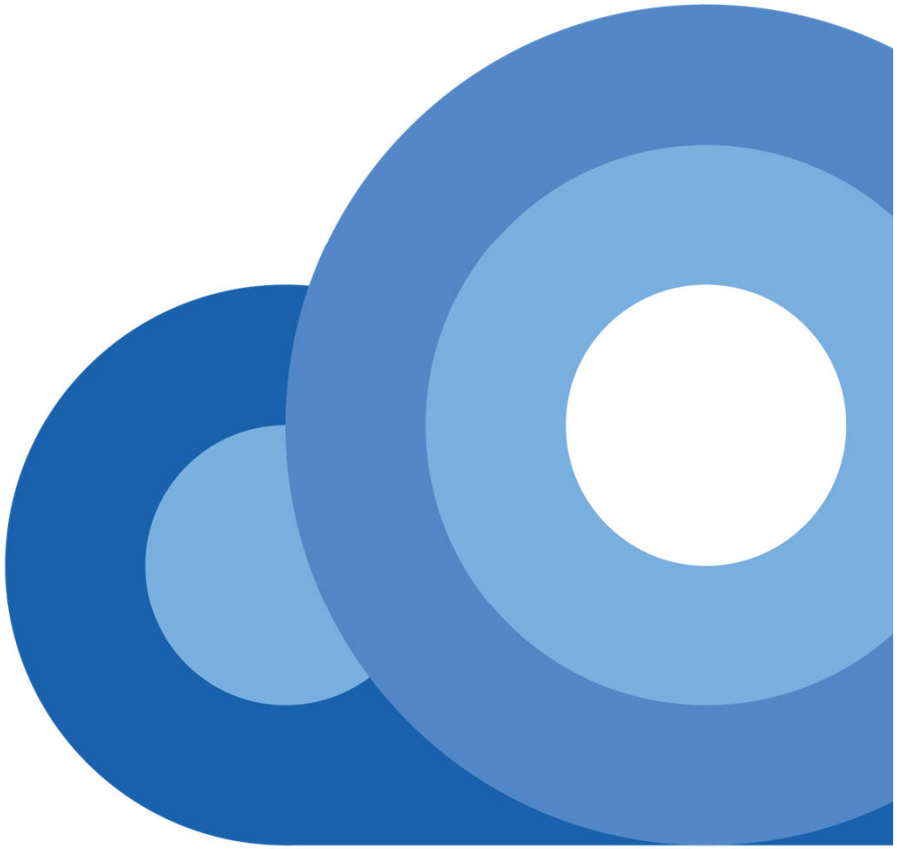
La gestione della sicurezza con il Cloud

Antonio Falzoni
Product & Tech Manager
antonio.falzoni@it.pandasecurity.com

Indice

1. La catena della sicurezza
2. Gli anelli della catena
3. Tecnologia e buon senso
4. Un riassunto delle tecnologie



La catena della Sicurezza

"Ho l'antivirus, sono a posto..."

Siamo dipendenti dalla tecnologia, forse troppo…

Dovremmo chiederci se il nostro sistema informatico è al sicuro da…

- Attacchi di "virus"?
- Intrusioni di cyber-criminali?
- Dipendenti infedeli?
- Guasti dell'hardware?
- Vulnerabilità del software?
- Incendio dei locali?
- Utilizzo improprio degli strumenti informatici?
- Mancanza di buon senso?

La catena della sicurezza

(farina del mio sacco, anno 2001)

1. Sensibilizzazione degli utenti contro i pericoli dell'Ingegneria Sociale (*Formazione e Informazione*)
2. Normative d'uso degli strumenti informatici (*Responsabilizzazione*)
3. Aggiornamento costante dei software (*Windows Update e non solo*)
4. Implementazione di Policy di sicurezza
5. Procedure di Backup/Disaster Recovery, alimentazione via UPS
6. Firewall, sistemi di Intrusion Detection
7. Protezione sugli Endpoint efficiente e costantemente aggiornata

In ogni istante della nostra “vita informatica” dobbiamo affrontare problemi di sicurezza… in merito a cosa?

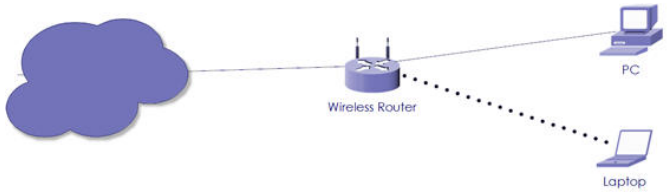
Ad esempio…

- sulle foto delle nostre vacanze
- sulla ricerca di nostro figlio studente
- sulla bozza di tesi di nostro figlio laureando
- sulle comunicazioni con la Banca o con l’azienda del Gas…
- sull’accesso alla Posta Elettronica e a Internet
- sui dati riservati e sensibili dei nostri clienti
- su **tutto quanto** è legato all’uso del computer…

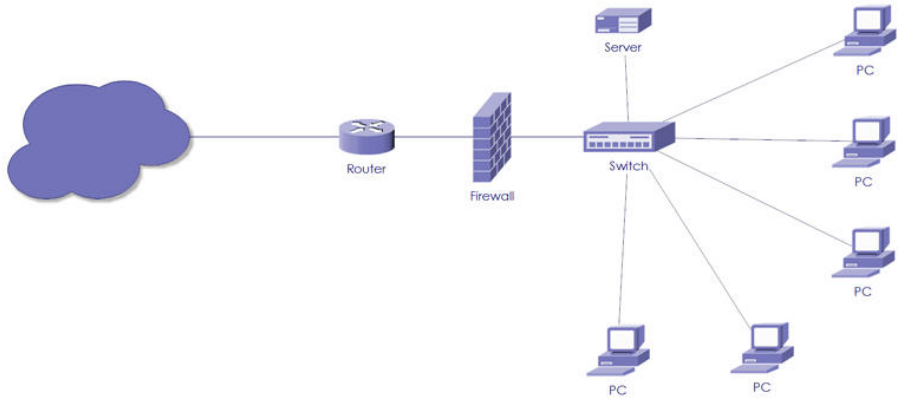
Da chi dobbiamo difenderci?

- Attacchi mirati per sottrazione di dati (spionaggio professionale/industriale)
- Attacchi vandalici (non mirati e per questo spesso letali)
- Malware (Virus, Worms, Trojans ecc…)
- Usi impropri dello strumento informatico
- Truffe perpetrate attraverso Ingegneria Sociale
- Ignoranza, negligenza, dolo della persona alla tastiera

Due tipici scenari di rete di studi professionali…



… con i medesimi problemi di sicurezza



Quando si compila il 730 si viene da voi...
Quando si ha un dolore si va dal medico...

Quando si ha un problema specifico, si va dallo specialista.

Perchè non far gestire la sicurezza a uno specialista informatico?

Gli anelli della catena

Partiamo dal fondo… 7, 6, 5, 4…

7: Last, but not least… l'antivirus

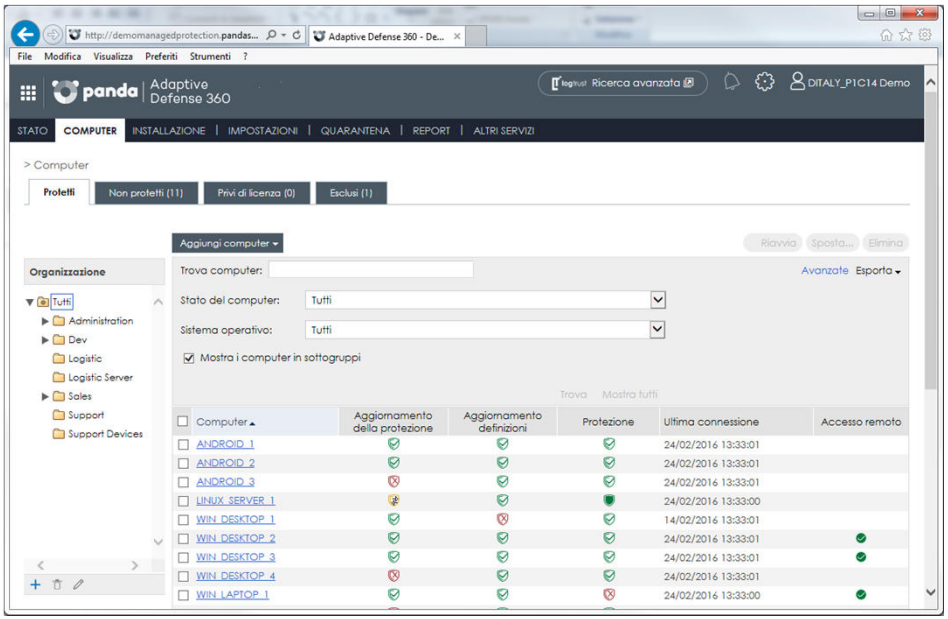
… *ma ricordate che la sicurezza informatica non si fa col solo "antivirus"*

Ieri "antivirus", oggi **Endpoint Protection**, perchè il computer è il punto finale, l'anello di congiunzione tra noi Umani e il mondo informatico.

E' la nostra ultima linea di difesa: impedisce sia il "proliferare" dei "virus" che l'esecuzione delle loro azioni dannose.

Deve essere attivo e costantemente aggiornato, perchè il numero di malware creato quotidianamente è elevatissimo.

Una soluzione di Endpoint Protection **cloud-based** permette di **gestire**, o di **far gestire** la sicurezza di una rete di uno, dieci, cento computer fissi e mobili, di smartphone, di tablet con diversi sistemi operativi (Windows, Linux, OS X, Android)



Panda Adaptive Defense 360

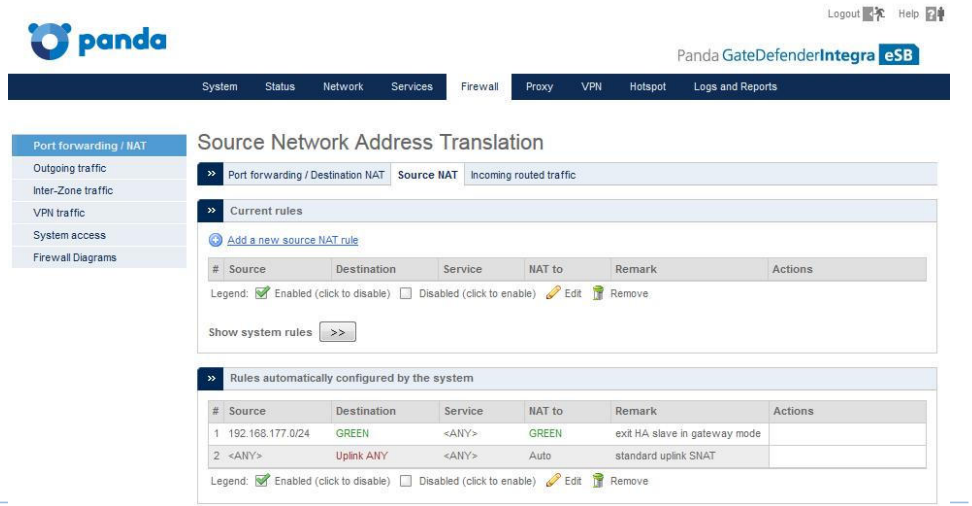
I benefici di una soluzione di sicurezza cloud-based

- Non richiede altro che l'installazione delle protezioni su ogni host.
- Non richiede un sistema di amministrazione locale.
- Non richiede alcuna complessità tecnica.
- Non richiede manutenzione
- Può essere gestita con un semplice browser web.
- Permette la delega della gestione a uno specialista.
- E' aggiornata costantemente e accede a un database nel cloud di dimensioni impensabili da gestire localmente su un computer.

6: il Firewall, per la sicurezza attiva

Software o dispositivo hardware che isola la rete aziendale dal mondo esterno, permettendo solo il **traffico autorizzato** e difendendo il punto di accesso a Internet da attacchi.

Panda Gatedefender
Panda Adaptive Defense 360



5: Sicurezza passiva

•Il computer può guastarsi, è nell'ordine naturale delle cose
•Manca improvvisamente l'energia elettrica (il server ha l'**UPS**?)
•L'ufficio si allaga o va a fuoco (avete l'estintore?)
•L'effrazione di un ladro vi ruba i computer (avete chiuso le finestre?)

Sono tutti eventi, e non i soli, che comportano la perdita di dati

I dati devono essere salvati in un **formato specifico** per un rapido ripristino in un **luogo diverso** da quello di utilizzo.

Una soluzione? Il **Backup sul Cloud**.

4: Criteri tecnologici di sicurezza

Gli utilizzatori del sistema informativo non devono poter compiere azioni pericolose per dolo, ma neanche per disinformazione o per errore.

E' opportuno concedere agli utilizzatori di una postazione di lavoro soltanto i **diritti a loro effettivamente necessari** in modo che non possano per errore, ingenuità, disattenzione, disinformazione o dolo, eseguire operazioni pericolose o installare software non autorizzato di dubbia provenienza che potrebbe contenere dei malware

3: Aggiornamento dei software e del sistema operativo dei computer

Avete notato quanti aggiornamenti sono richiesti da diversi programmi di uso corrente? **Eseguiteli!**

Il software è costituito da moduli scritti in diverse decine di milioni di istruzioni di codice sorgente.
L'Ingegneria del Software non è in grado di testare a fondo tutti i possibili comportamenti ottenuti interfacciando numerosi moduli.
E' possibile usare questi oggetti software per scopi non originariamente previsti, scopi che possono essere dannosi: librerie e routines possono essere usate in modo improprio aprendo delle "falle" nella sicurezza del computer eseguendo operazioni che non era possibile realisticamente prevedere.

2: Responsabilizzazione

Finora abbiamo parlato di strumenti tecnologici… ma la tecnologia non può tutto.

Il computer è uno strumento di lavoro che dovrebbe essere utilizzato solo per gli scopi a cui è preposto. Determinati utilizzi dovuti a ingenuità ed a disinformazione possono risultare dannosi per l'intera Azienda. Occorre responsabilizzare l'utilizzatore sulle operatività che possono e, soprattutto, che **non possono ne' devono** essere svolte con il sistema informatico in dotazione.

1: Formazione e informazione

•La diffusione dell'utilizzo degli strumenti informatici non è andata di pari passo con l'acculturamento informatico della società.
•Siamo dei cliccatori compulsivi: **Avanti-Avanti-Fine** non e' « saper usare un computer »
•Il lato più vulnerabile di un sistema informatico è la persona alla tastiera.

Apprendere poche indispensabili nozioni tecniche ci rende più consapevoli sui processi che svolgiamo con il computer e sui rischi correlati.

Tecnologia e buon senso

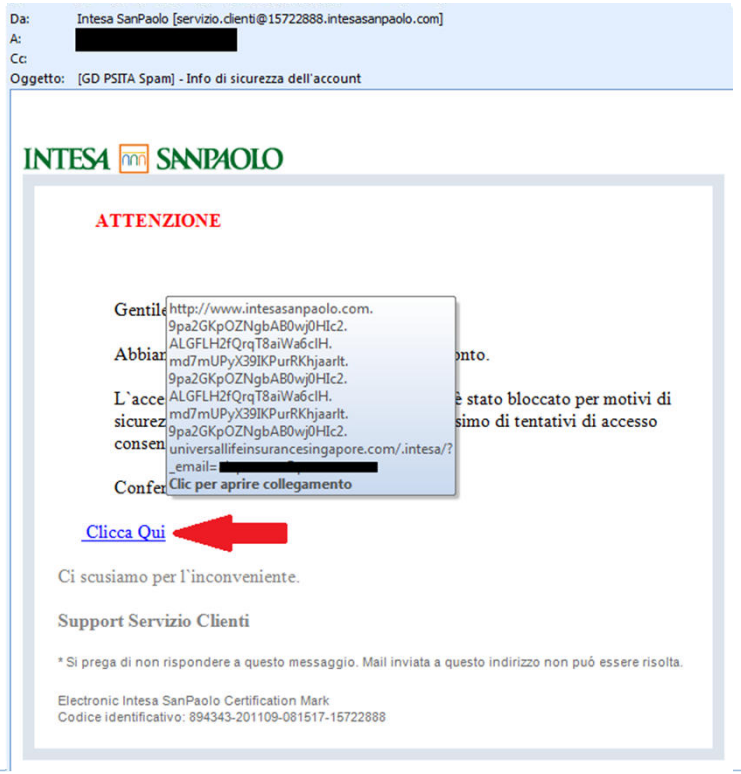
Mai mettere i "delicati" a 90° in lavatrice

Ingegneria Sociale

Insieme di tecniche psicologiche e di imbrogli «ad arte» eseguiti allo scopo di ottenere informazioni confidenziali e far eseguire azioni ingannando le persone.

- Siamo eccessivamente fiduciosi
- Attribuiamo erroneamente eccessiva autorità a persone o a comunicazioni falsamente formali
- Non siamo abbastanza "paranoici"
- Non siamo formati
- Non applichiamo il buon senso

Che credibilità ha questa mail?



Da: Intesa SanPaolo [servizio.clienti@15722888.intesasanpaolo.com]
A: [redacted]
Cc:
Oggetto: [GD PSITA Spam] - Info di sicurezza dell'account

INTESA SANPAOLO

ATTENZIONE

Gentile

http://www.intesasanpaolo.com.
9pa2GKpOZNgbAB0wj0HIc2.
ALGFLH2fQrqT8aiWa6cIH.
md7mUPyX39IKPurRKhjaarIt.
9pa2GKpOZNgbAB0wj0HIc2.
ALGFLH2fQrqT8aiWa6cIH.
md7mUPyX39IKPurRKhjaarIt.
9pa2GKpOZNgbAB0wj0HIc2.
universallifeinsurancesingapore.com/.intesa/?
_email=[redacted]
Clic per aprire collegamento

Abbiar onto.

L`acce è stato bloccato per motivi di
sicurez simo di tentativi di accesso
consen

Confer

Clicca Qui

Ci scusiamo per l'inconveniente.

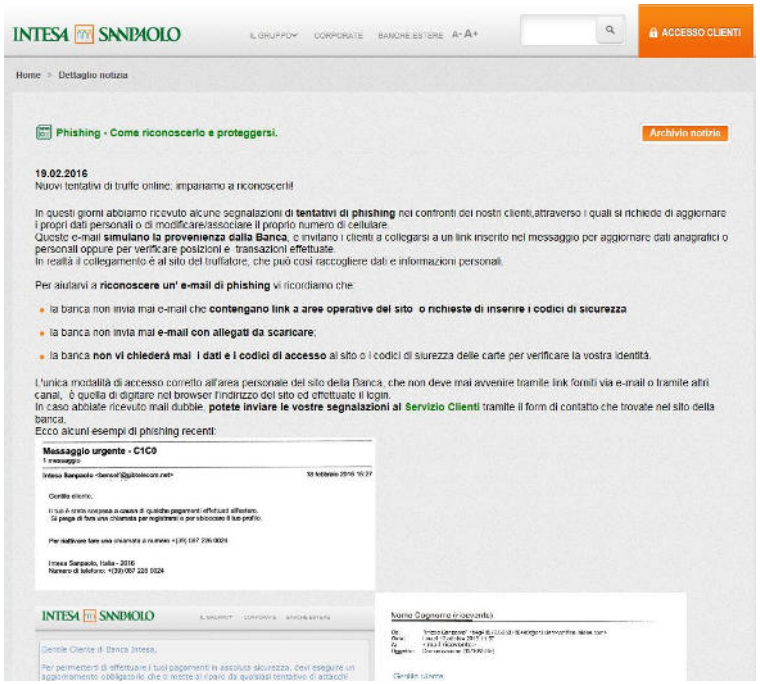
Support Servizio Clienti

* Si prega di non rispondere a questo messaggio. Mail inviata a questo indirizzo non puó essere risolta.

Electronic Intesa SanPaolo Certification Mark
Codice identificativo: 894343-201109-081517-15722888

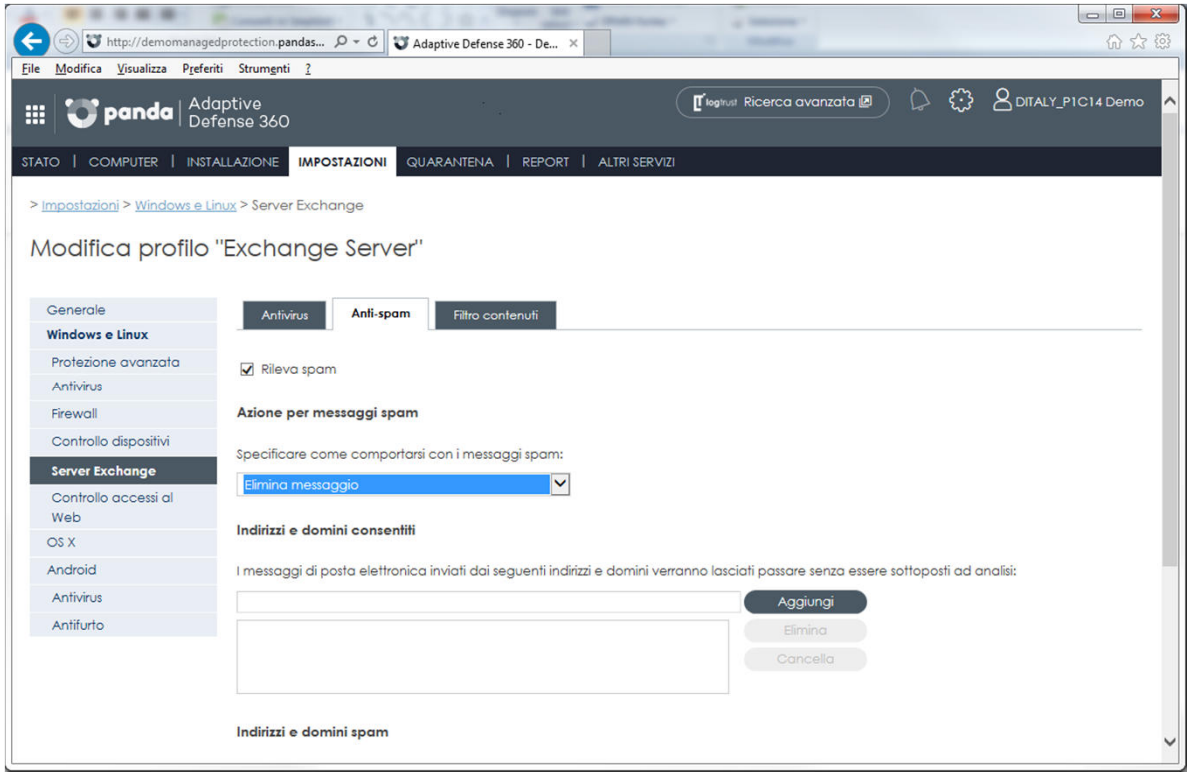
Eppure l'informazione c'è…

fonte: http://www.intesasanpaolo.com/info/sicurezza.jsp



Una prima linea di difesa: l'antispam

Coadiuva l'antivirus per bloccare sia le mail con allegati infetti sia quelle con contenuti inattendibili e fraudolenti



"Ma se io non ho un server Exchange?"

Panda Email Protection

Soluzione Cloud-Based per la protezione del traffico di posta elettronica, indpendente dal tipo di server di posta.

Cosa vi insospettisce in questi nomi di file?

FATTURA

FATTURA.PDF

Se il nome di un allegato di posta elettronica che avete ricevuto è "**FATTURA.PDF**" anziché "**FATTURA**", come siete normalmente abituati a vedere, va tutto bene? Aprirete l'allegato?

Il caro vecchio DOS

NOMEFILE.EXT: formato 8+3, otto caratteri per il nome del file e tre per l'estensione che ne identifica il tipo (**DOC**, **XLS**, **PDF**, **EXE** ecc….) separati da un punto "." che è un carattere riservato.

E poi arrivo' Windows 95…

"**Questo è il nome di un file perfettamente lecito, è la fattura n.665 del 13.07.2015.PDF**"

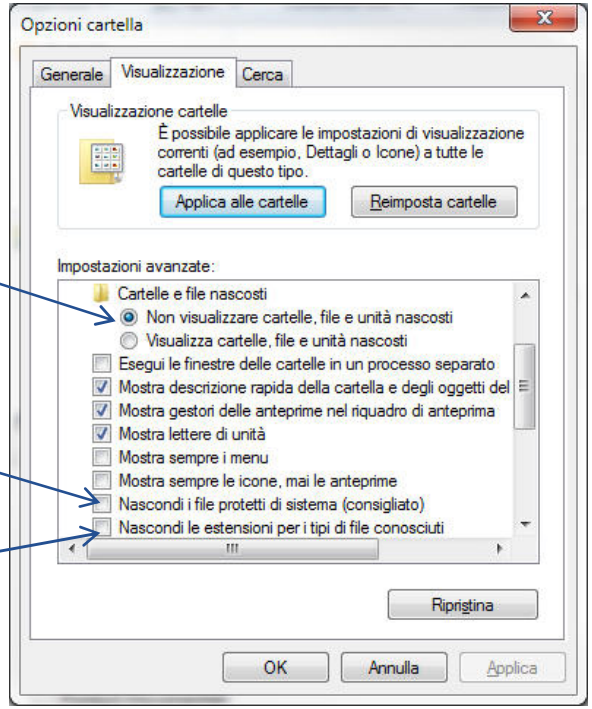
Il nome del file può arrivare a 254 caratteri e il punto "." può far parte del nome del file.
L'ultimo punto separa l'estensione, che non e' vincolata a tre caratteri (es. **DOCX**, **XLSX**, ecc)

… con la possibilità di nascondere le estensioni, e non solo quelle…

1: i file nascosti non vengono visualizzati

2: i file di sistema non vengono visualizzati

3: le estensioni note non vengono visualizzate



… col risultato di farvi recapitare un bel

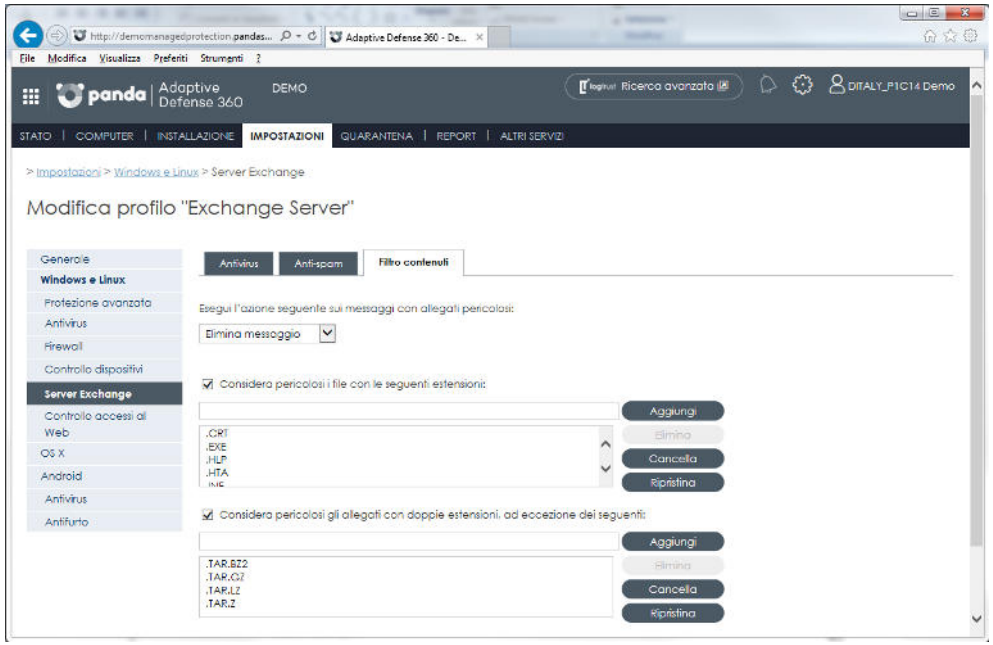
FALSO_DOCUMENTO.PDF

che in realtà è un:

FALSO_DOCUMENTO.PDF tanti spazi **.EXE**

Un’altra linea di difesa: il Content Filter

Impedisce il recapito di mail con allegati dai **formati** indesiderati perché potenzialmente pericolosi.

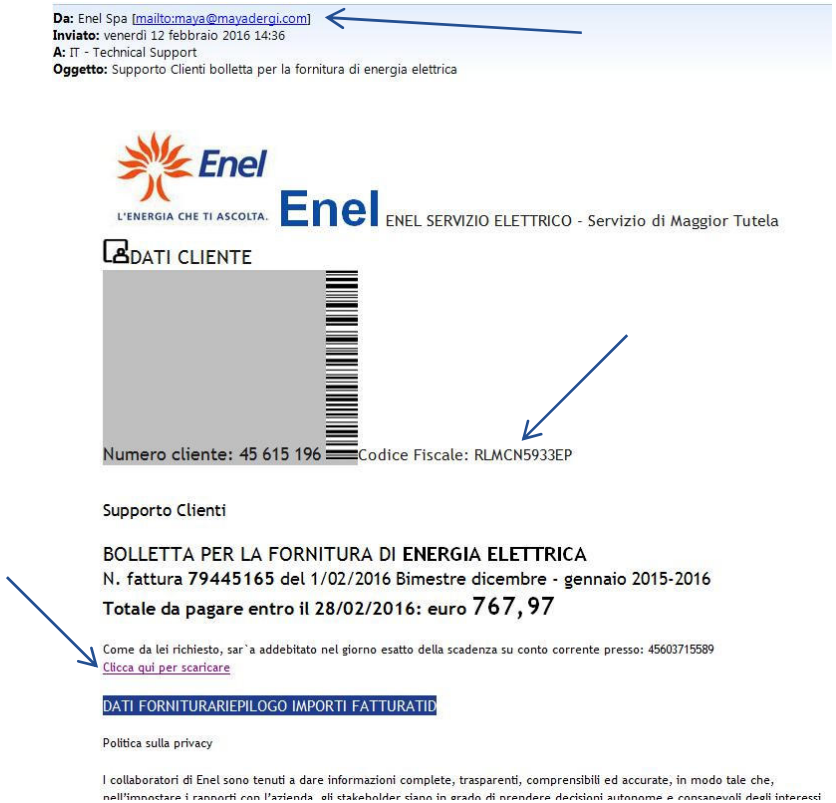


Panda Adaptive Defense 360, Panda Email Protection, Panda Gatedefender

Qualcosa può sempre passare tra le maglie, non facciamoci ingannare…

La mail è poco attendibile.
La stiamo aspettando davvero?
Il mittente è falso.
Il codice fiscale è errato.
Il link punta a un sito fake che vi convince a scaricare un file eseguibile… **Cryptolocker**!

Esempi recenti e meno recenti:
ENEL, DHL, SDA, ecc…



Da: Enel Spa [mailto:maya@mayadergi.com]
Inviato: venerdì 12 febbraio 2016 14:36
A: IT - Technical Support
Oggetto: Supporto Clienti bolletta per la fornitura di energia elettrica

Enel
L'ENERGIA CHE TI ASCOLTA.
Enel ENEL SERVIZIO ELETTRICO - Servizio di Maggior Tutela

DATI CLIENTE

Numero cliente: 45 615 196 Codice Fiscale: RLMCN5933EP

Supporto Clienti

BOLLETTA PER LA FORNITURA DI **ENERGIA ELETTRICA**
N. fattura **79445165** del 1/02/2016 Bimestre dicembre - gennaio 2015-2016
Totale da pagare entro il 28/02/2016: euro 767,97

Come da lei richiesto, sar`a addebitato nel giorno esatto della scadenza su conto corrente presso: 45603715589
Clicca qui per scaricare

DATI FORNITURARIEPILOGO IMPORTI FATTURATID

Politica sulla privacy

I collaboratori di Enel sono tenuti a dare informazioni complete, trasparenti, comprensibili ed accurate, in modo tale che,

Non occorre ricordare cos'è Cryptolocker, vero?

Milano, 9 dicembre 2014 - I Trojan della famiglia **Cryptolocker** continuano a colpire computer di utenti domestici, Soho, PMI e Enterprise mediante tecniche di Ingegneria Sociale, ovvero tramite l'invio di email che invitano l'ignaro utente ad aprire un allegato o, più recentemente, a scaricare un file che appare come un documento PDF, ma che in realtà è un file eseguibile.

Questo codice include la tecnica del "riscatto", caratteristica degli esemplari ransomware, che rende illeggibili, se non attraverso una procedura di decriptazione possibile soltanto ai cyber criminali responsabili dell'attacco, tutti i documenti presenti sul computer colpito e sugli altri dispositivi collegati in rete. A questo punto avviene il ricatto, attraverso una schermata che richiede il pagamento di una somma di danaro di alcune centinaia di euro per riottenere i propri documenti.

(estratto da un comunicato stampa di Panda Security)

Invece va ricordato che Cryptolocker NON E' UN VIRUS

Un virus informatico si propaga autonomamente, ma le sue caratteristiche sono intercettabili da diverse tecnologie di sicurezza.

Cryptolocker viene scaricato e lanciato dall'utente, usa routine di crittografia presenti nel sistema operativo, cifra tutti i file di dati de formati piu' frequentemente usati con una chiave scaricata da Internet, lascia una richiesta di riscatto e si cancella.

Non è un'infezione! E' disattenzione!

Una terza linea di difesa: l'URL Filter

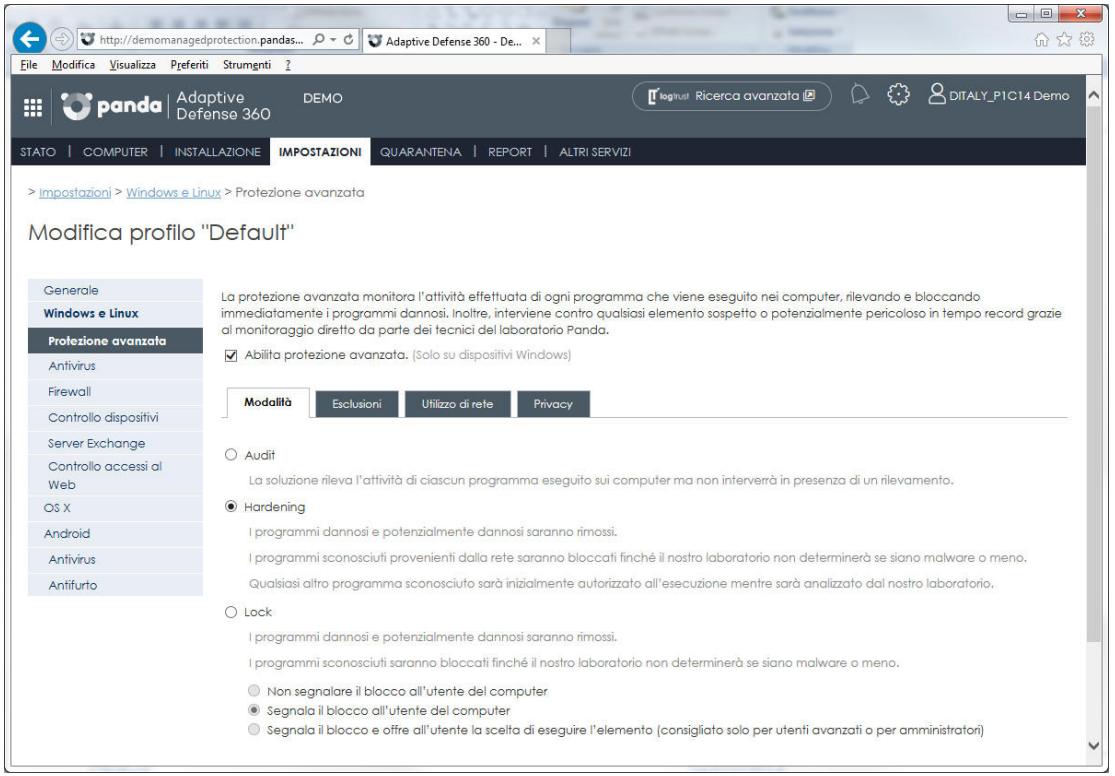
Impedisce la navigazione sia sui siti fake che su quelli i cui contenuti sono inappropriati, non di interesse aziendale e lesivi della produttività.

Panda Adaptive Defense 360, Panda Gatedefender

Abbiamo messo in opera un setaccio che protegge il punto di accesso più critico di un sistema informativo, l'accesso a Internet.

Ma se abbiamo a che fare con un contenuto che è passato attraverso il setaccio (non possiamo bloccare proprio tutto, dobbiamo pur lavorare), oppure inserito con una chiavetta USB?

L'estrema linea di difesa: la Protezione Adattiva



Panda Adaptive Defense 360 è una soluzione che protegge gli Endpoint contro qualsiasi Malware perché, diversamente da un antivirus che blocca solo oggetti noti come pericolosi, **non permette l'esecuzione di programmi sconosciuti** finchè essi non vengano automaticamente classificati come Goodware o Malware, in modo completamente automatico.

Un riassunto delle tecnologie

… e abbiamo finito…


CAROSELLO

	PRODUCT	DESCRIPTION	TARGET	MAIN FUNCTIONALITIES
Cloud-based product/service	Adaptive Defense	Panda managed service that ensures security of all running applications	KA (>1000)	• Protection against targeted attacks. • Monitoring of running applications. • Blocking of unauthorized programs. • Centralized administration from Web console. • Forensic reports. • Daily and on-demand reports.
	Endpoint protection	Cloud-based cross-platform protection for all the endpoints. Light, safe and simple complete solution.	SoHo (6-25) SB (26-100) MB (100-1000)	• Complete Anti-malware protection. • Advanced disinfection & remediation tools. • Managed and centralized firewall. • IDS/IPS. • Device Control. • Centralized Cloud console and Reporting.
	Endpoint protection plus	Security and productivity control from the cloud for all endpoints and Exchange servers.	SoHo (6-25) SB (26-100) MB (100-1000)	All above plus: • Integrated Exchange Anti-virus & Anti-spam. • Web monitoring & URL filtering.
	Systems management	Cloud-based Remote Management and Monitoring tool that lets SMBs manage, monitor and support their IT systems simply from anywhere.	SoHo (6-25) SB (26-100) MB (100-1000)	• HW & SW inventory and audit. • Agent and agent-less monitoring. • Task automation & scripting. • Patch Management. • Centralized SW deployment. • Non intrusive remote support. • Reporting.
	Fusion	Integrated solution that provides security, IT management and remote support for all the devices in the network.	SoHo (6-25) SB (26-100) MB (100-1000)	All above: • Panda Endpoint protection plus. • Panda Systems Management.
	Email protection	SaaS email Anti-malware and Anti-spam protection.	MB (100-1000) KA (>1000)	• Anti-virus & Anti-spam. • Content filtering. • Uninterrupted web mail access. • Complete backup of inbound mail.
Appliance	Gatedefender	UTM appliance family that provides a complete and flexible perimeter security for corporate networks.	SB (26-100) MB (100-1000) KA (>1000)	• Anti-malware protection. • Firewall and IPS. • Anti-spam filtering. • Application firewall. • Web filtering and Proxy cache. • Bandwidth control.

Il coordinamento delle azioni di diverse tecnologie di sicurezza permette di proteggere la propria attività contro gli attacchi informatici.
Panda Security vi mette a disposizione questi strumenti.

	Antivirus File	Firewall	Device Control	Antivirus allegati	Antispam	Content Filter	URL Filter	Adaptive
Panda Adaptive Defense 360	X	X	X	X	X	X	X	X
Panda Email Protection				X	X	X		
Panda Gatedefender		X		X	X	X		

Panda Security International *(www.pandasecurity.com), fondata nel 1990, è una multinazionale specializzata in soluzioni di sicurezza basate su cloud, disponibili in oltre 14 lingue per i milioni di utenti distribuiti in 195 paesi nel mondo. Panda Security è stata la prima azienda di sicurezza IT a sfruttare la potenza del cloud computing con la tecnologia dell'Intelligenza Collettiva. Questo modello di protezione innovativo è in grado di analizzare e classificare in modo automatico migliaia di nuovi esemplari di malware ogni giorno, garantendo ai clienti aziendali e domestici la protezione più efficace dalle minacce di Internet, con un impatto minimo sulle performance di sistema. Panda Security è presente con 80 sedi nel mondo, un headquarter in Florida, negli Stati Uniti e uno in Europa, situato in Spagna.*

Grazie!

pandasecurity.com