Aangifte doen van ransomware

Wanneer u slachtoffer bent geworden van ransom- of cryptoware is het van belang dat u daarvan aangifte doet bij de politie. Door aangifte te doen kan de politie in overleg met het Openbaar Ministerie besluiten om een onderzoek te starten en helpt u bij het in kaart brengen van criminaliteit. Hiermee kan de politie strafbare feiten opsporen en meer slachtoffers voorkomen.

Onderstaande informatie is bedoeld om u te helpen bij het doen van aangifte van een ransomwarebesmetting.

Het doen van een aangifte

Bij het opnemen van een aangifte worden een aantal vaste gegevens vastgelegd. Houd er rekening mee dat er naar de volgende gegevens gevraagd zal worden:

- Persoonsgegevens van u en die van de mogelijke benadeelde indien u dat niet zelf bent (inclusief adres- en contactgegevens);
- Doet u aangifte namens een ander en heeft u daarvoor toestemming gekregen;
- Plaats(en) waar het feit gepleegd is;
- Data en tijden waarop of waartussen het feit gepleegd is;
- Voorkeur voor het verhalen van mogelijke schade op een verdachte;
- Wensen aangever met betrekking tot slachtofferzorg;
- Relatie tussen personen en de goederen (bijvoorbeeld eigenaar, huurder, gebruiker).

Verder zal bij het opnemen van de aangifte een beschrijving worden gevraagd van het gepleegde feit en de omstandigheden. Hierbij kunt u denken aan de werkwijze van de dader.

Het helpt als u de benodigde stukken en bewijzen voor een mogelijk onderzoek kunt aanleveren.

Bij het beschrijven van het strafbare feit en de omstandigheden zullen u mogelijk de volgende vragen gesteld worden:

- Hoe bent u op de hoogte geraakt van het strafbare feit?
- Wat is de datum en het exacte tijdstip waarop het delict gepleegd of ontdekt is?
- Op welke manier heeft u contact gehad met de verdachte (e-mail, telefonisch, chat, etc.)

- Welke handeling heeft tot de besmetting geleid? (downloaden, websitebezoek, etc.)
- Hoe zag het ransomware-scherm er uit? (gebruikte taal, logo's en kleuren).
- Eventuele details over betalingen.
- Als er sprake is van hacken: wie maken er gebruik van de computer die gehackt is?
- Welke gegevens zijn er versleuteld?
- Welke acties heeft u zelf ondernomen?
- Zijn deze handelingen buiten uw goedkeuring om verricht?

Bij het mogelijke onderzoek naar een strafbaar feit probeert de politie zo veel mogelijk relevante informatie te verzamelen en analyseren. U kunt de politie hierbij helpen door voor zover mogelijk de volgende zaken aan de politie te overhandigen:

- IP-adressen van betrokkenen;
- E-mailadressen van verzender en ontvanger
- E-mailbericht en e-mailheader;
- Gebruikersnaam verdachte (in chats, e-mails etc.);
- Internetadres (URL);
- Telefoonnummer;
- Advertentienummer(s);
- Afbeeldingen;
- Chatlogs (indien die aanstaan);
- Unieke gegevens (bijvoorbeeld een serienummer of bitcoinadres);
- Encryptiesleutelgegevens.

Voor het vastleggen en overhandigen van eerder genoemde zaken kunt gebruik maken van meerdere middelen. Denkt u hierbij aan:

- digitaal (opgeslagen op cd-rom/usb-stick);
- printscreen;
- geprint op papier;
- foto gemaakt van het beeldscherm.

Wij adviseren u nooit betalingen te doen maar heeft u toch betalingen aan de verdachte gedaan dan zijn de volgende gegevens voor de politie interessant:

- Rekeningnummer(s) (bankafschriften bijvoegen);
- Kwitanties (rembours);
- Creditcard-/PayPal-gegevens;
- Contactgegevens;
- Bitcoinadressen.