Garantire sicurezza all'azienda quando è necessario lavorare da remoto

Sebastien Roche, Chief Information Security Officer di Alcatel-Lucent Enterprise, illustra l'approccio di Alcatel-Lucent Enterprise alla continuità di business e alla sicurezza in questi tempi complessi.

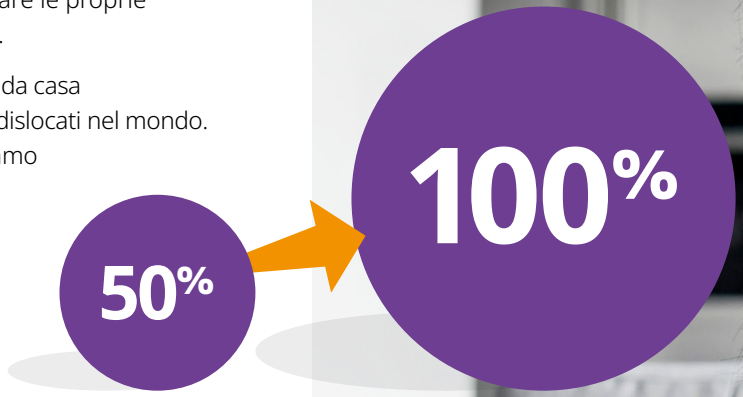
Brochure

Alcatel·Lucent Enterprise

La nuova realtà #WFH

A seguito della globale crisi sanitaria, le aziende, che in precedenza non offrivano la possibilità di lavorare da casa (#WFH), sono ora chiamate a trasformare le proprie organizzazioni per garantire la continuità e la sicurezza del business.

Nel 2008 Alcatel-Lucent Enterprise ha avviato un programma di lavoro da casa a cui ha aderito oltre il 50% dei 2.000 dipendenti, presenti nei 50 uffici dislocati nel mondo. Con oltre la metà dei dipendenti ALE che lavorano da casa, disponevamo già della rete e dell'architettura IT necessarie per supportare il lavoro a distanza. Pertanto, la sfida che abbiamo dovuto affrontare a causa della crisi globale, è stata quella di capire come passare dal 50% di lavoratori online al 100%.



Pronti all'azione

Nel 2017, ALE ha intrapreso un'ampia trasformazione informatica, adottando un'architettura di rete Service Defined WAN che ha fornito la sicurezza del cloud necessaria per bloccare in modo proattivo le minacce, identificare potenziali attacchi e garantire un accesso sicuro ai dipendenti.

La trasformazione comprendeva:

- Sicurezza in cloud grazie a access point virtuali
- Tracciamento dei dati in tempo reale
- Identificazione di modelli di comportamento insoliti per rilevare le minacce

Preparazione = risposta agile in situazioni di crisi

Quando siamo stati colpiti dalla crisi, abbiamo immediatamente deciso di implementare il lavoro a distanza, informado il personale il venerdì pomeriggio per il lunedì mattina. Ai dipendenti è stato chiesto di portare a casa laptop e monitor. Il lunedì mattina il lavoro è iniziato come di consueto, senza interruzioni, come se tutti lavorassero dall'ufficio e non da remoto. La trasformazione della rete intrapresa in precedenza ha garantito una connettività remota sicura, indipendentemente dal luogo di lavoro.

La sfida degli accessi

Una delle principali sfide che abbiamo dovuto affrontare riguardava i profili degli utenti, compresi quelli dei team di R&S e di assistenza tecnica, i quali hanno esigenze specifiche di accesso a determinati server e piattaforme di sviluppo che la nostra soluzione di accesso da remoto non consentiva. I profili di questi utenti passavano attraverso una soluzione di accesso privato diversa da quella utilizzata dal resto dei team.

Una volta iniziato il passaggio di tutti i dipendenti a #WFH, abbiamo adattato la nostra infrastruttura per aumentare la larghezza di banda per supportare l'aumento del numero di connessioni remote necessarie ai dipendenti che lavorano da casa.

La sicurezza è fondamentale

La sicurezza e la protezione dei dati aziendali sono estremamente importanti in tempi di incertezza soprattutto per le numerose organizzazioni che gestiscono dati sensibili, come organizzazioni del settore pubblico, ministeri, città e paesi.

Prima ancora di iniziare a parlare di #WFH in ALE, abbiamo implementato un'infrastruttura distribuita e protetta, nonché una soluzione di connessione privata completamente basata sul cloud per tutti i dipendenti, con l'obiettivo di garantire un accesso remoto sicuro alla rete. Abbiamo mantenuto la soluzione VPN legacy per una piccola percentuale di team con esigenze specifiche, come la connessione di apparecchi telefonici IP nei loro uffici remoti. Abbiamo anche fornito ai dipendenti PC professionali, con la possibilità di gestire il download automatico di software e gli aggiornamenti.

Impedire le violazioni alla sicurezza

Come previsto, durante il lavoro a distanza sono aumentate le chiamate e le e-mail relative a messaggi di posta elettronica sospetti e a richieste di aggiornamento delle password. Abbiamo anche assistito a un'impennata di attacchi di phishing e di attacchi mirati a software vulnerabili.

Sebbene l'uso dei proxy protegga ALE da importanti problemi di cybersecurity, ogni giorno assistiamo a nuove violazioni, dovute a e-mail, download o versioni non aggiornate di software/OS.

Mantenere aperte le comunicazioni

In ALE manteniamo un collegamento virtuale continuo con il personale, comunicando regolarmente, condividendo consigli e best practice e assicurandoci che il nostro team sia disponibile a supportare tutti i dipendenti.

Lista delle cose da fare di Alcatel-Lucent Enterprise per un lavoro remoto sicuro

- Evitare l'uso di dispositivi personali (PC) per lo scambio di dati e comunicazioni professionali
- Consentire l'accesso privato e sicuro ai dipendenti
- Automatizzare gli aggiornamenti software in tutta la rete aziendale
- Prestate attenzione alle richieste di posta elettronica sospette
- Utilizzare un software certificato. Gli audit e le certificazioni garantiscono l'autenticazione della sicurezza del software
- Semplificare i processi decisionali. In situazioni di emergenza, il CISO o il CIO devono prendere decisioni rapide per risolvere i problemi e garantire la continuità dei servizi

Sei raccomandazioni da parte di ALE per una connettività remota sicura

1. Automatizzare i promemoria per la modifica delle password

Aiutando i dipendenti a cambiare le password aziendali prima che scadano. Prima della scadenza i dipendenti riceveranno giornalmente un'e-mail con le istruzioni necessarie per cambiare la password.

2. Attivare il backup dei dati nel cloud

Incoraggiando i dipendenti a salvare regolarmente i loro dati per evitare qualsiasi perdita in caso di problemi ai computer portatili. Attivando spazi di archiviazione per il backup dei dati e offrendo assistenza remota attraverso il Service Desk IT o gli specialisti IT, se necessario.

3. Ricordare ai dipendenti le migliori pratiche di protezione dei dispositivi

Mantenendo il portatile in ottime condizioni:

- Spegnendolo alla fine di ogni giornata (evitare la modalità di sospensione/blocco).
- Tenendolo lontano da fonti di calore (come il sole o il riscaldamento).
- Evitando di mangiare o bere in sua prossimità.
- Fissando i cavi lontano da bambini e animali domestici

4. La sicurezza prima di tutto

Educare i team sui rischi e sulle migliori pratiche di sicurezza

- Incoraggiando i dipendenti a riflettere bene prima di cliccare sui link presenti nelle e-mail, anche quando sembra che siano state inviate da persone conosciute
- Offrendo un follow-up informatico in caso di dubbi
- Fornendo strumenti di segnalazione per le e-mail sospette
- Sfruttando la gamification per creare una cultura orientata alla sicurezza: in ALE, abbiamo impiegato la gamification per incoraggiare i dipendenti a rilevare e segnalare le e-mail sospette

5. Comunicare

L'isolamento rende le persone vulnerabili agli attacchi informatici, pertanto è necessario trovare il modo di mantenere in contatto il personale:

- Organizzando incontri di aggiornamento regolari, riunioni virtuali, eventi, spazi di collaborazione, happy hour.
- Incoraggiando le persone a connettersi regolarmente con i loro team
- Inviando regolarmente messaggi di posta elettronica per informare i dipendenti che il team IT è disponibile ad aiutarli e per ricordare loro le migliori pratiche di sicurezza

6. Incoraggiando abitudini di connessione sane

Il rischio del lavoro a distanza è quello di ritrovarsi con giornate lavorative di 12 ore con connessione sempre attiva e continue riunioni a distanza. E' fondamentale incoraggiare i dipendenti a prevedere tempi liberi lontani dallo schermo, a disconnettersi e a trascorrere del tempo con la propria famiglia o all'aria aperta.

Rainbow™ di Alcatel-Lucent Enterprise per la collaborazione connessa

Una piattaforma di collaborazione cloud per chat, chiamate video e audio, che consente la condivisione dello schermo e dei documenti e fornisce ai dipendenti ALE gli strumenti necessari per rimanere in contatto. La piattaforma è ampiamente utilizzata da tutti i dipendenti per collaborare con i colleghi.

Inoltre, anche i nostri partner e clienti hanno adottato Rainbow come soluzione di collaborazione preferita. Rainbow risponde ai requisiti di sicurezza del settore pubblico, della difesa, della sanità e di altri settori specifici ed è conforme alle rigorose normative di sicurezza, tra cui: GDPR, ISO 27001, HDS, ecc.

Brochure
Garantire sicurezza all'azienda quando è necessario lavorare da remoto

Sostenere la nostra comunità

ALE supporta gli sforzi della continuità di business di aziende, città e amministrazioni pubbliche, aiutandole a mantenere una continuità dei servizi in ambienti di lavoro remoti in sicurezza. Inoltre, per far fronte all'aumento della domanda e del numero di utenti, ALE ha ampliato la capacità di cloud hosting per soddisfare le esigenze dei clienti.

Per ulteriori best practice sulla sicurezza informatica, consultate le raccomandazioni dell'Agenzia europea per la cybersecurity (EU Cybersecurity Agency) .

Alcatel·Lucent
Enterprise