ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CASERTA

VERBALE DI RIUNIONE

DEL CONSIGLIO DIRETTIVO

		Anno	2020
Verbale nr.	8	***Data***	15/04/2020
Convocazione	Prot. n. 757/2020	***Del***	08/04/2020
Su richiesta	Presidente del Consiglio dell'Ordine		
Sede riunione	Sala Consiglio dell'Ordine	***Inizio***	Ore 16:20
		Fine	Ore 20:00

		Presente	***Assente***	***Entra***	***Esce***
Presidente	Dott. Ing. **Vitelli** Massimo	X			
Segretario	Ing. **Gentile** Fabrizio	X			
Tesoriere	Ing. **De Chiara** Federico	X			
Vice Presidente v.	Ing. **Motti** Ottavio	X			
Vice Presidente a.	Ing. **Di Leva Antonio**	X			

N.	***Consigliere***	***Presente***	***Assente***	***Entra***	***Esce***
1	**Chianese** Raffaele	X			
2	**De Lisa** Vincenzo	X			
3	**Ferrante** Adele	X			
4	**Maiorino** Rosa		X		
5	**Manzella** Antonio	X			
6	**Mascolo** Manlio		X		
7	**Pezone** Antonio	X		16:33	
8	**Polito** Tiziano	X			
9	**Ranucci** Antonio	X		17:38	
10	**Raucci** Carlo	X			17:10

Alle ore 16:20 il Presidente, costatata la presenza del numero legale, essendo presenti n. 13 Consiglieri su n. 15, dichiara aperta la riunione del Consiglio.
Verbalizza il Segretario, Ing. **Gentile** Fabrizio.

Via Sant'Antonio da Padova, 1
81100 – CASERTA (CE)
ordine@ingegneri.caserta.it
PEC: ordine@ordingce.it
Tel: 0823.326.767
Tel: 0823.555.984

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CASERTA

ESITI DELLA RIUNIONE

Punto n.	**1**

APPROVAZIONE DEL VERBALE DELLA SEDUTA PRECEDENTE

Il Segretario, Ing. Gentile, legge il verbale della seduta del 06 / 04 /2020

Esiti:

Il consiglio approva il verbale della seduta precedente.

"Il consigliere Raucci chiede di mettere a verbale la seguente motivazione di cui al voto contrario: Vorrei far presente che anche per la seduta odierna come per quelle precedenti viene utilizzato il software Microsoft Teams nella versione gratuita senza che questo ordine abbia acquistato nessuna licenza. Tale modalità di utilizzo genera dubbi sull'effettiva sussistenza di idonei parametri di sicurezza in grado di assicurare la segretezza delle sedute come previsto dal regolamento interno di funzionamento del consiglio. A questo proposito l'Ordine non ha fornito nessun documento sulle specifiche del software e sulla idoneità del software a garantire la riservatezza della seduta a tutela dei dati personali e la difesa da possibili attacchi informatici. Inoltre, non è stato predisposto alcuna modalità di tracciabilità di adesione e approvazione del verbale da parte dei presenti. In attesa pertanto che sia verificata e documentata l'effettiva idoneità del software Microsoft teams nella versione gratuita a soddisfare le prescrizioni puntualmente riportate nell'art. 5.10 del regolamento interno del consiglio chiedo il rinvio della seduta di consiglio."

Alle ore 16: 33 entra il consigliere in PEZONE.

Il consigliere ing POLITO a tal proposito allega il documento seguente.

Sicurezza e Microsoft Teams

Microsoft Teams, come parte del servizio Microsoft 365 (M365), segue tutte le migliori pratiche e procedure di sicurezza, come la protezione a livello di servizio attraverso difesa in profondità, controlli utente nell'ambito del servizio, potenziamento delle misure di sicurezza e best practice operative. Per i dettagli completi, consultare il Centro protezione Microsoft.

Affidabilità da progettazione

Teams è progettato e sviluppato in conformità con Microsoft Trustworthy Computing Security Development Lifecycle (SDL) descritto in Microsoft Security Development Lifecycle (SDL). Il primo passo verso la creazione di un sistema di comunicazioni unificato più sicuro è stato quello di progettare modelli di minacce e testare ciascuna funzionalità così come era stata progettata. Ulteriori miglioramenti relativi alla protezione venivano apportati durante il processo e le procedure di codifica. Gli strumenti della fase di compilazione rilevano sovraccarichi del buffer e altre potenziali minacce alla sicurezza prima che il codice venga archiviato nel prodotto finale. Naturalmente, è impossibile progettare un prodotto che sia al sicuro da tutte le possibili minacce alla protezione. Nessun sistema è in grado di garantire una sicurezza totale. Tuttavia, poiché lo sviluppo del prodotto ha accolto principi di progettazione sicuri fin dall'inizio, Teams incorpora tecnologie di protezione standard del settore come parte fondamentale della sua architettura.

Affidabilità per impostazione predefinita

Le comunicazioni di rete in Teams sono crittografate per impostazione predefinita. Richiedendo a tutti i server di utilizzare certificati e utilizzando OAUTH, TLS, SRTP (Secure Real-Time Transport Protocol) e altre tecniche di crittografia standard del settore, inclusa la crittografia AES (Advanced Encryption Standard) a 256 bit, tutti i dati di Teams sono protetti sulla rete.

In che modo Teams tratta le minacce alla sicurezza comuni

Questa sezione identifica le più comuni minacce alla sicurezza del servizio Teams e come Microsoft riduce ciascun pericolo.

Attacco basato su chiave compromessa

Teams utilizza le funzionalità PKI nel sistema operativo del Server Windows per proteggere i dati della chiave utilizzati per la crittografia nelle connessioni TLS (Transport Layer Security). Le chiavi utilizzate per la crittografia dei file multimediali vengono scambiate tramite le connessioni TLS.

Attacco Denial-of-Service di rete

L'attacco Denial-of-Service si verifica quando l'utente malintenzionato impedisce il normale utilizzo e funzionamento della rete da parte di utenti validi. Utilizzando un attacco Denial-of-Service, l'utente malintenzionato può:

- Inviare dati non validi alle applicazioni e ai servizi in esecuzione nella rete attaccata per interromperne la normale funzione.
- Inviare una grande quantità di traffico, sovraccaricando il sistema fino a quando non smette di rispondere o risponde lentamente alle richieste legittime.
- Nascondere l'evidenza degli attacchi.
- Impedire agli utenti di accedere alle risorse di rete. Teams attenua questi attacchi eseguendo la protezione di rete DDOS di Azure e limitando le richieste dei client dagli stessi endpoint, subnet e entità federate.

Intercettazione

L'intercettazione può verificarsi quando un utente malintenzionato accede al percorso dei dati in una rete e ha la capacità di monitorare e leggere il traffico. Si chiama anche sniffing o snooping. Se il traffico è in testo normale, l'utente malintenzionato può leggerlo quando accede al percorso. Un esempio è un attacco eseguito controllando un router sul percorso dei dati.
Teams utilizza Mutual TLS (MTLS) per le comunicazioni del server all'interno di O365 e TLS dai client al servizio, rendendo questo attacco molto difficile da raggiungere nel periodo di tempo in cui una determinata conversazione potrebbe essere attaccata. TLS autentica tutte le parti e crittografa tutto il traffico. Ciò non impedisce l'intercettazione, ma l'utente malintenzionato non può leggere il traffico a meno che la crittografia non sia interrotta.
Il protocollo TURN viene utilizzato per scopi multimediali in tempo reale. Il protocollo TURN non impone la crittografia del traffico e le informazioni che invia sono protette dall'integrità del messaggio. Sebbene sia aperto alle intercettazioni, le informazioni che invia (cioè gli indirizzi IP e la porta) possono essere estratte direttamente, guardando semplicemente gli indirizzi di origine e destinazione dei pacchetti. Il servizio Teams garantisce che i dati siano validi controllando l'Integrità del Messaggio tramite la chiave derivata da alcune voci, inclusa una password TURN, che non viene mai inviata non crittografata. SRTP viene utilizzato per il traffico multimediale ed è inoltre crittografato.

Spoofing d'identità (spoofing dell'indirizzo IP)

Lo spoofing si verifica quando l'utente malintenzionato determina e utilizza un indirizzo IP di una rete, un computer o un componente di rete senza essere autorizzato a farlo. La riuscita dell'attacco consente all'utente malintenzionato di operare come se tale utente malintenzionato fosse l'entità normalmente identificata dall'indirizzo IP.
TLS autentica tutte le parti ed esegue la crittografia di tutto il traffico. L'uso di TLS impedisce all'autore di un attacco di effettuare lo spoofing dell'indirizzo IP su una connessione specifica (ad esempio, connessioni Mutual TLS). Un utente malintenzionato può comunque falsificare l'indirizzo del server DNS. Tuttavia, poiché l'autenticazione in Teams viene eseguita con certificati, un utente malintenzionato non avrebbe un certificato valido richiesto per falsificare una delle parti nella comunicazione.

Attacco man-in-the-middle

Un attacco man-in-the-middle si verifica quando un utente malintenzionato dirige la comunicazione tra due utenti attraverso il proprio computer senza che i due utenti comunicanti lo sappiano. L'utente malintenzionato può monitorare e leggere il traffico prima di inviarlo al destinatario previsto. Ogni utente della comunicazione, inconsapevolmente, invia e riceve traffico dall'utente malintenzionato, il tutto pensando di comunicare solo con l'utente previsto. Ciò può accadere se un utente malintenzionato riesce a modificare i Servizi di Dominio di Active Directory per aggiungere il proprio server come server attendibile, o modificare il DNS (Domain Name System) per consentire ai client di connettersi tramite l'utente malintenzionato nel percorso verso il server.
Per impedire gli attacchi man-in-the-middle al traffico multimediale tra due endpoint che partecipano alla condivisione di audio, video e applicazioni di Teams è necessario crittografare il flusso multimediale con il protocollo SRTP. Le chiavi crittografiche vengono negoziate tra i due endpoint attraverso un protocollo di segnalazione proprietario (protocollo Teams Call Signaling), che sfrutta il canale UDP/TCP crittografato con TLS 1.2 e AES-256 (in modalità GCM).

Attacco di riproduzione RTP

Un attacco di riproduzione si verifica quando una trasmissione di file multimediali valida tra due parti viene intercettata e ritrasmessa per scopi illeciti. Teams utilizza SRTP in combinazione con un protocollo di segnalazione sicuro che protegge le trasmissioni dagli attacchi di ripetizione, abilitando il destinatario a mantenere un indice dei pacchetti RTP già ricevuti e confrontare ogni nuovo pacchetto con quelli già elencati nell'indice.

Messaggi istantanei indesiderati

Gli spim sono messaggi istantanei commerciali non desiderati o richieste di sottoscrizione di presenza, come spam, ma sotto forma di messaggio istantaneo. Sebbene non sia di per sé una compromissione della rete, è quanto meno fastidioso, può ridurre la disponibilità e la produzione delle risorse e può comportare una compromissione della rete. Un esempio di ciò è lo spimming reciproco degli utenti che si inviano richieste. Gli utenti possono bloccarsi a vicenda per impedirlo, ma con la federazione, se si stabilisce un attacco spim coordinato, può essere difficile da superare a meno che non si disabiliti la federazione per il partner.

Virus e worm

Un virus è un'unità di codice il cui scopo è riprodurre unità di codice aggiuntive e simili. Per funzionare, un virus ha bisogno di un host, come un file, un'e-mail o un programma. Come un virus, un worm è un'unità di codice, codificata per riprodurre unità di codice aggiuntive e simili, ma che, a differenza di un virus, non ha bisogno di un host. Virus e worm si manifestano principalmente durante i trasferimenti di file tra client, quando gli URL vengono inviati da altri utenti. Se un virus si trova sul computer, può, ad esempio, utilizzare l'identità dell'utente e inviare messaggi istantanei per suo conto. Le migliori pratiche standard di protezione del client, come la scansione periodica alla ricerca di virus, possono mitigare questo problema.

Framework di sicurezza di Teams

Questa sezione offre una panoramica degli elementi fondamentali che formano il framework di sicurezza di Microsoft Teams.
Gli elementi principali sono:

- Azure Active Directory (AAD), che fornisce un singolo repository back-end attendibile per gli account utente. Le informazioni sul profilo utente vengono archiviate in AAD attraverso le azioni di Microsoft Graph.
  - Tenere presente che potrebbero essere presenti più token emessi, visibili se si esegue il monitoraggio del traffico di rete. Sono inclusi i token Skype, di cui potrebbero essere visibili tracce mentre si osserva il traffico audio e chat.
- TLS (Transport Layer Security) e Mutual TLS (MTLS) che eseguono la crittografia del traffico dei messaggi istantanei e abilitano l'autenticazione degli endpoint. I flussi audio, video e di condivisione di applicazioni da punto a punto sono crittografati e la relativa integrità è verificata utilizzando il protocollo SRTP (Secure Real-Time Transport Protocol). Nella traccia potrebbe essere visibile anche traffico OAuth, specialmente relativo alle autorizzazioni di negoziazione quando si passa da una scheda all'altra in Teams, ad esempio per passare da Post a File. Per un esempio del flusso OAuth per le schede, vedere il documento.
- Teams usa protocolli standard del settore per l'autenticazione degli utenti, ove possibile.

Nelle sezioni successive vengono illustrate alcune di queste tecnologie principali.

Azure Active Directory

Azure Active Directory funziona come servizio directory per Office 365 (O365). Archivia tutte le informazioni della directory degli utenti e le assegnazioni dei criteri.

Punti di distribuzione CRL

Il traffico di Office 365 avviene su canali crittografati TLS/HTTPS, ossia vengono usati certificati per la crittografia di tutto il traffico. Teams richiede che tutti i certificati del server contengano uno o più punti di distribuzione dell'elenco di revoche di certificati (CRL). I punti di distribuzione CRL (CDP) sono posizioni da cui è possibile scaricare i CRL per verificare che il certificato non sia stato revocato dal momento in cui è stato rilasciato e che rientri ancora nel periodo di validità. Un punto di distribuzione CRL è indicato nelle proprietà del certificato come URL ed è HTTP protetto. Il servizio Teams controlla il CRL con ogni autenticazione del certificato.

Utilizzo delle chiavi avanzato

Tutti i componenti del servizio Teams richiedono che tutti i certificati del server supportino l'utilizzo chiavi avanzato (EKU, Enhanced Key Usage) ai fini dell'autenticazione del server. La configurazione del campo EKU per l'autenticazione del server indica che il certificato è valido ai fini dell'autenticazione dei server. Tale EKU è essenziale per MTLS.

TLS e MTLS per Teams

I protocolli TLS e MTLS forniscono comunicazioni crittografate e autenticazione degli endpoint su Internet. Teams utilizza questi due protocolli per creare la rete di server affidabili e per garantire che tutte le comunicazioni su quella rete siano crittografate. Tutte le comunicazioni tra server si verificano su MTLS. Le comunicazioni SIP rimanenti o legacy da client a server si verificano su TLS.

TLS consente agli utenti, tramite il proprio software client, di autenticare i server Teams a cui si connettono. In una connessione TLS, il client richiede un certificato valido dal server. Per essere valido, il certificato deve essere stato emesso da una CA che sia considerata affidabile anche dal client e il nome DNS del server deve corrispondere al nome DNS sul certificato. Se il certificato è valido, il client utilizza la chiave pubblica nel certificato per crittografare le chiavi di crittografia simmetriche da utilizzare per la comunicazione, quindi solo il proprietario originale del certificato può utilizzare la propria chiave privata per decrittografare il contenuto della comunicazione. La connessione risultante è affidabile e da quel momento non viene contestata da altri server o client affidabili.

Le connessioni tra server si basano su TLS reciproco (MTLS) per l'autenticazione reciproca. Su una connessione MTLS, il server che genera un messaggio e il server che lo riceve si scambiano i certificati da una CA reciprocamente attendibile. I certificati dimostrano l'identità di ciascun server all'altro. Nel servizio Teams, questa procedura è seguita.

TLS e MTLS consentono di impedire sia gli attacchi di intercettazione sia gli attacchi man-in-the-middle. In un attacco man-in-the-middle, l'utente malintenzionato dirige le comunicazioni tra due entità di rete attraverso il computer dell'utente malintenzionato all'insaputa delle due parti. Le specifiche di TLS e Teams di server attendibili attenuano il rischio di un attacco man-in-the-middle parzialmente sul livello dell'applicazione, utilizzando la crittografia coordinata, tramite la crittografia a chiave pubblica tra i due endpoint. Un utente malintenzionato dovrebbe avere un certificato valido e affidabile con la chiave privata corrispondente ed emesso a nome del servizio con cui il client sta comunicando per decrittografare la comunicazione.

Nota

I dati dei team vengono crittografati durante il transito e quando vengono archiviati. Microsoft usa le tecnologie standard del settore, come TLS e SRTP, per crittografare tutti i dati in transito tra i dispositivi degli utenti e i data center Microsoft e tra gli stessi data center Microsoft. Sono inclusi i messaggi, i file, le riunioni e altri contenuti. Vengono crittografati anche i dati aziendali archiviati nei data center Microsoft, in modo da consentire alle organizzazioni di decrittografare i contenuti, se necessario, per rispettare gli obblighi di sicurezza e conformità, ad esempio eDiscovery.

Crittografia di Teams

Teams utilizza TLS e MTLS per crittografare i messaggi istantanei. Tutto il traffico da server a server richiede lo standard MTLS, indipendentemente dal fatto che il traffico sia confinato alla rete interna o che attraversi il perimetro della rete interna.

In questa tabella sono riepilogati i protocolli usati da Teams.

Crittografia del traffico

Tipo di traffico
Da server a server
Da client a server (ad esempio, messaggistica istantanea e presenza)
Flussi multimediali (ad esempio, condivisione audio e video di contenuti multimediali)
Condivisione audio e video di contenuti multimediali
Segnalazione

Crittografia file multimediali

Il traffico di file multimediali viene crittografato tramite Secure RTP (SRTP), un profilo di Real-Time Transport Protocol (RTP) che offre riservatezza, autenticazione e protezione dagli attacchi di riproduzione al traffico RTP. SRTP utilizza una chiave della sessione generata utilizzando un generatore di numeri casuali sicuro e scambiata utilizzando il canale di segnalazione TLS. Il traffico dei contenuti multimediali tra client viene negoziato attraverso una connessione tra client e server, ma è crittografato con SRTP quando si passa direttamente da client a client.

Teams utilizza un token basato su credenziali per proteggere l'accesso ai contenuti multimediali inoltrati tramite TURN. I contenuti multimediali inoltrano lo scambio del token a un canale protetto tramite TLS.

FIPS

Teams utilizza algoritmi FIPS (Federal Information Processing Standard) per gli scambi di chiavi di crittografia. Per altre informazioni sull'implementazione di FIPS, vedere Pubblicazione Federal Information Processing Standard (FIPS) 140-2.

Autenticazione utente e client

Un utente affidabile è un utente le cui credenziali sono state autenticate da AAD in Office 365/Microsoft 365.

L'autenticazione è il provisioning delle credenziali utente a un server o servizio attendibile. Teams utilizza i seguenti protocolli di autenticazione, a seconda dello stato e della posizione dell'utente.

- **Autenticazione moderna (MA)** è l'implementazione Microsoft di OAUTH 2.0 per le comunicazioni da client a server. Offre funzionalità di sicurezza come l'autenticazione a più fattori e l'accesso condizionale di O365. Per usare MA, sia il tenant online sia i client devono essere abilitati per MA. Tutti i client di Teams su PC e dispositivi mobili, oltre al client Web, supportano MA.

Nota

Se è necessario rispolverare i metodi di autenticazione e autorizzazione di Azure Active Directory, l'introduzione di questo articolo e le sezioni "Informazioni di base sull'autenticazione in Azure AD" possono essere d'aiuto.

L'autenticazione di Teams viene eseguita tramite AAD e OAuth. Il processo di autenticazione può essere semplificato per:

- Accesso utente > Emissione di token > richiesta successiva per usare il token emesso.

Le richieste da client a server sono autenticate e autorizzate tramite AAD mediante l'uso di OAuth. Gli utenti con credenziali valide emesse da un partner federato sono considerati attendibili ed è possibile eseguire lo stesso processo come utenti nativi. Tuttavia, gli amministratori potrebbero applicare ulteriori limitazioni.

Per l'autenticazione dei contenuti multimediali, anche i protocolli ICE e TURN usano la challenge Digest come descritto nell'RFC su TURN di IETF.

Strumenti di gestione di Windows PowerShell e Teams
In Teams, gli amministratori IT possono gestire il proprio servizio tramite il portale di amministrazione di O365 o utilizzando TRPS (Tenant Remote PowerShell). Gli amministratori del tenant usano l'autenticazione moderna per eseguire l'autenticazione in TRPS.
Configurazione dell'accesso a Teams entro il limite Internet
Affinché Teams funzioni correttamente (affinché gli utenti riescano a partecipare alle riunioni e così via), i clienti devono configurare il proprio accesso Internet in modo tale che il traffico UDP e TCP in uscita verso i servizi nel cloud Teams sia consentito. Per ulteriori dettagli, vedere URL e intervalli di indirizzi IP di Office 365.
UDP 3478-3481 e TCP 443
Le porte UDP 3478-3481 e TCP 443 vengono utilizzate dai client per richiedere il servizio per i contenuti audiovisivi. Un client utilizza queste due porte per allocare rispettivamente le porte UDP e TCP e consentire questi flussi multimediali. I flussi multimediali su queste porte sono protetti con una chiave che viene scambiata su un canale di segnalazione protetto con TLS.
UDP/TCP 50.000–59.999 (facoltativo)
Le porte nell'intervallo alto non usano Transport Relay. Poiché si tratta di porte facoltative, non sono disponibili negli intervalli di indirizzi IP e URL di Office 365. Ciò significa anche che Teams funzionerà anche se queste porte sono bloccate, poiché il traffico usa gli intervalli di porte 3478-3481 (Transport Relay). Vengono usate per il transito dei contenuti multimediali, ma anche se questi intervalli sono sbloccati, la riduzione del ritardo sarà minima (qualche millisecondo). Nella maggior parte dei casi, i problemi relativi alla qualità dei contenuti multimediali non saranno interessati dallo sblocco e dall'uso di queste porte. Eventuali analisi di questi problemi dovranno concentrarsi su altro.
Protezioni federative di Teams
La federazione consente all'organizzazione di comunicare con altre organizzazioni per condividere messaggistica istantanea e presenza. In Teams, la federazione è attiva per impostazione predefinita. Tuttavia, gli amministratori del tenant hanno la possibilità di controllarla tramite il portale di amministrazione di Office 365.
Risposta alle minacce alle riunioni di Teams
Sono due le opzioni disponibili per controllare chi arriva nelle riunioni di Teams e chi potrà accedere alle informazioni presentate.

1. È possibile controllare chi partecipa alle riunioni tramite le impostazioni relative alla **sala di attesa**.

Opzioni per l'impostazione dei partecipanti che possono evitare la sala di attesa disponibili nella pagina Opzioni riunione	Tipi di utente che dispongono dell'acce alla riunione
Utenti dell'organizzazione	- Nel tenant - Ospite del tenant
Utenti dell'organizzazione e organizzazioni attendibili	- Nel tenant - Ospite del tenant - Federato
Tutti	- Nel tenant - Ospite del tenant - Federato Anonimo - Con accesso esterno PSTN

2. Il secondo metodo riguarda le **riunioni strutturate**, dove il relatore può effettuare praticamente tutte le operazioni e i partecipanti hanno un'esperienza controllata. Dopo aver partecipato a una riunione strutturata, i relatori controllano cosa possono fare i partecipanti alla riunione.

Azioni
Parlare e condividere il proprio video
Partecipare alla chat della riunione
Modificare le impostazioni nelle opzioni della riunione
Disattivare l'audio degli altri partecipanti
Rimuovere altri partecipanti
Condividere il contenuto
Ammettere altri partecipanti dalla sala di attesa
Rendere altri partecipanti relatori o partecipanti
Interrompere o avviare la registrazione
Prendere il controllo quando un altro partecipante condivide una presentazione PowerPoint

Teams offre agli utenti aziendali la possibilità di creare e partecipare in tempo reale a riunioni. Gli utenti aziendali possono anche invitare utenti esterni che non dispongono di un account AAD/Office 365 a partecipare a tali riunioni. Anche gli utenti impiegati da partner esterni con un'identità sicura e autenticata possono partecipare alle riunioni e, se autorizzati a farlo, possono agire da relatori. Gli utenti anonimi non possono creare o partecipare a una riunione come relatori, ma possono essere promossi a tale ruolo una volta che avranno partecipato. Affinché gli utenti anonimi possano partecipare alle riunioni di Teams, deve essere attivata l'impostazione Partecipanti nell'interfaccia di amministrazione di Teams.

Nota
Il termine *utenti anonimi* significa utenti che non sono autenticati nel tenant dell'organizzazione. In questo contesto, tutti gli utenti esterni sono considerati anonimi. Gli utenti autenticati includono gli utenti del tenant e gli utenti guest del tenant.
Consentire agli utenti esterni di partecipare alle riunioni di Teams può essere molto utile, ma comporta alcuni rischi per la sicurezza. Per affrontare questi rischi, Teams fornisce le seguenti misure aggiuntive:

- I ruoli dei partecipanti determinano i privilegi di controllo della riunione.
- I tipi di partecipante consentono di limitare l'accesso a specifiche riunioni.
- La pianificazione delle riunioni è limitata agli utenti che possiedono un account AAD e una licenza per Teams.

- Gli utenti anonimi, ovvero non autenticati, che desiderano partecipare a una conferenza telefonica con accesso esterno, compongono uno dei numeri di accesso alla conferenza. Se l'opzione "Consenti sempre ai chiamanti di evitare la sala di attesa" è *attivata*, dovranno attendere finché un oratore o un utente autenticato non parteciperà alla riunione.

Un organizzatore può anche configurare impostazioni per consentire ai chiamanti esterni di accedere per primi a una riunione. Questa impostazione è configurata nelle impostazioni Audioconferenza per gli utenti e viene applicata a tutte le riunioni pianificate dall'utente.

Nota

Per ulteriori informazioni sull'accesso di utenti guest ed esterni in Teams, vedere questo **articolo**. Nell'articolo vengono descritte quali funzionalità gli utenti guest o esterni possono vedere usare quando accedono a Teams.

Ruoli del partecipante

I partecipanti alla riunione si dividono in tre gruppi, ognuno con i propri privilegi e restrizioni:

- **Organizzatore**: l'utente che crea una riunione, sia estemporanea che pianificata. Un organizzatore deve essere un utente del tenant autenticato e avere il controllo su tutti gli aspetti di una riunione per gli utenti finali.
- **Relatore**: un utente autorizzato a presentare le informazioni durante una riunione, usando qualsiasi contenuto multimediale supportato. Un organizzatore della riunione è per definizione anche un relatore e determina chi altro possa essere un relatore. Un organizzatore può prendere questa decisione quando è in programma una riunione o mentre la riunione è in corso.
- **Partecipante**: un utente che è stato invitato a partecipare a una riunione, ma che non è autorizzato a partecipare come relatore.

Un relatore può anche promuovere un partecipante al ruolo di relatore durante la riunione.

Tipi di partecipante

I partecipanti alla riunione sono inoltre classificati per posizione e credenziali. È possibile utilizzare entrambe queste caratteristiche per decidere quali utenti possono accedere a riunioni specifiche. Gli utenti possono essere divisi in modo esteso nelle categorie seguenti:

1. **Utenti che appartengono al tenant**: questi utenti dispongono di credenziali in Azure Active Directory per il tenant. a. *Persone dell'organizzazione*: questi utenti dispongono di credenziali in Azure Active Directory per il tenant. *Persone dell'organizzazione* include gli account guest invitati. b. *Utenti remoti*: questi utenti partecipano dall'esterno della rete aziendale. Possono comprendere i dipendenti che lavorano da casa o in viaggio e altri, come dipendenti di fornitori affidabili, a cui sono state concesse credenziali aziendali per le rispettive condizioni d'uso. Gli utenti remoti possono creare e partecipare alle riunioni, anche come relatori. .
2. **Utenti che non appartengono al tenant**: questi utenti non dispongono di credenziali in Azure Active Directory per il tenant. a. *Utenti federati*: gli utenti federati dispongono di credenziali valide con partner federati e vengono pertanto trattati come autenticati da Teams, ma rimangono comunque anonimi per il tenant della riunione o dell'organizzatore. Gli utenti federati possono partecipare alle riunioni ed essere promossi a relatori dopo che hanno partecipato alla riunione, ma non possono creare riunioni in aziende con cui sono federati. b. *Utenti anonimi*: gli utenti anonimi non hanno un'identità di Active Directory e non sono federati con il tenant.

Molte riunioni coinvolgono utenti esterni. Queste stesse società desiderano anche rassicurazioni in merito all'identità degli utenti esterni prima di consentire a tali utenti di partecipare a una riunione. Nella sezione seguente viene descritto in che modo Teams limita l'accesso alle riunioni per i tipi di utenti che non sono stati autorizzati in modo esplicito e richiede a tutti i tipi di utente di fornire *credenziali* appropriate per l'accesso a una riunione.

Ammissione dei partecipanti

In Teams, gli utenti anonimi possono essere trasferiti a un'area di attesa chiamata sala di attesa. I relatori possono quindi scegliere di *ammettere* questi utenti alla riunione o di *rifiutarli*. Quando gli utenti vengono trasferiti nella sala di attesa, il relatore e i partecipanti ricevono una notifica e gli utenti anonimi devono attendere di essere accettati o rifiutati oppure che la connessione scada.

Per impostazione predefinita, i partecipanti che si collegano dalla PSTN accedono direttamente alla riunione, ma questa opzione può essere modificata per forzare i partecipanti esterni a passare per la sala di attesa.

Gli organizzatori della riunione controllano se i partecipanti possono partecipare a una riunione senza attendere nella lobby. Ogni riunione può essere configurata in modo da consentire l'accesso utilizzando uno dei seguenti metodi:

Le impostazioni predefinite sono:

- *Persone dell'organizzazione*: chiunque esterno all'organizzazione attenderà nella sala di attesa finché non verrà ammesso.
- *Persone dell'organizzazione e di organizzazioni attendibili*: gli utenti esterni e autenticati dei domini di Teams e Skype for Business, presenti nell'elenco degli utenti esterni consentiti, possono evitare la sala di attesa. Tutti gli altri utenti aspetteranno nella sala di attesa finché non saranno ammessi.
- *Tutti*: tutti i partecipanti alla riunione evitano la sala di attesa dopo che un utente autenticato ha partecipato alla riunione.

Funzionalità del relatore

Gli organizzatori della riunione controllano se i partecipanti possono presentare durante una riunione. Ogni riunione può essere configurata in modo da limitare i relatori a una delle seguenti opzioni:

- *Persone dell'organizzazione*: tutti gli utenti del tenant, inclusi gli utenti guest, possono presentare
- *Persone dell'organizzazione e di organizzazioni attendibili*: tutti gli utenti del tenant, inclusi gli utenti guest, possono presentare insieme agli utenti dei domini di Teams e Skype for Business presenti nell'elenco degli utenti con accesso esterno consentiti.
- *Tutti*: tutti i partecipanti alla riunione sono relatori.

Modifica delle impostazioni mentre una riunione è in corso

È possibile modificare le opzioni della riunione mentre questa è in corso. La modifica, se salvata, influirà sulla riunione in corso in pochi secondi. Interesserà anche le sessioni future della riunione.

A questo punto il presidente pone a votazione le modalità di riunione del consiglio direttivo così come specificate nella comunicazione di convocazione.
Votano a favore: VITELLI, DI LEVA, DE CHIARA, FERRANTE, MOTTI, CHIANESE, POLITO, DE LISA, PEZONE.
Il consigliere ing MANZELLA vota a favore con la precisazione che le determinazioni assunte verranno con una successiva presa d'atto ratificate in un consiglio svolto in modalità ordinarie.
Votano contro: RAUCCI

Il CD approva a maggioranza. Alle ore 17:10 esce l'ing RAUCCI			
Modalità di voto approvazione verbale seduta precedente		Nessuna	***Note:***
		Unanimità	Con il voto contrario del consigliere RAUCCI
	X	Maggioranza	

Punto n.	**2**

ATTIVITA' DELL'ORDINE

Sintesi della discussione e proposte:

Il Presidente informa il CD circa le informazioni relative ai nominativi individuati per le terne degli esami di stato nella scorsa seduta di consiglio.
In particolare, alcuni docenti universitari e dirigenti pubblici non sono in possesso dei requisiti necessari quali di ottemperanza al pagamento delle quote annuali e al possesso dei CFP in regola con la norma della formazione continua.

Il Presidente propone in sostituzione i seguenti nominativi:
Nardini Sergio, Pirozzi e Iervolino con Andreozzi assunta, Vitelli Massimo e De Matteis Gianfranco.
Parente Girolamo con Chiara Follera.

Che vengono posti a votazione.

Esiti:

Delibera n. _____ del / /2020

Modalità di voto		Nessuna	***Note:***
	X	Unanimità	
		Maggioranza	

Sintesi della discussione e proposte:

Il Presidente propone la revoca della sospensione dell'iscritto ing [redacted] a condizione che il Tesoriere ing DE CHIARA, verifichi l'avvenuto effettivo versamento di quanto dovuto dall'iscritto per le quote annuali.

Esiti:

Delibera n. _____ del / /2020

Modalità di voto		Nessuna	***Note:***
	X	Unanimità	

		Maggioranza	

Sintesi della discussione e proposte:

Il Presidente illustra la situazione circa le modalità lavorative in smartworking degli uffici di segreteria. Si evidenzia la carenza di attrezzatura hardware e software per l'attuazione di tale modalità.
Alle ore 17:38 entra il consigliere ing RANUCCI.
Il Presidente propone di demandare all'ing POLITO e ing DE LISA in qualità rispettivamente di Presidente della Fondazione FOICE e Presidente della Commissione Formazione Continua di raccogliere informazioni in merito e di rendicontare appena possibile in consiglio.

Esiti:

Delibera n. _____ del / /2020

Modalità di voto		Nessuna	***Note:***
	X	Unanimità	
		Maggioranza	

Sintesi della discussione e proposte:

Il Presidente informa il consiglio direttivo sull'attività del nostro DPO ing SPERA Giuseppe circa gli incontri formativi in materia di protezione dei dati personali rivolti ai dipendenti dell'ordine degli Ingegneri della Provincia di Caserta.

Esiti:

Delibera n. _____ del / /2020

Modalità di voto		Nessuna	***Note:***
	X	Unanimità	
		Maggioranza	

Sintesi della discussione e proposte:

Il Presidente informa il CD, sulla necessità di prolungare il contratto di lavoro al dipendente a tempo determinato e part time ing Salvatore DELL'AVERSANA, visto il prolungarsi dell'attuale stato di contingenza.
A tal proposito il presidente propone di incaricare il Responsabile degli Uffici dott.ssa Nicoletta COPPOLA che unitamente al consulente informatico (Salvatore SANTOSANASTASO) relazioni il CD circa le attività e le attrezzature necessarie al fine di poter attuare l'attività lavorative degli uffici di segreteria in modalità smartworking, incluso l'eventuale digitalizzazione e le conseguenti nuove procedure da adottare relative alla prescritta modalità.

Esiti:

Delibera n. _____ del / /2020

Modalità di voto		Nessuna	***Note:***
	X	Unanimità	
		Maggioranza	

Sintesi della discussione e proposte:

Il Segretario unitamente al Presidente propongono di dare mandato alla Commissione Sicurezza dell'Ordine di interagire con il RSSP ed il Medico Competente al fine di progettare le misure necessarie per l'adeguamento e aggiornamento del Piano di Sicurezza in relazione alla problematica COVID in particolare alle procedure e alle attrezzature da prevedere al fine di contrastare e/o ridurre al minimo i rischi conseguenti la situazione contingente.

Esiti:

Delibera n. _____ del / /2020

Modalità di voto		Nessuna	***Note:***
	x	Unanimità	
		Maggioranza	

Sintesi della discussione e proposte:

Per quanto attiene la richiesta di nominativi del Comune di Gricignano del **13/01/2020**, prot. n. **341/20**, vista la manifestazione d'interesse espletata e la candidatura dell'iscritto ing ADINOLFI Antonio quale componente della Commissione di pubblico spettacolo il CD delibera di inviare il nome dell'ing **ADINOLFI Antonio**.

Esiti:

Delibera n. _____ del / /2020			
Modalità di voto		Nessuna	***Note:***
	x	Unanimità	
		Maggioranza	
Sintesi della discussione e proposte:			
Si dà mandato agli uffici di segreteria di pubblicare sul sito ufficiale dell'Ordine la circolare CNI n. 538/2020.			
Esiti:			
Delibera n. _____ del / /2020			
Modalità di voto		Nessuna	***Note:***
	x	Unanimità	
		Maggioranza	

Punto n.	**3**
SMART WORKING, FORMAZIONE A DISTANZA, STREAMING SINCRONO	
Sintesi della discussione e proposte:	
L'ing POLITO mostra al CD il lavoro svolto dalla Commissione Privacy e Sicurezza dati in cui sono trattati tra l'altro gli argomenti relativi ai sistemi di video conferenza, scelta della piattaforma, sistemi VPN e il servizio di posta elettronica e relativa gestione. Propone di pubblicare sul sito il lavoro svolto. A seguito di quanto evidenziato dall'ing POLITO il Presidente propone di incaricare l'ing Giuseppe SPERA che unitamente all'attuale responsabile degli uffici dott.ssa Coppola rediga un progetto che preveda la necessità di fornire gli uffici di segreteria e l'ordine di appositi hardware e software oltre a istituire procedure organizzative sia in relazione all'attività degli uffici di segreteria, che per quella di formazione continua in FAD sia Sincrona che Asincrona e delle modalità di svolgimento via web delle riunioni del consiglio dell'ordine. Il progetto dovrà prevedere anche ipotesi di spesa. Per detta attività si prevede un impegno di spesa con un tetto pari a € 2500,00 (duemilacinquecento) ed un tempo massimo pari a 15 giorni dal conferimento dell'incarico all'ing. Giuseppe SPERA. La dott.ssa COPPOLA è incaricata della sua azione nella presente deliberazione.	
Esiti:	
Delibera n. _____ del / /2020	

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CASERTA

Modalità di voto		Nessuna	***Note:***
	X	Unanimità	
		Maggioranza	

Punto n.	**4**
NUOVE ISCRIZIONI E CANCELLAZIONI	
Sintesi della discussione e proposte:	
Prende la parola il Segretario, Ing. Gentile e viste le seguenti richieste	

ISCRIZIONI

Richiesta prot. n. _____ del ___/___/2020 del/lla Dott./Dott.ssa _________________________, il CD approva la richiesta iscrivendo il/la richiedente alla Sez. ☐ A ☐ B al n. ______,
al settore ☐ Civile e Ambientale ☐ Industriale ☐ Informazione

Richiesta prot. n. ______ del ___/____/2020 del/lla Dott./Dott.ssa ___________________________, il CD approva la richiesta iscrivendo il/la richiedente alla Sez. ☐ A ☐ B al n. _______,
al settore ☐ Civile e Ambientale ☐ Industriale ☐ Informazione

Richiesta prot. n. ______ del ___/____/2020 del/lla Dott./Dott.ssa ___________________________, il CD approva la richiesta iscrivendo il/la richiedente alla Sez. ☐ A ☐ B al n. _______,
al settore ☐ Civile e Ambientale ☐ Industriale ☐ Informazione

Richiesta prot. n. ______ del ___/____/2020 del/lla Dott./Dott.ssa ___________________________, il CD approva la richiesta iscrivendo il/la richiedente alla Sez. ☐ A ☐ B al n. _______,
al settore ☐ Civile e Ambientale ☐ Industriale ☐ Informazione

Richiesta prot. n. ______ del ___/____/2020 del/lla Dott./Dott.ssa ___________________________, il CD approva la richiesta iscrivendo il/la richiedente alla Sez. ☐ A ☐ B al n. _______,
al settore ☐ Civile e Ambientale ☐ Industriale ☐ Informazione

Richiesta prot. n. ______ del ___/____/2020 del/lla Dott./Dott.ssa ___________________________, il CD approva la richiesta iscrivendo il/la richiedente alla Sez. ☐ A ☐ B al n. _______,
al settore ☐ Civile e Ambientale ☐ Industriale ☐ Informazione

Richiesta prot. n. ______ del ___/____/2020 del/lla Dott./Dott.ssa ___________________________, il CD approva la richiesta iscrivendo il/la richiedente alla Sez. ☐ A ☐ B al n. _______,
al settore ☐ Civile e Ambientale ☐ Industriale ☐ Informazione

Richiesta prot. n. ______ del ___/____/2020 del/lla Dott./Dott.ssa ___________________________, il CD approva la richiesta iscrivendo il/la richiedente alla Sez. ☐ A ☐ B al n. _______,
al settore ☐ Civile e Ambientale ☐ Industriale ☐ Informazione

Richiesta prot. n. ______ del ___/____/2020 del/lla Dott./Dott.ssa ___________________________, il CD approva la richiesta iscrivendo il/la richiedente alla Sez. ☐ A ☐ B al n. _______,
al settore ☐ Civile e Ambientale ☐ Industriale ☐ Informazione

Richiesta prot. n. ______ del ___/____/2020 del/lla Dott./Dott.ssa ___________________________, il CD approva la richiesta iscrivendo il/la richiedente alla Sez. ☐ A ☐ B al n. _______,
al settore ☐ Civile e Ambientale ☐ Industriale ☐ Informazione

CANCELLAZIONI

Richiesta prot. n. 820 /20 del 14 / 04 /2020, viene cancellato l'Ing. **COPPOLA EMILIO** N° 2798 ,
Sez. ☒ A ☐ B - ☐ per iscrizione nella Sez. A ☒ su richiesta dell'iscritto

Richiesta prot. n. 726/20 del 03/04/2020, viene cancellato l'Ing. _______________ N° _______,
Sez. ☐ A ☐ B - ☐ per iscrizione nella Sez. A ☐ su richiesta dell'iscritto

Richiesta prot. n. _____/20 del __/__/2020, viene cancellato l'Ing. __________________ N° ________,
Sez. ☐ A ☐ B - ☐ per iscrizione nella Sez. A ☐ su richiesta dell'iscritto

Richiesta prot. n. ______/20 del ___/____/2020, viene cancellato l'Ing. ____________________________ N° ______,
Sez. ☐ A ☐ B - ☐ per iscrizione nella Sez. A ☐ su richiesta dell'iscritto

Richiesta prot. n. ______/20 del ___/____/2020, viene cancellato l'Ing. ____________________________ N° ______,
Sez. ☐ A ☐ B - ☐ per iscrizione nella Sez. A ☐ su richiesta dell'iscritto

Viene cancellato per decesso l'Ing. ________________ con decorrenza ___/___/2020, data del decesso.

Viene cancellato per decesso l'Ing. ________________ con decorrenza ___/___/2020, data del decesso.

TRASFERIMENTI

Vista la richiesta dell'Ordine della Provincia di _______, prot. n. ____/20 del ___/___/2020, il Consiglio delibera la cancellazione dell'Ing. _______________ con decorrenza ___/___/2020, data di iscrizione all'Ordine della Provincia di _____________.

Vista la richiesta dell'Ordine della Provincia di _______________, prot. n. ____/20 del ___/___/2020, il Consiglio delibera la cancellazione dell'Ing. _______________ con decorrenza ___/___/2020, data di iscrizione all'Ordine della Provincia di _____________.

Vista la richiesta dell'Ordine della Provincia di _______________, prot. n. ____/20 del ___/___/2020, il Consiglio

delibera la cancellazione dell'Ing. _____ con decorrenza ___/___/2020, data di iscrizione all'Ordine della Provincia di _____.

NULLA OSTA

Vista la comunicazione dell'Ordine della Provincia di ROMA, prot. n. 814/20 del 10/04 /2020, circa il trasferimento dell'Ing. **DI GIROLAMO ANTONIO – 2241 sez. A**, il Consiglio concede il Nulla Osta richiesto.

Vista la comunicazione dell'Ordine della Provincia di _____, prot. n. _____/20 del ___/___/2020, circa il trasferimento dell'Ing. _____, il Consiglio concede il Nulla Osta richiesto.

INTEGRAZIONI

Richiesta prot. n. _____ del ___/___/2020 del/lla Dott./Dott.ssa _____, iscritto/a alla Sez. ☐ A ☐ B al n. al settore Civile e ☐ Ambientale ☐ Industriale ☐ Informazione, il CD approva l'integrazione al settore ☐ Civile e Ambientale ☐ Industriale ☐ Informazione.

Richiesta prot. n. _____ del ___/___/2020 del/lla Dott./Dott.ssa _____, iscritto/a alla Sez. ☐ A ☐ B al n. _____ al settore ☐ Civile e Ambientale ☐ Industriale ☐ Informazione, il CD approva l'integrazione al settore ☐ Civile e Ambientale ☐ Industriale ☐ Informazione.

Delibera n. _____ del / /2020

Modalità di voto		Nessuna	***Note:***
	x	Unanimità	
		Maggioranza	

Punto n. **5**

VARIE ED EVENTUALI

Sintesi della discussione e proposte:

Esiti:

Delibera n. _____ del / /2020			
Modalità di voto		Nessuna	***Note:***
		Unanimità	
		Maggioranza	

Il presente verbale è composta da n° **14** pagine	
I lavori si chiudono alle ore **20:00 .**	
LETTO, CONFERMATO E SOTTOSCRITTO	
IL SEGRETARIO	**IL PRESIDENTE**
(Ing. Fabrizio GENTILE)	(Dott. Ing. Massimo VITELLI)