COME PROTEGGERE L'AZIENDA NELL'ERA DEL RANSOWMARE?

Claudio Panerai, CTO
claudio.panerai@achab.it

s|e s

ACHAB
Distribuiamo software e sicurezza

CHI DI VOI HA L'ANTIVIRUS?

s|e s

ACHAB
Distribuiamo software e serenità

Eppure…

R.it | Sicurezza

Cybercrimine, il nostro anno peggiore: rapporto Clusit 2017, l'Italia preda degli hacker

Per la prima volta siamo nella top ten globale per numero di vittime, Il Paese è nella morsa dei ransomware

social engineering hanno fatto +1.166%.

Kaspersky Lab: nel 2016 un attacco ransomware a un'azienda ogni 40 secondi

sies

ACHAB
Distribuiamo software e sicurezza

Perché?

Antivirus = vaccino

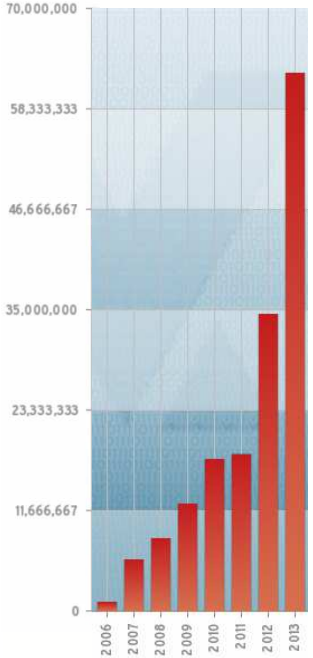
98%

delle infezioni
raggiunge 1 solo PC

…ma le malattie rare?

Corsa a inseguimento…

L’antivirus basato su firme è «morto»



Gli antivirus non reggono il ciclo virus-firme-rilascio

- firme richiedono “campioni” per l’analisi
- la maggior parte del malware colpisce “pochi” pc

Gli attacchi sono sofisticati e intelligenti

- sfruttano exploit zero-day
- si comprano programmi per generare virus e varianti

Serve una difesa diversa!

Esiste!!!

- Senza firme
  cioè sempre aggiornato
- Real-Time System Shield
  analisi comportamentale e protezione da malware in tempo reale
- Zero-day Shield
  azione immediate contro polimorfismi e multimorfismi
- Real-Time Anti-Phishing Shield
  99% di precisione contro siti di pishing
- Pesa < 1MB e si installa in 15 secondi

s|e s

ACHAB
Distribuiamo software e serenità

Dove trovarlo

WEBROOT®

Antivirus/antimalwar

- ✓ senza
- ✓ Sempr
- ✓ ultra ve

Area espositiva DESK SIES

sies

ACHAB
Distribuiamo software e sicurezza

E' evidente a tutti che gli antivirus, anche i migliori, non sono sufficienti.

Serve uno strato di protezione ulteriore, perché il vero costo di un incidente informatico per un'azienda non è il costo dei tecnici che devono rimettere in piedi un sistema, auspicando che ci siano i backup e i dati siano integri.

Il costo è il fermo dei sistemi aziendali, i sistemi che consentono alle aziende di lavorare e produrre reddito.

Un esempio: la ruota di scorta

A ognuno la sua

Tre parametri importanti

- Danno dell'interruzione
- Probabilità dell'interruzione
- Costo della contromisura

Ma che cosa può interrompere
il funzionamento del sistema IT?

Quali sono i **disastri**?

Terremoti

Finale Emilia,
29/05/2012

Allagamenti

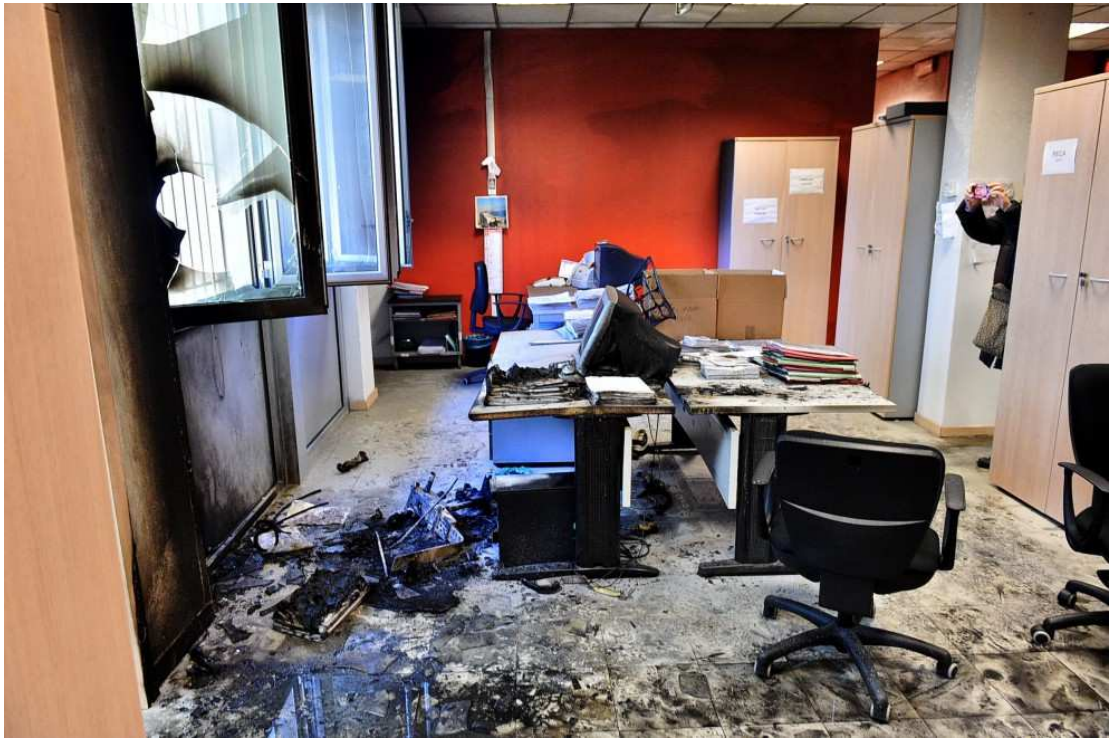
Genova,
10/10/2014

Trombe d’aria

Torino,

3/7/2016

Incendi



Milano,

19/11/2014

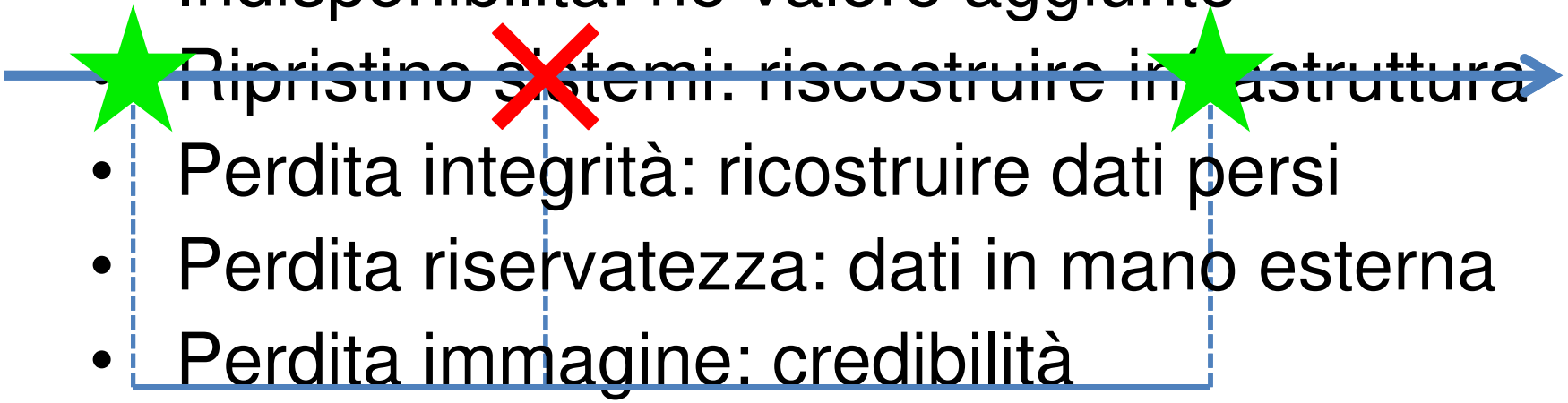
Altre cause, ben più frequenti

- Furti
- Guasti hardware (disco, alimentatore)
- Problemi software (aggiornamenti, corruzione di file)
- Cancellazione di file (colposa o dolosa)
- Virus (ransomware)

Anatomia di un disastro

Disastro, quali sono i danni

- Improduttività: struttura pagata per niente
- Indisponibilità: no valore aggiunto
- Ripristino sistemi: ricostruire infrastruttura
- Perdita integrità: ricostruire dati persi
- Perdita riservatezza: dati in mano esterna
- Perdita immagine: credibilità
- www.achab.it/costoincidenteIT



Ma non basta il backup?

No!

Siamo più precisi…

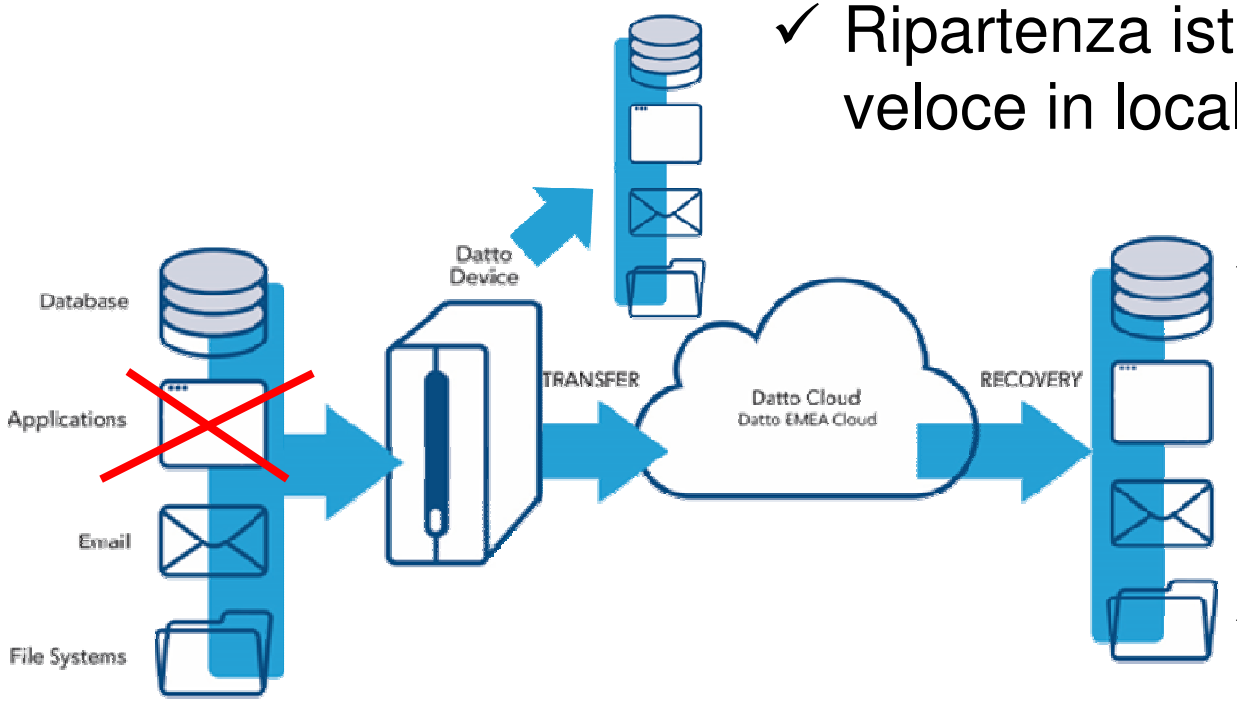
- Certezza del tempo di ripartenza (prove)
- Verifica successo e integrità dei dati
- Perdita di dati accettabile
- Copia (integra) fuori sede

s|e s

ACHAB
Distribuiamo software e serenità

Come risolviamo il problema?

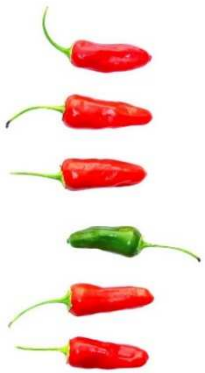
Business continuity «al volo»



- ✓ Ripartenza istantanea, facile e veloce in locale
- ✓ Riparenza istant. da remoto
- ✓ Protezione mista:
  - locale (on premise)
  - remota (cloud)

Rivolgendomi ai più tecnici

- ✓ Protezione basata su immagini, anche ogni 5 minuti
- ✓ garanzia di ripartenza
  (anche applicativa)
- ✓ virtualizzazione istantanea in locale
  (anche se non hai cluster o muletto)
- ✓ replica + accensione in remoto dei sistemi.
  (anche se non possiedi un datacenter tuo)



s|es

ACHAB
Distribuiamo software e serenità

LA SOLUZIONE E' UN INSIEME DI PROCESSI

1. Antivirus buono e sempre aggiornato

10. Backup e test del restore per essere pronti a ripartire…

LA SOLUZIONE E' UN INSIEME DI PROCESSI

1. Antivirus buono e sempre aggiornato
2. Patch di sicurezza sui sistemi (Windows e non)
3. Plugin, utility e applicazioni aggiornate (Flash, Adobe, ecc)
4. Applicare policy affinché utenti non siano admin
5. Bloccare «cose particolari» (Temp, appdata, ecc)
6. Filtri sull'email prima che arrivino alla inbox
7. Disabilitare VBS e Powershell (e macro di Office)
8. Accurato controllo sui permessi di rete
9. Fermare l'infezione sul nascere: scollegare il server dalla rete
10. Backup e test del restore per essere pronti a ripartire…

CONCLUSIONI

La soluzione al ransomware è un insieme di **processi** (e pagare il riscatto non è una soluzione)

Dobbiamo implementare best practice per ridurre al minimo il rischio di infezione

Dobbiamo essere pronti a ripartire nel caso in cui accada l'irreparabile

Agire in maniera **sistematica** come in un processo **industriale**.

s|es

ACHAB
Distribuiamo software e serenità

Vogliamo approfondire?

WEBROOT®

Antivirus/antimalwar

- ✓ senza
- ✓ ultra v
- ✓ ultra le

datto

R/BC

- ✓ za istantanea
- ✓ arriva dove gli altri non ce la fanno

Area espositiva DESK SIES

s|e s

ACHAB
Distribuiamo software e serenità