JURNAL RISET SISTEM INFORMASI
Halaman Jurnal: https://journal.smartpublisher.id/index.php/jissi
Halaman UTAMA Jurnal : https://journal.smartpublisher.id

OPEN ACCESS

DOI: https://doi.org/10.69714/g2pay047

FORENSIK JARINGAN UNTUK INVESTIGASI KEJAHATAN CYBER PADA STUDI KASUS PEMBOBOLAN DATA KOMINFO OLEH BJORKA

Aspiani Putri Ashilah[a*], Rakhmadi Rahman[b]
[a] Sistem Informasi , aspianiputriaa@gmail.com, Institut Teknologi Bacharuddin Jusuf Habibie, Parepare Sulawesi Selatan
[b] Information System Department, rakhmadi.rahman@ith.ac.id, Institut Teknologi Bacharuddin Jusuf Habibie, Parepare Sulawesi Selatan
[*] Korespondensi

ABSTRACT

The study is to investigate the phenomenon of cybercrime, specifically focusing on the Bjorka data breach at Kominfo. Cybercrime has grown to be a serious threat to Indonesia's cyber security, including data theft, hacking, and malware attacks. This study approach employs qualitative descriptive techniques via a methodical examination of documents, including journal articles from both domestic and foreign publications. Based on analysis, it was found that Bjorka committed data breaches to protest government policies and highlight security weaknesses. The study also explores measures to prevent cybercrime, such as the use of security technology, user training, and the implementation of strict security policies. Encryption tools like Veracrypt should be used to protect sensitive data from theft. The research results are expected to raise awareness and collaborative efforts among governments, associated organizations, and communities to address the threat of cybercrime as well as strengthen national cyber defences

Keywords: Cyber crime,Cyber security, Cyber attack prevention, Bjorka

Abstrak

Penelitian ini bertujuan untuk mengeksplorasi fenomena cybercrime, khususnya kasus pembobolan data Kominfo yang dilakukan Bjorka. Kejahatan siber, termasuk pencurian data, peretasan, dan serangan malware, telah menjadi ancaman signifikan terhadap keamanan siber di Indonesia. Tekhnik penelitiannya memakai cara deskriptif kualitatif melalui analisis dokumen secara sistematis, termasuk artikel dari jurnal dalam negeri dan internasional. Berdasarkan analisis, ditemukan bahwa Bjorka melakukan pelanggaran data untuk memprotes kebijakan pemerintah dan menyoroti kelemahan sistem keamanan. Studi ini juga mengeksplorasi langkah-langkah pencegahan kejahatan dunia maya, seperti penggunaan teknologi keamanan, pelatihan pengguna, dan penerapan kebijakan keamanan yang ketat. Alat enkripsi seperti Veracrypt harus digunakan untuk melindungi data sensitif dari pencurian. Hasil penelitian ini diharapkan dapat meningkatkan kesadaran dan upaya kolaboratif antara pemerintah, organisasi terkait, dan komunitas untuk mengatasi ancaman kejahatan siber serta memperkuat pertahanan siber nasional.

Kata Kunci: kejahatan cyber ,keamanan cyber , Pencegahan serangan Cyber , Bjorka

1. PENDAHULUAN

Teknologi berdampak pada banyak aspek kehidupan di seluruh dunia, dan penemuan-penemuan baru yang dihasilkan oleh kemajuan teknis ini akan membuat hidup lebih mudah bagi masyarakat, klaim M. Zaki Rizaldi (2023). Dunia maya, atau sekadar "ruang siber", adalah media elektronik yang merupakan bagian dari jaringan komputer global dan sering digunakan untuk komunikasi satu arah dan timbal balik berbasis telepon atau internet.[1].

Received Juni 2, 2024; Revised Juni 9, 2024; Accepted Juli 2, 2024; Published Juli 10, 2024

Saat ini mayoritas masyarakat Indonesia merupakan pengguna atau pernah terjun ke dunia maya. Pasalnya, teknologi digital yang selalu berkembang memberikan manfaat bagi masyarakat. Karena masyarakat semakin bergantung pada teknologi, segala sesuatu pasti akan terancam.

Salah satunya adalah cybercrime, menurut Fulan Yustinne Nadhotul Sufi (2023) yang didefinisikan sebagai serangkaian kegiatan kriminal yang menggunakan teknologi komputer, jaringan internet, dan sistem informasi. Dua dari lima ancaman utama yang mengancam umat manusia adalah bencana alam dan perubahan iklim; serangan siber adalah salah satunya, karena penjahat siber memiliki jaringan global, yang memungkinkan mereka melakukan serangan mereka di mana pun dan kapan pun. Berbagai jenis kejahatan ini termasuk pencurian data (skimming), peretasan (hacking), dan software berbahaya (malware)[2].

Sebuah survei yang dilakukan oleh badan siber Indonesia memperkirakan bahwa 403.990.813 lalu lintas anomali akan dihasilkan di Indonesia pada tahun 2023. Generic Trojan RAT, atau aktivitas komunikasi pintu belakang terhadap domain berbahaya yang diyakini digunakan oleh pelaku ancaman sebagai server komando dan kontrol, adalah yang paling umum. jenis lalu lintas anomali. Tercatat 1,011,209 ransomware dan 4,001,905 operasi APT. Anomali lalu lintas merupakan komunikasi yang paling sering disampaikan BSSN kepada pemangku kepentingan dari 1.762 peringatan indikator kejadian. Industri masuk dalam Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelestarian Infrastruktur Informasi Vital (IIV). Dugaan insiden siber juga diperiksa oleh BSSN berdasarkan temuan pemantauan dan analisis Cyber Threat Intelligence. Pelanggaran data merupakan jenis peristiwa siber yang paling sering terjadi, dengan 347 kasus yang dilaporkan. Hasil pencarian Darknet mengungkap 1.674.185 temuan data paparan.[3].

Oleh karna itu penulis ingin lebih mendalami salah satu kasus cyber crime yaitu kasus pembobolan data kominfo oleh bjorka. Penulis ingin mengetahui motif dan tujuan pelaku serta penulis ingin memberikan cara pencegahan kasus cyber crime agar tidak terjadi pada kita.

2. TINJAUAN PUSTAKA

2.1. Cyber crime

Cybercrime adalah jenis kejahatan yang terjadi dalam dunia digital, di mana pelaku melakukan aktivitas ilegal dengan menggunakan teknologi komputer dan internet. Pencurian data pribadi atau keuangan, penipuan online, serangan terhadap infrastruktur digital, atau penyebaran malware yang merusak mungkin termasuk dalam kategori ini. Pelaku memiliki banyak alasan, termasuk mencari keuntungan moneter dan alasan ideologis atau politik. Pelaku kejahatan cyber sering mengeksploitasi kerentanan sistem komputer dan jaringan, yang dapat berasal dari kesalahan konfigurasi hingga eksploitasi kelemahan perangkat lunak. Meskipun masalah global dan lintas batas.

2.2. Pembobolan data

Pihak yang tidak berhak mendapatkan, memperoleh, atau mengelola informasi atau data sensitif secara tidak sah. Ini dikenal sebagai "pembobohan data". Serangan peretasan (hacking), kehilangan perangkat fisik yang berisi data sensitif, atau tindakan tidak sengaja seperti kesalahan dalam mengelola atau mengamankan data adalah beberapa alasan pembohan data. Pembohan data dapat memiliki konsekuensi yang sangat berbahaya, seperti pencurian identitas, kehilangan uang, kehilangan kepercayaan pelanggan atau mitra bisnis, dan kemungkinan melanggar peraturan privasi data. Organisasi harus menerapkan praktik keamanan data yang ketat untuk mencegah pembohan data, seperti mengenkripsi informasi sensitif, menggunakan firewall dan sistem deteksi intrusi, dan mendidik karyawan tentang ancaman keamanan digital.

3. METODOLOGI PENELITIAN

Teknik deskriptif kualitatif fipakai pada penelitiannya guna menganalisa literatur secara menyeluruh. Maksud pada penelitiannya yakni guna meraih pemahamannya menyeluruh mengenai fenomena yang diteliti. Peneliti akan dapat mengumpulkan dan menganalisis berbagai jurnal nasional dan internasional tentang sosial engineering, seperti kasus penipuan investasi kripto dengan sistem biometrik. Untuk melakukan review, aplikasi Publish or Perish digunakan untuk menggunakan database literatur Google Scholar. Artikel penelitian menggunakan periode 2019–2024.

4. HASIL DAN PEMBAHASAN

4.1 Pembahasan cyber crime

Kejahatan dunia maya adalah penggunaan komputer atau perangkat elektronik lainnya secara kriminal untuk tujuan terlarang di dunia maya. Teknologi pendukung telepon seluler, telepon pintar, dan perangkat lain yang dapat beroperasi melalui jaringan elektronik internasional termasuk dalam kategori ini. Jaringan

komputer yang tidak diizinkan menjadi sasaran upaya akses kejahatan dunia maya. Kejahatan dunia maya dianggap melanggar hukum. Kemampuan serbaguna yang ditunjukkan oleh kemajuan teknologi informasi dan komunikasi membedakannya dari tindak pidana serupa.[4].

4.1.1. Jenis-jenis cyber crime

a. Peretasan
   Salah satu jenis pelanggaran adalah peretasan. Ini adalah penggunaan atau akses ilegal ke komputer atau sumber daya jaringan yang mengeksploitasi kerentanan keamanan yang ditemukan dalam jaringan. Peretasan dapat digunakan untuk mengumpulkan data atau informasi pribadi untuk penjahat merusak situs web atau digunakan sebagai bagian dari penolakan layanan (DoS) atau serangan DDoS (lihat di bawah). Denial of service ataupun serangannya denial of service terdistribusikan DoS dan DDoS terkait dengan membanjiri server internet dengan begitu banyak permintaan (seperti tautan yang telah diklik) sehingga mereka tidak dapat menangani serangan DoS atau DDoS. Ini dapat membebani server, membuatnya lambat atau tidak berfungsi.Impersonating(meniru)

   Untuk melakukan tindakan, penyerang menggunakan identitas palsu. Penyerang berusaha mendapatkan akses fisik ke lokasi yang aman dengan melakukan peniruan untuk mendapatkan izin dari orang yang memiliki akses yang sah. Serangan ini sebagian besar berfokus pada menciptakan situasi yang masuk akal untuk dilakukan kepada individu yang terpilih. Untuk menghindari kecurigaan, metode ini membutuhkan kisah yang dapat dipercaya. Oleh karena itu, sangat penting untuk melakukan penelitian pada target tersebut terlebih dahulu.

b. Cyber attack
   Serangan siber, juga dikenal sebagai perang siber, adalah suatu bentuk aktivitas jahat yang dilakukan oleh suatu negara, masyarakat, kelompok, atau organisasi untuk menargetkan jaringan, infrastruktur, sistem informasi komputer, atau komputer individu dengan berbagai cara. Biasanya, target yang ditemukan melalui pelanggaran sistem yang lemah dicuri, dimodifikasi, atau dihancurkan oleh sumber anonim yang menjalankan operasi ini. Dalam berbagai situasi, hal ini dapat disebut sebagai kampanye internet, perang internet, atau terorisme dunia maya. Serangan dunia maya mencakup, misalnya, pemasangan spyware pada komputer dalam upaya membahayakan infrastruktur nasional. Worm Stuxnet baru-baru ini menjadi bukti sifat serangan siber yang mematikan dan canggih. Serangan ini dihentikan dengan penggunaan Informasi Keamanan dan Manajemen Peristiwa (SIEM) dan analisis perilaku pengguna. Para ahli hukum berupaya membatasi kata-kata tersebut pada situasi yang dapat mengakibatkan cedera tubuh. Mereka membedakannya dari serangan siber yang lebih luas dan pelanggaran data biasa

c. Pencurian data
   Ini yakni istilahnya yang dipakai guna mengilustrasikan keadaan dimana data disalin ataupun diambil secara ilegal dari perusahaan atau orang lain. Biasanya, kategori ini mencakup informasi pengguna seperti nomor jaminan sosial, kata sandi, informasi kartu kredit, informasi pribadi lainnya, atau rahasia bisnis lainnya. Orang yang mencuri informasi ini mungkin menghadapi tuntutan hukum yang berat karena diperoleh secara ilegal.

d. Sabotase jaringan
   Manajer yang tidak kompeten atau "sabotase jaringan" mencoba melakukan pekerjaan orang yang biasanya mereka tangani? Bisa saja di atas, atau kombinasi dari keduanya. Namun, jika Verizon menggunakan bantuan anak-anak untuk menghalangi jalur respons pertama, masalah jaringan mungkin menjadi alasan bagi pemerintah federal untuk campur tangan demi keselamatan publik. Apa tujuan pemogokan dan serikat pekerja jika pemerintah federal memaksa orang-orang ini kembali bekerja?[3] Aktivitas kejahatan cyber yang menargetkan komputer dapat menggunakan malware untuk menginfeksi perangkat. Selain itu, malware dapat digunakan untuk menghapus, mencuri informasi, atau bahkan menghentikan pengguna untuk mengakses website. Berikut ini adalah penjelasan tentang konsekuensi Cyber Crime

4.1.2. Dampak cyber crime

Kurangnya pengawasan terhadap penggunaan internet menyebabkan kejahatan dunia maya. Kejahatan ini menggunakan akses internet, yang berarti mereka tidak terjadi hanya di satu daerah. Keberhasilan polisi dalam memerangi kasus kejahatan dunia maya dipengaruhi oleh keterbatasan tenaga ahli dalam melakukan

penyelidikan; jumlah anggota ahli yang sangat kecil menjadi hambatan untuk memerangi kasus kejahatan dunia maya dengan cepat, memungkinkan para pelaku memanfaatkannya dengan lebih mudah. Individu.

Kerugian yang disebabkan oleh kejahatan dunia maya dapat beragam. Pertama-tama, korban dapat berupa pengguna (individu atau kelompok) atau sistem komputer. Kedua, korban dapat dipengaruhi dengan cara yang sangat berbeda, mulai dari kerugian kecil hingga kerugian besar, dan bahkan efek yang halus dan tidak berwujud pada individu dapat terjadi, seperti menanamkan ketakutan dunia maya. Strategi global telah digunakan untuk menangani kejahatan dunia maya yang meningkat. Negara-negara ini membuat komitmen internasional untuk mewaspadai kejahatan dunia maya, mengusulkan undang-undang untuk memerangi kejahatan dunia maya, membangun kolaborasi internasional guna memeranginya kriminal dunia maya, dan menerapkan strategi non-alasan untuk memerangi kejahatan dunia maya. dunia maya. Perserikatan Bangsa-Bangsa telah mencapai beberapa perjanjian yang berkaitan dengan kejahatan di internet.Menurut kriminologi, duplikasi KTP konvensional melalui penipuan identitas dapat membuka jalan bagi seseorang untuk melakukan kejahatan berulang. Adanya identitas ganda pasti menjadi masalah yang dapat mengganggu masyarakat karena berpotensi melahirkan anak berulang. kriminal atau residivis.

Salah satu kejahatan dunia maya yang terjadi, menurut Neill Barrett, adalah pornografi dunia maya (khususnya anak pornografi) dan seks siber, yang mencakup penyimpanan, akses, atau penyebaran konten pornografi di media internet.Ini juga menjadi perhatian global. Ini terbukti pada Konferensinya Internasional mengenai "Memberantas Pornografi Anak diInternet" serta Kongresnya Dunia Pertama Melawan Eksploitasi Seks Komersial Anak di Stockholm, 27–31 Agustus 1996. Teori imitasi mengatakan bahwa media dapat membuat penonton meniru apa yang mereka lihat. Akibatnya, anak-anak dan remaja yang tak bisa memperbedakan mana yang betul serta salah hendak lebih cenderung meniru dan mencoba hal-hal baru yang mereka lihat. Akibatnya, terjadi penyimpangan seksual, seperti masturbasi tanpa tempat penyaluran, atau bahkan dapat terjadi sebelum pernikahan dan hamil di luar nikah. Cyberporn juga dapat mengganggu pertumbuhan pribadi seseorang, seperti berkhayal atau berkhayal, menjadi malas bekerja, atau kehilangan arah masa depan

4.2 Pembahasan kasus pembobolan data oleh bjorka

Bjorka adalah peretas anonim yang terkenal karena membobol dan membocorkan data dari banyak lembaga di Indonesia. Meskipun identitas asli Bjorka masih belum diketahui, tindakan yang dilakukan olehnya telah berdampak besar pada keamanan siber dan perlindungan data pribadi.

4.2.1. Alasan bjorka melakukan pembobolan data

a. Protes Terhadap Kebijakan Pemerintah: Bjorka mungkin memprotes terhadap kebijakan pemerintah Indonesia, seperti kebijakan privasi dan keamanan data. Pembobolan data Kominfo adalah bentuk protes terhadap kebijakan yang dianggap tidak memadai untuk melindungi data pribadi warga negara.
b. Menunjukkan Kelemahan Sistem Keamanan: Bjorka mungkin ingin menunjukkan kekurangan sistem keamanan siber yang ada di lembaga pemerintah Indonesia melalui pembobolan ini. Ini dapat merupakan upaya untuk meminta perbaikan pada sistem dan protokol keamanan data.
c. Mencari Ketertarikan Publik dan Media: Aksi pembobolan data Bjorka menarik perhatian publik dan media. Ini dapat membantunya meningkatkan profil dirinya dan mendapatkan pengakuan di komunitas hacker global.
d. Motivasi Keuangan: Pembobolan data mungkin juga dilakukan dengan alasan keuangan, seperti meminta tebusan atau menjual data yang dicuri di pasar gelap. Namun, ini mungkin tidak selalu menjadi alasan utama.
e. Aktivisme Digital: Bjorka dapat menyebut dirinya sebagai hacktivist atau aktivis digital yang menggunakan kemampuan peretasannya untuk memperjuangkan hal-hal seperti hak privasi, kebebasan informasi, dan transparansi.

4.3 Pencegahan cyber crime

Upaya terus-menerus untuk menghentikan kejahatan siber mencakup perlindungan data dan sistem dari serangan siber melalui penggunaan teknologi keamanan seperti antivirus, firewall, dan solusi deteksi intrusi, serta penerapan kebijakan keamanan yang ketat dan pembaruan perangkat lunak yang rutin. Selain itu, sangat penting bagi pengguna untuk dilatih tentang prakterk keamanannya yang baik, misalkan memakai password yang kokoh serta menghindarinya serangan phishing. Untuk mencegah ancaman siber, juga diperlukan pemantauan aktif aktivitas jaringan, enkripsi data, dan penyimpanan cadangan yang teratur. Menggabungkan langkah-langkah ini akan memungkinkan organisasi untuk melindungi aset digital mereka dari serangan siber.

a. Pencegahan sosial engginering pada kasus pembobolan data oleh bjorka

Kasus pembobolan data Kominfo Bjorka menunjukkan betapa pentingnya meningkatkan upaya mencegah kejahatan cyber. Pertama dan terpenting, peningkatan keamanan sistem harus menjadi prioritas utama, dengan melakukan audit menyeluruh untuk menemukan dan memperbaiki kerentanan yang mungkin. Ini termasuk penggunaan enkripsi data untuk melindungi data sensitif dan kontrol akses yang ketat guna menunjukkan bahwasanya Cuma individu yang berkuasa yang dapat mengaksesnya. Selain itu, kesadaran pengguna dan pelatihan sangat penting untuk mencegah serangan siber. Karyawan Kominfo harus dilatih untuk mengidentifikasi indikasi serangan phishing, menghindari tautan atau lampiran yang mencurigakan dalam email, dan memastikan bahwa data login mereka tetap rahasia.

Selain itu, pemantauan aktif aktivitas jaringan sangat penting untuk mendeteksi dan merespons serangan siber dengan cepat. Aktivitas mencurigakan dapat diidentifikasi dan ditindaklanjuti dengan menggunakan alat pemantauan jaringan yang canggih. Selain itu, pembaruan perangkat lunak harus dilakukan secara teratur untuk memperbaiki kerentanan dan menjaga system atas serangannya yang memanfaatkannya.

Namun, kebijakan keamanan yang ketat harus diterapkan untuk memastikan bahwa semua karyawan memahami dan mematuhi kebijakan keamanan. Terakhir, untuk memastikan bahwa organisasi dapat mengatasi serangan siber dengan cepat dan efektif, sangat penting untuk memiliki rencana pemulihan bencana yang menyeluruh, yang mencakup pencadangan data rutin dan penyimpanan salinan cadangan di tempat yang aman. Dengan melakukan tindakan ini, Kominfo dapat meningkatkan keamanan data mereka dan mengurangi kemungkinan terkena serangan siber dimasa depan..

b. Aplikasi yang dapat digunakan untuk mencegah sosial engginering

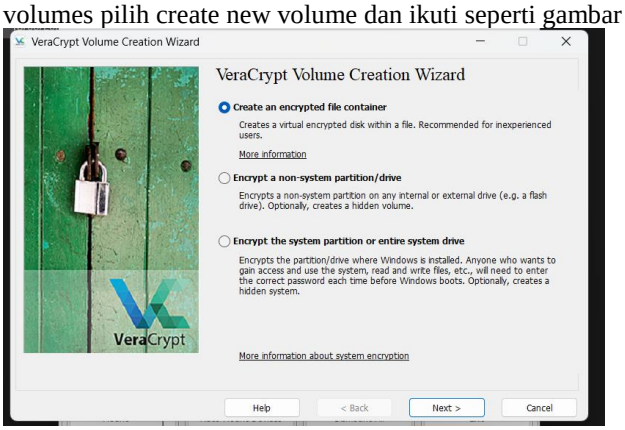
Veracrypt yakni perangkat lunak bersumber terbukanya yang dipakai guna mengenkripsi data pada disk, file, atau drive. Dikembangkan untuk menggantikan TrueCrypt yang dihentikan, Veracrypt bertujuan untuk menyediakan enkripsi yang kuat dan keamanan data yang tinggi kepada pengguna. Program ini tersedia untuk berbagai platform termasuk Windows, macOS dan Linux. Veracrypt memungkinkan pengguna membuat volume terenkripsi untuk file, mengenkripsi seluruh disk atau partisi, atau membuat volume terenkripsi yang terlihat seperti disk virtual. Enkripsi yang disediakan oleh Veracrypt adalah salah satu yang terkuat yang tersedia untuk umum dan telah diuji secara ekstensif oleh komunitas keamanan. Selain itu, Veracrypt menawarkan fitur seperti enkripsi kata sandi, penguncian file atau penguncian perangkat keras, dan kemampuan untuk menyembunyikan volume terenkripsi di dalam volume yang ada. Berkat fitur keamanan dan fleksibilitas yang ditawarkannya, Veracrypt adalah pilihan populer bagi mereka yang ingin meningkatkan keamanan data mereka terhadap ancaman kejahatan siber.

4.4 Penggunaan veracrypt

Veracrypt cukup baik dalam membantu menangani cyber crime , cyber crime sering kali melibatkan pencurian data oleh karna itu veracrypt akan membantu dalam meng enkripsi file yang kita miliki sehingga aman dari pencurian data, Berikut adalah cara mengenkripsi data menggunakan veracrypt:

a. Langkah-langkah membuat file container baru pada veracrypt

1) Pada menu volumes pilih create new volume dan ikuti seperti gambar dibawah

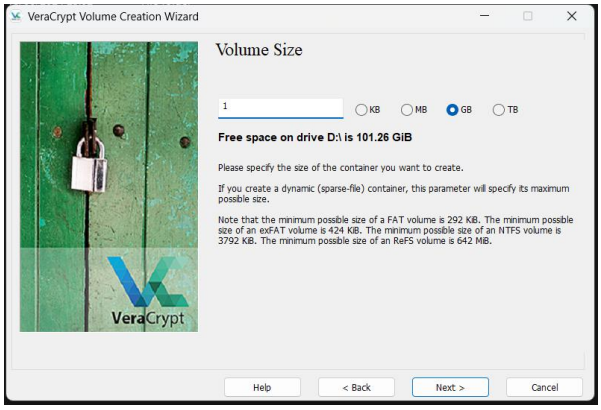


Gambar 1 Menu volume

2) Selanjutnya pilih tempat penyimpanan file container dan beri nama file container

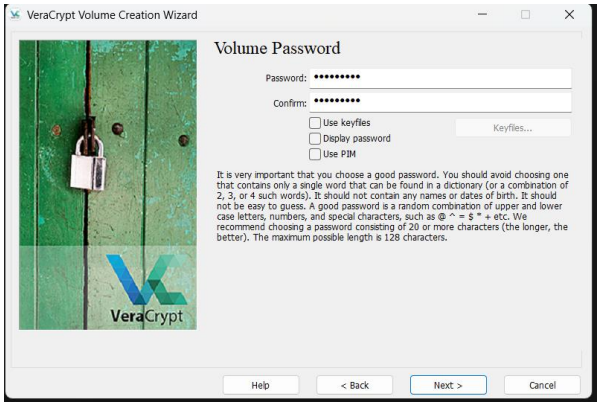
Gambar 2 Volume Location

3) Atur ukuran file container sesuai kebutuhan



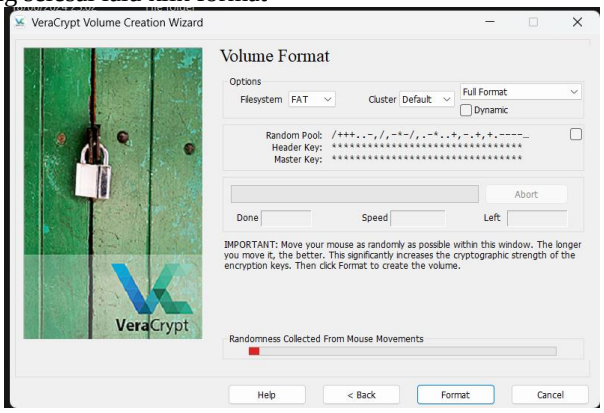
Gambar 3 Volume Size

4) Atur password file container



Gambar 4 Volume Pssword

5) Tunggu hingga loading selesai lalu klik format

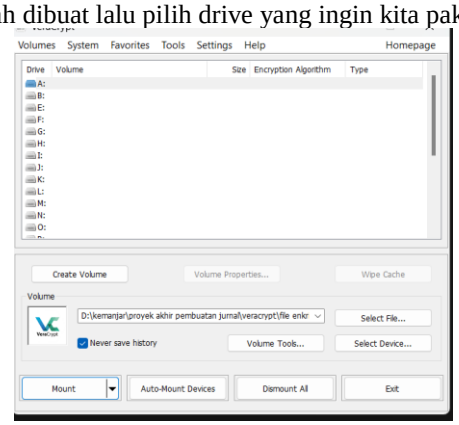


Gambar 5 Volume Format

6) File container telah selesai dibuat

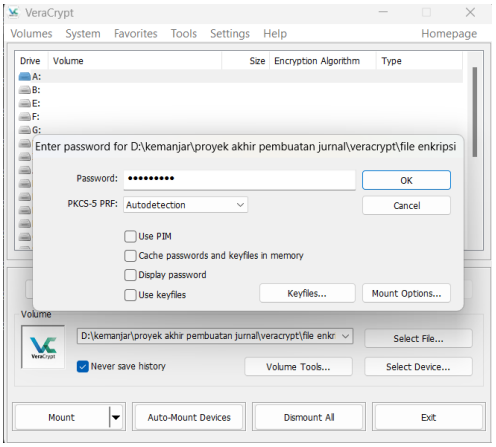
b. Cara mengenkripsi file di veracrypt

1) Pilih file container yang telah dibuat lalu pilih drive yang ingin kita pakai



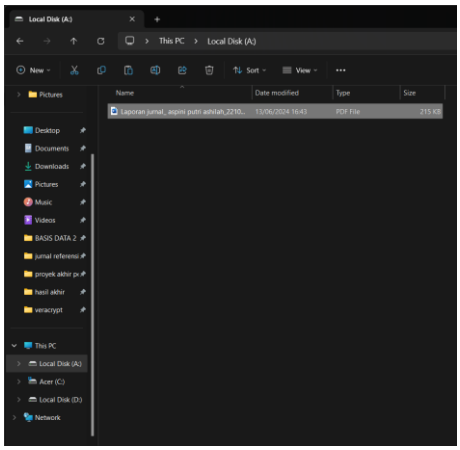
Gambar 6 File Container

2) Masukkan password yang telah di buat



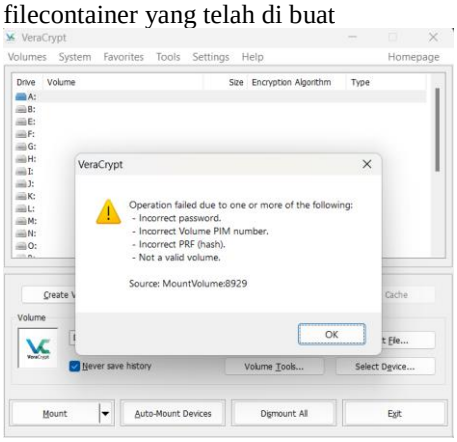
Gambar 7 Masukan Password

3) File container siap di gunakan



Gambar 8 File Container Siap digunakan

c. Tampilan jika gagal membuka filecontainer yang telah di buat



Gambar 9 Gagal membuka filecontainer

Dari gambar diatas ada beberapa kondisi yang dapat menyebabkan file container gagal di buka yaitu:

1) Password yang dimasukkan salah

Berdasarkan kondisi kegagalan diatas ada beberapa cara untuk mengatasinya berikutadalah caranya:

a) Periksa Ulang Password:
Pastikan bahwa Caps Lock tidak aktif, dan periksa kembali apakah password yang dimasukkan sudah benar. Coba ingat kembali password yang digunakan dan pastikan tidak ada kesalahan ketik.

b) Gunakan Password Manager:
Jika pengguna menggunakan password manager, pastikan untuk menyalin dan menempelkan password dengan benar.

2) Nomor PIM yang dimasukkan salah

Berdasarkan kondisi kegagalan diatas ada beberapa cara untuk mengatasinya berikut adalah caranya:

a) Periksa Nomor PIM:
Pada saat membuat volume terenkripsi, pengguna bisa menetapkan nomor PIM untuk meningkatkan keamanan. Pastikan memasukkan nomor PIM yang benar saat membuka volume.

b) Catat Nomor PIM yang Digunakan:
Simpan nomor PIM di tempat yang aman saat membuat volume.

3) PRF (hash) tidak tepat

Berdasarkan kondisi kegagalan diatas ada beberapa cara untuk mengatasinya berikut adalah caranya:

a) Coba Fungsi Hash Berbeda:
Saat mencoba membuka volume, di jendela VeraCrypt, pilih opsi Mount Options. Di bagian PRF (Hash), coba ganti dengan fungsi hash yang berbeda (misalnya, SHA-512, Whirlpool, atau lain-lain) dan coba buka kembali volume.
b) Ingat Fungsi Hash yang dipakai:
Simpan informasi tentang fungsi hash yang digunakan saat membuat volume untuk referensi di masa mendatang.

4) Disk yang dipilih tidak sesuai
Berdasarkan kondisi kegagalan diatas ada beberapa cara untuk mengatasinya berikut adalah caranya:
a) Periksa Lokasi Volume:
Pastikan memilih file volume yang benar. Klik Select File di VeraCrypt dan arahkan ke lokasi yang benar dari file volume terenkripsi.
b) Periksa Koneksi Drive:
Jika volume disimpan di drive eksternal, pastikan drive terhubung dengan benar ke komputer dan terdeteksi oleh sistem operasi.
c) Verifikasi Volume:
Pastikan file volume tidak rusak. Coba buka file volume di perangkat atau komputer lain untuk memastikan file tidak korup.

d. Kesimpulan dari penggunaan veracrypt
Setelah menggunakan Veracrypt, saya menemukan bahwa itu adalah alat yang bagus untuk melindungi data dari ancaman cybercrime, terutama pencurian data. Dengan menggunakan VeraCrypt untuk mengenkripsi file, saya dapat memastikan bahwa data sensitif saya aman serta tak bisa diaksesnya atas bagian yang tak berkuasa. Penggunaan VeraCrypt untuk mengenkripsi file dan pembuatan file container baru cukup mudah untuk dilakukan dengan mengikuti instruksi yang telah disediakan. Instruksi ini mencakup pembuatan file container baru dengan pengaturan password yang kuat dan penyesuaian ukuran, serta penggunaan file container untuk menyimpan dan mengakses data yang telah dienkripsi. Oleh karena itu, VeraCrypt adalah pilihan yang dapat diandalkan untuk melindungi Anda dari ancaman pencurian data cyber.

e. Startup yang menggunakan veracrypt
Sebuah startup teknologi berbasis di Jakarta bernama HealthTech Indonesia mengembangkan aplikasi kesehatan yang membantu pasien mengelola catatan medis mereka secara digital. Karena perusahaan ini menyimpan data pribadi dan medis pengguna, keamanan data sangat penting. Untuk melindungi data ini, HealthTech Indonesia menggunakan VeraCrypt dalam beberapa cara implementasi sebagi berikut :
1) Enkripsi Data Pengguna pada Server Backup
a) Kebutuhan: Untuk pemeliharaan dan pemulihan bencana, HealthTech Indonesia harus sering merekomendasikan data pengguna. Namun, data harus tetap aman saat disimpan dan dikirim.
b) Solusi VeraCrypt:
1. Perusahaan membuat volume terenkripsi dengan VeraCrypt pada server backup mereka.
2. Setiap kali data dicadangkan, data tersebut disalin ke dalam volume terenkripsi ini.
3. Volume ini hanya bisa diakses oleh administrator sistem yang memiliki password dan kunci enkripsi.

Keuntungan: Data tetap aman dari akses yang tidak sah selama proses pencadangan dan penyimpanan. Bahkan jika server backup dicuri atau diretas, data tetap tidak dapat diakses tanpa kunci enkripsi.

2) Perlindungan Data Pengembang
a) Kebutuhan: Laptop pengembang berisi kode sumber aplikasi, data pengujian, da informasi sensitif lainnya yang perlu dilindungi.
b) Solusi VeraCrypt:
1. Setiap laptop pengembang memiliki volume terenkripsi menggunakan VeraCrypt.
2. Pengembang menyimpan semua file kerja mereka di dalam volume ini.
3. Volume ini dienkripsi menggunakan algoritma kuat seperti AES (Advanced Encryption Standard).

Keuntungan: Jika laptop hilang atau dicuri, data yang tersimpan di dalamnya tetap aman dserta tak bisa diaksesnya atas bagian yang tak berkuasan. Ini pula mencegah kebocoran kode sumber dan informasi sensitif lainnya.

3) Kolaborasi aman
   a) Kebutuhan: Tim pengembang dan manajer proyek sering bekerja jarak jauh dan perlu berbagi file dan dokumen yang berisi informasi sensitif.
   b) Solusi VeraCrypt:
      1. Perusahaan membuat volume terenkripsi yang disimpannya dilayanan penyimpanannya cloud misalkan Google Drive ataupun Dropbox.
      2. Volume ini dibagikan di antara anggota tim. Setiap anggota tim yang memiliki password bisa mengakses dan mengedit file di dalam volume ini.
      3. Volume ini dipasang (mount) sebagai drive lokal saat bekerja dan dilepas (unmount) setelah selesai untuk memastikan data tidak terpapar secara terus-menerus.

   Keuntungan: Data yang dibagikan di layanan cloud tetap terlindungi. Hanya anggota tim yang diberi otorisasi yang dapat mengakses data tersebut. Ini memberikan lapisan keamanan tambahan dalam kolaborasi jarak jauh.

5. KESIMPULAN DAN SARAN

Temuan penelitian memastikan bahwasanya kejahatan cyber membahayakan keamanan siber Indonesia, terutama dalam kasus pembobolan data oleh Bjorka terhadap Kominfo. Pelaku seperti Bjorka memiliki banyak alasan, termasuk menentang kebijakan pemerintah dan mencari keuntungan finansial. Pembobolan data tersebut mengancam privasi dan keamanan nasional selain menunjukkan kelemahan sistem keamanan siber saat ini. Untuk mengatasi masalah ini, pemerintahan, lembaga terpautt, serta penduduk mesti berkolaborasi guna menumbuhkan kesadarannya tentang keamanan siber, menerapkan kebijakan keamanan yang ketat, dan mengadopsi teknologi yang dapat memperkuat pertahanan siber. Untuk melindungi data sensitif dan mencegah kejadian serupa di masa depan, individu dan organisasi harus menerapkan praktik keamanan siber yang baik dan menggunakan alat enkripsi seperti Veracrypt. Diharapkan bahwa langkah-langkah ini akan memungkinkan Indonesia untuk membangun fondasi yang lebih kuat untuk melawan ancaman kejahatan cyber dan untuk memastikan keamanan informasi yang berlebih baik akan penduduk secara universal.

DAFTAR PUSTAKA

[1] M. Z. Rizaldi, R. D. Putra, dan A. Ul Hosnah, “Analisis Kasus Cybercrime Dengan Studi Kasus Hacker Bjorka Terhadap Pembocoran Data,” JUSTITIA J. Ilmu Huk. dan Hum., vol. 6, no. 2, hal. 619, 2023, doi: 10.31604/justitia.v6i2.619-627.

[2] F. Y. N. Sufi, D. K. Putri, dan D. Suhartini, “Analisis Ancaman Cybercrime dan Peran Sistem Biometrik : Systematic Literature Review,” Pros. Senapan, vol. 3, no. 1, hal. 19–29, 2023.

[3] BSSN, “Lanskap Keamanan Siber Indonesia,” no. 70, 2024.

[4] C. Hidayatullah, “Jenis dan Dampak Cyber Crime,” Pros. SAINTEK Sains dan Teknol., vol. 2, no. 1, hal. 216–221, 2023, [Daring]. Tersedia pada: https://www.jurnal.pelitabangsa.ac.id/index.php/SAINTEK/article/view/2159

[5] Setyaji, A. G., Kurniawan, D., & Siswanto, E. (2023). KONTROL BERBASIS SYNCHRONVERTER DAN MODEL PREDIKTIF UNTUK MULTI-PORT AUTONOMOUS RECONFIGURABLE SOLAR PLANTS. *Informatika: Jurnal Teknik Informatika dan Multimedia*, *3*(1), 59-80.

[6] Asry, D. W., Siswanto, E., Kurniawan, D., & Huda, H. I. (2023). Deteksi Malware Statis Menggunakan Deep Neural Networks Pada Portable Executable. *Teknik: Jurnal Ilmu Teknik dan Informatika*, *3*(1), 19-34.

[7] Yulhendri, Y., Simorangkir, H., Faridho, F., & Kurniawan, D. (2022). Implementasi Digital Dashboard Untuk Mengontrol Wilayah Rt/Rw. *Jurnal Informatika Dan Tekonologi Komputer (JITEK)*, *2*(1), 43-54.