang di-update, penggunaan HTTP, serta akun mantan karyawan yang tidak dinonaktifkan juga penting, tapi masih bisa ditekan dengan kontrol sederhana seperti patch rutin, enforcement HTTPS, dan SOP offboarding.

Secara keseluruhan, hampir semua risiko bisa dikurangi dengan perbaikan dasar seperti kebijakan password, training keamanan, auto-lock, update berkala, dan penguatan kontrol akses.

VI. Kesimpulan

Secara keseluruhan, hasil analisis menunjukkan kalau sebagian besar risiko yang muncul di TokoShop sebenarnya hal-hal mendasar yang sering terjadi di lingkungan kerja, seperti password yang kurang aman, backup yang tidak rutin, perangkat yang dibiarkan tanpa pengawasan, dan akun yang tidak segera dinonaktifkan. Walaupun terlihat sepele, dampaknya bisa cukup besar kalau dibiarkan.

Dengan menerapkan kontrol sederhana misalnya update rutin, pelatihan keamanan, penerapan enkripsi, sampai disiplin dalam manajemen akses kebanyakan risiko tersebut bisa ditekan. Intinya, ketika prosedur dasar keamanan dijalankan dengan benar dan konsisten, tingkat risiko TokoShop jadi jauh lebih terkendali dan operasionalnya lebih aman.