Cyberaggressioni – come proteggersi

Lista checking per dirigenti d'azienda nel caso di un cyberattacco

Management summary

1. Una buona strategia contro i cyberattacchi incomincia da prima dell'incidente vero e proprio: la dirigenza dell'impresa deve riflettere prima su come avrà da reagire.

2. In caso di un cyberevento ostile, è indicato un intervento rapido: procedure ben consolidate fra di loro e percorsi di escalation giovano molto a mantenere il controllo della situazione.

3. Dopo l'attacco è prima dell'attacco: una rielaborazione sistematica dell'evento avvenuto è essenziale.

1. Preparazione

Misure generali della direzione d'impresa:
> Esiste nella Sua impresa un'unità di crisi per i casi di cyberattacchi? Sono stati definiti ambiti di responsabilità e criteri di competenza controllandoli in esercitazioni con l'unità di crisi?
> È stata attrezzata con le risorse e competenze necessarie l'unità di crisi? (In particolare, assistenza nell'ambito della gestione della crisi, comunicazione interna ed esterna, legislazione, personale e esperti tecnici)
> Dispone l'unità di crisi di un manuale aggiornato con importanti e attuali dati di contatto verso i (decisivi) rappresentanti di partner esterni?
> Si sottopone la squadra a esercitazioni regolari in modo che i suoi componenti si conoscano l'un l'altro e sappiano a perfezione quali siano i ruoli e le responsabilità all'interno del gruppo?
> L'unità ha familiarità con le procedure del diritto penale o con la consulenza tecnica della polizia rispettivamente degli interlocutori competenti?
> Esistono legami personali fra la Sua impresa o la squadra della Sua unità di crisi e gli organi della giustizia penale?

Misure legali:
> Esistono nella Sua impresa responsabilità chiaramente definite nel quadro di conduzione, comunicazione e reparto legale, se e quando sia necessario mettersi in contatto con la polizia per consigli pratici o per esortarla a indagare?
> È chiara ai responsabili la distinzione fra polizia consulente e polizia giudiziaria penale?[1]

2. Nel caso di danni

> Nel caso di un oltraggio personale serve la via al prossimo posto di polizia.
> Nel caso di un evento professionale, cioè una cyberaggressione in essere contro la Sua impresa, si tratta di consultare velocemente degli specialisti. Contatti immediatamente la polizia. Sul portale Suisse ePolice (www.suisse-epolice.ch) trova il numero telefonico del posto di polizia a Lei vicino.
    > Imprese private specializzate La assistono nella riparazione ed eventualmente restaurazione della Sua infrastruttura.

1 Confronti in merito il contenuto a pagina 2.

- La Sua polizia la consiglia e assiste nella procedura di seguito, specialmente anche sulla questione se pagare o no un riscatto.
  La polizia non è interessata per principio né ai Suoi segreti professionali né a interferire con la Sua infrastruttura. La polizia invece fa affidamento sul fatto che un'azienda presa di mira da aggressori sia spontaneamente disponibile a consegnare le tracce dei danneggiatori lasciate sui sistemi dei danneggiati.
  Nel caso di attacco acuto è raccomandabile mettersi in contatto telefonico diretto con gli specialisti della polizia tramite un collaboratore tecnicamente esperto. A questo collaboratore servirà assolutamente lo sblocco interno da parte tipicamente del management o dell'ufficio legale. L'impresa ha bisogno di una rispettiva policy, anche sul fare accompagnare o no la telefonata dall'ufficio legale.
- Il centro di annuncio e analisi della Confederazione MELANI La assiste nel valutare quale software nocivo abbia infettato il Suo sistema e se ne sono interessate anche altre imprese.

3. Rielaborazione

Esiste una rielaborazione sistematica di eventi con esiti dannosi (oppure anche «near misses» in cui si sono evitati danni per un pelo) riguardo a miglioramenti continuati?

La rielaborazione può migliorare in particolare
- il riconoscimento preventivo o immediato dell'evento,
- la qualità e la rapidità del riconoscimento (dimensione del danno, criticità ecc.),
- la reazione appropriata e immediata/l'escalation se necessaria,
- il superamento dell'incidente, rispetto sia a eventuali misure immediate per arginarne il danno, sia all'identificazione e all'eliminazione di cause originali e debolezze,
- le misure per il mantenimento di un'appropriata gestione aziendale di emergenza durante il trattamento dell'evento,
- la comunicazione verso l'interno e l'esterno,
- l'efficacia e l'efficienza delle misure tecniche e organizzative, dei mezzi ausiliari e delle procedure, inoltre
- la collaborazione interna e la cooperazione con entità esterne.

Un attivo scambio di esperienze rispetto al superamento dell'incidente assieme ad altre organizzazioni dello stesso ramo, ambiente legale e della stessa regione è un addizionale strumento per una rielaborazione attiva. Le conoscenze acquisite sono da inserire sistematicamente nel miglioramento della qualità nelle procedure interne, documentazioni, esercitazioni e nella conduzione e cultura aziendale.

In collaborazione con MELANI e Swiss Cyber Experts