



LA SICUREZZA ICT NELLA PUBBLICA AMMINISTRAZIONE

UNA CRITICITÀ CHE NON SI PUÒ PIÙ PROCRASTINARE

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

SOMMARIO

Verso una PA digitale	2
Il Codice dell'Amministrazione Digitale (CAD)	3
Sicurezza Outside-in e Inside-out	6
L'Agenda Digitale Italiana (ADI)	7
L'evoluzione delle minacce	9
Gli attacchi alla PA	9
Attacchi mirati: il nuovo volto delle minacce	10
L'approccio alla sicurezza di Trend Micro	12
La Smart Protection Network	13
Uno strumento per l'analisi di reputazione e comportamento	14
L'importanza di correlare gli eventi di sicurezza	15
Le soluzioni per la Data Protection	16
Trend Micro Deep Security per gli ambienti virtualizzati	16
Trend Micro Deep Discovery per rilevare gli attacchi mirati	17
Trend Micro OfficeScan per la sicurezza dei terminali	17
Conclusioni	18

LA SICUREZZA ICT NELLA PUBBLICA AMMINISTRAZIONE

UNA CRITICITÀ CHE NON SI PUÒ PIÙ PROCRASTINARE

VERSO UNA PA DIGITALE

Il rapporto tra informatizzazione e Pubblica Amministrazione in Italia è finora stato piuttosto travagliato.

Una delle critiche che più spesso si sente indirizzare verso la struttura amministrativa del nostro Paese è, infatti, l'eccessivo carico burocratico che permea ogni aspetto della vita comune e aziendale. Il ritardo tecnologico che grava sulla nostra Pubblica Amministrazione non consente, tuttavia, di predisporre l'introduzione di un livello di automazione in grado di favorire e accelerare i processi. Certamente negli ultimi anni si sono fatti notevoli passi in avanti in questa direzione, ma lo scenario d'adozione tecnologica appare ancora a macchia di leopardo e, in ogni caso, di livello ancora insufficiente se correlato all'importanza strategica della macchina amministrativa dello Stato.

Se dovessimo guardare alla PA in un'ottica aziendale, si potrebbe riconoscere un livello di complessità e un carico di criticità non inferiore a quello che può affliggere una grossa realtà enterprise o finanziaria che opera su larga scala con uffici distribuiti.

I "clienti" della PA sono infatti i milioni di cittadini italiani da cui l'amministrazione pubblica riceve informazioni e a cui deve fornire servizi.

Il numero di dati e di documenti che vengono raccolti, prodotti e archiviati dalle Pubbliche Amministrazioni nell'esercizio della propria attività istituzionale è impressionante e questi devono essere costantemente aggiornati e resi più precisi possibili, devono essere trasmessi tra diversi uffici mantenendo il riservo delle informazioni e preoccupandosi che non ci siano intrusioni esterne non autorizzate, devono essere custoditi e archiviati per lungo tempo e resi accessibili ogni volta che serve.

La Pubblica Amministrazione rappresenta uno dei settori più critici per il volume e l'importanza del patrimonio informativo che detiene e dei servizi che eroga. L'esigenza di sicurezza IT è stata recepita dalle nuove normative che risultano però ancora incomplete. Nel frattempo le amministrazioni centrali e locali non possono esimersi dal dovere di predisporre misure di protezione adeguate, anche perché gli attacchi indirizzati verso la PA crescono in numero e migliorano in efficacia.

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.

Il patrimonio informativo raccolto dalla Pubblica Amministrazione deve essere tutelato per una serie di finalità evidentemente irrinunciabili quali:

- mantenere l'integrità e quindi l'affidabilità delle informazioni pubbliche;
- impedire la diffusione non autorizzata di informazioni (qualcuno si ricorderà cosa accadde quando l'ufficio delle entrate decise di rendere accessibili su Internet le dichiarazioni dei redditi degli italiani);
- assicurare la continuità operativa (inclusa quella dei servizi online) per abilitare un corretto funzionamento dell'apparato burocratico;
- garantire la riservatezza di informazioni critiche, per esempio di carattere sanitario che potrebbero avere effetto su assicurazioni e contratti di lavoro;
- mantenere accessibili nel tempo le informazioni preoccupandosi di adeguarsi all'evoluzione degli standard dei dispositivi hardware e dei sistemi operativi.

Conseguire tali obiettivi richiede una pluralità di azioni sul piano delle tecnologie e soluzioni IT per predisporre:

- misure preventive per impedire intrusioni e attacchi in grado di nuocere al patrimonio informativo o all'operatività, inclusa la capacità di fronteggiare minacce quali i DDoS che sovraccaricano i server inibendone l'uso e bloccando i servizi;
- processi di "remediation" per limitare i danni in caso attacchi andati a buon fine;
- sistemi di cifratura delle informazioni e delle comunicazioni;
- modelli di certificazione e firma digitale;
- meccanismi di controllo dell'accesso e dell'identità;
- politiche di ripristino e di disaster recovery perché lo stato deve funzionare soprattutto in condizioni di emergenza;
- politiche di archiviazione sicura e di data retention a lungo termine che prevedano percorsi di migrazione sui media di archiviazione.

Tutto ciò va affrontato all'interno delle PA preoccupandosi di mantenere piena conformità a un imponente castello di normative e regole di carattere nazionale, regionale e comunale.

Insomma, se esiste un'organizzazione critica in cui la sicurezza in tutte le sue forme è imprescindibile più che per ogni altro settore questa è, o perlomeno dovrebbe essere, la Pubblica Amministrazione.

Il Codice dell'Amministrazione Digitale (CAD)

L'introduzione all'interno della PA di strumenti IT in generale e di soluzioni di sicurezza informatica in particolare, è stato caratterizzato negli anni da una serie di approcci diversificati solitamente perseguiti sulla base di iniziative autonome sia nelle scelte tecnologiche sia nelle modalità d'implementazione delle stesse. Le diverse amministrazioni e, a volte, persino i dipartimenti all'interno di uno stesso Ente, hanno privilegiato una propria risposta all'esigenza di sicurezza dando origine a una sovrapposizione di soluzioni prive di un unico disegno progettuale e difficilmente in grado di rispondere ai necessari requisiti di robustezza e affidabilità.

Un passo importante verso l'innovazione della PA è giunto con il Codice dell'Amministrazione Digitale (CAD) emanato come Decreto Legislativo n. 82 il 7 marzo del 2005. Il CAD ha ordinato e unificato molte norme già esistenti e ne ha introdotte alcune per abilitare nuovi servizi e opportunità al fine di creare un quadro legislativo in grado di dare validità giuridica alle innovazioni informatiche.

Questa normativa prevede che i dati della PA debbano essere resi disponibili in modalità digitale e questo implica che tali dati debbano essere formati, acquisiti e conservati all'interno dei sistemi informatici delle amministrazioni titolari.

Il CAD affronta aspetti quali la sicurezza logica, dell'infrastruttura, dei servizi dell'organizzazione, la riservatezza dei dati, la gestione documentale sicura e la sicurezza dei flussi della gestione documentale.

L'approccio adottato dal legislatore italiano è stato di rendere obbligatorio per Legge il processo d'innovazione all'interno della PA intervenendo, da una parte per fornire ai cittadini il diritto di interagire sempre, dovunque e verso qualsiasi amministrazione attraverso Internet, posta elettronica, reti e, dall'altra, stabilendo che tutte le amministrazioni (centrale, regionale e le autonomie locali) debbano organizzarsi in modo da assicurare la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale utilizzando le modalità più appropriate offerte dalle tecnologie ICT.

*Capo I - Principi generali, Sezione II - Diritti dei cittadini e delle imprese
Art.3. Comma 1. I cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni, con i soggetti di cui all' articolo 2, comma 2, e con i gestori di pubblici servizi ai sensi di quanto previsto dal presente codice.*

L'idea stessa di una Pubblica Amministrazione presuppone implicitamente che i sistemi su cui sono custoditi dati e informazioni siano sicuri. In particolare, in relazione alle Norme generali per l'uso delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa viene premesso nei Principi generali che guidano il CAD che:

Capo I, Sezione III, Art.12, comma 2. Le pubbliche amministrazioni adottano le tecnologie dell'informazione e della comunicazione nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati, con misure informatiche, tecnologiche, e procedurali di sicurezza, secondo le regole tecniche di cui all' articolo 71 .

La sicurezza dei dati diventa quindi un principio generale, tradotto in un requisito normativo che interviene sia all'interno della macchina amministrativa nelle sue differenti declinazioni territoriali e di competenza sia nell'interazione tra questa e i cittadini.

Il passaggio fondamentale è che le procedure indirizzate alla sicurezza non rappresentano solo un requisito da soddisfare per fornire un servizio migliore e più affidabile, ma un vincolo di legge che deve essere predisposto e rispettato secondo modalità specifiche e ben definite.

In attesa dei decreti attuativi per le norme tecniche

Un passaggio fondamentale del CAD relativo alla sicurezza IT è contenuto all'interno dell'art. 51 (Capo V,- Sezione I) del D. Lgs. n. 82/2005 così come modificato dal D. Lgs. n. 235/2010) relativo alla *Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni* è previsto che:

Capo V, Sezione I, Art. 51, comma 1. Con le regole tecniche adottate ai sensi dell'art. 71 sono individuate le modalità che garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture.

Capo V, Sezione I, Art. 51, comma 2. I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta.

I buoni propositi della normativa si sono però dovuti scontrare con un malcostume tipicamente italiano che ne impedisce l'attuazione, mettendo così a rischio la sicurezza informatica all'interno delle PA. A ottobre 2013, infatti, non è stato ancora emanato il decreto attuativo sulle norme tecniche inibendo, di fatto, la possibilità di predisporre una metodologia unitaria e coerente per la sicurezza ICT all'interno della Pubblica Amministrazione.

L'atteggiamento degli Enti, in una situazione di difficile congiuntura economica come quella attuale, può portare a procrastinare il compito di predisporre una sicurezza IT efficace fino all'arrivo delle regole tecniche. In realtà, una conferma di questo atteggiamento giunge dal Rapporto "La strategia e le azioni AgID per la sicurezza informatica delle PA" redatto dall'Agenzia per l'Italia Digitale (organo della Presidenza del Consiglio dei Ministri) e pubblicato il 10 luglio 2013 che riporta i risultati di un questionario sottoposto alle Amministrazioni Centrali.

Dal Rapporto si evidenzia che in meno della metà delle amministrazioni interpellate esiste una previsione di spesa dedicata specificatamente alla sicurezza informatica e che solo il 56% ha formalmente definito e approvato il piano della sicurezza informatica. Dati che plausibilmente diventano peggiorativi nella PA di tipo locale, generalmente più carente di risorse e competenze.

		SI	NO	Note
1	Esiste un responsabile della sicurezza informatica?	78%	22%	
2	E' stato formalmente definito ed approvato il piano della sicurezza informatica?	56%	44%	
3	Esiste un nucleo di riferimento per la sicurezza informatica?	89%	11%	
4	Esiste un gruppo di gestione degli incidenti informatici?	82% (*)	18%	(*) 52% no formale
5	E' stata istituita l'ULS dell'Amministrazione?	78%	22%	
6	Modalità di colloquio della ULS con il provider SPC	27%	73%	
7	Sono raccolte statistiche sulla sicurezza informatica?	73%	27%	
8	Se esistono contratti di outsourcing, i contratti prevedono verifiche dell'Amministrazione sulla gestione della sicurezza informatica?	74%	26%	
9	Esiste una previsione di spesa dedicata specificatamente alla sicurezza informatica?	48%	52%	
10	Sono state prese iniziative per informazione/formazione sulla sicurezza informatica rivolte al personale dell'Amministrazione ?	78%	22%	

Atteggiamento delle amministrazioni centrali italiane in merito alla sicurezza IT (Fonte: AgID)

In uno scenario di questo tipo va ostacolato il convincimento che, in assenza dell'arrivo delle regole tecniche, evitare di predisporre misure di protezione non implichi conseguenze. Questo perché deve essere modificato il paradigma in base al quale la sicurezza informatica costituisca un problema riconoscendo, invece, a questo tema, la sua natura di strumento necessario con cui tutelare il patrimonio informativo pubblico, la produttività degli operatori e rafforzare la fiducia dei cittadini nei confronti degli Enti governativi.

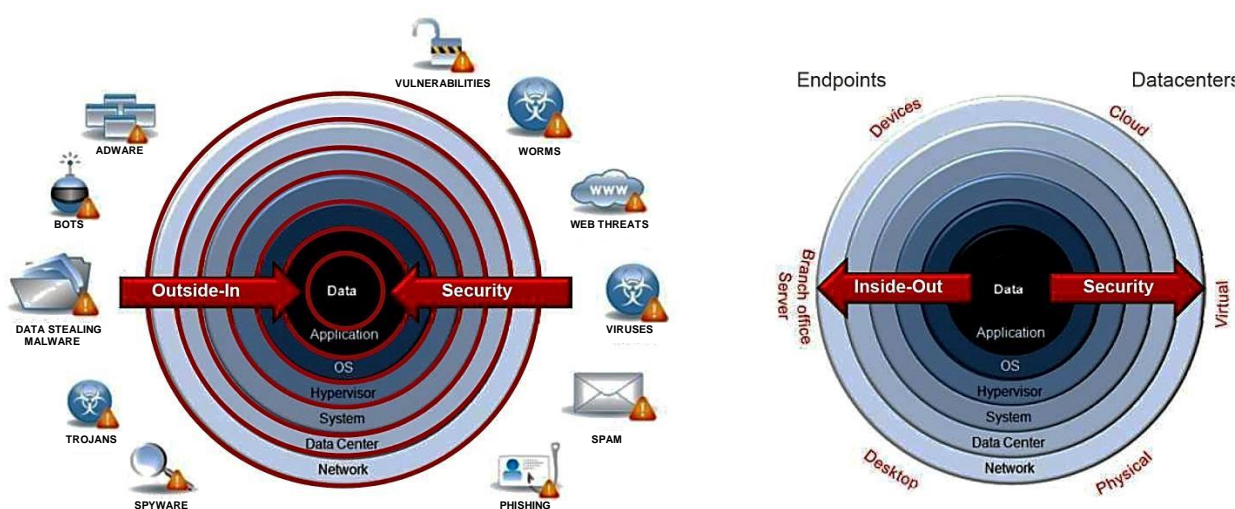
All'immobilismo della PA, infatti, non corrisponde quello del cyber crime che, anzi, diventa ogni giorno più attivo e sceglie sempre più spesso come target dei suoi attacchi le organizzazioni governative.

Sicurezza Outside-in e Inside-out

Le indicazioni fornite dal CAD forniscono indirizzi tecnologici precisi per predisporre condizioni di sicurezza che riducano al minimo i possibili rischi, ma sottintendono trasversalmente un approccio indirizzato in modo prevalente verso un modello di protezione del tipo outside-in, ovvero a una protezione essenzialmente perimetrale per allontanare le minacce il più possibile.

Tuttavia, l'esperienza mostra che una fonte molto rilevante di problemi per la sicurezza e la vulnerabilità di un'organizzazione giunge dal suo interno, a causa di incapacità, incuria, negligenza e anche per azioni nocive volontarie che possono avere svariate motivazioni. Tutto ciò è avvenuto e continua ad accadere anche nell'ambito della PA.

Per questo motivo a una protezione outside-in andrebbe sempre affiancata una sicurezza di tipo inside-out affrontata su molteplici versanti e tenendo conto degli aspetti legati al comportamento delle persone oltre che a quelli di tipo tecnologico.



Schematizzazione dei modelli di sicurezza outside-in e inside-out (Fonte: Trend Micro)

Soprattutto, per fronteggiare le vulnerabilità dovute a incuria o negligenza è fondamentale predisporre una cultura della sicurezza che si basi innanzitutto sulla conoscenza dei rischi e delle nuove modalità di attacco.

In effetti il CAD riconosce l'importanza della formazione prevedendo che:

Capo I, Sez. III, Art.13, comma 1. Le pubbliche amministrazioni nella predisposizione dei piani di cui all'articolo 7-bis, del decreto legislativo 30 marzo 2001, n. 165, e nell'ambito delle risorse finanziarie previste dai piani medesimi, attuano anche politiche di formazione del personale finalizzate alla conoscenza e all'uso delle tecnologie dell'informazione e della comunicazione, nonché dei temi relativi all'accessibilità e alle tecnologie assistive, ai sensi dell'articolo 8 della legge 9 gennaio 2004, n. 4

Tuttavia non vengono definite in modo preciso le modalità con cui realizzare la formazione e, in ogni caso, le risorse economiche della macchina statale appaiono insufficienti a garantire un efficace e capillare livello di formazione su un tema come quello della sicurezza tra i più dinamici e in rapida evoluzione.

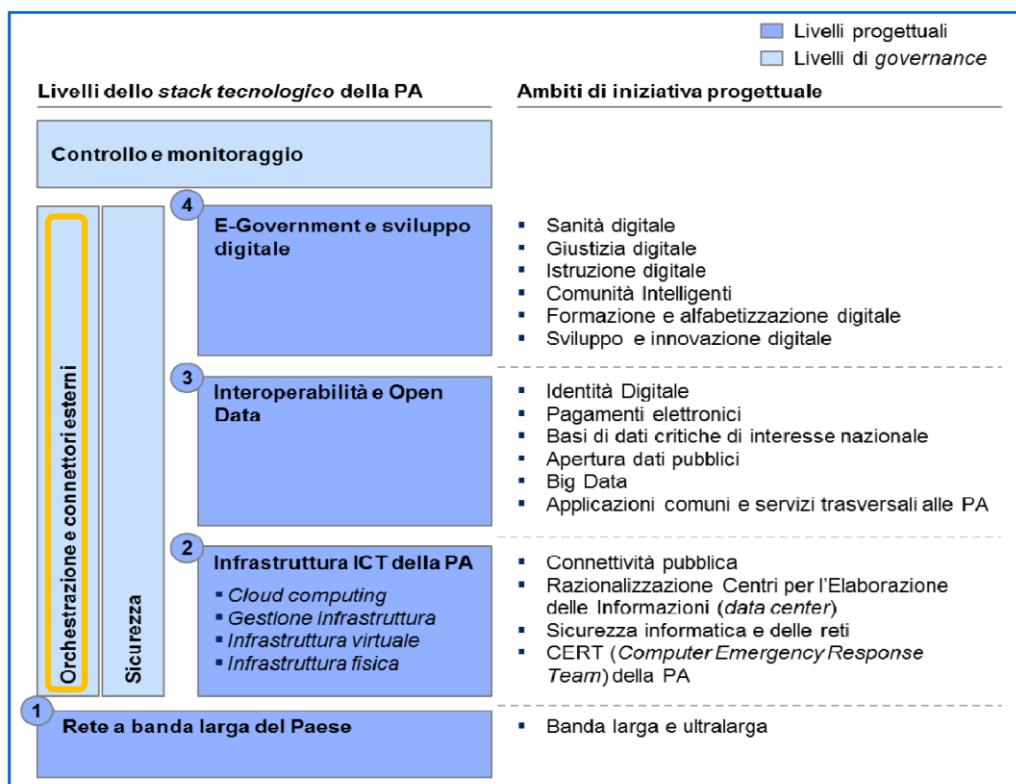
L'Agenda Digitale Italiana (ADI)

Un ulteriore passo in avanti verso l'introduzione degli strumenti digitali e la sicurezza informatica nella PA si è avuto con l'Agenda Digitale Italiana (ADI), istituita il primo marzo 2012 con decreto del Ministro dello sviluppo economico.

Le finalità dell'ADI sono di predisporre una serie di interventi nei settori: identità digitale, PA digitale/Open data, istruzione digitale, sanità digitale, divario digitale, pagamenti elettronici e giustizia digitale. All'Agenzia per l'Italia digitale (AGiD) è delegato il compito di dettare raccomandazioni, strategie, norme tecniche per perseguire gli obiettivi definiti dall'Agenda Digitale Italiana e di predisporre un'opera di monitoraggio sull'attuazione dei piani di ICT delle Pubbliche Amministrazioni.

All'interno dell'Agenda Digitale il tema della sicurezza si conferma prioritario per garantire l'integrità delle comunicazioni digitali, delle transazioni finanziarie e della trasmissione dati.

È soprattutto importante osservare come nei programmi dell'Agenda Digitale la sicurezza si collochi all'interno dello stack tecnologico per la Pubblica Amministrazione come un elemento infrastrutturale e di Governance unitaria, trasversale a tutti i livelli.



Modello per l'attuazione delle strategie per l'Agenda Digitale (Fonte AgID)

L'organo operativo dell'ADI è strutturato in sei gruppi di lavoro a cui corrispondono sei assi strategici tra cui quello dedicato a Infrastruttura e sicurezza che opera per il conseguimento dei seguenti obiettivi:

1. Assicurare la copertura a banda larga di base per tutti, completando il Piano Nazionale Banda Larga.
2. Definire una serie di provvedimenti normativi volti ad accelerare lo sviluppo di reti a banda larga e ultralarga.

3. Assicurare entro il 2020 la copertura con banda larga pari o superiore a 30 Mbps per il 100% dei cittadini UE, attuando il Progetto Strategico per la Banda Ultralarga.
4. Stimolare l'uso di reti a banda larga, incrementando il numero di abbonamenti al servizio di connettività, rispettando così entro il 2020 l'obiettivo europeo di avere il 50% degli utenti domestici europei abbonato a servizi con velocità superiore a 100 Mbps.
5. Gestione in modalità cloud computing dei contenuti e servizi della PA, mediante la realizzazione dei data center federati.
6. Assicurare la protezione dei dati di valore strategico e la relativa gestione del disaster recovery mediante i data center di prossima realizzazione.
7. Incremento dell'alfabetizzazione delle imprese, mediante l'attuazione del Progetto Strategico Data Center.
8. Definire politiche di rafforzamento della sicurezza delle reti, volte alla lotta agli attacchi cibernetici, mediante la costituzione di un CERT (Computer Emergency Response Team).

Questi obiettivi strategici recepiscono e si allineano alle indicazioni dell'Agenda Digitale Europea, organizzata a sua volta in sette punti fondamentali (pillar) di cui uno è dedicato al tema "Trust and security". Questo punto prevede una serie di azioni tra cui: combattere i cyber attack contro i sistemi critici (Action 29), creare reti di CERT (Action 38), adattare piattaforme nazionali di allerta per combattere i cyber attack anche intra confini (Action 41).

Principali norme in materia di sicurezza IT

Codice in materia di protezione dei dati personali L n. 196/2003

L'Allegato B) costituisce il disciplinare tecnico relativo alle misure minime di sicurezza

art. 51 del CAD. Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche Amministrazioni

Con le regole tecniche adottate ai sensi dell'articolo 71 (in attesa di definizione) individua le modalità che garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture

Art. 21 DPCM regole tecniche SPC (1 aprile 2008)

L'architettura di sicurezza del SPC è volta a consentire:

- lo sviluppo del SPC come dominio affidabile (trusted), costituito da una federazione
- di domini di sicurezza in cui diversi soggetti si impegnano reciprocamente ad adottare le misure minime definite nell'ambito del SPC, atte a garantire i livelli di sicurezza necessari all'intero sistema;

La Commissione SPC, sulla base dell'analisi dei rischi cui sono soggetti il patrimonio informativo e i dati della pubblica amministrazione, emana le linee guida riguardanti le misure di sicurezza e gli standard da adottare

Art. 20, comma 3, lett b) DL 83/2012

Attribuisce all'Agenzia per l'Italia Digitale (AgID) il compito di dettare indirizzi, regole tecniche e linee guida in materia di sicurezza informatica, ...

Decreto crescita 2.0: DL 18 ottobre 2012 n. 179 convertito nella legge 17 dicembre 2012 n. 221 Art. 33-septies, comma 1, Consolidamento e razionalizzazione dei siti e delle infrastrutture digitali del Paese.

L'AgID effettua il censimento dei CED della pubblica amministrazione ed elabora le linee guida finalizzate alla definizione di un piano triennale di razionalizzazione dei CED delle amministrazioni pubbliche che dovrà portare alla diffusione di standard comuni di interoperabilità, a crescenti livelli di efficienza, di sicurezza e di rapidità nell'erogazione dei servizi ai cittadini e alle imprese.

DPCM 24 gennaio 2013 GU n.66 del 19-3-2013 recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale

Prevede l'interazione con le corrispondenti autorità dell'Unione europea e della NATO e definisce un'architettura su tre distinti livelli d'intervento: di indirizzo politico e coordinamento strategico, di supporto permanente e di gestione delle crisi.

∞

L'EVOLUZIONE DELLE MINACCE

Il malware è quanto mai in aumento in termini numerici. 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.

Sul mercato clandestino online esiste un prezzo di listino associabile a ogni dato personale raccolto e consegnato nelle mani del cyber crime; un valore che aumenta al crescere del numero e della tipologia di informazioni associate al medesimo soggetto.

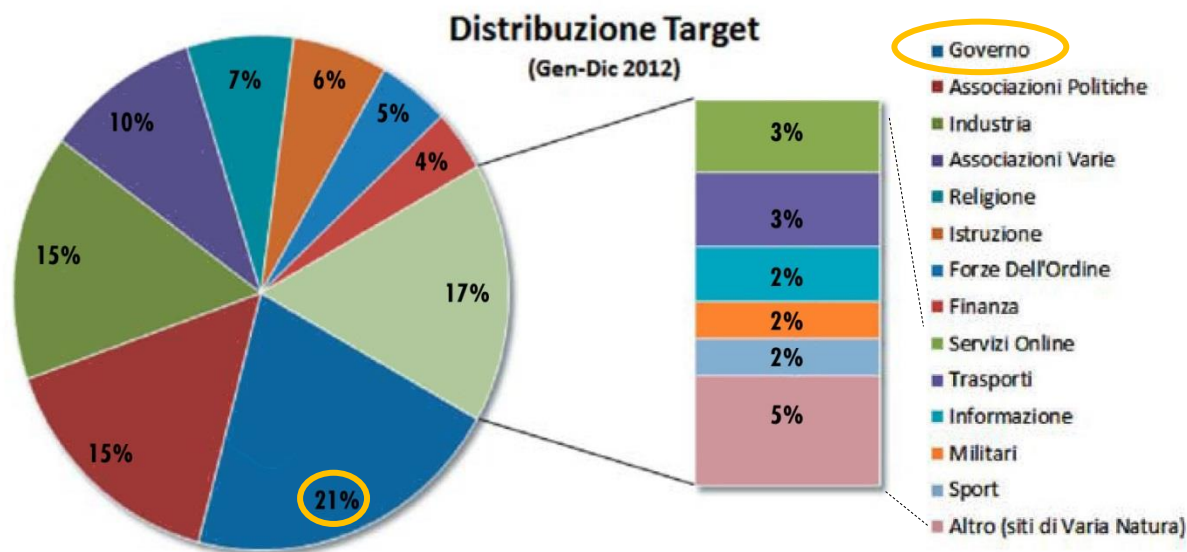
La PA rappresenta certamente un target "a valore" per il cyber crimine poiché gestisce un enorme volume di dati e poiché, purtroppo, è poco complicato trovare un anello debole nella catena della sicurezza.

Gli attacchi alla PA

Il numero e la gravità degli attacchi informatici che ha avuto come destinatari Pubbliche Amministrazioni o Enti pubblici nel nostro Paese è cresciuto vertiginosamente.

Il Rapporto 2103 sulla sicurezza ICT italiana redatto da Clusit, l'Associazione italiana per la sicurezza informatica, ha evidenziato come anche nel nostro Paese, in linea con i trend internazionali, il numero di attacchi indirizzati verso Enti governativi sia in forte aumento e rappresenti una percentuale rilevante di quelli totali. Il Clusit stima che il 21% degli attacchi totali perpetrati in Italia nel 2012 si sia indirizzato in modo specifico contro Enti governativi.

Le tipologie di attacco che la PA si trova a dover fronteggiare comprendono tutte le tecniche e i vettori di diffusione attualmente noti. In aggiunta agli attacchi "tipici" che interessano il mondo aziendale quali la diffusione di malware, il furto di credenziali per impersonare un soggetto o un'organizzazione, il Distributed Denial of Service, l'oscuramento di siti per danneggiare l'immagine dello Stato rispetto all'opinione pubblica o inibirne l'operatività, la PA si trova a dover affrontare anche minacce molto serie legate ai fenomeni di cyber terrorismo e messe in atto con i metodi più innovativi come quelli che vengono generalmente indicati con il termine APT, acronimo per Advanced Persistent Threat o come Targeted Attack.



Target degli attacchi IT in Italia nel 2012 (Fonte: Clusit)

I rischi sono elevatissimi e riguardano sia le Informazioni gestite dalla PA, che possono essere sottratte, modificate o cancellate, sia i servizi che possono essere interrotti o alterati. L'indisponibilità dei servizi, l'inaffidabilità dei registri, la distruzione di documenti o la diffusione di informazioni riservate genera non soltanto danni d'immagine, ma anche di tipo economico legati ad aspetti quali, per esempio, le spese di ripristino o del contenzioso legale.

In aggiunta a tutto ciò, si deve tenere conto anche dell'impatto che potrebbe avere l'alterazione dei livelli autoritativi e delle autorizzazioni legati alla Pubblica Amministrazione (si pensi a regolamenti edilizi, concessioni, bandi di gara, forniture) o la compromissione di sistemi di controllo legati all'erogazione di servizi di pubblica utilità in carico alla PA (per esempio si pensi all'impatto che potrebbe avere un intervento malevolo in grado di modificare una stazione di controllo della pressione dell'acqua di un acquedotto pubblico).

Attacchi mirati: il nuovo volto delle minacce

Gli attacchi mirati (Targeted Attack) 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 governative, delle realtà 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 "Targeted Attack" è un processo di attacco che segue regole precise e determinate e che è stato studiato e definito tanto da poter essere ricondotto a cinque 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.

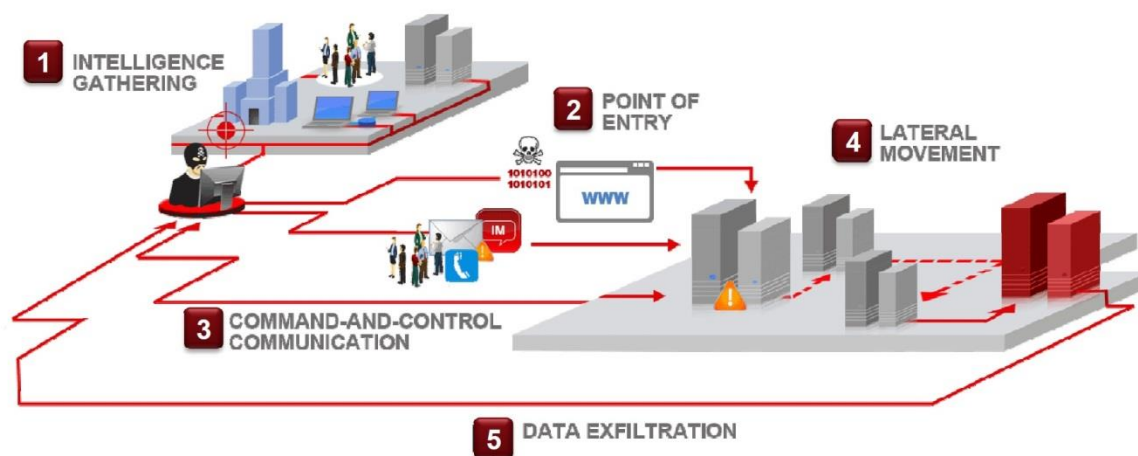
Tra questi ultimi possono esserci aziende partner, collaboratori o clienti dell'organizzazione sotto attacco, spesso aggirati con l'uso di tecniche di social engineering al fine di ottenere informazioni che, separatamente, possono sembrare poco rilevanti ma che, se correlate tra loro, possono fornire 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.

La fase 4 è quella che si potrebbe definire dei "lateral movement" durante la quale l'attaccante espande la propria presenza e il controllo all'interno della rete. Partendo da un sistema compromesso, l'attaccante comincia a spostarsi all'interno della rete raccogliendo informazioni sulle vulnerabilità dei server, gli hot-fix installati o la tipologia di comunicazione utilizzata e cercando di ottenere un accesso di livello superiore alle altre risorse di rete.

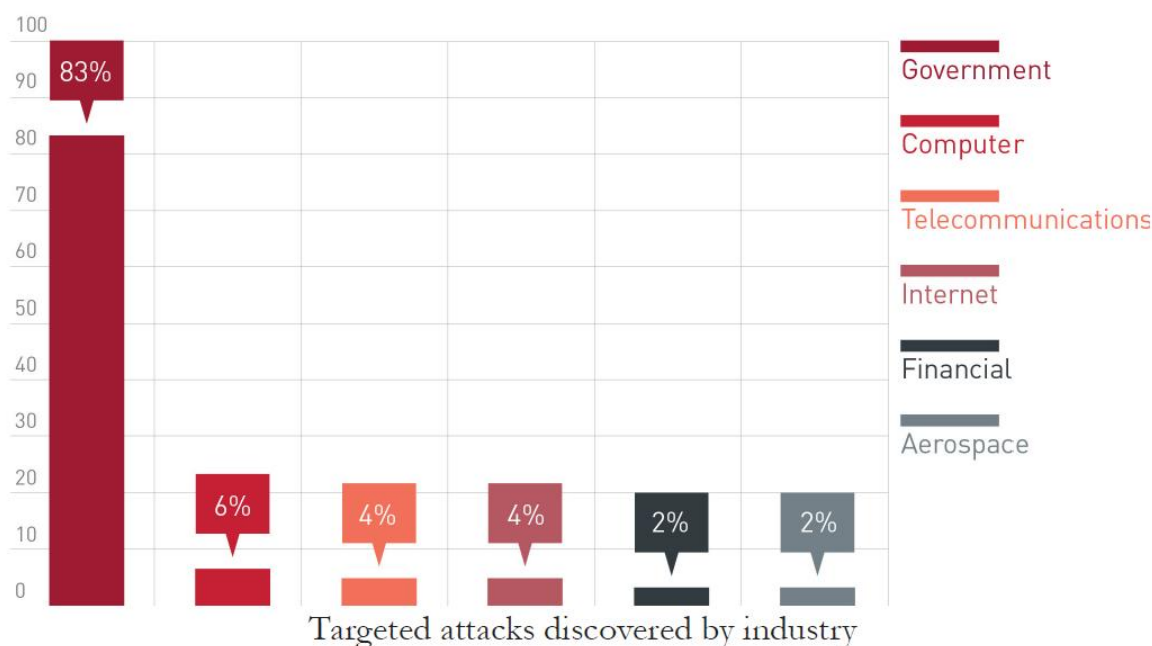
La quinta e ultima fase è quella in cui avviene l'effettiva sottrazione dei dati; attraverso una backdoor l'attaccante scarica una copia delle informazioni lasciando inalterato il dato originale in modo da mantenere nascosta la sua presenza e potere ripetere costantemente l'attacco.



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.

L'importanza di questi attacchi sta crescendo rapidamente e Trend Micro ha deciso di avviare una serie di Report periodici per monitorarli. Nel report relativo al secondo trimestre del 2013, il vendor giapponese ha evidenziato come principale target a livello mondiale degli attacchi mirati proprio le organizzazioni governative a cui si indirizza oltre l'80% del numero complessivo di questi attacchi.



Principali obiettivi degli attacchi mirati
(Fonte: Trend Micro 2Q Report on Targeted Attack Campaigns)

L'APPROCCIO ALLA SICUREZZA DI TREND MICRO

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 all'interno della PA.

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.

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 un'offerta altamente integrata di prodotti, servizi e soluzioni per la sicurezza dei contenuti.

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 (APT) 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.

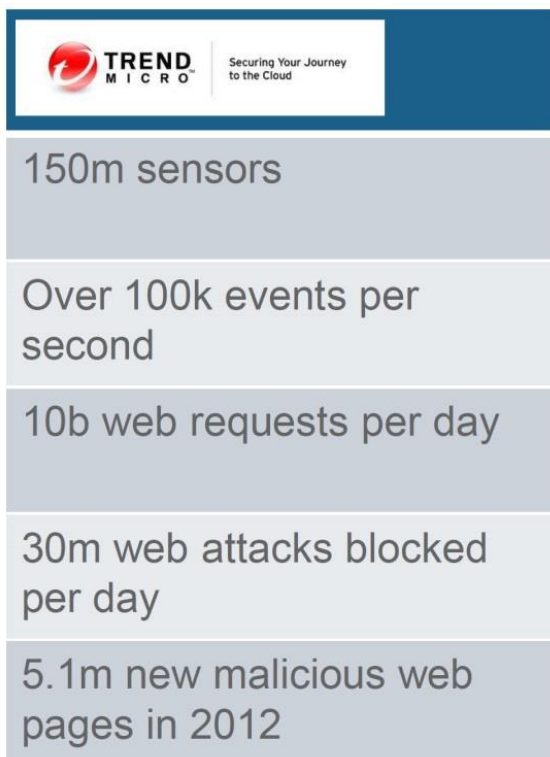
Trend Micro Smart Protection Network sfrutta un approccio di difesa intelligente basato sulle conoscenze collettive ottenute dell'ampio e globale bacino dei clienti Trend Micro, mettendo in relazione i dati provenienti da oltre 70 miliardi di query giornaliere.

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

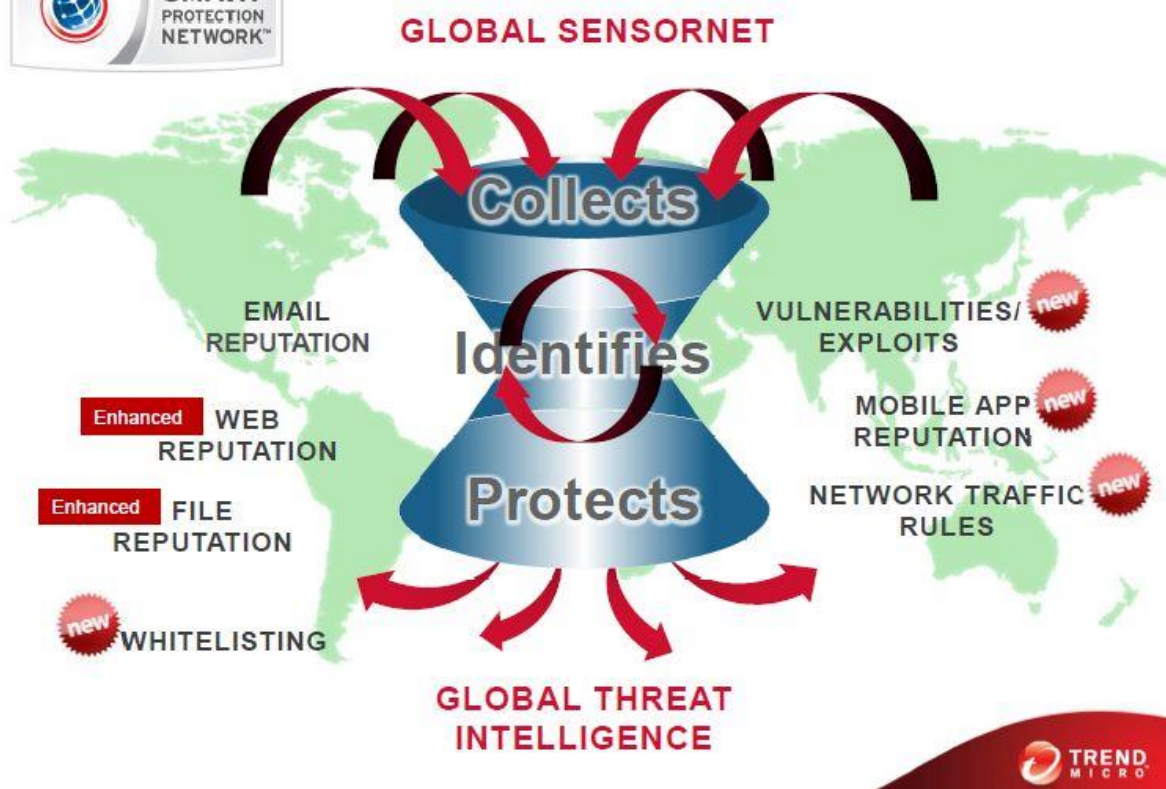
Uno strumento per l'analisi di reputazione e comportamento

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 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

Deep Discovery è il fulcro della soluzione di difesa personalizzata Trend Micro contro i Targeted Attack 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 OfficeScan per la sicurezza dei terminali

È la soluzione per la sicurezza dei terminali (endpoint) negli ambienti virtualizzati indipendente dall'hypervisor, indirizzata alle medie e grandi organizzazioni.

OfficeScan è pensata per rispondere alle sfide specifiche degli endpoint implementati all'interno di ambienti VDI e si integra con Citrix XenDesktop e VMware View.

OfficeScan permette di massimizzare il numero di desktop virtualizzati per host, contribuendo a migliorare il ROI legato agli ambienti VDI, senza incidere sugli standard di sicurezza.

È in grado di identificare gli endpoint virtualizzati e di ottimizzare l'efficienza della protezione risorse attraverso la serializzazione delle operazioni di scansione e degli aggiornamenti di sicurezza, evitando pertanto i tipici problemi di rallentamento che coincidono con gli update degli antivirus o il riavvio delle macchine.

CONCLUSIONI

Il numero delle minacce a cui è sottoposta la PA 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 o al cyber terrorismo.

La Pubblica Amministrazione italiana sta faticosamente procedendo verso un modello digitale che richiede l'adozione di soluzioni efficaci e strutturate per la protezione ICT. Le indicazioni normative fornite con il CAD e Agenda Digitale restano una guida ancora troppo inascoltata anche a causa della mancanza dei decreti attuativi delle norme tecniche.

L'adozione di strategie e soluzioni avanzate di sicurezza IT non può però essere più procrastinata adducendo incompletezze normative perché in gioco ci sono rischi molto elevati. È dunque importante che prevalga la consapevolezza che la sicurezza nella PA non deve essere vista come un problema ma, invece, come uno strumento necessario con cui tutelare il patrimonio informativo pubblico, la produttività degli operatori e rafforzare la fiducia dei cittadini nei confronti degli Enti governativi.

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 la Pubblica Amministrazione a rischi gravissimi che spaziano dal danno di immagine e fiducia da parte dei cittadini, a quello economico a veri e propri rischi di immobilità operativa della macchina statale.

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. Soprattutto in un contesto come quello della PA in cui non è sempre possibile disporre di persone competenti e risorse sufficienti.

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 amministrazioni pubbliche e a prevenire possibili danni economici.

Reportec

*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 Reseller** accessibili all'interno del dominio **tomshw.it**. Reportec è **Media e Content Conference Partner** di **IDC Italia**.*

La sicurezza ICT nella Pubblica Amministrazione. Una criticità che non si può più procrastinare.

© Reportec S.r.l. - Dicembre 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.

Reportec