Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF
Organo direzione informatica della Confederazione ODIC

Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI

Promemoria sui Ransomware

I ransomware (troiani che cifrano file a scopo di estorsione) fanno parte di una particolare famiglia di programmi nocivi (malware), che cifra sia i dati contenuti sul computer delle vittime, sia quelli salvati sui dispositivi di rete collegati ad essi (Network shares), rendendoli inutilizzabili. Il ransomware mostra poi alla vittima un „blocca schermo“ intimandole di pagare una certa somma di denaro, in forma di bitcoins (una valuta della rete), all'aggressore in cambio di una chiave per decifrare i dati, così da renderli nuovamente utilizzabili. Il panorama dei programmi nocivi usati al fine di estorcere denaro si amplia costantemente e le versioni attuali possiedono un potenziale di danneggiamento superiore rispetto alle prime conosciute, le quali si limitavano a bloccare lo schermo senza danneggiare i dati. I vettori d'entrata per malware di questo tipo sono, in particolare e-mail infette e siti internet manomessi.

Conseguenze e pericoli

- I dati sul computer vengono resi inutilizzabili
- Nel caso di pagamento del riscatto le vittime subiscono danni finanziari

Misure preventive

- Eseguite regolarmente una copia di sicurezza (backup) dei vostri dati. La copia di sicurezza dovrebbe essere salvata offline, cioè su un supporto esterno, ad esempio un disco rigido esterno. Assicuratevi che il supporto su cui eseguite la copia di sicurezza venga staccato dal computer subito dopo il processo di backup. In caso contrario l'attacco di un ransomware cifrerebbe probabilmente anche i dati salvati sul supporto per backup rendendoli inaccessibili.
- Sia il sistema operativo sia tutte le applicazioni installate sul computer (ad es. Adobe Reader, Adobe Flash, Sun Java ecc.) devono essere mantenute aggiornate allo stato più recente. Se disponibile tramite la funzione di update automatico.
- Diffidate da e-mail che vi giungono inaspettatamente, soprattutto se le considerate sospette o se provengono da un mittente sconosciuto. Non seguite in nessun caso eventuali istruzioni presenti nel testo. Non aprite nessun allegato e non cliccate su nessun link.
- Utilizzate sempre un antivirus attuale. Se decidete di utilizzare un antivirus a pagamento assicuratevi di pagare l'abbonamento alla fine dell'anno, altrimenti l'antivirus è inutile.
- È necessario installare un firewall personale e mantenerlo aggiornato.

Misure successive a un attacco riuscito

- Nel caso di infezione consigliamo di staccare il computer dalla rete. Quindi installate nuovamente il sistema e cambiate le password.
- Dopo aver effettuato la pulizia del computer è possibile ripristinare i dati (se disponibili) grazie al backup effettuato in precedenza. Se non è stato fatto alcun backup dei dati si consiglia comunque di conservare i file cifrati cosicché, nel caso venisse trovata una soluzione, questi possano essere ripristinati.
- In ogni caso MELANI consiglia di annunciare il caso al Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet (SCOCI) e di sporgere denuncia presso il posto di polizia più vicino.
- MELANI sconsiglia il pagamento di un riscatto in quanto ciò rafforza le infrastrutture criminali, permettendo agli aggressori di ricattare altre vittime. Inoltre non c'è nessuna garanzia di ricevere la chiave per decifrare i dati.

Misure per le PMI

Alle aziende MELANI suggerisce, oltre alle misure elencate finora, le seguenti:

- Potete rafforzare maggiormente la protezione delle vostre infrastrutture IT contro programmi nocivi (ad esempio i ransomware) attraverso l'utilizzo di Windows AppLocker[1]. Esso vi permetterà di definire che programmi potranno venir utilizzati sui computer delle vostre ditte.
- Utilizzando Microsoft Enhanced Mitigation Experience Toolkit (EMET)[2] potete impedire che falle di sicurezza, sia conosciute che non ancora conosciute, contenute in programmi utilizzati dalla vostra impresa, vengano impiegate, ad esempio, per l'installazione di programmi nocivi (malware).
- Bloccate la ricezione di allegati e-mail pericolosi nel Gateway della vostra mail. Tra questi ricordiamo:

.js (JavaScript)
.jar (Java)
.bat (Batch file
.exe (Windows executable
.cpl (Control Panel)
.scr (Screensaver)
.com (COM file)
.pif (Program Information File)
.vbs (Visual Basic Script)
.ps1 (Windows PowerShell)

- Assicuratevi che allegati del genere vengano bloccati anche se inviati sotto forma di dati d'archivio, ad esempio ZIP, RAR ma anche di dati d'archivio cifrati (come un file ZIP protetto da password).
- Infine si consiglia di bloccare tutti quegli allegati che contengono macro (ad es. Word, Excel o PowerPoint che contengono macro).

[1] https://technet.microsoft.com/en-us/library/dd759117.aspx
[2] https://support.microsoft.com/en-us/kb/2458544

Consultate il promemoria sulla sicurezza informatica per le PMI e il programma in dieci punti per l'aumento della sicurezza IT sul portale della Confederazione per le PMI: Infrastruttura informatica di sicurezza per le PMI.

Promemoria sulla sicurezza informatica per le PMI:
https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/promemoria-sulla-sicurezza-informatica-per-le-pmi.html

Infrastruttura informatica di sicurezza:
https://www.kmu.admin.ch/kmu/it/home/consigli-pratici/gestire-una-pmi/infrastruttura-e-it/infrastruttura-per-la-tecnologia-dell-informazione/infrastruttura-informatica-di-sicurezza.html

Trovate il „Promemoria sui Ransomware" anche online all'indirizzo seguente:
https://www.melani.admin.ch/ransomware