Media Akuntansi dan Perpajakan Indonesia
Volume 5, Nomor 2, Maret 2024

p-ISSN: 2685-9203
e-ISSN: 2686-5610

SPIONASE NEGERI TIRAI BAMBU: ANALISIS KEGIATAN INTELIJEN ATAS SUMBER DAYA INTELEKTUAL AMERIKA SERIKAT

Adeline Hamidy Kushandojo, Steven Sanjaya
Universitas Ciputra Surabaya

Abstract: *People's lives are increasingly reliant on the internet. Because of the ease it provides, everyone, including huge corporations, uses the internet and its information networks. However, all internet users and information systems are vulnerable to attacks, one of which is cyber espionage. Cyber espionage is espionage carried out using computer systems or the internet. One of the most significant cyber espionage instances of the century is Operation Aurora. The purpose of this research is to uncover the systematics of Aurora operations using the netnographic method. From this research it is known that hackers from the Aurora operation, Elderwood, are a hacking organization with hacking capabilities that have compromised data, specifically source code, for 30 private US corporations, including Google. Elderwood used a strategy known as Zero Day Exploit and attacked these private corporations through emails. Based on existing evidence, Elderwood is thought to have originated in China. Furthermore, they have done multiple attacks in the past few years aside from the Aurora operation, implementing various methods. Both the United States and the United Kingdom have agreed to a settlement as a means of resolving their differences. In the perspective of an accountant, it is possible that this event occurs, since there is a lack of management control, specifically education regarding level of data which resulted in weak securities, so an improvement in literature and education of the level of data is needed so it can be avoided in the future.*

Keywords: *cyber espionage, aurora operation, Google, Elderwood, management control*

Abstrak: Internet merupakan salah satu bagian besar dalam kehidupan masyarakat saat ini. Tiap individu bahkan perusahaan besar bergantung pada internet dan sistem informasinya karena kemudahan yang tersedia. Namun, dengan kemudahan tersebut terdapat ancaman bagi semua pengguna internet dan sistem informasi, salah satunya yakni *cyber espionage. Cyber*

*Corresponding Author.
e-mail: akushandojo@student.ciputra.ac.id

espionage merupakan spionase yang dilakukan melalui sistem informasi maupun secara siber. Operasi Aurora adalah salah satu kasus *cyber espionage* terbesar abad ini. Tujuan dari penelitian ini adalah mengungkap sistemasi dari operasi Aurora dengan menggunakan metode netnografi dalam menyelami realitas virtual (*online*). Dari penelitian ini diketahui bahwa *hacker* dari operasi Aurora, Elderwood, merupakan kelompok *hacker* dengan kemampuan hacking yang membuat 30 perusahaan swasta asal Amerika Serikat, termasuk Google, mengalami kebobolan data, lebih spesifiknya *source code*. Elderwood menggunakan strategi yang dikenal dengan *Zero Day Exploit* dan melancarkan serangannya melalui email. Berdasarkan bukti-bukti yang ada, Elderwood diyakini berasal dari Cina serta telah melakukan beberapa serangan selain operasi Aurora dalam beberapa tahun dan dengan menggunakan metode yang berbeda-beda. Sebagai bentuk penyelesaiannya baik Amerika Serikat dan Cina bersumpah untuk tidak melakukan *Espionage Cyber Attack* kedepannya. Berdasarkan perspektif akuntan, hal ini dapat terjadi karena kurangnya pengendalian manajemen khususnya edukasi *level of data* yang menyebabkan sistem keamanan yang lengah, maka diperlukan literasi dan edukasi akan *level of data* agar kejadian serupa tidak terulang ke depannya.

Kata kunci: cyber espionage, operasi aurora, Google, Elderwood, pengendalian manajemen

PENDAHULUAN

Di era globalisasi yang seringkali disebut dengan era 5.0, manusia sangat bergantung dengan teknologi dan digitalisasi, dalam 20 tahun terakhir teknologi dan internet berkembang pesat dan menghadirkan banyak kemudahan bagi penggunanya. Menurut Kemp (2022), total pengguna internet di dunia adalah 4.95 miliar atau setara dengan 62.5%. Dari data tersebut dapat disimpulkan bahwa lebih dari setengah populasi bumi bergantung kepada internet dalam kehidupan sehari-harinya, bahkan sampai ke ranah penyimpanan data. Internet tentu mempermudah penggunanya, namun seiring dengan berkembangnya internet, tingkat *cyber-crime*/*attack* pun turut meningkat. Salah satu bentuk *cyber-attack* yang paling merugikan ialah *cyber espionage.*

Cyber espionage sudah terjadi beberapa kali sejak awal tahun 2000-an. Kasus yang sempat menjadi perhatian publik adalah kasus Abin, seorang intelijen asal Brazil, yang melakukan spionase pada tahun 2003 hingga 2004 (Mustameer, 2022). Amerika Serikat juga sempat menjadi pelaku dari *cyber espionage* di mana

mereka mengintai masyarakatnya bahkan para pemimpin dunia melalui Badan Keamanan Nasional Amerika Serikat (NSA) (Pratiwi & Correia, 2020). Indonesia mengalami hal serupa saat percakapan telepon sejumlah pemimpinnya mengalami penyadapan oleh Amerika dan Australia di tahun 2007–2009 (Hastri, 2021).

Pada tahun 2009, dunia digemparkan dengan salah satu kasus *cyber espionage* terbesar abad ini, operasi Aurora. Investigasi akan operasi Aurora yang terjadi kurang lebih 13 tahun yang lalu ini dilakukan demi mengungkap kebenaran dan mengedukasi khalayak ramai mengenai kasus ini, walau terjadi lebih dari satu dekade yang lalu, pengetahuan masyarakat akan kasus ini masihlah minim. Sumber-sumber yang tersedia untuk diakses pun rata-rata menyediakan informasi yang sama. Google yang merupakan salah satu korban dari operasi Aurora seolah menutup rapat-rapat kasus tersebut dan menganggapnya sebagai aib dengan hanya menyediakan segelintir informasi mengenainya. Operasi Aurora yang merupakan salah satu kasus pembobolan sistem informasi terbesar abad ini tidak tersampaikan secara jelas dan transparan kepada masyarakat.

Setahun setelah operasi Aurora berlangsung, *hacker* yang sama kembali melancarkan serangannya menggunakan metode yang berbeda. Strategi yang digunakan dinamakan *Watering Hole Attack.* Menurut Krithika (2017) *Watering Hole Attack* bekerja dengan cara memasukkan *malware* pada *website*. Target dari penyerangan ini adalah perusahaan yang menyediakan senjata untuk Amerika. Di dalam perusahaan tersebut terdapat informasi terkait senjata keluaran terbaru Amerika. Informasi tersebut menjadi ketertarikan bagi *hacker* untuk dicuri. Mereka memanfaatkan *Supply chain* dalam serangannya dan menyerang pemasok pihak ketiga, di mana pemasok pihak ketiga memiliki tingkat keamanan yang lebih rendah dibandingkan perusahaan utama yang diincar. *Malware* yang sudah masuk ke dalam komputer perusahaan pemasok akan pindah tangan hingga akhirnya memasuki komputer perusahaan utama yang dituju tanpa terdeteksi.

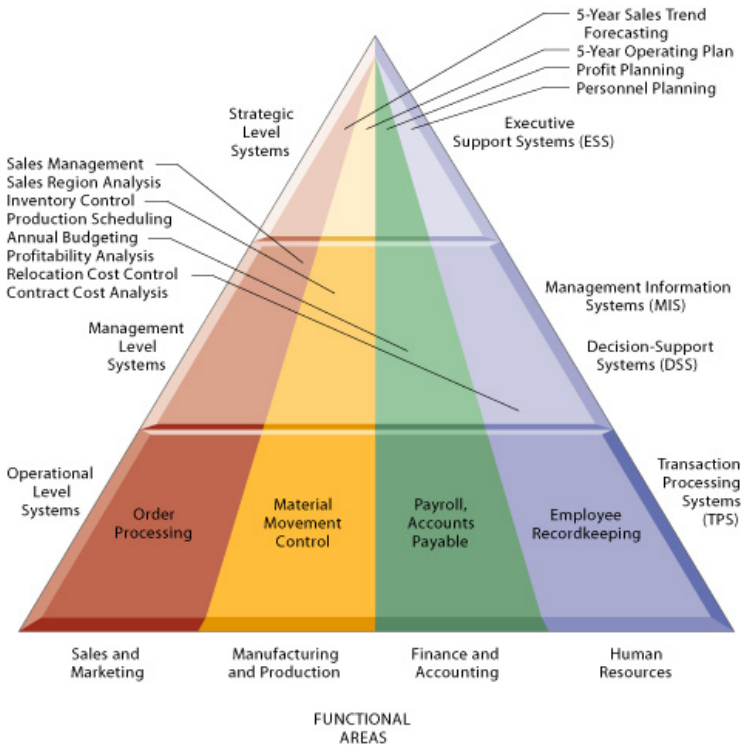
Saat ini, mayoritas aktivitas menggunakan teknologi informasi. Hal ini menjadi perhatian karena kejahatan siber merupakan upaya kejahatan yang dilakukan menggunakan media internet. Operasi Aurora pada tahun 2009 lalu merupakan kasus kejahatan siber yang tidak banyak orang ketahui. Tujuan dari penelitian ini adalah mengungkap kebenaran dari operasi Aurora kepada masyarakat, maka masyarakat mengerti apa yang harus diperhatikan dalam menggunakan internet dan sistem berbasis komputer. Selain itu, masyarakat akan

paham mengenai manajemen data yang benar dari tiap *level of data* yang ada. Investigasi lebih dalam mengenai operasi Aurora diharapkan dapat dijadikan sebagai acuan masyarakat, perusahaan atau lembaga dalam menindaki *cyber espionage*. Hasil kajian investigasi penelitian ini memberikan kontribusi pada pengembangan bidang keilmuan sistem pengendalian manajemen strategis khususnya terkait dengan sistem informasi data yang dimiliki suatu entitas. Pada akhir tulisan peneliti juga berupaya untuk mengaitkan peristiwa tersebut dengan kontribusi peran akuntan.

LANDASAN TEORI

Level of Data

Sistem informasi yang dititikberatkan dalam investigasi ini adalah *level of data*. Data merupakan bagian krusial dari sistem informasi manajemen sebuah



Gambar 1 Tampilan Level of Data
Sumber: *Management Information Systems Chapter 2* (2019)

perusahaan. Suatu perusahaan terdapat beragam jenis data dengan perannya masing-masing dan level yang berbeda. Semakin tinggi level suatu data maka semakin tinggi pula level keamanan yang harus diterapkan (IncludeHelp, 2023). Dalam operasi Aurora yang bertempat pada 2009 silam Google beserta sederet perusahaan ternama lainnya tidak menyadari pentingnya data yang mereka miliki. Hal ini dapat dilihat dari sistem keamanan atas data mereka yang masih banyak celah.

Level of data menjadi teori yang dapat digunakan dalam penelitian ini. Adanya celah pada manajemen sistem informasi menunjukkan bahwa perusahaan tidak mengimplementasikan tingkat keamanan yang seharusnya diterapkan berdasarkan tingkatan kepentingan data. Manajemen bagian teratas membutuhkan keamanan tertinggi karena menyimpan rancangan masa depan perusahaan hingga beberapa tahun ke depan. Prioritas keamanan diterapkan pada data yang berada di manajemen teratas. Penggolongan kepentingan data oleh manajemen menjadi krusial. Gambar 1 menunjukkan contoh data dan bobotnya masing-masing sesuai dengan penggolongan yang ada pada piramida.

METODE PENELITIAN

Pendekatan Penelitian

Penelitian ini menggunakan metode netnografi. Netnografi sendiri memiliki pengertian sebagai sebuah metode penelitian yang menggunakan pendekatan etnografi yang berfokus pada komunitas *online*, maka metode ini sering juga disebut metode etnografi *online* (Priyowidodo, 2020). Dalam melakukan investigasi berlandaskan metode netnografi maka haruslah dilakukan pengumpulan data dari berbagai sumber, bukan hanya melalui pencarian di internet maupun berdasarkan pengalaman, namun memanfaatkan keduanya dan memberdayakannya semaksimal mungkin. Pendekatan yang dilakukan dalam metode ini pun mencakup pendekatan secara kualitatif, sehingga hasil investigasi dapat memberikan jawaban maksimal atas pertanyaan yang ada. Pengumpulan data dilaksanakan pada bulan April hingga bulan Juni 2022.

Sumber Data dan Pengumpulan Data

Investigasi kasus aurora menggunakan sumber data yang disebut dengan sumber data sekunder. Sumber data sekunder memiliki pengertian sebagai sumber data dalam suatu penelitian yang didapatkan secara tidak langsung melalui media perantara (Idrianto & Supomo, 2013). Kasus aurora sendiri merupakan kasus yang terjadi pada tahun 2009–2010 di mana internet tidak semaju sekarang. Hal ini berdampak pada tingkat kesulitan dalam menginvestigasi kasus tersebut karena minimnya sumber informasi yang ada. Namun peneliti memandang hal ini perlu dikaji untuk menilik pelajaran berharga apa yang bisa didapatkan dari kasus tersebut dari sudut pandang pengendalian informasi dan datanya. Berdasarkan paparan tersebut dapat disimpulkan bahwa dalam melakukan investigasi kasus aurora peneliti bergantung pada sumber data sekunder karena sumber data primer merupakan hal yang sulit untuk diwujudkan dengan adanya kendala dari berbagai aspek. Demi menjaga etika publikasi maka nama akun dari berbagai sumber akun data yang dikumpulkan tidak ditampilkan dalam naskah artikel ini.

Tabel 1 Jumlah Sumber Data Observasi

No.	Aplikasi	Data
1	Youtube	148,445 penonton, 6,007 menyukai
2	Quora	14,100 pembaca, 218 menyukai
3	Facebook	8 kali dilihat, 2 menyukai
4	Instagram	0
5	Twitter	32 kali dibagikan, 64 menyukai

Dalam investigasi operasi Aurora penulis memutuskan untuk melakukan pengumpulan data, di mana metode pengumpulan data ini sendiri termasuk dalam pendekatan data arsip. Menurut Pakaya et al. (2022), data yang sudah tersedia di internet maupun dari komunitas *online* yang kemudian diduplikat oleh peneliti merupakan bentuk dari data arsip. Jenis data ini merupakan salah satu jenis data yang paling mudah untuk diakses maka sangatlah sesuai dengan investigasi kasus aurora yang minim sumber ini. Namun, dengan kemudahan yang ada maka rawan terjadi pemalsuan maupun data yang tidak relevan. Oleh karena itu, diperlukan penyaringan data yang ketat dalam investigasi ini.

Tahapan Analisis Data

Dalam melakukan investigasi, penulis menggunakan metode pengumpulan data berupa data arsip. Data tersebut diperoleh melalui akses internet, di mana informasi terkait kasus Aurora, video, dan jurnal dapat ditemukan dengan mudah. Melalui internet penulis dapat mengakses laman-laman yang berkaitan dengan kasus aurora maupun video serta jurnal. Literatur yang sudah dipublikasikan oleh penulis terdahulu menjadi acuan sumber data penelitian ini. Setelah data terkumpul, penulis melakukan pengecekan relevansi data dengan topik investigasi dan rumusan masalah penelitian. Penulis juga melakukan *coding* untuk mengklasifikasikan data dengan tanda tertentu agar mempermudah analisis data ke depannya. Setelah data diolah dan di-*coding*, penulis melakukan tabulasi di mana penulis akan menyusun dan menyajikan data sesuai dengan permasalahan yang ada.

Data kualitatif yang diperoleh dari internet ditafsirkan menjadi kalimat yang dapat mempermudah pengertian pembaca. Tahap terakhir adalah menafsirkan data hasil analisis. Penafsiran tersebut dilakukan dengan tujuan menafsirkan data-data yang sudah dikumpulkan, diolah, dan dianalisis menjadi sebuah kesatuan simpulan yang dapat dengan mudah dimengerti oleh pembaca. Penafsiran analisis ini haruslah objektif dan berdasarkan data relevan yang ada, bukan pandangan penulis semata.

ANALISIS DATA DAN PEMBAHASAN

Berdasarkan data yang didapatkan dari berbagai sumber maka ulasan disajikan dalam pembahasan berikut ini. Salah satu temuan penjelajahan di realitas *online* menemukan *timeline* operasi Aurora.

Gambar 2 Tampilan Timeline Operasi Aurora
Sumber: Koleksi Data Peneliti (2023)

Zero Day Exploit dan Sistemasi Hacking

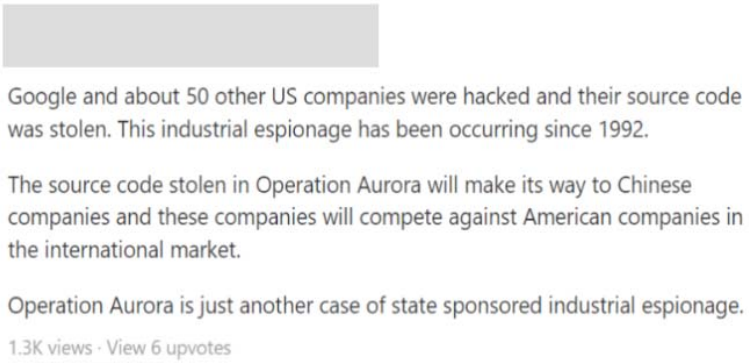
Operasi Aurora berlangsung dalam kurun waktu yang cukup singkat yakni kurang lebih 1 bulan. Kelompok yang melakukan serangan pun memilih waktu yang tepat untuk melakukan serangannya pada bulan Desember dan Januari di mana pekerja keamanan yang bekerja di perusahaan-perusahaan tersebut sedang berada dalam masa liburan. Menggunakan kesempatan ini peretas dapat mengakses data yang mereka perlukan. Operasi Aurora yang berlangsung dalam kurun waktu yang singkat mengindikasikan bahwa *hacker* sebelumnya sudah membuat serangkaian preparasi sebelum melakukan serangan. Ketika serangan diluncurkan mereka tidak perlu membuang waktu lebih lama lagi dan tidak memberikan celah bagi perusahaan yang ter *hack* untuk merespons terlebih dahulu. *Zero Day Exploit* adalah selisih hari di mana kerentanan diketahui dan hari di mana serangan pertama kali dilakukan (Cloudmatika, 2022). Serangan yang tiba-tiba dan tidak memberikan kesempatan bagi perusahaan untuk merespons merupakan salah satu faktor mengapa sistem informasi perusahaan target dapat ter-*hack*.

Gambar 3 Tampilan Video Mengenai Operasi Aurora
Sumber: Koleksi Data Peneliti (2023)

Gambar 4 Tampilan Video Mengenai Operasi Aurora
Sumber: Koleksi Data Peneliti (2023)

Berdasarkan data yang ada terdapat informasi yang cukup lengkap serta titik terang keterkaitan data dengan kajian pustaka yang sudah disampaikan sebelumnya. Seperti yang diketahui bahwa selama berlangsungnya operasi Aurora terdapat banyak perusahaan besar swasta asli Amerika yang mengalami kerugian karena

data mereka diambil. Sekumpulan informasi yang tersimpan dengan teratur dalam komputer dan ke depannya dapat dikaji menggunakan program komputer guna memperoleh informasi disebut database maupun basis data (Alfia & Waseso, 2020). Data yang diambil ini lebih dikenal dengan sebutan *source code*, di mana ketika data tersebut jatuh ke pihak lain maka pihak tersebut dapat membuat *web* serupa maupun menemukan *bug* dalam *source code* tersebut yang nantinya dapat dieksploitasi. *Source code* sendiri merupakan sekumpulan kode yang tertulis sehingga dapat dibaca manusia (Huda, 2022). Data berharga tersebut dapat jatuh ke tangan hacker dikarenakan adanya *malware advance* yang digunakan oleh *hacker*.



Gambar 5 Tampilan Artikel Mengenai Operasi Aurora
Sumber: Koleksi Data Peneliti (2023)

Tidak seperti *hacker* lainnya, *hacker* operasi Aurora menggunakan *Zero Day Exploit*. Mereka menyalurkan *link* menuju sebuah program kepada pihak-pihak yang menjadi target mereka. Namun, sebelumnya *hacker* operasi Aurora telah mempelajari latar belakang target mereka serta dengan siapa saja mereka biasa melakukan kontak (melalui *e-mail*). Mereka pun mengirimkan link tersebut dengan berlagak sebagai kontak erat dari target mereka, sehingga target mereka akan langsung jatuh ke dalam perangkap tersebut. Ketika program tersebut terunduh maka program tersebut akan berfungsi sebagai jembatan bagi *hacker* untuk masuk ke dalam sistem komputer target. Google yang merupakan salah satu korban dari operasi ini menyadari bahwa target dari operasi ini merupakan aktivis Hak Asasi Manusia (HAM) yang berada di Cina serta akun dari orang-orang yang diminta akunnya oleh *Unites State Law Enforcement*. Tetapi untungnya

Google berhasil menghentikan serangan ini sebelum *hacker* berhasil membuat kerusakan yang lebih parah pada sistem informasi Google.

Gambar 6 Tampilan Video Mengenai Operasi Aurora
Sumber: Koleksi Data Peneliti (2023)

Kelengahan Google dan Aktivitas Elderwood

Serangan ini mampu menembus berbagai macam pertahanan yang dimiliki oleh perusahaan-perusahaan besar swasta yang berada di Amerika. Padahal tiap perusahaan memiliki sistem pertahanan informasi yang berbeda-beda. Namun, tidak semua perusahaan ini mengungkapkan letak kelemahan sistem mereka setelah serangan ini terjadi. Google sendiri yang merupakan salah satu korban paling dirugikan dari serangan ini menutup rapat-rapat kelengahan sistem mereka. Melalui pencarian yang lebih dalam dan teliti maka dapat diketahui kelemahan dari sistem keamanan informasi Google.

Google diketahui menggunakan sebuah sistem yang dikenal dengan sebutan *Perforce*. *Perforce* merupakan bagian dari *Version Control System* (VCS), sebuah infrastruktur yang dapat mengembangkan software yang ada secara kolaboratif. Menurut Guerrero-Higueras et al. (2020) VCS digunakan untuk menyetorkan *source code* dan dokumentasi data. Di antara semua VCS yang ada Google menggunakan *Perforce* karena keunggulan yang dimilikinya. Berbeda dengan sistem lainnya *Perforce* memiliki sebuah sistem yang dapat merilis *software* menjadi *production* kapan saja, sistem ini dikenal dengan *Continuous Delivery.* Selain itu, Perforce juga memiliki *massive scalability, hybrid version control, social coding, large binaries,* dan *unified security.* Namun, setelah serangan dari operasi Aurora, Google menemukan kekurangan dari VCS tersebut.

Kekurangan pertama adalah semua orang dapat membuat *account* sendiri tanpa perlu adanya admin untuk men-setup account tersebut. *Password* yang biasa digunakan di Google pun bersifat *unencrypted* yang berarti data tersebut dapat dilihat orang lain. Dalam menggunakan Perforce pun pengguna dapat

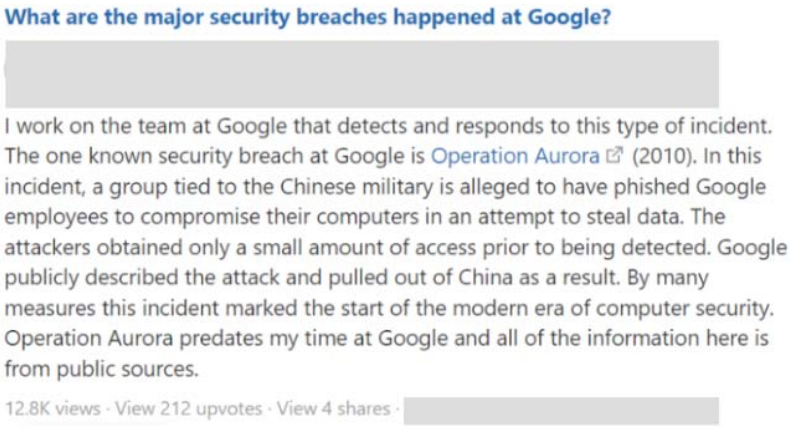
dengan mudah mengumpulkan data yang mereka inginkan tanpa perlu memiliki *privilege* tertentu, sehingga *hacker* pun dapat dengan mudah menemukan data yang mereka cari. Autentikasi yang ditetapkan oleh Google pun mudah dilewati. Data yang tersimpan dalam bentuk teks transparan pun menambah kekurangan dari VCS jenis *Perforce* ini. Berbagai kekurangan dari Perforce menjadi celah bagi *hacker* operasi Aurora untuk menjalankan serangan mereka.

Keterlambatan perusahaan dalam perkembangan sistem pertahanan yang mampu menciptakan perlindungan bagi akun-akun pengguna nya menjadi celah bagi peretas untuk mengakses data perusahaan dengan mudah. Skala prioritas keamanan dilakukan oleh Google untuk menciptakan keamanan yang lebih efektif untuk penggunaannya dan Google. Teori *level of data* berperan penting untuk menjadi acuan bagi perusahaan mengetahui di *level* manakah perusahaan membutuhkan implementasi keamanan yang lebih.

Begitu serangan keamanan sistem informasi terjadi, Google dan perusahaan-perusahaan lainnya bertindak cepat sehingga kerugian yang mereka alami masih dapat ditanggulangi. Namun, setelah menanggulanginya muncul pertanyaan mengenai siapa dalang di balik serangan yang begitu besar dan berbahaya ini. Perusahaan-perusahaan yang menjadi korban pun menyelidiki hal tersebut. Diketahui bahwa serangan tersebut berasal dari Cina, tepatnya berasal dari Shanghai Jiao Tong University dan Lanxiang Vocational School. Serangan ini juga menggunakan *Checksum Algorithm* (sebuah algoritma rangkaian huruf dan angka yang digunakan untuk memeriksa kesalahan data) yang hanya digunakan di Cina. Tak lupa bahwa akun-akun *Gmail* yang menjadi target utama penyerangan ini merupakan akun dari aktivis HAM yang berada di Cina. Hal ini menyebabkan perusahaan yang menjadi korban untuk berspekulasi bahwa pemerintah Cina berada di balik serangan ini. Karena dengan berbagai pertimbangan bahwa tidak memungkinkan bagi anak-anak kuliah pada umumnya untuk melakukan serangan sedemikian rupa.

Walaupun Cina menolak tuduhan dari Amerika terkait dengan serangan ini. Namun, seiring dengan pengecekan lebih lanjut perusahaan yang menjadi korban pun semakin yakin atas tuduhan tersebut. Mereka juga yakin bahwa Cina memiliki tim khusus yang bekerja sama untuk melakukan operasi aurora. Sistem keamanan perusahaan yang menjadi korban bukanlah sistem keamanan yang mudah ditembus begitu saja sehingga siapa pun yang meretas sistem keamanan

tersebut pasti membutuhkan dana yang besar serta *privilege* dalam mengakses data yang mereka perlukan.



Gambar 7 Tampilan Artikel Mengenai Operasi Aurora
Sumber: Koleksi Data Peneliti (2023)

Tiap perusahaan yang menjadi korban berusaha untuk menguak pelaku utama di balik kejahatan tersebut. "Setidaknya ada 30 perusahaan yang menjadi korban Operasi Aurora dengan keluhan yang sama dengan Google" (Simamora, 2010). Walau terdapat kurang lebih 30 perusahaan yang berusaha menguak kasus ini. Namun, hal tersebut tidaklah mudah karena Cina yang tidak mau bersikap kooperatif. Seiring berjalannya penyelidikan kelompok *hacker* di balik operasi Aurora mendapatkan sebuah nama. Kelompok *hacker* ini menyebarkan dan menggunakan kembali eksploitasi dan pengetahuan yang mereka dapatkan agar menghasilkan impact yang maksimal. Berdasarkan penemuan dari Symantec, yang merupakan salah satu korban dari operasi aurora, terdapat sebuah *malware* bernama Elderwood dalam operasi Aurora. Maka dari itu, hingga kini kelompok penyerang ini dikenal dengan nama grup Elderwood.

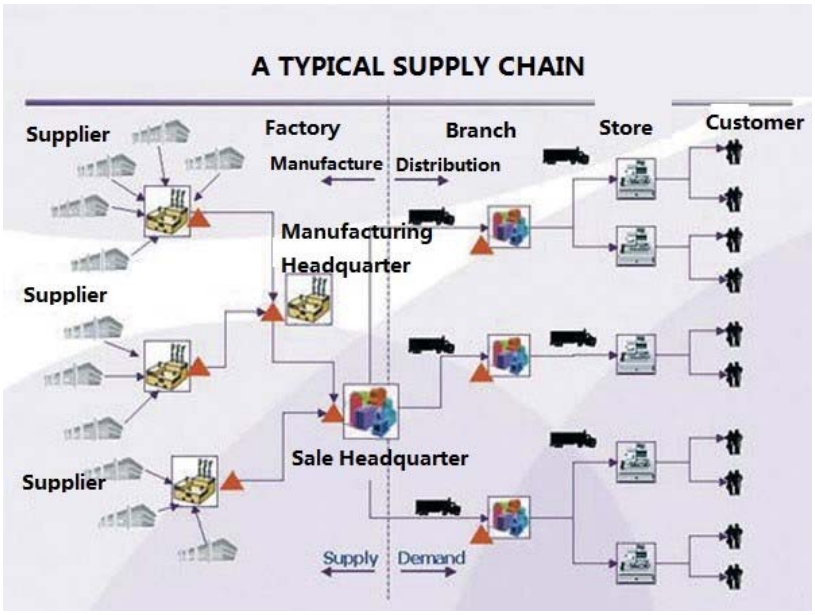
Kasus Serupa

Penyerangan dari *hacker* yang disebut sebagai Elderwood ini tidak berhenti di tahun 2010 saja. Pada tahun 2011 Elderwood beraksi kembali dengan target dan strategi yang berbeda. Strategi yang digunakan dinamakan *Watering Hole Attack*. Menurut Krithika (2017) *Watering Hole Attack* bekerja dengan cara

memasuki *malware* pada website. *Malware* yang ditanam pada *website* tersebut akan bekerja ketika ada seseorang yang menekan website tersebut, dan ketika hal itu terjadi peretas mendapatkan kendali penuh atas komputer korban.

Target dari Elderwood *group* ini adalah perusahaan yang menyediakan senjata untuk Amerika. Di dalam perusahaan tersebut terdapat informasi terkait senjata keluaran terbaru Amerika dan lain-lain. Informasi tersebut menjadi ketertarikan bagi Elderwood *group* untuk dicuri. Namun, Elderwood *group* memiliki sistematika terbaru dalam melaksanakan aksinya, yaitu dengan memanfaatkan *supply chain* dari perusahaan senjata tersebut. Pemasok yang menjadi pihak ketiga cenderung memiliki tingkat keamanan yang lebih rendah dibandingkan perusahaan utama yang diincar.

Celah tersebut akhirnya digunakan oleh Elderwood *group* dengan cara mengamati apa saja aktivitas perusahaan pemasok di internet. Kemudian melihat *website* apa saja yang dituju perusahaan pemasok. Dari situ Elderwood *group* dapat melaksanakan *Watering Hole Attack*. Kemudian, *malware* yang sudah masuk ke dalam komputer perusahaan pemasok akan pindah tangan hingga akhirnya memasuki komputer perusahaan utama yang dituju tanpa terdeteksi.



Gambar 8 Tampilan Supply Chain Management
Sumber: Supermap.com (2019)

Penyelesaian

Google pada akhirnya menarik seluruh kantornya yang berada di Cina. Google.cn berhenti beroperasi di Cina. Berhentinya Google yang ada di Cina ini juga dikarenakan faktor yang mendukung lainnya. Yaitu, kemauan Cina yang bertentangan dengan prinsip yang dimiliki Sergey (*co-founder* Google) pada saat itu. Sepanjang Google beroperasi di Cina, pemerintah Cina selalu memiliki permintaan untuk sensor beberapa konten yang ada di Google terkait dengan permasalahan yang pernah dilalui Cina seperti contoh protes di Tiananmen *Square* pada tahun 1989. Mundurnya Google dari Cina juga mengubah level of data yang dimiliki Google terutama pada level *upper management*. Pada level tersebut Google merancangkan rancangan perusahaan lima tahun ke depan di Cina, namun karena terjadinya ketidaksetujuan antara Cina dan Google maka rancangan tersebut pada level *upper management* dihapuskan.

Pada tahun 2008, saat *Olympics* dimulai Cina meminta Google untuk melakukan sensor terhadap beberapa konten. Google akhirnya menuruti kemauan Cina dan beranggapan bahwa selepas *olympics* Cina tidak akan melakukan sensor lebih banyak lagi. Namun, persepsi tersebut salah, setelah *olympics* usai Cina meminta Google untuk melakukan sensor kembali bahkan lebih luas dari sebelumnya. Informasi terkait dengan apa pun yang berhubungan dengan kritik untuk pemerintah Cina diblokir. Menurut Pratama (2017) langkah yang diambil oleh pemerintah Cina ini beralasan karena kekuatan sumber daya manusia, infrastruktur TIK, dan kekuatan modalnya mendukung, sehingga selain alasan ideologi alasan ini juga merupakan alasan ekonomi. Google merasa mereka malah membantu melaksanakan *oppression* Cina. Google memiliki motto yaitu *"Don't be evil"* namun, dengan membantu Cina maka google menjadi "*evil*". Menurut pembicara Google saat itu, Bill Echikson, hal yang dilakukan Cina adalah menyensor berbagai informasi penting, di mana pada saat yang bersamaan Google ingin memberikan informasi semaksimum mungkin kepada penggunanya (RadioFreeEurope, 2010). Maka dari itu, Google memutuskan untuk memutus hubungan dengan salah satu negara yang memiliki populasi terbesar di dunia tersebut. Pada tahun 2015 kedua presiden negara Cina dan Amerika setuju dan bersumpah untuk tidak melakukan *espionage cyber attack*.

Reaksi Masyarakat di Realitas Online

Dalam penelitian tentunya reaksi masyarakat merupakan salah satu hal penting yang harus dipertimbangkan dan dikaji. Setelah kasus ini muncul ke permukaan maka muncul pula pendapat dari masyarakat. Pendapat ini bervariasi, mulai dari pendapat yang menyuarakan pro hingga kontra. Masyarakat menyuarakan pendapat mereka di situs-situs media sosial yang ada, seperti di kolom komentar Youtube maupun laman Quora.

Gambar 9 Tampilan Komen Quora
Sumber: Koleksi Data Peneliti (2023)

Gambar 10 Tampilan Komen Quora
Sumber: Koleksi Data Peneliti (2023)

Peristiwa Operasi Aurora dalam Perspektif Level of Data seorang Akuntan

Dalam operasi Aurora, *hacker* memiliki fokus untuk mengambil data dari seluruh pengguna Google. Data-data yang diambil umumnya merupakan data-data pribadi pengguna Google yang digunakan untuk keuntungan *hacker*. Hal ini

sangatlah gawat bagi Google mengingat bahwa data pribadi tiap pengguna merupakan sebuah privasi. Data pribadi sendiri merupakan salah satu bagian dari level of data, yakni *management level systems*, yang harus dilindungi bersamaan dengan jenis data-data lainnya (*Management Information Systems*, 2019).

Berdasarkan perspektif akuntan, literasi dan edukasi akan *level of data* harus ditingkatkan (Rahmadyah & Aslami, 2022). Operasi Aurora terjadi karena kurangnya literasi *level of data* yang menyebabkan lemahnya sistem keamanan akan data yang dimiliki google. Selain itu, hal ini juga menyebabkan manajemen data yang tidak tepat. Melalui lebih dipahaminya tingkatan dari level of data, maka akan diketahui sistem keamanan seperti apa yang diperlukan untuk menjaga data-data tersebut. Dengan begitu kejadian serupa dapat dihindari ke depannya.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan penelitian yang dilakukan maka dapat disimpulkan bahwa operasi Aurora merupakan salah satu kasus *Cyber espionage* terbesar sepanjang sejarah. Operasi ini terjadi pada tahun 2009-2010 dan menarget perusahaan besar seperti Google, Adobe, Microsoft, dan lainnya. *Hacker* operasi Aurora berhasil menembus pertahanan perusahaan-perusahaan swasta besar asal Amerika Serikat menggunakan sistemasi *hacking* mereka yaitu *Zero Day Exploit*. Sistem pertahanan perusahaan yang memiliki banyak celah juga mempermudah jalan *hacker* operasi Aurora. Mereka pun memiliki fokus yang jelas yakni *source code* dari perusahaan-perusahaan tersebut. Selain itu, mereka juga menarget akun-akun *g-mail* aktivis HAM Cina dan orang-orang yang diminta akunnya oleh *United State Law Enforcement*. Setelah diselidiki lebih lanjut diketahui bahwa serangan itu berasal dari Shanghai Jiao Tong University dan Lanxiang Vocational School yang berada di Cina. Diketahui juga bahwa serangan tersebut menggunakan Checksum Algorithm yang digunakan Cina‘. Google pun mengonfirmasi Cina mengenai hal itu. Namun, hal ini ditolak dengan keras. Tak lama setelah itu *hacker* dari kasus ini lebih dikenal dengan sebutan Elderwood. Karena Cina terus menerus menolak dan hubungan Cina dengan Google yang kurang baik maka

Google menarik perusahaannya dari Cina, sedangkan perusahaan lainnya memilih untuk diam. Selain operasi Aurora, Elderwood juga merupakan pelaku dari berbagai kasus *hacking* skala besar lainnya, menggunakan sistem baru yaitu *Watering Hole Attack*. Sebagai upaya memperbaiki hubungan antara Amerika dan Cina maka pada tahun 2015 kedua negara tersebut bersumpah untuk tidak melakukan *espionage cyber attack* ke depannya. Perjanjian ini juga diperbarui tiap beberapa tahun sekali.

Saat ini perusahaan-perusahaan swasta yang menjadi target dari operasi Aurora telah belajar dari kesalahan mereka. Sistem keamanan mereka yang menyediakan banyak celah bagi hacker pun sudah diganti dan diperbaiki. Seiring berjalannya waktu maka hacker akan terus berevolusi dan menemukan cara-cara baru untuk meretas sistem. Maka dari itu, dari perspektif akuntan diperlukan literasi dan edukasi akan pentingnya *level of data* dan bagaimana cara menerapkan sistem keamanan yang tepat bagi tiap *level of data* agar kejadian serupa tidak terjadi lagi ke depannya.

Keterbatasan dan Saran

Berdasarkan pada pengalaman langsung pada peneliti dalam proses penelitian ini, ada beberapa keterbatasan yang dialami dan dapat menjadi beberapa faktor yang dapat dijadikan perhatian bagi peneliti-peneliti yang akan datang. Peneliti yang akan datang diharapkan dapat menyempurnakan penelitian ini, karena penelitian ini tentu memiliki kekurangan. Salah satunya adalah jumlah reaksi masyarakat yang kurang secara nominal, sehingga peneliti mengalami kesulitan dalam menggambarkan seberapa ramai isu yang diangkat. Selain itu, tidak ada sampel yang didapatkan melalui Instagram, sehingga menunjukkan kesulitan peneliti dalam mendapatkan data yang memadai. Berdasarkan penelitian yang telah dilakukan, terdapat beberapa saran yang dapat diberikan. Pertama, untuk penelitian selanjutnya, disarankan agar peneliti mendapatkan sampel lebih banyak menggunakan platform media sosial yang sedang populer. Hal ini diharapkan dapat mendukung keakuratan data. Selain itu, disarankan pula untuk melakukan penelitian berkelanjutan yang mengikuti perkembangan terkini, terutama pada perkembangan di negeri tirai bambu.

DAFTAR RUJUKAN

Alfia, N. E. & Waseso, B. (2020). Perancangan Aplikasi Retensi Data Pada Database MySQL (Studi Kasus: PT Telkomsigma). *JUSIBI Jurnal Sistem Informasi dan E-Bisnis, 2*(3), 364–374.

Associated Press. (2010, March 24). *Google's Action Angers China, Web Users Wonder*. YouTube. https://youtu.be/UXMIWIPcC3o?si=C_RYs6WTczgJMWGD.

Baker, K. (2023). What is Cyber espionage? Crowdstrike. Retrieved January 13, 2024, from: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/ *CloudGIS Technology Supports the Management of Supply Chains - SuperMap*. (2019). www.supermap.com. https://www.supermap.com/en-us/news/?82_726.html.

Cloudmatika. (2022). Kenali Apa Itu Zero Day Attack serta Cara Mencegahnya Terjadi pada Website Anda. Retrieved December 30, 2023, from: https://cloudmatika.co.id/blog-detail/apa-itu-zero-day-attack.

Fajar, R. (2014). *10 Version Control System yang Harus Kamu Kenal*. CODEPOLITAN. Retrieved January 13, 2024, from: https://www.codepolitan.com/10-version-control-system-yang-harus-kamu-kenal/.

Guerrero-Higueras, Á. M., Llamas, C. F., González, L. S., Fernández, A. G., Costales, G. E., & González, M. Á. C. (2020). Academic Success Assessment through Version Control Systems. *Applied Sciences*, *10*(4), 1–11.

Hastri, E. D. (2021). Cyber Espionage Sebagai Ancaman terhadap Pertahanan dan Keamanan Negara Indonesia. *Law & Justice Review Journal*, *1*(1), 12–25.

Huda, N. (2022). Source Code: Pengertian, Macam-Macam & Jenis Berkasnya. Blog Dewaweb. Retrieved February 10, 2024, from: https://www.dewaweb.com/blog/pengertian-source-code/.

IncludeHelp. (2023). *Levels of Management in MIS*. Retrieved January 10, 2024, from: https://www.includehelp.com/MIS/levels-of-management.aspx.

Idriantoro, N. & Supomo B. (2014). *Metode Penelitian Bisnis untuk Akuntansi dan Manajemen* (1st ed.). Yogyakarta: BPFE.

Kemp, S. (2022). *Digital 2022: Global Overview Report*. DataReportal. Retrieved January 13, 2023, from: https://datareportal.com/reports/digital-2022-global-overview-report.

Krithika, N. (2017). A Study On WHA (Watering Hole Attack) - The Most Dangerous Threat to the Organization. *International Journal of Innovation in Scientific and Engineering Research (IJISER), 4*(8), 196–198.

Management Information Systems. (2019). *Information Systems in the Enterprise*. Retrieved January 13, 2024, from: https://paginas.fe.up.pt/~acbrito/laudon/ch2/chpt2-1main.htm.

McAfee. (2010). "*Operation Aurora" Leading to Other Threats*. Retrieved January 15, 2024, from: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-aurora-leading-to-other-threats/.

Mulachela, H. (2021). *Database adalah Pengertian dan Jenisnya*. Katadata.co.id. Retrieved January 13, 2024, from: https://katadata.co.id/intan/digital/61c04e3f62f5b/database-adalah-pengertian-dan-jenisnya.

Mustameer, H. (2022). Penegakan Hukum Nasional dan Hukum internasional terhadap Kejahatan Cyber Espionage pada Era Society 5.0. *Jurnal Yustika: Media Hukum dan Keadilan*, *25*(1), 40–53.

Nabila, S., Dewi, M. S. W., Hilaly, S. G., & Mukaromah, S. (2023). Analisis Tingkat Kesadaran Pengguna Media Sosial Terkait Privasi dan Keamanan Data Pribadi. *Prosiding Seminar Nasional Teknologi dan Sistem Informasi*, *3*(1), 553–562.

Pakaya, H., Bo'do, S., & Akifah, A. (2022). Praktek Berbagi dalam Komunitas Virtual di Facebook: Studi Netnografi pada Komunitas Fotografi Indonesia. *Kinesik*, *9*(3), 312–326.

Pratama, B. (2017). Perspektif Hukum Siber dalam Menangkap Fenomena Disruptive Innovation [Conference Presentation]. *Seminar Nasional Disruptive Innovation Kajian Ekonomi dan Hukum*, Yogyakarta, Indonesia

Pratiwi, L. Y. E. & Correia, Z. F. M. (2022). Hukum Siber: Praktik Spionase dalam Kedaulatan Negara dan Hubungan Diplomasi Berdasarkan Ketentuan Hukum Internasional. *Jurnal Pendidikan Kewarganegaraan Undiksha*, *8*(3), 206–218.

Priyowidodo, G. (2020). *Monograf Netnografi Komunikasi: Aplikasi pada Tiga Riset Lapangan*. Depok: Rajawali Pers.

RadioFreeEurope. (2010). *U.S., Google Take Hard Line on China*. Retrieved February 13, 2023, from: https://www.rferl.org/a/Google_May_Pull_Out_Of_China_Over_Censorship/1927884.html.

Rahmadyah, N. & Aslami, N. (2022). Strategi Manajemen Perubahan Perusahaan di Era Transformasi Digital. *Ekonam: Jurnal Ekonomi, Akuntansi & Manajemen*, *4*(2), 91–96.

Rezkia, S. M. (2021). *Kenali 4 Perbedaan Data sekunder dan Data Primer Saat Melakukan Penelitian*. DQ Lab. Retrieved January 13, 2023, from: https://www.dqlab.id/kenali-4-perbedaan-data-sekunder-dan-data-primer-saat-melakukan-penelitian.

Shinta, A. (2022). *Cyber Espionage: Pengertian, Contoh Kasus, & Cara Mencegah*. Retrieved January 13, 2024, from: https://www.dewaweb.com/blog/apa-itu-cyber-espionage/.

Simamora, M. H. (1970). *McAfee: Hacker Operation Aurora Manipulasi Kelemahan IE Untuk Menyerang Google & Adobe*. Retrieved January 13, 2024, from: https://plazaegov.blogspot.com/2010/01/mcafee-hacker-operation-aurora.html.