



SPECIALE

LA SICUREZZA È ANCHE E SOPRATTUTTO MOBILE

L'esperienza digitale è sempre più mobile. Per avere la percezione di quale sia il livello di adozione attuale nella fruizione di contenuti digitali e nell'espletamento di attività transazionali e di acquisto online basta citare un dato fornito da Audiweb secondo cui in un mese oltre il 40% della popolazione italiana tra i 18 e i 74 anni si collega a Internet almeno una volta tramite smartphone o tablet.

pag. 9-15

CYBER ATTACK

L'AGGIORNAMENTO DEL RAPPORTO CLUSIT: ASSALTO ALLE BANCE

Ultima tappa per il Security Summit, la manifestazione sulla sicurezza informatica organizzata dal Clusit in collaborazione con Astrea, che a Verona presenta l'aggiornamento del Rapporto Clusit, con i dati relativi agli attacchi registrati nel primo semestre del 2016.

Lo scenario resta inquietante, ma il fatto che le imprese restano in piedi è, comunque, un segnale che le soluzioni per la sicurezza funzionano. **pag. 4**

SOLUZIONI

TREND MICRO: MACHINE LEARNING PER LA SICUREZZA DEGLI ENDPOINT

XGen endpoint security è il nome della nuova soluzione di sicurezza per gli endpoint introdotta da Trend Micro che si caratterizza per un approccio innovativo al modo di individuare e applicare tecnologie di difesa per proteggere l'attività degli utenti su desktop fisici e virtuali, laptop e dispositivi mobile.

Questa soluzione abbina tecnologie di machine learning con soluzioni di protezione dalle minacce. **pag. 18**

IN QUESTO NUMERO:

OPINIONE

pag. 3

- Un'impresa senza confini cerca protezione

CYBER ATTACK

pag. 4

- L'aggiornamento del rapporto Clusit: assalto alle bance

pag. 6

- Lo scenario degli attacchi in Italia secondo l'OAD

SPECIALE

pag. 10

- La sicurezza è anche, e soprattutto, mobile

pag. 14

- Dispositivi mobili: essenziali, ma fragili

SOLUZIONI

pag. 16

- Google, un minuto a tutela della cyber security

pag. 18

- Trend Micro: machine learning per la sicurezza degli endpoint

SICUREZZA COSTANTE, INTELLIGENTE

E PUOI AVERLA SUBITO.

Le tue aree di vulnerabilità aumentano. I contenuti si moltiplicano.

I cybercriminali sono sempre più scaltri.

Fortinet offre una singola infrastruttura di sicurezza intelligente che protegge la tua rete dalle minacce attuali e future.

Visita www.fortinet.it per maggiori informazioni.

FORTINET®

Sicurezza senza compromessi

UN'IMPRESA SENZA CONFINI CERCA PROTEZIONE

Gli anni Novanta hanno visto la diffusione di due tecnologie, oggi alla base delle comunicazioni e dell'informatica nelle imprese, nonché critiche per i processi aziendali stessi. La rete Internet e la telefonia mobile hanno modificato per sempre le relazioni tra le persone e tra le imprese e i loro clienti e fornitori. La stessa organizzazione aziendale sta affrontando importanti cambiamenti, sviluppando nuovi modelli derivati dalla collaboration e dall'open knowledge.

Le più recenti ondate innovative, dal cloud alla cosiddetta digital transformation, hanno ulteriormente contribuito a trasformare lo scenario delle soluzioni per la sicurezza. Oggi è inefficace il tradizionale approccio basato sulla protezione della rete intesa come perimetro aziendale. Quest'ultimo non esiste più: i dati, presi di mira dai cyber criminali, sono diffusi sui numerosi dispositivi utilizzati non solo dai dipendenti, teoricamente controllabili, ma anche su quelli di fornitori e clienti. Proprio il dispositivo mobile, ormai strumento irrinunciabile, rappresenta il principale punto debole della catena di protezione. La piaga dei ransomware è un'ulteriore minaccia che può colpire ogni impresa, anche la più piccola.

In questo scenario occorrono tecnologie innovative, ma soprattutto approcci più decisi sulla cultura della sicurezza. L'errore umano non può essere eliminato del tutto, ma un'azione educativa è fondamentale.

Nello speciale mobile security, realizzato su questo numero, tracciamo la preoccupante situazione delle vulnerabilità dei dispositivi mobili.

Non intendiamo fare terrorismo psicologico e, peraltro, il rapporto sugli attacchi digitali in Italia mostra che a essere attaccate sono soprattutto le imprese più grandi, ma anche che le piccole sono le più indifese e le meno consapevoli dei rischi.

Security & Business 39 ottobre 2016

Direttore responsabile:
Gaetano Di Blasio

In redazione:
Riccardo Florio, Giuseppe
Saccardi, Paola Saccardi,
Daniela Schicchi

Grafica: Aimone Bolliger

Immagini: dreamstime.com

www.securityebusiness.it

Editore: Reportec srl
Via Marco Aurelio 8
20127 Milano
tel. 02.36580441
Fax 02.36580444
www.reportec.it

Registrazione al tribunale
n.585 del 5/11/2010

Tutti i marchi sono
registrati e di proprietà
delle relative società

L'AGGIORNAMENTO DEL RAPPORTO CLUSIT: ASSALTO ALLE BANCHE

Crescono gli attacchi da una media di 84 al mese nel 2015 a una di 86,3 nei primi 6 mesi del 2016.

Aumenta lo spionaggio industriale del 9%.

Occorre, dunque, cambiare le prospettive

di Gaetano Di Blasio

Ultima tappa per il Security Summit, la manifestazione sulla sicurezza informatica organizzata dal Clusit in collaborazione con Astrea, che a Verona ha presentato l'aggiornamento del Rapporto Clusit, con i dati relativi agli attacchi registrati nel primo semestre del 2016.

Lo scenario resta inquietante, ma il fatto che le imprese restino in piedi è comunque un segnale che le soluzioni per la sicurezza funzionano.

Gli attacchi continuano nella loro crescita: se nel 2015 la media rilevata era di 84 attacchi al mese, nel primo semestre 2016 si è registrato un 86,3 con quasi un raddoppio della pressione verso il settore finance (+93,94% tra il secondo semestre 2015 e il primo semestre 2016). In calo gli attacchi rivolti verso il settore dell'hospitality: alberghi e ristoranti, presi di mira principalmente per sfruttarne il WiFi e arrivare a credenziali e carte di credito degli ospiti. Il cybercrime resta la principale fonte degli attacchi, che, passano dal 68% al 71%, mentre stupisce gli analisti il più 9% dello spionaggio industriale, anche in considerazione del campione preso in esame. Sono stati considerati solo gli attacchi di dominio pubblico più gravi, quindi una porzione molto bassa degli attacchi complessivi. In altre

parole, è probabile che lo spionaggio stia crescendo considerevolmente.

Ciò che gli esperti del Clusit evidenziano è l'industrializzazione del crimine informatico: non sono più gli hacker a pianificare gli attacchi, ma veri e propri criminali che facevano rapine fino a ieri. Non si tratta di esperti, ma di criminali comuni.

Il cambiamento è emblematico, basta l'episodio raccontato da Andrea Zapparoli Manzoni, membro del consiglio direttivo del Clusit, il quale ha letto il dibattito su un forum underground tra i "vecchi" hacker che criticavano gli attacchi rivolti agli ospedali e i "nuovi" cybercriminali, che attaccano con il ransomware chiunque sia disposto a pagare.

Rispetto alle tipologie di attacco, va sottolineato che il 26% rimane ancora un mistero totale, mentre un 19% di attacchi dovuti a vulnerabilità e un 12% di SQL injection, manifestano come anche nelle grandi imprese sia ancora difficile mantenere policy di sicurezza elementari.

Da segnalare anche il nuovo record per un attacco DDoS da 1 Tbps, cioè cento volte il traffico dal Mix di milano al resto del mondo. Attacco reso possibile dall'utilizzo dell'IoT, con la violazione di telecamere di videosorveglianza che hanno permesso di

Distribuzione delle vittime per tipologia

Vittime per tipologia	2011	2012	2013	2014	2015	2H v2015	1H 2016	Variazioni 1H 2016 su 2H 2015
Insitutions: Gov-Mil-LEAs-Intelligence	153	374	402	213	223	109	105	-3,67%
Others	97	194	146	172	51	22	39	77,27%
Entertainment/News	76	175	147	77	138	59	52	-11,86%
Online Services/Cloud	15	136	114	103	187	103	89	-13,59%
Research-Education	26	104	70	54	82	38	33	-13,16%
Banking/Finance	17	59	108	50	64	33	64	93,94%
Software/Hardware/Vendor	27	59	46	44	55	32	31	-3,13%
Telco	11	19	19	18	18	9	4	-55,56%
Gov. Contractors/Consulting	18	15	2	13	8	3	2	-33,33%
Security Industry	17	14	6	2	3	3	0	100,00%
Religion	0	14	7	7	5	1	4	300,00%
Health	10	11	11	32	36	16	39	143,75%
Chemical/Medical	2	9	1	5	2	0	0	0,00%
Critical/Infrastructures	-	-	37	13	33	13	24	84,62%
Automotive	-	-	17	3	5	1	1	0,00%
Org/ONG	-	-	19	47	46	21	5	-76,19%
GDO/Retail	-	-	-	20	17	12	14	16,67%
Hospitality/hotel industry	-	-	-	-	39	20	15	-25,00%

Clusit - Rapporto 2016 sulla Sicurezza ICT in Italia - Aggiornamento al 30 giugno 2016

accrescere smodatamente i volumi.

Saranno i social network la minaccia del futuro, perché i messaggi di phishing hanno un tasso di successo molto più alto (anche 85% su LinkedIn) se veicolati tramite strumenti che non filtrano i contenuti e non costano nulla.

Dalla tavola rotonda con il presidente onorario del Clusit, Gigi Tagliapietra, Giuseppe Caldiera, direttore generale di Cuoa Business School, Maurizio Martinozzi di Trend Micro, Paolo Florian di Intel Security, Andrea Piazza di Microsoft e Alessio Pennasilico e Andrea Zapparoli Manzoni del Consiglio Direttivo del Clusit, è emersa l'importanza della formazione e di una cultura per sicurezza che va rivolta soprattutto al management: «La sicurezza è un problema di business non tecnologico», sottolinea Caldiera. L'approccio deve essere legato alla gestione dell'impresa, che non può ignorare la sicurezza e, anzi, deve affrontarla come per qualunque altro tipo di rischio.

Da l'importanza di adottare strategie di risposta agli incidenti, secondo le linee guida che propongono protezione, detection e response. Martinozzi aggiunge anche la rilevanza della condivisione.

Su un fronte più tecnico, i relatori puntano i riflettori sulla protezione delle identità, perché le credenziali d'accesso sono la preda preferita dagli attacker. Questi ultimi, ormai, entrano facilmente all'interno dei sistemi e per rilevarne la presenza diventa fondamentale l'analisi comportamentale, che aiuta a capire cosa accada nel sistema informatico.

Per quanto, in Italia il pericolo maggiore è il ransomware e, per quanto possa sembrare banale, i relatori concordano che un forte aiuto arriva dall'application whitelisting.

Guardando al lato positivo, c'è da considerare che la sicurezza funziona, magari non blocca tutto, ma se le aziende restano in piedi è perché il grosso viene fermato.

LO SCENARIO DEGLI ATTACCHI IN ITALIA SECONDO L'OAD

L'Osservatorio degli Attacchi Digitali pubblicato da Aipsi mostra una pressione del cyber crime concentrata sulle grandi e medio grandi imprese

di R.F. e G.D.B.

Se la situazione internazionale mostra una preoccupante crescita degli attacchi compiuti dai cyber criminali, lo scenario italiano sembra molto più rassicurante, stando ai dati raccolti da Aipsi, l'associazione, capitolo italiano di ISSA (Information Security Systems Association), che unisce i professionisti della sicurezza informatica.

Quest'anno, lo storico rapporto OAI (Osservatorio Attacchi Italiani) si è rinnovato, anche grazie alla collaborazione con NextValue, diventando rapporto OAD (Osservatorio degli Attacchi Digitali) e sembra mostrare una situazione tranquilla. Infatti, il 62,4% delle aziende interpellate, tutte italiane appunto, hanno dichiarato di non aver mai subito o rilevato un attacco.

«Il sospetto è che non se ne siano accorte», commenta Marco Bozzetti, ideatore e curatore del rapporto, nonché presidente di Aipsi, che aggiunge: «È evidente che, almeno maggior parte non ha subito gravi danni, vista la mancata percezione, però è probabile che una parte abbia preferito non dichiararlo».

Peraltro, ricordando il caso Benetton di due anni fa, è difficile per una piccola impresa accorgersi che un documento (per esempio il design di un mobile) sia stato copiato e poi il mobile realizzato e messo in vendita su mercati esteri, magari non presidiati

dalla piccola impresa. Ma in un caso del genere come quantificare il danno?

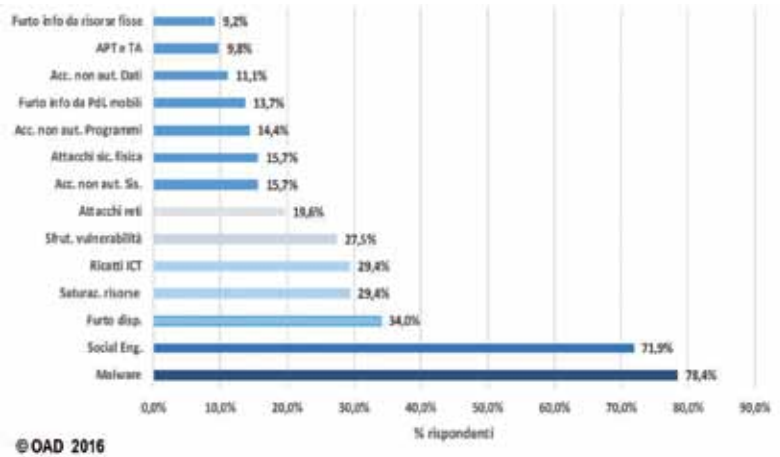
Sempre Bozzetti ritiene che il tessuto economico italiano, caratterizzato da milioni di piccolissime e piccole medie imprese, risulti di fatto meno appetibile. La controprova sarebbe che le aziende più grandi hanno, invece, proporzionalmente rilevato un certo numero di attacchi: il 28,2% del totale ha subito oltre 10 attacchi negli ultimi 12 mesi e il restante 9,4% oltre 10 casi. Dati che mostrano un trend essenzialmente costante dal 2008.

Anche le prime quattro tipologie di attacco sono sempre le stesse da quando viene redatto il rapporto: malware per il 78,4% dei casi, social engineering (71,9%), furto dei dispositivi (34%), DDoS (29,4%). Negli ultimi due anni il quarto posto è però condiviso dal ransomware.

Numero e tipo di minacce

Il numero di attacchi rilevati nei diversi Rapporti OAI dal 2007 al 2015, nonostante la variazione dei campioni dei rispondenti conferma una sostanziale stabilità del fenomeno in Italia. A subire attacchi è sempre all'incirca il 40% del campione con oscillazioni relativamente contenute. Un dato che da alcuni esperti è considerato troppo basso, indice che

Ripartizione percentuale per tipologia di attacco (risposte multiple)



molti attacchi non sono stati rilevati.

Gli attacchi aumentano con il crescere del numero di dipendenti e le organizzazioni nella fascia con oltre 5mila addetti sono quelle che registrano il maggior numero di attacchi per anno.

Costanti anche i primi quattro posti di attacco più diffusi che restano sempre appannaggio dei medesimi tipi di attacchi digitali.

Al primo il malware con un 78,4% che ha avuto un picco nel 2015 dovuto alla diffusione in Italia dei ransomware. Al secondo posto il social engineering (incluso il phishing) con il 71,9%, una categoria di attacco che spesso costituisce i prodromi di attacchi più complessi come APT (Advanced Persistent Threat) e gli attacchi mirati (Targeted Attack, in sigla TA) con il 34 %, il furto di dispositivi ICT che si è scambiato di posto rispetto all'edizione precedente del rapporto con il Denial of Service/Distributed Denial of Service, ora quarto con il 29,4%.

Il costo per l'azienda

Il danno economico causato da un attacco è l'elemento determinante e si manifesta in modo differente: dal disservizio, al tempo uomo speso, a quello di immagine, alla riduzione della competitività nel caso di diffusione di informazioni critiche aziendali.

La stima del valore del danno non è semplice ma neppure impossibile. Eppure il 43,5 % dei rispondenti non la effettua e solo il 25,9% la effettua per tutti gli attacchi subiti anziché limitarsi solo agli attacchi più gravi.

Una recente ricerca di Ponemon Institute, effettuata anche per l'Italia con il coinvolgimento di 24 aziende/enti italiani di 11 diversi settori merceologici, stima un costo medio di violazione dei dati per persona che è passato da 105 nel 2015 a 112 euro nel 2016; si tratta di un costo che aumenta nel caso di aziende che operano nei settori dei servizi, finanziario e della sanità.

Un quarto delle violazioni dei dati è causata da difetti dei sistemi ICT, spesso in combinazione con malfunzionamenti dei processi aziendali a essi associati, mentre il 29% delle violazioni dei dati è causata dalla negligenza degli operatori ICT e dei fornitori di ICT.

La gestione dell'attacco

Una volta individuato un attacco, il 60% dei rispondenti non lo comunica e solo il 15% avvisa le competenti autorità di sicurezza, solitamente la Polizia Postale e delle Comunicazioni, pochi segnalano l'attacco a centri specializzati tipo Cert e nessuno



Misure per la protezione dei dati (risposte multiple)

del campione avvisa una Assicurazione: indice che pochi del campione hanno stipulato assicurazioni sul rischio residuo di un attacco.

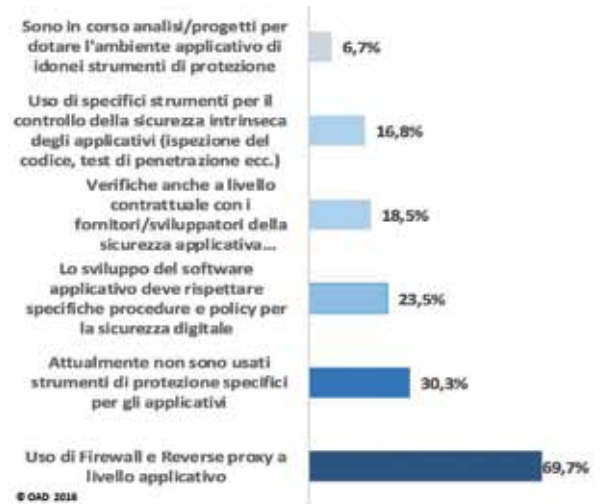
Il tempo massimo occorso per il ripristino dei sistemi ICT a seguito di un grave (o il più critico/grave) attacco subito nel 2015 nella maggior parte dei casi (44%) è meno di un giorno e nell'80% dei casi la situazione è ripristinata entro 3 giorni dall'attacco. Tuttavia i codici maligni (per esempio i ransomware) e i furti di dispositivi (con annesse denunce ed eventuale riacquisto e riconfigurazione del dispositivo) richiedono tempi di ripristino superiori a una settimana.

Le contromisure adottate

Gli strumenti per la sicurezza logica si differenziano in funzione delle unità ICT da proteggere, e si articolano in identificazione, autenticazione, autorizzazione degli utenti, sistemi di protezione delle reti dei sistemi e degli applicativi.

Per la protezione delle proprie reti interne e degli accessi ad Internet e alle reti "pubbliche" la quasi totalità dei rispondenti è dotato di dispositivi firewall e di DMZ e più del 72% utilizza soluzioni VPN. Per rendere sicure le comunicazioni da remoto.

Gli strumenti principali per la protezione logica dei



server sono, come prevedibile, gli anti-malware, utilizzati dal 93,3% dei rispondenti, mentre al secondo posto figurano la gestione delle patch e degli aggiornamenti che si dimostra una misura di crescente diffusione rispetto all'anno precedente.

Per la protezione dei dati, che costituiscono il reale e più importante asset ICT aziendale il 69,7%, utilizza l'archiviazione remota, tipicamente con ISP/ASP e fornitori cloud; con una tendenza a replicare in remoto tutti i dati o quelli più critici, in storage su cloud via IaaS (Infrastructure as a Service).

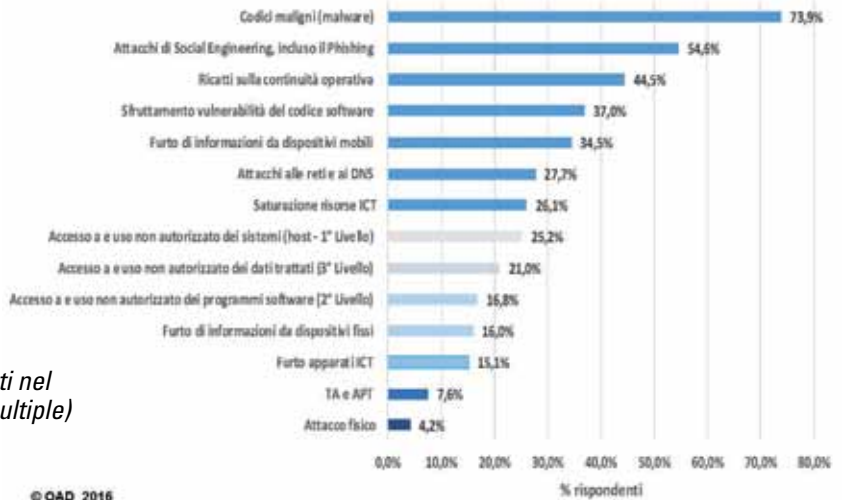
Il secondo strumento più diffuso, usato da circa il 48% del campione, è l'uso della crittografia nella trasmissione dei dati in rete, tipicamente nelle transazioni via web con HTTPS o con FTPS. La crittografia dei dati archiviati o almeno di quelli più critici, si riduce al 21% dei rispondenti, ed emerge una percentuale di poco inferiore per l'uso di strumenti DLP, Data Loss Prevention.

Una percentuale non trascurabile di quasi il 13,4% non usa alcuna specifica tecnica per la protezione dei dati.

Un altro aspetto critico per la sicurezza è quello delle applicazioni che sono sempre più frequentemente il veicolo preferenziale per sferrare attacchi.

*A sinistra:
strumenti tecnici
di sicurezza
digitale per
gli applicativi
(risposte multiple)*

*Attacchi più temuti nel
futuro (risposte multiple)*



L'indagine di Aipsi mette in evidenza che gli strumenti più diffusi (69,7%) per la protezione degli applicativi sono i firewall ed i reverse proxy posti a difesa dei server applicativi, dei data base server e dei sistemi di storage. Quasi un terzo del campione dichiara invece di non fare alcun uso di specifici strumenti di sicurezza per i propri applicativi.

Misure organizzative per la sicurezza digitale

Le misure organizzative nel loro complesso sono determinanti per l'attuazione e la gestione di una effettiva ed efficace sicurezza informatica eppure risultano ancora troppo poco diffuse.

Il 27% di aziende campione dichiara di non avere alcuna misura organizzativa per la sicurezza digitale, mentre il 43% utilizza procedure organizzative in merito alla sicurezza digitale, definite nell'ottica delle policy emanate. In particolare, circa il 42% utilizza strumenti informatici per il supporto e l'automazione dei processi per la sicurezza digitale (sistemi di work-flow, correlazione tra gli allarmi, banche dati e sistemi "smart" a supporto dell'help-desk e così via), il 28,6% usa procedure per la gestione di incidenti e il 26,9 per la gestione dell'help desk.

Gli attacchi più temuti

Nell'elenco degli attacchi ritenuti più pericolosi, e quindi più temuti nel prossimo futuro, per la propria azienda/ente da un punto di vista di impatto sul business, di impatto economico, di immagine e così via, figurano al primo posto i codici maligni seguiti dal social engineering.

Mentre in fondo alla classifica siano posizionati gli attacchi fisici e i sofisticati TA e APT.

A motivare gli attaccanti secondo oltre la metà dei rispondenti è la frode informatica, che permette lauti guadagni illegali con bassi rischi di essere scoperti e puniti. Segue al secondo posto il ricatto o ritorsione, cui sicuramente ha contribuito la diffusione in Italia dei ransomware con un percentuale del 51,3%.

Nella fascia percentuale compresa tra 30% e 40% figurano il vandalismo e l'hacktivismo, che rimangono "storicamente" diffuse motivazioni in ambito italiano a cui fanno seguito con percentuali variabili tra il 20% e il 30% il sabotaggio, l'azione dimostrativa, che include anche gli attacchi del così detto "ethical hacking", e lo spionaggio, soprattutto di tipo industriale che costituisce un problema crescente per il "made in Italy".

LA SICUREZZA È ANCHE, E SOPRATTUTTO, MOBILE



Sempre più informazioni critiche passano attraverso i dispositivi mobili ma la sicurezza è ancora troppo trascurata

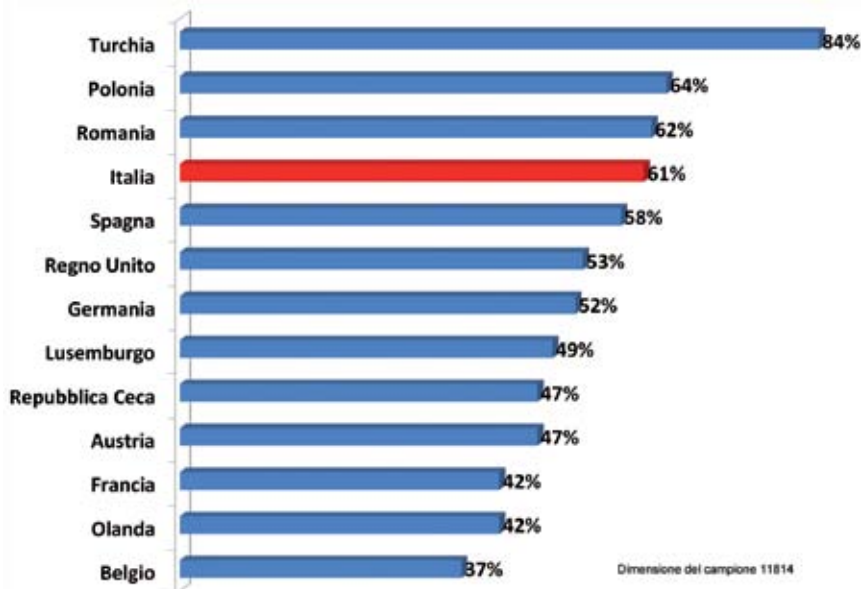
di Riccardo Florio

L'esperienza digitale è sempre più mobile. Per avere la percezione di quale sia il livello di adozione attuale nella fruizione di contenuti digitali e nell'espletamento di attività transazionali e di acquisto online basta citare un dato fornito da Audiweb secondo cui in un mese oltre il 40% della popolazione italiana tra i 18 e i 74 anni si collega a Internet almeno una volta tramite smartphone o tablet.

In uno scenario in cui i dispositivi mobili stanno scalzando i "vecchi" Pc è inevitabile affrontare il tema della sicurezza in relazione alle specificità introdotte dalla mobilità. L'importante tema è stato ripreso anche all'interno del rapporto 2016 realizzato dal Clusit, in particolare attraverso i contributi di Marco Landi e Andrea Ravaini che hanno fornito interessanti spunti di riflessione che vengono ripresi e ampliati di seguito.

Più consapevolezza dei rischi

I rischi crescono rapidamente non solo per l'evoluzione tecnologica che crea modalità sempre nuove e più efficaci di attacco, ma anche per il ritardo con



Percentuale di utenti che acquistano tramite dispositivo mobile (Fonte: Ing International Survey, aprile 2015)

cui la consapevolezza dell'utente finale si allinea al livello di minacce da fronteggiare. Si tratta, purtroppo, di una situazione già vista: il primo investimento "serio" in sicurezza da parte di un'azienda è molto spesso successivo ad aver subito un grave danno. In moltissimi casi, l'anello debole della catena di sicurezza sono le persone e questo tipo di vulnerabilità non si può eliminare semplicemente tramite la tecnologia.

L'adozione di regole aziendali condivise e la diffusione di cultura del rischio costituiscono un passaggio inevitabile, anche nell'utilizzo di dispositivi mobili, soprattutto in uno scenario in cui sempre più informazioni di valore critico vengono accedute, memorizzate e trasferite tramite smartphone e tablet e i dispositivi mobili sono anche sempre più uno strumento per effettuare transazioni.

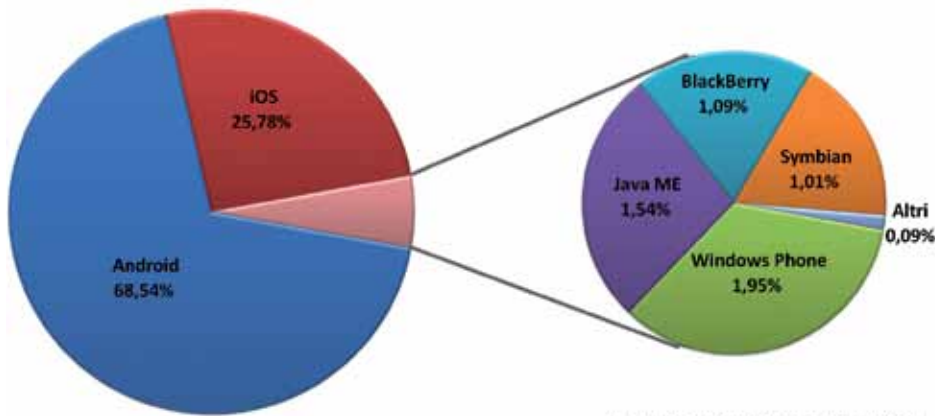
Secondo uno studio di Ing Direct (pubblicato ad Aprile 2015) il 61% degli italiani che dispone di uno smartphone o di un tablet lo utilizza anche per effettuare acquisti e la diffusione del mobile banking, che per ora interessa un terzo degli italiani, è in rapida crescita.

Tutti pazzi per Android

Android è l'ambiente per dispositivi mobile preferito a livello globale. Un dato che trova innumerevoli conferme tra cui quella di Netmarketshare che gli attribuisce il 68,54% di penetrazione nel mercato degli ambienti operativi per dispositivi mobili.

A preferire Android non sono, però, solo gli utenti, ma anche i cyber criminali che, nel 2015, hanno creato quasi un milione di nuovi malware rispetto al biennio 2013/2014 portando il totale dei nuovi ceppi di malware prodotti a oltre 2,3 milioni.

I rischi legati ad Android vanno da smartphone con firmware manipolati a scopo di lucro o con App spia per carpire dati riservati di utenti e aziende, ad attacchi multipiattaforma (Windows/Android) sempre più sofisticati per dirottare transazioni bancarie o di acquisto su siti illeciti, a una proliferazione di hacking tool disponibili sul mercato nero fino ad App che sembrano inoffensive ma che, in realtà, richiedono autorizzazioni "root" sul dispositivo o per funzionalità di sistema non necessarie, attraverso le quali poter accedere a dati personali e trasmetterli, dirottare la navigazione dell'utente su App e



Fonte: Netmarketshare, ottobre 2016

Diffusione degli ambienti operativi per dispositivi mobili

con la diffusione di aggiornamenti "custom" non ufficiali resi disponibili attraverso la comuni-

siti illeciti o sottoscrivere abbonamenti a servizi a pagamento mai richiesti dall'utente.

Si tratta di uno scenario sempre più preoccupante che, per vastità e sofisticatezza, non lascia alcuna possibilità alle aziende di riuscire a tenere il passo nella predisposizione di misure di sicurezza altrettanto efficaci. Ciononostante, i produttori di dispositivi mobili sembrano non prendere la situazione con la dovuta serietà.

I ritardi nell'aggiornamento del firmware Android

A dimostrazione di ciò basti pensare che, con l'arrivo alle porte della versione 7.1 la grande maggioranza degli utenti prevede sul proprio dispositivo mobile versioni vecchie di Android (4.4 e inferiori). È proprio l'obsolescenza che contraddistingue oltre l'80% dei dispositivi presenti sul mercato a rappresentare uno dei principali fattori di vulnerabilità di Android.

Una responsabilità che va attribuita anche ai produttori che non rendono disponibile l'aggiornamento come OTA per la maggior parte dei dispositivi mobile a causa di politiche di prodotto o di difficoltà a livello hardware

Come sempre capita, l'assenza dei produttori ufficiali ha lasciato spazio a un mercato libero alternativo

tà Android open source.

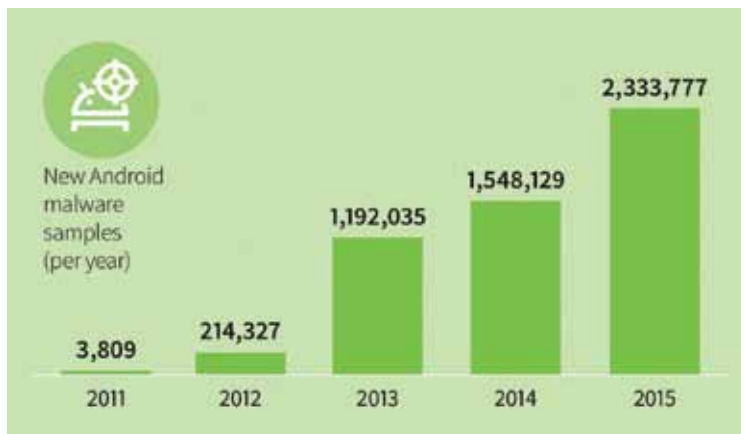
Uno degli esempi più noti in tal senso è il progetto CyanogenMod che, tuttavia, prevede una vera e propria manipolazione del firmware, provvedendo a rimuovere il brand e a richiedere permessi "root" sul telefono: un approccio che per risolvere problemi di sicurezza apre la strada a nuove vulnerabilità, soprattutto nei casi in cui il dispositivo mobile è nelle mani di utenti inesperti, che prestano poca o nessuna attenzione alle autorizzazioni richieste dalle App che installano successivamente all'installazione di CyanogenMod.

Poca richiesta e poche soluzioni

Non tutti i produttori di soluzioni di sicurezza affrontano il tema nello stesso modo e con la stessa attenzione. Una parte di responsabilità è, quindi, da attribuire anche a quei vendor che tendono a concentrare i loro sforzi prevalentemente sugli aspetti di protezione delle infrastrutture IT in azienda non occupandosi in modo altrettanto esaustivo dei rischi legati al mondo mobile.

Una trascuratezza che trae probabilmente le sue motivazioni dalla scarsa consapevolezza evidenziata in precedenza che fa sì che la domanda di sicurezza sui dispositivi mobili da parte degli utenti sia ancora

*Numero di nuovi ceppi di malware registrati nel corso degli anni
(Fonte: G Data Security Labs)*



poco rilevante numericamente: se si valuta la percentuale di utenti italiani che ha dotato il proprio smartphone o tablet di soluzioni antimalware adeguate o che ritiene necessario farlo, si deve constatare come si tratti di un numero irrisorio.

Il rischio invece c'è ed è reale. Non solo per le aziende più grandi ma anche per le PMI in cui le politiche di BYOD sono tollerate, utilizzate e non controllate lasciando spesso che ogni dipendente possa impiegare liberamente lo stesso dispositivo mobile per il lavoro e per la vita personale, senza predisporre una soluzione per la gestione centralizzata dei device mobili e delle rispettive policy di sicurezza.

Vulnerabile anche iOS

Uno dei miti moderni è che smartphone e tablet basati su iOS siano esenti da rischi.

In realtà l'esperienza ha mostrato che iOS non è scevro da vulnerabilità. Non solo i dispositivi con iOS manipolati dagli utenti (jailbreak) sono soggetti alle più varie forme di malware, ma anche smartphone e tablet con firmware originale ne subiscono le conseguenze. La sostanziale differenza tra i dispositivi basati su iOS e quelli che utilizzano Android è che, nel primo caso, esiste un unico produttore (Apple) che provvede a sviluppare il proprio firmware e ad aggiornarlo con regolarità chiudendo le falle più evidenti.

Neanche App Store è completamente sicuro. Nel

recente passato Apple si è accorta troppo tardi della presenza sul proprio App Store ufficiale di numerose App manipolate create con un Xcode contraffatto e contenenti codice dannoso, non riuscendo a proteggere milioni di utenti dai danni cagionati tramite violazione degli account iCloud.

Un futuro sempre più a rischio

L'evoluzione in atto lascia poche speranze per il 2017, soprattutto alla luce del fatto che gli smartphone saranno utilizzati per avvalersi di funzioni superiori a quelle offerte dal Pc (per esempio i pagamenti tramite NFC) e che, in un'ottica di Smart working lo smartphone rappresenta il "gateway" per lo scambio di tutte le comunicazioni, informazioni riservate aziendali e private di ogni singolo utente. Infine, non va sottovalutato il fatto che per flessibilità e impatto sul mercato, Android sarà presumibilmente la piattaforma più utilizzata per applicazioni IoT, che interesseranno ogni aspetto della nostra vita quotidiana, dal monitoraggio della salute, alle gestione delle autovetture al controllo dei sistemi di automazione industriale.

Uno scenario che apre la strada a nuove potenziali situazioni di rischio diffuse su una scala finora impensata e impensabile.

DISPOSITIVI MOBILI: ESSENZIALI, MA FRAGILI

Troppe aziende compromettono i loro dati sensibili dimenticando di mettere in sicurezza i dispositivi personali dei loro dipendenti

di Giuseppe Saccardi

Gli smartphone sono tanto vulnerabili quanto indispensabili. Pieni di informazioni riservate dell'azienda, se lasciati senza protezione, rappresentano una seria minaccia per l'organizzazione.

I dati aziendali, come le mail riservate, possono essere monitorate in tempo reale su reti wi-fi pubbliche. Applicazioni e siti web dannosi possono far perdere ancora più dati e causare fatture telefoniche astronomiche. E cosa succede se un dispositivo viene perso o rubato?

Non è facile trovare una soluzione. I dispositivi, non solo possono essere di diverso tipo, ma spesso sono anche fuori dal perimetro della rete, limitando visione e controllo.

Il BYOD va gestito

La cultura del lavoro 24h/7gg è anche uno dei motivi che porta a usare gli stessi dispositivi sia per la propria attività lavorativa che nel tempo libero (Bring Your Own Device). Questo può portare a situazioni in cui le attività sui social media, i dati e le soluzioni di un'azienda, come il CRM, vengono gestite sullo stesso dispositivo.

I rischi connessi alla sicurezza nella nostra società connessa sono numerosi – dalla perdita o

danneggiamento dei dispositivi alla crescita di minacce alla sicurezza mobile, dalla perdita o furto di dati, corruzione e frodi, ad applicazioni trojan e siti di phishing. Ma cosa significa questo per un'azienda? Oggi i dispositivi mobili dei dipendenti contengono sia le app che i dati personali dell'utente, sia le password di accesso che i dati aziendali, compresi quelli del CRM. Se lasciati senza protezione, questi rappresentano una seria minaccia per l'organizzazione. Senza la crittografia VPN i dispositivi sono vulnerabili alle intercettazioni delle comunicazioni tramite hotspot wi-fi non protetti. Senza un anti-malware completo i dispositivi sono vulnerabili alle minacce delle applicazioni e del web. Cosa succede se il dispositivo viene perso o rubato? Nel peggiore dei casi, potrebbe significare la fine della stessa azienda.

Cosa si può fare?

Il numero di dispositivi e connessioni usati attualmente dalle aziende non ha pari nel passato. È evidente che l'aumento dei dispositivi e dei software implica una vulnerabilità maggiore.

Gli attacchi raddoppiano di anno in anno e diventano sempre più sofisticati, rendendo quindi difficile



rimanere aggiornati in fatto di sicurezza informatica. In che modo è possibile ottenere una protezione completa con le risorse e il tempo limitati di cui dispone un'azienda?

F-Secure, azienda europea di cyber security, affronta queste problematiche con Protection Service for Business, soluzione che risponde alle esigenze di sicurezza e gestione e non richiede particolare manutenzione.

È pensata per proteggere un'ampia gamma di endpoint, in ufficio e ovunque l'utente si trovi. Offre protezione per tutti i dispositivi, inclusi computer Windows e Mac, smartphone iOS e Android e una grande varietà di piattaforme server. In un'unica soluzione si hanno antimalware, antifurto, VPN e gestione dei dispositivi mobili.

Dal punto di vista operativo Protection Service for Business è una soluzione gestita disponibile tramite la rete di reseller partner certificati di F-Secure. Poiché si tratta di una soluzione hosted non occorre, dunque, investire in hardware server e, grazie a una manutenzione che F-Secure evidenzia essere davvero minima, le aziende hanno la possibilità di focalizzarsi maggiormente sulle quelle che sono le loro competenze.

Supporto MDM di terze parti

Il client mobile in Protection Service for Business è progettato per supportare un'implementazione standard con soluzioni MDM di terze parti, come AirWatch, MobileIron, Intune e MaaS360. L'utilizzo di un componente per la sicurezza dedicato, in aggiunta alle funzionalità di sicurezza base offerte dalla soluzione MDM esistente, evidenzia F-Secure, aumenta la protezione da minacce come malware, furto di dati, phishing e altro. Tra i benefici che con il servizio è possibile ottenere vanno annoverati: disponibilità della visione e del controllo essenziali sui dispositivi mobili, prevenzione delle possibili violazioni di dati crittografando tutto il traffico su dispositivi mobili con una VPN personale e cancellazione dei dispositivi in caso di furto o perdita.

Possibilità di mantenere le prestazioni della batteria e del dispositivo a livelli ottimali tramite tecnologia ultraleggera sviluppata da F-Secure.

Aumento della velocità di navigazione su dispositivi mobili fino al 30% tramite la compressione del traffico, il blocco della pubblicità e il monitoraggio online. F-Secure ha anche elaborato un apposito test che misura il livello di conoscenza della propria organizzazione rispetto ai rischi, le tecnologie necessarie, i processi comprovati e l'approccio olistico. Per il test utilizzate il Qrcode.



GOOGLE, UN MINUTO A TUTELA DELLA CYBER SECURITY

Il mese della sicurezza informatica, firmato dal colosso americano si è concluso. Il tour per informare e informatizzare ha registrato numeri di successo

di Daniela Schicchi



È partito, da Milano, il 15 e 16 ottobre, nell'ex Campo di Grano di Porta Nuova, il tour di Google dal titolo "Vivi Internet, al sicuro" che ha avuto, come obiettivo, quello di aiutare, tutti gli utenti, a verificare la sicurezza del loro account Gmail. Se può apparire un discorso trito e ritrito, è bene sapere – infatti - che ci sono sempre dettagli che sfuggono agli utenti, in termini di sicurezza e controlli. Intanto i numeri parlano chiaro. Il 59% degli italiani afferma di utilizzare più tecnologia rispetto a due anni fa, ma il 55% degli intervistati nutrirebbe una preoccupazione crescente circa la protezione, l'accessibilità e la conservazione dei dati online.

Si chiama Account Personale ed è lo spazio, che è stato mostrato, raccontato e dimostrato durante il tour, di Google. Account Personale è in grado di fornire accesso immediato alle impostazioni e agli strumenti che possono aiutare le persone a proteggere i propri dati e la propria privacy e a decidere quali informazioni fornire a Google per rendere i suoi servizi ancora più utili, accessibili e sicuri.

Un mese... al sicuro

Il progetto "Vivi Internet, al sicuro", quest'anno, ha avuto il duplice obiettivo di sensibilizzare e formare

gli italiani circa l'uso di strumenti per la tutela della sicurezza dei dati sul web e, nel contempo, di stimolare un dibattito informato sui temi della privacy e della sicurezza online attraverso convegni e incontri di formazione nelle principali università italiane. L'iniziativa ha girato l'Italia grazie alla collaborazione tra Polizia Postale e delle Comunicazioni, Altroconsumo e dell'Accademia italiana del codice di internet.

Un bus Google ha attraversato le piazze di cinque città italiane (Milano, Cagliari, Napoli, Bologna e Roma), con l'obiettivo di sensibilizzare gli italiani sulla necessità di prestare maggiore attenzione a come vengono gestiti i propri dati online. In ogni tappa gli utenti hanno avuto la possibilità di scoprire, insieme agli esperti, le funzionalità di Google Account Personale e, in particolare, hanno effettuato - insieme a loro - un controllo della sicurezza del proprio account Google oltre ad aver ricevuto informazioni e consigli per approfondire il tema della prevenzione digitale.

Account Personale: cosa si può fare

Lanciato a giugno 2015, Account Personale, fornisce accesso immediato alle impostazioni e agli



strumenti che possono aiutare le persone a proteggere i propri dati e la propria sicurezza su Google. Nel corso dell'ultimo anno sono stati oltre un miliardo gli utenti che lo hanno utilizzato. Nel gazebo, allestito da Altroconsumo, gli esperti dell'organizzazione hanno fornito assistenza e consulenza ai consumatori che hanno chiesto di poter interagire, nel modo più efficace possibile, in ambiente digitale. Tra le varie funzioni utilizzabili di Account Personale, ci sono:

- La sezione "accesso e sicurezza" dove è possibile verificare le impostazioni relative alla propria password e all'accesso al proprio account ed effettuare il controllo di sicurezza .

- La sezione "informazioni personali e privacy" nella quale si possono gestire le impostazioni di visibilità e i dati usati da Google per personalizzare la nostra user experience legata a Ricerca, Maps e Youtube.
- La nuova funzione "Trova il tuo telefono" che è una recente implementazione in grado di supportare l'utente in caso di smarrimento dello smartphone in un raggio di una decina di metri. Grazie a questa funzione si potrà, dunque, far squillare il telefono (anche se lasciato in modalità silenziosa), bloccarlo, chiamarlo o lasciare un numero da richiamare sullo schermo. La funzionalità è compatibile su device Android e iOS.



TREND MICRO: MACHINE LEARNING PER LA SICUREZZA DEGLI ENDPOINT

XGen è una nuova soluzione di sicurezza, in grado di adattare dinamicamente la protezione al tipo di minaccia da fronteggiare

di Riccardo Florio

XGen endpoint security è il nome della nuova soluzione di sicurezza per gli endpoint introdotta da Trend Micro che si caratterizza per un approccio innovativo al modo di individuare e applicare tecnologie di difesa per proteggere l'attività degli utenti su desktop fisici e virtuali, laptop e dispositivi mobile.

Questa soluzione abbina tecnologie di machine learning con soluzioni di protezione dalle minacce, salvaguardia dei dati, controllo delle applicazioni, prevenzione delle vulnerabilità e cifratura. In tal modo è in grado di applicare, in maniera intelligente, la tecnologia più adeguata, al momento corretto. Questo tipo di protezione viene ritenuto essenziale da Trend Micro, in considerazione del modo con cui gli attacchi agli endpoint si sono evoluti nel corso degli ultimi anni. Se, infatti, in precedenza le uniche preoccupazioni erano i malware e lo spam ora, sempre più spesso, gli attacchi sono più insidiosi, sfruttano tecniche di social engineering, meccanismi di phishing e sono sempre più frequentemente realizzati ad hoc per colpire in modo mirato uno specifico target anziché rivolgersi in modo indifferenziato verso qualsiasi obiettivo che incontrano. Il risultato è una minaccia che riesce a essere più efficace e che, nel contempo, spesso non viene individuata



*Eva Chen,
CEO di Trend Micro*

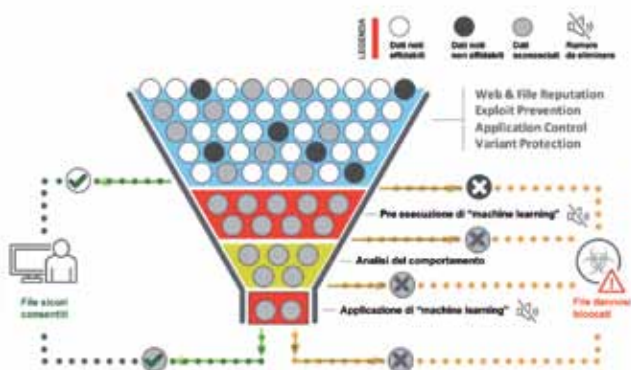
dalle tecnologie di difesa più standardizzate. «Il nome XGen è stato scelto con attenzione per indicare la tecnologia intergenerazionale che alimenta il nostro approccio - ha affermato Eva Chen, chief executive officer di Trend Micro. Sono anni che utilizziamo il machine learning come parte della nostra intelligence globale contro le minacce, la Smart Protection Network. Ora, abbiamo alzato il livello, includendo nelle nostre tecniche di protezione il machine learning ad alta affidabilità, per affrontare specificatamente le minacce più avanzate come i ransomware. A differenza nostra, gli altri vendor di security offrono solo una o due tecniche di protezione».

Come funziona XGen

Tramite l'applicazione di tecnologie di machine learning, la soluzione di Trend Micro analizza i file sia prima della loro esecuzione sia durante. L'utilizzo di una serie di funzioni di controllo e il confronto con "white list" permette di ridurre i falsi positivi.

I dati che arrivano a XGen subiscono l'azione di

Il funzionamento di Trend Micro XGen endpoint security



molteplici tecniche di sicurezza e vengono suddivisi in tre categorie: quelli noti per essere affidabili che vengono resi accessibili all'utente, quelli noti per essere dannosi grazie a indicazioni provenienti dalla intelligence di Trend Micro e che vengono istantaneamente bloccati e quelli di tipo sconosciuto che attraversano stadi successivi di analisi.

Il secondo livello di protezione esamina i dati sconosciuti con tecnologie di machine learning, quindi con tecniche di analisi del comportamento e ancora con machine learning ad alta affidabilità, differenziando così i file che devono essere bloccati da quelli leciti. XGen endpoint security è inserito all'interno della suite Trend Micro Smart Protection Complete che fornisce una gamma di soluzioni integrate per proteggere endpoint, e-mail e Web gateway e fornire visibilità e controllo centralizzati.

L'efficacia delle soluzioni Trend Micro per la protezione degli endpoint è confermata da Gartner che, dal 2002 fino a oggi, posiziona il vendor giapponese nel quadrante dei leader del suo Magic Quadrant for Endpoint Protection Platforms. Una posizione che si è ulteriormente migliorata nel 2016 in relazione alla "completezza di visione", una delle due direttrici, oltre alla capacità di rilascio, che compongono il noto diagramma della società di analisi americana.

Trend Micro Smart Protection Complete Suite

Trend Micro Smart Protection Complete è una suite che raggruppa più funzionalità di sicurezza collegate tra loro, che lavorano insieme per fornire protezione a livello di endpoint, applicazioni e rete.

Questa suite unisce la sicurezza integrata multilivello con caratteristiche di elevata flessibilità di deployment in cloud, modelli di licensing semplificati e una gestione centralizzata per ottenere visibilità sui differenti vettori di minacce da una singola postazione.

La suite fornisce i seguenti livelli di protezione:

- sicurezza degli endpoint: tramite XGen, il componente principale della suite, che raggruppa machine learning con altre tecniche di protezione;
- mobile security: per una gestione sicura, tracciata e monitorata dei dispositivi mobili dei dipendenti e dei dati aziendali, in modo da abitare politiche efficaci e controllate di BYOD;
- protezione di e-mail e sistemi di collaborazione: per difendersi contro spam, phishing, malware e attacchi mirati presso il server di posta, il gateway nonché per le applicazioni basate su cloud come Office 365;
- protezione Web: per abilitare l'accesso sicuro al Web e ai social media su qualsiasi dispositivo e da qualsiasi posizione garantendo, nel contempo, piena visibilità e controllo sull'utilizzo del Web. Tutto ciò sia nel caso in cui vengano adottati modelli di SaaS basati su cloud sia soluzioni "on site" di Web gateway sicuro.

The World is Your Workplace

FUJITSU

shaping tomorrow with you



Fujitsu LIFEBOOK S936 Massima sicurezza con PalmSecure integrato

Il notebook touch LIFEBOOK S936 è la scelta ideale per chi è sempre in movimento e necessita di tanta autonomia e funzioni di sicurezza al top.

- Processore Intel® Core™ i7 vPro™
- Windows 10 Pro
- Sottile e leggero (1,37 kg) con display WQHD da 13,3" e opzione touch
- Modular bay per drive ottico o seconda batteria

Windows 10 Pro è sinonimo di business.

I dispositivi Windows 10 Pro ti offrono tutta la potenza e gli strumenti di cui hai bisogno per i PC aziendali: più funzionalità di sicurezza, maggiore controllo, dispositivi solidi e innovativi che consentono di lavorare al massimo della produttività.



Schermate simulate, soggette a modifica. App Windows Store vendute separatamente. La disponibilità di app e l'esperienza possono variare in base al mercato.

workplace.it.fujitsu.com

© Copyright 2015 Fujitsu Technology Solutions. Fujitsu, il logo Fujitsu e i marchi Fujitsu sono marchi di fabbrica o marchi registrati di Fujitsu Limited in Giappone e in altri paesi. Altri nomi di società, prodotti e servizi possono essere marchi di fabbrica o marchi registrati dei rispettivi proprietari e il loro uso da parte di terzi per scopi propri può violare i diritti di detti proprietari. I dati tecnici sono soggetti a modifica e la consegna è soggetta a disponibilità. Si esclude qualsiasi responsabilità sulla completezza, l'attualità o la correttezza di dati e illustrazioni.



Windows 10 Pro