LO STATO DEL RANSOMWARE IN ITALIA

Visto da chi si occupa di IT

datto WEBROOT

ACHAB
Distribuiamo software e serenità

INTRODUZIONE

Questo report fornisce una panoramica dello stato del ransomware in Italia, visto dalla parte del canale.

Se cerchi su Google «CryptoLocker» o «ransomware», l'attacco informatico che consiste nel cifrare e tenere in «ostaggio» i dati delle aziende finché non viene pagato un riscatto, troverai moltissimi articoli e statistiche che hanno una conclusione comune: il malware, e il ransomware in particolare, è diventato il più diffuso e globale problema da risolvere per chi si occupa di sicurezza.

Per come i dati oggi vengono trattati in azienda e per la centralità del dato in ogni tipo di attività, il ransomware ha la capacità di distruggere aziende, anche grandi, nel giro di pochi minuti. E benché alcune aziende inizino a utilizzare sistemi antivirus di nuova generazione e soluzioni di business continuity, la verità è che la maggior parte delle imprese non sono preparate per attacchi di questo tipo.

E questo è maggiormente vero nel mercato delle piccole e medie imprese dove spesso non c'è un informatico dedicato a gestire l'IT e dove spesso si utilizzano sistemi informatici «vecchi». La verità è che queste realtà fanno affidamento ai propri dati per lavorare né più né meno delle multinazionali, ma a differenza di queste ultime non hanno gli strumenti, la protezione e la preparazione per difendersi e reagire ad attacchi di ransomware.

I cybercriminali oggi sono consapevoli di questa situazione e ne approfittano guadagnando miliardi di dollari. Sì, miliardi!
E il downtime dovuto al ransomware alle aziende costa migliaia di euro. I numeri che circolano sui report ufficiali, come quelli del Clusit, nella realtà sono molto più drammatici perché solo una minoranza degli attacchi viene denunciata alle autorità.

Per essere pronti a resistere ad attacchi come quelli del ransomware è necessario innanzitutto che le imprese siano consapevoli di questi rischi, e solo in seguito possono provvedere a mettere in atto best practice e sistemi di ripartenza dopo gli attacchi affidandosi a fornitori di serviti IT e consulenti preparati.

Per il secondo consecutivo Achab ha condotto un'indagine alla quale hanno preso parte oltre 150 fornitori di servizi IT che hanno dichiarato le loro esperienze in merito agli attacchi ransomware.

datto WEBROOT

ACHAB
Distribuiamo software e serenità

LA SITUAZIONE A COLPO D'OCCHIO 1/2

- **Il pericolo numero uno è il ransomware in tutto il mondo.** Si stima che il 5% delle PMI a livello mondiale abbia subito attacchi ransomware. In Italia quasi li 90% degli MSP intervistati ha eseguito interventi in seguito ad attacchi ransomware negli ultimi 2 anni. E oltre il 30% ha dovuto eseguire 5 o più interventi nel solo 2017.
- **Il ransomware continuerà ad aumentare e mietere vittime.** Oltre l'80% degli MSP dichiara che il ransomware è destinato ad aumentare dei prossimi 12 mesi e il 19% di questi pensano che aumenterà in modo significativo.
- **Aumenta il numero di denunce e diminuiscono le aziende che pagano il riscatto.** Il 40% de partecipanti al sondaggio ha denunciato almeno una volta alle autorità l'attacco, un balzo in avanti rispetto alla precedente edizione del sondaggio da cui emergeva che solo il 25% aveva fatto denuncia. Inoltre la percentuale di chi è stato disponibile a pagare almeno una volta il ricatto è calata dal 37% al 24%. E di questi il 9% non è comunque riuscito a recuperare i dati.
- **Il riscatto chiesto dal ransomware non manda in bancarotta le aziende. Sono il downtime e la perdita di dati a creare i veri danni.** Quasi il 90% degli MSP dichiara che i propri clienti hanno subito downtime e quasi il 50% ha subito delle perdite di dati.
- **Il ransomware moderno non risparmia niente e nessuno.** Tutte le aziende vengono attaccate, indipendentemente dai sistemi di sicurezza messi in atto e una vola entrato il ransomware cifra tutto quello che trova: il 38% degli intervistati dichiara di aver visto cifrare anche i backup.

LA SITUAZIONE A COLPO D'OCCHIO 2/2

- **CryptoLocker continua ad essere l'infezione più diffusa, ma nuove ed aggressive varianti spuntano come funghi ogni giorno.** Il 67% degli MSP che hanno fronteggiato il ransomware dichiara di aver avuto a che fare con CryptoLocker. Ma non mancano segnalazioni di attacchi di Locky, CryptWall e WannaCry (new entry!).
- **Nessuna azienda, sistema operativo, dispositivo o piattaforma cloud è al sicuro dagli attacchi.** Non esiste sistema o tecnologia immune. Le applicazioni cloud (SaaS) continuano a crescere come bersaglio del ransomware: se Dropbox è il più attaccato anche gli utilizzatori di OneDrive/GDrive non possono dormire sonni tranquilli. Ma sono in aumento anche le infezioni in ambienti Mac, Linux, tablet e smartphone.
- **Quando si parla di consapevolezza dei danno da ransomware, le aziende, la maggior parte brancola nel buio.** Benché tutti i fornitori di servizi IT siano consapevoli del problema ransomware, solo il 12% delle imprese è pienamente consapevole dei possibili danni. Questo potrebbe spiegare la (tuttora) carenza di formazione sulla cybersecurity per il personale, segnalata dagli MSP come una delle principali cause di infezione.
- **Il ransomware «buca» le attuali soluzioni di sicurezza, quindi il backup è fondamentale.** Gli MSP dichiarano che le infezioni ransomware avvengono nonostante la presenza di Antivirus, filtri Antispam sulla email, Ad Blockers, e nonostante i sistemi fossero aggiornati. La soluzione più efficace per proteggere le aziende dal ransomware, oggi, è un sistema di backup e disaster recovery seguito da training sulla cybersecurity.
- **Grazie a soluzioni affidabili di backup e disaster recovery, gli MSP riescono a ripartire velocemente dopo un'attacco ransomware.** Con un'affidabile soluzione di backup e recovery in piedi, il 90% degli MSP dichiara di essere riuscito a ripartire velocemente e senza perdite in seguito a attacchi ransomware.

IL PROBLEMA DI SICUREZZA #1 AL MONDO: IL RANSOMWARE

Si stima che **il 5% DI TUTTE LE PMI** del pianeta abbiano **SUBITO UN ATTACCO RANSOMWARE** fra il 2016 e il 2017

datto WEBROOT

ACHAB
Distribuiamo software e serenità

GLI ATTACCHI RANSOMWARE SONO DESTINATI AD AUMENTARE

81%

PREVEDE CHE IL RANSOMWARE CONTINUERÀ AD AUMENTARE NEI PROSSIMI 12 MESI.

Di questi, il **19%**

RITIENE CHE IL RANSOMWARE AUMENTERÀ DRAMMATICAMENTE.

datto WEBROOT

ACHAB
Distribuiamo software e serenità

NON È PIÙ UNA QUESTIONE DI «SE»
MA DI «QUANDO»

89% MSP

HA AVUTO CLIENTI COLPITI DA RANSOMWARE NEL 2016-2017.

31%

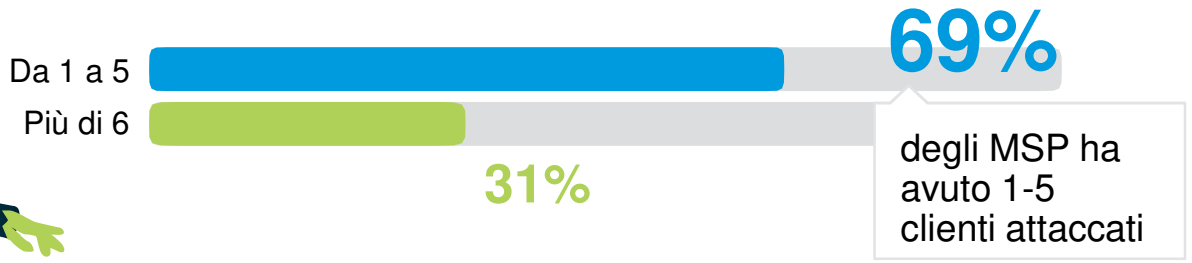
DEGLI MSP HA DOVUTO AFFRONTARE **PIÙ DI 5 ATTACCHI** NEL 2017.

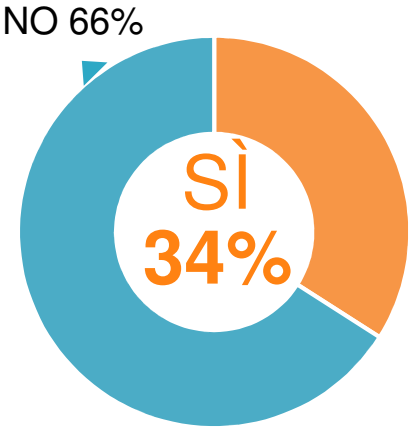
datto WEBROOT

ACHAB
Distribuiamo software e serenità

IL RANSOMWARE È UN'EPIDEMIA CHE SI DIFFONDE A MACCHIA D'OLIO

Quanti clienti sono stati attaccati dal ransomware?





Un drammatico **34%** ha affrontato **attacchi multipli** nella stessa giornata.

datto WEBROOT

ACHAB
Distribuiamo software e serenità

AUMENTANO LE DENUNCE ALL'AUTORITÀ

IL **40%**

HA DENUNCIATO ALMENO UNA VOLTA ALLE AUTORITÀ.

NETTO AUMENTO RISPETTO AL 25% DEL PRECEDENTE SONDAGGIO

datto WEBROOT

ACHAB
Distribuiamo software e serenità

DIMINUISCE IL NUMERO DI CHI PAGA IL RISCATTO

34% DICHIARA DI AVER PAGATO IL RISCATTO ALMENO UNA VOLTA

DATO IN DIMINUIZIONE RISPETTO AL PRECEDENTE SONDAGGIO.

2016: **37%**

2017: **34%**

Di quelli che hanno pagato, il **9%**

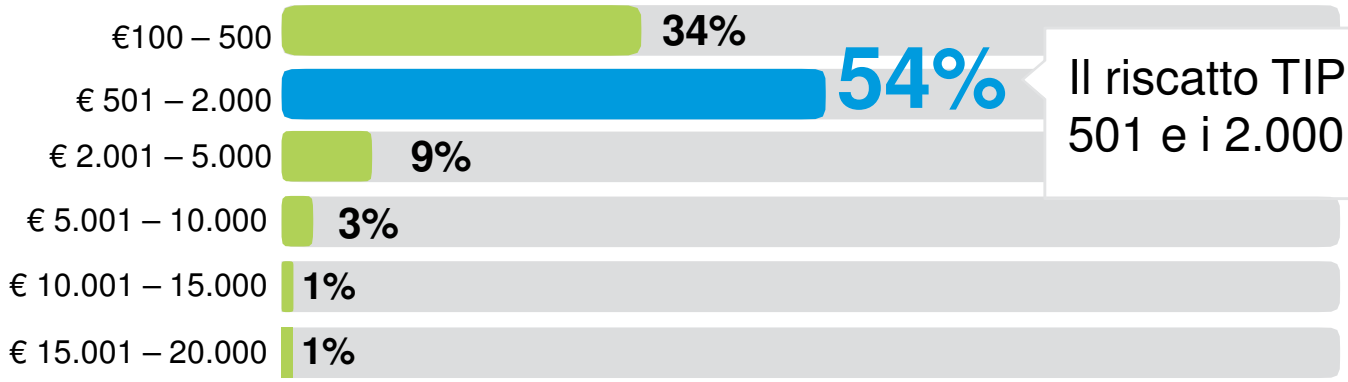
NON È RIUSCITO A RECUPERARE I DATI

datto WEBROOT

ACHAB
Distribuiamo software e serenità

NON È IL RISCATTO CHE MANDA IN BANCAROTTA LE AZIENDE

Qual è il valore del riscatto (medio) richiesto?



Il riscatto TIPICO è fra i 501 e i 2.000 euro.

datto WEBROOT

ACHAB
Distribuiamo software e serenità

IL DOWNTIME È IL PROBLEMA DEGLI ATTACCHI

Durante gli attacchi
cosa hai visto
dai tuoi clienti?

datto WEBROOT

ACHAB
Distribuiamo software e serenità

IL RANSOMWARE PRENDE DI MIRA LE PMI E CIFRA TUTTO QUELLO CHE TROVA

96% degli MSP LAVORA CON
AZIENDE FINO A 100 DIPENDENTI.

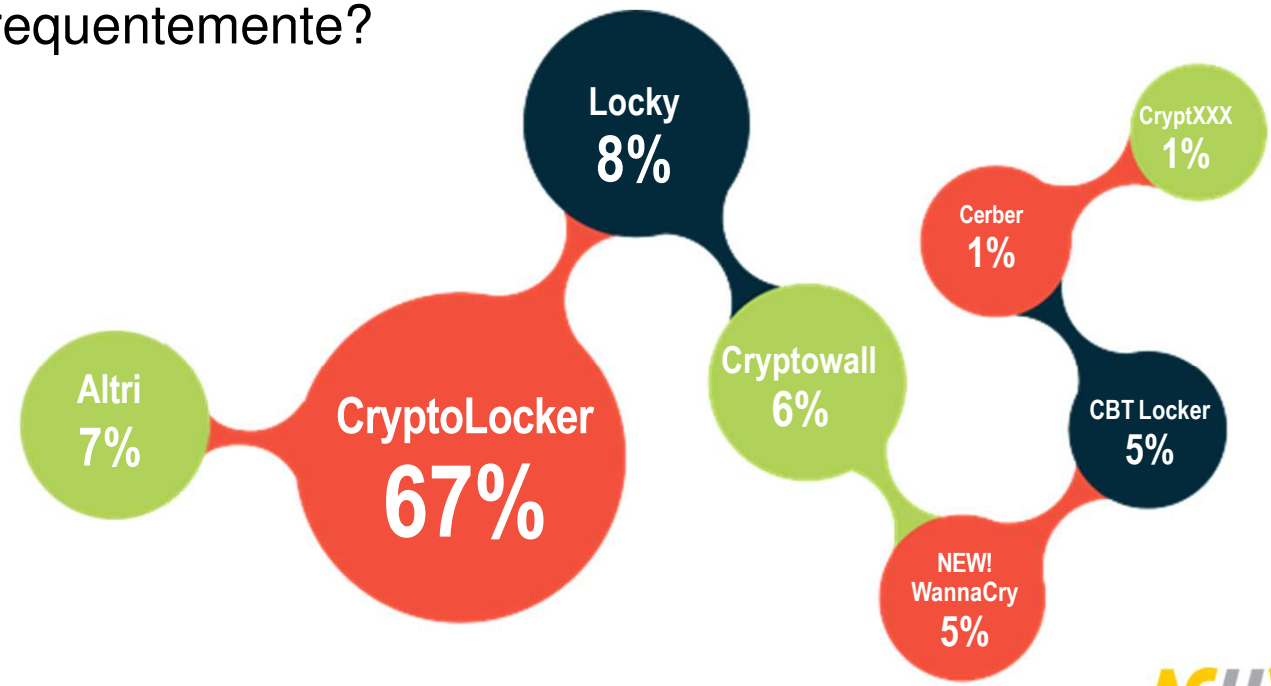
38%
DICHIARA CHE
IL RANSOMWARE HA CIFRATO ANCHE I BACKUP.

datto WEBROOT

ACHAB
Distribuiamo software e serenità

CRYPTOLOCKER RIMANE IL RE, MA ALTRI NOMI ENTRANO IN CLASSIFICA

Quale di questi ransomware hai incontrato più frequentemente?



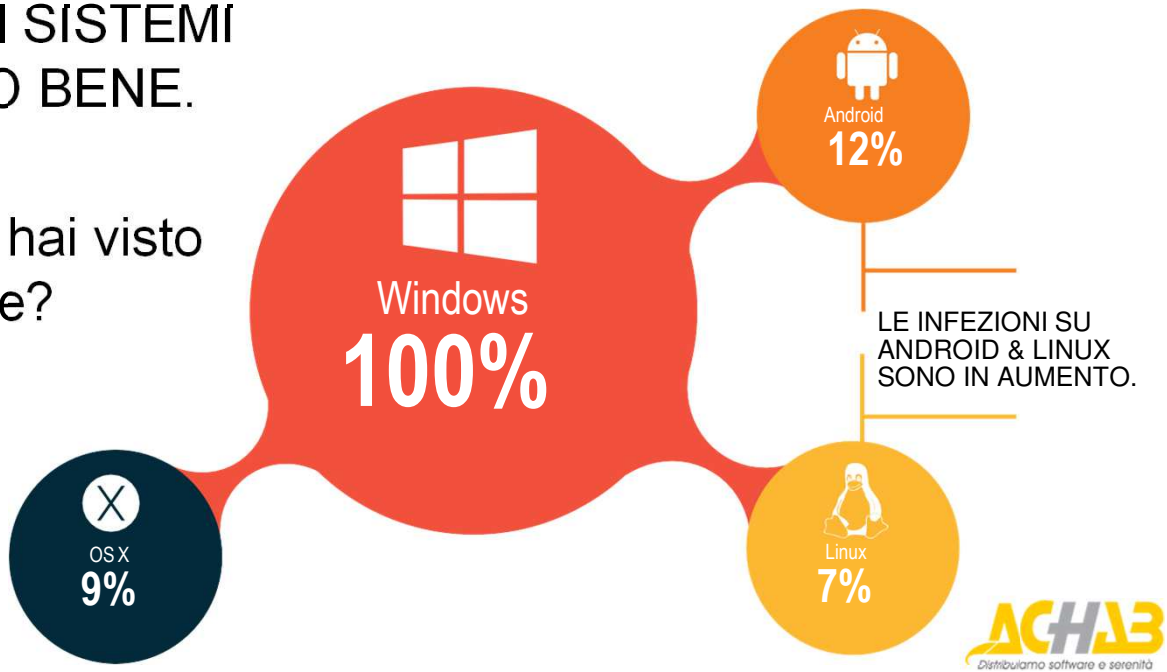
datto WEBROOT

ACHAB
Distribuiamo software e serenità

TUTTI I SISTEMI OPERATIVI SONO A RISCHIO

IL **100%** DEGLI MSP DICHIARA DI AVERE VISTO **WINDOWS ATTACCATO DAL RANSOMWARE**, MA ANCHE GLI ALTRI SISTEMI NON SE LA PASSANO BENE.

Quali sistemi operativi hai visto infettati da ransomware?



datto WEBROOT

ACHAB
Distribuiamo software e serenità

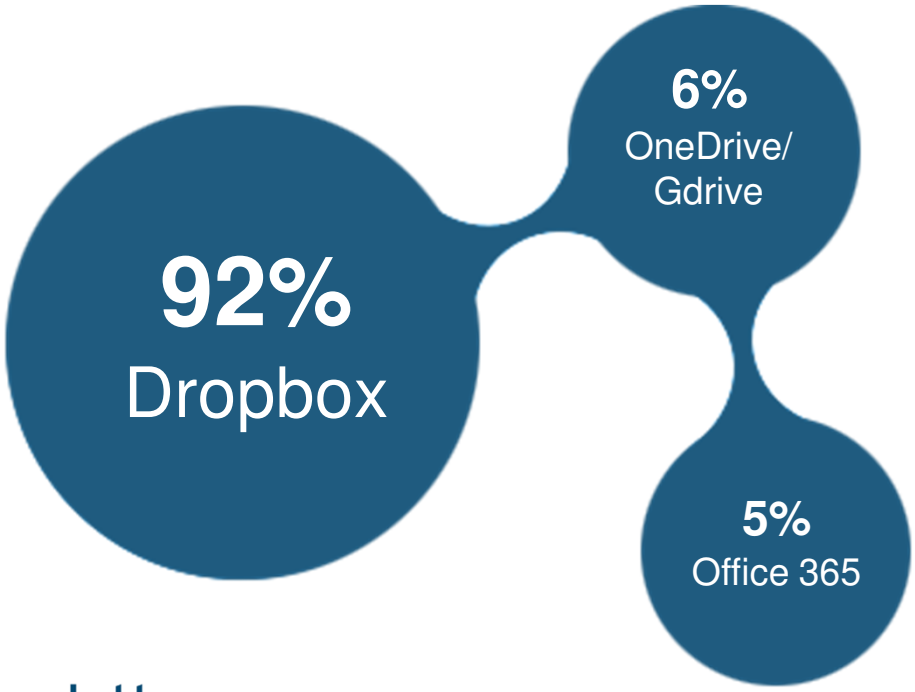
ATTACCHI RANSOWMARE SU MOBILE/TABLET INIZIANO A FARSI SENTIRE

datto WEBROOT

ACHAB
Distribuiamo software e serenità

IL CLOUD NON È IMMUNE AL RANSOMWARE

Gli MSP che hanno visto ransomware in applicazioni SaaS dicono che i sistemi più colpiti sono:

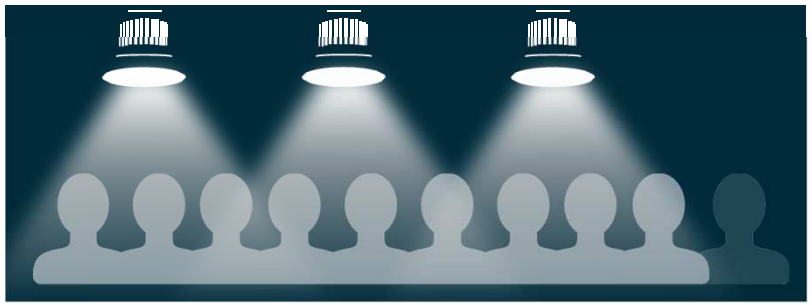


IL **38%**
DICHIARA DI AVER VISTO **ATTACCHI RANSOMWARE** ANCHE **IN APPLICAZIONI CLOUD**

datto WEBROOT

ACHAB
Distribuiamo software e serenità

LE AZIENDE SONO CONSAPEVOLI DEI RISCHI LEGATI AL RANSOMWARE?



IN PARTE O PER NULLA CONSAPEVOLI
dei rischi legati al ransomware

88%

DELLE IMPRESE

PIENAMENTE CONSAPEVOLI
dei rischi legati al ransomware

12%

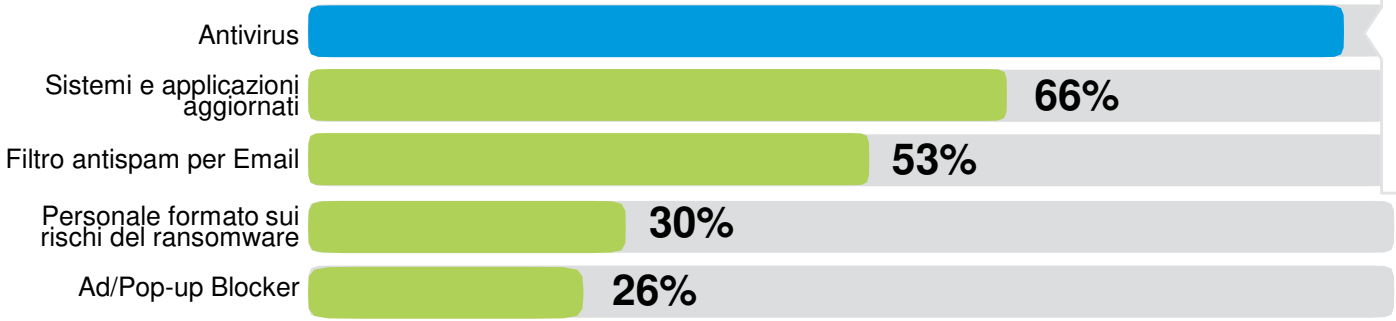
DELLE IMPRESE

datto WEBROOT

ACHAB
Distribuiamo software e serenità

LE SOLUZIONI DI CYBERSECURITY NON SONO EFFICACI CONTRO IL RANSOMWARE

Nei casi di attacco i clienti avevano implementato una o più delle seguenti misure i sicurezza?



98%

Dichiara che il ransomware ha bucato il software antivirus.

NON ESISTE UNA SINGOLA SOLUZIONE CERTA E SICURA, **PER PREVENIRE IL RANSOMWARE È NECESSARIO UN APPROCCIO MULTIVELLO ALLA SICUREZZA.**

datto WEBROOT

ACHAB
Distribuiamo software e serenità

BACKUP & DR È LA SOLUZIONE PIÙ EFFICACE CONTRO IL RANSOMWARE

Quale delle seguenti soluzioni è la più efficace in termini di protezione del business?

LA SOLUZIONE #1 PER PROTEGGERSI DAL RANSOMWARE?

BACKUP & DISASTER RECOVERY SEGUITO DALLA FORMAZIONE DEL PERSONALE E ANTIVIRUS.

datto WEBROOT

ACHAB
Distribuiamo software e serenità

CON BACKUP & DR È POSSIBILE RIPARARE VELOCEMENTE A UN ATTACCO

CON soluzioni Backup/Disaster Recovery

+90% DICHIARA UN **RIPRISTINO VELOCE**

DOPO UN ATTACCO RANSOMWARE

SENZA soluzioni Backup/Disaster Recovery

63% INCAPACE DI RIPRISTINARE VELOCEMENTE E COMPLETAMENTE

DOPO UN ATTACCO RANSOMWARE

MSP più «pronti» se hanno una soluzione di disaster recovery

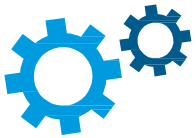
datto WEBROOT

ACHAB
Distribuiamo software e serenità

CONCLUSIONI

Le aziende devono attivare la prima linea di difesa: il personale. Le aziende devono prevedere una formazione regolare (e obbligatoria) per il proprio personale affinché questo sia in grado di individuare e evitare le email pericolose nella propria casella di posta, che resta il principale veicolo di infezione per il ransomware.

Le aziende devono lavorare su soluzioni multilvello per evitare il peggio. Le soluzioni di sicurezza presenti sul mercato non sono in grado di garantire protezione certa e sicura contro il ransomware, che riesce a penetrare le difese in modi sempre diversi. Per ridurre il rischio è necessario un approccio «a livelli» piuttosto che affidarsi a un singolo prodotto.



Le aziende devono «assicurarsi» con una soluzione di business continuity. Non esiste alcune soluzione che possa prevenire con certezza il ranswomare. È necessario focalizzarsi su come mantenere operativa l'azienda nonostante il verificarsi di un attacco ransomware. E c'è un solo modo per farlo: un soluzione di backup e recovery sicura, rapida ed efficiente.

Le aziende hanno bisogno di personale in grado di affrontare le sfide della cybersecurity per garantire la continuità del business. Le PMI spesso si affidano agli «smanettoni» per gestire la propria IT e non ai professionisti. Se un'azienda non si può permettere personale IT esperto in cybersecurity in grado di assicurare la continuità operativa 24/7, dovrebbe rivolgersi a un fornitore di servizi IT (MSP) che ha risorse e competenze per proteggere le imprese dai più recenti attacchi.

datto WEBROOT

ACHAB
Distribuiamo software e serenità

SCOPRI DI PIÙ SU COME PROTEGGERTI

Achab distribuisce software e soluzioni che permettono alle imprese italiane di costruire infrastrutture ICT flessibili, efficaci ed economicamente convenienti.
Relazione, ascolto, condivisione, coinvolgimento e spirito di gruppo sono gli ingredienti che fanno dei nostri prodotti delle vere e proprie soluzioni e che rendono la nostra offerta, un'offerta di valore.
Dalla scelta dei prodotti, alla loro commercializzazione, all'erogazione dei servizi che li completano, il nostro obiettivo è semplificare la vita di clienti, rivenditori e utenti finali, permettendo loro di lavorare meglio guadagnando di più. ***www.achab.it***

Datto, fondata nel 2007, sviluppa soluzioni innovative di backup, disaster recovery e business continuity utilizzate da migliaia di fornitori di servizi IT in tutto il mondo.
Le soluzioni Datto forniscono un sistema completo di hardware e software per la protezione delle macchine, fisiche o virtuali, e includono ripartenza in rete locale e in cloud, repliche e servizi di ripristino in caso di disaster recovery.
Il Fondatore Austin McChord è stato menzionato nella classifica di Forbes tra i migliori giovani imprenditori del pianeta. ***www.datto.com***

Webroot, fondata nel 1997, fornisce soluzioni antivirus e di sicurezza che proteggono in tempo reale dispositivi endpoint e mobili contro le minacce malware, garantendo la riservatezza e integrità dei dati aziendali.
Leggerezza, semplicità ed efficacia nel contrastare le minacce sono le caratteristiche di punta che il mercato riconosce e apprezza. ***www.webroot.com***

Achab S.p.A.

Piazza Luigi di Savoia, 2
20124 Milano

Tel. 02 54108204
info@achab.it

www.achab.it

datto WEBROOT

ACHAB
Distribuiamo software e serenità