LAPORAN RESMI
KEMANAN JARINGAN

Resume Bab 2 Cyber Security in Organization

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

Keamanan siber sangat penting bagi organisasi karena adanya berbagai ancaman yang dapat mengancam keberlangsungan bisnis dan reputasi organisasi tersebut. Beberapa alasan mengapa organisasi membutuhkan keamanan siber adalah.

Pernyataan tersebut menjelaskan tentang alasan mengapa organisasi perlu mempertimbangkan dan mengambil tindakan untuk mengurangi risiko atau kerentanan dalam bisnis mereka. Alasan utama adalah karena ancaman yang memanfaatkan kerentanan dapat merugikan atau mengganggu aktivitas bisnis.

Contohnya, jika organisasi tidak memiliki keamanan yang memadai dalam sistem IT mereka, hacker dapat mengeksploitasi kerentanan tersebut dan menyebabkan pencurian data, gangguan operasi, atau kerugian finansial lainnya. Oleh karena itu, organisasi harus mempertimbangkan risiko dan mengambil tindakan pencegahan seperti memasang sistem keamanan yang memadai, melakukan pengujian keamanan secara teratur, dan melatih karyawan untuk meningkatkan kesadaran keamanan.

Pernyataan ini juga memberikan contoh bagaimana organisasi dapat mengurangi risiko kebakaran. Organisasi memasang smoke detector dan alarm kebakaran di lokasi strategis untuk mendeteksi kebakaran sejak dini dan memberi waktu bagi orang untuk keluar dari gedung. Selain itu, mereka melakukan latihan kebakaran secara teratur untuk memastikan bahwa semua orang tahu apa yang harus dilakukan jika terjadi kebakaran. Terakhir, organisasi juga membeli asuransi kebakaran sebagai bentuk perlindungan finansial jika terjadi kerusakan atau kehilangan akibat kebakaran.

Secara keseluruhan, pernyataan tersebut menekankan pentingnya mempertimbangkan risiko dan mengambil tindakan untuk mengurangi kerentanan dalam bisnis agar dapat melindungi bisnis dari kerusakan dan gangguan yang dapat terjadi akibat ancaman atau risiko. Terdapat beberapa jenis dampak bisnis atau Business Impact yang dapat terjadi akibat insiden keamanan siber.

Insiden keamanan dapat berdampak pada berbagai aspek bisnis, antara lain:

1. Database server down karena serangan Distributed Denial of Service (DDoS)
2. Waktu tambahan yang dibutuhkan untuk pulih dari infeksi malware massal
3. Bisnis didenda oleh otoritas setempat karena pelanggaran informasi pelanggan
4. Insiden keamanan menyebabkan pelanggan merasa bahwa organisasi tidak serius dalam melindungi informasi pelanggan
5. Operasi bisnis terganggu karena masalah yang terkait dengan pemasok, kerusakan infrastruktur, dan sebagainya.
6. Biaya operasional bisnis meningkat
7. Tidak dapat memberikan layanan berdasarkan kontrak atau tidak dapat memenuhi peraturan
8. Citra atau merek organisasi terpengaruh.

Dari teks tersebut, dapat disimpulkan bahwa insiden keamanan dapat berdampak negatif pada berbagai aspek bisnis, termasuk reputasi, biaya operasional, kepatuhan terhadap regulasi, dan hubungan dengan pelanggan dan pemasok. Oleh karena itu, penting bagi organisasi untuk mengidentifikasi dan mengelola risiko keamanan dengan baik untuk meminimalkan dampak negatif dari insiden keamanan.

Managing Risks merupakan salah satu strategi untuk mengurangi dampak keamanan siber terhadap organisasi. Risiko keamanan siber dapat diidentifikasi, dievaluasi, dan diatasi dengan langkah-langkah yang tepat untuk mengurangi dampaknya terhadap organisasi. Berikut adalah beberapa langkah yang dapat diambil untuk mengelola risiko keamanan siber:

1. Identifikasi Risiko: Pertama, organisasi perlu mengidentifikasi risiko keamanan siber yang mungkin terjadi dalam infrastruktur mereka. Langkah ini dapat dilakukan

dengan melakukan audit keamanan, memeriksa sistem keamanan, dan mengevaluasi ancaman yang mungkin terjadi.

2. Evaluasi Risiko: Setelah risiko diidentifikasi, organisasi perlu mengevaluasi potensi dampak dan kemungkinan risiko tersebut terjadi. Evaluasi risiko harus mempertimbangkan potensi dampak finansial, operasional, reputasi, legal, dan regulasi.
3. Penanganan Risiko: Setelah risiko dievaluasi, organisasi perlu menentukan bagaimana risiko tersebut akan ditangani. Pilihan yang dapat diambil termasuk pengurangan risiko, transfer risiko, penerimaan risiko, atau penghindaran risiko.
4. Implementasi: Setelah rencana pengelolaan risiko disusun, langkah selanjutnya adalah mengimplementasikan langkah-langkah tersebut. Implementasi dapat melibatkan perubahan dalam sistem keamanan, pelatihan karyawan, atau investasi dalam infrastruktur keamanan.
5. Monitor dan Evaluasi: Terakhir, organisasi perlu memonitor dan mengevaluasi efektivitas langkah-langkah pengelolaan risiko yang diambil. Hal ini penting untuk memastikan bahwa sistem keamanan tetap efektif dan mengatasi risiko keamanan siber yang mungkin terjadi.

Dalam mengelola risiko keamanan siber, organisasi perlu memperhatikan berbagai faktor seperti kebutuhan bisnis, biaya, dan tingkat risiko yang dapat diterima. Dalam hal ini, pengambilan keputusan harus didasarkan pada keseimbangan antara risiko yang dapat diterima dan biaya yang dikeluarkan untuk mengurangi risiko tersebut.

Increasing Cyber Security Preparedness adalah langkah-langkah yang dapat dilakukan oleh organisasi untuk meningkatkan kesiapan mereka dalam menghadapi ancaman keamanan siber. Kesiapan keamanan siber melibatkan langkah-langkah yang diambil untuk mengidentifikasi, melindungi, mendeteksi, merespon, dan memulihkan diri dari serangan keamanan siber.

Meningkatkan kesiapan atau persiapan dalam hal keamanan siber atau cyber security. Teks tersebut menyatakan bahwa untuk meningkatkan kesiapan keamanan siber, diperlukan pendekatan yang komprehensif dalam manajemen risiko.

Pendekatan yang komprehensif dalam manajemen risiko harus melibatkan orang-orang dari berbagai bagian organisasi untuk meningkatkan kualitas pengambilan keputusan dalam mengelola risiko. Hal ini menunjukkan bahwa penanganan risiko keamanan siber tidak hanya tanggung jawab dari satu atau beberapa orang saja, tetapi melibatkan seluruh bagian organisasi.

Dalam hal ini, meningkatkan kesiapan keamanan siber tidak hanya terkait dengan teknologi atau sistem, tetapi juga terkait dengan aspek manusia, seperti meningkatkan kesadaran akan risiko keamanan siber dan pengetahuan tentang praktik terbaik dalam mengelola risiko keamanan siber. Dengan melibatkan orang-orang dari berbagai bagian organisasi dalam manajemen risiko, maka organisasi dapat meningkatkan kemampuan untuk mengidentifikasi, menganalisis, dan mengatasi risiko keamanan siber dengan lebih efektif dan efisien.

Tanggung jawab manajemen terhadap keamanan siber atau cyber security dalam sebuah organisasi. Teks tersebut menyatakan bahwa pada akhirnya, manajemen tingkat atas atau top management organisasi bertanggung jawab untuk memastikan keamanan organisasi.

Hal ini menunjukkan bahwa manajemen tingkat atas memiliki peran penting dalam memastikan keamanan siber organisasi dan harus memimpin upaya untuk meningkatkan kesiapan keamanan siber secara keseluruhan.

Manajemen tingkat atas harus memastikan bahwa organisasi memiliki kebijakan keamanan siber yang komprehensif, serta menentukan dan mengalokasikan sumber daya yang cukup untuk mengatasi risiko keamanan siber yang mungkin terjadi. Selain itu, manajemen

tingkat atas juga harus memastikan bahwa seluruh anggota organisasi, termasuk staf dan karyawan, memahami dan mematuhi kebijakan keamanan siber yang telah ditetapkan.

Dengan memastikan bahwa manajemen tingkat atas secara aktif terlibat dalam upaya meningkatkan keamanan siber, maka organisasi dapat menciptakan lingkungan yang aman dan dapat diandalkan bagi pelanggan dan mitra bisnisnya, serta melindungi aset dan informasi penting dari serangan siber.

Upaya yang diperlukan untuk meningkatkan kesiapan atau persiapan dalam hal keamanan siber atau cyber security. Teks tersebut menyatakan bahwa untuk meningkatkan kesiapan keamanan siber, organisasi perlu berinvestasi dalam sumber daya, seperti uang, waktu, dan personel, serta mengembangkan program keamanan siber yang komprehensif.

Investasi sumber daya ini meliputi pengembangan dan penerapan kebijakan dan prosedur keamanan siber, pengembangan dan pelatihan karyawan dalam hal keamanan siber, penggunaan teknologi keamanan siber yang mutakhir, serta pelaksanaan audit dan evaluasi secara berkala terhadap program keamanan siber yang telah diterapkan.

Pengembangan program keamanan siber yang komprehensif mencakup aspek teknis dan non-teknis yang terkait dengan keamanan siber organisasi, seperti manajemen risiko keamanan siber, pelaporan insiden keamanan siber, pemantauan dan deteksi ancaman keamanan siber, dan pemulihan dari serangan siber.

Dengan menginvestasikan sumber daya dan mengembangkan program keamanan siber yang komprehensif, organisasi dapat meningkatkan kesiapan dan mampu menghadapi ancaman keamanan siber dengan lebih efektif dan efisien.

Kesadaran atau awarenes terhadap tingkat dan kemungkinan risiko memungkinkan organisasi untuk menjadi lebih proaktif dan siap menghadapi risiko tersebut.

Dalam konteks keamanan siber atau cyber security, kesadaran akan tingkat dan kemungkinan risiko berarti bahwa organisasi memahami jenis-jenis serangan siber yang mungkin terjadi, potensi kerugian atau dampak yang dapat ditimbulkan, serta seberapa sering serangan tersebut mungkin terjadi.

Dengan memahami hal ini, organisasi dapat mempersiapkan diri secara proaktif dan mengambil tindakan yang tepat untuk mengurangi kemungkinan terjadinya serangan siber atau meminimalkan dampaknya. Hal ini dapat mencakup pengembangan kebijakan dan prosedur keamanan siber yang lebih ketat, penerapan teknologi keamanan siber yang lebih baik, serta pelatihan karyawan dan staf tentang cara mengenali dan melaporkan ancaman keamanan siber.

Dengan menjadi lebih proaktif dan siap, organisasi dapat mengurangi risiko keamanan siber dan melindungi aset dan informasi penting mereka dari serangan siber yang merugikan.

Organisasi dapat menghadapi berbagai macam ancaman keamanan siber yang dapat membahayakan sistem, data, dan operasi bisnis mereka. Berikut adalah beberapa ancaman keamanan siber yang umum terjadi:

1. Malware: Malware adalah program yang dirancang untuk merusak atau mengambil alih sistem dan data. Malware dapat menyebabkan kerusakan pada sistem, mencuri data sensitif, dan menyebarkan diri ke sistem lain dalam jaringan.
2. Serangan DDoS: Serangan Distributed Denial of Service (DDoS) adalah serangan di mana penyerang mencoba membuat sistem tidak dapat diakses oleh pengguna yang sah dengan cara menyerang jaringan dengan traffic palsu sehingga jaringan menjadi lambat atau bahkan down.
3. Phishing: Phishing adalah taktik penipuan di mana penyerang mencoba untuk memperoleh informasi sensitif dari korban seperti username dan password dengan cara membuat email palsu atau situs web yang meniru perusahaan atau organisasi tertentu.

4. Ransomware: Ransomware adalah program yang mengenkripsi data pada sistem dan meminta uang tebusan agar data dapat dipulihkan. Ransomware sering kali menyebar melalui email palsu atau situs web yang tidak aman.
5. Serangan APT: Serangan Advanced Persistent Threat (APT) adalah serangan yang canggih dan terus menerus yang dilakukan oleh kelompok penyerang yang memiliki sumber daya dan kemampuan yang tinggi. Penyerang APT biasanya mencoba untuk memperoleh informasi rahasia dari organisasi atau perusahaan.
6. Insider Threat: Insider threat adalah ancaman keamanan siber yang berasal dari orang dalam organisasi yang memiliki akses ke data sensitif dan dapat menyalahgunakannya.
7. Serangan Zero-Day: Serangan Zero-Day adalah jenis serangan siber yang mengeksploitasi kelemahan atau kerentanan pada perangkat lunak atau sistem yang belum diketahui oleh vendor atau pengembangnya. Kelemahan atau kerentanan ini kemudian dieksploitasi oleh penyerang untuk melancarkan serangan tanpa bisa dideteksi oleh sistem keamanan yang ada.

Dalam keamanan siber, tidak ada solusi yang sempurna atau satu solusi tunggal yang dapat mencegah atau menghilangkan masalah keamanan. Oleh karena itu, untuk mengatasi risiko serangan siber, kita harus menerapkan kontrol pada berbagai level.

Pertama, kontrol teknis untuk mendeteksi dan mencegah serangan seperti firewall, filter spam, sistem deteksi intrusi, dan perangkat lunak antivirus dapat membantu mengurangi risiko serangan siber.

Kedua, pendidikan dan pelatihan bagi karyawan sangat penting terutama dalam hal phishing dan bagaimana mengembangkan aplikasi web secara aman. Dalam hal ini, upaya ini melibatkan pengembangan keahlian dan kesadaran karyawan mengenai risiko serangan siber.

Terakhir, penting juga untuk memastikan bahwa penyedia layanan jaringan memiliki kemampuan untuk mendukung kita saat kita diserang. Ini termasuk perencanaan keamanan yang matang dan penggunaan infrastruktur yang andal untuk mengurangi risiko serangan siber.

Dengan menerapkan kontrol pada berbagai level ini, organisasi dapat meningkatkan tingkat keamanan mereka dan mengurangi risiko serangan siber. Namun, perlu diingat bahwa pengamanan tidaklah statis, dan organisasi harus selalu berupaya untuk memperbarui dan meningkatkan sistem keamanan mereka untuk mengatasi serangan siber yang semakin canggih.

Soal

Knowledge Check 2

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.

The primary impact of a distributed denial of service attack is on which of the following security objectives

- ○ Safety
- ◉ Availability
- ○ Integrity
- ○ Confidentiality

Upon infection, what a malware does is dependent on the

- ○ Exploit Kit
- ○ Trojan
- ○ Worm
- ◉ Payload

Which of the following is not affected by a web defacement incident?

- ○ Server uptime
- ◉ Information Integrity
- ○ Organization's reputation
- ○ Information Availability

Impersonating a user to gain access to systems accessible to that user is an example of

- ○ Social Engineering
- ○ Email Spoofing
- ○ Email Theft
- ◉ Identity Theft

Tricking users to give away their login credentials is an example of

- ○ Denial of Service
- ○ Malware
- ○ Password Sniffing
- ◉ Phishing

In risk management, implementing counter measures such as a firewall or running security awareness campaigns are an example of

- ○ Risk Analysis
- ◉ Risk Mitigation
- ○ Risk Assessment
- ○ Risk Transfer

In an organization, positive security culture and awareness can be achieved by which of the following approach?

- ○ Monitoring network activities
- ◉ Security Awareness Campaigns
- ○ Vulnerability and Patch Management
- ○ Risk Management

Which one of the following is not considered good practice when managing passwords?

- ○ the password should not be shared with others
- ○ the password should be stored and transmitted securely
- ◉ the password should be sent in plaintext by email
- ○ the password should be long and complex enough to make it difficult for someone else to guess

Finish Quiz

Course Progress

Course Navigation

Module 1: Cyber Security Fundamentals

Module 2: Cyber Security in the Organization

Knowledge Check 2

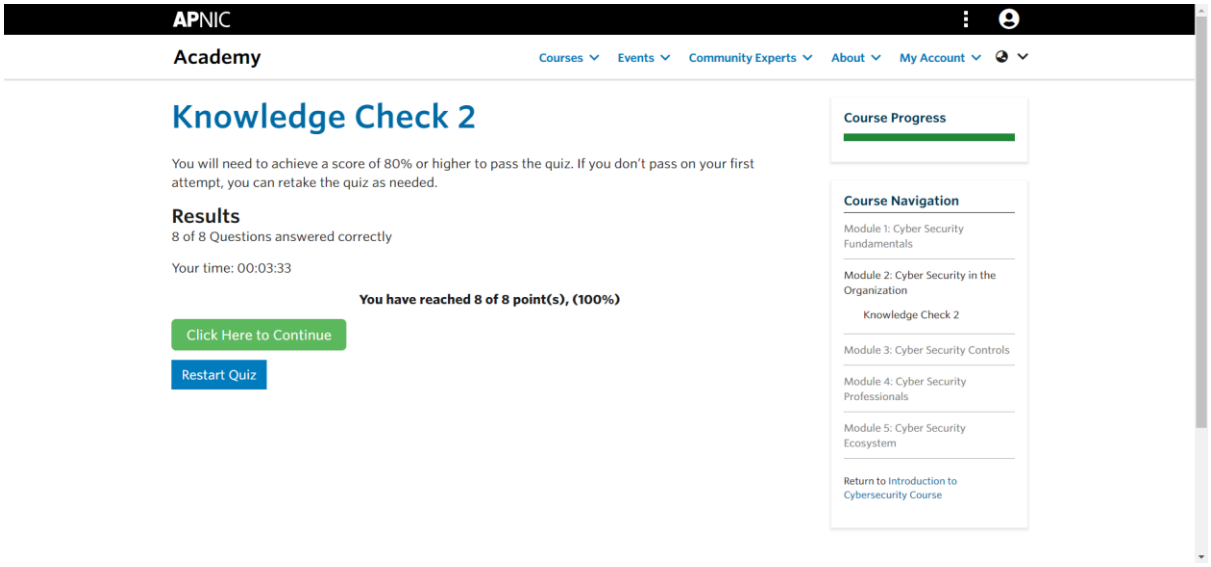
Module 3: Cyber Security Controls

Module 4: Cyber Security Professionals

Module 5: Cyber Security Ecosystem

Return to Introduction to Cybersecurity Course

Hasil


APNIC
Academy
Courses
Events
Community Experts
About
My Account
Knowledge Check 2
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
8 of 8 Questions answered correctly
Your time: 00:03:33
You have reached 8 of 8 point(s), (100%)
Click Here to Continue
Restart Quiz
Course Progress
Course Navigation
Module 1: Cyber Security Fundamentals
Module 2: Cyber Security in the Organization
Knowledge Check 2
Module 3: Cyber Security Controls
Module 4: Cyber Security Professionals
Module 5: Cyber Security Ecosystem
Return to Introduction to Cybersecurity Course