

LA SICUREZZA ICT NEL MERCATO MANIFATTURIERO

**SOLUZIONI PER AUMENTARE IL VANTAGGIO
COMPETITIVO**

Un'analisi indipendente realizzata da Reportec S.r.l e commissionata da Trend Micro Italia

SOMMARIO

Sommario	1
Uno scenario in evoluzione	2
Essere più sicuri per essere più competitivi	2
Sicurezza e manufacturing	3
Modelli di business e minacce in evoluzione	3
Attacchi mirati: il nuovo volto delle minacce alle imprese industriali	4
SCADA: un rischio trascurato	5
Correlare i Big Data della sicurezza	7
L'approccio alla sicurezza di Trend Micro	8
La Smart Protection Network	8
Uno strumento per l'analisi di reputazione e comportamento	9
L'importanza di correlare gli eventi di sicurezza	10
Un approccio originale per la protezione dei sistemi SCADA	11
Le soluzioni per la Data Protection	12
Trend Micro Deep Security per gli ambienti virtualizzati	12
Trend Micro Deep Discovery per rilevare gli attacchi mirati e persistenti	13
Conclusioni	13

LA SICUREZZA ICT NEL MERCATO MANIFATTURIERO

SOLUZIONI PER AUMENTARE IL VANTAGGIO COMPETITIVO

UNO SCENARIO IN EVOLUZIONE

Il settore manifatturiero rappresenta l'asse trainante della crescita economica italiana.

In base ai dati 2012 di Banca d'Italia, in Europa l'Italia è seconda solo all'economia tedesca per importanza del settore industriale sul valore aggiunto complessivo e si mantiene ai vertici mondiali nonostante la crisi l'abbia fatta arretrare dietro Giappone e Corea del Sud. Un importante contributo a questi risultati viene dalle eccellenze del made in Italy ovvero dalle cosiddette 4 A: automazione-meccanica, alimentari e bevande, abbigliamento-moda, arredo-casa.

Quello industriale è anche uno dei contesti più competitivi e, nell'attuale periodo di congiuntura economica, tra i più difficili dal dopoguerra, diventa ancora più rilevante il tema dell'innovazione che si traduce anche e sempre più nell'utilizzo di risorse ICT.

Essere più sicuri per essere più competitivi

Le tecnologie informatiche intervengono, infatti, attraverso l'intera struttura di un sistema produttivo che ruota attorno a tre variabili fondamentali: le caratteristiche del prodotto, l'interazione a monte con i fornitori e quella a valle con i clienti.

I processi associati a ognuna di queste fasi 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" nonché di proteggere la proprietà brevettuale.

In questo contesto diventa evidente lo stretto legame tra sicurezza IT e competitività. Va definitivamente superata l'idea, per molti anni prevalente, che la sicurezza rappresenti un costo; se è vero che non è possibile correlare direttamente la spesa in sicurezza IT alla produzione ovvero a un ritorno dell'investimento va però valutato il costo (o il mancato ritorno) del non investimento.

Il settore manifatturiero italiano si presenta ai nuovi appuntamenti del mercato globale con una debole propensione alla sicurezza IT nonostante i rischi a cui è esposto siano molto elevati. Il mercato si trova infatti a fronteggiare una nuova generazione di attacchi, più ampia nel numero e più efficace nei risultati, guidata da organizzazioni criminali che utilizzano nuove metodologie e vettori.

Per combatterli serve un approccio strutturato e automatizzato in grado di ridurre alla fonte le possibili vulnerabilità. Trend Micro propone un approccio alla "content security" in grado di contribuire a soddisfare le nuove esigenze di protezione.

Un recente studio di Ponemon Institute (*2013 Cost of Cyber Crime Study: United States*, Ottobre 2013) condotto sulla base di un campione di 60 organizzazioni USA operanti in vari settori industriali, di cui la maggior parte multinazionali con oltre 2mila postazioni, ha stimato che il costo medio per un'organizzazione dovuto al cybercrime corrisponde a oltre 11 milioni di dollari all'anno.

Si tratta di un costo destinato a crescere con l'incremento nel numero di minacce e la contestuale maggiore efficacia degli attacchi odierni.

Infatti, predisporre i necessari meccanismi di controllo, protezione e garanzia è un compito reso sempre più difficile dall'evoluzione delle minacce e dal rinnovato scenario tecnologico caratterizzato da temi quali cloud computing, mobilità e virtualizzazione.

Sicurezza e manufacturing

Il settore manifatturiero italiano si presenta ai nuovi appuntamenti del mercato globale con una debole propensione alla sicurezza IT.

La maggior parte delle imprese manifatturiere e industriali dispone di piani di emergenza e di processi di risposta relativamente completi, ma questi spesso non sono adatti per fronteggiare in modo efficace i rischi legati alla sicurezza IT.

Per esempio, se è vero che la maggior parte delle imprese del settore manifatturiero ha predisposto strumenti efficaci per controllare e gestire i propri dipendenti, spesso relativamente poco è stato fatto in relazione ad appaltatori, fornitori, lavoratori temporanei, autisti non aziendali e altri collaboratori esterni che possono disporre di livelli di accesso e di esposizione ai rischi assimilabili a quelli dei dipendenti.

Le aziende che hanno una presenza globale, difficilmente hanno pienamente armonizzato le policy di sicurezza tra le diverse filiali sebbene, magari, queste si trovino a utilizzare la stessa base dati centralizzata. A ciò si aggiungono differenti requisiti normativi che possono anche risultare in contrasto con SLA di riservatezza contrattualizzati.

Peraltro, molte imprese industriali sono prive di un security manager dedicato la cui funzione è spesso delegata a una persona su cui ricade la responsabilità di diverse mansioni quali il servizio di prevenzione e protezione dei lavoratori, la sicurezza fisica, la gestione delle risorse umane, la manutenzione della struttura e così via.

MODELLI DI BUSINESS E MINACCE IN EVOLUZIONE

Il tema della sicurezza aziendale si arricchisce ogni giorno di nuove sfaccettature, approcci e metodologie. Protezione olistica, integrata, sistemi di prevenzione e di protezione proattiva, gestione delle identità e profilazione dei ruoli, sicurezza degli endpoint, assessment, social engineering, targeted attack, hardening sono tutti termini che fanno riferimento a tematiche di grande attualità e di cui è certamente necessario occuparsi.

Il malware è quanto mai in aumento in termini numerici e il settore manifatturiero è uno di quelli in cui l'incremento si dimostra più consistente. 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, mentre la previsione di Trend Micro che si sarebbe arrivati entro la fine del 2013 a identificare 1 milione di minacce per Android, da molti considerata eccessivamente allarmista quando venne fatta nel dicembre del 2012, è stata superata dalla realtà: a settembre 2013 questo numero è stato raggiunto, spostando le previsioni di fine anno a circa 1 milione e 200mila.

L'escalation delle minacce 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 hacker attuali 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.

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 lanciare attacchi del tipo Distributed Denial of Service: da questo punto di vista una realtà manifatturiera con una rete estesa su scala internazionale rappresenta un target molto "appetibile".

I cyber criminali non puntano solo a sottrarre i dati dell'azienda, ma attaccano anche la sua interfaccia di comunicazione verso l'esterno ovvero il sito Web, al fine di danneggiarne l'immagine o ridurre l'operatività, magari per l'azione di un concorrente che si è rivolto a un'organizzazione di cybercrime. Il numero complessivo delle pagine Web infette continua così a crescere a un ritmo di migliaia al giorno e l'Italia si posiziona ai primi posti nella lista dei Paesi che ospitano il maggior numero di siti Web infetti.

Attacchi mirati: il nuovo volto delle minacce alle imprese industriali

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 è prevalentemente quello delle organizzazioni Enterprise, delle utility, delle aziende del settore energetico o delle grandi imprese industriali. Si tratta di processi di attacco sofisticati che 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.

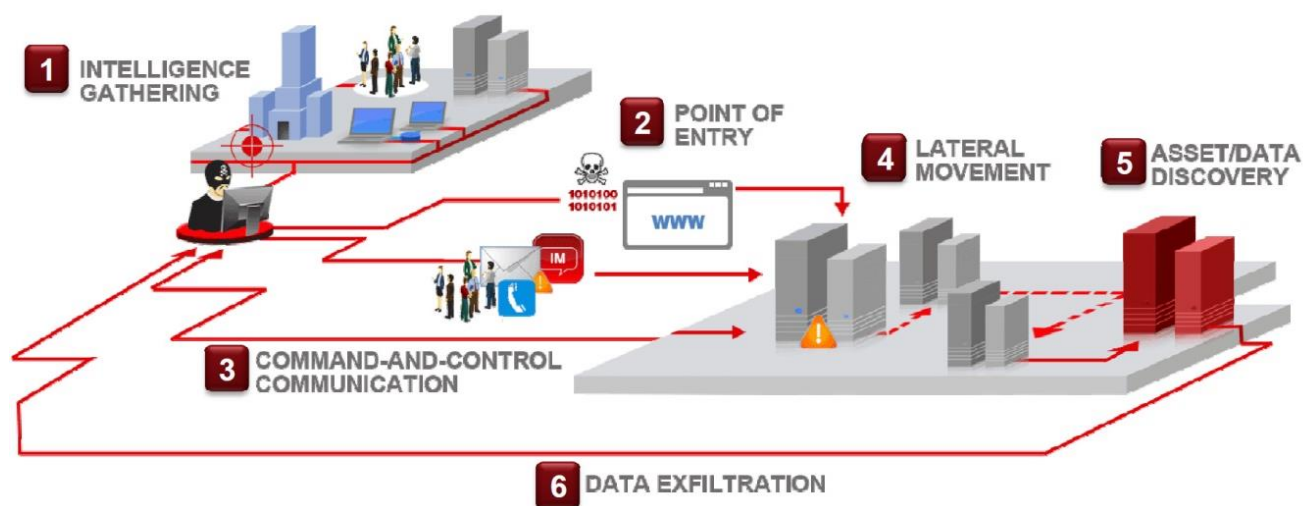
La prima fase è quella di preparazione dell'attacco, in cui viene effettuata l'investigazione e sono utilizzati semplici tool per raccogliere le informazioni sull'organizzazione target e sui soggetti indirettamente collegati a essa. Tra questi ultimi possono esserci aziende partner, collaboratori o clienti 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 la comunicazione 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.

SCADA: un rischio trascurato

I sistemi ICS (Industrial Control Systems) e le reti SCADA (Supervisory Control And Data Acquisition) sono presenti in quasi ogni settore industriale, dalla produzione di veicoli, al trasporto, dall'energia, al trattamento delle acque, fornendo agli operatori i dati per le attività di supervisione e la capacità di controllo necessaria per la gestione dei processi.

La sicurezza di sistemi ICS/SCADA resta un tema importante nel contesto della sicurezza che interessa il settore manifatturiero perché questi sistemi sono comunemente utilizzati per il funzionamento di industrie di grande rilevanza.

In ambito industriale i sistemi ICS/SCADA sono utilizzati da tempo e, mano a mano che l'automazione continua a evolversi e diventa più importante a livello mondiale, la loro diffusione e importanza cresce.

Una crescita a cui, purtroppo, fa eco una mancanza di protezione ben documentata e ampiamente conosciuta. È noto, per esempio, che attraverso Internet si possono effettuare ricerche che restituiscono facilmente l'accesso ai pannelli di controllo di sistemi SCADA, l'identificazione delle macchine e delle loro funzioni. Altri siti, come per esempio Pastebin, vengono sempre più spesso utilizzati per la diffusione di informazioni legate ai dispositivi ICS/SCADA come, per esempio, i loro indirizzi IP.

Tutto ciò ha favorito e continua a favorire le azioni del cyber crimine che, negli ultimi anni, ha segnato importanti punti a proprio favore con minacce quali Stuxnet e Flame indirizzate a questi sistemi.

In particolare, Stuxnet è considerato uno dei codici malware più sofisticati che sia mai stato scritto tanto che la sua analisi e comprensione ha richiesto molti mesi; recentemente sono stati identificati file infetti con questo malware che era presente in modo dormiente da 6 anni, in attesa di essere sfruttato per attacchi su larga scala.



Va rimarcato che i sistemi ICS/SCADA, sebbene simili nelle funzioni ai sistemi di ICT Security, differiscono notevolmente da questi ultimi nel modo di interpretare l'esigenza di sicurezza. La prima priorità dei sistemi IT di sicurezza è tipicamente la protezione dei dati mentre nei dispositivi ICS/SCADA si tende a privilegiare l'affidabilità e l'accessibilità dei dati per non compromettere la produttività.

Ogni sistema SCADA presenta poi caratteristiche specifiche in termini di requisiti di disponibilità, architettura, obiettivi e requisiti prestazionali e questo richiede che vengano trattati in modo unico.

Solitamente i sistemi SCADA non prevedono di default la presenza di soluzioni anti malware. Questo è legato sia alla loro natura intrinsecamente legacy sia perché si tratta di macchine deputate al controllo di altri strumenti per cui una qualsiasi forma di ritardo nel calcolo computazionale introdotta da un sistema di controllo potrebbe causare inconvenienti. Per questa ragione solitamente il controllo dei sistemi SCADA viene effettuato a livello di singola macchina in modalità batch e, in molti casi, non è neppure possibile effettuare controlli in rete.

Un altro problema di cui le aziende solitamente non si preoccupano è che le macchine SCADA sono gestite e mantenute da terze parti. Pertanto, se non si ha la possibilità di esercitare un'azione di controllo sui processi di queste terze parti o se non si mette a loro disposizione un sistema per effettuare un controllo in linea della macchina, il rischio di introdurre malware su uno di questi dispositivi diventa elevato.

Per favorire la protezione dei sistemi SCADA è opportuno che un'azienda del settore manifatturiero si doti di strumenti automatizzati in grado di intervenire in modo integrato su più fronti per effettuare azioni quali:

- controllo dell'accesso alle risorse aziendali,
- aggiornamento e monitoraggio costante delle patch;
- scansione di rete e protezione anti malware in tempo reale
- predisporre regole di accesso che prevedano nome utente/password anche per i sistemi ritenuti "affidabili";
- impostare credenziali di accesso sicure senza basarsi su valori predefiniti;
- implementare autenticazione forte a due fattori sui sistemi critici;
- disabilitare protocolli remoti insicuri;
- disattivare tutti i protocolli che comunicano in entrata alle risorse considerate "affidabili" che non siano fondamentali per la funzionalità di business;
- utilizzare segmentazione di rete;
- sviluppare un sistema di modellazione delle minacce per la propria organizzazione.

Correlare i Big Data della sicurezza

L'analisi effettuata delinea uno scenario preoccupante e mette in evidenza alcuni requisiti che dovrebbero caratterizzare una piattaforma di sicurezza ICT a supporto di una strategia efficace di protezione in ambito manifatturiero.

Il primo punto è che, innanzitutto, è necessario affrontare in maniera unificata i rischi associati a tutti i processi aziendali. 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'azienda 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.

Peraltro la maggior parte delle aziende, attualmente, non è interessata o non dispone delle risorse necessarie per conservare i dati della sicurezza per poter effettuare analisi e previsioni utili a sviluppare modelli di protezione. 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.

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.

L'APPROCCIO ALLA SICUREZZA DI TREND MICRO

Trend Micro si propone di rispondere a questi requisiti 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.

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).

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.

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.

∞

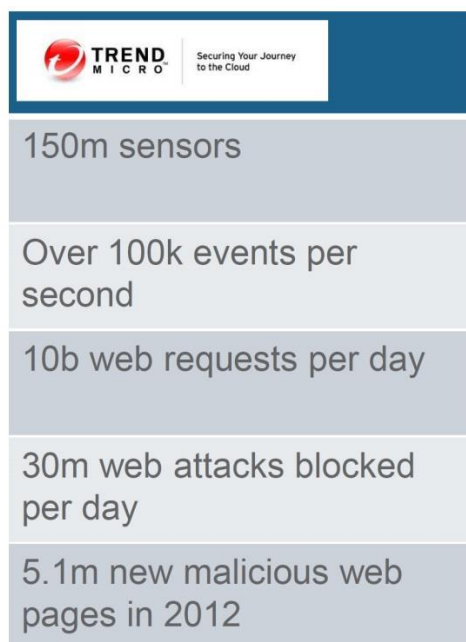
Trend Micro Smart Protection Network sfrutta un approccio di difesa intelligente basato sulle conoscenze collettive ottenute dall'ampio e globale bacino dei clienti Trend Micro, mettendo in relazione i dati provenienti da oltre 70 miliardi di query giornaliere.

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

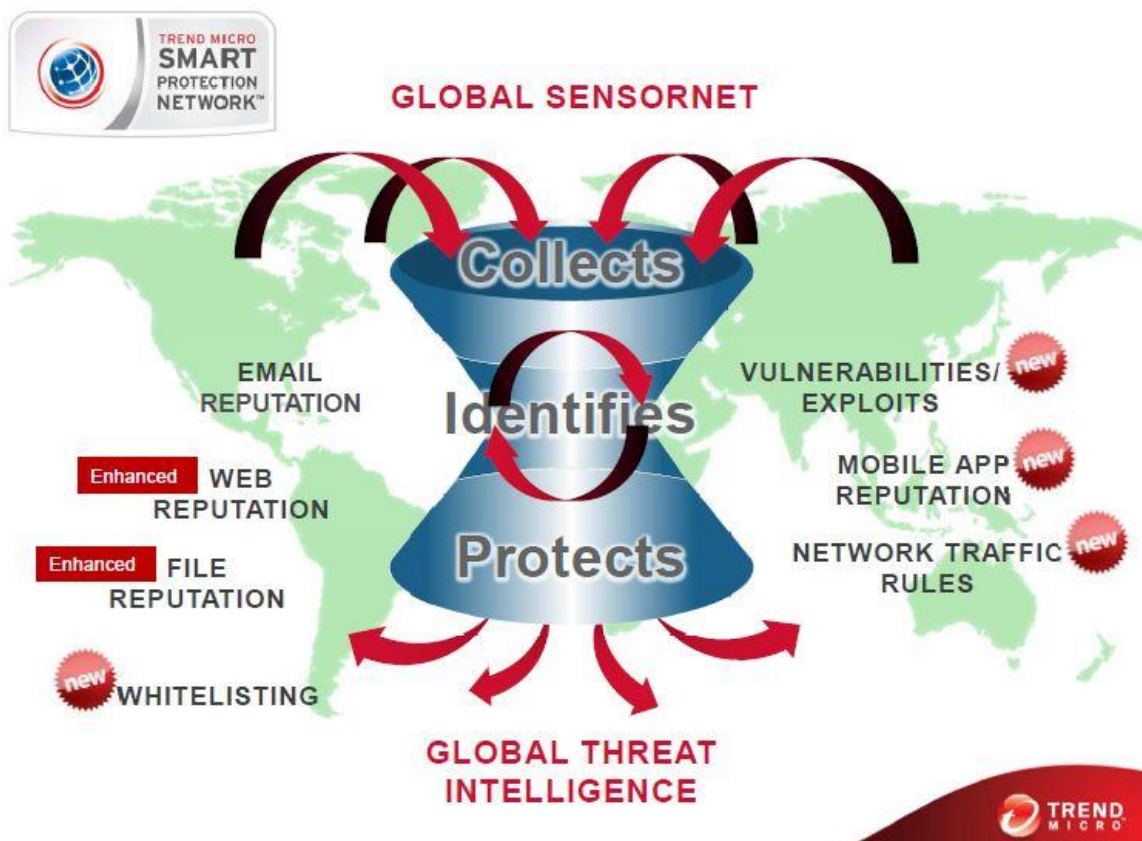
La tecnologia di reputazione Web di Trend Micro rileva la credibilità dei domini Web tramite l'assegnazione di un punteggio basato su fattori quali l'età del sito Web, le modifiche cronologiche all'ubicazione del sito e le indicazioni di attività sospette scoperte tramite l'analisi del comportamento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

Un approccio originale per la protezione dei sistemi SCADA

Questi strumenti e tecnologie possono essere utilizzati anche per proteggere gli ambienti SCADA aggirando l'ostacolo della difficoltà di effettuare controlli diretti, puntando sull'analisi di anomalie nel traffico di rete che caratterizzano i sistemi correlati alla macchina SCADA.

Un'altra soluzione è rappresentata dai sistemi di Application Control che, una volta installati su macchine SCADA, chiedono all'amministratore di selezionare le applicazioni che possono girare, evitando l'installazione non solo di applicazioni potenzialmente nocive, ma anche di quelle inutili.

Tra le soluzioni sviluppate da Trend Micro figura anche Portable Security; si tratta di una soluzione ospitata su una chiavetta USB che, all'atto dell'inserimento su macchine SCADA con sistema Windows embedded, effettua automaticamente una scansione certificando la macchina prima di metterla nuovamente in linea.

LE SOLUZIONI PER LA DATA PROTECTION

Per rispondere alle sfide della Data Protection 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.

Trend Micro Deep Discovery per rilevare gli attacchi mirati e persistenti

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.

CONCLUSIONI

Il numero delle minacce cresce a ritmi vertiginosi e, nel contempo, cambia la loro natura che 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.

Il settore manifatturiero, uno degli assi portanti dell'economia del nostro Paese, si trova particolarmente esposto a questi attacchi. I rischi sono molteplici e spaziano dalla sottrazione di proprietà intellettuale, al sabotaggio, alla compromissione di sistemi per sferrare altri attacchi.

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.

Una sicurezza trascurata espone a costi estremamente ingenti, che nelle realtà enterprise sono stimabili in diversi milioni di euro ma che in alcuni casi può anche rappresentare la definitiva uscita dal mercato.

In uno scenario di minacce così diversificato, un approccio alla sicurezza IT concentrato unicamente sulla difesa del perimetro aziendale, peraltro sempre più evanescente, e su aspetti singoli risulta inefficace.

Va predisposto un modello di sicurezza strategico, pervasivo, integrato, personalizzato e, preferibilmente, in grado di automatizzare il più possibile le operazioni e di 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 manifatturiero 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**.*

Reportec

La sicurezza ICT nel settore manifatturiero. Soluzioni per aumentare il vantaggio competitivo

© Reportec S.r.l. - Ottobre 2013 - 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.