



SICUREZZA ICT E MERCATO "FINANCE"

**INNOVAZIONE TECNOLOGICA E
GOVERNANCE CONTRO I NUOVI RISCHI**

SOMMARIO

Verso una business transformation	2
Nuove vulnerabilità per il mondo finance	3
Attacchi mirati: il nuovo volto delle minacce	5
Una minaccia reale	7
La conformità alle Normative	7
La governance della sicurezza	10
Correlare i Big Data della sicurezza	10
La gestione e il controllo del rischio	11
L'importanza della governance	11
L'approccio alla sicurezza di Trend Micro	12
La Smart Protection Network	14
Uno strumento per l'analisi di reputazione e comportamento	15
L'importanza di correlare gli eventi di sicurezza	16
Le soluzioni per la Content Security	16
Trend Micro Deep Security per gli ambienti virtualizzati	17
Sicurezza che favorisce il ROI	18
Trend Micro Deep Discovery per rilevare gli attacchi mirati	19
Trend Micro SecureCloud	20
Trend Micro Mobile Security	20
Conclusioni	21

→

SICUREZZA ICT E MERCATO "FINANCE"

INNOVAZIONE TECNOLOGICA E GOVERNANCE CONTRO I NUOVI RISCHI

VERSO UNA BUSINESS TRANSFORMATION

Il momento attuale è caratterizzato da un processo di "business transformation" che sta ridefinendo i processi aziendali e sta cambiando le relazioni di lavoro. A guidare questo cambiamento contribuiscono in modo consistente le tecnologie ICT, che promuovono nuovi modelli orientati al servizio, delocalizzazione dei workflow, social collaboration e che sfruttano virtualizzazione, tecnologie mobili e cloud computing.

Questo processo di trasformazione interessa trasversalmente ogni tipologia di azienda perché ha un impatto diretto sul modo in cui le persone interagiscono tra loro e con il mondo esterno. Accanto alle opportunità si affacciano, tuttavia, nuovi rischi con cui le organizzazioni di ogni tipo devono confrontarsi. Il numero di vulnerabilità IT è, infatti, anche grazie ai nuovi sviluppi, in costante e rapido aumento tanto che le più recenti analisi prodotte dai laboratori di ricerca di Trend Micro (TrendLabs), tra i più avanzati del mondo, stimano in 12mila all'ora il numero delle nuove minacce.

Il settore finanziario si dimostra uno dei principali target di riferimento e quello in maggiore crescita per numero di attacchi subiti. L'escalation di minacce che le aziende che operano in questo settore si trovano ad affrontare non è però solo quantitativa, ma anche qualitativa. Come il resto delle tecnologie software, infatti, anche il malware è in costante miglioramento in termini di funzionalità, efficienza ed efficacia.

Siamo di fronte a una nuova generazione di attacchi che non è altro che il riflesso di un'evoluzione nelle logiche e metodiche del mondo degli hacker. Tutti gli operatori del settore informatico sono ormai definitivamente concordi sul fatto che l'era goliardica dell'hacker si sia definitivamente chiusa. Gli artefici delle nuove minacce informatiche sono professionisti del crimine che preferiscono decisamente il profitto alla notorietà e che operano in modo organizzato e strutturato, con logiche e modalità identiche a quelle del business legale, vendendo servizi illeciti a listino, coperti persino da garanzie contrattuali sul livello di servizio fornito.

Il settore finanziario è uno di quelli più esposti ai rischi legati alla sicurezza ICT.

La tipologia di dati che si trova ad amministrare è, infatti, tra quelle più appetibili per il cyber crime che rappresenta ormai la leva trainante delle minacce online in costante aumento per numero e sofisticazione.

Il tema va affrontato con una governance che tenga conto degli aspetti sia organizzativi sia tecnologici.

Su quest'ultimo versante diventa importante perseguire un modello personalizzato e automatizzato che riduca alla fonte le possibili vulnerabilità.

Trend Micro propone un approccio alla "content security" in linea con questi dettami e in grado di contribuire a soddisfare le nuove esigenze di protezione.

Tutte le informazioni hanno un valore sul mercato illegale ma, ovviamente, i dati bancari sono tra i più ricercati



Esempi del valore delle informazioni bancarie sul mercato illegale

Nuove vulnerabilità per il mondo finance

Questo scenario richiede di ripensare alla sicurezza e questo vale soprattutto per le organizzazioni finanziarie che sono caratterizzate da:

- possedere elevati volumi di dati a valore,
- consentire una facile monetizzazione di tali dati,
- disporre usualmente di una rete di uffici distribuiti a livello globale con una pluralità di possibili punti di ingresso da cui sferrare attacchi.

Per il settore finanziario la capacità di fruire delle informazioni rappresenta uno dei principali asset strategici per il raggiungimento degli obiettivi di business e determina, pertanto, stringenti esigenze di protezione.

Peraltro, non solo i dati ma anche le altre risorse aziendali rappresentano un target per il cyber crimine poiché, per esempio, i server compromessi possono essere utilizzati come base per inviare altro malware o per lanciare attacchi del tipo Distributed Denial of Service.

Questo tipo di attacchi negli ultimi anni si sono moltiplicati, allargando gli ambiti di impiego e diventando un problema particolarmente serio per le aziende di intermediazione finanziaria e transazionale, per le quali un'interruzione del servizio, anche per breve tempo, determina danni economici molto ingenti.

In queste condizioni così mutevoli la protezione deve essere capace di adattarsi e rispondere in "dinamico", utilizzando strumenti costantemente aggiornati in grado di analizzare dati sia strutturati sia destrutturati che includano e-mail, documenti, siti Web e applicazioni (anche mobili).

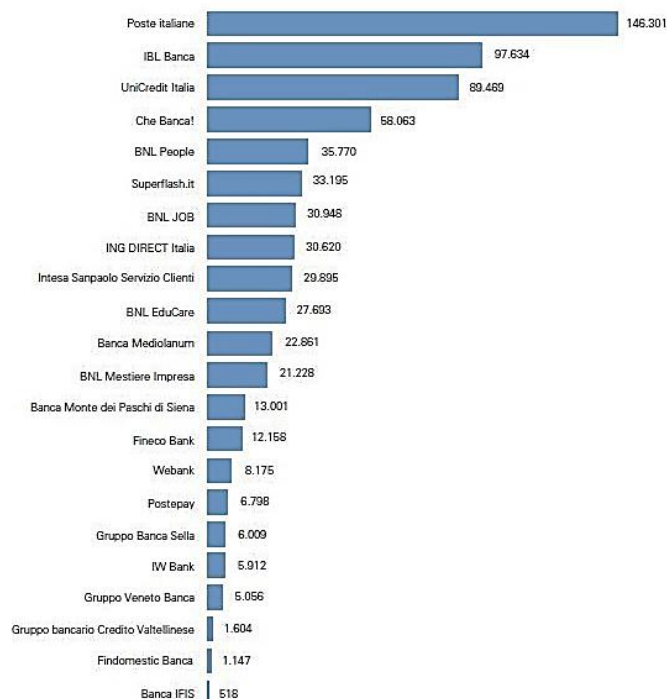
La mobilità e la tendenza a utilizzare dispositivi personali anche per il lavoro, il cosiddetto fenomeno del BYOD (Bring Your Own Device), introduce ulteriori vulnerabilità. Quella di privilegiare l'utilizzo di uno strumento di comunicazione unico è, peraltro, un'abitudine particolarmente diffusa all'interno del mondo dei business manager, che facilmente si trovano a ospitare sul proprio dispositivo mobile informazioni aziendali importanti e riservate, incluse password di accesso alla rete aziendale, dati sensibili o business critical. Non è poi insolito l'uso di software o di servizi online (per esempio Dropbox) per trattare o archiviare dati critici con modalità che sfuggono al controllo dell'IT, spesso con insufficiente consapevolezza dei rischi.

Queste nuove falle nella sicurezza vanno affrontate attraverso un approccio strategico che definisca modalità e regole per l'uso dei dispositivi mobili e preveda altresì opportune tecnologie di gestione e controllo per minimizzare il rischio della diffusione di malware.

Un altro aspetto determinante nel nuovo scenario della sicurezza è quello legato alla crescente diffusione dell'utilizzo di risorse IT sotto forma di servizio o in modalità cloud. Si tratta di un tema che trova un crescente consenso anche nelle organizzazioni del mercato finanziario per l'opportunità che offre di avere a disposizione risorse di elaborazione virtualmente infinite con cui effettuare operazioni di analytics, in tempo reale, su grandi volumi di dati distribuiti. Strettamente connesso alla sicurezza dei dati nel cloud vi è anche il tema delle diverse normative (non sempre coerenti tra loro) delle varie nazioni in cui questi dati possono essere memorizzati fisicamente.

Anche i social media comportano nuovi rischi e le banche si stanno aprendo sempre più verso questo mondo. Sono infatti più di 700mila gli italiani che ottengono informazioni e assistenza sugli account Facebook e Twitter delle principali banche italiane, soprattutto nelle fasce orarie esterne a quelle dell'apertura al pubblico degli sportelli.

Una recente indagine effettuata da KPMG dedicata al social banking ha analizzato i principali indicatori legati a Facebook e Twitter relativi a 18 banche italiane differenti per profilo e dimensione, inclusi alcuni operatori che operano esclusivamente online. Di queste 18 banche, al primo maggio 2013, 17 avevano una pagina attiva su Facebook e raccoglievano in totale 684mila fan. Solo 14 su 18 erano invece presenti su Twitter con un numero di follower totali di poco inferiore a 25mila (conseguenza della più recente apertura dei canali Twitter). Su questi media, accanto ai principali Gruppi, si presentano in ottima posizione anche le banche dalla forte vocazione online, che possiedono una clientela limitata ma molto attiva nel mondo dei social media.



Numero di Fan Facebook al primo maggio 2013
(Fonte KPMG; elaborazione su dati pubblici a cura di ECCE Customer/Decisyon)

La presenza sui canali social richiede di predisporre specifiche misure di protezione. Per esempio, è necessario predisporre meccanismi automatizzati per garantire la sicurezza delle pagine Web da possibili compromissioni. Nel caso delle banche, anche in assenza di conseguenze dirette, il danno di immagine causato dalla semplice compromissione della pagina Facebook, si tradurrebbe immediatamente in un importante danno economico per la perdita di fiducia da parte di investitori e clienti che potrebbero decidere di non affidare i propri risparmi a un istituto di credito che abbia dimostrato di non essere stato in grado di proteggere neanche sé stesso.

Attacchi mirati: il nuovo volto delle minacce

Gli attacchi mirati (Advanced Persistent Threat) sono tra le ultime novità in fatto di minaccia e stanno conquistando una crescente notorietà per l'elevato danno che sono in grado di arrecare, ulteriormente aggravato dall'alto livello di efficacia che solitamente riescono a conseguire, favorito dalla difficoltà incontrata dalle soluzioni di protezione tradizionale nel contrastarle.

Il target di questi attacchi si sta progressivamente spostando dalle organizzazioni governative verso quelle di carattere finanziario ed enterprise. È soprattutto l'elevata redditività offerta dalla compromissione della rete di una società che opera in ambito finanziario a giustificare gli sforzi e gli investimenti necessari per questo tipo di attacchi.

Si tratta di processi di attacco sofisticati che si protraggono nel tempo e fanno ricorso a tecniche diversificate, con un uso massiccio del social engineering favorito dalla disponibilità di informazioni presenti sui siti di social network.

Un "Advanced Persistent Threat" è un processo di attacco che segue regole precise e determinate e che è stato studiato e definito tanto da poter essere ricondotto a sei fasi specifiche.

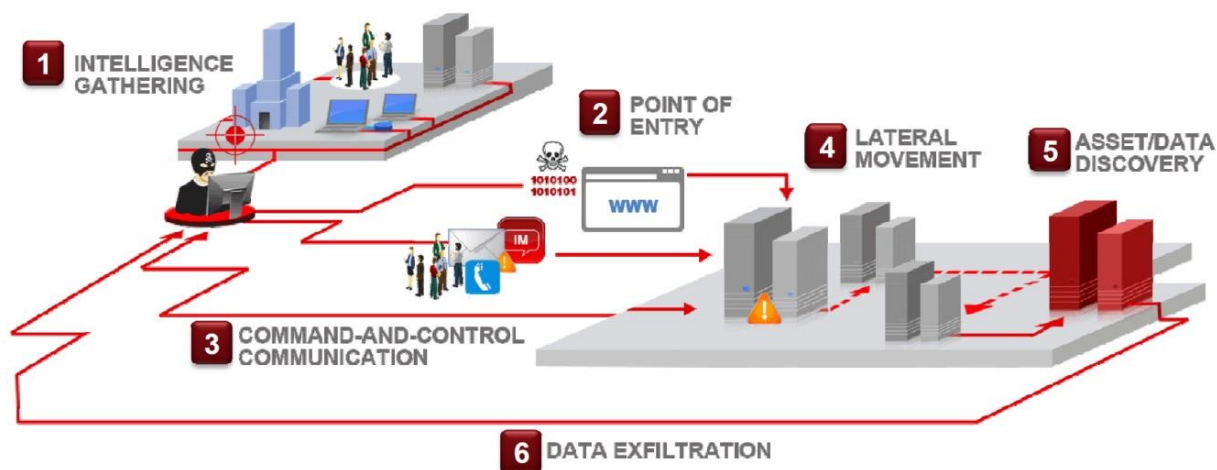
La prima fase è quella di preparazione dell'attacco, in cui viene effettuata l'investigazione e sono utilizzati semplici tool per raccogliere le informazioni sull'organizzazione target e sui soggetti indirettamente collegati a essa. Tra questi ultimi possono esserci aziende partner, collaboratori o clienti dell'organizzazione sotto attacco, spesso aggirati con l'uso di tecniche di social engineering al fine di ottenere informazioni che, separatamente, possono sembrare poco rilevanti ma che, se correlate tra loro, possono fornire chiavi per la compromissione della sicurezza.

La fase 2 di un attacco mirato è quella di penetrazione iniziale in cui si cerca di installare un malware per ottenere la compromissione del primo sistema (solitamente uno poco importante e quindi più vulnerabile) che sarà deputato a costituire il tassello di partenza per la costruzione di una vera e propria piattaforma di attacco.

La fase successiva prevede la predisposizione di un centro di comando e controllo (C&C) per garantire la comunicazione continua tra l'host compromesso e il server C&C e, quindi, con la fase 4, lo spostamento all'interno della rete alla ricerca di sistemi che ospitano informazioni sensibili o in grado di fornire un accesso di livello superiore alle altre risorse di rete in modo da espandere la propria presenza e il controllo.

La fase 5 prevede un'investigazione sui sistemi interni, resa possibile dal fatto di essere già saldamente presenti all'interno della rete: prevede l'analisi delle vulnerabilità sui server, degli hot-fix installati o della tipologia di comunicazione utilizzata. A questo livello gli hacker sfruttano una backdoor per scaricare informazioni.

L'ultima fase è quella dell'attacco vero e proprio verso il target prefissato, durante la quale vengono sottratte informazioni chiave attraverso la backdoor e in cui l'attacco viene costantemente ripetuto.



Le fasi di un attacco mirato

Da questa descrizione appare evidente che la predisposizione di una protezione efficace da un attacco mirato deve tenere conto delle vulnerabilità associate a ognuna di queste fasi, predisponendo contromisure in grado di operare non solo in modo efficace ma anche sinergico tra loro.

Una minaccia reale

Molti sono gli esempi che si possono citare a dimostrazione di quanto sia critico il tema delle minacce alla sicurezza IT nei confronti di istituzioni finanziarie e banche che, sempre più spesso, si presentano sotto forma di attacchi mirati. Elemento comune a tutti questi attacchi è l'elevato danno economico e di immagine che sono in grado di arrecare.

Tra i vari esempi possiamo ricordare quello denominato "Eurograbber", un sofisticato attacco, multi-dimensionale, mirato e nascosto che è riuscito a sottrarre oltre 36 milioni di Euro da più di 30mila clienti di differenti banche in tutta Europa. Gli attacchi sono iniziati in Italia e, subito dopo, decine di migliaia di utenti di sistemi di online banking infetti sono stati rilevati in Germania, Spagna e Olanda. L'attacco era completamente trasparente e i clienti bancari non avevano idea di essere stati infettati con trojan che compromettevano le loro sessioni di online banking e causavano una sottrazione diretta di fondi dai loro conti.

L'attacco infettava da prima i computer e i dispositivi mobili di clienti bancari online e, una volta che i trojan Eurograbber erano stati installati su entrambi i dispositivi, consentiva agli aggressori di controllare completamente e di manipolare le sessioni di online banking del cliente. Persino il meccanismo di autenticazione a due fattori utilizzato dalle banche per garantire la sicurezza delle transazioni online era stato aggirato dall'attacco e, anzi, veniva utilizzato dagli attaccanti per autenticare il loro trasferimento finanziario illecito. Il trojan utilizzato per attaccare i dispositivi mobili era stato sviluppato sia per la piattaforma Blackberry sia Android al fine di ampliare al massimo il target dell'attacco, riuscendo a infettare sia gli utenti corporate sia di "private banking" e a prelevare illecitamente cifre variabili tra 500 e 250mila Euro.

Un altro caso recente ha previsto l'attività strettamente coordinata di più persone che hanno operato simultaneamente e con precisione in più di due dozzine di Paesi riuscendo a rubare 45 milioni dollari da migliaia di sportelli bancomat in poche ore. Nella sola New York City, i ladri hanno effettuato prelievi illeciti su 2904 ATM in poco più di 10 ore sottraendo 2,4 milioni dollari.

L'operazione ha coinvolto sia esperti di computer che operano nel mondo dell'Internet hacking, che hanno manipolato le informazioni finanziarie sia criminali "da strada" che hanno utilizzato queste informazioni per saccheggiare gli ATM.

La prima fase dell'attacco è partita da un'infiltrazione all'interno del sistema di un'insignificante società indiana di elaborazione di carte di credito, che gestisce carte di debito prepagate Visa e MasterCard.

La conformità alle Normative

Un altro tema centrale che coinvolge il mondo finanziario con importanti risvolti di sicurezza è l'imponente castello di normative nazionali e internazionali che interessano questo settore e che si traducono nell'esigenza di predisporre processi e modalità per la gestione delle informazioni durante il loro ciclo di vita, che siano allineati con i requisiti di riservatezza, tracciabilità e protezione richiesti.

Nell'ambito finanziario esistono normative indirizzate a garantire la tutela delle informazioni privilegiate, la trasparenza e a fare in modo che non si creino abusi nel mercato. La normativa comunitaria in materia di Market Abuse ha determinato in Italia la nuova disciplina in materia di "internal dealing" (entrata in vigore il primo aprile 2006) che regola la trasparenza sulle operazioni aventi come oggetto azioni di società quotate e strumenti finanziari a esse collegati compiute da esponenti aziendali delle società medesime e da persone a questi ultimi strettamente legate.

Sempre in ambito finanziario, gli accordi di Basilea hanno profondamente modificato i meccanismi con cui gli organismi finanziari effettuano il controllo e la valutazione dei rischi derivanti dai crediti concessi, imponendo alle banche di modificare radicalmente i propri processi per conformarsi ai nuovi requisiti.

Non sono trascurati neppure i contenuti trasmessi tramite telefono e Internet, a cui sono riconducibili il Decreto Gentiloni (Legge per il filtraggio di Internet) e il Decreto Pisanu, che rientra nelle misure per contrastare il terrorismo internazionale.

Il Payment Card Industry Data Security Standard

Gli attacchi alla sicurezza nell'utilizzo delle carte credito si stanno costantemente moltiplicando ed espandendo, anche a seguito della progressiva diffusione di negozi online e della familiarità con cui si utilizza Internet. Il settore finanziario ha così finito, nel corso degli anni, con l'emettere continuamente normative regolamentari sempre più severe per quanto concerne le modalità di realizzazione e di protezione dei sistemi di pagamento e delle card che vengono utilizzate nell'ambito dei diversi circuiti di pagamento.

Tra questi, lo standard Payment Card Industry (PCI) Data Security Standard (DSS) ha un ruolo molto importante e ha visto l'adesione di tutte le principali società di carte di credito. Contrariamente ad altri casi, la richiesta di conformità alle norme stabilite dallo standard è particolarmente severa ed è del tipo "tutto o niente": non è prevista un'adesione parziale o il rispetto esclusivamente di alcune sue parti.

Le entità e le persone interessate a soluzioni conformi allo standard PCI DSS sono raggruppabili in due diversi insiemi:

- **Industrie:** società che svolgono attività commerciale, mercantile o service provider che immagazzinano, elaborano o trasmettono in qualsiasi modo i dati delle persone che possiedono una regolare carta di pagamento e utilizzano un software che supporta il commercio elettronico. È un gruppo molto ampio che comprende, solo per citare alcuni esempi, società del retail, dell'hospitality (ristoranti, hotel e così via), dei trasporti (linee aeree, car rental, ferrovie), dei servizi finanziari (banche, gestori carte di credito, broker, assicurazioni), Ospedali, utility pubbliche.
- **Responsabili:** spaziano dai CIO agli IT manager sino ai manager responsabili della compliance.

A entrambi le categorie lo standard PCI mette a disposizione un insieme di regole che aiutano adeguatamente nell'implementare una politica per la sicurezza dei dati inerenti i proprietari di carte di pagamento.

Lo standard PCI indirizza una serie di 12 requirement, suddivisi in sei diversi temi di intervento, che nel complesso stabiliscono i criteri e le attività di sicurezza da espletare nell'ambito di un sistema/processo che tratti i dati di un proprietario di una card, di debito o di credito, utilizzata come sistema di pagamento.

I sei temi sono:

1. realizzazione e mantenimento di una rete sicura,
2. protezione dei dati del possessore di una card,
3. mantenimento di un programma di gestione delle vulnerabilità,
4. implementazione di misure forti di controllo dell'accesso,
5. test e monitoraggio periodico della rete,
6. mantenere una adeguata policy per la sicurezza delle informazioni.

Il Testo Unico sulla Privacy

Alla garanzia di integrità dei dati si indirizza anche il Testo Unico sulla Privacy (D.Lgs. 196/2003) che ha introdotto importanti novità tra cui l'obbligo di creare una catena di comando formalizzata, dedicata alla garanzia della privacy, in cui vengono definiti ruoli specifici (Titolare del trattamento, Responsabile, Incaricato) a cui corrispondono compiti e responsabilità altrettanto definiti.

In particolare, nell'articolo 34 del testo unico sulla privacy (relativo al Trattamento con strumenti elettronici), vengono definite, nei modi previsti dal disciplinare tecnico, le seguenti misure minime di sicurezza:

- autenticazione informatica;
- adozione di procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- tenuta di un aggiornato documento programmatico sulla sicurezza;
- adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Una questione fondamentale riguarda l'attribuzione di responsabilità per la sicurezza nell'accesso a dati e applicazioni. Di fatto, poiché la questione ha risvolti sia penali sia amministrativi, il rappresentante legale della società diventa un soggetto perseguibile anche penalmente. La possibilità (anche se remota) di un coinvolgimento penale dell'amministratore delegato a fronte di inadempienze di questo tipo, apre comunque una serie di questioni in grado di modificare scelte importanti nell'impostazione della strategia di sicurezza e nell'adozione di soluzioni informatiche.

Gli obblighi di un'organizzazione in merito alla privacy devono anche tenere in considerazione una serie di provvedimenti specifici del Garante della Privacy differenzianti in base alla tipologia di mercato. In particolare, per l'ambito finanziario, i dati rilevanti ai fini della privacy sono riconducibili a tre tipologie:

- protezione dei dati dei clienti utilizzati per le operazioni di monetica,
- protezione delle anagrafiche relative alla gestione dei consensi,
- gestione del customer profiling che comprende i dati di gestione del rischio finanziario.

Tutto ciò richiede all'azienda una capacità di rispondere in modo rapido e puntuale e, implicitamente, le impone di disporre di un'infrastruttura tecnologica continuamente aggiornata e flessibile che consenta di mantenerla "privacy compliant" nel tempo.

Ciò che si delinea è che la conformità ai requisiti normativi sottintende un approccio strategico alla protezione dei dati che riguarda non solo l'ambito tecnologico ma anche quello organizzativo e di processo attraverso la predisposizione di opportune metodologie. Peraltro, i processi di tracciabilità che consentono di attribuire le responsabilità in modo inequivocabile richiedono sistemi per la gestione e il controllo dei privilegi attraverso opportune policy formalizzate.

LA GOVERNANCE DELLA SICUREZZA

Correlare i Big Data della sicurezza

Lo scenario delineato mette in evidenza alcuni requisiti che dovrebbero caratterizzare una piattaforma di sicurezza ICT a supporto di una strategia efficace di protezione in ambito finanziario. Il primo punto è che, innanzitutto, è necessario affrontare in maniera unificata i rischi associati a tutti i processi di business. È, dunque, importante predisporre un modello di protezione integrato in cui tutti gli strumenti di controllo possano essere gestiti e osservati da un punto unico in grado di fungere da collettore delle informazioni.

L'integrazione, però, da sola non basta, perché gli attacchi operano contemporaneamente su più fronti e con più vettori, con tecniche sofisticate che gli consentono di occultarsi molto bene e di superare controlli di primo livello. Diventa allora importante predisporre un meccanismo di analisi che sia in grado di comprendere quello che sta accadendo e di correlare le informazioni di sicurezza per riuscire a individuare eventuali anomalie che rappresentano i prodromi per l'identificazione di azioni nocive e che possono emergere solo da una visione dello scenario complessivo.

Quelli della sicurezza sono veri e propri Big Data. Si stima che in media i sistemi di un'organizzazione di livello enterprise producano 10-15 Terabyte di dati di sicurezza a settimana: una quantità di informazioni enorme che, peraltro, la comunità degli analisti prevede raddoppierà ogni anno fino al 2016. Si tratta di numeri che rendono complesso se non impossibile per un'azienda mantenere in casa i processi di analisi. La capacità di gestire e analizzare correttamente i Big Data della sicurezza è, invece, quella che consente di individuare una violazione in pochi minuti e il fattore tempo diventa fondamentale per poter prevenire la perdita di dati.

Gli istituti di credito e le aziende finanziarie sono chiamate a un uso responsabile e consapevole delle risorse ICT che permetta loro di gestire i rischi IT e, nel contempo, di sfruttare le opportunità che il mercato offre, massimizzando i benefici forniti da una politica di protezione.

I processi delle aziende del mondo finance associati all'interazione interna e con i propri clienti richiedono l'adozione di meccanismi di automazione e informatizzazione, di archiviazione di informazioni digitali business critical, di scambio e condivisione sicura dei dati, di accesso controllato alla rete oltre che la predisposizione di misure in grado di evitare l'interruzione dell'attività e ritardi nel "go to market" sull'offerta di servizi finanziari.

Anche le soluzioni di protezione migliore diventano però inefficaci se non sono affrontate in un contesto strategico e inquadrare all'interno dei processi aziendali per attivare strumenti capaci di intervenire in modo proattivo e di fornire una capacità di risposta in tempo reale.

Va quindi compreso che la sicurezza, avendo profonde implicazioni organizzative è un tema che non va affrontato unicamente a livello tecnologico, ma richiede di definire l'idea di una Governance della Sicurezza.

In altre parole, la sicurezza dei dati presuppone il coinvolgimento di diverse funzioni: una parte di Governance che si occupi di definire le linee strategiche e valutare i rischi associati; una parte di IT Security indirizzata a valutare il livello di rischio e definire, di conseguenza, misure di protezione basate sull'utilizzo di strumenti tecnologici e criteri di tipo organizzativo.

La gestione e il controllo del rischio

Pensare alla governance della sicurezza significa porsi come obiettivo quello della gestione del rischio. Il “rischio” è il punto di partenza di ogni considerazione sulla sicurezza, ma la complessità delle tecnologie rende il manager incapace di comprendere quali siano le reali minacce e, quindi, di valutare correttamente quali asset aziendali siano in pericolo, nonché quanto sia grande tale pericolo.

Questo, però, non deve rimanere l'unico approccio alla sicurezza, altrimenti potrebbe limitare le scelte e le considerazioni all'ambito del threat management, cioè a proteggere l'azienda dalle minacce, esterne o interne, ma non consentirebbe di sfruttare alcuni elementi abilitanti della sicurezza.

Le soluzioni di CRM (Customer Relationship Management), per esempio, sono un chiaro esempio di come si possano introdurre in una banca o un'azienda nuove tecnologie per estendere e ottimizzare i processi di business. Queste attività, peraltro, richiedono necessariamente l'impiego di tool di sicurezza al fine di garantire l'autenticità e l'integrità delle transazioni con clienti e partner. Anche qui esiste, in effetti, un rischio: per esempio, che un cliente non riconosca un ordine o che non siano rispettati i necessari vincoli legali.

Solo considerando tutti gli aspetti della sicurezza e, quindi, i rischi e le opportunità che un'azienda deve fronteggiare, è possibile valutare correttamente quali soluzioni sono indispensabili, quali utili e quali probabilmente inutili. Quello che emerge è una sorta di trade-off tra l'investimento richiesto e il livello di protezione che si vuole o può ottenere e che, in ambito finance, è comunque molto elevato.

L'analisi del rischio relativo alla sicurezza delle informazioni è il punto di partenza per impostare un processo di pianificazione volto alla realizzazione di un sistema per l'Information Security Management. Il rischio è tanto più alto quanto più elevato è il valore della risorsa che si ritiene di dover proteggere e quanto maggiore è la minaccia che incombe su quella risorsa. Per un'azienda finanziaria uno dei principali asset critici sono proprio le informazioni, la cui perdita o diffusione non autorizzata potrebbe determinare la cessazione stessa dell'attività.

L'importanza della governance

Adottare un modello di governance della sicurezza significa seguire un approccio alla gestione della sicurezza dell'informazione basato su criteri di controllo e di gestione manageriale per organizzare le risorse umane, tecnologiche, logistiche ed economiche necessarie per soddisfare integrità, riservatezza e disponibilità dell'informazione.

In altre parole per impostare una governance della sicurezza è necessario predisporre una serie di processi che siano anche in grado di produrre informazioni significative e utilizzabili dai manager.

In generale si possono individuare quattro aspetti fondamentali:

- la gestione delle vulnerabilità, ovvero un insieme minimo di regole da seguire per soddisfare dei requisiti di sicurezza;
- la rilevazione degli eventi con uno standard ben definito;
- la gestione degli eventi legati alla sicurezza con delle politiche di ritenzione dei log;
- le politiche di risposta agli incidenti.

La sicurezza non può fermarsi a una semplice questione tecnologica. Il successo degli Advanced Persistent Threat sta dimostrando ulteriormente che il recupero di informazioni riservate tramite tecniche di social engineering costituisce una grave minaccia anche in presenza di politiche di sicurezza altrimenti difficilmente eludibili. La formazione e il coinvolgimento di tutto il personale a conoscenza di informazioni riservate di qualunque livello è quindi un passo necessario per integrare la sicurezza da tutti i punti di vista.

Un ulteriore elemento da prendere in considerazione è la valutazione dei risultati individuando nella gestione della sicurezza dei parametri oggettivi per misurare l'efficacia della protezione. Per esempio, è possibile definire un tempo di esposizione all'attacco come somma del tempo di rilevamento della vulnerabilità o di un attacco più il tempo di reazione, ovvero il tempo necessario per rispondere ed eliminare il problema incontrato; chiaramente, minore è il tempo di esposizione che la gestione della sicurezza riesce a garantire, maggiore sono la sua efficacia e di conseguenza la produttività che un'azienda riesce a garantire in caso di attacco.

L'APPROCCIO ALLA SICUREZZA DI TREND MICRO

Trend Micro si propone di rispondere a molti dei requisiti finora espressi mettendo sul piatto della bilancia un patrimonio di conoscenze che deriva da 25 anni di attività dedicata esclusivamente al tema della Content Security, risorse distribuite per combattere il cyber crime tra le più imponenti a livello globale e una gamma di soluzioni tecnologiche che sono il riflesso di una vocazione alla Ricerca e Sviluppo.

L'azienda giapponese si è posta, in anticipo sui tempi, molte questioni legate alle nuove sfide tecnologiche e dei nuovi modelli di archiviazione, accesso e distribuzione delle informazioni per arrivare a proporre un modello di sicurezza basato su un framework unificato per la gestione e la protezione di dati, infrastrutture, applicazioni e dispositivi mobili.

L'offerta di sicurezza integra prodotti, servizi e soluzioni per la sicurezza dei contenuti, adatte a far fronte alle esigenze di organizzazioni di grandi dimensioni che operano nell'ambito finance.

Per riuscire a fornire il miglior livello di difesa e una protezione proattiva, Trend Micro ritiene che si debbano affrontare due sfide critiche legate alle tempistiche. La prima sfida critica è di minimizzare il tempo necessario per proteggere l'azienda da minacce nuove e sconosciute, accelerando il periodo necessario per identificare le minacce, sviluppare una protezione e per renderla operativa. La seconda sfida riguarda la necessità di ridurre il tempo per gestire la sicurezza adottando una soluzione che sia in grado di minimizzare la complessità oltre che di fornire una protezione efficace.

Trend Micro si propone di far fronte a entrambi questi requisiti per la sicurezza dei contenuti coniugando una protezione immediata capace di "chiudere" le finestre delle vulnerabilità con una sicurezza integrata che riduce la complessità e minimizza il tempo necessario per acquisire, rilasciare e gestire la sicurezza dei contenuti. Il modello Trend Micro integra la protezione dei dati estesa attraverso l'intera organizzazione con la sicurezza dalle minacce e dagli attacchi mirati che sfrutta a livello locale le analisi e le correlazioni effettuate su scala globale mediante un'intelligenza distribuita.

Il risultato è una protezione in grado di affrontare il tema della riservatezza e della protezione dei dati in ambienti fisici, virtuali e in-the-cloud. A completare questo quadro per una sicurezza data centrica Trend Micro pone una piattaforma di gestione unificata e basata su policy che coordina in modo sinergico le diverse attività di analisi intelligente.

Una caratteristica distintiva dell'approccio di Trend Micro è la capacità delle soluzioni di sicurezza di essere consapevoli del contesto per capire chi accede a quali dati, come (tramite e-mail, Instant Messaging, USB e così via), quando (consapevolezza temporale) e dove (consapevolezza geografica).

Il vendor promuove anche una difesa di tipo personalizzato basata su un modello ciclico organizzato in quattro fasi:

- Rilevamento: il primo step prevede di identificare gli attacchi con tecniche avanzate di rilevazione sulla rete e la protezione dei punti chiave come il gateway e-mail.
- Analisi: vengono quindi valutate le minacce utilizzando analisi "sandbox" specifiche per ogni azienda e l'accesso integrato a un meccanismo di intelligenza globale (Smart Protection Network).
- Adattamento: per bloccare ulteriori attacchi con black list e firme personalizzate che vengono rilasciate verso la rete, i gateway e gli endpoint.
- Risposta: utilizzando profili di attacco e analisi intelligente degli eventi che avvengono su tutta la rete, per consentire un contenimento e attività di bonifica



I pilastri alla base del modello di difesa personalizzata proposto da Trend Micro

Gli strumenti tecnologici, l'intelligenza e l'approccio basato sull'analisi dell'intero ciclo di vita definiscono un approccio metodologico adatto per predisporre difese preventive utili anche contro gli attacchi mirati.

Tra le innumerevoli soluzioni che traducono in realtà questo modello, possiamo ricordare: Deep Security, la soluzione sviluppata in stretta collaborazione con VMware per la sicurezza multilivello di ambienti fisici, virtuali e cloud; Deep Discovery per difendersi dalle minacce avanzate (Advanced Persistent Threat) e OfficeScan per la protezione degli endpoint.

Trend Micro dispone, inoltre, di una consolidata esperienza nella gestione di grandi clienti bancari italiani. Per esempio, il vendor può vantare, presso uno dei principali Gruppi bancari italiani, l'installazione delle proprie soluzioni Enterprise Security for Endpoint su oltre 100mila client e 8mila licenze server di altre soluzioni di sicurezza. Agli aspetti tecnologici Trend Micro affianca un'articolata offerta di servizi e un'attività di supporto dedicato.

La Smart Protection Network

Alla base del suo approccio verso la sicurezza Trend Micro pone la Smart Protection Network, un'infrastruttura per la protezione automatizzata degli ambienti fisici, mobili, virtuali e cloud progettata per tutelare gli utenti dalle minacce a fronte di un impatto ridotto su reti e sistemi. Abbinando tecnologie "in-the-cloud" a client leggeri, diventa possibile accedere alle più recenti misure di protezione ovunque e in qualsiasi modo ci si connetta: da casa, dalla rete aziendale o anche in viaggio.

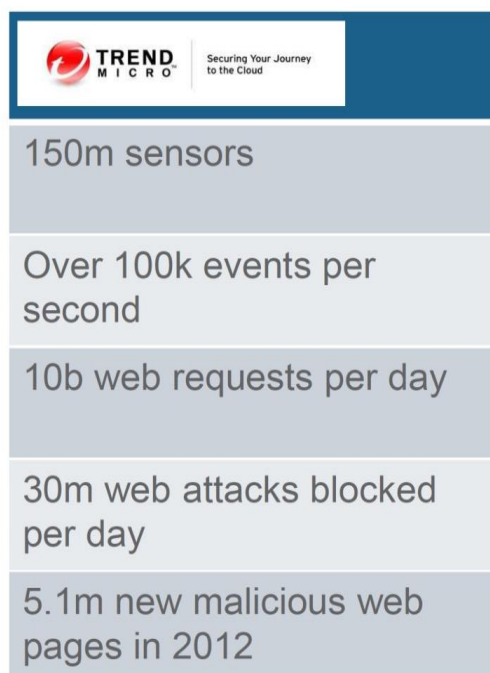
Trend Micro Smart Protection Network sfrutta un approccio di difesa intelligente basato sulle conoscenze collettive ottenute dall'ampio e globale bacino dei clienti Trend Micro, mettendo in relazione i dati provenienti da oltre 70 miliardi di query giornaliere.

Smart Protection Network prevede l'assegnazione del livello di reputazione di URL, e-mail, file e anche un meccanismo per valutare dinamicamente la reputazione delle App rispetto ad attività dannose, uso improprio delle risorse e violazioni della privacy.

La Smart Protection Network è integrata nei prodotti e nei servizi Trend Micro fra cui le proposte mobile, endpoint, server, network, messaging, gateway e SaaS destinate sia a un pubblico consumer sia business.

Per rispondere alle nuove tipologie di minacce Trend Micro ha anche sviluppato funzioni analitiche in grado di intervenire su Big Data per identificare una gamma più ampia di nuove minacce.

Il vendor ha predisposto anche i Threat Intelligence Services, che rispondono alle esigenze di grandi realtà enterprise, pubbliche amministrazioni e partner. Si tratta di un'offerta di servizi che permette di utilizzare l'intelligence della Trend Micro Smart Protection Network per costruire o ottimizzare le infrastrutture di sicurezza, in un'ottica di contrasto alle sottrazioni di dati e altre possibili minacce.



I numeri della Smart Protection Network

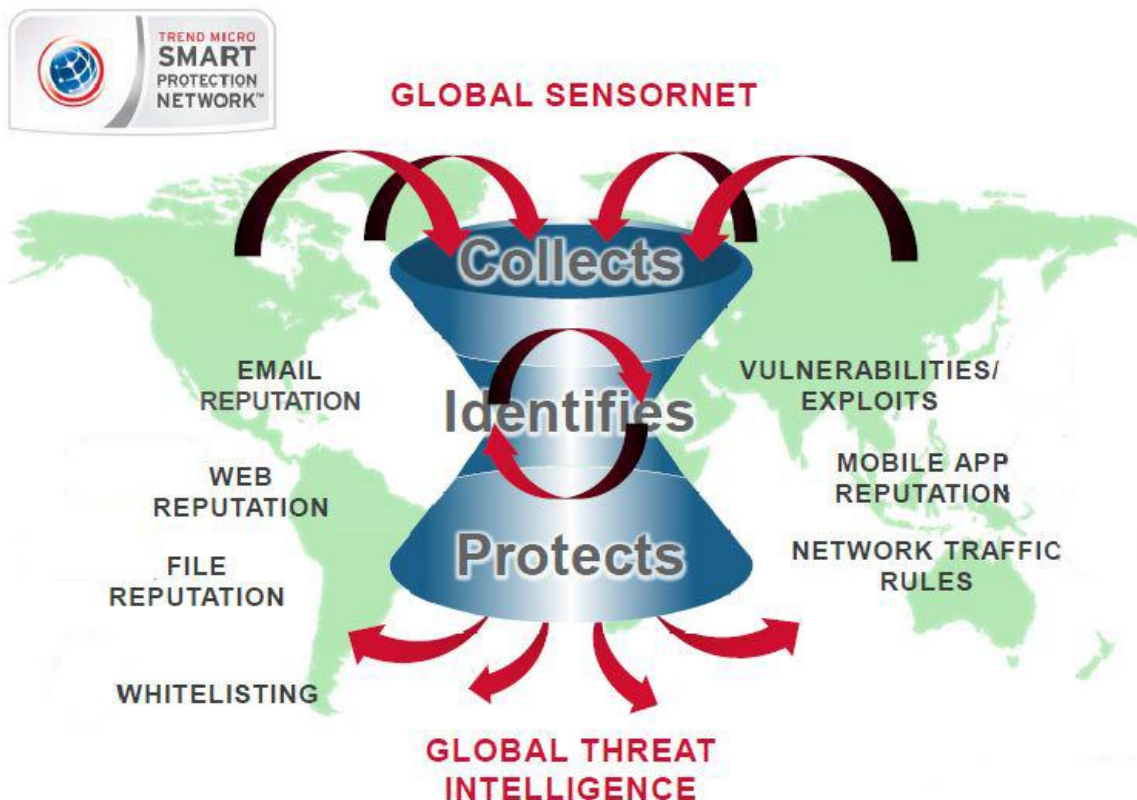
Uno strumento per l'analisi di reputazione e comportamento

La tecnologia di reputazione Web di Trend Micro rileva la credibilità dei domini Web tramite l'assegnazione di un punteggio basato su fattori quali l'età del sito Web, le modifiche cronologiche all'ubicazione del sito e le indicazioni di attività sospette scoperte tramite l'analisi del comportamento delle minacce informatiche.

Trend Micro convalida gli indirizzi IP verificandoli a fronte di un database della reputazione di fonti di spam note e utilizzando un servizio dinamico capace di valutare la reputazione del mittente in tempo reale. Le classificazioni della reputazione vengono perfezionate tramite un'analisi continua del "comportamento" degli indirizzi IP, della portata dell'attività e della cronologia precedente. I messaggi e-mail dannosi vengono bloccati in-the-cloud in base all'indirizzo IP del mittente, impedendo così alle minacce di raggiungere la rete dell'utente.

A livello di file, la tecnologia Trend Micro verifica la reputazione di ciascun file ospitato su un sito Web o allegato a un messaggio e-mail a fronte di un ampio database, prima di consentire l'accesso all'utente. Le reti di trasmissione dei contenuti a elevate prestazioni e i server di cache locale minimizzano la latenza. Le informazioni sulle minacce informatiche sono memorizzate in-the-cloud e quindi possono essere rese immediatamente disponibili a tutti gli utenti nella rete.

L'infrastruttura di Trend Micro fornisce agli utenti anche informazioni sulle App utilizzate, impedendo di scaricare quelle dannose e identificando quelle che potrebbero abusare della privacy o dell'uso del dispositivo. La tecnologia di reputazione delle App mobili può essere integrata dai fornitori di servizi e dagli sviluppatori delle applicazioni per fornire App di migliore qualità e un maggiore livello di protezione agli App store. La correlazione con altre tecnologie di reputazione abilita la protezione per le pagine Web in cui sono presenti App pericolose.



Smart Protection Network

L'importanza di correlare gli eventi di sicurezza

Stabilire il livello di reputazione prevede l'interazione tra due attività.

La prima è la raccolta degli eventi di sicurezza che avviene in tempo reale a livello globale; la seconda è la correlazione di questi eventi, che costituisce uno degli elementi in cui Trend Micro rivendica la propria eccellenza tecnologica e che consente di intervenire in modo accurato e selettivo, garantendo un elevato livello di protezione senza penalizzare in modo inutile l'utente.

La tecnologia di correlazione con l'analisi del comportamento mette in relazione tra loro diversi gruppi di attività per determinare se queste siano o meno dannose. Infatti, un'attività singola prodotta da una minaccia Web potrebbe apparire innocua, ma quando più attività vengono rilevate insieme, è più facile identificare la presenza di una minaccia reale.

Aggiornando continuamente il proprio database delle minacce in base a questo tipo di analisi, Trend Micro abilita una reazione automatica che interviene in tempo reale per proteggere dalle minacce e-mail e Web.

Attraverso cicli integrati di feedback si realizza una comunicazione continua tra i prodotti Trend Micro, le tecnologie e i centri di ricerca delle minacce attivi 24 ore su 24 e 7 giorni su 7. Ogni nuova minaccia identificata tramite una verifica di routine della reputazione di un singolo cliente aggiorna automaticamente tutti i database delle minacce di Trend Micro e blocca ogni successiva interazione del cliente e di tutti i clienti Trend Micro con una specifica minaccia.

Poiché le informazioni raccolte sulle minacce sono basate sulla reputazione dell'origine della comunicazione e non sul contenuto della specifica comunicazione, la riservatezza delle informazioni personali o aziendali resta tutelata.

La Smart Protection Network mette anche a disposizione white list in-the-cloud che sfruttano uno dei database più grandi al mondo, il GRID (Goodware Resource and Information Database), per un'identificazione rapida e accurata degli eventi sicuri al fine di minimizzare i falsi positivi. Le soluzioni Trend Micro per la protezione degli endpoint interrogano le white list ogni volta che viene individuato un file sospetto per verificare se sia o meno sicuro.

Questo database è utilizzato anche dai ricercatori Trend Micro per impedire che contenuti noti per essere sicuri vengano analizzati durante i processi di identificazione di codice nocivo. Inoltre, per identificare le possibili vulnerabilità delle applicazioni, Trend Micro collabora continuamente con i software vendor ed effettua un monitoraggio costante degli exploit.

L'infrastruttura Trend Micro esercita anche un controllo per definire policy in grado di identificare traffico di rete potenzialmente dannoso, sfruttando le informazioni provenienti dalla gestione di grandi ambienti di analisi (sandnet) continuamente alimentati con campioni di minacce informatiche.

LE SOLUZIONI PER LA CONTENT SECURITY

Per rispondere alle sfide della Content Security Trend Micro ha predisposto un ampio portafoglio di prodotti che punta a garantire la sicurezza dei dati ovunque questi risiedano, dagli endpoint fino al cloud, mettendoli al riparo da incidenti casuali o volontari.

La gamma di soluzioni software per la protezione dei dati comprende Trend Micro Data Loss Prevention, Cloud Encryption, Port and Device Control, Messaging Security, Endpoint Security,

Web Site Security, File Integrity Monitoring, Worry-Free Business Security e Safe Sync. Si tratta di soluzioni che vengono vendute sia singolarmente sia come add-on ai tradizionali prodotti anti-malware di Trend Micro.

Le soluzioni software di Trend Micro sono in grado anche di rispondere alle nuove esigenze di sicurezza che caratterizzano il progressivo percorso verso la virtualizzazione, che solitamente inizia con il consolidamento server, prosegue con la virtualizzazione estesa per server e desktop, per approdare infine al cloud.

La visione che guida la strategia di Trend Micro è che sia giunta a completamento la prima fase del percorso che prevede la messa in sicurezza dei workload dei server virtualizzati e che il futuro sarà caratterizzato da un lavoro di ottimizzazione delle performance della sicurezza virtuale in uno sforzo teso a virtualizzare le applicazioni a più alto traffico. Sulla base di questo presupposto Trend Micro ha sviluppato una serie di tecnologie di sicurezza capaci di integrarsi con gli hypervisor delle macchine virtuali.

Trend Micro Deep Security per gli ambienti virtualizzati

Una di queste soluzioni è Trend Micro Deep Security che include un ventaglio di differenti tecnologie di sicurezza e anti malware specializzate come IDS/IPS, protezione delle applicazioni Web, firewall, monitoraggio dell'integrità e moduli di "log inspection" e si avvale di funzioni anti-malware di tipo *agentless*.

Sviluppata in stretta collaborazione con VMware, Deep Security è adatta a proteggere i sistemi virtualizzati e supporta VMware vSphere 5.0 e VMware vShield Endpoint 2.0 garantendo compatibilità retroattiva con gli ambienti vSphere 4.1 e supportando anche ambienti a modalità mista.

Deep Security si integra con VMware e le sue API vShield Endpoint e VMsafe, fornendo protezione per le Virtual Machine sia *agentless* sia basata su agent.

L'architettura della piattaforma prevede i seguenti componenti:

- Deep Security Virtual Appliance, che applica in modo trasparente i criteri di protezione sulle macchine virtuali VMware;
- Deep Security Agent, un componente software installato su server fisico o su macchine virtuali non VMware, garantisce il rispetto dei criteri di protezione del data center.
- Deep Security Manager per la gestione centralizzata, con possibilità di creare profili di sicurezza e di applicarli ai server, di monitorare gli avvisi e le azioni preventive eseguite in risposta alle minacce, di distribuire gli aggiornamenti della protezione ai server e di generare rapporti su tutto il data center, sia esso fisico che virtuale, qualsiasi sia la piattaforma di virtualizzazione scelta.

Il livello di sicurezza fornito da Deep Security prevede molteplici funzionalità di protezione.

- *Intrusion Detection e Prevention (IDS/IPS)*. Fornisce un'analisi approfondita dei pacchetti per rilevare e bloccare possibili attacchi, analizzando il traffico alla ricerca di anomalie a livello di protocollo, di indicazioni su exploit e di violazioni delle policy di sicurezza.
- *Virtual Patching*. Consente di individuare le vulnerabilità a livello host e suggerisce le regole da applicare per proteggere applicazioni e sistemi.

- *Firewall*. Un sistema "stateful" di classe enterprise, che abilita la segmentazione della rete e le operazioni di audit richieste dallo standard PCI.
- *Protezione delle applicazioni Web*. Protegge le applicazioni Web da attacchi sofisticati come "SQL injection" e "cross-site scripting".
- *Protezione antivirus*. Fornisce una protezione malware "agentless" attraverso un'appliance virtuale VMware.
- *Integrity Monitoring*. Rileva e segnala modifiche potenzialmente nocive e inconsuete relative ai file critici del sistema operativo e delle applicazioni.
- *Controllo applicativo*. Prevede una serie di regole per fornire visibilità e controllo sulle applicazioni che accedono alla rete.
- *Analisi del registro e dei Log*. Analizza il log del sistema operativo e delle applicazioni per individuare importanti eventi di sicurezza, generare avvisi e fornire informazioni ai sistemi SIEM.
- *Virtualization Compliance*. Abilita l'isolamento delle virtual machine e funzionalità di "hardening" che proteggono e isolano le applicazioni per l'elaborazione dei pagamenti da altre macchine virtuali presenti sullo stesso hardware. La maggior parte delle funzioni sono disponibili come appliance VMware sia con agent sia in modalità agentless.

Queste caratteristiche, oltre a intervenire per la protezione dei server business-critical e degli endpoint, consentono a Deep Security di favorire la conformità allo standard PCI DSS tramite una soluzione unica, gestita centralmente, che risponde a 7 regole PCI e oltre 20 sotto controlli.

Sicurezza che favorisce il ROI

Per sfruttare la flessibilità e i potenziali risparmi offerti da virtualizzazione e cloud computing è importante disporre di un livello di sicurezza capace di massimizzare tali benefici e ottimizzare il ritorno sull'investimento (ROI).

Le prestazioni sono un aspetto in grado di avere un forte impatto sui costi e la sicurezza, pertanto, non deve avere un impatto significativo su di esse. Inoltre, le soluzioni di sicurezza devono garantire un'efficace protezione dei dati per evitare costose attività di ripristino.

Va poi osservato che uno dei modi primari per ridurre i costi e migliorare il ROI attraverso la virtualizzazione all'interno del data center è quello di aumentare la densità di macchine virtuali per singolo sistema fisico.

Le best practice suggeriscono anche di separare in zone i server e i dati in base alla loro sensibilità, alla proprietà o ai requisiti di conformità. Queste zone possono essere protette utilizzando software di sicurezza certificato per lo standard EAL4.

Trend Micro punta a favorire il conseguimento di tali obiettivi tramite soluzioni in grado di fornire protezione integrata per ambienti fisici, virtuali e cloud con sistemi di Intrusion Detection/Prevention, firewall, monitoraggio dell'integrità, ispezione dei log, anti-malware di tipo agentless e funzionalità di crittografia.

Il fatto che Trend Micro Deep Security sia specificamente progettato per gli ambienti virtuali, con una stretta integrazione con le API dell'hypervisor di VMware, un'architettura di sicurezza di tipo agentless e la certificazione EAL4 consente, pertanto, di massimizzare la densità di macchine virtuali senza pregiudicare la sicurezza.

Analogamente, nel caso dei desktop virtuali (VDI), gli stessi obiettivi si possono perseguire aumentando la densità di VDI per hardware fisico.

Attraverso l'integrazione con le API dell'hypervisor e l'uso di anti-malware agentless, la soluzione Trend Micro si propone di favorire la riduzione di carico sul sistema, eseguendo scansioni più intelligenti del desktop virtuale, evitando di analizzare più volte lo stesso file ed eliminando la necessità di scaricare un file di firma separato per ogni desktop virtuale.

Infine anche la capacità della soluzione Trend Micro di integrare la sicurezza e le console dell'hypervisor rappresenta un aspetto che riduce i compiti amministrativi e che va nella direzione del conseguimento di un migliore ROI.

Trend Micro mette anche a disposizione una serie di strumenti di calcolo per effettuare delle valutazioni sia online sia offline tra cui un interessante ROI Calculator.

Cost Saving Calculator

Workload type: Server
 Number of physical hosts: 192
 Number of CPUs per host: 2
 Number of cores per CPU: 8
 Total number of VMs: 4,000
 Current average host resource utilization: 60
 Maximum acceptable host resource utilization: 80

System admin cost per hour: \$ 100
 Time to provision new host server (hours): 4
 Setup time for legacy AV for existing VMs (hours): 16
 Setup time for new AV for existing VMs (hours): 0.25
 Ongoing administration time for legacy AV (hours per week per 100 VMs): 0.5
 Annual cost of legacy AV per agent: \$ 25
 Incl. VMware vShield Endpoint in Quote: Yes

VM Growth Rate: 1st year 20%, 2nd year 20%, 3rd year 20%

Your Results:

Legacy AV:			
Initial hosts:	192	Additional hosts added over 3 yrs:	32
Deep Security Agentless AV:			
Initial hosts:	139	Net Savings from easier operational administration (3 yrs):	\$500,028
Additional hosts added over 3 yrs:	23	Net Savings from avoidance of legacy AV renewal (3 yrs):	\$444,566
Fewer hosts needed with Deep Security:	62	Price of Trend Micro Deep Security and VMware vShield Endpoint (3 years):	\$483,000
Net Savings from fewer hosts (3 yrs):	\$1,307,766	Per Month Savings over 36 Months:	\$62,566
Overall Metrics:		Simplified Payback on Investment (months):	7.7
Reduction in Total Cost of Ownership:	\$1,769,361		
Return on Investment - 36 Month Period:	366%		

[about ROI-Calc](#) Print

Trend Micro online ROI Calculator

Trend Micro Deep Discovery per rilevare gli attacchi mirati

Deep Discovery è il fulcro della soluzione di difesa personalizzata Trend Micro contro gli Advanced Persistent Threat e consente di rilevare e analizzare le minacce e anche di adattare i meccanismi di protezione per reagire agli attacchi.

Deep Discovery prevede il monitoraggio a livello di rete con tecnologia sandbox personalizzata e in tempo reale, per rilevare precocemente eventuali attacchi. L'approccio di Deep Discovery punta a individuare contenuti, comunicazioni e comportamenti dannosi su tutte le fasi della sequenza di attacco.

La soluzione è costituita da due componenti.

- Deep Discovery Inspector che effettua l'ispezione del traffico di rete, il rilevamento delle minacce e l'analisi e la segnalazione in tempo reale.
- Deep Discovery Advisor, opzionale, che abilita un'analisi personalizzata aperta e scalabile della sandbox, la visibilità sugli eventi di sicurezza a livello di rete e le esportazioni di aggiornamento della sicurezza.

Trend Micro SecureCloud

Trend Micro fornisce sicurezza "dal cloud" con l'infrastruttura Trend Micro Smart Protection Network e sicurezza "per il cloud" con server e tecnologie crittografiche.

Per la protezione multilivello per i dati che risiedono all'interno dei cloud pubblici o privati Trend Micro ha sviluppato SecureCloud, una soluzione che protegge i dati di livello enterprise all'interno degli ambienti cloud mediante l'uso di crittografia e di tecniche di key management basate su policy. Questa tecnologia permette di tutelare i dati del cloud e di favorire la flessibilità necessaria per rivolgersi a cloud provider differenti, senza essere vincolati al sistema crittografico di un unico vendor.

SecureCloud consente di esercitare il controllo sulle modalità e sui punti di accesso alle informazioni per mezzo di funzioni che permettono di autenticare l'identità e l'integrità dei server che richiedono di accedere a volumi storage sicuri.

Questa soluzione abilita il rilascio automatico delle chiavi di cifratura. Gli utenti possono gestire le loro chiavi crittografiche per ambienti Amazon EC2, Eucalyptus e VMware vCloud direttamente tramite il servizio hosted Trend Micro SecureCloud o da un key server SecureCloud installato all'interno dei loro data center fisici.

Trend Micro SecureCloud è disponibile mediante abbonamento mensile o annuale, oppure tramite licenze software tradizionali.

Trend Micro Mobile Security

A supporto delle esigenze di protezione alimentate dal BYOD Trend Micro mette a disposizione Trend Micro Mobile Security, una soluzione di sicurezza rivolta alle aziende enterprise e di media dimensione per la protezione di un'ampia gamma di dispositivi mobili quali iPhone, iPad, sistemi in ambiente Android e Blackberry OS e Apple.

Questa soluzione utilizza tecnologie di prevenzione delle minacce, per la protezione dei dati e prevede una singola console di gestione centralizzata consentendo al business di avere visibilità e controllo ma, nel contempo, lasciando la libertà ai dipendenti di condividere i dati in modo sicuro attraverso ambienti fisici, virtuali e cloud. Gli amministratori hanno visibilità su numero, tipologia e configurazione dei sistemi mobili e possono applicare policy di sicurezza comuni su differenti dispositivi, differenziate in base alla posizione geografica del dispositivo. Tra le funzionalità offerte vi è la possibilità di disabilitare la fotocamera del dispositivo mobile, la connessione Bluetooth e il lettore di schede SD.

CONCLUSIONI

Il mondo delle organizzazioni finanziarie si trova al centro di attacchi che crescono in numero e in sofisticazione. La natura delle minacce diventa più aggressiva e nascosta, con azioni guidate da organizzazioni criminali strutturate, che mirano al profitto e che ormai operano secondo modelli analoghi a quelli delle imprese legali.

Sempre più spesso gli attacchi sono lanciati in modo mirato e portati avanti in modo meticoloso per un tempo prolungato durante il quale gli attaccanti cercano di continuare a operare mantenendosi nascosti o, in altre parole, in modo latente.

Il settore finanziario si trova a dover garantire la protezione dei dati e il rispetto alle normative in un contesto complesso, globale e in costante evoluzione. I rischi sono molteplici e spaziano dalla sottrazione di denaro, al danno di immagine, alle sanzioni fino alla compromissione di sistemi per sferrare altri attacchi.

Per affrontare queste sfide è richiesto un approccio strutturato che predisponga una governance della sicurezza in cui, in modo strategico e pervasivo, vengono coniugati gli aspetti organizzativi e procedurali con quelli tecnologici indirizzati a prevenire possibili minacce.

Sul versante tecnologico è utile perseguire un modello di protezione personalizzabile e in grado di automatizzare il più possibile le operazioni di sicurezza, per bloccare alla fonte le possibili cause di rischio.

Trend Micro, attraverso la Smart Protection Network e una gamma di soluzioni software basate su questa infrastruttura, propone un modello di protezione dei contenuti in linea con questi requisiti, che può contribuire a proteggere dai nuovi rischi le risorse delle aziende che operano nel settore finanziario e prevenire possibili danni economici.

*REPORTEC opera dal 2002 nel settore dell'editoria specializzata sull'ICT professionale, realizzando e pubblicando riviste, report, survey, e-magazine, libri. Pubblica le riviste cartacee **Direction, Solutions, Partners** (edito dalla consociata **Reportrade**) e gli e-magazine **Update Reportec, Security & Business, Cloud & Business, PartnersFlip**. Ha siglato un accordo con **Tom's Hardware Italia** per la gestione dei tre canali **B2B IT Pro, Manager e Resellers** accessibili all'interno del dominio **tomshw.it**. Reportec è **Media e Content Conference Partner di IDC Italia**.*

The logo for Reportec, featuring the word "Reportec" in a white, sans-serif font inside a dark blue rectangular box.

Sicurezza ICT e mercato Finance. Innovazione tecnologica e governance contro i nuovi rischi

© Reportec S.r.l. - Gennaio 2014 - Tutti i diritti riservati

Reportec S.r.l. via Marco Aurelio, 8 - 20127 Milano

Tel: (+39) 02 36580441 Fax: (+39) 02 36580444

www.reportec.it - www.tomshw.it/index/itpro.html - www.tomshw.it/index/manager.html - www.tomshw.it/index/reseller.html

Tutti i marchi citati in questo documento sono registrati e di proprietà delle relative società.

The logo for Reportec, featuring the word "Reportec" in a white, sans-serif font inside a dark blue rectangular box.