Invulformulier bij aangifte ransomware

Omdat u de aangifte niet tussentijds kunt opslaan, is het belangrijk om vooraf te controleren welke gegevens u nodig heeft. In onderstaande checklist vindt u een overzicht van de informatie die u bij de hand moet hebben om de aangifte volledig en correct in te vullen.

Inloggen

- Om zakelijk aangifte te doen van ransomware logt u eerst in met eHerkenning en vervolgens met DigiD. Zorg ervoor dat u deze inloggegevens bij de hand heeft.

Wanneer is het gebeurd?

- De datum en het tijdstip waarop de versleuteling is begonnen. Weet u niet wanneer de versleuteling precies is gestart? Noteer dan de datum en het tijdstip waarop u de versleuteling heeft opgemerkt.

- Zijn de bestanden weer vrijgegeven? Noteer dan de datum en het tijdstip waarop de bestanden weer toegankelijk zijn geworden.

Hoe is de ransomware binnengekomen?

- Noteer hoe de ransomwarebesmetting volgens u is ontstaan en wat de vermoedelijke bron van de infectie is (bijvoorbeeld een e-mail, download of URL (link).

    - Is de besmetting mogelijk via een e-mail ontstaan? Verzamel dan de volledige e-mailheader (met informatie zoals afzender, ontvanger, onderwerp en verzenddatum). Raadpleeg voor meer uitleg over het vinden van emailheaders https://internetsporen.nl/emailheaders

    - Is de besmetting mogelijk via een (gedownload) bestand ontstaan? Noteer dan de naam van het bestand, de locatie (map of schijf), de bestandsgrootte en hoe u aan dit bestand bent gekomen.

    - Is de besmetting mogelijk via een URL (link) ontstaan? Noteer dan de volledige URL.

Details van de ransomware

- Door welk type ransomware bent u getroffen en welke versie heeft deze? Noteer, indien bekend, de naam van de ransomware en de specifieke versie die uw systeem heeft geïnfecteerd.

- Noteer de extensie van de getroffen bestanden, dat is het deel van de bestandsnaam achter de punt. Als een bestand de naam ‘voorbeeld.txt’ heeft, dan is ‘.txt’ de extensie. Als de extensie niet zichtbaar is, kunt u deze ook vinden via de eigenschappen van het bestand.

Losgeldbrief

- Noteer de bestandsnaam en de inhoud van de losgeldbrief of ransom notitie. Een losgeldbrief of ransom notitie is meestal een nieuw bestand dat geplaatst is op een opvallende plek, zoals het startscherm, bureaublad of bestandsverkenner en bevat uitleg en instructies voor een betaling. Een losgeldbrief is vaak herkenbaar aan de volgende bestandsnamen: readme, how_to_decrypt, decrypt my files, decrypt_readme, readme_decrypt, attention, important_readme, recover, recover_your_files, howto_recover.

- Noteer het bedrag van de losgeldeis en de valuta waarin deze wordt gevraagd.

- Noteer naar welke wallet of rekeningnummer de betaling moet worden overgemaakt. Let op: een walletadres is hoofdlettergevoelig. Neem de hoofdletters en kleine letters exact over zoals vermeld.

Getroffen apparaten

- Noteer welk type apparaat of apparaten getroffen zijn door de ransomware en vermeld hierbij het merk, het model, het besturingssysteem en de versie van het besturingssysteem.

Contact met afperser

- Noteer op welke wijze het contact met de afperser heeft plaatsgevonden en vermeld daarbij de datum en het tijdstip van het contact, evenals een zo volledig mogelijke omschrijving van de inhoud en de wijze van communiceren.
    - Indien het contact via e-mail heeft plaatsgevonden, noteer dan het e-mailadres.
    - Indien het contact via Jabber is verlopen, noteer dan de gebruikte contactgegevens.
    - Indien het contact via Tox heeft plaatsgevonden, noteer dan de Tox-identifier.
    - Indien het contact via TorChat is verlopen, noteer dan het TorChatadres.

Schade door betalingen

- Noteer het totaalbedrag van alle betaalde losgelden, inclusief betalingen in euro of andere valuta, en geef de dagwaarde van eventuele cryptobetalingen omgerekend naar één valuta. Denk ook aan overige schade die niet direct het gevolg is van betalingen. Dit kan bijvoorbeeld gaan om bijkomende kosten, gemiste inkomsten, psychische schade of andere schade die u heeft geleden.

- Noteer of de schade door een verzekeraar wordt vergoed en vermeld in dat geval de naam van de verzekeraar.

Betalingen

- Noteer alle gedane betalingen afzonderlijk en vermeld daarbij voor elke betaling de gebruikte valuta, het wallet- of rekeningnummer, de transactiehash en de datum en het tijdstip van de betaling.

- Noteer of de bestanden na het doen van de betaling(en) zijn vrijgegeven.

ICT-dienstverlener of ICT-afdeling

- Indien een ICT-dienstverlener of ICT-afdeling is ingeschakeld, noteer dan de naam, het ticketnummer en de contactgegevens van de contactpersoon van deze dienstverlener of afdeling.