INFOGRAFICA

Zero trust: la difesa definitiva contro i ransomware

Gli attacchi dei ransomware in evoluzione bypassano la sicurezza di rete tradizionale

Dato che negli ultimi due anni utenti, applicazioni e dati sono usciti dal perimetro, la portata e l'impatto dei ransomware sono aumentati. I singoli aggressori sono stati soppiantati da dei veri e propri gruppi, all'interno dei quali si acquistano e vendono competenze e kit di strumenti specializzati. Gli attacchi, che un tempo erano estesi e unidimensionali, ora utilizzano tattiche mirate e multilivello che sono quasi impossibili da bloccare con le architetture di sicurezza legacy a castello e fossato.

$20 MRD
di danni stimati dovuti ai ransomware nel 2020

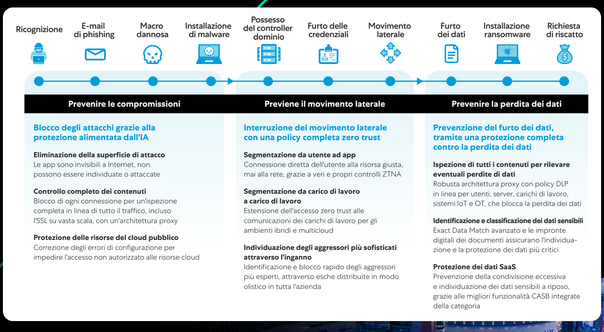
Ogni 14 secondi
nel mondo si verifica un attacco ransomware

500%
di incremento dei ransomware nascosti nell'SSL per bypassare le difese tradizionali

I ransomware rappresentano il più grande rischio per il business digitale.

Compromissione iniziale	Movimento laterale	Esfiltrazione dei dati per la doppia estorsione	Installazione del ransomware e crittografia delle macchine	Richiesta del ransomware
80% degli attacchi inizia con e-mail di phishing	**94%** delle infezioni impiega meno di 4 ore per diffondersi	**50%** di tutti gli attacchi ransomware è rappresentato da violazioni dei dati	**200%** di incremento dei tempi di inattività a causa del ransomware	**$234K** riscatto medio per un ransomware

Architettura zero trust



Zero trust: la strategia più efficace per la protezione dai ransomware

Prevenzione dei ransomware di livello superiore:
L'ispezione in linea di tutto il traffico per le aziende mobili e cloud-first di oggi riduce al minimo la superficie di attacco ed elimina il movimento laterale.

Soppiantare le soluzioni tradizionali:
Lo zero trust offre un approccio completamente diverso rispetto alle tradizionali architetture di sicurezza della rete a castello e fossato, in quanto collega direttamente gli utenti alle app, mai alla rete.

Sicurezza a supporto del business:
Complessità e costi vengono abbattuti grazie a un modello in cui la sicurezza è interamente fornita sul cloud, il quale elimina l'infrastruttura tradizionale e potenzia l'agilità aziendale e l'esperienza utente.

I vantaggi aziendali e di sicurezza dell'adozione dello zero trust

Riduzione dei rischi impareggiabile

La superficie di attacco e i movimenti laterali vengono eliminati, grazie a una protezione dalle minacce informatiche e dei dati di livello superiore

35x
riduzione delle macchine infette

NOV

Time to value più rapido

Essendo una soluzione distribuita come un vero e proprio insieme di servizi cloud senza infrastruttura, è operativa in <24 ore

Distribuzione di
oltre 10 mila utenti
in <48 ore

NORDSTROM

Miglior valore

Vengono eliminati i prodotti puntuali di sicurezza e le operazioni vengono rese più semplici

70%
di riduzione dei costi

SIEMENS

Vuoi saperne di più su come salvaguardare l'azienda con la difesa ransomware più completa del settore? Scarica l'eBook.

Leggi l'eBook →

Fonte: https://www.unitrends.com/solutions/ransomware-education

zscaler™