Makalah Tentang Cyber Security

Nama Kelompok
Robbi Aminudin
Wandi
Andika

Fakultas Ilmu Komputer
Universitas Bina bangsa
2019/2020

KATA PENGANTAR

DAFTAR ISI

BAB 1

PENDAHULUAN

BAB 11

2.1.Konsep Dasar

Dalam era globalisasi teknologi dalam perkembangan teknologi semakin banyak seseorang mengenalkan akan kemajuan teknologi semakin banyaknya juga seseorang menyalahkan gunakan arti dari teknologi tersebut.Dengan adanya makalah ini kita dapat mengetahui pengertian cyber security for electronic devices secara luas, Cyber security merupakan suatu bagian terpentingnya dalam berkembangan teknologi supaya kita bisa dapat menggunakan teknologi tidak semuanyax kita,karena ada undang-undang dan hokum bagaimana batasan apa yang perbolehkan tidaknya.

2.2. Tujuan cyber Security

Cyberlaw sangat dibutuhkan,kaitannya dengan upaya pencegahan tindakan pidana atau penanganan tindakan pidana.Cyberlaw akan menjadi dasar hukum dalam proses penegakan hokum terhadap kejahatan-kejahatan dengan sarana elektronik dan komputer-komputer,termasuk kejahatan pencucian uang dan kejahatan terorisme.

BAB III :PEMBAHASAN

3.1.Pengantar cyber Security cyber Space

Cyber Space di denfisikan sebagai media elektronik dan jaringan computer dimana komunikasi terjadi secara online.Komunikasi yang terjadi dalam cyber space bisa melibatkan siapa saja,kapan saja,dan dari mana saja selama media komunnikasi memungkinkan,berbeda dengan darat laut,dan udara yang memiliki batasan jelas sebagai wilayah territorial sebuah Negara cyber space tidak memiliki batasan tersebut dan menjadi entitas baru dalam national security.

Cyber Threat

Definisi threat dalam operasi informasi adalah semua jenis ancaman yang adalah semua jenis ancaman yang mengganggu kerfahasiaan(confidentiality),integritas (integrity),dan ketersedian (availability) informasi,threat ini bisa berupa ancaman secara fisik yang di sengaja dan /atau bencana alam serta ancaman yang muncul dari rahan cyber.Ancaman yang muncul dari rahan cyber ini di kenalkan sebagai cyber threat.

Perkembangan teknologi yang di anggap memiliki resiko tinggi dan berpotensi sebagai jalan masuk tidak sah dalam ranah cyber adalah sebagai berikut:

1. .Next Generation Network (NGN) yang mana lalu lintas paket data untuk telekomunikasi dan Internet tergabung dalam suatu protocol IP yang di sebut Triple Play.
2. Mesin- mesin yang menggunakan RFID (Radio Frequency Identification) telah dapat melakukan komunikasi antar media menggunakan jalur internet.

3. Remote control dan maintenance dalam sector industrial control system (ICS) atau menggunakan supervisory Control and Data Acquisition(SCADA) yang memungkinkan untuk melakukan komunikasi antara mesin – mesin industry melalui internet.
4. Network - based atau network – centric warfare yang focus pada yang berfokus pada C4ISR(Command,Control Computers,communications,information for interlligence,surveillance and Reconnaissance) telah menjadi masalah baru di dunia militer karena bentuk komunikasi dan integrasi telah tersedia untuk jalur internet.
5. Adanya teknologi terbaru di dunia computer yaitu Grid Computing dan cloud computing telah menjadi ISU baru dalam hal keamanan data dan informasi.
6. Perkembangan mobile phone dengan akses internet(Smartphone) telah terintegrasi dengan fungsi navigasi atau global positioning system (GPS) yang mana menimbulkan isu baru terhadap dunia intelijen dan militer.
7. Penyebaran akses internet untuk individu telah sampai pada teknologi mobile broadband yang bisa diakses dengan biaya yang relative terjangkau.
8. Teknologi yang secara khusus di kembangkan untuk masalah keamanan belum sampai kepada teknologi yang secara presisi memiliki kemampuan untuk meramalkan (forecasting) terhadap adanya rencana serangan.Teknologi yang berkembang saat ini hanya mampu untuk membaca adanya gejala atau anomaly yang telah terjadi.

Jalan masuk dari ranah cyber (cyber threat) ini menjadi ancaman jenis baru pada national security yang bisa dating karena ulah keisengan atau aktifitas terkordinasi dari individu,kelompok bahkkan antara Negara.

Cyber Attack

Definisi attack dalam operasi informasi adalah semua jenis tindakan yang sangaja di lakukan untuk mengganggu kerahasiaan(confidentiality),integritas(integrity),dan ketersediaan (availability) informasi tindakan ini bisa di tujukan untuk mengganggu secara fisik maupun dari alur logic system informasi.Cyber attack merupakan upaya mengganggu informasi yang berfokus pada alur logic system informasi.Berikut ini teknik umum yang sering digunakan terkait dengan metode cyber attack.

1. Reconnaissance merupakan upaya untuk memperoleh sebanyak mungkin informasi terkait target serangan,contoh aktifitas ini adalah pencairan melalui search engine,social website,enumerasi dan scanning pada infrastruktur system informasi.
2. Interception and tampering merupakan pelanggaran pada kerahasiaan dan integritas dan informasi selama di pertukarkan.Contoh aktifitas ini adalah man in the middle,sniffing,dan replay attack.
3. Exploit attack merupakan upaya untuk menerobos keamanan system informasi dengan menfaatkan celah keamanan pada protocol komunnikasi,system operasi ,dan aplikasi contoh aktifitas ini adalah serangan buffer overflow dan SQL injection.

4. Malware attack merupakan upaya untuk menerobos keamanan system informasi dengan menggunakan virus worm Trojan horse,backdoor,dan rookit.
5. Denial of servise merupakan pelanggaran pada ketersediaan informasi tujuan dari serangan ini adalah membuat system unresponsive atau crash misalnya radio signal jamming dan membanjiri jaringan dengan traffic atau dikenal sebagai flooding.
6. Social engineering merupakan upaya untuk menerobos keamanan dengan mentargetkan sumber daya manusia yang bertugas sebagai pengelola atau pengguna system informasi.

Cyber Attack
Pada kenyataannya cyber attack dan physical attack tidak terpisahkan dan sering di gunakan berhasil di gunakan bersama untuk mengganggu operasi informasi

Cyber Security
Definisi security dalam operasi informasi adalah semua mekanisme yang di lakukan untuk melindungi dan meminimalkan gangguan kerahasiaan(confidentiatily),integritas (integrity) dan ketersediaan (availability) informasi mekanisme ini harus bisa melindungi informasi baik dari physical attack maupun cyber attack.Cyber security merupakan upaya untuk melindungi informasi dari adanya cyber attack adapun elemen pokok cyber security adalah:

1. Dokumen Security policy merupakan dokumen standard yang di jadikan acuan dalam menjalankan semua proses terkait keamanan informasi.
2. Information infrastructure merupakan media yang berperan dalam kelangsungan hardware dan softwer .contohnya adalah router,switch,server,system operasi,database,dan website.
3. Perimeter defense merupakan media yang berperan sebagai komponen pertahan pada pada infrastruktur informasi misalnya IDS,IPS,dan firewall.
4. Network monitor System merupakan media yang berperan untuk memonitor kelayanan,untilinasi,dan performance infrastruktur informasi.
5. System information and eventa management merupakan media yang berperan dalam memonitor berbagai kejadian di jaringan termasuk kejadian terkait pada insiden keamanan.
6. Network security Assessment merupakan elemen cyber security yang berperan sebagai mekanisme control dan memberikan measurement level keamanan informasi.
7. Human resource dan security awareness berkaitan dengan sumber daya manusia dan awareness-nya pada keamanan informasi.

Cyber Security selain cyber sucerity kelangsungan pada operasi informasi juga bergantung pada physical security yang tentunya berkaitan dengan semua elemen fisikal misalnya bangunan data center,disaster recovery system,dan media transmisi.

Cyber Crime

Definisi cyber crime adalah semua tindakan yang dilakukan dengan niat kejahatan dimana computer atau jaringan computer menjadi target dan/atau menjadi alat kejahatan.berdasarkan definisi tersebut,berikut aktifitas yang bisa dikategorikan sebagai cyber crime:

a. Tindakan kejahatan dimana computer atau jaringan computer menjadi target yang termasuk dalam kategori ini adalah malicious code (malware),exploit attacks,dan denial of services.
b. Tindakan kejahatan dimana computer atau jaringan computer menjadi alat kejahatan,yang termasuk dalam kategori ini adalah identitt theft,fraud,cyberstalking,dan phising scams.

Selain kedua kategori tindak kejahatan tersebut di atas,beberapa orang juga mengkategoorikan high-tech crime seperti ATM skimming sebagai bentuk cyber crime:

Cyber War

Definis cyber war adalah semua tindakan yang di lakukan secara sengaja dan terkordinasi dengan tujuan menggangu kedaulatan sebuah Negara .Cyber war bisa berupa cyber attack,cyber terrorisme,maupun cyber espionage yang mengganggu keamanan nasional.Berikut beberapa cyber attack yang bisa dikategorikan dalam cyber war:

a. Cyber attackspada Estonia,2007 berupa serangan distributed denial of servies terkordinasi yang berhasil melumpuhkan website-website parlement,bank,kementria,surat kabar dan media berita lainnya di Estonia.
b. StuxNet,2010(waktu komplikasi terindikasi pada 2009) berupa serangan mentargetkan gangguan pada control system reactor,nuklir iran,stuxnet merupakan “high class” malware dilengkapi beberapa zero day exploit windows menunjukkan bahwa malwareini dibuat dengan rencana,budget dan kordinasi yang sangat baik.
c. Duqu 2011 merupakan malware yang memiliki kemiripan struktur dengan stuxnettetapi memiliki tujuan yang berbeda.Duqu melakukan cyber espionage/intelligience activity pada data dan asset kritikal.

Banyak pendapat yang mengatakan bahwa stuxnet merupakan salah satu cyber warfare tool terbaik saat ini dan sangat mungkin ditiru untuk masa yang akan dating.

Cyber law

Definisi cyber law adalah hokum terkait dengan proses dan resiko teknologi pada cyber space.Dari perspektif teknologi,cyber law dui gunakan untuk membedakan mana cyber activity yang bersifat legal dan mana yang tergolong tindakan kejahatan dunia maya(cyber crime) atau pelanggaran kebijakan (policy violation).

Saat ini Indonesia memiliki satu regulasi terkait dengan transakti elektronik yaitu UU

informasi dan transaksi elektronik (UU ITE).Dengan perkembangan berbagai issue pada ranah cyber,perlu dibuat regulasi baru agar bisa mencakup keseluruhan issue tersebut.

3.2.1.Mengapa cybersecurity melampaui Komputer

Sebenernya masalah ini tidak cybersecurity yang melampaui komputer,melainkan bahwa computer melampuai leptop dan destop tradisional.Banyak perangkat elektronik computer-dari ponsel dan PDA untuk video game dan system navigasi mobil.
Sementara computer menyediakan fitur peningkatan dan fungsionalitas mereka juga memperkenalkan risiko baru.penyerang mungkin dapat mengambil keuntungandari kemajuan teknologi untuk menargetkan perangkat sebelumnya dianggap”aman”sebagai contoh,seorang penyerang mungkin dapat menginfeksi ponsel Anda dengan virus mencuri ponsel atau layanan nnirkabel atau mengakses catatan pada PDA Anda,tidak hanya kegiatan ini memiliki implikasi untuk informasi pribadi anda,tapi mereka juga bisa memiliki konsekuensi serius jika anda menyimpanan iinformasi perusahan pada peringkat.Keamanan cyber melampaui desktop dan laptop tradisional computer,tetapi juga mencakup: ponsel personal digital assistant(PDA) system navigasi mobil,dll.

3.2.2.Apa Jenis Elektronik yang rentan

Setiap bagian dari peralatan elektronik yang menggunakan beberapa jenis komponen computer adalah rentan terhadap ketidak sempuranan perangkat lunak dan rentanan.Risiko meningkat jika perangkat terhubung ke internet atau jaringan yang seorang penyerang mungkin dapat mengakses ingat bahwa koneksi nirkabel juga memperkenalkan risiko ini luar koneksi menyediakan cara lagi penyerang untuk mengirim informasi ea tau mengekstrak informasi dari perangkat anda.Manjaga perangkat portabel anda untuk melindungi mesin dan informasi yang di kandungnya,semua peralatan elektronik menggunakan beberapa jenis komponen terkomputerisasi rentan.Resiko meningkat jika perangkat terhubung ke internet atau jaringan di mana penyerang bisa mendapatkan akses koneksi nirkabel juga rentan terhadap penyerang memperoleh akses ke perangkat anda,mereka dapat mengirimkan informasi kea tau mengekstrak informasi dari perangkat anda.Hanya anda yang dapat menentukan apa yang sebenernya beresiko,tanyakan kepada diri sendiri ,apa informasi pada perangkat saya saya tidak ingin orang untuk memiliki akses

3.2.3.Bagaimana Anda dapat melindungi diri

Inget keamanan fisik memiliki akses fisik keparangkat memudahkan untuk penyerangan untuk mengekstrak atau informasi yang korup Jangan meninggalkan perangkat anda tanpa pengawasan di depan umum atau daerah mudah diakses (lihat melindungi perangkat portabel;keamanan fisik untuk lebih informasi jauhkan perangkat lunak up to date – jika rilis penjual patch untuk perangkat lunak operasi perangkat anda menginstal mereka sesegera mungkin,patch ini dapat di

sebut update firmare instalasi mereka akan mencegah penyerang mampu mengambil keuntungan dari masalah di kenalkan atau kerentanan (lihat memahami patch untuk informasi lebih lanjut).Penggunaan password yang baik – pilih perangkat yang memungkinkan anda untuk melindungi informasi anda dengan password yang akan sulit bagi pencuri untuk menebak, dan menggunakan berbagai password untuk program yang berbeda dan perangkat (lihat memilih dan melindungi password untuk informasi lebih lanjut),jangan memilih pilihan yang memungkinkan computer anda untuk mengingat anda password,nonaktifkan konektivitas remote beberapa PDA dan ponsel yang di lengkapi dengan teknologi nirkabel,seperti Bluetooth,yang dapat di gunakan untuk terhubung ke perangkat lain atau computer,anda harus menonaktifkan fitur ini ketika mereka tidak digunakan (lihat memahami teknologi Bluetooth untuk informasi lebih lanjut),mengenkripsi file-meskipun sebagian besar perangkat tidak menawarkan anda pilihan untuk mengenkripsi file,anda mungkin memiliki perangkat lunak ekripsi pada PDA anda jika Anda menyimpanan informasi pribadi atau perusahaan,lihat apakah anda memiliki pilihan untuk mengenkrepsi file,oleh mengekrepsi file,anda memastikan bahwa orang yang tidak berhak tidak dapat melihat data bahkan jika mereka secara fisik dapat mengaksesnya,bila anda menggunakana enkripsi,penting untuk diingat anda password dan passphrase,jika anda lupa atau kehilangan mereka,Anda mungkin kehilangan data anda.

3.2.4. Peranan Cyber Security Dalam Android

Perangkat Android kini lebih sering diserang oleh malware dari PC,menurut sebuah laporan yang selasa oleh pembuatan perangkat lunak keamanan cyber,2013 security threat report dari Sophos mengungkapkan bahwa hampir 10 persen perangkat android di AS mengalami serangan malware selama tiga bulan pada tahun2012 ,di bandingkan dengan sekitar 6 persen dari PC. Situasi ini lebih buruk di Australia,di mana lebih dari 10 persen perangkat android telah di serang oleg malware di bandingkan dengan sekitar 8 persen untuk PC.
Dengan 52,2 persen pasar smartphone di amerika serikat,android telah menjadi target yang menggiurkan,Sophos melaporkan target ini besar sulit bagi pennulisan malware untuk menolak,”kata laporan itu,”Dan mereka tidak menolak serangan terhadap android meningkat pesat,”Sophos mencatat bahwa serangan malware yang paling umum pada android menlibatkan menginstal aplikasi palsu pada handset dan diam mengirimkan pesanan mahal untuk layanan SMS premium- rate.Cyber penjahat juga telah menemukan cara untuk menumbangkan otentikasi dua factor yang di gunakan otentikasi dua factor yang di gunakan oleh lembaga keuangan untuk melindungi transaksi mobile menurut laporan tersebut,mereka melakukan itu dengan menanan menguping malware pada handset untuk mendapatkan kode otentikasi yang di kirim ke telepon oleh bank untuk menyelesaikan transaksi.

3.2.5.Ponsel Cyber Security For National Cyber Security Awareness month

National Cyber Security Awareness month (NCSAM) mendeskripsikan keselamatan dan keamanan tips on the Go ponsel,penelitian ini,musim panas ini oleh consumer reports jelas menunjukkan bahwa keamanan cyber ponsel adalah masalah nyata,lebih dari 85% dari orang yang di survey tidak melindungi smartphone mereka dengan aplikasi keamanan meninggalkan

diri mereka rentan terhadap hampir satu juta virus ponsel di luar sana,sekarang lebih dari sebelumnya,sangat penting untuk memastikan perangkat mobile anda amanan berikut adalah beberapa tips keselamatan dan keamanan untuk gaya hidup mobile anda: Dapatkan sebuah aplikasi anti-virus dan anti malware: smartphone dan tablet membutuhkan anti- virus dan perlindungan anti-malware juga,dengan lebih dari 5 miliar orang diperkirakan akan menggunakan smartphone pada 2017 penulisan malware menargetkan smartphone dan tablet karena mereka begitu sering dibiarkan tanpa jaminan.

Aktifkan fitur anti- pencurian tidak hanya fitur anti pencurian melindungi perangkat anda dari pencuri,anda juga dapat menggunakan GPS fitur lokasi perangkat untuk melacak lokasi anak anda dalam keadaan darurat.

Sandi melindungi perangkat anda: melindungi smartphone atau tablet dengan password atau pin untuk mendapatkan akses adalah garis pertama pertahanan terhadap penjahat cyber.

BAB 1V

PENUTUP

4.1.KESIMPULAN

Dari hasil penulisan makalah ini penulis dapat mengambil beberapa kesimpulan di antaranya sebagai berikut,Cyber security adalah segala bentuk system keamanan di dalam dunia maya yang berhubungan dengan segala macam bentuk kegiatan menggunakan internet dan sebagai system keamanan informasi atau data.

1. Cyber security sangat berguna untuk banyak orang.karena data data yang penting dan rahasia dapat di jaga kerahasiaan data tersebut.
2. Berbagai upaya telah di lakukan pemerintah salah satunya dengan cyber security ini untuk menanggulangi terjadinya pencurian data oleh cybercrime dan pemerintah juga bahkan membuat undang- undang tentang tindakan pidana cyber security.