LINEE GUIDA PER IL LAVORO DA REMOTO PER PMIs

Guida per l'amministratore IT per la gestione della sicurezza del lavoro a distanza

La tua organizzazione potrà restare produttiva, e soprattutto sicura, ora che la pandemia da COVID-19 costringe molti dipendenti a lavorare da casa? Molte aziende di alto profilo come Google e Microsoft incoraggiano questo cambiamento senza grandi battute d'arresto. Tuttavia, per molte aziende e organizzazioni più piccole, la situazione è con tutta probabilità molto diversa.

La possibilità di lavorare in remoto è probabilmente riservata a pochi, e realisticamente è limitata a email e altri sistemi non operativi. Come fare in modo che l'infrastruttura e le disposizioni siano tutte in linea per garantire la continuità dell'attività?

Requisiti di base

Prima di tutto, per rimanere produttivi, ci sono alcuni requisiti comuni di cui tutti i lavoratori a distanza hanno bisogno.

- Un computer
- Una buona connessione internet
- Applicazioni di chat e videoconferenza
- Uno spazio di lavoro dedicato (preferenziale)
- Facoltativamente, un telefono
- Motivazione e disciplina
- Una rigida routine

Oltre alla consueta impostazione, un aspetto importante sta nel fatto che le aziende devono prepararsi e preparare i propri dipendenti agli **accresciuti rischi di sicurezza informatica** che il lavoro in remoto comporta.

Ma quali sono le sfide che ci si può trovare ad affrontare? Scopriamone alcune.

1. La sicurezza fisica dei dispositivi aziendali
2. La sicurezza IT aziendale quando i dipendenti sono a casa
3. Cosa aspettarsi nell'ambiente tecnologico di casa
4. Accedere alle reti e ai sistemi aziendali
5. Strumenti di collaborazione e processi di autorizzazione
6. Formazione sulla sicurezza informatica
7. Supporto e gestione delle crisi

1 La sicurezza fisica dei dispositivi aziendali

I dipendenti espongono i dispositivi aziendali a maggiori rischi nel momento in cui escono dalla sicurezza del posto di lavoro. I dispositivi devono quindi essere protetti contro lo smarrimento e il furto. Ecco alcune misure chiave e consigli su come assicurarsi che tutti i dispositivi rimangano sicuri.

- **Eseguire il logout quando non si utilizza il dispositivo**: ciò vale sia quando si è a casa che in spazi pubblici. Così è facile mettersi al riparo da figli curiosi che mandano per errore email al capo o ai clienti, o dall'eventualità che qualcuno acceda al dispositivo in un attimo di disattenzione al bar.
- **Una solida politica di utilizzo delle password:** imposta un timeout di inattività ed elimina i post-it con le password (sì, la gente ancora lo fa).
- **Non lasciare mai il dispositivo incustodito** o in bella vista. Se devi lasciarlo in auto, mettilo nel bagagliaio.

SUGGERIMENTO

La crittografia dell'intero disco è una soluzione semplice ma potente che garantisce che anche se il dispositivo cade nelle mani sbagliate, i dati dell'azienda non sono accessibili.

2 La sicurezza IT aziendale quando i dipendenti sono a casa

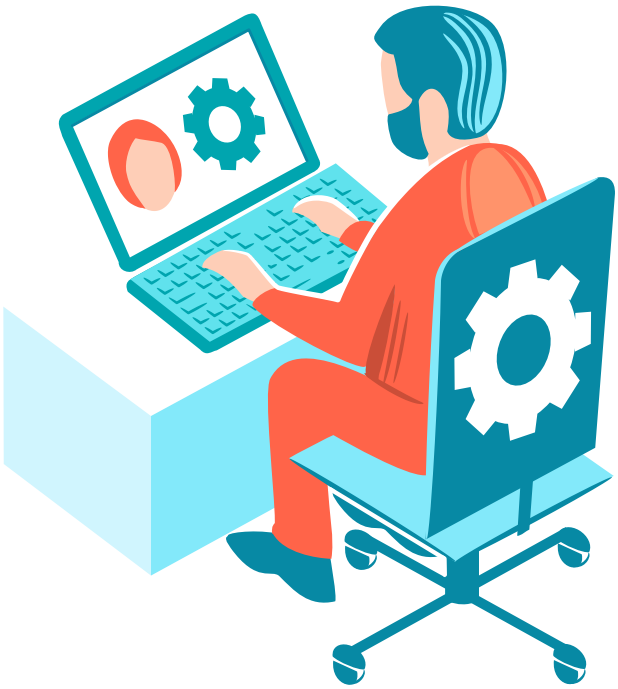
Ora che i dipendenti sono da soli nelle loro case, si ha una visibilità limitata su ciò che accade, soprattutto se non si è abituati a gestire e monitorare i dispositivi a distanza. Ora è un buon momento per imparare tutti i vantaggi della gestione remota e ridurre notevolmente il numero di problemi informatici che dovranno comunque affrontare.

L'utilizzo della gestione remota vi farà risparmiare tempo:

- Configurare e mantenere facilmente aggiornati tutti i sistemi. Subito, senza passare dall'uno all'altro.
- Pianificare le attività, definire le disposizioni ed eseguirle da parte di diversi gruppi di dipendenti.
- Ricevi notifiche sugli incidenti in tempo reale in modo da poter agire immediatamente quando si verifica un incidente.

SUGGERIMENTO

Se si dispongono fino 250 dispositivi, è possibile gestire facilmente la rete di computer tramite una console basata sul cloud. L'attivazione richiede solo pochi minuti.



3 Cosa aspettarsi nell'ambiente tecnologico di casa

È importante chiedere ai dipendenti di individuare eventuali vulnerabilità nel proprio ambiente casalingo prima che di collegare i dispositivi di lavoro. Riceviamo sempre più notizie sulla vulnerabilità dei dispositivi legati all'internet delle cose (IoT), e questo è un ottimo momento per far intervenire i dipendenti: basta che mettano in sicurezza i dispositivi con password solide e aggiornando firmware e software alle versioni più recenti.

Prendi in considerazione l'idea di promuovere, o addirittura di imporre, l'utilizzo di un app di home monitoring prima di permettere la connessione di dispositivi aziendali alle reti casalinghe. La scansione o il monitoraggio evidenzieranno quali dispositivi presentano vulnerabilità note, il cui software o firmware necessita di aggiornamento, e quali dispositivi hanno password predefinite da cambiare.

4 Accedere alle reti e ai sistemi aziendali

Stabilisci se il dipendente ha bisogno di accedere alla rete interna dell'azienda o se è sufficiente l'accesso ai servizi cloud e all'email. Valuta inoltre se è il caso di dare anche fuori sede lo stesso livello di accesso ai dati sensibili garantito in sede.

Se è necessario accedere alla rete interna dell'azienda:

- Si raccomanda vivamente di utilizzare solo dispositivi di proprietà dell'organizzazione in modo che il pieno controllo del dispositivo di connessione sia sotto la gestione del reparto di sicurezza informatica.
- Usa sempre un VPN per far collegare i lavoratori in remoto alla rete interna dell'azienda. In questo modo si evitano gli attacchi man-in-the-middle da reti decentrate. Ricorda che ora che si lavora da casa, il traffico passa per le reti pubbliche.
- **Controllare l'uso di dispositivi esterni come dispositivi di memorizzazione USB e periferiche**
- **Con molte persone che lavorano da casa, stanno diventando bersaglio di truffe o e-mail di phishing. Con le soluzioni di cloud-sandboxing è possibile tenere le e-mail sospette fuori dai limiti dei dispositivi dei dipendenti.**
- Limita la possibilità di archiviare, scaricare o copiare dati. Una fuga di dati può verificarsi da qualsiasi dispositivo che contenga dati sensibili dell'azienda.
- Considerate l'uso di macchine virtuali per fornire l'accesso. È più complesso da attuare, ma potrebbe rivelarsi una scelta migliore sul lungo termine.

Nel caso in cui alcuni (o tutti) i vostri dipendenti utilizzino dispositivi BYOD (i loro dispositivi personali), assicuratevi che, se consentite loro l'accesso ai servizi e-mail e ai servizi cloud, applichiate la stessa policy di sicurezza degli endpoint per gli antimalware, i firewall, ecc.di un dispositivo aziendale **Se necessario, fornisci al dipendente una licenza per le stesse soluzioni utilizzate nei dispositivi aziendali.** Se hai bisogno di licenze in più, contatta il fornitore di servizi. Potrebbe avere delle soluzioni per venire incontro alle tue esigenze in questa situazione senza precedenti.

SUGGERIMENTO

L'autenticazione a più fattori (MFA) assicura che ogni accesso, che sia per servizi cloud o per accessi di rete, sia consentito soltanto a utenti autorizzati. Cerca di usare quanto più possibile un sistema, tramite app o chiavetta fisica, per generare codici usa e getta per garantire accessi autenticati.

5 Strumenti di collaborazione e processi di autorizzazione

Può suonare strano accomunare questi due elementi nello stesso titolo, ma uno può aiutare a prevenire problemi con l'altro.

- È importante dare accesso a sistemi di chat e videoconferenza per permettere ai dipendenti di comunicare tra loro. Ciò garantisce gli strumenti necessari alla produttività e aiuta a mantenere la socialità tra colleghi.
- Usa gli strumenti collaborativi per evitare istruzioni o transazioni non autorizzate. I criminali informatici tendono a sfruttare le opportunità date dai lavoratori in remoto per lanciare attacchi BEC (Business Email Compromise). Si tratta di una richiesta fasulla inviata da un impostore, in cui si chiede un urgente trasferimento di fondi, senza la possibilità di convalidare la richiesta di persona.

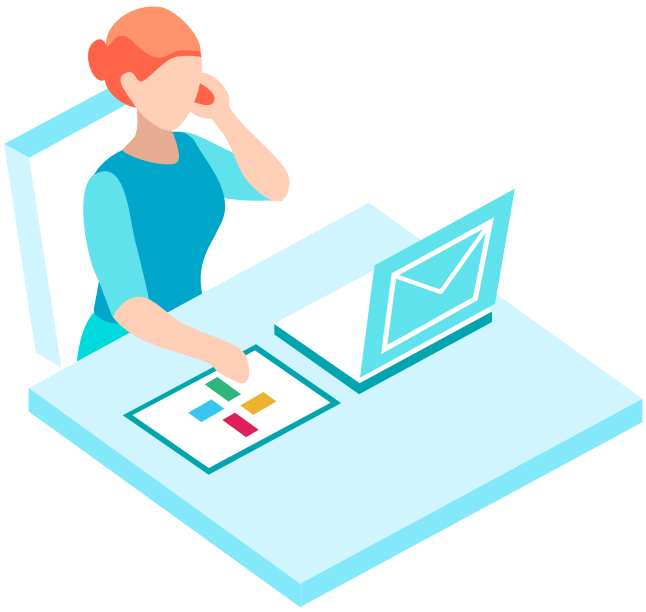
Assicurati di usare sistemi di videoconferenza e chat come parte formale del sistema di approvazione, così che le convalide siano effettuate "di persona" anche da remoto.

6 Formazione sulla sicurezza informatica

Stanno circolando diverse truffe a tema COVID-19 che rimandano a mascherine, vaccini e disinformazione. Quando i dipendenti passano dal posto di lavoro all'atmosfera ben più rilassata del lavoro da casa, potrebbero cedere ad aprire dei link, ora che non ci sono colleghi che rischiano di vederli guardare quel video divertente o aprire quella pagina web.

SUGGERIMENTO

La formazione sul tema della sicurezza informatica è in genere un requisito annuale per i dipendenti. Soprattutto ora, quando si lavora a distanza, si deve condurre una campagna ad hoc e chiedere ai dipendenti di seguire tale formazione.



7 Supporto e gestione delle crisi

Non sacrificate la sicurezza informatica o la possibilità di gestire sistemi e dispositivi nella fretta di approntare l'accesso remoto. La possibilità di dare supporto in remoto agli utenti è essenziale per evitare intoppi, soprattutto se si trovano in quarantena per motivi di sicurezza sanitaria. I lavoratori in remoto devono avere dei chiari protocolli di comunicazione col supporto informatico e di gestione delle crisi, nell'eventualità in cui riscontrino problemi insoliti o sospetti che potrebbero essere causati da una violazione.

Non dare per scontato che tutti i dipendenti riescano a passare al lavoro in remoto efficacemente e senza assistenza o indicazioni. La casa non è un ufficio, e potrebbero avere bisogno di consistente aiuto per adattarsi.

Come può essere d'aiuto ESET?

Quando si tratta di sicurezza in smartworking e delle sue sfide emergenti, potete fare affidamento su ESET. Ecco alcune delle nostre soluzioni che aiuteranno la vostra azienda a rimanere sicura e produttiva in questi tempi difficili.

GESTIONE REMOTA

ESET Cloud Administrator

La sicurezza gestita in cloud fino a 250 dispositivi consente di risparmiare costi e tempo e di semplificare la protezione della rete.

- Messa in funzione e attivazione in pochi minuti
- No hardware o software aggiuntivi
- Single point di gestione della sicurezza della rete
- Accessibile in modo sicuro tramite browser web da qualsiasi luogo

Scopri ora

DISPOSITIVI DI SICUREZZA

ESET Endpoint Protection

Tecnologia multistrato, machine learning e competenze umane combinate con la gestione automatizzata della sicurezza.

- Protezione facile da eseguire con la gestione remota cloud-based
- Protegge da attacchi mirati, ransomware e fileless
- Full Disk Encryption add-on

Scopri ora

ACCESSO SICURO

ESET Secure Authentication (Autenticazione sicura ESET)

Un modo semplice ed efficace per le aziende di tutte le dimensioni per implementare l'autenticazione a più fattori attraverso i sistemi comunemente utilizzati.
Consente alla vostra organizzazione:

- Prevenire le violazioni di dati
- Soddisfare i requisiti di conformità
- Soddisfare centralizzata dal proprio browser
- Utilizzare il telefono, o i token hardware

Scopri ora

Per ulteriori informazioni sulle soluzioni di Remote Working, visitate la nostra pagina web dedicata