Dynabook crede nei notebook Windows 10 Secured-core, con Microsoft

- Ultima modifica: Giovedì, 07 Novembre 2019 19:47
Pubblicato: Giovedì, 07 Novembre 2019 19:38
Scritto da Laura Benedetti

Dynabook collabora ai PC Secured-core Windows 10 con Microsoft, per offrire dispositivi più sicuri con una stretta integrazione tra hardware, software e funzionalità avanzate. I primi "già certificati" sono Portégé X30-F, Tecra X40 e Tecra X50F.

Dynabook ha annunciato una collaborazione con Microsoft per la realizzazione dei dispositivi Windows più sicuri. I **notebook "Windows 10 Secured-core"** sono progettati con una stretta integrazione tra **hardware** e **software** e sono dotati delle più **avanzate CPU** disponibili per garantire la sicurezza contro le cyber minacce attuali e future. I primi device dynabook a offrire questo nuovo livello di protezione hardware, software e dell'identità out-of-the-box sono disponibili sul mercato, rendendo l'azienda uno dei primi produttori a portare sul mercato i PC Secured-core. Si tratta nello specifico di **Portégé X30-F** da 13.3 pollici, **Tecra X40-F** da 14 pollici e **Tecra X50-F** da 15.6 pollici.

Dynabook crede nei notebook Windows 10 Secured-core, con Microsoft

- Ultima modifica: Giovedì, 07 Novembre 2019 19:47
Pubblicato: Giovedì, 07 Novembre 2019 19:38
Scritto da Laura Benedetti

I PC Secured-core sono destinati alla gestione dei **dati mission-critical** e alla protezione dei dipendenti che operano in settori maggiormente data-sensitive, come gli operatori sanitari che gestiscono cartelle cliniche e altre informazioni di identificazione personale (PII), industrie di alto profilo obiettivo di phishing e di altri attacchi così come le aziende con mobile worker che richiedono l'accesso alle informazioni business-critical al di fuori dell'ufficio.

In particolare, un notebook Secured-core utilizza **componenti di sicurezza** basati sull’hardware come **Platform Module 2.0 (TPM) e CPU di ultima generazione** insieme alla sicurezza virtualisation-based (VBS) e al servizio Windows hypervisor code integrity (HVCI) per creare un ambiente sicuro e separato dall’hardware, che isoli efficacemente la memoria e i componenti critici per prevenire gli attacchi e gli accessi non autorizzati agli elementi critici del

sistema operativo.

Basandosi sulle funzionalità di sicurezza avanzate integrate nelle moderne CPU, i PC Secured-core proteggono l'integrità di Windows e il processo di avvio contro gli attacchi sofisticati a livello firmware. Il PC usa il metodo **Dynamic Root of Trust Measurement (DRTM)** per lanciare il sistema nella massima sicurezza, trasferendo il controllo dalla CPU direttamente al loader **hypervisor di Windows** tramite un handoff sicuro e misurato. Con l'hypervisor Windows lanciato in modo sicuro in uno stato misurato dall'hardware, l'ambiente VBS viene quindi creato nella memoria per isolare le chiavi e i processi critici dal normale sistema operativo Windows che verrà presto avviato.

Per garantire ulteriormente la loro sicurezza contro furti, compromissioni e attacchi di phishing, i

Dynabook crede nei notebook Windows 10 Secured-core, con Microsoft

- Ultima modifica: Giovedì, 07 Novembre 2019 19:47
Pubblicato: Giovedì, 07 Novembre 2019 19:38
Scritto da Laura Benedetti

PC Secured-core utilizzano **Windows Hello** per prevenire gli attacchi all'identità dell'utente e quelli basati sulle credenziali attraverso una combinazione di sensori biometrici e lo storage delle credenziali basata su hardware. Questo include il volto, le impronte digitali, la chiave FIDO2 sicura o l'autenticazione tramite PIN, mentre Credential Guard sfrutta la **sicurezza della virtualizzazione (VBS)** per bloccare gli strumenti utilizzati in questi attacchi e garantire che il malware in esecuzione nel sistema operativo non possa estrarre i token di autenticazione.

In caso di smarrimento o furto, uno degli anelli più deboli della catena della sicurezza è l'accesso fisico al dispositivo stesso. Un PC Secured-core è un device Windows moderno dotato del più alto livello di protezione di hardware, software e identità già pronto all'uso. Fornisce massima sicurezza contro la potenziale perdita di dati, proteggendoli da attacchi drive-by che possono portare alla divulgazione di informazioni sensibili o all'iniezione di malware. I PC Secured-core impediscono alle periferiche esterne di avviare ed eseguire il **Kernel Direct Memory Access (DMA)** a meno che i driver di queste periferiche non supportino l'isolamento della memoria. Le periferiche con driver compatibili saranno automaticamente riconosciute, avviate e autorizzate ad eseguire il DMA nelle regioni di memoria loro assegnate.

Come impostazione predefinita, le periferiche con driver incompatibili non effettueranno l'avvio e l'esecuzione del DMA fino a quando un utente autorizzato non accede al sistema o sblocca lo schermo. Inoltre, il PC usa **BitLocker Drive Encryption** per proteggere i dati dell'utente e garantire che il computer non sia stato manomesso mentre il sistema era offline. Queste misure addizionali di sicurezza forniscono l'autenticazione multi-fattore e garantiscono che il PC non si avvii o riprenda dall'ibernazione fino a quando non vengono inseriti PIN o chiave di avvio corretti.