MATERI L1 SOC ANALYST

UNIT KOMPETENSI 6

Menganalisis Dampak Insiden Kemanan Siber

MEDIA PEMBELAJARAN L1 SOC ANALYST

Unit Kompetensi

Menganalisis Dampak Insiden Kemanan Siber

Elemen Kompetensi

1. Melakukan analisis profil insiden keamanan siber
    a. Kerusakan dan/atau kehilangan pada aset dianalisis berdasarkan informasi profil insiden keamanan siber dan aset TI.
    b. Aset TI/sistem terdampak insiden keamanan siber ditentukan berdasarkan hasil analisis.
2. Menilai kerugian finansial yang diakibatkan insiden keamanan siber yang terjadi
    a. Biaya langsung dihitung berdasarkan biaya yang ditimbulkan agar sistem yang terdampak insiden keamanan siber dapat beroperasi kembali.
    b. Biaya tidak langsung dihitung berdasarkan besarnya kerugian nonoperasional yang timbul karena sistem terdampak insiden keamanan siber.
    c. Biaya pemulihan untuk setiap sistem terdampak insiden keamanan siber dihitung berdasarkan jumlah biaya langsung dan biaya tidak langsung.
3. Mengindentifikasi kerugian nonfinansial yang diakibatkan insiden keamanan siber yang terjadi
    a. Dampak kerugian nonfinansial diidentifikasi berdasarkan analisis jangka panjang.
    b. Dampak terhadap industri diidentifikasi berdasarkan laporan terkait.

A. DAMPAK INSIDEN SIBER

Berdasarkan Keputusan Menteri Ketenagakerjaan No 391 Tahun 2020 J.62SOC00.018.1 definisi insiden keamanan siber sebagai berikut.

Informasi profil insiden keamanan siber:

1. Nama
2. Deskripsi Ancaman
3. Threat Agent
4. Kerentanan
5. IoC
6. Aset terdampak

Jenis biaya dampak insiden siber:

1. Biaya langsung
   Biaya yang langsung dapat dihitung sesuai dengan nilai kerusakan akibat insiden keamanan siber, termasuk biaya penggantian kerusakan dan/atau kehilangan aset, biaya perangkat baru yang harus dibeli, biaya konsultan untuk pemulihan, dan biaya langsung lainnya.
2. Biaya tidak langsung
   Biaya akibat rusaknya reputasi, kehilangan kesempatan bisnis, produktifitas karyawan, dan biaya terhadap pelanggaran kode etik, dan biaya tidak langsung lainnya.
3. Biaya pemulihan
   Biaya yang dibutuhkan untuk sistem sampai dalam kondisi sebelum insiden keamanan siber terjadi.

Dampak terhadap industri

meningkatnya risiko investasi dan premi asuransi, tata kelola kebijakan baru serta kebutuhan industri untuk membangun *Computer Security Incident Response Team* (CSIRT), *Information Sharing and Analysis Center* (ISAC), dan *Honeynet*.

Kerugian Finansial

Kategori	Detail Biaya
Biaya Langsung	biaya penggantian kerusakan dan/atau kehilangan aset
	biaya perangkat baru yang harus dibeli
	biaya konsultan untuk pemulihan
Biaya Tidak Langsung	biaya akibat rusaknya reputasi
	kehilangan kesempatan bisnis
	kehilangan data pribadi

Kategori	Detail Biaya
	kehilangan produktivitas karyawan
	biaya terhadap pelanggaran kode etik
Biaya Pemulihan	biaya Langsung + biaya Tidak Langsung

Kerugian Non Finansial :

1. Terhambatnya kegiatan operasional
2. Penurunan Reputasi
3. Pertanggujawaban hukum
4. Perubahan *Policy*

Langkah Mengatasi Dampak Insiden Siber:

1. Manajemen insiden
2. Mengelola risiko
3. Meminimalkan dampak insiden
4. Meningkatkan kesadaran keamanan
5. Memperbarui perangkat lunak
6. Menggunakan teknologi keamanan yang tepat
7. Membuat tim CSIRT (*Computer Security Incident Response Team*)

B. BISNIS VS SECURITY

CISO VS *BOARD*

CISO (*Chief Information Security Officer*) adalah pegawai senior yang bertanggung jawab atas keamanan informasi dalam sebuah organisasi

Board yaitu dewan direksi (*Board of Directors*), sekelompok orang yang bertugas mengawasi strategi dan arah bisnis perusahaan. *Board* terdiri dari eksekutif senior dan pemegang saham utama yang membuat keputusan tingkat tinggi tentang anggaran, investasi, dan kepatuhan terhadap regulasi

1. Love it or hate it — CISO percaya bahwa kehadiran AI memberikan keuntungan bagi attackers dibandingkan *defender*s, bahkan *attacker*s sudah menggunakan AI untuk pertahanan di dunia maya seperti: *malware analysis*, mengotomasi alur kerja dan penilaian risiko. Tapi peningkatan tidak dimulai dengan AI: 93% dari CISO sudah mengimplementasikan proses *automation* secukupnya, dan AI hanya akan meningkatkan persentase tersebut di masa depan.
2. CISO seringkali menggunakan bahasa yang berbeda dengan dewan direksi, sehingga meskipun memiliki prioritas yang semakin mendekati satu sama lain, masih terdapat ketidakselarasan. CISO berpendapat bahwa dewan direksi lebih peduli pada kepatuhan terhadap peraturan dibandingkan praktik terbaik keamanan.
3. CISO kini menjadi *C-suite*. 47% CISO kini melapor langsung kepada CEO mereka. Dewan menjadi pemangku kepentingan keamanan yang lebih aktif.

CISO diminta untuk membenarkan investasi mereka, tapi ini bukanlah hal yang buruk. Hal ini menunjukkan bahwa para pemimpin mereka mendengarkan dan mengalokasikan lebih banyak anggaran untuk tahun depan (meskipun anggaran tersebut masih belum cukup).

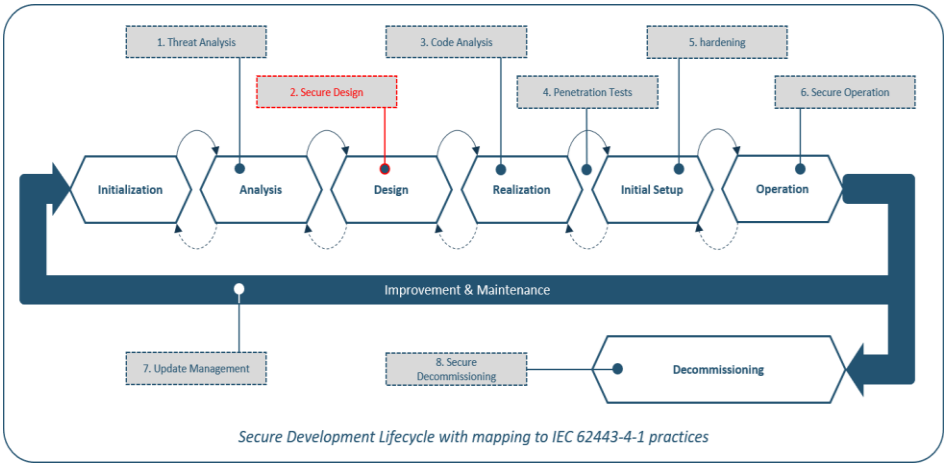
4. Sebagian besar tuntutan *ransomware* berbayar Sembilan puluh persen CISO melaporkan bahwa organisasi mereka mengalami setidaknya satu serangan yang mengganggu tahun lalu. Yang lebih mengejutkan lagi, 83% membayar penyerang setelah serangan *ransomware* – secara langsung, melalui asuransi siber atau dengan negosiator – dan lebih dari setengahnya membayar setidaknya $100.000.

Keselarasan Bisnis dan Investasi Keamanan

Grafik ini membandingkan kinerja CISO dan *Board* pada sejumlah faktor yang mereka yakini penting untuk menentukan efektivitas program siber. Faktor yang digunakan untuk menilai keberhasilan program keamanan meliputi ROI (*Return on Investment*) dari investasi, status audit dan kepatuhan, hasil uji keamanan, risiko paparan, kemajuan dalam mencapai tujuan keamanan, dan waktu yang dibutuhkan untuk mengidentifikasi dan menyelesaikan masalah.

Rekomendasi Keselarasan Bisnis Dan Investasi Keamanan: Definisikan Kebutuhan Sejak Awal

1. Kecenderungan pendefinisian keamanan dilakukan setelah terjadi insiden keamanan.
2. Implikasinya biaya yang ditimbulkan lebih besar.
3. Tim keamanan kerap kali diidentikan sebagai "*Project Stopper*".
4. Fokus pengembangan sistem lebih kepada kesesuaian terhadap proses bisnis.



Secure Development Lifecycle with mapping to IEC 62443-4-1 practices

Gambar diatas menunjukkan *Secure Development Lifecycle* (SDLC) dengan pemetaan ke praktik IEC 62443-4-1. IEC 62443-4-1**,** *framework* yang digunakan untuk memastikan bahwa produk perangkat lunak atau sistem yang dikembangkan aman sejak awal hingga akhir dan memiliki tahapn sebagai berikut:

Tahapan-tahapan *Secure Development Lifecycle* (SDLC):

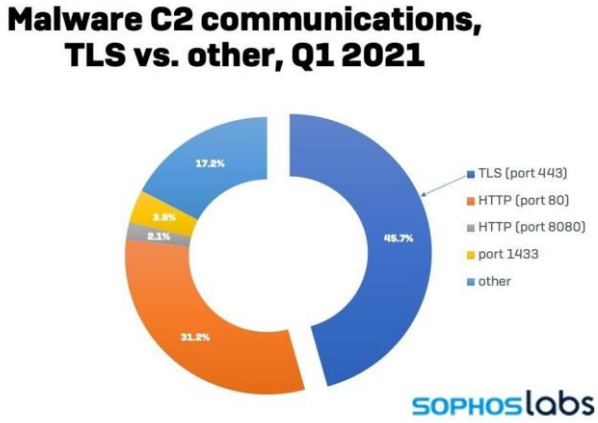
1. *Initialization* (Inisialisasi):
   Tahap awal di mana proyek dimulai dan perencanaan dasar dilakukan.
2. *Analysis* (Analisis)
   Analisis ancaman dilakukan untuk memahami potensi kerentanannya.
3. *Secure Design* (Desain Aman)
   Desain sistem yang aman dibangun dengan memperhatikan faktor-faktor keamanan. Pada gambar, tahap ini disorot dengan warna merah, yang menunjukkan pentingnya desain yang aman untuk mencegah potensi masalah di kemudian hari.
4. *Code Analysis* (Analisis Kode)
   Pemeriksaan dan evaluasi kode sumber untuk memastikan tidak ada kelemahan atau kerentanannya.
5. *Penetration Tests* (Uji Penetrasi)
   Melakukan simulasi serangan untuk mengidentifikasi potensi celah yang dapat dieksploitasi.
6. *Hardening* (Penguatan)

Mengamankan sistem dengan cara menghapus komponen yang tidak perlu dan menambah lapisan perlindungan.

7. *Secure Operation* (Operasi yang Aman)
   Memastikan sistem berjalan dengan aman dan sesuai dengan standar yang telah ditentukan.
8. *Realization* (Realization)
   Implementasi dari desain dan pengujian yang sudah disetujui.
9. *Initial Setup* (Pengaturan Awal)
   Pemasangan dan konfigurasi awal sistem.
10. *Operation* (Operasi)
    Sistem mulai berfungsi dalam kondisi nyata, dan pemeliharaan dilakukan untuk memastikan kinerja yang berkelanjutan.

C. LESSON LEARNED BASED ON INCIDENT HANDLING

Pembelajaran 1: Bangun Visibilitas dan Perlindungan hingga *Level Endpoints*

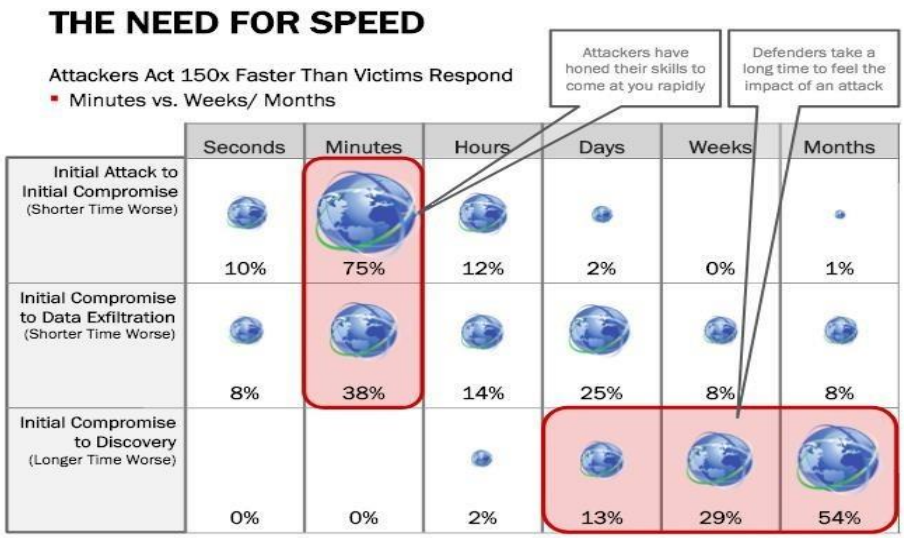


Saat ini hampir Sebagian trafik pada jaringan merupakan trafik terenkripsi. Berdasarkan riset yang dilakukan oleh Cisco, lebih dari 70% infeksi *malware* pada tahun 2020 akan menggunakan enkripsi untuk menyembunyikan proses pengiriman *malware*, aktivitas CnC, atau eksfiltrasi data. 60% organisasi tidak memiliki visibilitas terhadap trafik terenkripsi, sehingga akan mengalami kesulitan dalam melakukan identifikasi ancaman pada trafik yang terenkripsi. Membangun visibilitas dan proteksi pada layer *endpoint* akan membantu dalam hal mendeteksi dan memproteksi sistem.

Pembelajaran 2: Lakukan Pemonitoran Sistem Anda (Tim yang didedikasikan khusus)

Banyak yang beranggapan bahwa dengan menerapkan perimeter keamanan saja semua permasalahan keamanan terselesaikan. Pemonitoran sistem akan membantu kita mengidentifikasi dan mendeteksi secara dini bilamana terjadi

insiden, *fraud*, atau lainnya. Penyerang saat ini selalu mencari upaya untuk melakukan evasi terhadap deteksi dari perimeter keamanan.



Dari gambar diatas menunjukkan perbandingan kecepatan antara serangan siber dan respons korban dalam bentuk persentase waktu yang dibutuhkan dalam detik hingga bulan. Pada tahapan *Initial Attack to Initial Compromise* (Serangan Awal ke Kompromi Awal):

1. 75% serangan berhasil diubah menjadi kompromi dalam menit pertama.
2. Hanya 10% serangan yang memerlukan waktu dalam detik untuk menjadi kompromi awal.
3. Setelah itu, presentase penurunan di jam, hari, minggu, dan bulan secara signifikan lebih rendah.

Pada tahapan *Initial Compromise to Data Exfiltration* (Kompromi Awal ke Ekstraksi Data):

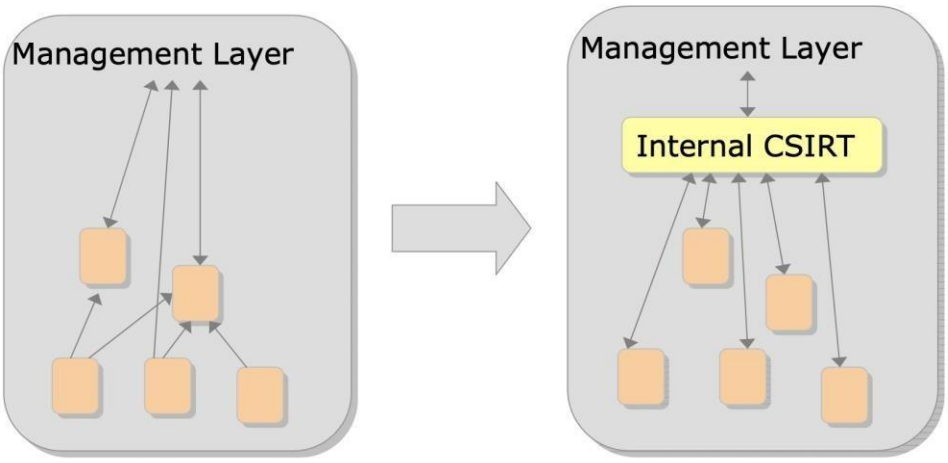
1. 38% dari serangan dapat mengekstrak data dalam menit pertama.
2. Dalam detik dan jam, jumlahnya lebih kecil, tetapi meningkat di hari dan minggu (masing-masing 25% dan 8%).
3. Meskipun serangan terjadi cepat, data baru terungkap setelah jangka waktu yang lebih lama.

Pada tahapan Initial *Compromise to Discovery* (Kompromi Awal ke Penemuan):

1. Proses ini membutuhkan waktu yang lebih lama dan hanya 13% dari serangan yang terdeteksi dalam minggu pertama.
2. 54% baru ditemukan setelah bulan-bulan berlalu.

Pembelajaran 3: Bangun Tim Tanggap Insiden / Poin Kontak Penanganan Insiden

Tim CSIRT melakukan pengelolaan informasi yang berkaitan dengan insiden



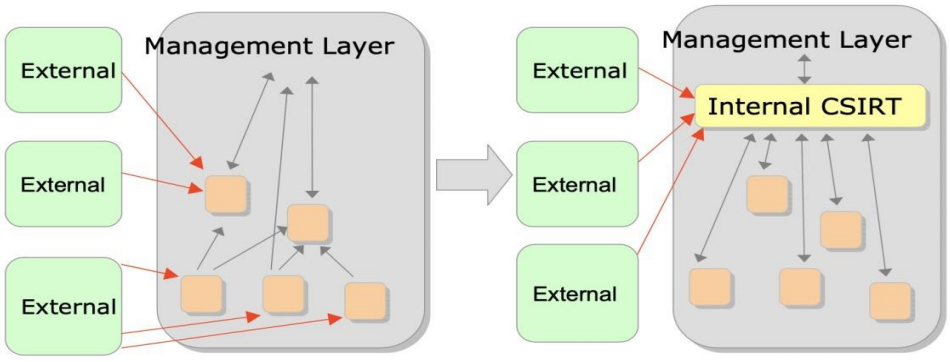
Struktur Sebelum Adanya Internal CSIRT (Kiri):

1. *Management Layer*nya menunjukkan struktur manajerial atau pengelolaan secara umum tanpa pengkhususan khusus.
2. Gambar ini menunjukkan hubungan antar unit manajemen yang saling berhubungan satu sama lain, di mana beberapa unit saling berinteraksi, namun tidak ada struktur khusus untuk menangani insiden atau ancaman siber.

Struktur Setelah Menambahkan Internal CSIRT (Kanan):

1. Pada gambar sebelah kanan, kita melihat adanya **Internal CSIRT** yang terintegrasi langsung dalam lapisan manajemen.
2. Internal CSIRT adalah tim yang bertanggung jawab untuk merespons, mengelola, dan memitigasi insiden keamanan siber di dalam organisasi. Dengan penambahan tim ini, struktur manajemen menjadi lebih terfokus dalam menangani masalah keamanan siber secara lebih efektif.

Tim CSIRT menjadi poin kontak bagi pihak eksternal untuk mempermudah proses tanggap insiden



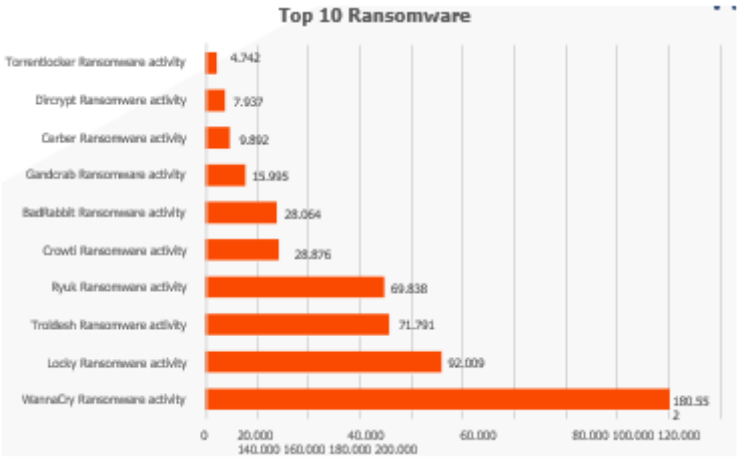
Sebelum Penambahan Internal CSIRT (Kiri):
Struktur manajerial yang ada sebelum adanya Internal CSIRT. Di sini, *external units* (pihak eksternal) berinteraksi langsung dengan lapisan manajerial.

- Pihak eksternal yang mungkin terlibat dalam respons insiden, seperti penyedia layanan pihak ketiga, lembaga keamanan, atau pihak yang memiliki hubungan kerja.
- Terdapat beberapa hubungan antara unit eksternal dan manajerial yang tidak terkoordinasi dengan sistem internal yang fokus pada ancaman siber.

Setelah Penambahan Internal CSIRT (Kanan):

1. Setelah adanya tim Internal CSIRT, struktur organisasi menjadi lebih terkoordinasi. CSIRT bertugas untuk menangani ancaman dan insiden keamanan siber secara internal.
2. Internal CSIRT berfungsi untuk menyatukan dan mengatur komunikasi antara unit internal dan eksternal, yang memungkinkan respons yang lebih cepat dan lebih efektif. Unit eksternal tetap berhubungan dengan Internal CSIRT, namun hubungan ini terkoordinasi dengan lebih baik dan dikelola melalui tim CSIRT yang terpusat.

Pembelajaran 4 : Lakukan backup dan percobaan untuk me-restore dari Backup



Salah satu cara agar terhindar dari dampak kerugian insiden *ransomware* adalah dengan membuat salinan/*backup* dari sistem/data yang dimiliki. Pastikan juga melakukan backup pada media penyimpanan yang terpisah untuk menghindari sinkronisasi antara sistem produksi dan backup jika terkena *ransomware*.

Pembelajaran 5 : Kontrol Pengembangan dan Penggunaan Aplikasi pada Organisasi

1. Tetapkan kebijakan pengembangan aplikasi pada organisasi.
2. Lakukan evaluasi terhadap aplikasi yang dikembangkan dan digunakan untuk mengidentifikasi aplikasi yang tidak lagi digunakan dan berpotensi memiliki celah kerawanan untuk dieksploitasi.

3. Tetapkan *standard* pengelolaan keamanan aplikasi Beberapa kasus insiden peretasan dan kebocoran data yang terjadi karena organisasi tidak mengetahui unit kerja yang melakukan pengembangan aplikasi mandiri.
4. Beberapa kasus insiden peretasan dan kebocoran data yang terjadi karena organisasi tidak mengetahui unit kerja yang melakukan pengembangan aplikasi mandiri.

Pembelajaran 6 : Lakukan Pengujian Keamanan pada Sistem secara Berkala atau Setiap Kali ada Perubahan

Miskonsepsi yang terjadi

- Sebagian besar organisasi berpikir bahwa pengujian keamanan hanya cukup dilakukan sebelum aplikasi digunakan/diluncurkan
- Organisasi tidak melakukan pengujian keamanan terhadap aplikasi ketika ada perubahan yang bersifat major, karena beranggapan baru dilakukan pengujian keamanan dalam beberapa waktu yang lalu.
- Pemilik sistem tidak melakukan perbaikan terhadap temuan kerentanan pada aplikasi setelah dilakukan pengujian.

Lakukan pengujian keamanan oleh pihak internal (yang *independent*) dan eksternal untuk mendapatkan perspektif yang berbeda terkait dengan hasil pengujian keamanan.

Pentingnya pengujian keamanan

- Mengidentifikasi resiko keamanan dari aplikasi sejak dini untuk dilakukan perbaikan
- Bagian dari bentuk kepatuhan terhadap regulasi
- Menjaga reputasi organisasi

Pembelajaran 7 : Lakukan Prosedur *Patch* terhadap Sistem secara Berkala

Penyebab utama dari beberapa kasus peretasan yang terjadi adalah

- Aplikasi tidak lagi dikelola
- Tidak digunakan namun tidak dilakukan proses penon-aktifan aplikasi, sehingga apabila terdapat kerentanan pada aplikasi tidak dilakukan *patching*/perbaikan
- Tidak dikenali pengelolanya karena sudah mutasi/*resign*

Manajemen kerentanan terhadap sistem yang dikelola menjadi salah satu hal yang penting untuk mengidentifikasi secara dini asset yang rentan dan perlu dilakukan patch keamanan.

Pembelajaran 8: Terapkan 1 akun 1 orang untuk mempermudah penelusuran apabila terjadi *fraud*/insiden

1. Proses penelusuran insiden atau mengidentifikasi terjadinya *fraud* menjadi lebih sulit pada saat penggunaan akun bersama untuk kegiatan operasional.
2. Lakukan proses penghapusan/penonaktifan akun yang sudah tidak lagi digunakan untuk menghindari penyalahgunaan akun.
3. Lakukan *review* secara berkala terhadap akun yang ada untuk mengidentifikasi adanya *fraud* atau *compromise account*.

Pembelajaran 9: Pertimbangkan untuk melakukan perpanjangan lisensi sehingga tetap mendapatkan dukungan

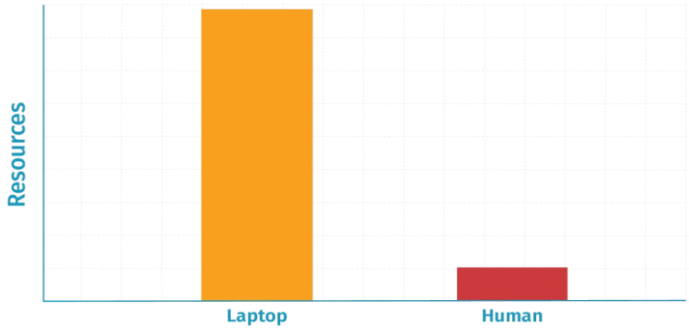
1. Untuk tetap mendapatkan *updates support* keamanan serta agar perangkat yang digunakan berjalan optimal.
2. Pertimbangkan untuk melakukan perpanjangan lisensi/*support* apabila tidak memiliki sumber daya yang memadai apabila terjadi permasalahan yang memerlukan dukungan *principal*.

Pembelajaran 10: Lakukan Evaluasi Penggunaan Sistem yang telah dinyatakan EOS

1. • Setiap sistem *memiliki end of life atau end of support* sehingga produsen/komunitas tidak lagi mendukung update/patch bila ada permasalahan keamanan. Umumnya ini menjadi celah yang dimanfaatkan peretas akibat
2. • Lakukan *planning* untuk migrasi ke versi terbaru.

Pembelajaran 11: Melatih Personel

Sebagian besar organisasi hanya fokus pada pembelian/investasi pada teknologi tapi tidak pada pengembangan kapasitas SDM.



Pembelajaran 12: Bangun budaya keaman, bukan sekadar kesadaran

1. Program kesadaran keamanan adalah program formal dengan tujuan melatih pengguna tentang potensi ancaman terhadap informasi

organisasi dan cara menghindari situasi yang dapat membahayakan data organisasi.

2. Salah satu hal yang menjadi catatan dalam Sebagian program kesadaraan adalah karena tidak mendefinisikan *focus* dan metrik ukuran keberhasilan/capaian.

Pembelajaran 13: Aktifkan fitur log pada sistem anda

1. *Logging* pada sistem merupakan salah satu hal yang paling penting selain untuk memudahkan proses *trouble shooting*, meningkatkan kinerja operasional, logging juga sangat penting dalam proses tanggap insiden, mendeteksi adanya aktifitas anomaly dalam sistem.
2. Beberapa hal penting yang perlu didefinisikan dalam logging
    - Masa retensi terhadap log
    - Besaran ukuran log
    - Review terhadap log
    - Backup log secara berkala
    - Informasi apa saja yang harus dilogging

Pembelajaran 14: *Fine Tuning* Sistem

Dalam beberapa kasus insiden yang terjadi, salah satu penyebab dari terjadinya peretasan/sulitnya untuk melakukan penelusuran insiden yang terjadi adalah karena tidak dilakukannya penyesuaian (*fine tuning*) dari sistem/perimeter keamanan. Sehingga menimbulkan tingginya tingkat *FALSE POSITIVE*.

Beberapa alasan mengapa fine tuning terhadap sistem umumnya tidak dilakukan

- Mendapatkan *complain* dari pemilik sistem jika perimeter keamanan melakukan *blocking* terhadap layanan
- Aplikasi harus segera diluncurkan dan digunakan sehingga *fine tuning* beresiko terhadap operasional layanan, sehingga *fine tuning* dilakukan saat operasional berlangsung.
- Tidak ada kebijakan maupun mekanisme atau prosedur yang ditetapkan untuk melakukan fine tuning terhadap sistem keamanan.

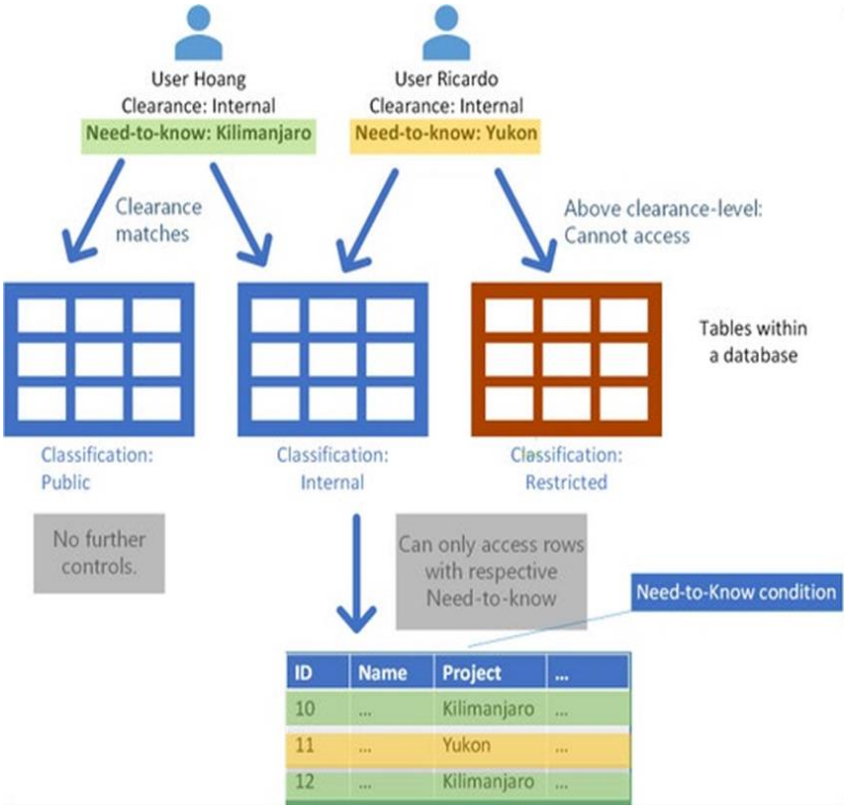
Materi Pembelajaran 15: Pahami Basis

Pengguna hanya memiliki akses terhadap informasi yang relevan dengan pekerjaannya, terlepas dari *security clearance* atau persetujuan lainnya. Kecenderungan dari beberapa insiden yang terjadi tidak ada pembatasan hak akses berdasarkan *role base* akses kontrol terhadap akun pengguna.

Need to know basis memberikan keuntungan dalam beberapa hal

1. Membatasi dampak dari serangan *social engineering*
2. Membuat data tetap aman akibat dari *remote access attack*

3. Mereduksi dampak pada data akibat serangan/insiden yang terjadi



Akses Pengguna Berdasarkan Kebutuhan Pekerjaan

Dalam diagram, sistem memastikan bahwa pengguna hanya bisa melihat data yang berhubungan dengan tugas mereka. Misalnya, Hoang bekerja pada proyek "Kilimanjaro", jadi ia hanya bisa melihat data dengan ID 10 dan 12 yang terkait proyek itu. Sementara itu, Ricardo bekerja pada proyek "Yukon", sehingga ia hanya bisa melihat data dengan ID 11. Dengan cara ini, mereka tidak bisa mengakses informasi yang tidak ada hubungannya dengan pekerjaan mereka.

Ketiadaan Pembatasan Berbasis *Role-Based Access Control*

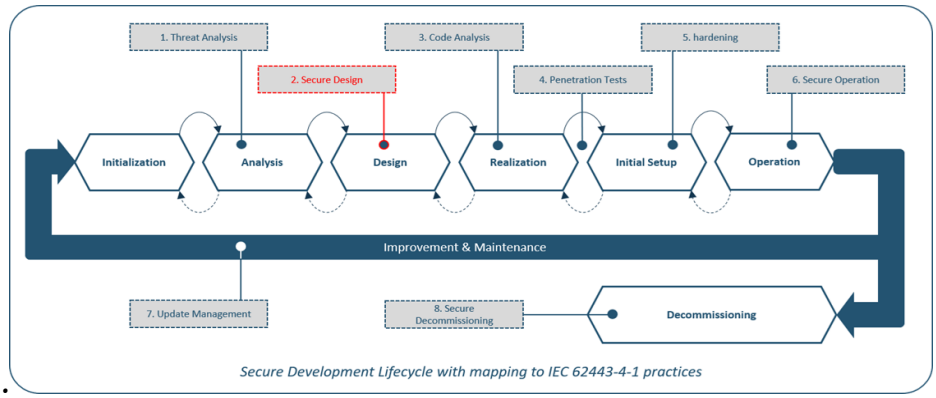
Diagram menunjukkan bahwa Hoang dan Ricardo sama-sama memiliki tingkat *clearance* "Internal". Namun, mereka tidak bisa mengakses tabel dengan klasifikasi "*Restricted*" karena tingkat clearance mereka tidak cukup tinggi. Di tabel dengan klasifikasi "Internal", mereka juga hanya bisa melihat data yang sesuai dengan proyek mereka masing-masing. Hal ini menunjukkan bahwa tanpa aturan *need-to-know*, mereka mungkin bisa melihat data yang tidak perlu, yang bisa membahayakan keamanan informasi.

Pembelajaran 16: Dapatkan dukungan dari *top level* manajemen dan pemangku kepentingan terkait

Langkah-Langkah Penyusunan Rencana Strategis Keamanan

1. Memahami Bisnis: Langkah pertama adalah memahami kebutuhan dan tujuan bisnis. Ini penting agar rencana keamanan yang dibuat sesuai dengan kebutuhan organisasi.
2. Melakukan Analisis Lanskap Ancaman: Langkah kedua adalah menganalisis ancaman yang mungkin dihadapi, seperti serangan siber atau kebocoran data, untuk mengetahui risiko yang ada.
3. Mengembangkan *Roadmap* dan Program Keamanan terhadap Kondisi Saat Ini: Langkah ketiga adalah membuat peta jalan (*roadmap*) dan program keamanan berdasarkan kondisi saat ini, sehingga langkah-langkah yang diambil relevan dengan situasi organisasi.
4. Mengevaluasi dan Mengembangkan Kebijakan Keamanan: Langkah keempat adalah mengevaluasi kebijakan keamanan yang sudah ada dan mengembangkannya agar lebih baik, sehingga kebijakan tersebut dapat mendukung tujuan keamanan.
5. Mengeloa, Mengawasi, dan Menentukan Prioritas: Langkah terakhir adalah mengelola, mengawasi, dan menentukan prioritas dalam pelaksanaan rencana keamanan, agar sumber daya digunakan secara efektif.

Materi Pembelajaran 17: Definisikan Kebutuhan Keamanan Sejak Awal



.

Kecenderungan Pendefinisian Keamanan Setelah Insiden

Diagram menunjukkan siklus pengembangan sistem yang aman (Secure Development Lifecycle) dengan langkah-langkah seperti *Initialization, Analysis, Design, Realization, Initial Setup, Operation, Update Management, dan Decommissioning*. Setiap langkah memiliki praktik keamanan, seperti Threat *Analysis* pada tahap *Analysis* dan *Secure Design* pada tahap *Design*. Namun, jika keamanan hanya diterapkan setelah insiden terjadi, misalnya setelah tahap *Operation*, maka biaya untuk memperbaiki masalah akan lebih besar. Seharusnya, keamanan sudah diterapkan sejak awal, seperti pada tahap *Secure Design*, untuk mencegah insiden dan mengurangi biaya.

Tim Keamanan sebagai "*Project Stopper*"

Dalam diagram, langkah-langkah keamanan seperti *Code Analysis, Penetration Tests, Hardening, dan Secure Operation* sering kali dianggap memperlambat proyek. Misalnya, pada tahap *Realization*, tim keamanan mungkin meminta *Code Analysis* untuk memastikan tidak ada celah keamanan. Hal ini bisa membuat tim pengembang merasa terhambat, sehingga tim keamanan sering disebut sebagai "*Project Stopper*". Padahal, langkah ini penting untuk memastikan sistem aman sebelum digunakan.

Fokus Pengembangan Sistem pada Proses Bisnis

Diagram menunjukkan bahwa siklus pengembangan sistem sering kali lebih fokus pada kesesuaian dengan proses bisnis, seperti pada tahap Initialization dan Analysis, di mana kebutuhan bisnis menjadi prioritas utama. Namun, keamanan juga harus menjadi bagian penting sejak awal. Misalnya, pada tahap *Design*, *Secure Design* harus dilakukan untuk memastikan sistem tidak hanya mendukung proses bisnis, tetapi juga aman dari ancaman. Dengan mengintegrasikan keamanan sejak awal, seperti yang ditunjukkan dalam mapping ke *IEC 62443-4-1 practices*, sistem dapat berjalan dengan baik tanpa mengorbankan aspek keamanan.