Protezione contro WannaCry, un ransomware “arma di distruzione di massa”

Potente. Senza precedenti. Un’arma di distruzione di massa. Ecco come gli esperti di cyber security descrivono il worm ransomware, WannaCry, che ha scosso le organizzazioni di tutto il mondo. Ad oggi, sono stati danneggiati centinaia di migliaia di computer in 150 Paesi, dai sistemi di assistenza sanitaria nel Regno Unito alle università di tutta l’Asia, e la minaccia non è finita. Sono già state rilevate nuove versioni di WannaCry: varianti alle quali manca il kill switch che ha mitigato gli effetti negativi dell’originale.

Come è possibile far fronte alla minaccia WannaCry?

Correggete immediatamente la vulnerabilità di Windows

I malintenzionati hanno sfruttato la nota vulnerabilità di Microsoft, EternalBlue, sottolineando l’importanza dell’installazione immediata di patch di protezione e del mantenere aggiornati e supportati i sistemi operativi e il software.

Pertanto, si consiglia alle aziende di:

- Installare con continuità le nuove patch di sicurezza
- Aggiornare il sistema operativo Microsoft per ottenere una versione supportata
- Installare le patch sui server dell’appliance Arcserve UDP e RPS
- Bloccare i protocolli legacy, come SMBv1, per mantenerli protetti contro le future evoluzioni del malware
- Installare tempestivamente le patch di tutti i sistemi insieme all’Aggiornamento di sicurezza MS17-010 di Microsoft

Non pagate il riscatto

Nel caso di WannaCry è richiesta la decrittografia manuale da parte dell’aggressore. Data la ricerca meticolosa effettuata per individuare i responsabili, i pagamenti dei riscatti sono destinati a rimanere intatti in indirizzi Bitcoin e le richieste di decrittografia a restare senza risposta.

Detto questo, i file memorizzati al di fuori di desktop, documenti o supporti removibili possono ancora essere recuperabili tramite i tool di ‘undelete’.

Analizzate le vostre procedure di backup e di strategia per il disaster recovery

WannaCry ha evidenziato nettamente la necessità improrogabile di rimedi contro il ransomware. Pertanto, consigliamo a tutte le aziende di adottare misure immediate per avere la sicurezza di eseguire correttamente il backup e il ripristino dei dati:

- **Esaminate i requisiti di RPO e RTO.**
  Assicuratevi che i sistemi vitali siano sottoposti a backup frequenti e che il ripristino del sistema sia conforme ai requisiti del vostro business.
- **Assicuratevi che tutte le fonti di dati vengano sottoposte a backup.**
  Identificate tutti i server o le fonti di dati non inclusi nel vostro piano di protezione dati e applicate il corretto livello di disponibilità dei dati per garantire che siano recuperabili.

- **Accedete al server di backup come utente.** Quando si accede a un server sicuro, accertarsi di eseguire l'accesso come utente e non come amministratore. Non utilizzare mai l'account di amministratore quando si apre la posta elettronica o si fanno ricerche su web.
- **Proteggete il difensore.** Assicuratevi che i file di backup siano memorizzati su un server sicuro con accesso limitato solo a quelli che ne hanno assolutamente bisogno. Questi file sono la vostra migliore possibilità di recupero, quindi dovete garantire che siano sicuri.
- **La regola 3-2-1.** Effettuare almeno tre diverse copie dei dati su due diversi supporti con una copia memorizzata offsite. È di fondamentale importanza che la strategia di backup disponga di ridondanze e sfrutti le opzioni di storage non vulnerabili agli attacchi, come nastro, disco offline e cloud.
- **Praticate il principio del minimo privilegio.** Quando si configurano gli account, concedere esclusivamente i livelli di accesso realmente necessari a ciascun ruolo.

Recovery da ransomware nel mondo reale

"L'ultimo attacco ransomware è stato incredibilmente potente. Ha colpito 45 server diversi, si è diffuso ed è impazzito. Per un po' di tempo, la direzione in pratica si è trasferita nel mio ufficio, per darvi un'idea".

Con Arcserve UDP, l'amministratore di rete è stato in grado di ripristinare rapidamente il backup dalla sera precedente, evitando un riscatto di $30.000.

Eludere le richieste di riscatto con Arcserve Unified Data Protection:

Utilizzato da più di 48.000 clienti in 150 Paesi in tutto il mondo e vincitore di numerosi premi, Arcserve UDP offre funzionalità da grande azienda e la facilità di utilizzo necessaria ai team IT piccoli e oberati di lavoro.

Ottenete la flessibilità di cui avete bisogno per recuperare i dati dopo i massicci attacchi ransomware o più ordinarie catastrofi quotidiane, soddisfacendo le esigenze specifiche della vostra azienda::

- Distribuite con facilità Arcserve come software, appliance o soluzione in cloud
- Proteggete i dati fisici e virtuali, non importa dove risiedono: in locale, offsite e in cloud
- Valutate con facilità i reali obiettivi RPO e RTO, impostate test automatizzati e identificate i computer non protetti grazie alla funzionalità di Assured Recovery
- Dimensionate senza problemi la copertura delle vostre procedure di backup e recovery a mano a mano che la vostra azienda cresce: da 1TB a 1PB e oltre
- Riattivate istantaneamente le applicazioni critiche con virtual standby o Instant Virtual Machine
- Recuperate i dati da backup file-based e su immagini, o con le soluzioni a disponibilità continua

E potete fare tutto questo da un'unica console di gestione, semplice ed elegante

Assicuratevi di essere protetti

Contattate il vostro rappresentante Arcserve o chiamate il numero 800 148275 per attivarvi da subito

Per ulteriori informazioni su Arcserve, si prega di visitare il sito web **arcserve.com**