ivanti

Report 2021 sulla sicurezza informatica per gli utenti:

Forza lavoro remota e sicurezza informatica

Il comportamento degli utenti mette a rischio la sicurezza informatica

La pandemia esplosa nel 2020 non solo ha scatenato un virus devastante a livello mondiale, ma ha anche stravolto ogni aspetto della nostra vita quotidiana, compreso il lavoro. In ogni settore, le persone hanno iniziato a lavorare da casa in ogni situazione in cui questo fosse possibile. La nuova modalità di lavoro in remoto ha consentito alle aziende di restare operative. Ma molte organizzazioni devono ora affrontare un forte incremento di minacce alla sicurezza informatica, dovuto all'utilizzo di dispositivi personali non protetti e al comportamento degli utenti stessi. Dopo oltre un anno di pandemia, come si presenta il panorama delle minacce informatiche?

A febbraio 2021, Ivanti ha pubblicato il Report 2021 sulla sicurezza informatica per gli utenti, che fa luce sulle minacce principali a cui sono ora esposte le aziende. I risultati si basano su un sondaggio condotto a novembre 2020 che ha coinvolto più di 2.000 persone maggiorenni che lavorano negli Stati Uniti e nel Regno Unito.

Nonostante le organizzazioni siano consapevoli delle vulnerabilità associate ad app e dispositivi personali non gestiti, questo report evidenzia anche comportamenti a rischio da parte di chi lavora da casa con un computer aziendale. Ad esempio, un utente su quattro ammette di usare l'e-mail o la password di lavoro per accedere a siti web e applicazioni consumer, quali app per la consegna di cibo a domicilio, siti per acquisti online e persino app di incontri.

Sicurezza aziendale più complessa

Molto probabilmente, anche quando si ritornerà a una certa normalità post-COVID, il lavoro in remoto è un aspetto che resterà una realtà. Le organizzazioni stanno tentando di arginare le lacune di sicurezza informatica associate al lavoro in remoto, ma occorre andare oltre la fornitura di hardware e software aziendali. Per meglio comprendere le sfide che ci attendono, esaminiamo alcuni risultati del sondaggio.

1 utente su 4

ammette di usare l'e-mail o la password di lavoro per accedere a siti web e applicazioni consumer, quali app per la consegna di cibo a domicilio, siti per acquisti online e persino app di incontri.

Le abitudini dei lavoratori remoti mettono a rischio le aziende

Per meglio comprendere il livello di sicurezza del tipico ambiente di lavoro a casa, sono state poste ai partecipanti al sondaggio domande che riguardano il loro comportamento e le prassi di sicurezza per tutti i loro dispositivi, inclusi i dispositivi IoT presenti in casa.

Credenziali riciclate:
Quasi il 25% dei partecipanti dagli Stati Uniti e il 20% di quelli dal Regno Unito ammettono di usare l'e-mail o la password di lavoro per accedere ad app e siti web consumer.

Dispositivi personali per accedere a risorse di lavoro:
Quasi il 50% dei partecipanti dagli Stati Uniti e il 33% di quelli dal Regno Unito affermano di essere autorizzati a usare un dispositivo personale (come un laptop, smartphone, tablet o smartwatch) per accedere alle applicazioni e reti aziendali.

Autenticazione a due fattori per dispositivi IoT:
Quasi il 50% dei partecipanti dagli Stati Uniti e dal Regno Unito non ha impostato l'autenticazione a due fattori per i dispositivi smart usati in casa.

Punti chiave: Non trascurare pratiche di sicurezza di base a casa

La carenza di misure di protezione di base nei dispositivi IoT utilizzati in ambiente domestico lascia gli utenti e le aziende vulnerabili a minacce informatiche, come l'hackeraggio delle telecamere Ring diventato virale nel 2019.

Cattive abitudini in fatto di sicurezza (ad esempio, utilizzare le stesse password sia per lavoro che per accedere a siti consumer) possono esporre le aziende a un maggior rischio di violazioni. È quindi importante assicurare una chiara distinzione tra app e siti usati per lavoro e a scopo personale.

La sicurezza aziendale non è sufficiente per tutta la forza lavoro remota

Dall'inizio della pandemia si è verificato un netto aumento di attacchi informatici che hanno preso di mira i dispositivi personali e i dispositivi IoT domestici non protetti. Questi sono in parte attribuibili alle cattive abitudini degli utenti in fatto di sicurezza.
Ma dal sondaggio emerge anche che le aziende stesse possono migliorare la sicurezza in alcune aree chiave.

25%

Sicurezza software:
Più del 25% dei partecipanti afferma che non era stato richiesto loro di dotare il proprio dispositivo di un software di sicurezza per accedere da casa ad alcune applicazioni aziendali.

Aggiornamento delle password:
Per circa il 25% dei partecipanti negli USA e in UK, l'azienda non richiede di aggiornare la password ogni sei mesi o di usare un generatore di codici monouso.

30%

Strumento per accesso sicuro:
Per quasi il 30% dei partecipanti negli USA e in UK, l'azienda non richiede l'uso di uno strumento per accesso sicuro, ad esempio una VPN.

Punti chiave: La sicurezza zero-trust è fondamentale.

L'ambiente di lavoro remoto è una realtà destinata a durare nel tempo. Le organizzazioni IT aziendali hanno migliorato la sicurezza mobile in alcune aree, ma è necessario migliorare anche l'autenticazione su tutti i dispositivi che vengono usati per lavorare.

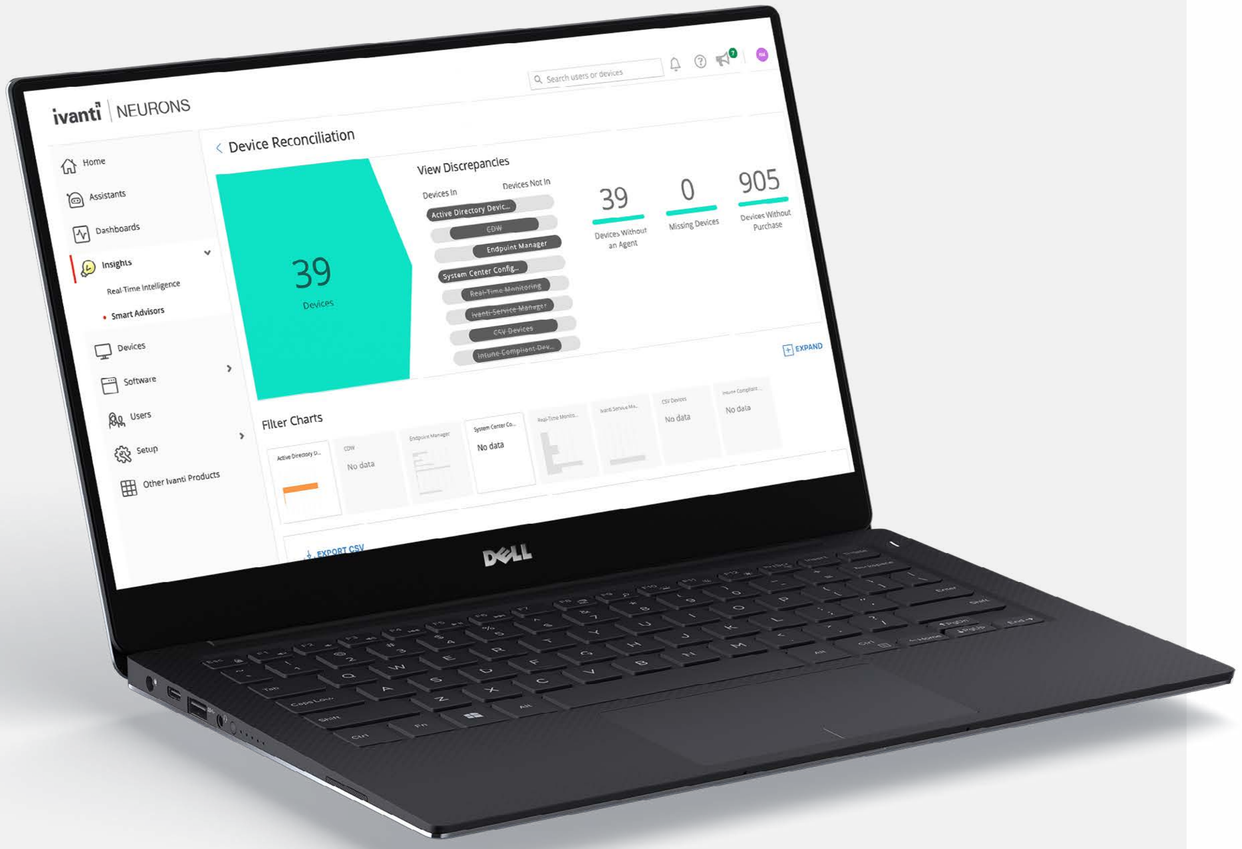
Per garantire la protezione dell'intero ambiente nel nuovo Everywhere Workplace, serve un framework zero-trust che assicuri la verifica diretta, automatizzata e continua degli utenti, dei dispositivi, delle applicazioni, delle reti e del cloud.

Utenti protetti, aziende protette

La crescita esponenziale delle persone che lavorano in remoto ha portato alla rapida espansione del panorama delle minacce informatiche. Le organizzazioni devono quindi considerare strategie chiave per garantire la protezione di applicazioni e dati e sopperire alle lacune nella sicurezza IoT e nell'ambiente di lavoro a casa. Con la sempre maggiore diffusione di dispositivi consumer, per chi lavora in remoto può essere difficile attivare e mantenere impostazioni di sicurezza complesse. I criminali informatici contano proprio su questo e sono pronti a sfruttare le porte lasciate aperte dalla mancanza di misure di sicurezza adeguate. Oltre a minacciare la salute delle persone su scala globale, la pandemia da COVID-19 mette anche a rischio la nostra sicurezza.

Ma ecco le buone notizie: un approccio zero-trust può essere adottato fin da subito

È possibile iniziare subito a implementare protocolli zero-trust applicabili all'intera forza lavoro. Grazie a un modello zero-trust, le aziende possono eliminare il rischio di furto di credenziali e verificare che chiunque acceda a dati, applicazioni o reti aziendali sia effettivamente un'entità affidabile. Inoltre, con il consolidarsi del lavoro in remoto e la proliferazione dei dispositivi, la sicurezza zero-trust può facilitare l'applicazione di policy di utilizzo accettabile, quali autenticazione a più fattori, protezione dei dispositivi e connettività sicura delle reti.



Metodologia

I risultati presentati in questo primo Report sulla sicurezza informatica per gli utenti si basano su un sondaggio condotto a novembre 2020. L'obiettivo dello studio era esaminare il cambiamento delle abitudini di utenti e aziende in fatto di sicurezza informatica nel corso della pandemia. Al sondaggio ha partecipato un campione rappresentativo di 2000 persone maggiorenni residenti negli Stati Uniti e nel Regno Unito che lavorano da casa con un computer fornito dall'azienda.

Informazioni su Ivanti

La piattaforma di automazione di Ivanti aiuta le aziende a rendere ogni connessione IT più smart e più sicura per tutti i dispositivi, le infrastrutture e le persone. Dai PC ai dispositivi mobili, all'infrastruttura di desktop virtuali e i data center, Ivanti rileva, gestisce, protegge ed eroga servizi agli asset IT dal cloud all'ambiente perimetrale nella nuova realtà dell'Everywhere Workplace, fornendo al contempo esperienze personalizzate ai dipendenti. Nell'Everywhere Workplace, i dati aziendali scorrono liberamente attraverso dispositivi e server, consentendo agli utenti di lavorare al meglio ovunque e con la modalità che preferiscono. Ivanti ha sede centrale a Salt Lake City (UT, Stati Uniti) e uffici in tutto il mondo. Per ulteriori informazioni, visitate www.ivanti.com e seguiteci su Twitter @GoIvanti

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com