IMPLEMENTASI CIS BENCHMARK UNTUK STANDARISASI KEAMANAN INFORMASI PADA APLIKASI ZOOM CLOUD MEETINGS LEMBAGA PELATIHAN XYZ

Mohammad Afdhal Jauhari[1], Bheta Agus Wardijono[1] dan Ega Hegarini[2]

[(1)]STMIK Jakarta STI&K
Jl. BRI No.17, Radio Dalam, Kebayoran Baru, Jakarta Selatan 12140
[(2)]Universitas Gunadarma
Jl. Margonda Raya No. 100, Depok, Jawa Barat 16424
{afdhaljauhari, bhetaagus, hegarini}@gmail.com

ABSTRAK

Lembaga Pelatihan XYZ menjadi salah satu entitas yang terkena dampak diberlakukannya WFH (Work From Home), sejak pandemi COVID-19 khususnya saat mulai berlakunya PSBB hingga PPKM. Lembaga Pelatihan XYZ telah banyak melakukan kegiatan belajar mengajar secara daring melalui Zoom sebagai platform pendukung berjalannya kegiatan belajar mengajar. Di tengah meningkatnya jumlah pengguna Zoom selama pandemi COVID-19, pihak pengembang Zoom Video Communications, Inc mengalami berbagai masalah kejahatan siber (cyber crime). Terkait dengan semua isu keamanan yang dialami pihak Zoom dan penggunanya, diperlukan adanya tindakan pencegahan dengan menerapkan praktik terbaik (best practice) menggunakan Center for Internet Security (CIS) Benchmark untuk memberikan konfigurasi yang aman terhadap aplikasi Zoom yang digunakan oleh Lembaga Pelatihan XYZ. Asesmen dilaksanakan sebagai tahap pra implementasi dan memberikan hasil bahwa Lembaga Pelatihan XYZ hanya menerapkan 40,5% dari 163 kontrol konfigurasi yang direkomendasikan oleh CIS Benchmark, sehingga Lembaga Pelatihan XYZ dianggap belum menerapkan konfigurasi yang aman untuk akun Zoom yang dimilikinya dan perlu dilakukan remediasi sesuai dengan rekomendasi konfigurasi pada CIS Zoom Benchmark untuk menjamin keamanan penggunaan Zoom Cloud Meeting dari serangan siber yang mungkin terjadi.

Kata Kunci : *zoom, keamanan, informasi, cis, benchmark*

PENDAHULUAN

Latar Belakang

Pandemi COVID-19 telah melanda dunia lebih dari satu tahun dan hampir memasuki tahun kedua sejak pertama kali terdeteksi di kota Wuhan, Cina pada tahun 2019. Pada tanggal 7 Januari 2020, COVID-19 teridentifikasi oleh Cina sebagai jenis baru dari Virus Corona yang menyebabkan pneumonia [1]. Pneumonia adalah peradangan paru-paru yang terjadi akibat adanya infeksi. Gejala yang muncul dapat bervariasi mulai dari ringan hingga berat. Batuk berdahak, demam dan sesak nafas merupakan gejala paling umum yang dapat diamati dari pengidap pneumonia [2]. Jumlah kasus terkonfirmasi hingga saat ini sudah mencapai 250.715.502 dengan total meninggal dunia sebanyak 5.062.106 di 226 negara di dunia. Di Indonesia sendiri, kasus terkonfirmasi sebanyak 4.249.758 dengan total meninggal dunia sebanyak 143.608 [3]. Kondisi terparah sempat terjadi di Indonesia di pertengahan tahun 2021. Banyak masyarakat yang kehilangan jiwa setelah varian delta menyebar di Indonesia pada saat itu.

Menyikapi hal tersebut, Presiden Republik Indonesia Joko Widodo melalui konferensi pers yang diselenggarakan di Bogor pada tanggal 14 Maret 2020, menghimbau kepada seluruh masyarakat Indonesia untuk bekerja, sekolah dan beribadah dari rumah masing-masing dalam rangka mencegah semakin meluasnya penyebaran virus corona [4]. Berdasarkan himbauan presiden tersebut, banya perusahaan, sekolah dan instansi pemerintah yang menerapkan kebijakan *Work From Home* (WFH). Sebagai dampak diberlakukannya WFH, perlu dilakukan adaptasi di berbagai sektor pekerjaan, segala bentuk kegiatan yang memerlukan pelayanan tatap muka telah diubah menjadi palayanan daring via konferensi video. Kampus perguruan tinggi dan sekolah-

sekolah yang pada awalnya hanya sebagian kecil saja yang menerapkan sistem pembelajaran daring, kini sebagian besar sisanya juga ikut turut menerapkan sistem pembelajaran secara daring.

Besarnya animo masyarakat untuk beralih ke pertemuan tatap muka secara daring, berdampak pada meningkatnya jumlah pengguna layanan aplikasi penunjang untuk bekerja dari rumah hingga lebih dari 443%, yakni layanan konferensi video seperti *Zoom*, Microsoft Teams dan CloudX Telkomsel [5]. Dari seluruh aplikasi tersebut, *Zoom Cloud Meetings* menjadi salah satu aplikasi konferensi video yang paling banyak digunakan.

Zoom merupakan salah satu aplikasi yang dirancang untuk membantu tim dalam bisnis dan organisasi untuk tetap dapat terhubung dengan orang lain secara aman melalui konferensi video tanpa harus bertatap muka secara fisik dalam rangka menyelesaikan lebih banyak pekerjaan. *Zoom* didirikan pada tahun 2011. Perusahaan ini diperdagangkan secara publik (NASDAQ:ZM) dan berkantor pusat di San Jose, California [6]. Aplikasi *Zoom* dapat digunakan untuk berbagai kegiatan, khususnya segala kegiatan yang saat ini harus dilakukan secara daring, seperi kegiatan belajar mengajar, perkantoran, layanan publik dan lain sebagainya. *Zoom* menyediakan *platform* konferensi video secara daring yang dapat digunakan secara gratis dengan batasan fitur tertentu. Salah satu batasan fitur tersebut adalah durasi koferensi video yang dapat dilakukan dalam satu sesi pertemuan, di mana setiap pengguna hanya dapat melakukan konferensi video selama 40 menit dan tidak dapat melakukan perekaman. Hal ini berbeda untuk *platform* berbayar yang disediakan oleh *Zoom*, yakni *Zoom Meetings Pro, Business* dan *Enterprise*, di mana setiap penggunanya dapat melakukan konferensi video sepuasnya tanpa batasan waktu dan dapat merekam kegiatan konferensi video yang sedang dilakukan, serta fitur-fitur menarik lainnya yang tidak dapat ditemukan di *Zoom Meetings* versi gratis.

Di tengah meningkatnya jumlah pengguna *Zoom* selama pandemi COVID-19, pihak pengembang *Zoom Video Communications, Inc* mengalami berbagai masalah kejahatan siber. Widodo mendefinisikan kejahatan siber sebagai suatu kegiatan individu, sekumpulan orang atau badan hukum yang memanfaatkan komputer sebagai sarana melakukan kejahatan, atau menargetkan komputer sebagai sasaran kejahatan. Semua kejahatan tersebut termasuk dalam bentuk perbuatan yang bertentangan dengan peraturan perundang-undangan, baik dalam maksud melawan hukum secara material maupun melawan hukum secara formal [7]. Hal seperti ini dapat terjadi di berbagai *platform* yang ada di Internet, khususnya pada perusahaan teknologi komunikasi seperti *Zoom* . *Zoom* sempat mengalami kebocoran data pengguna, berdasarkan informasi yang dilaporkan oleh pakar keamanan Internet *Bleeping Computer,* ditemukan sebanyak 530.000 data pengguna *Zoom* yang dijual di situs kejahatan dunia maya dan forum peretas dengan harga US$ 0,002 atau sekitar Rp 31 per akun. Informasi yang dijual terdiri dari alamat email, kata sandi, URL, *private meeting* dan *HostKey* pengguna. Selain itu, aplikasi *Zoom* juga dilaporkan mengalami suatu serangan yang dikenal dengan istilah *Zoombombing*, yakni aksi serangan dari pihak luar yang masuk ke ruang rapat daring dengan tujuan untuk mengganggu berjalannya rapat secara daring [8]. *Zoombombing* ini terjadi di berbagai pertemuan daring, baik yang dilakukan oleh kantor, kampus, sekolah dan yang lainnya. Aplikasi *Zoom* kemudian mendapatkan banyak kritik terkait dengan berbagai isu *cyber crime* tersebut, walaupun isu tersebut tidak berpengaruh terhadap jumlah pengguna *Zoom*, karena jumlah pengguna *Zoom* dilaporkan terus meningkat setiap minggunya [9]. Kejahatan siber yang dialami pengguna *Zoom* dapat terjadi akibat batasan privasi pengguna. Penyedia jasa teknologi informasi seringkali tidak jelas dalam menetapkan kebijakan privasi dan seringkali tunduk pada pada interpretasi hukum, akibatnya pengguna memiliki kewajiban untuk menyadari ancaman dan melindungi informasi pribadinya. Perilaku dalam penggunaan teknologi yang tidak tepat dan tingkat kesadaran individu masih rendah menyebabkan tingginya resiko

terkait dengan kejahatan siber [10]. Menanggapi isu keamanan tersebut, *Zoom* mengklaim bahwa aplikasinya telah didukung dengan *end-to-end encryption* untuk seluruh rapat yang telah dijadwalkan melalui aplikasi *Zoom*. Selain itu, juga telah ditambahkan fitur perlindungan ruang pertemuan dengan menggunakan kata sandi untuk meningkatkan keamanan pengguna [11].

Lembaga traning XYZ merupakan salah satu Lembaga Pelatihan di bidang TI yang sudah berdiri lebih dari 20 tahun. Lembaga Pelatihan ini menjadi salah satu entitas yang terkena dampak diberlakukannya WFH. Sejak pandemi COVID-19 dan pemberlakukan PSBB hingga PPKM, Lembaga Pelatihan XYZ telah banyak melakukan kegiatan belajar mengajar secara daring melalui platform konferensi video, di mana Lembaga Pelatihan XYZ ini memilih aplikasi *Zoom* sebagai platform pendukung berjalannya kegiatan belajar mengajar tersebut. Terkait dengan semua isu yang dialami pihak *Zoom* dan penggunanya, diperlukan adanya tindakan pencegahan dengan menerapkan praktik terbaik (*best practice*) dalam rangka memberikan konfigurasi yang aman pada aplikasi *Zoom* yang digunakan oleh Lembaga Pelatihan XYZ.

Terdapat berbagai kerangka kerja *(framework)* yang dapat digunakan sebagai panduan untuk melakukan praktik terbaik terhadap keamanan informasi di dunia siber, antara lain NIST, ISO 27001/27002, PCI, DSS dan lain-lain. Selain itu, juga terdapat panduan terbaik untuk keamanan informasi yang dipromosikan oleh *Center for Internet Security (CIS),* yakni *CIS Controls* dan *CIS Benchmarks*. CIS adalah organisasi nirlaba yang didikan pada tahun 2000. CIS memiliki misi untuk mengidentifikasi, mengembangkan, memvalidasi dan mempromosikan praktik terbaik dalam perlindungan siber di seluruh dunia. *CIS Controls* dan *CIS Benchmarks* adalah produk dari CIS yang dapat digunakan oleh berbagai pihak secara gratis. Keduanya dibuat bukan untuk menggantikan *framework* lainnya seperti yang telah disebutkan sebelumnya. *CIS Controls* dan *CIS Benchmarks* dapat digunakan sebagai alternatif panduan keamanan informasi pada tataran organisasi. Panduan yang terdapat dalam *CIS Controls* dan *CIS Benchmarks* terbilang sangat mudah untuk dilakukan, bahkan oleh pemula sekalipun [12].

Berdasarkan pemaparan fenomena dan masalah yang telah diuraikan di atas, peningkatan pengguna aplikasi *Zoom* di masa pandemi COVID-19 berbanding lurus dengan meningkatnya kejahatan siber yang menyerang pengguna aplikasi *Zoom*.

Tujuan Penelitian

Meningkatnya kejahatan siber yang dialami oleh para pengguna aplikasi *Zoom* membawa dampak yang cukup signifikan bila dilihat dari aspek keamanan informasi. Lembaga Pelatihan XYZ menginisiasi dilakukannya asesmen terhadap konfigurasi akun *Zoom* yang dimilikinya untuk mengidentifikasi celah keamanan yang mungkin dapat disusupi oleh para pelaku kejahatan siber.

Tujuan penelitian adalah melakukan analisis pada konfigurasi keamanan *Zoom* yang dimiliki Lembaga Pelatihan XYZ melalui proses asesmen berdasarkan pada standar *CIS Benchmark*. Kemudian akan diberikan rekomendasi dari hasil pengukuran, sehingga dapat digunakan untuk meningkatkan keamanan aplikasi *Zoom* yang dimiliki Lembaga Pelatihan XYZ dari ancaman serangan siber.

Tinjauan Literatur

Center for Internet Security (CIS) Benchmarks merupakan pedoman praktik terbaik yang dapat diikuti sebagai panduan dalam penerapan konfigurasi sistem yang aman. Terdapat lebih dari 100 *benchmark* atau tolok ukur CIS di lebih dari 25 produk vendor. *CIS Benchmarks* ini dikembangkan melalui proses konsensus yang unik, di mana para anggotanya berasal dari profesional keamanan siber di seluruh dunia, seperti *subject matter experts*, vendor teknologi, anggota komunitas publik dan swasta, serta tim pengembangan *CIS Benchmarks* [12].

Proses pengembangan *benchmark* diawali dengan mendefinisikan ruang lingkup *benchmark* dan dilanjutkan dengan diskusi, lalu pembuatan dan pengujian *draft*

kerja. Serangkaian diskusi dan dialog dilakukan melalui situs web *CIS Workbench* hingga tercapai konsensus mengenai rekomendasi yang diusulkan dan *draft* kerjanya. Setelah berhasil mencapai konsensus, *benchmark* dapat dirilis dan diterbitkan secara daring. *CIS Benchmark* dapat diunduh secara gratis dalam format PDF. *File* dengan format lainnya seperti XCCDF, *Word* dan sebagainya hanya dapat diunduh oleh anggota *CIS SecureSuite*.

Sebagian besar *CIS Benchmark* menyertakan beberapa profil konfigurasi, yakni Profil *Level* 1, *Level* 2 dan STIG. Definisi profil menjelaskan konfigurasi yang ditetapkan untuk rekomendasi *benchmark*. Profil *Level* 1 dianggap sebagai rekomenasi dasar yang dapat diterapkan dengan cukup cepat dan dirancang untuk tidak memiliki dampak kinerja yang luas. Tujuannya adalah untuk mengurangi *attack surface* organisasi, sekaligus memastikan agar mesin tetap dapat berjalan dan tidak menghalangi fungsionalitas bisnis. Profil *Level* 2 dianggap sebagai pertahanan yang lebih mendalam dan ditujukan untuk lingkungan yang mengutamakan keamanan. Rekomendasi pada profil *Level* 2 dapat berdampak buruk pada organisasi apabila tidak diterapkan dengan tepat atau tanpa kehati-hatian. Profil yang ketiga disebut dengan STIG (*Security Technical Implementation Guide*). Profil STIG ini menggantikan profil *Level* 3 yang ada sebelumnya. Profil STIG menyediakan semua rekomendasi yang khusus untuk STIG. Tumpang tindih rekomendasi dari profil lain, yakni *Level* 1 dan *Level* 2 ada di profil STIG sebagaimana yang berlaku. Setiap rekomendasi dalam setiap *CIS Benchmark* dikaitkan dengan setidaknya satu profil. Terlepas dari profil *Level* mana yang direncanakan untuk diterapkan di lingkungan organisasi, sebaiknya terapkan *CIS Benchmark* di lingkungan pengujian terlebih dahulu untuk menentukan potensi dampak yang ditimbulkan.

Audit atau asesmen berdasarkan praktik terbaik *CIS Benchmarks* dapat dilakukan secara manual atau pun dengan bantuan perangkat lunak bernama CIS-CAT Pro. Perangkat lunak ini hanya dapat dinikmati oleh anggota *CIS SecureSuite*.

Penelitian Sebelumnya

Beberapa penelitian sejenis pernah dilakukan dengan melakukan studi kasus pada sistem yang sudah berjalan, di antaranya sebagai berikut:

1. Implementasi *Security Auditor* Untuk Standardisasi Instalasi Server Pada Layanan SaaS Ecampuz Menggunakan *CIS Benchmark* [13] oleh Muhammad Najib pada tahun 2020. Penelitian ini berfokus pada penggunaan *CIS Benchmark* sebagai *security auditor* untuk mengaudit layanan SaaS Ecampuz. Hasil dari penelitian ini menyatakan bahwa *CIS Benchmark* dapat mendukung *system administrator* dalam melaksanakan evaluasi dari layanan SaaS dengan menggunakan hasil audit berdasarkan *CIS Benchmark* sebagai dokumen pendukung dalam melakukan langkah evaluasi.
2. Audit Dan Implementasi *CIS Benchmark* Pada Sistem Operasi *Linux Debian Server* (Studi Kasus: Server Laboratorium Jaringan Dan Komputer 6, Institut Sains & Teknologi Akprind Yogyakarta) [14] oleh Dika Priska Prastika, Joko Triyono dan Uning Lestari pada tahun 2018. Penelitian ini membahas tentang pelaksanaan audit dan penerapan *CIS Benchmark* untuk jaminan keamanan pada *Linux Debian Server 8* yang digunakan di Laboratorium Jaringan dan Komputer 6, IST AKPRIND Yogyakarta dari ancaman serangan siber. Berdasarkan audit yang telah dilakukan, 70% dari rekomendasi *CIS Benchmark* untuk *Linux Debian Server* telah dijalankan. Dengan kata lain, server pada Laboratorium tersebut telah berhasil menerapkan praktik terbaik pengamanan sistem operasi *Linux Debian Server* berdasarkan *CIS Benchmark* yang disusun oleh CIS.
3. Analisa Kerentanan Pada *Vulnerable Docker* Menggunakan Alienvault Dan *Docker Bench For Security* Dengan Acuan *Framework CIS Control* [15] oleh Fatin Hanifah, Avon Budiyono dan Adityas Widjajarto pada tahun 2021. Penelitian ini bertujuan untuk menguji secara empiris tentang analisis

kerentanan pada *Docker* menggunakan pemindai kerentanan yang mengacu pada *framework CIS Control* yang didasarkan pada *CIS Docker Benchmark v1.3.1*. Pada penelitian ini, *CIS Control* tersebut digunakan dalam rangka mengurangi risiko yang mungkin muncul pada penelitian ini.

METODE PENELITIAN

Objek Penelitian

Objek dalam penelitian ini adalah aplikasi *Zoom Cloud Meetings* yang digunakan oleh Lembaga Pelatihan XYZ untuk mendukung proses belajar dan mengajar secara daring melalui konferensi video. Produk yang digunakan oleh Lembaga Pelatihan XYZ adalah *Zoom* Pro.

Instrumen Penelitian

Instrumen atau alat utama yang akan digunakan dalam penelitian ini adalah panduan praktik keamanan terbaik *CIS Zoom Benchmark v1.0.0* yang dirilis pada tanggal 22 Oktober 2020 dalam format PDF. Dokumen ini berisi 3 (tiga) konfigurasi utama yang terdiri dari 171 rekomendasi konfigurasi yang aman untuk menjadi tolok ukur dalam mengukur tingkat keamanan konfigurasi pada aplikasi *Zoom* Lembaga Pelatihan XYZ dan nantinya akan dijadikan sebagai panduan untuk penerapan konfigurasi yang aman di aplikasi *Zoom* tersebut.

Selain *CIS Zoom Benchmark*, juga diperlukan satu unit perangkat komputer atau laptop yang sudah terhubung ke Internet dan dengan sistem operasi apapun, untuk dapat menjalankan aplikasi *Zoom Cloud Meeting*s di perangkat tersebut. Kegiatan asesmen dilakukan secara manual dan seluruh informasi yang diperoleh akan diinput dan diolah menggunakan perangkat lunak Microsoft Excel.

Tahapan Penelitian

Penelitian ini akan dilakukan dalam dua tahap. Tahap pertama adalah asesmen terhadap pengaturan akun *Zoom* yang dimiliki oleh Lembaga Pelatihan XYZ, berdasarkan daftar kontrol atau rekomendasi yang terdapat di *CIS Zoom Benchmark.* Proses asesmen dilakukan melalui *web browser* dan bukan pada aplikasi *Zoom* yang terinstal di ponsel atau komputer *desktop*. Di tahap ini dikumpulkan informasi terkait pengaturan apa saja yang belum diterapkan dan berpotensi menjadi celah keamanan pada akun *Zoom* Lembaga Pelatihan XYZ. Tahap kedua adalah penerapan konfigurasi yang aman untuk akun *Zoom* Lembaga Pelatihan XYZ berdasarkan panduan *CIS Zoom Benchmarks*.

HASIL DAN PEMBAHASAN

Seperti yang telah dijelaskan pada bagian sebelumnya, *CIS Zoom Benchmark v1.0.0* berisi 171 rekomendasi konfigurasi yang aman yang dapat diterapkan pada akun *Zoom*. Namun, tidak semua rekomendasi tersebut relevan dengan versi *Zoom* yang tersedia dan dijalankan saat penelitian ini dilakukan. Dari 171 rekomendasi, hanya 163 rekomendasi yang dapat digunakan pada saat pelaksanaan asesmen yang dilakukan pada tanggal 31 Mei 2022. Hal ini dapat disebabkan akibat adanya pemutakhiran dari pihak *Zoom* ataupun terkait dengan versi *Zoom* yang digunakan oleh Lembaga Pelatihan XYZ.

Hasil asesmen menggunakan *CIS Zoom Benchmark* dapat dilihat pada Tabel 1, 2 dan 3.

Account Settings Configuration

Pengaturan akun merupakan bagian paling vital yang harus dikonfigurasi secara aman. Pada bagian ini, Lembaga Pelatihan XYZ hanya menerapkan 58 atau 44% dari 132 kontrol yang direkomendasikan. Terdapat 74 kontrol yang belum dilaksanakan sehingga dapat menciptakan celah keamanan. Kontrol yang tidak diterapkan pada bagian ini termasuk kategori kontrol paling dasar seperti persyaratan minimum pembuatan kata sandi yang rumit dan pengaktifan kata sandi untuk *room meeting ID.*

Pada tabel asesmen, kontrol atau rekomendasi yang sudah diimplementasi ditandai dengan tanda centang pada kolom *Implemented*. Sedangkan kontrol yang diberi keterangan "*Not assessed*" artinya tidak diasesmen oleh sebab adanya pemutakhiran dari pihak *Zoom* ataupun

terkait dengan versi *Zoom* yang digunakan oleh Lembaga Pelatihan XYZ.

Tabel 1. *Hasil Asesmen Account Settings Configuration Menggunakan CIS Zoom Benchmark*

No.	*Controls*	*Implemented*
1	***Account Settings***	
1.1	***Meeting***	
1.1.1	***Security***	
1.1.1.1	***Passcode Requirement***	
1.1.1.1.1	*Ensure minimum passcode length is set to at least 6 characters (Manual)*	
1.1.1.1.2	*Ensure passcode is set to have at least 1 letter (Manual)*	
1.1.1.1.3	*Ensure passcode is set to have at least 1 number (Manual)*	
1.1.1.1.4	*Ensure passcode is set to have at least 1 special character (Manual)*	
1.1.1.1.5	*Ensure passcode include both uppercase and lowercase characters is set to enabled (Manual)*	
1.1.1.1.6	*Ensure passcode cannot contain consecutive characters is set to enabled (Manual)*	
1.1.1.1.7	*Ensure enhanced weak passcode detection is set to enabled (Manual)*	
1.1.1.1.8	*Ensure only allow numeric passcode is set to disabled (Manual)*	✓
1.1.1.2	*Ensure waiting room is set to enabled (Manual)*	✓
1.1.1.3	*Ensure waiting room options is set to everyone (Manual)*	✓
1.1.1.4	*Ensure require a passcode when scheduling new meetings is set to enabled (Manual)*	✓
1.1.1.5	*Ensure room meeting ID passcode is set to enabled (Manual)*	
1.1.1.6	*Ensure require a password for instant meetings is set to enabled (Manual)*	✓
1.1.1.7	*Ensure require a password for Personal Meeting ID (PMI) is set to enabled (Manual)*	✓
1.1.1.8	*Ensure embed password in meeting link for one-click join is set to enabled (Manual)*	✓
1.1.1.9	*Ensure only authenticated users can join meetings is set to enabled (Manual)*	
1.1.1.10	*Ensure require password for participants joining by phone is set to enabled (Manual)*	✓
1.1.1.11	*Ensure only authenticated users can join meetings from Web client is set to enabled (Manual)*	
1.1.2	***Schedule Meeting***	
1.1.2.1	***Meeting password requirement***	
1.1.2.1.1	*Have a minimum password length (Automated)*	*Not assessed*
1.1.2.1.2	*Specify a password length: (Automated)*	*Not assessed*
1.1.2.1.3	*Have at least 1 letter (a, b, c...) (Automated)*	*Not assessed*
1.1.2.1.4	*Have at least 1 number (1, 2, 3...) (Automated)*	*Not assessed*

No.	Controls	Implemented
1.1.2.1.5	Have at least 1 special character (!, @, #...) (Manual)	Not assessed
1.1.2.1.6	Include both uppercase and lower case letters (Automated)	Not assessed
1.1.2.2	Ensure host video is set to disabled (Manual)	✓
1.1.2.3	Ensure participants video is set to disabled (Manual)	✓
1.1.2.4	Ensure join before host is set to disabled (Automated)	✓
1.1.2.5	Ensure enable personal meeting ID is set to enabled (Manual)	✓
1.1.2.6	Ensure use personal meeting ID (PMI) when scheduling a meeting is set to disabled (Manual)	✓
1.1.2.7	Ensure use personal meeting ID (PMI) when starting an instant meeting is set to disabled (Manual)	✓
1.1.2.8	Ensure add watermark is set to enabled (Manual)	
1.1.2.9	Ensure add audio watermark is set to enabled (Manual)	
1.1.2.10	Ensure always display "Zoom Meeting" as the meeting topic is set to enabled (Manual)	
1.1.2.11	Ensure bypass the password when joining meetings from meeting list is set to enabled (Manual)	✓
1.1.2.12	Ensure mute participants upon entry is set to enabled (Manual)	
1.1.2.13	Ensure upcoming meeting reminder is set to enabled (Manual)	
1.1.3	**In Meeting (Basic)**	
1.1.3.1	**Chat**	
1.1.3.1.1	Ensure allow meeting participants to send a message visible to all participants is set to disabled (Manual)	
1.1.3.1.2	Ensure prevent participants from saving chat is set to enabled (Manual)	
1.1.3.2	**Sound notification when someone joins or leaves**	
1.1.3.2.1	Ensure sound notification when someone joins or leaves is set to enabled (Manual)	
1.1.3.2.2	Ensure play sound for "Host and co-host only" is set to enabled (Manual)	
1.1.3.2.3	Ensure when someone joins by phone, ask to record their voice to use as the notification is set to enabled (Manual)	
1.1.3.3	**File transfer**	
1.1.3.3.1	Ensure hosts and participants can send files through the in- meeting chat is set to disabled (Manual)	
1.1.3.3.2	Ensure only allow specified file types is set to enabled (Manual)	
1.1.3.4	**Screen sharing**	
1.1.3.4.1	Ensure screen sharing is set to enabled (Manual)	✓
1.1.3.4.2	Ensure "who can share?" is set to "Host Only" (Manual)	
1.1.3.4.3	Ensure "Who can start sharing when someone else is sharing?" is set to "Host Only" (Manual)	✓
1.1.3.5	**Annotation**	
1.1.3.5.1	Ensure annotation is set to disabled (Manual)	

No.	*Controls*	*Implemented*
1.1.3.5.2	*Ensure allow saving of shared screens with annotations is set to disabled (Manual)*	
1.1.3.5.3	*Ensure only the user who is sharing can annotate is set to enabled (Manual)*	
1.1.3.6	***Whiteboard***	
1.1.3.6.1	*Ensure whiteboard is set to disabled (Manual)*	
1.1.3.6.2	*Ensure allow saving of whiteboard content is set to disabled (Manual)*	
1.1.3.6.3	*Ensure auto save whiteboard content when sharing is stopped is set to disabled (Manual)*	✓
1.1.3.7	*Ensure require encryption for 3rd party endpoints (SIP/H.323) is set to enabled (Manual)*	
1.1.3.8	*Ensure allow meeting participants to send a private 1:1 message to another participant is set to disabled (Manual)*	
1.1.3.9	*Ensure auto saving chats is set to enabled (Manual)*	
1.1.3.10	*Ensure feedback to Zoom is set to enabled (Manual)*	✓
1.1.3.11	*Ensure co-host is set to enabled (Manual)*	
1.1.3.12	*Ensure polling is set to enabled (Manual)*	
1.1.3.13	*Ensure always show meeting control toolbar is set to enabled (Manual)*	
1.1.3.14	*Ensure show Zoom windows during screen share is set to enabled (Manual)*	
1.1.3.15	*Ensure disable desktop/screen share for users is set to enabled (Manual)*	
1.1.3.16	*Ensure remote control is set to disabled (Manual)*	
1.1.3.17	*Ensure nonverbal feedback is set to disabled (Manual)*	✓
1.1.3.18	*Ensure meeting reactions is set to disabled (Manual)*	
1.1.3.19	*Ensure allow removed participants to rejoin is set to disabled (Manual)*	
1.1.3.20	*Ensure allow participants to rename themselves is set to enabled (Manual)*	✓
1.1.3.21	*Ensure hide participant profile pictures in a meeting is set to disabled (Manual)*	✓
1.1.4	***In Meeting (Advanced)***	
1.1.4.1	***Select data center regions for meetings/webinars hosted by your account***	
1.1.4.1.1	*Ensure select data center regions for meetings/webinars hosted by your account is set to enabled (Manual)*	
1.1.4.1.2	*Ensure data center regions is set to local countries (Manual)*	
1.1.4.2	***Breakout room***	
1.1.4.2.1	*Ensure breakout room is set to enabled (Manual)*	
1.1.4.2.2	*Ensure allow host to assign participants to breakout rooms when scheduling is set to enabled (Manual)*	
1.1.4.3	***Virtual background***	
1.1.4.3.1	*Ensure virtual background is set to enabled (Manual)*	✓
1.1.4.3.2	*Ensure allow use of videos for virtual backgrounds is set to disabled (Manual)*	

No.	*Controls*	*Implemented*
1.1.4.3.3	*Ensure allow users to upload custom backgrounds is set to disabled (Manual)*	
1.1.4.4	***Peer to Peer connection while only 2 people in a meeting***	
1.1.4.4.1	*Ensure peer to peer connection while only 2 people in a meeting is set to disabled (Manual)*	
1.1.4.4.2	*Enable listening ports range is set as appropriate for organization (Manual)*	
1.1.4.5	*Ensure report participants to Zoom is set to enabled (Manual)*	✓
1.1.4.6	*Ensure remote support is set to disabled (Manual)*	✓
1.1.4.7	*Ensure closed captioning is set to disabled (Manual)*	✓
1.1.4.8	*Ensure save captions is set to disabled (Manual)*	✓
1.1.4.9	*Ensure far end camera control is set to disabled (Manual)*	✓
1.1.4.10	*Ensure identify guest participants in the meeting/webinar is set to enabled (Manual)*	
1.1.4.11	*Ensure auto-answer group in chat is set to disabled (Manual)*	✓
1.1.4.12	*Ensure only show default email when sending email invites is set to enabled (Manual)*	
1.1.4.13	*Ensure use HTML format email for Outlook plugin is set to enabled (Manual)*	
1.1.4.14	*Ensure show a "Join from your browser" link is set to enabled (Manual)*	
1.1.4.15	*Ensure allow live streaming meetings is set to disabled (Manual)*	✓
1.1.4.16	*Ensure allow Skype for Business (Lync) client to join a Zoom meeting is set to disabled (Manual)*	✓
1.1.4.17	*Ensure request permission to unmute is set to enabled (Manual)*	
1.1.5	***Calendar and Contacts***	
1.1.5.1	*Ensure calendar and contacts integration is set to disabled (Manual)*	✓
1.1.5.2	*Ensure ask users to integrate Office 365 calendar when they sign in is set to disabled (Manual)*	
1.1.5.3	*Ensure consent to Office 365 calendar integration permissions on behalf of entire account is set to disabled (Manual)*	✓
1.1.5.4	*Ensure enforce OAuth 2.0 for Office 365 calendar integration is set to enabled (Manual)*	
1.1.6	***Email Notification***	
1.1.6.1	***When a cloud recording is available***	
1.1.6.1.1	*Ensure when a cloud recording is available is set to enabled (Manual)*	✓
1.1.6.1.2	*Ensure Send a copy to the person who scheduled the meeting/webinar for the host is set to enabled (Manual)*	
1.1.6.1.3	*Ensure send a copy to the Alternative Hosts is set to enabled (Manual)*	
1.1.6.2	*Ensure when attendees join meeting before host is set to enabled (Manual)*	✓

No.	*Controls*	*Implemented*
1.1.6.3	*Ensure when a meeting is cancelled is set to enabled (Manual)*	✓
1.1.6.4	*Ensure when an alternative host is set or removed from a meeting is set to enabled (Manual)*	✓
1.1.6.5	*Enable when someone scheduled a meeting for a host is set to enabled (Manual)*	✓
1.1.6.6	*Ensure when the cloud recording is going to be permanently deleted from trash is set to enabled (Manual)*	
1.1.7	***Admin Options***	
1.1.7.1	*Ensure blur snapshot on iOS task switcher is set to enabled (Manual)*	✓
1.1.7.2	*Ensure display meetings scheduled for others is set to enabled (Manual)*	✓
1.1.7.3	*Ensure use content delivery network (CDN) is set to "Default" (Manual)*	✓
1.1.7.4	*Ensure allow users to contact Zoom's support via chat is set to enabled (Manual)*	✓
1.2	***Recording***	
1.2.1	***Local recording***	
1.2.1.1	*Ensure local recording is set to enabled (Manual)*	✓
1.2.1.2	*Ensure hosts can give participants the permission to record locally is set to enabled (Manual)*	✓
1.2.2	***Cloud recording***	
1.2.2.1	*Ensure cloud recording is set to enabled (Manual)*	✓
1.2.2.2	*Ensure record active speaker with shared screen is set to enabled (Manual)*	✓
1.2.2.3	*Ensure record gallery view with shared screen is set to enabled (Manual)*	
1.2.2.4	*Ensure record active speaker, gallery view and shared screen separately is set to enabled (Manual)*	
1.2.2.5	*Ensure record an audio only file is set to enabled (Manual)*	✓
1.2.2.6	*Ensure save chat messages from the meeting / webinar is set to enabled (Manual)*	✓
1.2.3	***Advanced cloud recording settings***	
1.2.3.1	*Ensure add a timestamp to the recording is set to enabled (Manual)*	
1.2.3.2	*Ensure display participants' names in the recording is set to enabled (Manual)*	✓
1.2.3.3	*Ensure record thumbnails when sharing is set to enabled (Manual)*	✓
1.2.3.4	*Ensure optimize the recording for 3rd party video editor is set to enabled (Manual)*	
1.2.3.5	*Ensure save panelist chat to the recording is set to enabled (Manual)*	
1.2.4	***Automatic recording***	
1.2.4.1	*Ensure automatic recording is set to enabled (Manual)*	
1.2.4.2	*Ensure automatic recording is set to "Record in the Cloud" (Manual)*	

No.	*Controls*	*Implemented*
1.2.4.3	*Ensure host can pause/stop the auto recording in the cloud is set to enabled (Manual)*	
1.2.5	***Cloud recording downloads***	
1.2.5.1	*Ensure cloud recording downloads is set to enabled (Manual)*	✓
1.2.5.2	*Ensure only the host can download cloud recordings is set to enabled (Manual)*	
1.2.6	***Set minimum passcode strength requirements***	
1.2.6.1	*Ensure have a minimum passcode length is set to 8 characters or greater (Manual)*	✓
1.2.6.2	*Ensure passcode have at least 1 letter is set to enabled (Manual)*	✓
1.2.6.3	*Ensure passcode have at least 1 number is set to enabled (Manual)*	✓
1.2.6.4	*Ensure passcode have at least 1 special character is set to enabled (Manual)*	✓
1.2.6.5	*Ensure allow numeric passcode is set to disabled (Manual)*	
1.2.7	*Recording disclaimer*	
1.2.7.1	*Ensure recording disclaimer is set to enabled (Manual)*	*Not assessed*
1.2.7.2	*Ensure ask participants for consent when a recording starts is set to enabled (Manual)*	*Not assessed*
1.2.7.3	*Ensure ask host to confirm before starting a recording is set to enabled (Manual)*	
1.2.8	*Ensure prevent hosts from accessing their cloud recordings is set to enabled (Manual)*	
1.2.9	*Ensure IP address access control is set to organization approved ranges (Manual)*	
1.2.10	*Ensure require passcode to access shared cloud recordings is set to enabled (Manual)*	✓
1.2.11	*Ensure the host can delete cloud recordings is set to disabled (Manual)*	
1.2.12	*Ensure allow recovery of deleted cloud recordings from trash is set to enabled (Manual)*	✓
1.2.13	*Ensure multiple audio notifications of recorded meeting is set to enabled (Manual)*	
1.3	***Telephone***	
1.3.1	*Ensure toll call is set to enabled (Manual)*	✓
1.3.2	*Ensure mask phone number in the participant list is set to enabled (Manual)*	
1.3.3	*Ensure global dial-in countries/regions is set to enabled (Manual)*	

IM Management Configuration

IM atau *Instant Messaging* merupakan fitur *chat* yang disediakan oleh *Zoom* untuk mengirim dan menerima pesan dengan pengguna lain atau di saluran tertentu dengan beberapa pengguna yang dapat mengirim dan menerima pesan dalam percakapan yang sama. Pada bagian ini, Lembaga Pelatihan XYZ hanya menerapkan tujuh atau 36,8% dari 19 kontrol konfigurasi yang direkomendasikan. Salah satu kontrol yang tidak diterapkan pada bagian ini adalah pengaturan enkripsi *chat* tingkat lanjut, padahal fitur ini dapat menjamin pesan yang

dikirim antara dua pengguna agar tidak dapat dibaca oleh pihak lainnya termasuk pihak *Zoom*.

Tabel 2. *Hasil Asesmen IM Management Configuration Menggunakan CIS Zoom Benchmark*

No.	*Controls*	*Implemented*
2	***IM Management***	
2.1	***IM Settings***	
2.1.1	***Sharing***	
2.1.1.1	*Ensure screen capture is set to disabled (Manual)*	
2.1.1.2	*Ensure code snippet is set to disabled (Manual)*	
2.1.1.3	*Ensure animated GIF images is set to disabled (Manual)*	
2.1.1.4	*Ensure file transfer is set to disabled (Manual)*	
2.1.2	***Visibility***	
2.1.2.1	*Ensure set chat as a default tab for first-time users is set to disabled (Manual)*	✓
2.1.2.2	*Ensure show H.323 contacts is set to disabled (Manual)*	✓
2.1.2.3	*Ensure company contacts is set to disabled (Manual)*	
2.1.2.4	*Ensure IM groups is set to enabled (Manual)*	
2.1.2.5	*Ensure announcements is set to disabled (Manual)*	✓
2.1.3	***Security***	
2.1.3.1	*Ensure enable advanced chat encryption is set to enabled (Manual)*	
2.1.3.2	*Ensure enable personal channel in chat window is set to disabled (Manual)*	
2.1.3.3	*Ensure allow users to add contacts is set to disabled (Manual)*	
2.1.3.4	*Ensure allow users to chat with others is set to disabled (Manual)*	
2.1.3.5	*Ensure show status to external contacts is set to disabled (Manual)*	
2.1.4	***Storage***	
2.1.4.1	*Ensure cloud storage is set to enabled (Manual)*	✓
2.1.4.2	*Ensure delete local data is set to disabled (Manual)*	✓
2.1.4.3	*Ensure store edited and deleted message revisions is set to disabled (Manual)*	✓
2.1.4.4	*Ensure third party archiving is set to disabled (Manual)*	✓
2.2	*Enable IM groups is set to the organization's needs (Manual)*	

Advanced Configuration

Advanced Configuration merupakan opsi pengaturan tingkat lanjut yang disediakan oleh *Zoom*, seperti autentikasi, kebijakan kata sandi (*Password Policy*) dan keamanan dalam rangka menaikkan level keamanan. Pada bagian ini, Lembaga Pelatihan XYZ hanya menerapkan satu atau 8,3% dari 12 kontrol yang direkomendasikan. Padahal 11 kontrol lain yang tidak diterapkan merupakan konfigurasi yang dianggap lebih penting untuk diterapkan ke dalam konfigurasi, seperti mengatur jumlah karakter minimum dalam membuat kata sandi menjadi 9 karakter atau lebih, mensyaratkan minimal

terdapat satu karakter khusus di dalam kata sandi yang akan dibuat dan kemampuan mendeteksi kata sandi yang lemah. Kebijakan penggantian kata sandi setiap 365 hari juga ada di konfigurasi ini.

Tabel 3. *Hasil Asesmen Advanced Configuration Menggunakan CIS Zoom Benchmark*

No.	*Controls*	*Implemented*
3	***Advanced***	
3.1	***Security***	
3.1.1	***Authentication***	
3.1.1.1	***Enhanced Password Requirement***	
3.1.1.1.1	*Ensure minimum password length is set to 9 characters or greater (Manual)*	
3.1.1.1.2	*Ensure password have at least 1 special character is set to enabled (Manual)*	
3.1.1.1.3	*Ensure password cannot contain consecutive characters is set to enabled (Manual)*	
3.1.1.1.4	*Ensure use enhanced weak password detection is set to enabled (Manual)*	
3.1.1.2	***Password Policy***	
3.1.1.2.1	*Ensure new users need to change their passwords upon first sign-in is set to enabled (Manual)*	
3.1.1.2.2	*Ensure password expires automatically and needs to be changed after 365 days (Manual)*	
3.1.1.2.3	*Ensure users cannot reuse any password used in the last 5 times or more (Manual)*	
3.1.1.2.4	*Enable users can change their password 1 time every 24 hours (Manual)*	
3.1.1.3	***Security***	
3.1.1.3.1	*Ensure only account admin can change licensed users' personal meeting ID and personal link name (Manual)*	
3.1.1.3.2	*Ensure allow importing of photos from the photo library on the user's device is set to disabled (Manual)*	
3.1.1.3.3	*Ensure hide billing information from administrators is set to enabled (Manual)*	
3.2	*Ensure integration is set to appropriate organizational needs (Manual)*	✓

Hasil dari asesmen menunjukkan bahwa akun *Zoom* milik Lembaga Pelatihan XYZ hanya menjalankan sebanyak 66 rekomendasi atau 40,5% dari 163 kontrol yang direkomendasikan.

PENUTUP

Berdasarkan hasil asesmen yang telah dilakukan sebagai tahap pra implementasi, dapat disimpulkan bahwa Lembaga Pelatihan XYZ belum menerapkan konfigurasi yang aman untuk akun *Zoom* yang dimilikinya dan perlu dilakukan remediasi sesuai dengan rekomendasi konfigurasi pada *CIS Zoom Benchmark* untuk menjamin keamanan penggunaan *Zoom Cloud Meeting* dari serangan siber yang mungkin terjadi.

Implementasi *CIS Zoom Benchmark* sebagai standar keamanan informasi sebaiknya tidak hanya diterapkan pada akun admin Lembaga Pelatihan XYZ, namun juga diterapkan di seluruh akun *Zoom* staf Lembaga Pelatihan XYZ yang sering melakukan konferensi video melalui *Zoom.* Penggunaan *CIS Zoom Benchmark* versi

terbaru juga harus selalu dilakukan untuk penerapan standar konfigurasi yang selalu terjaga keamanannya.

DAFTAR PUSTAKA

[1] Z. Muharir, "Dampak COVID-19 Terhadap Perekonomian Indonesia," *J. Ilm. Mhs. Ekon. Syariah*, vol. 1, no. 1, pp. 7–12, 2021.

[2] M. D. C. Pane, "Pneumonia," *Alodokter*, 2020. https://www.alodokter.com/pneumonia (accessed Nov. 26, 2021).

[3] Anonim, "Satuan Tugas Penanganan COVID-19," *Satuan Tugas Penanganan COVID-19*, 2021. https://covid19.go.id/ (accessed Nov. 11, 2021).

[4] Anonim, "COVID-19, Work From Home, dan Revolusi Industri 4.0," *DJKN Kementerian Keuangan Republik Indonesia*, 2020. https://www.djkn.kemenkeu.go.id/kpknl-parepare/baca-artikel/13058/COVID-19-Work-From-Home-dan-Revolusi-Industri-40.html (accessed Nov. 11, 2021).

[5] Anonim, "Pengguna Internet Kala WFH Corona Meningkat 40 Persen di RI," *CNN Indonesia*, 2020. https://www.cnnindonesia.com/teknologi/20200408124947-213-491594/pengguna-internet-kala-wfh-corona-meningkat-40-persen-di-ri (accessed Nov. 11, 2021).

[6] Anonim, "About Zoom," *Zoom Video Communications, Inc*. https://explore.zoom.us/en/about/ (accessed Nov. 11, 2021).

[7] Widodo, *Aspek Hukum Pidana Kejahatan Mayantara*, 1st ed. Yogyakarta: Aswaja Pressindo, 2013.

[8] G. Elmer, S. J. Neville, A. Burton, and S. Ward-Kimola, "Zoombombing During a Global Pandemic," *Soc. Media Soc.*, vol. 7, no. 3, 2021, doi: 10.1177/20563051211035356.

[9] Anonim, "Jumlah Pengguna Zoom Terus Naik meskipun Ada Isu Keamanan," *Kompas.com*, 2020. https://tekno.kompas.com/read/2020/04/25/17160067/jumlah-penggunazoom-terusnaik-meskipun-ada-isu-keamanan (accessed Nov. 11, 2021).

[10] G. O. Ulas, Ö. M. Testik, and O. Chouseinoglou, *Analysis of personal information security behavior and awareness*. Amsterdam: Elsevier, 2016.

[11] D. S. Dewi, "Mengenal Aplikasi Meeting Zoom: Fitur dan Cara Menggunakannya," *Tirto.id*, 2021. https://tirto.id/mengenal-aplikasi-meeting-zoom-fitur-dan-cara-menggunakannya-eGF7 (accessed Nov. 11, 2021).

[12] Anonim, "CIS Benchmarks™ FAQ," *Center for Internet Security*, 2020. https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq (accessed Nov. 26, 2021).

[13] M. Najib, "Implementasi Security Auditor Untuk Standardisasi Instalasi Server Pada Layanan SaaS Ecampuz Menggunakan CIS Benchmark," STMIK AKAKOM Yogyakarta, 2020.

[14] D. P. Prastika, J. Triyono, and U. Lestari, "Audit dan Implementasi CIS Benchmark Pada Sistem Operasi Linux Debian Server (Studi Kasus: Server Laboratorium Jaringan dan Komputer 6, Institut Sains & Teknologi AKPRIND Yogyakarta)," *J. JARKOM*, vol. 5, no. 2, pp. 173–183, 2019.

[15] F. Hanifah, A. Budiyono, and A. Widjajarto, "Analisa Kerentanan Pada Vulnerable Docker Menggunakan Alienvault Dan Docker Bench For Security Dengan Acuan Framework CIS Control," in *e-Proceeding of Engineering*, 2021, vol. 8, no. 5, pp. 8879–8885. [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/15914