Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.3 (Agustus 2023)

KAJIAN CYBER SECURITY DALAM RANGKA KOPERASI MENGHADAPI REVOLUSI INDUSTRI 4.0

Kuncoro Wibowo[1], Udin Hidayat[2], Verdi Yasin[3]

Program Studi Manajemen[1], Program Studi Sains dan Teknologi[2]
Program Studi Teknik Informatika[3].
Fakultas Ekonomi dan Bisnis[1], Fakultas Sains dan Teknologi[2],
Fakultas Ilmu Komputer[3]
STIE Jayakarta[1], Universitas IKOPIN[2], STMIK Jayakarta[3]

kuncoro_wibowo@stie.jayakarta.ac.id[1], tigaputu7@gmail.com[2],
verdi_yasin@stmik.jayakarta.ac.id[3]

Received: June 5, 2023 **. Revised:** July 17, 2023 **. Accepted:** July 18, 2023**.**
Issue Period: Vol.7 No.3 (2023), Pp.634-645

Abstrak: Cyber Security merupakan upaya untuk melindungi informasi dari adanya Cyber Attack. Tujuan dari pembuatan makalah ini adalah untuk memberitahukan pentingnya Cyber Security di perangkat aplikasi, software serta perangkat lainnya pada era revolusi industry 4.0. Keamanan data mengacu pada langkah-langkah perlindungan privasi digital yang diterapkan untuk mencegah akses tidak sah ke komputer, database, dan situs web.
Contohnya misalkan dalam Android Cyber Security sangatlah penting karena untuk melindungi informasi-informasi yang kita miliki dan cyber security ini banyak di gunakan di kalahan perusahaan perusahaan juga. Sesuai dengan pembahasan diatas tadi bisa disimpulkan bahwa Cyber Security di era revolusi industry 4.0 ini, mengapa demikian? Karena Cyber Security itu sendiri dirancang dan dibuat untuk mengatasi masalah-masalah yang kemungkinan bisa terjadi dalam dunia cyber, kegunaan nya pun sudah sangat bermanfaat , terjamin dan layak untuk di pergunakan bahkan untuk sistem cyber security itu sendiri berkembang dan terus semakin baik dengan seiring nya jaman maka sudah tidak di ragukan lagi mengenai keamanan kenyamanan serta kegunaan dari cyber security itu sendiri.

Kata kunci: Keamanan Cyber, Aplikasi, Software, Revolusi Industri

Abstract: *Cyber Security is an effort to protect information from Cyber Attacks. The purpose of making this paper is to inform the importance of Cyber Security in application devices, software and other devices in the era of the industrial revolution 4.0. Data security refers to digital privacy protection measures enforced to prevent unauthorized access to computers, databases, and websites. For example, in Android Cyber Security is very important because to protect the information that we have and this cyber security is widely used by corporate companies as well. In accordance with the discussion above, it can be concluded that Cyber Security in the era of the industrial revolution 4.0, why is that? Because Cyber Security itself is designed and made to overcome problems that might occur in the cyber world, its use is very useful, guaranteed and feasible to use even for the cyber security system itself to develop and continue to get better with time. then there is no doubt about the security, comfort and usefulness of the cyber security itself.*

Keywords: *Cyber Security, Applications, Software, Industrial Revolution*

DOI: 10.52362/jisamar.v7i3.1132

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.3 (Agustus 2023)

I. PENDAHULUAN

Pada era teknologi, penggunaan komunikasi online melalui internet menjadi suatu norma. Penggunaan internet terus meningkat, karena saat ini internet merupakan sebagai suatu kebutuhan. Penyalahgunaan internet banyak terjadi, salah satunya yang disebabkan oleh bebasnya dalam penggunaan internet. Sistem pemerintah yang diterapkan pada suatu negara dapat pula menjadikan terjadinya meningkatnya penyerangan dari dunia maya. Kejahatan cyber berkembang dan terus meningkat, kejahatan cyber pun merubah fokusnya pada informasi keuangan, memata-matai bisnis, informasi dan akses pemerintahan dan lainya. Perkembangan kejahatan cyber sangatlah cepat, berkembang luas diseluruh dunia.

Dalam dunia usaha ketika perusahaan membuat suatu teknologi berbasis digital yang dapat diakses oleh banyak orang, mengharuskan perusahaan untuk menjaga asset – asset rahasia terkait perusahaan tersebut yang tidak boleh diketahui oleh khalayak ramai. Oleh karena itu, perusahaan harus memperkuat keamanan system agar asset-asset rahasia perusahaan dapat terjaga dengan baik dan tidak dapat dibobol oleh seorang pun. Sistem keamanan ini dinamakan dengan cyber security. Cyber security berfungsi untuk melindungi asset atau informasi perusahaan dari cyber attack. Cyber attack merupakan upaya mengganggu informasi yang berfokus pada alur logic sistem informasi. Cyber security dirancang sedemikian rupa untuk meminimalisir risiko bocornya asset atau informasi rahasia perusahaan ke publik.

Semua Perusahaan yang bertransformasi dari data berbasis digital sangat dianjurkan untuk memperhatikan dan menggunakan *cyber security* dalam menyimpan, mengakses dan mengambil informasi penting. Melindungi informasi dan data merupakan kebutuhan sebagian besar perusahaan dan instansi pemerintah di seluruh dunia karena data merupakan aset berharga dari suatu perusahaan dan bisa menjadi masalah di kemudian hari apabila data tersebut jatuh ke tangan orang yang tidak berhak.

II. METODE DAN MATERI

Perusahaan di era revolusi industri 4.0 sekarang saling berlomba dalam inovasi pengembangan teknologi. Dapat dilihat berbagai perusahaan saling mengungguli dan saling berkompetisi dalam menciptakan teknologi baru yang belum ada di pasaran. Namun perlu diingat juga ketika perusahaan menciptakan teknologi baru, maka harus diperkuat juga system keamanan nya agar teknologi tersebut tidak mudah dibobol oleh pihak yang tidak bertanggung jawab yang dapat merugikan perusahaan kedepannya.

Sistem keamanan teknologi yang diciptakan perusahaan terkadang dapat terkena cyber crime. Cyber crime merupakan tindak kriminal yang dilakukan dengan menggunakan teknologi komunikasi. Cyber crime yang dimaksud adalah pembobolan data atau informasi rahasia yang sengaja di hack untuk kepentingan pribadi atau pihak tertentu. Oleh karena itu pihak perusahaan harus memperkuat Cyber Security-nya.

Cyber security berguna untuk melindungi data atau informasi rahasia perusahaan. Terdapat tiga konsep cyber security (ISACA, 2015:6) yaitu :

A) confidentiality untuk perlindungan informasi yang belum diotorisasi atau diungkapkan.
B) integrity untuk perbaikan data yang rusak harus secepatnya diganti.
C) availability untuk menjamin akses yang tepat untuk penggunaan sistem informasi.

2.1. Pengertian Cyber Security

Cyber security adalah teknologi, proses dan praktik yang dirancang untuk melindungi jaringan, komputer, program dan data dari serangan, kerusakan atau akses yang tidak sah. *Cyber security* juga disebut sebagai upaya untuk melindungi informasi dari adanya *cyber attack*. *Cyber attack* dalam operasi informasi adalah semua jenis tindakan yang sengaja dilakukan untuk mengganggu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersedian (*availability*) informasi.

2.2. Istilah – istilah Cyber Security yang ada di Indonesia

2.2.1. Cyber Space

Cyber space didefinisikan sebagai media elektronik dan jaringan komputer di mana komunikasi terjadi secara online. Komunikasi yang terjadi dalam cyber space bisa melibatkan siapa saja, kapan saja, dan dari mana saja selama media komunikasi memungkinkan. Berbeda dengan darat, laut, dan udara yang memiliki batasan

DOI: 10.52362/jisamar.v7i3.1132

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.3 (Agustus 2023)

jelas sebagai wilayah territorial sebuah negara, cyber space tidak memiliki batasan tersebut dan menjadi entitas baru dalam national security.

2.2.2. Cyber Threat

Definisi threat dalam operasi informasi adalah semua jenis ancaman yang mengganggu kerahasiaan (confidentiality), integritas (integrity), dan ketersedian (availability) informasi. Threat ini bisa berupa ancaman secara fisik yang disengaja dan/atau bencana alam serta ancaman yang muncul dari ranah cyber. Ancaman yang muncul dari ranah cyber ini dikenal sebagai cyber threat.

2.2.3. Cyber Attack

Definisi attack dalam operasi informasi adalah semua jenis tindakan yang sengaja dilakukan untuk mengganggu kerahasiaan (confidentiality), integritas (integrity), dan ketersedian (availability) informasi. Tindakan ini bisa ditujukan untuk mengganggu secara fisik maupun dari alur logic sistem informasi. Cyber attack merupakan upaya mengganggu informasi yang berfokus pada alur logic sistem informasi. Berikut ini teknik umum yang sering digunakan terkait dengan metoda cyber attack:

- Reconnaissance merupakan upaya untuk memperoleh sebanyak mungkin informasi terkait target serangan. Contoh aktifitas ini adalah pencarian melalui search engine, social website, enumerasi dan scanning pada infrastruktur sistem informasi.
- Interception and tampering merupakan pelanggaran pada kerahasiaan dan integritas informasi selama dipertukarkan. Contoh aktifitas ini adalah man in the middle, sniffing, dan replay attack.
- Exploit attack merupakan upaya untuk menerobos keamanan sistem informasi dengan memanfaatkan celah keamanan pada protokol komunikasi, sistem operasi, dan aplikasi. Contoh aktifitas ini adalah serangan buffer overflow dan SQL injection.
- Malware attack merupakan upaya untuk menerobos keamanan sistem informasi dengan menggunakan virus, worm, trojan horse, backdoor dan rootkit.
- Denial of service merupakan pelanggaran pada ketersediaan informasi. Tujuan dari serangan ini adalah membuat sistem unresponsive atau crash misalnya radio signal jamming dan membanjiri jaringan dengan traffic atau dikenal sebagai flooding.
- Social engineering merupakan upaya untuk menerobos keamanan dengan mentargetkan sumber daya manusia yang bertugas sebagai pengelola atau pengguna sistem informasi.

Pada kenyataannya cyber attack dan physical attack tidak terpisahkan dan sering digunakan bersama untuk mengganggu operasi informasi.

2.2.4. Cyber Crime

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

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

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

2.2.5. Cyber War

Definisi cyber war adalah semua tindakan yang dilakukan secara sengaja dan terkoordinasi dengan tujuan mengganggu kedaulatan sebuah negara. Cyber war bisa berupa cyber attack, cyber terrorism, maupun cyber espionage yang mengganggu keamanan nasional. Berikut beberapa cyber attack yang bisa dikategorikan dalam cyber war:

- Cyber attacks pada Estonia, 2007 berupa serangan distributed denial of services terkoordinasi yang berhasil melumpuhkan website – website parlement, bank, kementerian, surat kabar, dan media berita lainnya di Estonia.
- StuxNet, 2010 (waktu kompilasi terindikasi pada 2009) berupa serangan malware yang secara spesifik mentargetkan gangguan pada control system reaktor nuklir iran. Stuxnet merupakan “high class” malware dilengkapi beberapa zero day exploit windows menunjukkan bahwa malware ini dibuat dengan rencana, budget, dan koordinasi yang sangat baik.

DOI: 10.52362/jisamar.v7i3.1132

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.3 (Agustus 2023)

- Cyber attacks pada Diginotar, 2011 berupa cyber attack pada root certificate authority dimana certificate organisasi besar di-sign. Ada 23 organisasi yang certificate-nya dikuasai diantaranya google, microsoft, yahoo, twitter, facebook, wordpress, mossad, SIS (MI6), dan CIA. Certificate ini memungkinkan bagi attacker "mengintip" data pada jalur terenkripsi (SSL).
- Duqu, 2011 merupakan malware yang memiliki kemiripan struktur dengan stuxnet tetapi memiliki tujuan yang berbeda. Duqu melakukan cyber espionage/intelligence activity pada data dan asset kritikal.

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

2.2.6. Cyber Law

Definisi cyber law adalah hukum terkait dengan proses dan resiko teknologi pada cyber space. Dari perspektif teknologi, cyber law digunakan untuk membedakan mana cyber activity yang bersifat legal dan mana yang tergolong tindak kejahatan dunia maya (cyber crime) atau pelanggaran kebijakan (policy violation).
Saat ini Indonesia memiliki satu regulasi terkait dengan transaksi 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.

2.3. Elemen – Elemen Cyber Security

1. Dokumen *security policy*, merupakan dokumen standar yang dijadikan acuan dalam menjalankan semua proses terkait keamanan informasi.
2. *Information infrastructure*, merupakan media yang berperan dalam kelangsungan operasi informasi meliputi hardware dan software. Contohnya adalah router, switch, server, operation system, database, dan website.
3. *Perimeter Defense*, merupakan media yang berperan sebagai komponen pertahanan pada infrastruktur informasi misalnya IDS, IPS, dan firewall.
4. *Network Monitoring System*, merupakan media yang berperan untuk memonitor kelayakan, utilisasi, dan performance infrastruktur informasi.
5. *System Information and Event 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 kontrol dan memberikan *measurement level* keamanan informasi.
7. *Human resource and security awareness*, Berkaitan dengan sumber daya manusia dan *awareness*-nya pada keamanan informasi.

2.4. Jenis Serangan Cyber di Era Digital

2.4.1. Phishing

Phishing adalah jenis rekayasa sosial yang biasanya digunakan untuk mencuri data pengguna seperti nomor kartu kredit dan kredensial masuk. Itu terjadi ketika seorang penyerang, menyamar sebagai individu tepercaya, menipu korban untuk membuka pesan teks, email, atau pesan instan. Korban kemudian ditipu untuk membuka tautan jahat yang dapat menyebabkan pembekuan sistem sebagai bagian dari serangan ransomware, mengungkapkan informasi sensitif, atau pemasangan malware. Pelanggaran ini dapat memiliki hasil bencana. Untuk seorang individu, ini termasuk pencurian identitas, pencurian dana, atau pembelian tanpa izin.
Phishing sering digunakan untuk mendapatkan pijakan di jaringan pemerintah atau perusahaan sebagai bagian dari plot yang lebih signifikan seperti Advanced Persistent Threat (APT). Dalam kasus seperti itu, karyawan dikompromikan untuk mendapatkan akses istimewa ke data aman, mendistribusikan malware di lingkungan tertutup, dan memintas parameter keamanan.

2.4.2. Malware

Malware adalah kode yang dibuat untuk secara diam-diam memengaruhi sistem komputer yang disusupi tanpa persetujuan pengguna. Definisi luas ini mencakup banyak jenis perangkat lunak jahat (malware) tertentu seperti spyware, ransomware, perintah, dan kontrol. Banyak pelaku bisnis dan pelaku kriminal yang terkenal telah terlibat dan menemukan penyebaran malware. Malware berbeda dari perangkat lunak lain karena dapat menyebar ke seluruh jaringan, menyebabkan perubahan dan kerusakan, tetap tidak terdeteksi, dan kuat dalam sistem yang terinfeksi. Itu dapat menghancurkan jaringan dan membuat kinerja mesin bertekuk lutut.

DOI: 10.52362/jisamar.v7i3.1132

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.3 (Agustus 2023)

2.4.3. Ransomware

Ransomware memblokir akses ke data korban, biasanya menghapusnya jika tebusan dibayarkan. Tidak ada jaminan bahwa membayar uang tebusan akan mendapatkan kembali akses ke data. Ransomware sering dilakukan melalui Trojan yang mengirimkan muatan yang disamarkan sebagai file yang sah.

2.4.4. Worms

Worms berbeda dari virus karena mereka tidak melampirkan ke file host, tetapi merupakan program mandiri yang menyebar di seluruh jaringan dan komputer. Worms biasanya menyebar melalui lampiran email, membuka lampiran akan mengaktifkan program cacing. Eksploitasi cacing biasanya melibatkan worm yang mengirimkan salinan dirinya ke setiap kontak di alamat e-mail komputer yang terinfeksi. Selain melakukan aktivitas jahat, worms yang menyebar di internet dan server e-mail yang berlebihan dapat mengakibatkan serangan penolakan layanan terhadap node pada jaringan.

2.4.5. Drive-by Attack

Serangan **Drive-by** Attack adalah metode umum penyebaran malware. Penyerang dunia maya mencari situs web tidak aman dan menanam skrip berbahaya ke dalam PHP atau HTTP di salah satu halaman. Skrip ini dapat menginstal malware ke komputer yang mengunjungi situs web ini atau menjadi IFRAME yang mengarahkan ulang browser korban ke situs yang dikendalikan oleh penyerang. Dalam kebanyakan kasus, skrip ini dikaburkan, dan ini membuat kode menjadi rumit untuk dianalisis oleh peneliti keamanan. Serangan-serangan ini dikenal sebagai drive-by karena mereka tidak memerlukan tindakan apapun dari pihak korban kecuali mengunjungi situs web yang dikompromikan. Ketika mereka mengunjungi situs yang dikompromikan, mereka secara otomatis dan diam – diam terinfeksi jika komputer mereka rentan terhadap malware, terutama jika mereka belum menerapkan pembaruan keamanan untuk aplikasi mereka.

2.4.6. Trojan Horses

Trojan adalah program perangkat lunak berbahaya yang salah mengartikan dirinya agar tampak berguna. Mereka menyebar dengan terlihat seperti perangkat lunak rutin dan membujuk korban untuk menginstal. Trojan dianggap sebagai salah satu jenis malware yang paling berbahaya, karena sering dirancang untuk mencuri informasi keuangan.

2.4.7. SQL Injection

SQL Injection, juga dikenal sebagai SQLI, adalah jenis serangan yang menggunakan kode jahat untuk memanipulasi database backend untuk mengakses informasi yang tidak dimaksudkan untuk ditampilkan. Ini mungkin termasuk banyak item termasuk detail pelanggan pribadi, daftar pengguna, atau data perusahaan yang sensitif.

SQLI dapat memiliki efek buruk pada bisnis. Serangan SQLI yang berhasil dapat menyebabkan penghapusan seluruh tabel, tampilan daftar pengguna yang tidak sah, dan dalam beberapa kasus, penyerang dapat memperoleh akses administratif ke database. Ini bisa sangat merugikan bisnis. Saat menghitung kemungkinan biaya SQLI, kalian harus mempertimbangkan hilangnya kepercayaan pelanggan jika informasi pribadi seperti alamat, detail kartu kredit, dan nomor telepon dicuri. Meskipun SQLI dapat digunakan untuk menyerang basis data SQL apa pun, pelakunya sering menargetkan situs web.

2.4.8. Cross Site Scripting

Cross Site Scripting (XSS) adalah sejenis pelanggaran injeksi tempat penyerang mengirimkan skrip berbahaya ke dalam konten dari situs web yang memiliki reputasi baik. Itu terjadi ketika sumber yang meragukan diizinkan untuk melampirkan kode sendiri ke dalam aplikasi web, dan kode jahat tersebut digabungkan bersama dengan konten dinamis yang kemudian dikirim ke browser korban.

Kode berbahaya biasanya dikirim dalam bentuk potongan – potongan kode Javascript yang dijalankan oleh browser target. Eksploitasi dapat menyertakan skrip yang dapat dieksekusi berbahaya dalam banyak bahasa termasuk Flash, HTML, Java, dan Ajax. Serangan XSS bisa sangat menghancurkan, namun mengurangi kerentanan yang memungkinkan serangan ini relatif sederhana.

2.4.9. Denial of Service (DDoS)

Denial Of Service (DDoS) bertujuan untuk mematikan jaringan atau layanan, menyebabkannya tidak dapat diakses oleh pengguna yang dituju. Serangan mencapai misi ini dengan membanjiri target dengan lalu lintas atau membanjirinya dengan informasi yang memicu kecelakaan. Dalam kedua situasi tersebut, serangan DoS menyangkal pengguna yang sah seperti karyawan, pemegang akun, dan anggota sumber daya atau layanan yang mereka harapkan.

DOI: 10.52362/jisamar.v7i3.1132

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.3 (Agustus 2023)

Serangan DDoS sering ditargetkan pada server web organisasi profil tinggi seperti organisasi perdagangan dan pemerintah, perusahaan media, perdagangan, dan perbankan. Meskipun serangan-serangan ini tidak mengakibatkan hilangnya atau pencurian informasi penting atau aset lain, mereka dapat menghabiskan banyak uang dan waktu bagi korban untuk memitigasi. DDoS sering digunakan dalam kombinasi untuk mengalihkan perhatian dari serangan jaringan lainnya.

2.4.10. Brute Force

Serangan **Brute Force** adalah serangan jaringan di mana penyerang mencoba masuk ke akun pengguna dengan secara sistematis memeriksa dan mencoba semua kata sandi yang mungkin sampai menemukan yang benar. Metode paling sederhana untuk menyerang adalah melalui pintu depan karena Anda harus memiliki cara masuk. Jika Anda memiliki kredensial yang diperlukan, Anda dapat memperoleh entri sebagai kalian biasa tanpa membuat log yang mencurigakan, memerlukan entri yang belum ditambal, atau tersandung tanda tangan IDS. Jika Anda memiliki kredensial sistem, hidup kalian bahkan disederhanakan karena penyerang tidak memiliki kemewahan ini.

Istilah brute force berarti mengalahkan sistem melalui pengulangan. Saat meretas kata sandi, brute force memerlukan perangkat lunak kamus yang menggabungkan kata-kata kamus dengan ribuan variasi berbeda. Ini adalah proses yang lebih lambat dan tidak efesien. Serangan – serangan ini dimulai dengan huruf – huruf sederhana seperti “a” dan kemudian pindah ke kata-kata penuh seperti “snoop” atau “snoopy”. Serangan kamus brute force dapat melakukan 100 hingga 1000 upaya per menit. Setelah beberapa jam atau berhari-hari, serangan brute force akhirnya dapat memecahkan kata sandi apa pun. Serangan brute force menegaskan kembali pentingnya praktik terbaik kata sandi, terutama pada sumber daya penting seperti switch jaringan, router dan server.

III. PEMBAHASA DAN HASIL

3.1. Penanggulangan Kejahatan Di Dunia Maya

Penanggulangan kejahatan di dunia maya atau yang biasa dikenal dengan keamanan komputer adalah suatu cabang teknologi yang dikenal dengan nama keamanan informasi yang diterapkan pada komputer. Sasaran keamanan komputer antara lain adalah sebagai perlindungan informasi terhadap pencurian atau korupsi, atau pemeliharaan ketersediaan, seperti dijabarkan dalam kebijakan keamanan Menurut Garfinkel dan Spafford, ahli dalam computer security, komputer dikatakan aman jika bisa diandalkan dan perangkat lunaknya bekerja sesuai dengan yang diharapkan. Penanggulangan kejahatan memiliki 6 tujuan, yaitu :

1. Privacy/Confidentiality
   a. Definisi : menjaga informasi dari orang yang tidak berhak mengakses
   b. Privacy : lebih kearah data-data yang sifatnya privat, Contoh e-mail seorang pemakai (user) tidak boleh dibaca oleh administrator.
   c. Confidentiality : berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut. Contoh : data – data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) harus dapat diproteksi dalam penggunaan dan penyebarannya.
   d. Bentuk Serangan usaha penyadapan (dengan program sniffer).
   e. Usaha – usaha yang dapat dilakukan untuk meningkatkan privacy dan e-confidentiality adalah dengan menggunakan teknologi kriptografi.
2. Integrity
   a. Definisi : informasi tidak boleh diubah tanpa seijin pemilik informasi Contoh e-mail di intercept di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju.
   b. Bentuk serangan : Adanya virus, trojan horse, atau pemakai lain yang mengubah infomasi tanpa ijin, "man in the middle attack" dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.

DOI: 10.52362/jisamar.v7i3.1132

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.3 (Agustus 2023)

3. Authentication
   a. Definisi : metode untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud.
   b. Adanya Tools membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermarking (untuk menjaga "intelectual properry", yaitu dengan menandai dokumen atau hasil karya dengan "signature" pembuat) dan digital signature.
   c. Access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. User harus menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.
4. Availability
   a. Definisi : berhubungan dengan ketersediaan informasi ketika dibutuhkan Contoh hambatan: "denial of service attack" (DoS attack), dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai down, hang, crash.
   b. mailbomb, dimana seorang pemakai dikirimi e-mail bertubi-tubi (katakan b ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka surat elektroniknya atau kesulitan mengakses surat elektoniknya.
5. Access Control
   a. Definisi : cara pengaturan akses kepada informasi. Berhubungan dengan masalah authentication dan juga privacy
   b. Metode : menggunakan kombinasi user id dan password atau dengan menggunakan mekanisme lain.
6. Non-repudiation

   Definisi : Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Dukungan bagi electronic commerce penanggulangan kejahatan di dunia maya memberikan persyaratan terhadap komputer yang berbeda dari kebanyakan persyaratan sistem karena sering kali berbentuk pembatasan terhadap apa yang tidak boleh dilakukan komputer. Ini membuat penanggulangan menjadi lebih menantang karena sudah cukup sulit untuk membuat program komputer melakukan segala apa yang sudah dirancang untuk dilakukan dengan benar. Persyaratan negatif juga sukar untuk dipenuhi dan membutuhkan pengujian mendalam untuk verifikasinya, yang tidak praktis bagi kebanyakan program komputer. Penanggulangan kejahatan di dunia maya memberikan strategi teknis untuk mengubah persyaratan negatif menjadi aturan positif yang dapat ditegakkan. Pendekatan yang umum dilakukan untuk penanggulangan kejahatan dunia maya antara lain adalah dengan membatasi akses fisik terhadap komputer, menerapkan mekanisme pada perangkat keras dan sistem operasi untuk penanggulangan kejahatan, serta membuat strategi pemrograman untuk menghasilkan program komputer yang dapat diandalkan.

3.2. Metode Menghadapi Ancaman

Menghadapi ancaman (managing threats) terhadap sistem keamanan komputer dapat digunakan suatu model yaitu Risk Management Model. Manajemen ini membagi 3 (tiga) komponen yang dapat memberikan kontribusi terhadap risk, yaitu :

1. Aset (assets), yaitu pemilik sistem informasi harus mendiskripsikan segala kekayaan pada sistem dan memperhitungkan segala resiko yang akan timbul dari kegagalan terhadap salah satu komponen tersebut, seperti :
   a. Hardware
   b. Software
   c. Dokumentasi
   d. Data

DOI: 10.52362/jisamar.v7i3.1132

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.3 (Agustus 2023)

e. Komunikasi
f. Lingkungan
g. Manusia

2. Ancaman (Threats), yaitu mendeskripsikan semua ancaman yang akan terjadi terhadap sistem, seperti :
   a. Pemakai (user)
   b. Teroris
   c. Kecelakaan (accident)
   d. Crackers
   e. Penjahat kriminal
   f. Mata-mata
3. Kelemahan (Vulneralbilities), yaitu mendeskripsikan semua kelemahan yang ada pada system, seperti :
   a. Software bugs
   b. Hardware bugs
   c. Radiasi (layar monitor, transmisi)
   d. Cetakkan, hard copy, atau print out
   e. Keteledoran (oversight)
   f. Cracker

3.3. Metode Mengamankan File

Dari banyaknya resiko yang akan dihadapi oleh suatu sistem informasi, semuanya itu merupakan hal yang sangat penting dan tidak dapat dianggap remeh. Salah satunya terhadap file data, yang merupakan suatu aset yang banyak digunakan dan selalu ada dalam suatu sistem informasi.

Metode untuk mengamankan file dapat dilakukan dengan 3 (tiga) cara, yaitu :

1. Attribut Keying, yaitu suatu penguncian terhadap attribut sebuah file data Setiap file data dalam sistem informasi (komputer) selalu dikuti oleh attribut file, yang berfungsi untuk mengamankan file agar tidak dapat diserang oleh orang lain. Attribut itu terdiri atas :
   a. R (read), yaitu penguncian atribut sehingga pemakai hanya dapat melakukan pembacaan saja terhadap terhadap isi file.
   b. W (write), yaitu penguncian attribut sehingga pemakai dapat melakukan penulisan (simpan) terhadap isi file.
   c. X atau A (access), yaitu penguncian atrribut sehingga pemakai dapat melakukan pengaksesan (eksekusi) file.

   Perintah penguncian ini dapat dilakukan dengan menggunakan perintah eksternal dari Sistem Operasi (Operating System) seperti :
   a. CLI (Command Line Interface) dalam Disk Operating System (DOS) dengan menggunkan perintah ATTRIB.
   b. GUI (Grafics User Interface) dalam sistem operasi Windows.
2. Compress Keying, yaitu suatu penguncian terhadap hasil pemadatan file data Setiap file data dapat dirobah kedalam bentuk yang lebih padat dengan menggunakan aplikasi kompres, seperti RAR, ZIP dan lain-lain. Hasil dari kompres dapat di kunci dengan menambahkan password (kata kunci) pembuka apabila fle tersebut di decompress atau dikembalikan kedalam bentuk semula (extract). Prinsip kerja dari kompres adalah mencari character atau byte yang sering atau banyak berada dalam sebuah file data Karakter tersebut akan dirobah kedalam kumpulan bit yang lebih sedikit (kurang dari 8 bit)

DOI: 10.52362/jisamar.v7i3.1132

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.3 (Agustus 2023)

3. Encription (Enkripsi), yaitu merupakan suatu teknik merubah isi file data dengan bentuk rahasia yang tidak dimengerti oleh orang lain Jenis-jenis proteksi data enkripsi terdiri atas :
   a. Teknik Substitusi (Substitution Technique), yaitu teknik yang melakukan proteksi data dengan cara menggantikan setiap elemen data atau karakter dengan karakter lain.
   b. Teknik Blok (Blocking Technique), yaitu teknik proteksi data dengan cara mengelompokan beberapa karakter ke dalam blok-blok yang berisi beberapa karakter.
   c. Teknik Permutasi (Permutation Technique), yaitu teknik proteksi data dengan cara menukarkan letak karakter-karakter yang ada.
   d. Teknik Ekspansi (Expansion Technique), yaitu teknik proteksi data dengan cara menambahkan suatu karakter kedalam data.
   e. Teknik Pemadatan (Compaction Technique), yaitu teknik proteksi data dengan cara menghilangkan sejumlah karakter dalam data.

3.4. Pentingnya dan Manfaat Cyber Security bagi Perusahaan

Cyber security untuk perusahaan sebetulnya bertujuan sederhana, yaitu melindungi perangkat berbasis komputer beserta data milik perusahaan di dalamnya dari pengaksesan yang tidak berizin (unauthorized) dan tidak diharapkan, perubahan data secara illegal, maupun potensi kerusakan lainnya.

Pasalnya, laporan dari Cyber security Venture bekerja sama dengan Herjavec Group dalam 2017 Cyber crime Report menunjukkan bahwa dari hari ke hari jenis kerusakan yang diakibatkan oleh serangan cyber ini semakin meningkat. Pihak-pihak yang disasar pun tidak pandang bulu. Apalagi jumlah perusahaan yang berpindah ke aktivitas online semakin banyak, termasuk yang bergerak di bidang periklanan, penjualan, pencarian pangsa pasar baru, kontak pelanggan, perekrutan pegawai, hingga transaksi finansial. Melihat pentingnya jenis – jenis usaha yang bersinggungan langsung dengan teknologi tersebut, tentu saja perusahaan tidak mengharapkan akan adanya upaya untuk menyabotase data maupun transaksi perusahaan yang ada.

Lalu, apa saja hal yang rentan terkena serangan cyber? Ketika berkaitan dengan sistem jaringan, hampir semua aspek bisa diserang: transaksi, piranti keras, layanan berbasis TI, data pelanggan, serta informasi sensitif lainnya.

Selain itu, serangan cyber juga bisa mewujud beberapa hal, antara lain: pencurian maupun pengambilalihan akses secara illegal atas komputer, laptop, tablet, maupun perangkat seluler yang dimiliki oleh perusahaan; serangan ke sistem TI dan website dari jarak jauh; hingga pencurian informasi perusahaan yang kebetulan dititipkan ke sistem pihak ketiga semisal di layanan cloud.

Dari beragam potensi ancaman yang ada, nyatanya masih banyak perusahaan yang awam dengan dampak kerugian yang bisa terjadi. Beda halnya dengan serangan ataupun pencurian pada umumnya, kerugian serangan cyber justru bisa lebih besar karena bisa menyasar ke banyak titik secara bersamaan.

Apabila itu terjadi, perusahaan bisa mengalami kerugian finansial (kehilangan dana yang tersimpan), peningkatan biaya untuk pemulihan dan penggantian komponen perangkat yang diserang, hancurnya reputasi perusahaan, hingga kerusakan berantai karena sistemnya terhubung ke banyak perusahaan lain.

Manfaat dari cyber security yaitu untuk menjaga dan mencegah penyalahgunaan akses maupun pemanfaatan data dalam sistem Teknologi Informasi dari seseorang yang tidak memiliki hak untuk mengakses maupun memanfaatkan data dalam sistem tersebut.

Selain itu, dengan adanya cyber security, reputasi dari perusahaan tetap terjaga, khususnya yang berhubungan dengan pihak pengguna jasa perusahaan tersebut.

DOI: 10.52362/jisamar.v7i3.1132

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.3 (Agustus 2023)

3.5. Tantangan Cyber Security di Revolusi Industri 4.0

Ada beberapa tantangan besar yang dapat menjadi sandungan bagi dunia industri di tahun mendatang, yaitu ancaman – ancaman terkini yang dapat menyebabkan kerusakan dan kerugian besar bagi banyak perusahaan.

Berikut adalah tantangan utama yang akan dihadapi oleh perusahaan saat masa peralihan industri yang mendorong efektifitas dan efisiensi:

1. Targetted Attack

   Menurut studi yang dilakukan oleh Enterprise Enviromental Factor (EEF), 48 persen produsen di beberapa titik telah mengalami insiden keamanan, dan setengah dari organisasi tersebut menderita kerugian finansial atau gangguan terhadap bisnis mereka. Menurut survei, industri manufaktur adalah yang paling ditargetkan untuk serangan cyber, tepat berada di belakang sektor publik dan bisnis keuangan.

   Industrial Control System (ICS) atau Supervisory Control And Data Acquisition (SCADA) adalah perangkat lunak yang paling sering digunakan dalam industri manufaktur, infrastruktur dan berbagai bidang lain, merupakan titik terlemah dalam sistem keamanan perusahaan.

   Contoh kasusnya adalah Grey Energy (2018), yang dirancang untuk sasaran lebih luas. PICS/SCADA digunakan bukan hanya di manufaktur, tetapi juga pada pembangkit listrik, perusahaan transmisi, pengolahan minyak dan gas, pabrik – pabrik, bandara sampai layanan pengiriman.

2. Ransomware

   Menurut laporan Verizon 2018 mengatakan bahwa 56 persen insiden malware melibatkan ransomware sehingga menjadikannya sebagai bentuk malware yang paling umum. Sayangnya, peretas mengalihkan perhatian mereka ke sistem penting seperti server daripada perangkat karyawan.

   Dalam praktiknya, ransomware oleh pengembangnya dikolaborasikan dengan botnet bahkan Crypto Jacking untuk mendapatkan keuntungan ganda. Menghadapi ransomware memang bukan perkara mudah, bagi sebuah perusahaan memiliki alat proteksi dari ransomware bukan suatu hal yang bisa ditawar – tawar karena ransomware tidak pernah pilih – pilih ketika menyerang korbannya.

3. Orang dalam/Insider

   Akar masalah dari kerentanan 52 persen berasal dari kesalahan karyawan yang dilakukan secara tidak sengaja, seperti salah copy file, salah kirim file, meninggalkan komputer dalam keadaan terbuka saat tidak dipakai, dan lain-lain. Sementara, Ponemon Institute dalam studinya di tahun ini mengatakan bahwa 1 dari 4 kebocoran data disebabkan oleh orang dalam yang dilakukan dengan sengaja dengan motivasi finansial, spionase dan persaingan bisnis.

3.6. Tenaga kerja yang dibutuhkan untuk Cyber Security

1. **Analis Keamanan**, bertugas untuk memetakan potensi ancaman keamanan, lalu memberikan rekomendasi untuk mitigasi terhadap potensi ancaman tersebut.
2. **Spesialis Forensik**, sesuai namanya, spesialis forensik ini bertugas untuk melakukan penyelidikan pasca insiden kebocoran keamanan. Seorang spesialis forensik harus memiliki kemampuan teknis yang mumpuni untuk bisa mencari dan memetakan jejak-jejak yang ditinggalkan oleh pelaku, untuk bisa melacak dan menemukan pelaku.
3. **Hacker/Peretas**, istilah hacker selama ini telah mengalami distorsi makna, dimana seolah – olah tindakan hacking adalah sebuah tindakan kriminal padahal tidak sepenuhnya seperti itu. Hacker sendiri adalah istilah yang diberikan kepada orang – orang yang

DOI: 10.52362/jisamar.v7i3.1132

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.3 (Agustus 2023)

memiliki kemampuan untuk melakukan tindakan eksploitasi terhadap sistem telematika melalui berbagai cara.

4. **Consultan Security**, consultan *security* bertugas memberikan solusi keamanan yang dihadapi oleh perusahaan. Tanggung jawabnya cukup luas. Mulai dari menemukan cara paling efektif dalam melindungi jaringan, perangkat lunak, hingga melakukan pengujian dan analisis risiko. Hal tersebut bisa dinegosiasikan dalam kontrak kerja.
5. **Chief Information Security Officer**, sesuai dengan namanya, *chief information security officer* (CISO) merupakan pimpinan yang mengatur sektor keamanan TI sebuah perusahaan.
6. **Security Engineer**, *security engineer* merupakan karyawan tingkat menengah yang bertugas membangun dan memelihara sistem keamanan perusahaan. Terkadang, mereka harus memasang *firewall*, menguji keamanan, mengembangkan skrip automasi untuk melacak insiden atau pun menguji keamanan.
7. ***Security Architect***, *security architect* adalah karyawan senior yang bertugas mengimplementasikan dan mengawasi keamanan jaringan komputer perusahaan. Mereka harus mendesain, meriset, arsitektur keamanan yang kuat.
8. ***Incident Responder***, kalau ada insiden keamanan, seorang *incident responder* merupakan sosok yang pertama kali harus bertindak. Selain itu, mereka juga bertugas dalam edukasi serta pencegahan terjadinya insiden.
9. **Penetration Tester**, istilah lainnya adalah *hacker*, tapi dalam makna yang positif. Bertugas untuk mencari celah keamanan dalam sistem perusahaan dan melakukan analisis secara mendalam.
10. **Developer Sofware Security**, sesuai dengan namanya, mereka bertugas untuk mengembangkan *software* keamanan dan mengintegrasikannya ke dalam sistem perusahaan. Mereka juga punya tanggung jawab memberikan dukungan serta pengujian perangkat lunak yang diciptakan.
11. **Auditor Security**, auditor *security* harus memiliki kemampuan memeriksa efektivitas sebuah sistem keamanan. Di samping itu, mereka juga harus mampu memberikan solusi peningkatan sistem.

.

IV. KESIMPULAN

Cyber security adalah segala bentuk sistem keamanan di dalam dunia maya yang berhubungan dengan segala macam bentuk kegiatan menggunakan internet dan sebagai system keamanan informasi atau data. Penegakan hukum perlu diterapkan guna melindungi pengguna internet serta Kerjasama internasional untuk menanggulangi serta menyelidiki dan menuntut segala kejahatan siber dunia maya yang merugikan pengguna internet. Cyber security sangat berguna untuk banyak orang, karena data – data yang penting dan rahasia dapat di jaga kerahasiaan data tersebut. Berbagai upaya telah dilakukan pemerintah salah satunya dengan cyber security ini untuk menanggulangi terjadinya pencurian data oleh cyber crime dan pemerintah juga bahkan membuat undang-undang tentang tindak pidana cyber crime.

REFERENASI

[1] Brij B. Gupta, Gregorio Martinez Perez, Dharma P. Agrawal (2019), *Handbook of Computer Networks and Cyber Security*, Springer, Switzerland.
[2] Dimas Bhoby Handoko, Cyber Security. Diakses pada 23 Juni 2023 dari https://www.scribd.com/doc/304856546/Cyber-Security#

DOI: 10.52362/jisamar.v7i3.1132

[3] Fujiama Diapoldo Silalahi (2022), *KEAMANAN CYBER (CYBER SECURITY)*, Semarang, Penerbit Yayasan Prima Agus Teknik&Universitas STEKOM
[4] Gamatechnoblog, Pahami Pentingnya Cyber Security Bagi Perusahaan. Diakses pada 23 Juni 2023 dari https://blog.gamatechno.com/pahami-pentingnya-cyber-security-bagi-perusahaan/
[5] Hanafi, (2022), *Dasar Cyber Security dan Forensic*, Penerbit Buku Pendidikan Deepublish. Yogyakarta.
[6] Herman Suryokumono, Hikmatul Ula, (2020) Kopersi Indonesia dalam Era MEA dan Ekonomi Digital, Penerbit UB Press, Malang.
[7] Iwan Sofana, Rifkie Primartha (2019), *Network security dan cyber security*, Penerbit Informatika Bandung, Bandung.
[8] Phintraco, Pentingnya Cyber Security. Dia kses pada 23 Juni 2023 dari http://www.phintraco.com/pentingnya-cyber-security/
[9] Reno Hamdani, Cyber Security For Electronic Devices. Diakses pada 23 Juni 2023 dari http://fabyandreno28.blogspot.com/2013/12/makalah-cyber-security.html?m=1
[10] Suryana, Yoga Perdana, (2019), Bisnis Digital, Cara Mudah Bisnis di Era Industri 4.0, Penerbit Salemba Empat, Jakarta
[11] Iwan Sofana, Rifkie Primartha (2019), *Network Security Dan Cyber Security*, Informatika, Bandung.

DOI: 10.52362/jisamar.v7i3.1132