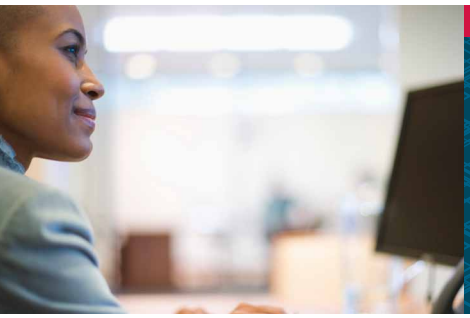

Il panorama in evoluzione della sicurezza desktop

Il panorama della sicurezza desktop si è evoluto a causa di vari fattori, fra i quali il malware mirato, le esigenze di comodità degli utenti e i costi di assistenza e di operatività del reparto informatico. Tradizionalmente, implementare soluzioni per la protezione dei desktop è come acquistare una polizza assicurativa contro i possibili rischi senza prendere in considerazione altri fattori. Nell'impostazione COE (Common Operating Environment) aziendale, la protezione dei desktop si è dimostrata una sfida per i gruppi IT, che si sono trovati a dover bilanciare la flessibilità a vantaggio dell'utente con le esigenze di sicurezza.

Ambienti desktop

Come indicato da vari studi, esistono due differenti gruppi di ambienti desktop:

- *Utenti normali* - Immagini di tipo COE ad accesso limitato, denominate anche a funzione fissa, oppure desktop con immagini comuni. In tali ambienti, l'utente finale non dispone dei privilegi per installare o disinstallare il software.
  Esempi di immagini COE: workstation in ambienti commerciali al dettaglio, finanziari e ospedalieri
- *Utenti avanzati* - Gli utenti sono abilitati all'installazione del proprio software
  Esempi: ambienti progettuali e di grafica

Per le finalità di questo documento, ci concentreremo sul modello di protezione del COE.

Attuali problematiche della sicurezza desktop

Negli ultimi 20 anni, dato che ci siamo spostati verso un'economia basata sulle conoscenze, le problematiche di sicurezza poste dal mantenere l'integrità dell'infrastruttura IT sono aumentate enormemente. Si è verificato un massiccio aumento dei campioni di malware rilevati dai ricercatori di sicurezza in tutto il mondo, da migliaia di campioni all'anno a migliaia al giorno. Sul piano operativo, la sicurezza degli endpoint (desktop/laptop) è diventata più complessa e i responsabili della sicurezza informatica segnalano spesso un misto di problemi, sia dovuti alle minacce ma anche operativi.

Il boom del malware

L'eccezionale aumento del malware in circolazione è in cima alle preoccupazioni dei responsabili della sicurezza. C'è un chiaro aumento della complessità e della quantità di malware fornedo diversi vettori di attacco all'infrastruttura informatica.

Prestazioni

Un secondo problema è rappresentato dalle prestazioni delle soluzioni tradizionali a causa del significativo aumento della quantità di signature del malware.

Sicurezza operativa

In terzo luogo è da tenere in considerazione l'aspetto operativo della sicurezza. Quando il malware attraversa un ambiente informatico, debilita l'infrastruttura di sicurezza. In aggiunta, le tradizionali soluzioni di sicurezza basate sulle firme possono non essere in grado di mitigare l'esposizione agli attacchi zero-day e alle minacce persistenti avanzate (Advanced Persistent Threats, APT)

La proliferazione delle applicazioni non autorizzate

Infine, particolarmente preoccupante è il contenimento delle applicazioni non autorizzate che proliferano sui desktop degli utenti finali. Nei mercati emergenti ciò include anche la prevenzione della diffusione di software piratato e senza licenza all'interno degli ambienti aziendali.

Problematiche comportamentali nella gestione della sicurezza

Dal punto di vista dei comportamenti, negli ambienti COE c'è un costante braccio di ferro fra l'esigenza degli amministratori di applicare la sicurezza e il bisogno degli utenti di un ambiente flessibile e protetto. Entrambi questi obiettivi devono essere raggiunti senza compromettere la sicurezza o la produttività interne all'azienda. Una soluzione deve soddisfare le esigenze sia dell'amministratore che dell'utente, senza compromettere il principio fondamentale di una produttività prolungata.

Esiste una soluzione?

Le funzioni di whitelisting di McAfee® Application Control, unite alla tradizionale tecnologia antivirus, offrono una soluzione praticabile per molti di questi problemi. McAfee Application Control costituisce un passo in avanti rispetto alla tradizionale protezione desktop, perché offre resistenza al malware e migliori capacità di gestione delle epidemie.

Whitelisting delle applicazioni

L'approccio basato sul whitelisting si basa sostanzialmente sull'identificazione di file "notoriamente buoni" per l'ambiente informatico e solo a questi file viene consentito l'accesso al sistema. Le sue implementazioni hanno molte varianti: sia come installazioni autonome che come soluzioni di whitelisting coesistenti con le tradizionali soluzioni di blacklisting, come gli antivirus. Qui ci stiamo concentrando su un ambiente IT con un antivirus che può essere migliorato incorporando la tecnologia di whitelisting.

Modalità osservazione

McAfee Application Control offre una funzione operativa denominata "modalità osservazione". In pratica si tratta delle versioni senza applicazione, a solo monitoraggio, di McAfee Application Control. Una volta che McAfee Application Control è stato installato e ha completato una scansione dell'inventario, può essere attivata la modalità osservazione. Durante l'iniziale installazione in un'azienda, questa modalità può aiutare a costruire delle policy che agevolino la scoperta di eventuali non conformità agli standard di sicurezza, identificando le eccezioni operative valide.

Quando implementata con un tradizionale strumento antivirus, la modalità osservazione permette a quest'ultimo di rimanere lo strumento di protezione primario. Ciò aiuta un amministratore della sicurezza a mantenere il monitoraggio delle risorse informatiche e permette all'antivirus di proteggere gli endpoint degli utenti. Complessivamente, questo si traduce in produttività dell'utente dei computer desktop, con una migliore visibilità della protezione da parte degli amministratori IT.

Funzioni di reputazione dei file abilitate da McAfee Global Threat Intelligence™ (McAfee GTI™)

McAfee Application Control include inoltre le funzioni di reputazione dei file abilitate da McAfee GTI; può recuperare l'intero inventario file degli endpoint contenuto nel software McAfee® ePolicy Orchestrator® (McAfee ePO™). Questo inventario viene poi confrontato con i punteggi di reputazione dei file provenienti dal server McAfee GTI. Viene così messa a disposizione una funzione offline e scaricata, per controllare che i file presenti nell'azienda non siano dei malware o comunque problematici. Se un file viene identificato come malware, l'interfaccia McAfee ePO offre un singolo pannello per individuare rapidamente la posizione di tutte le istanze di tale malware nell'ambiente informatico.

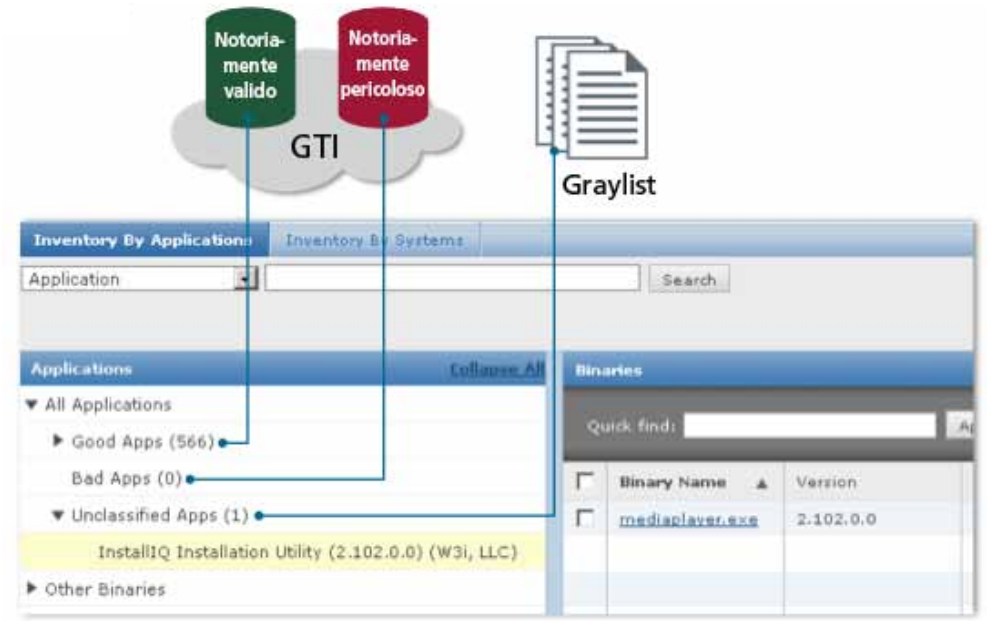

Figura 1. La reputazione dei file di McAfee GTI categorizza ogni applicazione in azienda.

Resistenza alle epidemie di malware

La capacità di McAfee Application Control di operare in modalità osservazione, con l'antivirus come software di sicurezza primario, fornisce un vantaggio senza precedenti per resistere alle epidemie di malware e permette inoltre all'amministratore di passare dalla modalità osservazione alla modalità applicazione e viceversa, a seconda delle circostanze. Quando si sospetta un'epidemia di malware, il passaggio di McAfee Application Control alla modalità applicazione blocca efficacemente lo stato del sistema nell'infrastruttura informatica, impedendo al malware di penetrare in profondità nell'azienda. Questo, unito alla capacità di McAfee ePO di gestire il rilevamento del malware in base all'inventario, consente attività di remediation semplificate e tempestive dei computer infetti.

Interattività dell'utente grazie al whitelisting dinamico

Infine, se McAfee Application Control viene installato in modalità applicazione, dunque si trova a un più alto livello di protezione, per eseguire modifiche al suo computer l'utente finale deve inviare una richiesta al reparto IT. Essenzialmente questa è la parte dinamica del whitelisting, mediata tramite una ben definita interazione tra utente e amministratore. Con questa funzionalità, McAfee Application Control è in grado di offrire maggior sicurezza mentre gestisce l'esperienza dell'utente allo stesso livello di uno strumento antivirus tradizionale.

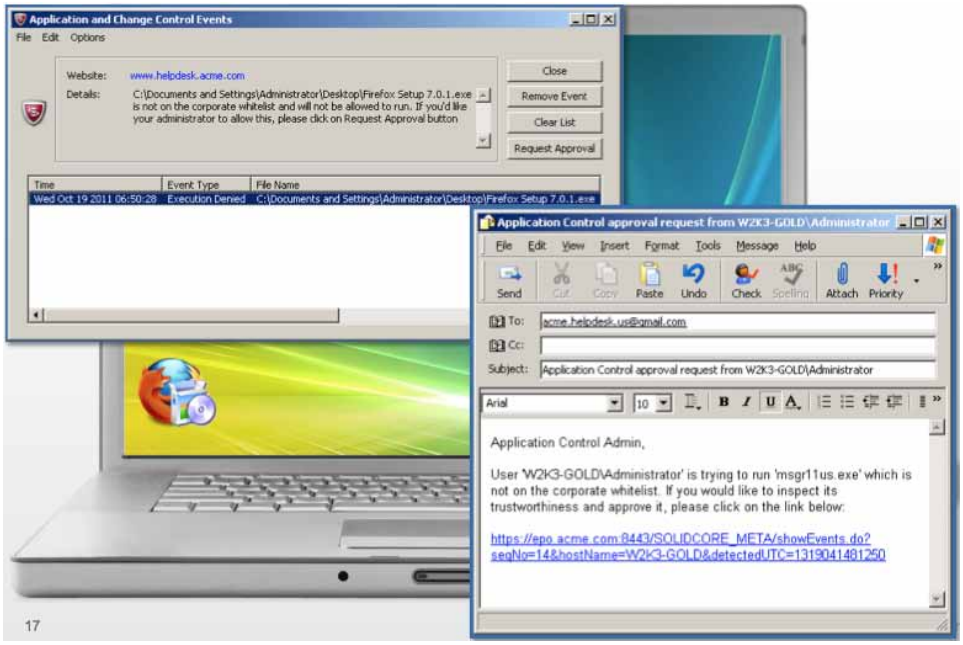

Figura 2. Notifiche sul desktop e richieste di approvazione per le applicazioni non incluse nelle whitelist.

Gestione delle applicazioni non autorizzate

Nei mercati emergenti, il contesto della sicurezza viene anche definito con la possibilità di rintracciare nell'ambiente informatico il software non autorizzato e non protetto. Non appena l'inventario è disponibile anche a livello del software McAfee ePO, è possibile esportarlo e fonderlo con l'elenco software protetto e approvato dall'azienda. Le differenze tra quest'ultimo elenco e l'inventario esportato da McAfee ePO sono utilizzabili per identificare la violazione delle policy di sicurezza generali o dei requisiti di licenza, a seconda dei casi.

Conclusioni

Il whitelisting delle applicazioni si sta evolvendo in un concreto livello di difesa primario per una certa classe di sistemi desktop. Se usato congiuntamente alle soluzioni antivirus esistenti, non solo fornisce una difesa robusta contro le minacce emergenti, quali le APT e il malware mirato, ma contribuisce anche a ridurre i costi operativi mettendo sotto controllo la diffusione delle applicazioni non autorizzate. Con gli ampi vantaggi del whitelisting delle applicazioni e dei recenti avanzamenti tecnologici che ne facilitano l'implementazione, gli amministratori possono aspettarsi un modello di protezione desktop più semplice.

A proposito di McAfee

McAfee, società interamente controllata da Intel Corporation (NASDAQ:INTC), è la principale azienda focalizzata sulle tecnologie di sicurezza. L'azienda offre prodotti e servizi di sicurezza riconosciuti e proattivi che proteggono sistemi e reti in tutto il mondo, consentendo agli utenti di collegarsi a Internet, navigare ed effettuare acquisti sul web in modo sicuro. Supportata dal suo ineguagliato servizio di Global Threat Intelligence, McAfee crea prodotti innovativi destinati a utenti consumer, aziende, pubblica amministrazione e service provider che necessitano di conformarsi alle normative, proteggere i dati, prevenire le interruzioni dell'attività, individuare le vulnerabilità e monitorare e migliorare costantemente la propria sicurezza. McAfee è impegnata senza sosta a ricercare nuovi modi per mantenere protetti i propri clienti.
www.mcafee.com/it

McAfee
An Intel Company

McAfee Srl
via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.mcafee.com/it

41101brf_desktop-security_0112_fnl_ETMG