Malware – che fare?
Lista checking per tecnici di imprese aggredite

Procedure generali fiancheggianti

Come dipendente di un'impresa danneggiata Lei è ben consigliato a tenere presente, prendendo le misure di carattere tecnico-tattico sotto descritte, che vanno informati eventualmente anche i responsabili delle relazioni affari e clienti, di modo che possano riuscire a loro volta a comunicare. A Sua propria discarica si raccomanda di coinvolgere l'ufficio comunicazioni aziendale – esso può pure identificare gli stakeholder interessati e proporre una definizione delle priorità.

1. Informi il corpo di polizia del Suo cantone come anche MELANI e definisca assieme a loro la procedura di seguito

> Informi il corpo di polizia del Suo cantone e MELANI e li consulti se il malware sia da osservare in un primo tempo o se siano da prendere subito delle contromisure. La decisione sulla procedura di seguito dipende essenzialmente (ma non soltanto) dal fatto che il danneggiato si trovi o meno in contatto con i colpevoli o dal fatto che i colpevoli aspettino o no una risposta dal danneggiato. La polizia la consiglia nella procedura di seguito; particolarmente sulla comunicazione con i colpevoli e sull'atteggiamento da tenere con essi.
> Discuti se giovi un immediato intervento di assistenza da parte della polizia.

2. Prenda contromisure nella rete aziendale

> Scopra l'URL e l'indirizzo IP come anche l'estensione dell'infezione.
  > I link dei colpevoli (URL e indirizzo IP) sono da scoprire e da bloccare immediatamente sul proxy server interno rispettivamente sul firewall. Con ciò si impedisce una comunicazione indesiderata verso il server intruso.
  > Se l'infezione avviene per e-mail, i link dei colpevoli (URL e indirizzo IP) si lasciano in molti casi visualizzare in maniera relativamente facile direttamente dall'e-mail (hyperlink) o dal documento a essa allegato.
  > L'estensione infettiva si può determinare in base ai log di server e-mail, server proxy e firewall, nonché grazie a eventuali altri software di sicurezza nella rete dell'impresa danneggiata, arrivando così a identificare URL e indirizzo IP della parte colpevole.
> Blocchi URL e indirizzo IP avversari nel proxy server interno rispettivamente sul firewall.
> Scolleghi immediatamente per quanto possibile computer e periferici dalla rete. Fino a quando tuttavia il malware non sarà stato analizzato dall'autorità inquirente cantonale e MELANI o dall'impresa danneggiata stessa, computer e apparecchi infetti non dovrebbero essere spenti dall'impresa danneggiata ma andrebbero invece conservati accesi.

3. Metta al sicuro i dati rilevanti

> Salvi i log file e li trasmetta assieme ai seguenti file rilevanti all'autorità inquirente al fine di permettere la scoperta della parte colpevole:
  > I log del proxy server rispettivamente del firewall contenenti i veri URL e indirizzo IP si lasciano inviare all'autorità inquirente come allegati e-mail.
  > Se il malware ha raggiunto l'impresa danneggiata via e-mail, l'intera e-mail, inclusi gli allegati, va impacchettata in un file ZIP e questo file deve poi essere trasmesso in allegato e-mail all'autorità inquirente.
  > Se l'infezione malware è entrata invece per «drive-by download», il malware va se possibile isolato da parte della danneggiata, impacchettato in un file ZIP e poi trasmesso in allegato e-mail all'autorità inquirente.
  > Se l'infezione malware è avvenuta per memoria di massa USB, è quest'ultima a essere messa a disposizione dell'autorità inquirente (per posta o consegna di persona).
  > Eventuali proprie analisi del software nocivo da parte della danneggiata possono essere trasmesse all'autorità inquirente per allegato e-mail.

In collaborazione con MELANI e Swiss Cyber Experts