Device Trust: gestione e sicurezza dei dispositivi nell’architettura Zero Trust

Questo articolo fa parte di una serie di approfondimenti dedicati al modello Zero Trust: il seguente testo si concentra sul pilastro fondamentale del Device Trust. Il contenuto esplora le strategie di gestione dei dispositivi in un contesto Zero Trust, analizzando le diverse categorie di dispositivi, le tecnologie di sicurezza essenziali e i rischi mitigati attraverso un approccio strutturato alla sicurezza degli endpoint.

Una volta verificata l’identità dell’utente, è fondamentale valutare il dispositivo che l’utente sta utilizzando. Come accennato nella sezione introduttiva, le modalità di lavoro agile e in mobilità hanno ampliato l’utilizzo non solo di dispositivi aziendali, ma anche di dispositivi di proprietà dell’utente (Bring Your Own Device, BYOD) o dispositivi utilizzati in contesti estemporanei, come quelli di terzi, di internet café o stazioni condivise pubbliche.

La classificazione del livello di fiducia da riporre in un dispositivo è un aspetto cruciale, poiché determina se il dispositivo può accedere ai sistemi dell’organizzazione e a quali risorse. Questa classificazione dipende dal controllo che l’organizzazione ha sul dispositivo e dal suo stato di sicurezza. Con l’evoluzione delle modalità di lavoro e la varietà di dispositivi nelle organizzazioni di medio-grandi dimensioni, è essenziale categorizzare i dispositivi in base al livello di sicurezza e al controllo esercitato dall’organizzazione.

Le principali categorie di dispositivi sono:

Dispositivi completamente gestiti dall’organizzazione

Questi dispositivi sono dotati di un client specifico per la gestione degli endpoint e dei dispositivi mobili, siano essi on-premise o in cloud. La presenza di un client di gestione consente all’organizzazione di assicurarsi che il dispositivo sia aggiornato, protetto da sistemi antivirus, anti-malware ed EDR/XDR, e conforme alle policy di sicurezza. Inoltre, permette di controllare il software installato, operare remotamente sul dispositivo e applicare policy per garantire la sicurezza, nonché configurare l’accesso alla rete.

Questo rappresenta il livello più alto di protezione possibile, poiché i dispositivi possono essere resi sicuri tramite l’applicazione delle policy di conformità prima di concedere l’accesso ai sistemi. Di solito, questi dispositivi sono di proprietà dell’organizzazione, ma potrebbero essere inclusi anche dispositivi personali con il consenso del proprietario, che deve accettare una riduzione del controllo sul proprio dispositivo. I dispositivi particolarmente critici, come quelli utilizzati dagli amministratori di sistema, possono essere integrati con tecnologie di Security Information and Event Management (SIEM) per raccogliere dettagli sugli eventi del dispositivo e correlare queste informazioni con altre attività di rete, al fine di individuare potenziali segnali di attacco.

Dispositivi con gestione limitata

Questi dispositivi utilizzano sistemi di endpoint management limitato, come antivirus, anti-malware o EDR con console di gestione centralizzata. Sebbene il livello di sicurezza e controllo non sia paragonabile a quello dei dispositivi completamente gestiti, è comunque possibile intervenire in caso di incidente, ad esempio disconnettendo il dispositivo dalla rete aziendale o rimuovendo minacce identificate. Questa

categoria può includere dispositivi personali, oltre a quelli aziendali, purché siano dotati di agenti software adeguati. Il livello di fiducia è intermedio, consentendo un certo grado di accesso ai sistemi aziendali, ma con restrizioni in funzione del profilo di rischio.

Dispositivi non gestiti

Questa categoria include dispositivi privi di agenti di gestione o con agenti che non sono sotto il controllo dell'organizzazione. Tipicamente, si tratta di dispositivi personali, dispositivi dei fornitori o altri dispositivi esterni che non sono stati integrati nella gestione centralizzata dell'organizzazione. Tali dispositivi non sono considerati affidabili e il loro accesso alla rete e ai sistemi dell'organizzazione deve essere limitato, per evitare il rischio di compromissioni e movimenti laterali che potrebbero compromettere altri dispositivi connessi alla rete.

Gli accessi dei dispositivi sono strettamente correlati alle modalità di accesso alla rete dell'organizzazione, un aspetto che sarà trattato più approfonditamente nella sezione dedicata alla gestione della rete e degli accessi. La questione di come permettere l'accesso a utenti con dispositivi non gestiti rappresenta una sfida complessa, ma può essere affrontata mediante l'uso di macchine virtuali o infrastrutture di desktop virtuale (VDI), ospitate su infrastrutture gestite dall'organizzazione. In questo modo, il dispositivo dell'utente diventa un mero visualizzatore di un ambiente remoto sicuro, controllato dall'amministrazione.

Un livello maturo di gestione dei dispositivi, supportato da policy di conformità attive, consente all'organizzazione di mantenere il controllo anche quando l'utente ha privilegi di amministratore sul proprio dispositivo, come la possibilità di installare o rimuovere applicazioni. In tali situazioni, quando il dispositivo si connette alla rete aziendale, viene classificato come dispositivo a basso livello di fiducia fino

a quando non viene ristabilita la conformità con i requisiti di sicurezza stabiliti dall'amministrazione. Questo controllo della conformità deve essere un processo continuo e aggiornato, adattandosi ai cambiamenti nei rischi e nella consapevolezza dell'organizzazione stessa.

Evoluzione e Tecnologie del Device Trust

La gestione dei dispositivi in un contesto Zero Trust si è evoluta significativamente con l'emergere di nuove minacce e modalità di lavoro. Il National Security Agency (NSA) ha pubblicato linee guida specifiche che enfatizzano l'importanza della "Advance Device Security Posture", definendo criteri stringenti per la valutazione continua dello stato di sicurezza dei dispositivi.

Un aspetto cruciale, non completamente affrontato nel modello tradizionale, è la gestione dei dispositivi IoT e OT (Operational Technology). Secondo un recente studio di Gartner, entro il 2025 oltre il 75% dei dati aziendali sarà generato e processato al di fuori del tradizionale data center aziendale.

L'architettura di gestione dei dispositivi necessita quindi di essere potenziata con capacità di:

- Continuous Diagnostics and Mitigation (CDM)
- Asset Discovery and Classification automatizzata
- Security Configuration Assessment in tempo reale
- Vulnerability Assessment continuo
- Patch Management automatizzato

La MITRE Corporation ha sviluppato un framework specifico per la valutazione della postura di sicurezza dei dispositivi, che include:

- Hardware Root of Trust

- Secure Boot
- Runtime Integrity Monitoring
- Secure Storage
- Secure Communication

Tecnologie Avanzate per il Device Trust Management

Molte delle tecnologie che rientrano nell'approccio Zero Trust possono facilitare il processo di gestione e conformità dei dispositivi. Tra queste, i sistemi di gestione degli endpoint e gli EMM (Enterprise Mobility Management) per dispositivi mobili, insieme ai relativi client da installare, rappresentano un punto centrale per l'enforcement delle policy di conformità e per il monitoraggio continuo dello stato del dispositivo.

Questi strumenti consentono aggiornamenti costanti e controllati, l'aggiornamento dei sistemi antivirus, anti-malware e EDR/XDR, nonché l'assistenza remota e la gestione centralizzata del dispositivo. L'integrazione degli strumenti antivirus con EDR/XDR in un contesto di gestione centralizzata consente non solo di proteggere il dispositivo, ma anche di analizzare le interazioni tra il dispositivo e l'ambiente esterno o altri dispositivi interni alla rete, identificando tempestivamente movimenti laterali e potenziali gruppi di dispositivi a rischio.

Inoltre, l'integrazione dei log, in particolare quelli di EDR/XDR, con tecnologie SIEM permette di alzare ulteriormente il livello di sicurezza e di migliorare la risposta agli incidenti. Anche l'adozione di infrastrutture di virtualizzazione del desktop, pur non essendo una misura strettamente legata alla sicurezza informatica, può contribuire a risolvere problematiche organizzative, fornendo soluzioni di accesso sicuro per specifiche categorie di utenti. Le tecnologie per il Trust dei Dispositivi si sono

evolute significativamente negli ultimi anni, introducendo capacità avanzate di gestione e protezione. Un'architettura attuale di Device Trust richiede l'integrazione di molteplici tecnologie che operano in sinergia per garantire un controllo completo e granulare dei dispositivi aziendali.

Le piattaforme UEM rappresentano l'evoluzione dei tradizionali sistemi MDM/MAM ed EMM, offrendo una gestione unificata di tutti i tipi di endpoint, dai laptop ai dispositivi mobili, fino ai dispositivi IoT. Queste piattaforme integrano diverse funzionalità avanzate che spaziano dalla gestione del ciclo di vita alla detection di incidenti fino ad un controllo dell'integrità dell'hardware.

La gestione del ciclo di vita completo del dispositivo, dalla registrazione iniziale alla dismissione, viene automatizzata attraverso policy granulari. Il sistema può orchestrare automaticamente l'installazione di applicazioni e configurazioni di sicurezza, mantenendo un inventario accurato e aggiornato di tutti i dispositivi gestiti. La capacità di applicare policy contestuali permette di adattare le configurazioni di sicurezza in base alla posizione del dispositivo, al livello di rischio rilevato e al profilo dell'utente.

I sistemi Endpoint Detection and Response (EDR) hanno evoluto le loro capacità ben oltre il semplice rilevamento di malware. Utilizzando tecniche di machine learning e analisi comportamentale, questi sistemi possono infatti coadiuvare nelle operazioni legate a:

- Identificare attacchi fileless e zero-day
- Analizzare il comportamento delle applicazioni in tempo reale
- Correlare eventi su multiple dimensioni temporali
- Automatizzare la risposta agli incidenti
- Fornire threat hunting proattivo

Extended Detection and Response (XDR) L’XDR rappresenta l’evoluzione naturale dell’EDR, estendendo la visibilità e il controllo oltre il singolo endpoint. Questa tecnologia permette di:

- Correlare eventi tra endpoint, rete e cloud
- Identificare minacce complesse che si manifestano su multiple superfici
- Automatizzare la risposta attraverso l’integrazione con altri sistemi di sicurezza
- Fornire analisi predittive basate su machine learning

L’implementazione di un hardware root of trust rappresenta un elemento fondamentale per garantire l’integrità dei dispositivi. Tecnologie come TPM 2.0 e secure enclaves permettono di:

- Verificare l’integrità del boot process
- Proteggere le chiavi crittografiche, incluse quelle di cifratura dei device
- Implementare attestazione remota
- Garantire l’isolamento delle applicazioni sensibili

Le soluzioni Mobile Threat Defense (MTD) proteggono i dispositivi mobili da minacce sofisticate attraverso:

- Analisi delle app in tempo reale
- Rilevamento di reti malevole
- Protezione da phishing su tutti i canali di comunicazione Identificazione di configurazioni pericolose
- Rilevamento di jailbreak e root

L’integrazione di Cloud Access Security Broker (CASB) con il device trust permette di:

- Controllare l’accesso alle applicazioni cloud in base allo stato del dispositivo
- Applicare policy di Data Loss Prevention (DLP)

contestuali Monitorare il comportamento delle app cloud
- Proteggere i dati aziendali su dispositivi non gestiti

I sistemi Network Access Control (NAC) integrano capacità avanzate di:

- Posture assessment continuo
- Micro-segmentazione dinamica
- Quarantena automatica dei dispositivi compromessi Integrazione con sistemi di threat intelligence

La gestione automatizzata dei certificati dei dispositivi permette di:

- Implementare autenticazione forte basata su certificati Automatizzare il lifecycle dei certificati
- Integrare con sistemi di PKI enterprise
- Supportare protocolli moderni come EST (Enrollment over Secure Transport)

L'integrazione con piattaforme Secure Access Service Edge (SASE) permette alle organizzazioni fortemente ibridate verso il cloud di:

- Applicare policy di sicurezza consistenti indipendentemente dalla location
- Proteggere l'accesso alle risorse cloud e on-premise Implementare Zero Trust Network Access (ZTNA)
- Fornire protezione web e email contestuale

Le piattaforme moderne di asset intelligence forniscono:

- Discovery continuo dei dispositivi
- Valutazione automatica della compliance
- Analisi delle vulnerabilità in tempo reale
- Reporting automatizzato per audit e compliance

Le soluzioni di application control e Software Management permettono di:

- Implementare whitelisting dinamico delle applicazioni
- Gestire il patching automatizzato
- Controllare l’uso di software non autorizzato
- Monitorare le licenze software

L’integrazione tra questi sistemi permette di implementare un controllo granulare e contestuale dei dispositivi, bilanciando sicurezza e usabilità. La chiave del successo sta nella capacità di automatizzare la maggior parte delle operazioni di gestione e sicurezza, riducendo il carico operativo sul team IT e garantendo una risposta rapida agli incidenti di sicurezza.

Gestione dei Rischi e Mitigazione delle Minacce

Una gestione completa dei dispositivi, supportata da policy di conformità rigorose, riduce significativamente il rischio che un dispositivo compromesso possa accedere in modo incontrollato alla rete e ai sistemi critici dell’organizzazione. Inoltre, consente di bloccare i dispositivi sospetti non appena vengono rilevate anomalie operative.

Vengono anche ridotti i rischi associati al mancato aggiornamento del sistema operativo o dei componenti di sicurezza, poiché la gestione centralizzata garantisce che tutti i dispositivi siano costantemente aggiornati e conformi alle policy di sicurezza stabilite dall’organizzazione.

L’evoluzione del panorama delle minacce ha reso necessario un approccio più sofisticato alla protezione dei dispositivi endpoint.

Rischi legati ai Dispositivi Compromessi

La compromissione dei dispositivi rappresenta una delle

minacce più significative per le organizzazioni al giorno d'oggi. Un sistema maturo di Device Trust permette di mitigare questi rischi attraverso livelli diversificati di protezione. Gli attacchi cyber spesso utilizzano tecniche di living-off-the-land (LotL), sfruttando strumenti legittimi già presenti sul sistema per evitare il rilevamento con lo scopo di eseguire azioni dannose rispetto a tali sistemi.

L'implementazione di controlli granulari sull'esecuzione dei processi e il monitoraggio comportamentale permettono di identificare l'uso anomalo anche di applicazioni legittime. Il rischio di compromissione della supply chain software, evidenziato da incidenti come SolarWinds e Kaseya, viene mitigato attraverso il controllo rigoroso delle fonti software e la verifica dell'integrità delle applicazioni. I sistemi moderni di application control possono verificare non solo le firme digitali ma anche l'integrità del codice e il comportamento delle applicazioni in esecuzione.

Rischi di Data Exfiltration

La perdita di dati attraverso i dispositivi endpoint rappresenta un rischio significativo per le organizzazioni. I sistemi di Device Trust implementano controlli multilivello per prevenire l'esfiltrazione dei dati andando anche oltre i tradizionali controlli DLP. Il sistema può identificare e bloccare tentativi di esfiltrazione attraverso canali nascosti, come la modulazione del traffico di rete o l'uso di protocolli legittimi per scopi malevoli.

Rischi di Credential Theft

Il furto delle credenziali direttamente dai dispositivi endpoint rappresenta una minaccia crescente. I sistemi di Device Trust implementano protezioni avanzate per le credenziali:

- Prevenzione del dumping della memoria

- Protezione delle credenziali cached
- Monitoraggio dell’accesso ai processi di gestione delle credenziali
- Identificazione di tentativi di pass-the-hash e pass-the-ticket

Rischi di Lateral Movement

I movimenti laterali all’interno della rete aziendale vengono significativamente limitati attraverso:

- Micro-segmentazione dinamica della rete
- Controllo granulare delle comunicazioni tra dispositivi
- Monitoraggio delle connessioni di rete anomale
- Identificazione di pattern di movimento sospetti

Rischi legati ai Dispositivi IoT

La proliferazione di dispositivi IoT introduce nuovi rischi che vengono mitigati attraverso:

- Isolamento dei dispositivi IoT in segmenti di rete dedicati
- Monitoraggio continuo del comportamento dei dispositivi
- Implementazione di policy di accesso restrittive
- Aggiornamenti automatici del firmware

Rischi di Configuration Drift

Il drift delle configurazioni di sicurezza viene prevenuto attraverso:

- Monitoraggio continuo delle configurazioni
- Ripristino automatico delle configurazioni corrette
- Alerting su modifiche non autorizzate
- Reporting delle deviazioni dalle baseline

Rischi legati al BYOD

I rischi specifici dei dispositivi personali vengono gestiti attraverso:

- Containerizzazione dei dati aziendali
- Controlli di accesso contestuali
- Monitoraggio selettivo delle attività business
- Capacità di wipe remoto selettivo

Rischi di Compliance

La non conformità normativa viene prevenuta attraverso:

- Monitoraggio automatico della compliance
- Enforcement delle policy di sicurezza
- Documentazione automatica delle configurazioni
- Reporting regolare sullo stato di conformità

Rischi legati al Remote Work

Il lavoro remoto introduce rischi specifici che vengono mitigati attraverso:

- Verifica continua dello stato di sicurezza dei dispositivi
- Controllo dell’accesso basato sulla postura di sicurezza
- Protezione delle comunicazioni remote
- Monitoraggio del comportamento in contesti remoti

Rischi Emergenti

Le tecnologie moderne di Device Trust permettono anche di affrontare rischi emergenti come:

- Attacchi basati su intelligenza artificiale
- Minacce firmware e hardware
- Attacchi alla supply chain
- Tecniche di evasione avanzate

L’efficacia di queste mitigazioni dipende non solo dall’implementazione tecnica ma anche dalla maturità dei processi di gestione e dalla consapevolezza degli utenti.

Un programma completo di Device Trust deve includere:

- Formazione continua degli utenti
- Aggiornamento regolare delle policy di sicurezza
- Monitoraggio continuo dell’efficacia dei controlli
- Adattamento rapido a nuove minacce

Il sistema deve essere in grado di evolvere continuamente per affrontare nuove classi di minacce man mano che emergono, mantenendo al contempo un equilibrio tra sicurezza e usabilità per garantire l’accettazione da parte degli utenti e l’efficacia operativa.

In questo approfondimento abbiamo esaminato come il Device Trust rappresenti un elemento cruciale nell’architettura Zero Trust, fornendo una panoramica completa delle strategie di gestione, delle tecnologie disponibili e dei rischi mitigati. Nel prossimo articolo della serie esploreremo il tema legato al trust della Rete Interna al perimetro aziendale. Per approfondire ulteriormente questi concetti, vi invitiamo a scaricare il white paper del Dott. Ing. Fabrizio Fioravanti “Zero Trust: solo un problema tecnologico?”, che offre un’analisi completa sull’integrazione tra aspetti tecnologici e organizzativi nell’implementazione dello Zero Trust.

Profilo Autore

Fabrizio Fioravanti è attualmente responsabile dell’Unità di Processo Sistemi, tecnologie cloud e di sicurezza informatica presso l’Università degli Studi di Firenze.

Laureato in Ingegneria Elettronica, ha successivamente conseguito il dottorato di ricerca in Ingegneria Informatica e delle Telecomunicazioni e da oltre 25 anni lavora nel settore ICT.

Ha diverse pubblicazioni scientifiche al suo attivo sia su riviste italiane che internazionali, sia che in conferenze, oltre a monografie complete o contributi a monografie.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/device-trust/