MICRO FOCUS

Opuscolo sul prodotto

ZENworks Endpoint Security Management
ZENworks Full Disk Encryption

ZENworks Endpoint Security Management e ZENworks Full Disk Encryption

Sono le sei di un venerdì mattina. Sapete dove si trovano i vostri endpoint? Uno di essi sta subendo l'intrusione di un hacker. Si tratta di un computer portatile. L'utente si trova nel WifiCafe. Naviga nel Web, convinto di essere al sicuro perché la connessione è etichettata come "WifiCafe". Accanto a lui, però, anche qualcun altro si trova sulla stessa interfaccia Web, intento a effettuare un tunneling tramite collegamento diretto al vostro database.

Informazioni su ZENworks Endpoint Security Management e ZENworks Full Disk Encryption

- **Cifratura:**
  Cifrate i dati salvati sui dispositivi portatili
- **Sicurezza dinamica:**
  Implementate una protezione che valuta i livelli delle minacce e risponde in modo appropriato, in base al tipo di utente e alla sua posizione
- **Produttività e sicurezza continue:**
  Offrite agli utenti il controllo di ciò di cui hanno bisogno per mantenere la produttività, evitando di far loro aggirare le policy di sicurezza
- **Acquisto standalone o come parte di:**
  ZENworks Suite

Qualcuno sta tentando di attaccare il vostro sistema e il vostro utente non ne è al corrente. Non sa che può verificarsi; pensa di essere al sicuro.

Si tratta di un attacco "man-in-the-middle", in cui un soggetto esterno si è impadronito di informazioni da un portatile della vostra azienda.

Gli endpoint sono fonte di preoccupazione

I dispositivi endpoint rappresentano uno dei principali rischi per la sicurezza delle organizzazioni. Infatti, fino al 70% dei dati aziendali più importanti viene conservato e trasportato su dispositivi endpoint.

Non si tratta di uno scenario di furto convenzionale in cui vi vengono sottratti i computer (per quanto dobbiamo fermare anche questa minaccia). Stiamo parlando di protezione contro criminali che possono impossessarsi dei vostri dati mentre i dispositivi sono in uso.

Gli attacchi man-in-the-middle non sono che un esempio di decine di gravi minacce da cui è necessario proteggersi. Ne esistono infatti altre, come:

- **Drive bombing.** Gli utenti vengono invitati a collegare ai dispositivi aziendali pen drive gratuiti o trovati, causando il rilascio automatico di pericolosi virus senza che nemmeno se ne accorgano.
- **Utilizzo di pen drive non autorizzato.** Gli utenti usano i propri pen drive al lavoro e inseriscono dati su di essi, provocando così movimenti incontrollati dei dati, che restano fuori dalla portata delle policy di sicurezza.
- **Furto.** Qualcuno ruba un computer portatile. O, peggio ancora, dei dipendenti con cattive intenzioni impiegano endpoint non sicuri e sfruttano le vulnerabilità dall'interno.
- **Hacking.** Un hacker esterno può far penetrare software dannoso nei dispositivi aziendali, sperando che non venga intercettato dal firewall e riesca a infettare l'intero sistema.

Potete cercare di impedire tutto questo. Siete voi a stabilire regole e policy. Ma non potete essere certi che le persone rispettino tali policy. La cifratura potrebbe essere una soluzione, ma è costosa. E se l'utente smarrisse la sua password? Nessuno potrebbe recuperare i dati. Deve esserci una soluzione migliore.

Vi serve un modo per garantire che le policy che proteggono l'azienda vengano sempre applicate. In questo modo, non dovrete più semplicemente sperare che il personale rispetti le regole. Avrete la certezza che lo farà, perché le policy lo garantiscono.

Il potere delle policy

La verità è che non potete semplicemente contare sul fatto che le persone non creeranno problemi. Dagli hacker ce lo si aspetta, ma il personale interno rappresenta una minaccia altrettanto grande. La maggior parte di loro semplicemente non sa come comportarsi in modo sicuro davanti a un computer e un solo dipendente con intenzioni negative è già sufficiente per creare danni.

Vi serve un modo per garantire che le policy che proteggono l'azienda vengano sempre applicate. In questo modo, non dovrete più semplicemente sperare che il personale rispetti le regole. Avrete la certezza che lo farà, perché le policy lo garantiscono.

Ogni singola volta.

Voi potrete modificare tali policy in qualunque momento, al contrario dei vostri utenti. Ed è questo il punto cruciale: non dipenderà dagli utenti, bensì dalle policy.

Come rimediare agli errori

Gli utenti commettono errori, come dimenticare un computer portatile in aeroporto. Benché la perdita di un computer sia comunque sgradevole e costosa, con Micro Focus® ZENworks® Full Disk Encryption tutti i dati più importanti in esso contenuti risultano indecifrabili a chiunque se ne appropri. Grazie a Full Disk Encryption, non dovete più preoccuparvi della posizione in cui l'utente salva i dati sul disco rigido: sull'unità tutto è cifrato.

Per citare una possibilità più ordinaria, seppure altrettanto comune, l'utente potrebbe perdere una password. Con altri software di cifratura, gli addetti dell'help desk non hanno potere: senza quella password il disco rigido è totalmente impenetrabile. Con ZENworks, invece, il recupero dei dati diventa una procedura standard di assistenza. L'utente viene aiutato a reimpostare la propria password oppure potete occuparvi voi stessi della gestione del dispositivo: in un modo o nell'altro la cifratura che protegge i dati non vi esclude completamente dalla loro portata.

Sono le otto di un mercoledì mattina. Siete al corrente di cosa sta scaricando sul suo pen drive il dipendente alla postazione sei? Il vostro CFO in viaggio si ricorderà di portare con sé la sua borsa per il computer portatile quando sale sull'aereo?

Poliziotto buono, poliziotto cattivo

Micro Focus ZENworks Endpoint Security Management è il più avanzato strumento per l'applicazione delle policy su dispositivi endpoint. Riconosce i vostri utenti e sa cosa possono (e non possono) fare. A differenza di qualsiasi altra soluzione, sa anche dove si trovano gli utenti e si regola in modo dinamico per adeguarsi al livello di rischio.

Quando si combina la potenza di applicazione delle policy di Endpoint Security Management

con la sicurezza fornita da Full Disk Encryption, è facilissimo tenere a distanza i malintenzionati esterni, mentre i dipendenti interni determinati a comportamenti lesivi dell'azienda non hanno gli strumenti per mettere in pratica i loro propositi e gli utenti virtuosi, che desiderano solo fare il proprio lavoro, non incapperanno in guai. I vostri dati sono al sicuro.

Produttività sicura

Ottenete il perfetto equilibrio tra produttività e protezione. Con ZENworks Endpoint Security Management e ZENworks Full Disk Encryption, potete:

- Applicare un tipo di sicurezza che valuta in modo dinamico i livelli di rischio in base agli utenti e a dove si trovano, quindi agisce di conseguenza modificando le policy (ad es. le connessioni WiFi) al volo.
- Cifrare i dati salvati sui dispositivi portatili.
- Applicare policy severe contro gli usi impropri, ad esempio il controllo di ciò che gli utenti di dispositivi USB possono e non possono utilizzare.
- Lasciare ai dipendenti il controllo totale sulle attività necessarie alle loro mansioni, impedendo loro però di eludere standard e policy di sicurezza.

Sicurezza eccezionale

ZENworks Endpoint Security Management è il più avanzato strumento per l'applicazione delle policy. Non cede a tentativi di corruzione o bullismo e non dorme mai. Garantisce che le vostre policy siano rispettate in ogni occasione.

Sono le otto di un mercoledì mattina. Siete al corrente di cosa sta scaricando sul suo pen drive il dipendente alla postazione sei? Il vostro CFO in viaggio si ricorderà di portare con sé la sua borsa per il computer portatile quando sale sull'aereo?

Se disponete di ZENworks Endpoint Security Management e ZENworks Full Disk Encryption, non dovrete preoccuparvene.

Informazioni su Micro Focus

Dal 1976, Micro Focus ha aiutato oltre 20.000 clienti a liberare il valore della propria logica di business, realizzando soluzioni che consentono di colmare il divario tra le tecnologie più affermate e le funzionalità moderne. I due portafogli concorrono a realizzare una visione chiara e unificata: fornire prodotti innovativi con il supporto di un servizio clienti eccezionale.
www.microfocus.com

"Dobbiamo proteggere la nostra rete contro virus, hacker e un'enorme quantità di minacce per l'azienda. Con ZENworks Endpoint Security Management di Novell (oggi parte di Micro Focus), otteniamo il meglio su due fronti: gli utenti mobili sono liberi di usare l'accesso remoto, mentre noi abbiamo la certezza che non esistano rischi per la rete."

LAURA DAVIS
Technology Lead
Woolpert, Inc.

“Il ROI di ZENworks Endpoint Security Management di Novell (oggi parte di Micro Focus) è stupefacente già di per sé. Se evitiamo anche una sola violazione di dati, possiamo risparmiare 3 milioni di dollari di spese legali.”

ROBB PETTIGREW
Manager, Technical Systems e Help Desk
Wyoming Medical Centre

Micro Focus
Italia
+39 02 366 349 00

Micro Focus
Sede centrale
Regno Unito
+44 (0) 1635 565200

www.novell.com