ISL Member of the DTS Group

DTS IDENTITY CLIENT

L'"endpoint" vale oro per qualsiasi hacker poiché siamo circondati ovunque da dispositivi finali, basti pensare che il numero di dispositivi collegati in rete sta raggiungendo il miliardo. Tuttavia, alcuni di essi sono obsoleti e dipendono dall'utilizzo che ne fa l'utente. L'88% di tutte le violazioni di dati è causato infatti dall'errore umano. Se le aziende non si assicurano che ogni dispositivo che ha accesso alle risorse interne sia anche conforme alle policy di sicurezza, queste offrono agli aggressori una via di accesso perfetta. DTS Identity è LA piattaforma per tutte le identità. Con il DTS Identity Client, rafforziamo ulteriormente la soluzione offrendo il VERO Zero Trust di Identity.

CHE COS'È IL "CLIENT" DI DTS IDENTITY?

Il DTS Identity Client non è una soluzione indipendente, ma è direttamente collegata all'IAM di DTS Identity. Permette non solo di identificare e autenticare l'utente, ma anche di includere come fattore importante il dispositivo associato all'utente e il suo stato. Allo stesso tempo, tutte le funzionalità di DTS Identity vengono estese anche al client. In questo modo, il nostro Identity & Access Management, interamente sviluppato da noi, è in grado di garantire al meglio l'implementazione di una strategia Zero Trust.

Per garantire che utilizziate sempre l'ultima versione disponibile, la soluzione viene offerta esclusivamente "as a Service". Ciò significa che DTS Identity Client può essere utilizzato senza dispendio di risorse e senza doversi preoccupare dell'hosting. Naturalmente, la soluzione viene ospitata esclusivamente nei nostri data centre tedeschi certificati.

CHE COS'È IL "CLIENT" DI DTS IDENTITY?

1. TRASPARENZA

- Visibilità di tutti i dispositivi nella rete
- Stato dei dispositivi visualizzabile con un clic
- Panoramica di quanti dispositivi accedono alle applicazioni aziendali e di quando accedono
- Una maggiore trasparenza consente di stabilire più regole

2. IMPOSTAZIONE DI REGOLE

- Impostazione di policy specifiche o universali per endpoint e MFA
- L'impostazione di regole per le policy di conformità avviene in maniera centrale su DTS Identity utilizzando la nostra Conditional Access Feature
- Esempio di use case: secondo le policy di conformità, l'accesso alle app aziendali è permesso solo con dispositivi sicuri. I dispositivi necessitano di una versione aggiornata del sistema operativo e, ad esempio, di un firewall attivo e/o un antivirus. L'accesso alle applicazioni (importanti) è consentito solo dopo aver verificato che il dispositivo soddisfi tutti i criteri.

3. APPLICAZIONE DELLE REGOLE, AUDIT E LOG

- Tracciamento e assegnazione delle policy di conformità
- La trasparenza dei log consente di vedere direttamente quali client sono/erano attivi, in quale forma e perché
- Utilizzabile per audit e documentazione di conformità

4. COMBINAZIONE DI SICUREZZA DELLA RETE, DEI DISPOSITIVI E DELLE IDENTITÀ

- Combinazione ottimale per la messa in sicurezza della rete, dei dispositivi e delle identità:
  - DTS Identity: login, MFA e Conditional Access (applicazione di policy)
  - DTS Identity Client: visibilità del dispositivo e dello stato del dispositivo stesso
  - ARP-GUARD NAC: protezione della rete

ISL Internet Sicherheitslösungen GmbH
+49 234 976672-0

Alte Wittener Str. 70
44803 Bochum

isl.de/it
italy@isl.de

DTS Red Teaming Service 06112024 it