Jawaban UAS Sistem Pengamanan Komputer

1. Langkah Mendapatkan Sertifikasi ISO 27001

Proses mendapatkan sertifikasi ISO 27001 dimulai dengan melakukan analisis kesenjangan (*gap analysis*) untuk mengevaluasi apakah sistem manajemen keamanan informasi (ISMS) yang ada sudah memenuhi persyaratan standar internasional. Proses ini melibatkan peninjauan dokumen, wawancara dengan tim terkait, dan identifikasi area yang perlu diperbaiki. Selanjutnya, perusahaan harus membentuk tim ISMS yang bertanggung jawab mengkoordinasikan implementasi kontrol keamanan. Tim ini akan melakukan penilaian risiko untuk mengidentifikasi ancaman, kerentanan, dan dampak potensial terhadap aset informasi, lalu merancang perlindungan yang sesuai. Setelah itu, kontrol keamanan seperti enkripsi data, autentikasi dua faktor, dan manajemen akses harus diimplementasikan sesuai lampiran Annex A ISO 27001. Seluruh kebijakan, prosedur, dan catatan keamanan (seperti log aktivitas atau hasil audit) harus didokumentasikan secara rinci. Perusahaan juga perlu melakukan audit internal untuk memastikan kesesuaian dan memberikan pelatihan kepada karyawan agar memahami peran mereka dalam menjaga keamanan informasi. Tahap akhir adalah mengajukan sertifikasi ke badan akreditasi ISO 27001, yang akan melakukan audit eksternal untuk memvalidasi kepatuhan.

2. Langkah Pertama Respons Insiden Siber

Ketika tim IT Bank Aman menemukan akses mencurigakan ke server utama, langkah pertama yang harus diambil adalah segera mengisolasi server tersebut dari jaringan untuk mencegah penyebaran serangan ke sistem lain. Isolasi ini bisa dilakukan dengan memutus koneksi fisik atau mengonfigurasi firewall agar memblokir lalu lintas ke server. Selama proses ini, penting untuk mendokumentasikan semua bukti digital, termasuk log sistem, screenshot antarmuka, dan informasi metadata, karena data ini akan menjadi kunci dalam investigasi forensik. Tim respons insiden kemudian harus melakukan analisis awal untuk menentukan jenis serangan, vektor masuk, serta dampak yang terjadi. Jika diperlukan, hasil temuan harus dilaporkan ke manajemen dan otoritas terkait, terutama jika insiden berpotensi melibatkan pelanggaran hukum atau kebocoran data sensitif. Tujuan utama langkah pertama ini adalah meminimalkan kerugian dan mempertahankan integritas bukti untuk investigasi lebih lanjut.

3. Strategi Pemulihan Layanan Pasca Kebakaran

Setelah kebakaran mengganggu operasi pusat data, perusahaan teknologi harus mengaktifkan rencana pemulihan bencana (*Disaster Recovery Plan*) yang telah disusun sebelumnya. Langkah pertama adalah memulihkan data dari cadangan (*backup*) yang disimpan di lokasi geografis berbeda, seperti pusat data cadangan atau layanan cloud. Jika cadangan tidak tersedia, perusahaan mungkin perlu memanfaatkan layanan cloud seperti AWS atau Azure sebagai solusi sementara untuk menjalankan aplikasi kritis. Selain itu, komunikasi transparan dengan pelanggan sangat penting untuk menjaga kepercayaan, termasuk memberikan estimasi waktu pemulihan dan langkah-langkah darurat yang sedang diambil. Perusahaan juga harus mengevaluasi infrastruktur fisik untuk mencegah risiko kebakaran di masa depan, seperti memperbarui sistem pemadam api otomatis atau meningkatkan ventilasi server room.

4. Langkah Meningkatkan Keamanan Kata Sandi

Untuk mengatasi penggunaan kata sandi lemah seperti ”123456” atau ”password”, Dimas dapat merekomendasikan penerapan kebijakan kata sandi kompleks yang mewajibkan kombinasi huruf besar, huruf kecil, angka, dan karakter khusus, serta panjang minimum 12 karakter. Selain itu, autentikasi dua faktor (*2FA*) harus diwajibkan untuk semua akun, terutama yang memiliki akses ke data sensitif. Implementasi manajer kata sandi perusahaan seperti Bitwarden atau LastPass juga dapat membantu karyawan menyimpan kata sandi kuat secara aman tanpa harus mengingatnya secara manual. Pelatihan keamanan rutin harus diberikan untuk meningkatkan kesadaran karyawan tentang risiko penggunaan kata sandi lemah dan praktik keamanan dasar, seperti tidak membagikan kredensial atau menggunakan kata sandi yang sama di berbagai platform.

5. Rekomendasi Kebijakan Pengelolaan Akses ISO 27001

Rina harus merekomendasikan penerapan prinsip *least privilege* dan *segregation of duties* untuk memastikan setiap pengguna hanya memiliki akses minimal yang diperlukan untuk menjalankan tugasnya. Perusahaan juga perlu mengimplementasikan Role-Based Access Control (*RBAC*), di mana hak akses ditentukan berdasarkan peran dalam organisasi. Contohnya, staf administrasi hanya bisa mengakses dokumen HR, sementara insinyur hanya bisa mengakses sistem teknis. Tinjauan berkala terhadap hak akses pengguna harus dilakukan untuk memastikan tidak ada akun yang memiliki izin berlebihan karena perubahan jabatan atau pengunduran diri. Seluruh prosedur pemberian, modifikasi, dan pencabutan akses harus didokumentasikan secara rinci untuk memenuhi persyaratan audit ISO 27001.

6. Langkah Menghapus Malware

Ketika komputer Rina terinfeksi malware, langkah pertama adalah memutuskan koneksi internet dan jaringan lokal untuk mencegah penyebaran atau komunikasi dengan server pelaku. Setelah itu, sistem harus dijalankan dalam mode aman (*safe mode*) untuk membatasi aktivitas malware. Pemindaian dengan antivirus terpercaya seperti Malwarebytes atau Kaspersky harus dilakukan untuk mendeteksi dan menghapus komponen berbahaya. Jika malware tidak dapat dihapus, langkah ekstrem seperti menginstal ulang sistem operasi mungkin diperlukan untuk memastikan semua jejak infeksi terhapus. Setelah pembersihan, semua perangkat lunak dan sistem operasi harus diperbarui ke versi terbaru untuk menambal kerentanan. Sebagai langkah pencegahan, Rina disarankan menginstal antivirus real-time, memblokir situs web mencurigakan dengan *content filter*, dan tidak mengklik tautan atau lampiran dari sumber yang tidak dikenal.

7. Strategi Melawan Serangan DDoS

Untuk mengatasi serangan DDoS yang memengaruhi situs e-commerce, perusahaan harus menggunakan layanan mitigasi DDoS seperti Cloudflare atau AWS Shield, yang dapat memfilter lalu lintas ilegal dan mendistribusikan beban serangan ke server yang tersebar secara global. Firewall jaringan harus dikonfigurasi untuk memblokir IP yang mencurigakan dan membatasi jumlah permintaan per detik. Kapasitas bandwidth sementara juga dapat ditingkatkan untuk menyerap lalu lintas berlebihan selama serangan. Selain itu, perusahaan harus bekerja sama dengan penyedia layanan internet (*ISP*) untuk mengidentifikasi sumber serangan dan memblokirnya di tingkat jaringan. Sebagai langkah jangka panjang, sistem harus dirancang dengan arsitektur terdistribusi dan redundansi untuk meningkatkan ketahanan terhadap serangan masa depan.

8. Faktor Memilih Sistem Operasi

Anto harus mempertimbangkan beberapa faktor saat memilih sistem operasi, termasuk tujuan penggunaan. Misalnya, Windows cocok untuk pengguna yang membutuhkan kompatibilitas luas dengan perangkat

lunak dan game, sementara Linux lebih fleksibel untuk pengembangan perangkat lunak dan server. macOS biasanya dipilih oleh pengguna yang fokus pada desain grafis atau ekosistem Apple. Kompatibilitas perangkat keras dan perangkat lunak juga penting; jika Anto menggunakan aplikasi khusus seperti AutoCAD atau MATLAB, Windows mungkin lebih sesuai. Dari segi keamanan, Linux dianggap lebih aman karena sifat open-source yang memungkinkan komunitas memperbaiki celah keamanan secara cepat. Biaya lisensi juga menjadi pertimbangan: Linux gratis, sementara Windows dan macOS memerlukan pembelian lisensi atau perangkat keras tertentu. Terakhir, kemudahan penggunaan dan kurva pembelajaran harus dinilai berdasarkan pengalaman Anto sebelumnya.

9. Respons terhadap Ransomware

Dalam kasus serangan ransomware di Perusahaan ABC, langkah pertama adalah tidak membayar tebusan karena tidak ada jaminan data akan dikembalikan. Selanjutnya, sistem yang terinfeksi harus diisolasi untuk mencegah penyebaran ke perangkat lain. Data harus dipulihkan dari cadangan offline yang tidak terinfeksi, seperti server eksternal atau layanan cloud yang telah diverifikasi kebersihannya. Setelah pemulihan, tim IT harus mengidentifikasi vektor serangan, misalnya melalui email phishing atau eksploitasi kerentanan perangkat lunak. Semua sistem dan aplikasi harus diperbarui untuk menambal celah keamanan, dan antivirus harus ditingkatkan untuk mendeteksi ancaman serupa. Pelatihan keamanan rutin untuk staf juga diperlukan untuk mencegah insiden ulangan, termasuk mengenali email phishing dan praktik keamanan dasar.

10. Meningkatkan Keamanan Jaringan Rumah Sakit

Untuk mengatasi akses tidak sah ke sistem rumah sakit, langkah pertama adalah mengimplementasikan firewall generasi baru (*next-gen firewall*) yang dilengkapi deteksi intrusi (*IDS*) dan pencegahan intrusi (*IPS*). Data pasien harus dienkripsi menggunakan algoritma kuat seperti AES-256 baik saat disimpan (*at rest*) maupun saat dikirim (*in transit*). Sistem operasi dan aplikasi medis harus diperbarui secara berkala untuk menambal kerentanan, termasuk menginstal patch keamanan terbaru. Akses jaringan harus dibatasi dengan VLAN (*Virtual Local Area Network*) untuk memisahkan sistem kritis seperti database pasien dari jaringan umum. Audit log aktivitas sistem harus dilakukan secara rutin untuk mendeteksi anomali, dan kebijakan keamanan harus diperbarui sesuai dengan perkembangan ancaman terkini.