Panduan Keamanan Pemanfaatan Aplikasi *Video Conference*:

Upaya Mencegah Penyusup dan Melindungi Data pada Rapat Virtual di Sektor Infrastruktur Kritis Nasional

Ringkasan Eksekutif

1. Sebagai implikasi merebaknya pandemik virus Corona (COVID-19) dan masifnya dampak yang ditimbulkan virus tersebut, maka beberapa aktivitas yang melibatkan banyak orang, interaksi jarak dekat dan di keramaian perlu dibatasi, dan semua lapisan masyarakat diimbau agar dapat tetap di rumah.
2. Fungsi infrastruktur kritikal nasional harus tetap berjalan selama berlangsungnya pandemik COVID-19, terutama untuk menjamin kesehatan, keselamatan, dan kesejahteraan masyarakat. Industri-industri yang ada di sektor Infrastruktur Kritis Nasional (IKN) memiliki tanggungjawab untuk tetap menjalankan fungsinya selama kondisi ini berlangsung. Pengelola pada sektor IKN dapat menyesuaikan sistem kerja melalui pelaksanaan tugas di rumah (*work from home*/WFH) dengan mempertimbangkan penetapan status darurat bencana pada daerah/lokasi infrastruktur kritis berada.
3. Dengan adanya kebijakan ini, maka diperlukan perangkat *teleworking* salah satunya *video conference* sebagai media komunikasi pertemuan jarak jauh (telekonferensi) untuk menjaga fungsi administrasi dan operasional pada sektor infrastruktur kritis tetap berjalan.
4. Berdasarkan laporan dan informasi yang BSSN himpun, terdapat beberapa celah kerawanan pada beberapa aplikasi *video conference* yang dapat mengancam keamanan data baik itu data pribadi maupun data organisasi.
5. Mengingat dan memperhatikan substansi yang disampaikan pada rapat melalui *video conference*, maka BSSN merasa perlu untuk mengeluarkan panduan keamanan dalam pemanfaatan *video conference* agar tetap menjamin keamanan dan kenyamanan selama telekonferensi berlangsung.

Pendahuluan

Untuk mencegah meluasnya penyebaran dan penularan virus COVID-19, Pemerintah Indonesia mengimbau untuk setiap lapisan masyarakat agar dapat menerapkan *social distancing* dan *physical distancing,* salah satunya melalui program *work from home* (WFH). Fungsi infrastruktur kritis sangat penting selama tanggap darurat COVID-19 untuk menjamin kesehatan, keselamatan, dan kesejahteraan masyarakat. Industri infrastruktur kritis harus tetap berjalan di tengah kondisi ini sehingga harus tetap beroperasional sebagaimana mestinya.

Sejak bulan Januari Tahun 2020, beberapa sumber melaporkan adanya peningkatan aktivitas serangan siber yang dilakukan oleh aktor jahat dengan memanfaatkan situasi wabah virus COVID-19. Aktor jahat melakukan serangan dengan menggunakan dua taktik utama untuk menargetkan korban, yaitu:

1. **Memanfaatkan Konten Bertemakan COVID-19 sebagai umpan**

   Aktor jahat menggunakan tema COVID-19 untuk membuat umpan *phising* kemudian mencuri informasi dan kredensial milik korban. Beberapa jenis malware sudah teridentifikasi melakukan hal tersebut seperti AZORult, Cerberus, Lokibot dan TrickBot. (Silahkan baca artikel Himbauan Keamanan BSSN tentang Malware COVID-19: https://bssn.go.id/analisis-spyware-coronalive1-1-apk/)

   Adapun metode distribusinya menggunakan tautan-tautan yang dikirimkan melalui platform-platform yang ada seperti e-mail, pesan instant, sms, serta situs web palsu. (silahkan baca artikel Himbauan Keamanan: https://bssn.go.id/sms-worm-corona-safety-mask-apk-aplikasi-malicious-yang-memanfaatkan-momentum-kelangkaan-masker-sebagai-alat-pelindung-diri-terhadap-covid-19/)

2. **Menyamar Sebagai Otoritas dan/atau Sumber Resmi**

   Dengan meningkatnya kekhawatiran terhadap COVID-19, dimungkinkan munculnya aktor jahat yang menyamar sebagai pejabat dari Lembaga Pemerintah, terutama Instansi yang bertugas dalam Gugus Tugas Penanggulangan COVID-19 untuk meminta informasi tertentu. Taktik ini terutama memanfaatkan informasi-informasi resmi yang dikeluarkan oleh Instansi terkait seperti infografis, press-release, grafik, dll yang digunakan sebagai umpan phising. Organisasi Kesehatan Dunia (WHO) dilaporkan telah ditargetkan oleh kelompok APT yang membuat website palsu untuk mengelabuhi pegawai internal WHO dalam rangka mencuri data [3].

   Untuk meningkatkan kewaspadaan dan kesiapan dalam menanggulangi insiden siber, Deputi III BSSN telah membuat Buku Putih Mitigasi Insiden Siber saat Pandemi COVID-19 (silahkan baca artikel disini : https://bssn.go.id/buku-putih-mitigasi-insiden-siber-saat-pandemi-covid-19/)

Terkait dengan hal tersebut, sebagai instansi Pemerintah yang bertugas di bidang keamanan siber dan keamanan informasi, BSSN melihat ada hal yang perlu menjadi perhatian serius dalam pelaksanaan telekonferensi tersebut, yaitu bagaimana sarana yang digunakan dan informasi yang dikomunikasikan dengan menggunakan media *video conference* tetap memperhatikan aspek keamanan dan kenyamanan.

Panduan ini dimaksudkan untuk mendukung stakeholder pada sektor IKN dalam memanfaatkan *video conference* yang aman guna mempertahankan operasional layanan dan fungsinya selama adanya *social distancing* dan *physical distancing* akibat pandemik COVID-19.

Ruang Lingkup

Panduan ini berisi langkah-langkah yang dapat menjadi acuan bagi sektor Infrastruktur Kritis Nasional dalam penyelenggaraan pertemuan jarak jauh (telekonferensi) melalui video conference dengan tetap memperhatikan keamanan informasi. Hal-hal yang dimuat dalam pedoman sebagai berikut:

1. Penyiapan Sarana *Video Conference;*
2. Informasi yang dapat disampaikan;
3. Pengamanan *Video Conference;*
4. *Best Practice* untuk *Video Conference* yang Efektif
    a. Tips sebelum memulai pertemuan;dan
    b. Selama pertemuan;

#1 PENYIAPAN SARANA VIDEO CONFERENCE

Sarana video conference yang perlu disiapkan meliputi aplikasi video conference, perangkat komunikasi, dan jaringan yang digunakan. Kesiapan perangkat untuk memastikan penyelenggaraan video conference berlangsung efektif dan aman.

Aplikasi Video Conference

1. Gunakan aplikasi *video conference* yang resmi/berlanggaran dan merupakan versi terbaru dan diunduh dari sumber resmi.
2. Disarankan *server* aplikasi berada pada organisasi pengguna dan dikelola secara mandiri (*on-premise*), atau jika belum demikian agar menggunakan aplikasi dengan pengelolaan *server* berada di dalam wilayah Indonesia.
3. Jika server aplikasi berada di dalam organisasi sebaiknya dikonfigurasi untuk jaringan local dan setiap partisipan yang ingin bergabung wajib memiliki akses VPN.
4. Gunakan aplikasi yang salah satunya memiliki fitur enkripsi, *end-to-end encryption*, *private chat, link communication*, atau sejenisnya dan dapat diaktifkan pada saat telekonferensi berlangsung.
5. Pilih aplikasi yang memiliki fitur ‘pembatasan’ pada saat seluruh partisipan telah bergabung di *conference*, untuk menghindari pengguna lain masuk tanpa ada konfirmasi terlebih dahulu.
6. Agar dipastikan *ID, PIN atau Password* selalu diperbarui dan diganti setiap pelaksanaan *meeting*.
7. Pastikan akun yang digunakan adalah akun resmi dinas atau akun milik pribadi, bukan milik orang lain.
8. Pastikan *Profile Name* sesuai dengan ketentuan yang disepakati sehingga mempermudah untuk melakukan kontrol terhadap partisipan yang tergabung.
9. Pastikan aplikasi video conference meminta izin ketika mengaktifkan kamera atau mikrofon, dan pastikan tidak ada permintaan akses kamera atau mikrofon yang tersembunyi.

Perangkat Komunikasi

Sisi Host:

1. Gunakan kata kunci yang kuat (minimal 8 karakter kombinasi huruf besar kecil dan karakter khusus) untuk *password meeting.*

2. Identitas dan *password meeting* didistribusikan secara aman kepada partisipan, tidak secara publik.
3. Jika ada, aktifkan fitur 'pembatasan' pada saat seluruh partisipan telah bergabung di *conference*, untuk menghindari pengguna lain masuk tanpa ada konfirmasi terlebih dahulu.
4. Pastikan identitas pertemuan dan *password meeting* selalu diperbarui dan diganti setiap pelaksanaan *meeting*.
5. Lakukan monitoring dan verifikasi terhadap setiap partisipan yang telah dan akan bergabung pada *Conference*.

Sisi Client:

1. Gunakan perangkat milik dinas atau milik pribadi untuk kegiatan *video conference*
2. Pastikan sistem operasi resmi versi terbaru sudah terinstal di perangkat yang digunakan.
3. Pastikan perangkat yang digunakan sudah terpasang antivirus/antimalware dan diperbaharui secara berkala.
4. Pastikan akun yang digunakan adalah akun resmi dinas atau akun milik pribadi, bukan milik orang lain.
5. Pastikan *Profile Name* sesuai dengan ketentuan yang disepakati sehingga mempermudah untuk melakukan kontrol terhadap partisipan yang tergabung.
6. Pastikan untuk berkoordinasi dengan Host apakah terdapat beberapa *settings*/pengaturan dan konfigurasi yang harus dilakukan terhadap sistem operasi dan aplikasi *video conference.*
7. Laksanakan kegiatan *video conference* di tempat atau ruangan yang situasinya kondusif.
8. Tidak mengunggah tangkapan layar telekonferensi yang menampilkan meeting ID, nama peserta atau informasi yang dianggap terbatas lainnya.

Lingkungan Kerja

1. Pastikan lingkungan kerja yang digunakan untuk melakukan telekonferensi tidak terdapat hal-hal yang sensitif atau terbatas seperti, catatan-catatan yang ditulis pada papan tulis yang menjadi *background* kita, dokumen-dokumen berklasifikasi yang masuk ke dalam jangkauan kamera, atau ruangan-ruangan lain yang juga masuk ke dalam jangkauan kamera.
2. Jika rapat tersebut merupakan rapat terbatas, pastikan tidak ada orang lain yang tidak berkepentingan masuk ke ruangan atau melihat secara langsung tampilan layar.

Jaringan

1. Pastikan untuk menggunakan jaringan internet pribadi atau jaringan internet yang terpercaya (*trusted*).
2. Agar tidak menggunakan jaringan internet untuk publik atau yang terpasang di tempat-tempat umum, seperti café, mal, atau restoran.

3. Sangat disarankan untuk menggunakan jaringan yang sudah dilengkapi dengan perangkat atau aplikasi *Virtual Private Network* (VPN) resmi/berlangganan.
4. Pastikan ketersediaan *bandwidth* yang tercukupi selama conference berlangsung.
5. Siapkan rencana komunikasi cadangan jika terjadi permasalahan, misalnya meminta partisipan untuk tetap terhubung melalui *tools* lainnya yang disepakati.

#2 PANDUAN INFORMASI BERKLASIFIKASI YANG DIKOMUNIKASIKAN

Bagian ini berisikan mengenai rekomendasi terhadap subtansi informasi yang sebaiknya tidak disampaikan selama berada dalam *video conference*. Hal ini terkait dengan sensitifitas informasi yang berisiko ketika disampaikan secara *online* atau bukan untuk konsumsi publik. Berikut adalah hal-hal yang harus diperhatikan secara teknis dan substansi:

Sisi Teknis

1. Umumnya, aplikasi merupakan aplikasi berbasis *cloud* dimana *server* dikelola oleh perusahaan pengelola aplikasi atau pihak ketiga, maka pemanfaatan aplikasi untuk telekonferensi disarankan untuk koordinasi yang sifatnya umum dan **bukan** untuk koordinasi informasi yang sifatnya berklasifikasi**.**
2. Hapus riwayat percakapan yang dinilai berklasifikasi dan pastikan tidak tersimpan dalam *database* aplikasi.
3. Gunakan mekanisme enkripsi atau kata kunci untuk data atau rekaman rapat telekonferesi yang akan disimpan baik pada media penyimpanan berbasis *cloud* maupun pada perangkat masing-masing.

Sisi Substansi

1. Pastikan kebenaran informasi yang akan disampaikan dan perhatikan kapasitas partisipan sebagai pemilik dan pengirim informasi
2. Untuk informasi yang sifatnya terbatas dan memang perlu diketahui oleh anggota organisasi/unit kerja yang tergabung dalam telekonferensi, maka pastikan partisipan menyampaikan kata '**TERBATAS**' sebelum menyampaikan informasi tersebut.
3. Semua partisipan *video conference* harus bertanggung jawab terhadap informasi yang diterima atau disampaikan melalui sarana telekonferensi ini.
4. Selalu memperhatikan peraturan perundang-undangan yang berkaitan dengan klasifikasi informasi dan peraturan perundang-undangan tentang informasi dan transaksi elektronik.

#3 Langkah-langkah Mengamankan Video Conference

Informasi rahasia dan sensitif sering dibahas dalam rapat. Pengungkapan informasi kepada orang yang salah dengan cara yang salah dapat mengakibatkan pelanggaran terhadap regulasi seperti perlindungan data.

Berikut beberapa langkah untuk melakukan *video conference* dengan aman:

1. **Prioritaskan keamanan jaringan**
   End point dan *platform* video conference sering membutuhkankan *Session Boarder Controller* (SBC) untuk mengatur traffic, termasuk mencari dan memblok koneksi mencurigakan. Pastikan aplikasi yang digunakan memiliki fitur SBC ini, selanjutnya lakukan pengaturan jaringan perlu di-*review* secara teratur untuk memastikan selalu *up to date*.

2. **Pentingnya penggunaan enkripsi**
   Bersama dengan keamanan jaringan, enkripsi merupakan hal yang mutlak bagi *video conference*. Algoritma standar untuk video conference saat ini adalah AES 128 bit. Pastikan aplikasi yang digunakan minimal telah memiliki fitur enkripsi tersebut.

3. **Lindungi diri dengan "Permission"**
   Tidak semua kebocoran data terjadi karena *hacker* yang masuk kedalam sistem. Masalah keamanan dapat terjadi jika ada orang yang tidak berkepentingan dengan secara tidak sengaja diberi akses komunikasi yang seharusnya tidak dilihat misalnya karena tidak mendapatkan pengaturan yang benar. Oleh karenanya pastikan setiap peserta rapat yang diundang mendapatkan *permission* yang dikirim melalui jalur yang aman.

4. **Buat dan patuhi kebijakan untuk *video conference***
   Jaringan yang aman dan enkripsi tidak akan berdampak besar pada keamanan *video conference* jika SDM yang menggunakan tidak memahami budaya keamanan. Kesalahan manusia (*human error*) merupakan penyebab terbesar terjadinya kebocoran data. Untuk itu perlu dibuat kebijakan/policy yang diantaranya mengatur bagaimana menggunakan sistem, bagaimana menggunakan perangkat mobile dan remote secara aman, hingga informasi apa saja yang dapat disampaikan pada saat *teleworking* (salah satu referensi yang dapat digunakan adalah NIST SP 800-46 Revisi 2)

#4 *Best Practices* untuk Video Conference yang Efektif

Untuk membuat rapat melalui video conference yang lebih produktif dan efektif, dapat dilakukan hal-hal berikut:

Sebelum rapat video conference:

1. Ketika menggunakan peralatan atau lokasi yang tidak biasa, lakukan pengujian koneksi sebelum rapat
2. Jika mungkin, buat koneksi video conference beberapa menit sebelum mulai rapat.
3. Pastikan setiap peserta rapat telah mendapatkan *permission* untuk bergabung pada *video conference*.
4. Buat rencana komunikasi cadangan jika terjadi permasalahan koneksi, misalnya meminta peserta/partisipan untuk tetap terhubung melalui laptop, menggunakan mobile atau speakerphone, dan/atau bekolaborasi melalui *tool* kolaborasi online.

5. Pastikan persyaratan keamanan telah terpenuhi seperti yang dijelaskan pada bab 1 sampai 3.

Selama rapat *video conference* berlangsung:

1. Minta semua peserta membagikan tampilan video dan audio.
2. Minta peserta mematikan mikropon jika lokasinya memiliki *noise* atau jika tidak sedang berbicara.
3. Diperlukan fasilitator rapat yang akan menyampaikan agenda rapat dan mengatur jalannya rapat.
4. Pastikan semua peserta memperoleh akses yang sama terhadao konten yang dibagikan selama *video conference* dan menggunakan *tools* online jika mungkin.
5. Batasi penggunaan berbagi layar, pastikan fitur berbagi layer dapat dikontrol oleh admin. Hal ini bertujuan untuk menghindari adanya peserta rapat yang berbagi layar yang tidak dibutuhkan.

Referensi

1) https://www.nist.gov/blogs/cybersecurity-insights/preventing-eavesdropping-and-protecting-privacy-virtual-meetings diakses pada tanggal 6 April 2020

2) https://www.nist.gov/blogs/cybersecurity-insights/telework-security-basics diakses pada tanggal 6 April 2020

3) https://threatpost.com/who-attacked-possible-apt-covid-19-cyberattacks-double/154083/

4) https://www.us-cert.gov/ncas/current-activity/2020/04/02/fbi-releases-guidance-defending-against-vtc-hijacking-and-zoom

5) https://uit.stanford.edu/videoconferencing/best-practices

6) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

Riwayat Dokumen

Versi 1.0 : 7 April 2020

Ditandatangani secara elektronik oleh:
DIREKTUR PROTEKSI INFRASTRUKTUR INFORMASI KRITIKAL NASIONAL, DEPUTI II

NUR ACHMADI SALMAWAN, S.Kom., M.M.
NIP. 19700901 199110 1 001