LAPORAN RESMI
KEMANAN JARINGAN

Resume Bab 3 Cyber Security Controls

Dosen :
Dr. Ferry Astika Saputra ST, M.Sc
Oleh :
Septiana Dyah Anissawati
D4 LJ Teknik Informatika B
3122640031

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
TAHUN AJARAN
2022/2023

Bab 3 APNIC membahas mengenai kontrol keamanan atau countermeasures, yang terdiri dari tindakan atau mekanisme yang dapat digunakan untuk mengelola risiko keamanan. Countermeasures dapat berupa pedoman, praktik atau struktur organisasi, dan dapat bersifat administratif, teknis, manajerial, atau legal.

Pedoman mengacu pada aturan atau panduan yang harus diikuti oleh organisasi dalam mengelola keamanan informasi. Pedoman ini dapat meliputi kebijakan keamanan informasi, prosedur operasional standar, dan pedoman penggunaan yang aman.

Praktik keamanan informasi mencakup tindakan teknis dan operasional yang dilakukan untuk melindungi informasi. Contohnya adalah melakukan backup secara rutin, enkripsi data, pemantauan sistem, dan melakukan patching terhadap kerentanan keamanan.

Struktur organisasi keamanan informasi adalah bentuk pengaturan dalam organisasi yang membahas masalah keamanan informasi secara sistematis dan terstruktur. Struktur organisasi dapat mencakup unit keamanan informasi, komite keamanan informasi, dan pemegang tanggung jawab keamanan informasi.

Selain itu, kontrol keamanan juga dapat bersifat teknis seperti penggunaan firewall, deteksi intrusi, dan enkripsi data. Kontrol manajerial seperti pelatihan keamanan dan pengelolaan akses juga dapat digunakan untuk mengelola risiko keamanan.

Terakhir, kontrol keamanan juga dapat bersifat legal seperti regulasi dan undang-undang keamanan informasi yang dapat memberikan pengaruh pada praktek bisnis dan teknologi informasi suatu organisasi.

Cyber Security Framework atau standar keamanan siber adalah serangkaian proses terdokumentasi yang digunakan untuk menentukan kebijakan dan prosedur seputar implementasi serta pengelolaan kontrol keamanan pada lingkungan perusahaan. NIST Cybersecurity Framework adalah salah satu contoh standar keamanan siber yang dikembangkan oleh National Institute of Standards and Technology (NIST) di Amerika Serikat. Standar ini menyediakan kerangka kerja umum dan fleksibel untuk membantu organisasi mengembangkan, menerapkan, dan meningkatkan program keamanan siber mereka. NIST terdiri dari :

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

Beberapa kerangka kerja/standar Keamanan Siber populer, antara lain:

1. Seri ISO 27000 (Sistem Manajemen Keamanan Informasi)
   Seri ISO 27000 adalah kumpulan standar internasional untuk sistem manajemen keamanan informasi yang memberikan panduan tentang praktik terbaik dalam manajemen keamanan informasi, termasuk pengelolaan risiko, kontrol keamanan, dan pemeliharaan keamanan informasi.
2. NIST Cyber Security Framework
   NIST Cyber Security Framework adalah sebuah kerangka kerja keamanan siber yang dikembangkan oleh National Institute of Standards and Technology (NIST) Amerika Serikat. Kerangka kerja ini memberikan panduan tentang cara membangun, mengintegrasikan, dan meningkatkan program keamanan siber organisasi.
3. Standar Keamanan Data Industri Kartu Pembayaran (PCIDSS)
   PCIDSS adalah standar keamanan yang dirancang untuk melindungi informasi pembayaran dari pelanggan, seperti nomor kartu kredit, ketika berada dalam sistem perusahaan. Standar ini dirancang oleh Payment Card Industry Security Standards Council (PCI SSC).
4. Kontrol Keamanan Kritis CIS

CIS Critical Security Controls adalah kerangka kerja keamanan siber yang disusun oleh Center for Internet Security (CIS) untuk membantu organisasi dalam melindungi sistem informasi mereka dari serangan siber. Kerangka kerja ini terdiri dari 20 kontrol keamanan yang dianggap kritis dan memberikan panduan tentang cara mengimplementasikan kontrol keamanan tersebut dalam organisasi.

Kebijakan keamanan pada dasarnya menjelaskan apa yang harus dilakukan untuk melindungi organisasi dan aset informasinya.Biasanya berbentuk dokumen tertulis yang mencakup area-area kunci seperti:

1. Kebijakan Penggunaan Aset IT
2. Kebijakan Kata Sandi
3. Kebijakan Internet
4. Kebijakan Backup

Sangat penting bahwa kebijakan keamanan dibagikan kepada semua pemangku kepentingan sehingga mereka menyadari tanggung jawab mereka dan harapan organisasi.

Firewall adalah suatu sistem keamanan yang berfungsi untuk mencegah akses tidak sah ke dalam suatu komputer atau jaringan. Biasanya, firewall diinstal pada batas antara dua jaringan, dan dapat berupa perangkat keras atau perangkat lunak yang dijalankan pada sebuah komputer yang bertindak sebagai gateway. Firewall dapat melakukan beberapa tindakan untuk mengelola risiko, di antaranya adalah melakukan inspeksi terhadap lalu lintas data berdasarkan kebijakan tertentu, kemudian memblokir atau mengizinkannya, serta membatasi akses ke sistem atau layanan tertentu. Selain itu, firewall juga dapat memfilter lalu lintas data berdasarkan sumber dan tujuan alamat atau nomor port, jenis lalu lintas jaringan, atau atribut lain dari paket jaringan.

Anti-malware sebagai salah satu countermeasures atau pengendali risiko dalam keamanan siber. Anti-malware adalah software yang dapat melindungi sistem komputer dari serangan malware seperti virus, trojan, ransomware, worm, dan spyware.

Penting untuk selalu memperbarui anti-malware yang digunakan karena malware cenderung berkembang dengan cepat. Hal ini dapat dilakukan dengan melakukan update pada software atau database definisi virus agar dapat mendeteksi dan mengatasi jenis malware terbaru. Dengan menggunakan anti-malware yang efektif dan terbaru, dapat membantu mengurangi risiko terhadap serangan malware pada sistem komputer atau jaringan.

Vulnerability Management, dijelaskan tentang praktik siklus dalam mengidentifikasi, mengelompokkan, memperbaiki, dan mengurangi kerentanan pada sistem atau jaringan. Hal ini dilakukan untuk mengurangi risiko serangan dan kebocoran data yang dapat merugikan organisasi.

Selain itu, presentasi juga menyoroti pentingnya mengevaluasi tingkat keparahan dari setiap kerentanan yang ditemukan. Hal ini dikarenakan terkadang, kerentanan yang ditemukan pada software atau firmware dapat memberikan kesempatan bagi penyerang untuk mendapatkan akses tidak sah ke jaringan atau data. Oleh karena itu, dengan mengetahui tingkat keparahan kerentanan tersebut, organisasi dapat mengambil tindakan yang sesuai dan memprioritaskan penanganannya.

Presentasi tersebut menekankan pada pentingnya Vulnerability Management dalam upaya meningkatkan keamanan dan mengurangi risiko serangan pada sistem atau jaringan. Dengan melakukan praktik siklus ini secara teratur, organisasi dapat mengidentifikasi kerentanan secara dini, memperbaikinya, dan mengurangi risiko serangan yang dapat merugikan.

Intrusion Detection System (IDS), yang merupakan sebuah perangkat atau software yang digunakan untuk memantau jaringan dan sistem untuk aktivitas yang bersifat merusak.

IDS dapat melakukan investigasi terhadap konten dari paket data dan mencari atribut yang terkait dengan aktivitas yang bersifat merusak atau pelanggaran kebijakan. Kemudian

aktivitas tersebut dicatat dan dilaporkan kepada administrator sehingga tindakan selanjutnya dapat diambil.

IDS dapat berbasis jaringan atau host. IDS juga dapat beroperasi hanya sebagai detektor atau sebagai Intrusion Prevention System (IPS) yang dapat memblokir atau menghentikan aktivitas yang bersifat merusak. Dengan adanya IDS, organisasi dapat mengidentifikasi dan menanggulangi serangan keamanan secara lebih efektif, sehingga membantu dalam meningkatkan keamanan jaringan dan sistem mereka.

Enkripsi sebagai salah satu solusi dalam mengamankan data dan informasi. Enkripsi adalah proses mengubah data menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang dengan menggunakan algoritma khusus. Dalam konteks keamanan siber, enkripsi digunakan untuk melindungi file sistem, transaksi jaringan, media yang dapat dilepas, dan email dari akses oleh pihak yang tidak berwenang. Data dan informasi yang dienkripsi hanya dapat diakses dengan kunci atau sandi yang tepat.

Enkripsi merupakan salah satu upaya penting dalam mengurangi dampak kebocoran atau pencurian data sensitif. Di dalam organisasi, enkripsi umumnya digunakan dalam protokol jaringan seperti SSH, HTTPS, dan VPN. Selain itu, enkripsi juga sering digunakan dalam email dengan menggunakan protokol PGP atau SMIME. Dengan menggunakan enkripsi, data dan informasi yang dikirimkan dapat terlindungi dari pengintai dan penjahat siber.

Pada slide Two-Factor Authentication (2FA), dijelaskan mengenai konsep dasar 2FA. 2FA adalah metode verifikasi identitas pengguna dengan menggunakan kombinasi dua komponen yang berbeda. Dalam hal ini, 2FA secara signifikan mengurangi risiko peretas dapat mengakses akun online dengan menggabungkan kata sandi (sesuatu yang Anda ketahui) dengan faktor kedua, seperti ponsel atau token perangkat keras (sesuatu yang Anda miliki).

Slide tersebut juga menjelaskan bahwa karena semakin banyaknya pelanggaran keamanan yang disebabkan oleh kata sandi yang lemah atau dicuri, banyak organisasi yang menerapkan 2FA untuk memberikan lapisan keamanan tambahan bagi pengguna mereka. Selain itu, 2FA juga dapat membantu mengurangi biaya kerugian yang diakibatkan oleh peretasan.

Login with username & password → Choose to receive your code → Enter your 2FA code

Menjelaskan mengenai dua hal yang berbeda, yaitu security audit dan security vulnerability. Security audit merupakan evaluasi teknis yang dapat diukur terhadap sistem atau aplikasi, yang bertujuan untuk menemukan kelemahan atau celah dalam keamanan, dan memberikan rekomendasi untuk meningkatkan keamanan sistem tersebut. Proses ini dapat melibatkan analisis fisik, wawancara dengan orang-orang yang terlibat dalam sistem tersebut, serta pemindaian untuk mencari kelemahan atau celah dalam keamanan.

Sementara itu, security vulnerability adalah kelemahan atau celah dalam sistem atau aplikasi yang dapat dieksploitasi oleh penyerang untuk melakukan serangan dan mengakses informasi atau sumber daya yang seharusnya terbatas. Untuk mengidentifikasi kelemahan atau celah dalam keamanan, auditor dapat melakukan analisis fisik, wawancara, dan pemindaian. Setelah kelemahan atau celah diidentifikasi, rekomendasi dapat diberikan untuk memperbaikinya dan meningkatkan keamanan sistem atau aplikasi.

Pentingnya memiliki kemampuan untuk merespons dan menangani insiden keamanan dalam upaya meminimalkan dampak kebocoran atau serangan keamanan serta memulihkan keadaan dengan cepat. PPT tersebut menjelaskan bahwa persiapan yang baik dalam menangani insiden keamanan dapat dilakukan dengan menetapkan prosedur untuk:

1. Mendeteksi berbagai jenis insiden keamanan
2. Menghapus akar penyebab insiden
3. Memulihkan keadaan menjadi seperti sebelum insiden terjadi
4. Meninjau pelajaran yang dipetik dari insiden untuk perbaikan di masa depan

Selain itu, PPT tersebut juga membahas bahwa beberapa organisasi memiliki tim respons keamanan yang didedikasikan (CERT/CSIRT) yang memiliki keterampilan dalam melakukan analisis log, investigasi malware, dan forensik digital. Tim CSIRT ini kadang-kadang juga bekerja sama dengan entitas eksternal seperti agen penegak hukum, operator jaringan, atau CERT pemerintah.

Pentingnya pendidikan dan pelatihan dalam menciptakan budaya keamanan yang kuat di dalam organisasi. Kultur keamanan yang kuat sangat krusial dalam melindungi organisasi dari ancaman siber. Tanpa dukungan dari semua stakeholder dalam organisasi, keamanan tidak dapat dicapai secara efektif.

Staf di dalam organisasi harus sadar akan pentingnya keamanan, kebijakan dan tindakan pencegahan yang telah diterapkan, serta peran dan tanggung jawab mereka dalam menjaga keamanan. Edukasi dan pelatihan dapat membantu staf memahami pentingnya keamanan siber, memperkuat kultur keamanan, serta meningkatkan kesadaran akan ancaman siber yang mungkin terjadi.

Beberapa cara untuk mencapai tujuan ini adalah melalui kampanye kesadaran keamanan, pelatihan, atau latihan desktop. Melalui pelatihan dan pendidikan yang tepat, staf dapat memperoleh pengetahuan, keterampilan, dan sikap yang diperlukan untuk membantu mengurangi risiko dan memperkuat keamanan organisasi.

"Putting It All Together" pada modul APNIC membahas tentang pentingnya memahami cara mengintegrasikan berbagai countermeasures atau pengendalian keamanan untuk mencapai tujuan keamanan yang diinginkan. Ada banyak pengendalian keamanan yang dapat diterapkan tergantung pada jenis serangan yang dimaksudkan dan apa yang ingin dicapai.

Presentasi ini menekankan bahwa pengendalian keamanan tidak dapat berdiri sendiri dan harus diterapkan secara terpadu untuk efektif dalam melindungi jaringan dan sistem. Misalnya, firewall, antivirus, enkripsi, dan kebijakan akses yang kuat harus digunakan secara bersama-sama untuk meningkatkan keamanan sistem.

Dalam beberapa kasus, beberapa lapisan pengendalian keamanan digunakan untuk memperkuat pertahanan. Misalnya, firewall dapat dipasang di antara jaringan internal dan eksternal, sementara antivirus dan enkripsi dapat diterapkan pada level sistem dan file. Melalui pendekatan terpadu ini, organisasi dapat meningkatkan keamanan dan mengurangi risiko serangan yang mengancam sistem dan data mereka.

KESIMPULAN : Mengenai cyber controls dan countermeasures sebagai upaya untuk mengurangi risiko keamanan siber. Terdapat berbagai macam jenis countermeasures yang dapat diterapkan, seperti firewall, access control, encryption, dan monitoring. Penting untuk memahami bahwa semua countermeasures tersebut bekerja secara terintegrasi dan perlu diterapkan dalam lapisan yang berbeda untuk memperkuat pertahanan. Selain itu, perlu diingat bahwa countermeasures hanyalah salah satu aspek dari keamanan siber dan harus dipadukan dengan praktik keamanan lainnya seperti pelatihan pengguna dan manajemen keamanan yang baik untuk menciptakan lingkungan keamanan yang kokoh.

HASIL :

Knowledge Check 3

You will need to achieve a score of 80% or higher to pass the quiz. If you don't pass on your first attempt, you can retake the quiz as needed.

Results

7 of 7 Questions answered correctly

Your time: 00:07:17

You have reached 7 of 7 point(s), (100%)

Click Here to Continue

Restart Quiz