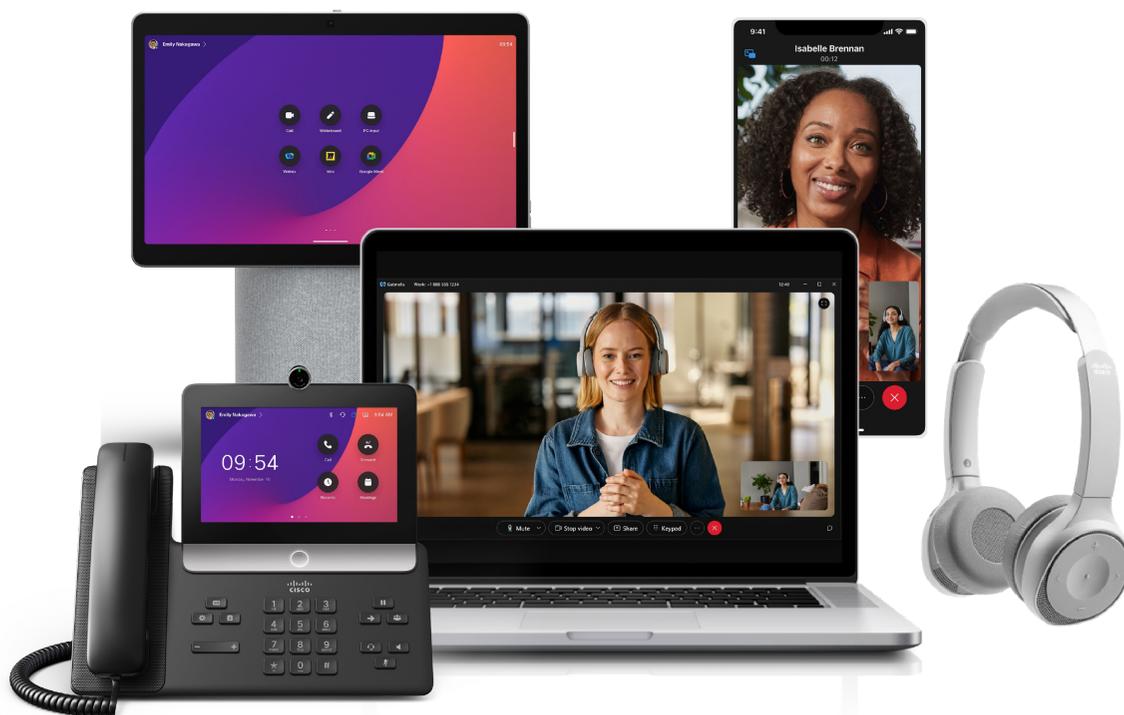


Let's Co

Communication and Collaboration



REQUISITI MINIMI DI RETE

Premessa	p. 3
Requisiti tecnici	p. 4
Servizi di Rete	p. 5
Server DHCP.....	p. 5
Server DNS.....	p. 5
Server NTP	p. 5
Funzionalità e applicazioni di Routing	p. 6
Network Address Translation	p. 6
Application Layer Gateway	p. 6
SIP Session Audit	p. 6
Qualità del servizio	p. 7
Larghezza di Banda	p. 7
Banda internet WAN	p. 7
Banda della rete locale LAN.....	p. 8
Specifiche di configurazione del firewall del cliente	p. 9
Subnet pubbliche	p. 9
Riepologo porte TCP e UDP	p. 10
Tempi di Timeout delle sessioni TCP e UDP	p. 10
Configurazione del Trunksip	p. 11
Configurazione Cordless Multicella	p. 11
Prevenzioni delle frodi	p. 11

Premessa

Let's Co è la soluzione di Collaboration e Communication erogata in Cloud mediante differenti infrastrutture informatiche dislocate su diverse sedi nel mondo. Il servizio è costituito da più componenti, tra cui applicazioni vocali, video, desktop e mobili, applicazioni web e strumenti di controllo e monitoraggio della qualità del servizio.

Questi componenti richiedono la comunicazione tra i dispositivi nella rete locale del cliente (LAN) verso l'infrastruttura Let's Co; tali comunicazioni avvengono attraverso connessioni internet pubbliche (WAN) o mediante connessioni di rete private (MPLS).

Affinché queste comunicazioni funzionino correttamente, le connessioni delle reti interne ed esterne del cliente devono rispettare dei requisiti minimi e i dispositivi di protezione installati presso la sede del cliente, come i firewall, non devono bloccare gli indirizzi IP e le porte dei servizi TCP / UDP utilizzati dal servizio Let's Co.

Le seguenti sezioni di questo documento forniscono informazioni necessarie per dimensionare correttamente le connessioni e configurare correttamente il firewall cliente per consentire tutte le comunicazioni tra i dispositivi e le applicazioni cliente verso i servizi Let's Co.

Vista la natura tecnica delle argomentazioni trattate nel presente documento consigliamo di affidare il presente documento al referente dei sistemi informatici aziendali o all'azienda esterna incaricata. Il presente documento unitamente all'offerta commerciale è da considerarsi parte integrante delle condizioni generali e viene richiamato al punto 14 e 16 delle condizioni generali stesse.

ATTENZIONE: La mancata o errata configurazione dei dispositivi di rete può causare anomalie nel funzionamento di Let's Co e incidere nella qualità del servizio.

ATTENZIONE: Si raccomanda l'utilizzo di un sistema firewall opportunamente configurato che sia in grado di proteggere la rete aziendali e i dispositivi collegati a Let's Co scongiurando così problematiche di sicurezza e frodi.

REQUISITI TECNICI

La progettazione e la configurazione della rete del cliente sono caratterizzate da molte variabili, che possono influenzare le prestazioni e la qualità del servizio VoIP (Voice over IP). Affinché il servizio VOIP Let's Co funzioni nella maggior parte degli ambienti di rete dei clienti, ci sono una serie di requisiti minimi che tale rete deve soddisfare per garantire il funzionamento del servizio come previsto. Questi requisiti si applicano sia ai telefoni SIP che agli adattatori analogici (ATA), da qui in avanti generalmente definiti come dispositivi VOIP.

Di seguito, il riepilogo dei requisiti minimi richiesti:

- ✓ La rete LAN del cliente deve contenere un server DHCP capace di fornire all'avvio un indirizzo IP ai dispositivi VOIP.
- ✓ La rete LAN del cliente deve contenere un server DNS o deve poter fornire un inoltro DNS per la risoluzione degli URL utilizzati dai dispositivi VOIP per comunicare con piattaforme di servizio esterne.
- ✓ Il server DNS deve essere in grado di risolvere sia i record SRV sia i record A.
- ✓ Il firewall del cliente deve permettere il traffico specificato nelle sezioni seguenti affinché i dispositivi VOIP possano effettuare e ricevere chiamate.
- ✓ Il router/firewall del cliente non deve manipolare i pacchetti SIP o RTP a livello di applicazione. Se qualsiasi dispositivo CPE può funzionare come gateway di accesso a livello SIP (ALG), la funzionalità ALG deve essere disabilitata.
- ✓ Il router del cliente deve supportare DSCP (Differentiated Service Code Point) e garantire che i pacchetti con maggiore priorità abbiano la precedenza su tutti gli altri pacchetti in uscita.
- ✓ Il router del cliente deve essere configurato per contrassegnare con priorità alta tutti i pacchetti SIP e RTP dalle piattaforme di controllo delle chiamate Let's Co così da garantire che questi abbiano la massima priorità su tutti gli altri pacchetti in entrata. Le piattaforme di monitoraggio delle chiamate Let's Co possono essere identificate in modo univoco da un insieme di indirizzi IP specifici. I pacchetti SIP e RTP possono essere individuati dalle porte indicate nella sezione Firewall di questo documento.
- ✓ La larghezza di banda Internet del cliente deve essere proporzionata in modo da consentire la quantità minima di larghezza di banda dati richiesta oltre al numero totale di chiamate vocali simultanee richieste dall'azienda.
- ✓ Le dimensioni della rete locale (LAN) del cliente devono essere proporzionata in modo da consentire la massima quantità di larghezza di banda dati richiesta oltre al numero totale di chiamate vocali simultanee richieste dall'azienda.

Server DHCP

Tutti i dispositivi VOIP Let's Co sono configurati di default per ottenere informazioni sull'indirizzo IP e sul server DNS da un server DHCP locale. Quando un dispositivo VOIP viene avviato, tenta di individuare il server DHCP locale e di ottenere queste informazioni. Se la rete del cliente non contiene un server DHCP o non fornisce le informazioni richieste, il dispositivo VOIP non si avvierà correttamente e sarà inutilizzabile.

Alcuni server DHCP forniscono "opzioni" come parte della risposta alla richiesta di un client. Per quanto riguarda le applicazioni SIP, l'opzione 66 viene comunemente utilizzata per fornire al client, in questo caso un dispositivo VOIP, l'indirizzo del server di configurazione che deve contattare per ottenere la sua configurazione. Nel caso del servizio Let's Co, questa opzione non è richiesta. Tutti i dispositivi VOIP Let's Co sono codificati per puntare all'indirizzo di uno specifico server di configurazione e se un'opzione 66 viene ricevuta dal dispositivo VOIP in risposta a una richiesta DHCP, il dispositivo VOIP la ignorerà.

Server DNS

Tutti i dispositivi VOIP Let's Co richiedono il DNS per tradurre i nomi di dominio in indirizzi IP.

Durante il processo di avvio, il nome di dominio del server di configurazione del dispositivo VOIP viene tradotto in modo che il dispositivo VOIP possa individuare e ricevere le informazioni di configurazione dal server di configurazione corretto.

Inoltre, una volta che il telefono ha completato il processo di avvio, il nome di dominio del server per il controllo delle chiamate viene tradotto in modo che il dispositivo VOIP possa individuare e comunicare con questi server. Se un server DNS non è disponibile per fornire la traduzione del nome, il dispositivo VOIP non si avvierà correttamente e sarà inutilizzabile.

Il servizio Let's Co utilizza record "A" (indirizzo) e "SRV" (servizio). I record "SRV" vengono utilizzati per fornire un meccanismo di ridondanza per le piattaforme di controllo delle chiamate. Affinché Let's Co funzioni correttamente, i due record devono essere supportati sulla rete del cliente.

Server NTP

Let's Co gestisce le sorgenti NTP durante la configurazione automatica del telefono VOIP, questi ultimi non saranno in grado di completare il loro ciclo (iniziale o costante) di aggiornamento della configurazione senza una risorsa NTP.

Network Address Translation

Il servizio Let's Co, per aggirare le limitazioni imposte dal NAT, utilizza una tecnica denominata NAT Traversal e parte della piattaforma di controllo delle chiamate Let's Co è responsabile del mantenimento della comunicazione costante con tutti i dispositivi VOIP.

Questa comunicazione costante garantisce che il timer del NAT non scada mai, rendendo il collegamento dinamico di fatto permanente. Senza questo, un dispositivo VOIP in una rete privata non sarebbe in grado di ricevere chiamate. Poiché il NAT non manipola le informazioni sull'application layer, la piattaforma di controllo delle chiamate Let's Co utilizza una tecnica chiamata Media Relay per aggirare il problema. Questa funzionalità consente alla piattaforma di controllo delle chiamate di rilevare l'indirizzo IP pubblico e la porta del flusso RTP una volta che il dispositivo VOIP invia il suo primo pacchetto RTP. La piattaforma di controllo delle chiamate esegue questa funzione su entrambe le estremità di una chiamata e le collega, trasmettendo efficacemente il traffico da un dispositivo ad un altro.

Si segnala, infine, che in presenza di un doppio NAT il servizio Let's Co potrebbe presentare malfunzionamenti. In tal caso, per risolvere il problema, occorrerà rimuovere uno dei due NAT.

Application Layer Gateway

Anche se questa funzionalità ha lo scopo di migliorare il traffico VOIP, non tutti i dispositivi ALG eseguono correttamente la conversione dei pacchetti sull'application layer. In molti casi, parti del pacchetto vengono modificate in maniera errata e ciò causa problemi di funzionamento tra il dispositivo VOIP e la piattaforma di controllo delle chiamate. Se ciò accade, ALG fa sì che il dispositivo SIP non funzioni correttamente.

Con il servizio Let's Co, si consiglia di disattivare tutte le funzionalità di "Sip Aware" ovvero SIP ALG tra il dispositivo VOIP e la piattaforma di controllo delle chiamate. In questo modo, si elimina la possibilità che l'ALG traduca erroneamente pacchetti, azione che potrebbe rendere inutilizzabile il servizio. Tuttavia, in alcuni casi, questa funzionalità potrebbe non essere configurabile. Per soddisfare questa necessità, il servizio Let's Co utilizza porte non comuni per il traffico SIP e RTP. Le porte dalla 8933 alla 8943 vengono utilizzate al posto della 5060, che è comunemente usata per il SIP. Dato che la maggior parte degli ALG presumono l'uso della porta 5060 per il SIP, l'utilizzo della porta dalla 8933 alla 8943 farà sì che l'ALG ignori completamente il pacchetto e non esegua alcuna manipolazione. Inoltre, lo stesso processo vale per RTP. Sebbene non specificamente definito da uno standard, l'intervallo di porte più comunemente utilizzato per RTP è 16384-16482. Per evitare l'interazione con l'ALG, il prodotto Let's Co utilizza le porte RTP 19560-65535.

SIP Session Audit

Per proteggersi da potenziali frodi nel caso di chiamate eccessivamente lunghe, la piattaforma Let's Co esegue una Session Audit ogni 15 minuti. La Session Audit invierà un messaggio UPDATE o re-INVITE SIP a seconda di cosa può supportare il dispositivo VOIP. Si prevede una risposta con 200 OK. Se non viene ricevuto tale messaggio, l'UPDATE o il re-INVITE saranno riavviati e se non viene ricevuta alcuna risposta, la chiamata sarà ritenuta non valida e verrà terminata.

Qualità del servizio

Una conversazione vocale avviene in tempo reale, pertanto il traffico associato ad una chiamata vocale deve essere elaborato in modo efficiente o si verificano problemi come il clipping o l'audio discontinuo.

Il servizio Let's Co utilizza il DSCP (Differentiated Services Code Point), comunemente noto anche come DiffServ, per la marcatura della priorità dei pacchetti. Ogni dispositivo VOIP imposta automaticamente ogni pacchetto che invia come prioritario. Tuttavia, ciò non garantisce che tutte le apparecchiature di rete nel percorso del traffico rispettino le impostazioni e consentano al traffico vocale di avere la priorità sul traffico dati. Per garantire che i pacchetti vocali abbiano la priorità sui pacchetti dati, i router dei clienti e dell'operatore che fornisce il servizio di connettività devono essere configurati correttamente per gestire il DSCP.

Si consiglia di configurare il router con una coda di priorità rigorosa, in modo che i pacchetti contrassegnati con valori DSCP più alti abbiano una priorità maggiore. Se ciò non viene eseguito correttamente, la qualità della chiamata potrebbe peggiorare notevolmente durante i periodi di traffico intenso.

Si consiglia inoltre di stabilire regole di priorità per consentire a tutto il traffico SIP e RTP in entrata di avere una priorità maggiore rispetto al resto del traffico. Le porte associate a SIP e RTP sono definite nella sezione Firewall di questo documento. Potrebbe, inoltre, essere necessario assegnare agli indirizzi IP delle piattaforme di controllo delle chiamate Let's Co una priorità maggiore rispetto al resto del traffico. Anche se soggetti a modifiche, in allegato al presente documento vengono dettagliati gli indirizzi IP specifici.

LARGHEZZA DI BANDA

Banda Internet WAN

La quantità di banda disponibile determinerà l'ammontare di chiamate vocali simultanee e di traffico dati che la connessione Internet supporterà. Se dimensionato correttamente e con le corrette impostazioni QOS nel router del cliente, il servizio Let's Co funzionerà senza errori.

Tuttavia, se sottodimensionato o se il QOS non viene impostato nel modo giusto, la qualità della chiamata percepita potrebbe deteriorarsi notevolmente durante i periodi di traffico di punta. Le seguenti informazioni forniscono dati e linee guida per il corretto dimensionamento del servizio vocale per una determinata larghezza di banda Internet.

Per determinare il numero di telefoni che possono essere supportati su una determinata larghezza di banda, è necessario innanzitutto calcolare il numero massimo di chiamate simultanee che possono essere supportate.

Tale calcolo deve considerare anche l'effetto degli algoritmi di compressione (Codec), nello specifico per gestire ciascuna chiamata audio la banda Internet utilizzata da Let's Co è di 50 kbps/chiamata con Codec G.729 e 100 kbps/chiamata con Codec G.711, quest'ultimo di norma viene utilizzato per i fax. Per le chiamate video, il calcolo dipende dalla risoluzione scelta: nella tabella seguente sono presenti i dati di occupazione per il desktop client:

Codecs	Communicator Video Size	H.264 Profile Level	Video Size	FPS Default	Recommended CPU	Default Maximum Bit Rate (Kbps)	Minimum RAM (GB)	H.263 Resolutions
Any supported codec	Small	1.1	174 x 144	15 through 30	Pentium Dual Core 1.7 GHz	192	1	SQCIF
Any supported codec	Medium	2	352 x 288	15 through 30	Pentium Dual Core 1.7 GHz	384	1	QCIF
Any supported codec	Large	3	640 x 480	15 through 30	Pentium Dual Core 1.7 GHz	512	1	CIF
G.722 for audio, H.264 for video	HD	3.1	1280 x 720	15 through 30	Pentium Quad Core	4096	2	4CIF

I dati della tabella sono indicativi e si riferiscono a una sola direzione, vanno quindi moltiplicati per due. Per le linee asimmetriche come l'ADSL e dati cellulari, bisogna tenere presente che la banda in upload è molto più bassa di quella in download.

Banda della rete locale LAN

La larghezza di banda della LAN è la quantità di traffico che la rete interna di un cliente può supportare. Questo quantitativo è determinato dalla capacità di trasmissione dell'infrastruttura di rete LAN. Nella maggior parte dei casi, l'infrastruttura di rete LAN del cliente è composta da un singolo switch di livello 2. La quantità di banda disponibile determinerà la quantità di chiamate vocali simultanee e il traffico dati che la LAN supporterà. Se dimensionato correttamente, il servizio Let's Co funzionerà correttamente. Tuttavia, se sottodimensionato, la qualità delle chiamate percepite potrebbe deteriorarsi notevolmente durante i periodi di traffico di punta.

È responsabilità del cliente assicurarsi che la propria rete interna sia ridimensionata correttamente per supportare l'aggiunta del VOIP alla propria rete.

SPECIFICHE DI CONFIGURAZIONE DEL FIREWALL DEL CLIENTE

Il firewall e le relative funzionalità di sicurezza e protezione sono un requisito fondamentale per il buon funzionamento del servizio Let's Co e per proteggere la rete del cliente da attacchi informatici scongiurando anche possibili frodi. Le impostazioni del firewall necessarie per il corretto funzionamento del servizio Let's Co sono documentate come segue.

Subnet pubbliche

La configurazione del firewall deve garantire la raggiungibilità dell'infrastruttura di Let's Co e, nello specifico, delle subnet e dei relativi indirizzi IP pubblici riportati in seguito:

Subnet IP per i servizi Let's Co			
3.20.185.219/32	72.163.15.128/26	150.253.128.0/17	192.133.220.0/26
3.130.87.169/32	72.163.24.0/23	170.72.0.0/16	192.133.220.64/26
3.134.166.179/32	85.119.56.0/23	170.133.128.0/18	199.19.196.0/23
23.89.0.0/16	128.177.14.0/24	173.36.127.0/26	199.19.199.0/24
62.109.192.0/18	128.177.36.0/24	173.36.127.128/26	199.59.64.0/21
64.68.96.0/19	135.84.168.0/21	173.37.26.0/23	207.182.160.0/19
72.163.10.96/27	139.177.64.0/21	173.37.146.128/25	
72.163.10.128/25	139.177.72.0/23	173.37.149.96/27	
72.163.15.64/26	144.196.0.0/16	185.115.196.0/22	

Riepilogo porte TCP e UDP

Affinché ogni servizio funzioni correttamente è necessario permettere il raggiungimento delle porte TCP e UDP verso le subnet pubbliche. Di seguito le porte designate:

Scopo connessione	Protocollo	Indirizzi di destinazione	Porte di destinazione
Segnalazione e controllo (SIP over TLS, etc.)	TCP	Subnet IP per i servizi Let's Co	1025, 1061, 1081, 2197, 2208, 5060-5062, 5222-5223, 5228-5230, 5280-5281, 6970, 8060-8070, 8933-8943, 19560, 52644-52645, 65525, 65535
Contenuto multimediale (SRTP, etc.)	UDP	Subnet IP per i servizi Let's Co	5004, 5060, 5061, 8060-8070, 8500-8699, 8933-8943, 9000, 15000-19000, 19560-65535
Configurazione e gestione del firmware dei dispositivi	TCP	Subnet IP per i servizi Let's Co	443, 697, 8443
DNS	UDP e TCP	Definito dall'host	53
NTP ¹	UDP	- Subnet IP per i servizi Let's Co - Definito dall'host	123

¹: il protocollo NTP deve essere garantito sia verso le subnet pubbliche relative agli specifici servizi Let's Co sia verso eventuali server NTP di terze parti impostati, ad esempio, sui pc dell'azienda. Se il dispositivo non riesce a contattare il server NTP si possono verificare dei problemi durante la validazione del certificato HTTPS utilizzato per stabilire la connessione necessaria alla configurazione del dispositivo stesso.

Tempi di Timeout delle sessioni TCP e UDP

Per una corretta gestione del servizio, in particolare dei trasferimenti di chiamata, è necessario impostare i seguenti timeout minimi relativi alle sessioni e disabilitare il SIP-ALG, per evitare che il traffico voce venga scartato o deviato inaspettatamente.

Protocollo	Timeout minimo (secondi)
TCP	60
UDP	300
NAT	300

Protocollo	Stato
SIP-ALG	Disabilitato

CONFIGURAZIONE DEL TRUNK SIP

Se all'interno del servizio Let's Co viene richiesta l'abilitazione del servizio Trunk SIP, è necessario che il media gateway (d'ora in poi CPE, Customer Premise Equipment) sia configurato correttamente all'interno della rete aziendale. La configurazione del servizio Let's Co Trunk SIP richiede la configurazione del CPE per abilitare i servizi di accesso remoto affinché sia possibile effettuare la manutenzione.

ATTENZIONE: è estremamente importante, per qualsiasi IP PBX o media gateway multimediale accessibile via Internet tramite un indirizzo IP, che vengano implementate nella rete del cliente tutte le protezioni necessarie al CPE. Tutti i CPE devono quindi essere protetti da un firewall configurato in modo appropriato per impedire l'accesso al CPE da fonti sconosciute.

CONFIGURAZIONE CORDLESS MULTICELLA

Se all'interno del servizio Let's Co viene richiesta l'abilitazione di un servizio cordless multicella (mesh della rete DECT), è necessario assicurarsi che sugli switch presenti il traffico multicast (IGMP) sia consentito e correttamente instradato su tutta la struttura di rete coinvolta, pena il funzionamento anomalo dei dispositivi cordless.

Il protocollo multicast consente la comunicazione simultanea di un host verso diversi client e viene utilizzato per la sincronizzazione delle informazioni tra diversi dispositivi, tra cui anche le celle (basi) che necessitano di intercomunicazione per istituire la rete DECT.

PREVENZIONI DELLE FRODI

Assicurare la prevenzione delle frodi è una priorità chiave per Let's Co e pertanto i CPE collegati alla LAN del cliente vengono gestiti con file di configurazione creati con l'intento di prevenire le frodi. Tutte le password di autenticazione SIP sono complesse e criptate all'interno del signaling per garantire l'impossibilità di essere intercettate.

Let's Co gestisce uno strumento complesso di intercettazione delle frodi che analizza attivamente le chiamate nel caso di attività sospette. Il sistema può adottare misure proattive per prevenire le frodi quando le chiamate risultano anomale e vengono, di conseguenza, bloccate. L'implementazione di questo strumento non deve essere considerata come una rete di sicurezza che consente la configurazione e l'utilizzo di un dispositivo CPE scarsamente protetto. E' pertanto unica responsabilità del cliente finale quella di proteggere l'infrastruttura tecnologica di Let's Co, attuando e configurando correttamente tutti i dispositivi on premises (switch, firewall, router, IP PBX, access point, etc.). Il responsabile IT o della sicurezza informatica del cliente finale dovrà accertarsi che gli utenti utilizzino correttamente il servizio, procedendo all'utilizzo di password e abilitazioni che rispecchino i requisiti minimi di sicurezza e confinino al massimo il rischio di frodi aziendali.

Nota bene: per sensibilizzare la giusta attenzione in merito alle frodi informatiche, vi segnaliamo che abbiamo pubbliche evidenze di come alcuni Hacker si intromettano in modo fraudolento nel sistema di comunicazione (applicazioni, centralino, gateway, etc.), approfittando di una scarsa protezione informatica o di un comportamento poco responsabile

da parte dell'utente finale. La finalità dei collegamenti è spesso quella di generare chiamate automatiche a pagamento verso numerazioni premium anche internazionali. In pochi minuti si possono generare frodi per decine di migliaia di euro non risarcibili. Vi invitiamo, quindi, a controllare costantemente il livello di sicurezza informatica aziendale, anche per le apparecchiature di comunicazione, e disabilitare, tramite il pannello di controllo di amministratore, le chiamate premium e quelle internazionali per gli utenti che non ne fanno uso o che non sono autorizzati. Il nostro servizio di assistenza tecnica è a vostra disposizione per supportarvi nelle attività di prevenzione delle frodi.