Infezione WannaCry su macchina Windows 7 in una rete aziendale

WannaCry è un ransomware che sfrutta la vulnerabilità EternalBlue nel protocollo Microsoft Windows Server Message Block (SMB) versione 1. Una volta che ha accesso a un sistema, WannaCry cripta una serie di tipi di file e presenta all'utente un messaggio che richiede un riscatto in Bitcoin per decrittare i file.

Server Message Block (SMB) consente la condivisione di file, la condivisione di stampanti, la navigazione in rete e la comunicazione tra processi (tramite pipe denominate) su una rete informatica. SMB funge da base per l'implementazione del Sistema di File Distribuito di Microsoft.

EternalBlue sfrutta una vulnerabilità nell'implementazione di Microsoft del protocollo Server Message Block (SMB). Questa vulnerabilità è indicata dalla voce CVE-2017-0144 nel catalogo Common Vulnerabilities and Exposures (CVE). La vulnerabilità esiste perché il server SMB versione 1 (SMBv1) in varie versioni di Microsoft Windows non gestisce correttamente pacchetti appositamente creati da attaccanti remoti, permettendo loro di eseguire codice a distanza sul computer bersaglio.

Misure di sicurezza per proteggere i sistemi da WannaCry:

1) Come prima cosa, è necessario disconnettere dalla rete la macchina Windows 7 infetta per evitare che il ransomware si diffonda ad altri dispositivi.

2) Successivamente, è necessario accertarsi che ilmalware non si sia già diffuso ad altri dispositivi della rete. In tal caso è necessario applicare le misure di sicurezza anche agli altri dispositivi infettati.

3) Successivamente, possono essere adottate misure di sicurezza per impedire il ripetersi della problematica:

Misure immediate e temporanee che possono essere applicate alla macchina Windows 7 infetta

Disabilitazione di SMBv1

- **Pro**: Rimuove la vulnerabilità che WannaCry sfrutta.
- **Contro**: Alcune applicazioni o dispositivi potrebbero dipendere da SMBv1 e potrebbero smettere di funzionare correttamente senza di esso.

Configurazione del Firewall per bloccare l'accesso esterno alle porte 139 e 445, che WannaCry sfrutta per diffondersi nella rete.

- **Pro**: Riduce significativamente la superificie di attacco di WannaCry ed eventuali altri malware che sfruttano la stessa vulnerabilità.
- **Contro**: Si tratta di una soluzione temporanea, che potrebbe interrompere il funzionamento di altri servizi o applicativi che dipendono da queste porte.

Misure di sicurezza a lungo termine che è possibile applicare alla rete aziendale

Applicazione di Patch MS17-010

- **Pro**: Questa patch, rilasciata da Microsoft, risolve la vulnerabilità sfruttata da WannaCry.
- **Contro**: Come con qualsiasi aggiornamento, c'è un potenziale rischio di incompatibilità o problemi con software o hardware specifico, anche se sono rari.

Aggiornamento della versione di SMB

- **Pro**: SMBv2 e SMBv3 sono protocolli più sicuri rispetto a SMBv1. Hanno implementato misure di sicurezza più robuste e sono meno vulnerabili agli attacchi. Le versioni più recenti di SMB (SMBv2 e SMBv3) offrono prestazioni migliori rispetto a SMBv1. Ciò significa trasferimenti di file più veloci e una migliore efficienza della rete.
- **Contro**: Windows 7 supporta sia SMBv2 che una parte di SMBv3, tuttavia ci possono essere probemi di compatibilità con alcuni dispositivi della rete. Il processo di transizione è più lungo rispetto all'applicazione di una patch poiché ha un maggiore impatto.

Sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS)

- **Pro**: Offrono monitoraggio in tempo reale della rete, consentendo una pronta identificazione di attività sospette o anomale. Sfruttando un database di firme, possono identificare e bloccare attacchi noti alla rete.
- **Contro**: L'acquisizione, la manutenzione e l'aggiornamento dei sistemi IDS/IPS possono rappresentare un investimento significativo sia in termini economici che di risorse. Inoltre i sistemi IDS/IPS possono talvolta identificare erroneamente il traffico legittimo come malevolo, portando a falsi allarmi che devono essere analizzati e gestiti (falsi positivii), o viceversa non rilevare minacce reali (falsi negativi).

Altre misure di sicurezza "ausiliarie" a lungo termine che è possibile applicare alla rete aziendale

Impostare/verificare la configurazione di backup regolari

- **Pro:** Avere backup recenti e funzionanti consente di ripristinare i dati senza pagare il riscatto in caso di infezione.
- **Contro:** Richiede risorse di archiviazione e una gestione costante dei backup. I backup devono anche essere isolati per evitare di essere criptati dal ransomware.

Segmentazione della rete

- **Pro**: Limita la diffusione del malware all'interno della rete rendendo difficoltoso il alteral movement da parte di un attaccante.
- **Contro**: Può richiedere una riconfigurazione complessa della rete e potrebbe influenzare le prestazioni o la funzionalità di alcune applicazioni.

Restrizione dei privilegi e del controllo degli account

- **Pro**: Limita le capacità del malware di eseguire operazioni ad alto privilegio e di diffondersi.
- **Contro**: Può richiedere una maggiore gestione degli account e potrebbe complicare alcune operazioni per gli utenti.

Filtraggio e-mail e web

- **Pro**: Blocca l'accesso a siti malevoli e impedisce l'ingresso di e-mail sospette.
- **Contro**: Può talvolta bloccare anche contenuti legittimi, richiedendo interventi di whitelist.

Educazione e formazione degli utenti

- **Pro**: Gli utenti informati sono meno suscettibili di cadere vittima di tentativi di phishing o altre tattiche che potrebbero portare all'introduzione del ransomware.
- **Contro**: Richiede tempo e risorse per fornire formazione continua.