IBM Software
Thought Leadership White Paper

Ottobre 2014

Rispondere in modo rapido ed efficace alle minacce odierne

IBM BigFix per ridurre i rischi

Indice

Introduzione

Il moderno mondo digitale non è a prova di errore. Si possono sempre presentare incidenti, involontari o volutamente causati. Per ridurre i danni e l'impatto sulle organizzazioni, un'impresa agile deve saper rispondere rapidamente. Inoltre al fine di limitare i rischi prima che il danno si presenti, un'organizzazione deve essere in grado di garantire un ottimo livello per la sicurezza, controllando che gli endpoint rispettino gli standard di conformità, automatizzando gli interventi per abbreviare i tempi di risposta e applicando le misure necessarie a controllare le infezioni con soluzioni di quarantena fino all'eliminazione del problema.

Per raggiungere questo grado di agilità sono necessari un controllo complessivo degli endpoint e un'affidabile visualizzazione in tempo reale, non solo per identificare scostamenti dalle regole di conformità, ma anche per riportare rapidamente l'ambiente a un livello stabile. Un sistema di risposta efficiente deve quindi gestire al meglio i dispositivi in remoto - sia in rete che non - con sistemi operativi eterogenei. Deve essere scalabile, per rispondere alle crescenti richieste di rete. Deve saper combinare velocità, rilevamento preciso e tecniche di correzione di altissima qualità, dato che gli attacchi e le minacce risultano sempre più rapidi, sofisticati e difficili da prevenire.

La soluzione IBM® BigFix, aiuta le imprese a rispondere alle esigenze di conformità per prevenire le minacce, e include capabilities per rispondere rapidamente a incidenti di sicurezza, mitigandone l'impatto. BigFix, potenziato da un'architettura di agent intelligenti, fornisce una visibilità in tempo reale e un controllo per garantire alle operazioni informatiche una protezione "0 day" in vari ambienti e indipendentemente dal roaming dei portatili. Comprende capabilities basate su analytics che rafforzano l'infrastruttura nei confronti di attacchi alla rete, server ed endpoint.

Risposta alle minacce con interventi rapidi ed efficaci

Il mondo è oggi interconnesso, tecnologico e intelligente, con imprese che operano a livello internazionale, più complesse e più mobili che nel passato, e quindi l'importanza della sicurezza e dell'adeguamento della protezione per gli endpoint sono continuamente in crescita. Le minacce sono sempre più sofisticate, dinamiche, pericolose e difficili da individuare, pertanto la necessità di trovare un sistema di risposta ad alte prestazioni diventa irrinunciabile.

In passato, lo scarto temporale tra la scoperta di una vulnerabilità e l'abilitazione di un codice exploit si misurava in mesi. Successivamente si è ridotto a settimane e quindi giorni. Oggigiorno si parla di poche ore per l'identificazione di vulnerabilità precedentemente non note o per exploit nuovi su vulnerabilità note (meglio noti come attacchi "zero day"). In molti casi i criminali cibernetici non devono nemmeno scoprire direttamente le vulnerabilità di sistemi e applicazioni. Attendono semplicemente che le informazioni sulla vulnerabilità risultino pubbliche grazie ai ricercatori e fornitori software. Tale informazione viene quindi sfruttata per creare il codice di exploit che attacca il punto vulnerabile più rapidamente di quanto sia possibile rispondere da parte dell'impresa.

Attacchi all'infrastruttura tecnologica dell'impresa - soprattutto in seguito ad un attacco zero day, rapido e inatteso - possono comportare gravi perdite a livello di fatturato, produttività, relazioni con la clientela e reputazione. La risposta adeguata a questi rischi richiede di mantenere un livello elevato e costante della sicurezza, per prevenire, se possibile gli attacchi, e di implementare un sistema di risposta ad alte prestazioni in grado di far fronte agli attacchi sempre più veloci e sofisticati.

BigFix è in grado di fornire conformità continua e risposte rapide. L'agent intelligente di BigFix assicura continuamente la conformità con le prescrizioni vigenti, automatizza gli interventi di risposta e segnala immediatamente eventuali cambiamenti di stato alla console centrale. Questo tipo di approccio garantisce alle imprese visibilità e controllo istantanei degli endpoint, identificando rapidamente rischi e punti deboli della sicurezza, per applicare quindi le correzioni adeguate. Le sue capabilities di analytics forniscono reporting e monitoraggio per soddisfare gli standard della compliance e gli obiettivi informatici di sicurezza.

BigFix supporta le organizzazioni per rispondere rapidamente alle minacce odierne con:

- **Velocità:** BigFix effettua in pochi minuti modifiche che interessano l'intera organizzazione, ad esempio con patch per riparare una nuova vulnerabilità identificata su centinaia o migliaia di endpoint o modificando la configurazione di un sistema per renderlo conforme agli standard. Con BigFix la valutazione e l'analisi sono effettuate sull'endpoint stesso - aumentando la velocità di rilevamento, la fornitura del software e la convalida. La comunicazione tra server di gestione ed endpoint viene ridotta, per aumentare la velocità e diminuire i consumi di banda della rete.
- **Accuratezza:** BigFix è in grado di eseguire query accurate di ogni variabile di un endpoint per esaminare in tempo reale i problemi dell'ambiente. Permette alle imprese di identificare rapidamente i problemi, mettendo a disposizione un'ulteriore difesa nel caso in cui le tradizionali soluzioni standard falliscano completamente o rispondano troppo lentamente per prevenire il danno. La console centrale di gestione fornisce una vista singola e granulare, assicurando visibilità globale e il controllo di tutte le reti distribuite. Gli operatori sono in grado di applicare le contromisure di correzione in pochi minuti, ricevendo immediatamente la conferma del buon esito dell'intervento.
- **Controlli di qualità:** virus, worm e botnet modificano la configurazione del computer e questo genere di exploit "furtivi" spesso non è identificato da strumenti comuni di sicurezza come i programmi anti virus e anti spyware. Grazie alla visibilità granulare sulle proprietà caratteristiche degli endpoint, BigFix permette all'impresa di individuare tali modifiche e di automatizzare le contromisure per garantire la conformità. Analogamente BigFix è in grado di scoprire le applicazioni installate nella propria infrastruttura. Se un codice malevolo tenta di installare applicazioni non autorizzate, BigFix identifica l'attacco in tempo reale e interviene automaticamente.
- **Protezione cloud based:** BigFix è in grado di fornire soluzioni di sicurezza per endpoint fissi, in rete, in roaming e per endpoint connessi a Internet più rapidamente dei signature file distribuiti dai vendor. I riferimenti incrociati di BigFix sulle informazioni relative alle minacce con il database basato sul cloud consentono di controllare file e indirizzi web in tempo reale, per individuare codici potenzialmente dannosi e fornire la protezione anti malware necessaria per gli endpoint. Ad esempio un computer portatile utilizzato in un aeroporto è in grado di ricevere dovunque e in qualsiasi momento una protezione basata sul cloud contro le minacce potenzialmente presenti nei siti visitati o nei file ricevuti.

- **Quarantena automatica in rete:** BigFix è in grado di valutare automaticamente gli endpoint in base alle configurazioni di conformità richieste - e se un endpoint non risulta conforme, la soluzione IT lo configura in modo che risulti in quarantena in rete fino ad ottenere la conformità. BigFix mantiene l'accesso gestionale all'endpoint, mentre tutti gli altri accessi risultano disabilitati.

Come tenere rapidamente sotto controllo gli attacchi dei virus

Un anno dopo aver subito un grave attacco informatico con un worm su Internet - con interventi di quattro ore per sistema per rimediare al danno e costi complessivi di 1,6 milioni di dollari statunitensi - una grande università ha deciso di implementare BigFix quale soluzione di difesa contro i successivi attacchi.

In tal modo i worm successivi hanno infettato solo circa il due percento degli oltre 12.000 computer dell'università dotati di BigFix. Inoltre i sistemi infetti sono stati riparati rapidamente e automaticamente, con disagi minimi per gli utenti. Oltre il 15 percento degli 8.000 computer che non avevano installato BigFix sono invece risultati infettati, richiedendo notevoli interventi per le riparazioni.

Proteggere un'impresa moderna, complessa e distribuita

Nel momento in cui le aziende diventano globali, le loro infrastrutture di rete spesso non riescono a far fronte alle nuove necessità di business. Utilizzano infatti larghezze di banda ridotte e reti a latenza elevata. Visibilità insufficiente e ritardi notevoli comportano una diffusione insoddisfacente dei dati e maggiori rischi. L'IT non conosce lo stato dei dispositivi, né se hanno subito un attacco exploit o, se su un endpoint è implementata una soluzione fix. I criminali cibernetici hanno imparato a sfruttare il rapporto di dipendenza delle aziende dal traffico e-mail e sul web - semplici azioni come aprire l'allegato di una e-mail o cliccare un link possono comportare la perdita di dati riservati, danni all'infrastruttura o alla reputazione aziendale.

Molte imprese dispongono poi di vari sistemi informatici legacy e devono gestire le risorse su diverse piattaforme. Spesso un'infrastruttura eterogenea viene considerata una buona strategia difensiva di sicurezza, ma in realtà complica la possibilità di gestire e proteggere efficacemente gli endpoint. All'espansione di un'impresa aumenta proporzionalmente anche la sfida per gestire e proteggere un numero di endpoint in crescita.

BigFix è progettato per fornire alle imprese le soluzioni necessarie per gestire e proteggere ambienti complessi ed eterogenei:

- **Gestione ottimizzata di dispositivi in remoto e mobili:** l'architettura con agent intelligente e distribuito di BigFix consente di identificare e valutare di continuo i portatili in roaming, indipendentemente dalla loro ubicazione. Qualsiasi sistema dotato dell'agent può funzionare come un relay - un punto di comunicazione per policy e remediation - e ogni relay può valutare e garantire la conformità di configurazione degli endpoint connessi a Internet. Ogni agent dispone di una copia locale della policy e quindi il relay non appena connesso ad Internet, può inviare qualsiasi modifica delle policy direttamente all'endpoint.

- **Conformità continua:** BigFix è dotato di checklist di "best-practice", utilizzabili "out of the box" per valutare la conformità. L'agent intelligente controlla continuamente l'applicazione della policy e protegge l'endpoint, indipendentemente dal fatto che sia collegato o meno alla rete aziendale. Non appena si modifica la configurazione di un endpoint, l'agent rileva se opera in modo conforme o meno e quindi esegue automaticamente gli interventi necessari a ripristinare la conformità dell'endpoint. Quindi segnala al server di gestione le attività. Ne risulta una protezione costante dagli exploit, indipendente dal roaming dell'endpoint.
- **Supporta una piattaforma multipla:** il supporto a piattaforma multipla di BigFix semplifica la gestione di ambienti diversi - compresi quelli con sistemi e applicazioni legacy. La soluzione BigFix supporta ambienti con diverse generazioni di Microsoft Windows e i sistemi operativi UNIX, Linux e Mac - anche in ambienti virtualizzati.
- **Vulnerabilità ridotte prima di un attacco exploit:** BigFix è in grado di raggiungere ogni chiave di registro, file, servizio o componente dell'endpoint. Pertanto può gestire ogni applicazione o servizio dell'endpoint. Se il personale IT intende analizzare una chiave di registro, utilizza BigFix per la query dell'ambiente, ottenendo in pochi minuti una risposta dettagliata. In caso di endpoint offline, la risposta verrà inviata non appena il dispositivo sarà connesso ad Internet.
- **Integrazione Security Information ed Event Management:** le informazioni BigFix relative alle vulnerabilità aggiornano il database IBM Security QRadar®, per una migliore correlazione tra rischio e attacco e migliori report di conformità. Le soluzioni QRadar in sinergia con BigFix monitorano, controllano la conformità, applicano i rimedi necessari e forniscono di continuo i report relativi, fornendo correlazioni tra vulnerabilità ed eventi di sicurezza degli endpoint e della rete, identificando e facendo remediation sui dispositivi a rischio.
- **Supporto DLP (data loss prevention):** BigFix permette di migliorare la protezione dei dati, tenendo sotto controllo i costi operativi. Policy DLP possono essere create ed applicate per prevenire o limitare la trasmissione di asset digitali tra canali , come le e-mail, proteggendo i dati sui dispositivi anche al di fuori dell'azienda. BigFix regola l'accesso a device storage esterni a risorse di rete, e, in sinergia con la scansione dei file, favorisce la protezione dai rischi legati alla sicurezza. Si possono utilizzare templates predefiniti per identificare, monitorare ed eventualmente bloccare la trasmissione di dati sensibili, come ad es. i codici delle carte di credito.
- **Protezione in tempi rapidi:** BigFix può gestire da un solo server di gestione fino a 250.000 endpoint in infrastrutture distribuite e molto complesse. L'impresa inoltre non deve gestire un'importante infrastruttura server per gli endpoint, in quanto gli endpoint sono in grado di eseguire autonomamente valutazione e applicazione dei criteri di policy. BigFix può essere implementato rapidamente, di solito in poche ore, indipendentemente dalle dimensioni o dalla complessità della rete.

Concord Hospital cambia il fornitore di sw antivirus

Durante le migrazioni di antivirus da un vendor ad un altro, spesso si verifica che l'impresa rimanga esposta agli attacchi durante il periodo di transizione. Sfruttando le capabilities di automazione di BigFix, il Concord Hospital ha potuto eseguire la migrazione senza interruzioni o esposizioni rischiose ottenendo una migliore performance.

Gli interventi di disinstallazione e installazione richiedono in media tra i cinque e i dieci minuti per macchina, o tra 30 e 60 minuti in caso di scansioni complete. L'implementazione non è quasi stata notata - nessun utente si è infatti rivolto all'helpdesk durante la fase di rollout. Dopo tale fase, il voto assegnato alle caratteristiche di utilizzo delle postazioni di lavoro è passato da uno a sette, su una scala di dieci. Gli aggiornamenti di definizione e le scansioni di controllo manuali, che precedentemente avevano letteralmente paralizzato numerose postazioni di lavoro, si lasciano ora implementare con una tale rapidità da passare inosservati.

Assicurare una risposta rapida in caso di incidente

Gli incidenti si presentano anche negli ambienti gestiti con la massima sicurezza. Oltre a offrire soluzioni per supportare l'impresa nel mantenere continuamente un ottimo livello di sicurezza e nel prepararsi con efficienza ad affrontare un possibile incidente, BigFix mette a disposizione funzioni specifiche di remediation per mitigare i danni e riportare il più rapidamente possibile gli endpoint alle condizioni di stabilità dopo un incidente.

La visibilità in ordine cronologico dello stato di conformità può risultare uno strumento particolarmente efficace per individuare uno stato che nel passato ha portato al problema. Ad esempio un'impresa che ha subito un attacco può esaminare il proprio stato di conformità al momento dell'attacco per individuare le vulnerabilità esistenti. La possibilità di approfondire la ricerca fin nei minimi dettagli degli endpoint, conformi oppure no, garantisce di identificare le lacune critiche e fornire spunti per rendere conformi gli endpoint, rafforzando la postura complessiva di sicurezza dell'impresa.

Gli esempi di seguito riportati dimostrano come BigFix possa essere utilizzato in diversi contesti

- **Disabilitare i controlli ActiveX o le librerie DLL attaccate:** BigFix può rapidamente utilizzare varie policy per disabilitare un elemento di controllo o una libreria DLL (dynamic-link library) attaccato non appena si identifica una vulnerabilità - limitando i danni di un attacco ancor prima che sia disponibile una fix del fornitore. Quando si individua un exploit "zero day", la soluzione può attivare le policy per eseguire politiche che trasformano i passi manuali di remediation forniti dal fornitore in policy automatizzate per identificare se gli endpoint sono potenzialmente vulnerabili e quindi mitigare i problemi.
- **Migrazione da una soluzione tecnica di controllo a un'altra:** la sostituzione di una soluzione anti virus per motivi legati a costi eccessivi o inefficienza spesso risulta una sfida e durante la migrazione gli endpoint possono risultare esposti ad attacchi. BigFix permette all'impresa di disinstallare in modo semplice e in sicurezza una soluzione anti virus in un solo giorno. Facilita quindi anche l'installazione dei prodotti da un nuovo fornitore. In entrambe le operazioni, la velocità della soluzione IT garantisce di ridurre al minimo la finestra di vulnerabilità all'attacco.

- **Aggiornamento rapido dei controlli di protezione degli endpoint:** BigFix può garantire che i client di sicurezza dell'endpoint siano sempre in funzione e che le definizioni dei virus siano aggiornate. Il processo di verifica a circuito chiuso assicura che aggiornamenti e altre modifiche siano completati, compresa la verifica per gli endpoint non collegati alla rete. Un'impresa può pertanto usare BigFix per disattivare servizi - ad es. chiudendo le porte telnet aperte - che espongono il sistema alle vulnerabilità.
- **Migrazione a un nuovo browser:** un exploit del browser può esporre l'impresa al pericolo di permettere agli aggressori in remoto di lanciare un codice arbitrario quando gli utenti accedono a determinati siti. Con BigFix, le imprese sfruttano la flessibilità di migrazione a un altro browser - e anche infrastrutture complesse e di grandi dimensioni sono in grado di completare la migrazione in pochi giorni.
- **Identificazione e inattivazione di malware che non può essere rimosso:** per combattere un attacco malware, BigFix può applicare regole di firewall IPSec per mettere in quarantena i sistemi infettati separandoli dal resto della rete. Permettendo la comunicazione in uscita solo con un server di correzione, il team IT crea definizioni di policy che identificano l'impatto del virus. Il team IT quindi può controllare gli altri endpoint per rilevare se mostrano lo stesso comportamento, mettendo in quarantena gli endpoint interessati. Quando la fix è disponibile, BigFix garantisce che gli endpoint non sono più infetti e che risultano aggiornati.

Componenti principali della soluzione

Le soluzioni di risposta agli incidenti ad alte prestazioni del portafoglio BigFix sono:

- IBM BigFix Compliance: rafforza in modo continuo la configurazione di sicurezza IT e fornisce la remediation , unitamente a capabilities di analytics per identificare e archiviare in modo automatico i risultati dei controlli di sicurezza. Fornisce varie indicazioni relative allo stato di conformità e ai punti deboli della sicurezza, da viste aggregate, all'identificazione degli hot spot fino a ricerche drill-down per informazioni dettagliate.
- IBM BigFix Protection: identifica ed elimina i malware prima che possano sfruttare le vulnerabilità. Sfrutta riferimenti incrociati sulle informazioni relative alle minacce con un database basato su cloud e continuamente aggiornato. Controlla i file e gli indirizzi web rispetto al suddetto database per individuare attività potenzialmente dannose in tempo reale e fornisce una protezione anti malware per endpoint Mac e Windows.

Conclusione

IBM BigFix aiuta le imprese a mantenere livelli costanti di conformità per prevenire le minacce, fornendo soluzioni basate su analytics in grado di rafforzare l'infrastruttura rispetto agli attacchi. La tecnologia con agent intelligente offre livelli multipli di sicurezza e aiuta a identificare in tempo reale operazioni anomale. Gli amministratori possono concentrarsi sui sistemi infetti con interventi su misura per un certo tipo di configurazione di endpoint o di tipologia di utente. BigFix offre una visibilità affidabile in tempo reale, correzioni automatizzate e scalabilità globale per il processo di risposta. Ciò permette alle imprese di proteggere gli endpoint senza tener conto di ubicazione, modalità di connessione o collegamento o meno in rete, minimizzando l'impatto degli exploit su rete, endpoint e utenti finali.

Per ulteriori informazioni

Per avere maggiori informazioni su IBM BigFix, contattare il rappresentante IBM o l'IBM Business Partner, o visitare il sito: **ibm.com**/security/bigfix

Dichiarazione di pratiche di sicurezza efficaci: la sicurezza del sistema IT implica la protezione di sistemi e informazioni tramite la prevenzione, il rilevamento e la risposta ad accessi inappropriati provenienti dall'interno o dall'esterno dell'azienda. Un accesso inappropriato può avere come risultato l'alterazione, la distruzione, l'uso non idoneo o non corretto di informazioni o può causare un danno o un utilizzo non corretto dei sistemi, incluso l'utilizzo per attacchi verso altri. Nessun prodotto o sistema IT dovrebbe essere considerato totalmente sicuro e nessun singolo prodotto o misura di sicurezza può essere completamente efficace nella prevenzione dall'accesso inappropriato. I sistemi e i prodotti IBM sono progettati per fare parte di un approccio alla sicurezza nel completo rispetto delle norme, che implicherà necessariamente ulteriori procedure operative e può richiedere l'installazione di altri sistemi, prodotti o servizi per realizzare la massima efficienza. IBM non garantisce che sistemi e prodotti siano immuni da o rendano un'azienda immune da condotte dannose o illecite da parte di terzi.

IBM Italia S.p.A.
Circonvallazione Idroscalo
20090 Segrate (MI)
Italia

WGW03131-ITIT-00