Aangifte Ransomware

“Ineens zat ons hele systeem op slot!”

Ransomware, wat is dat?

Helaas bent u slachtoffer geworden van ransomware. Ransomware is een programma dat gegevens op een computer versleutelt en vervolgens van de gebruiker losgeld vraagt om de computer weer te ‘bevrijden’. In extreme gevallen blokkeert ook de toegang tot de computer, doordat systeembestanden die nodig zijn voor de goede werking van de computer mee worden versleuteld. Het losgeld wordt vaak geëist in de vorm van een cryptocurrency, zoals Bitcoin of Monero. In sommige gevallen steelt de crimineel ook gevoelige data, zoals financiële documenten of paspoortgegevens. Deze data kan gebruikt worden als drukmiddel om u te laten betalen.

Gegevens aangifte

U maakt een afspraak voor het doen van aangifte. Voordat u de afspraak heeft, is het belangrijk dat u alle benodigde gegevens al bij de hand heeft. Vul hieronder uw gegevens in.

U dient dit document op een *computer* in te vullen. Om het document in te vullen klikt u boven in beeld op “BEELD” en vervolgens op “Document bewerken”.

Gegevens aangever

- Voornaam (voluit)
- Achternaam
- Geboortedatum
- Adres
- Postcode
- E-mailadres
- Telefoonnummer
- Burgerservicenummer
- Welk identiteitsbewijs neemt u mee naar de aangifte? Dit kan een paspoort, identiteitskaart, rijbewijs of Nederlands vreemdelingendocument zijn.
- Documentnummer identiteitsbewijs

Vragen aangifte

Wilt u ter voorbereiding van de aangifte alvast antwoord geven op onderstaande vragen? De antwoorden vult u in onder de vraagstelling achter ‘A:’. De informatie in dit aangifteformulier wordt vertrouwelijk behandeld door de politie en zal niet openbaar worden gemaakt.

Gegevens benadeelde

- Naam bedrijf
- Adres
- Vestigingsplaats
- KVK-nummer
- E-mailadres
- Telefoonnummer

Gegevens IT-partij benadeelde

- Naam bedrijf (indien externe partij)
- Adres (indien externe partij)
- Vestigingsplaats (indien externe partij)
- KVK-nummer (indien externe partij)
- Naam contactpersoon
- E-mailadres
- Telefoonnummer

Algemene vragen

Toevoegen technisch onderzoeksrapport:
Heeft uw IT-afdeling of een ingehuurd bedrijf voor u onderzoek gedaan naar de ransomware aanval?

In het onderzoek naar een ransomware aanval komen feitelijke gegevens zoals rekeningnummers, telefoonnummers, IP-adressen, logbestanden en e-mailadressen etc. naar voren. Ook informatie over het verloop van het incident en de gedragingen en communicatie van de criminelen blijken uit het onderzoek. Deze feitelijke informatie en informatie over het incident en de criminelen is zeer relevant voor het politieonderzoek. We vragen u daarom deze informatie met ons te delen aan de hand van onderstaande vragen.

Uit eerdere onderzoeken blijkt dat de rapportage van externe bedrijven vaak belangrijke, zo niet de belangrijkste, informatie bevat voor het politieonderzoek. Heeft u een extern bedrijf ingehuurd om het onderzoek te doen, dan

ontvangen wij in aanvulling op de onderstaande vragen ook graag het rapport dat u naar aanleiding van dit onderzoek krijgt.

V: Kunt u in uw eigen woorden, chronologisch, vertellen wat er is gebeurd? Ook alle feitelijke gegevens zoals wallet/crypto-adressen, IP-adressen en e-mailadressen etc. moet u hier noemen.
Verwijs niet naar eventuele bijlagen die u heeft, maar benoem ze hier ook.
A:

V: Wat is de naam en de versie van de ransomware?
A:

V: Heeft u backups van de versleutelde bestanden, en zo ja, heeft u daarmee de bestanden volledig weten te herstellen?
A:

V: Bent u eerder slachtoffer geweest van ransomware, of eventueel andere cyberaanvallen (phishing, DDoS, ...)?
A:

V: Is er (gevoelige) data gestolen? Zo ja, kunt u aangeven wanneer dat is gebeurd en of er gedreigd is met het openbaar maken van de data als er niet betaald zou worden? (datum en tijd)
A:

Ontdekking

V: Hoe en wanneer heeft u de ransomware ontdekt?
A:

V: Heeft u een ransomware notitie gevonden? Vermeld in dat geval de naam van de notitie en zoveel mogelijk wat hierin stond; kunt u een afbeelding daarvan met ons delen?
A:

V: Heeft u versleutelde bestanden gevonden? Zo ja, vermeld dan de extensie.
A:

V: Is er nog andere relevante informatie betreft de ontdekking van ransomware?
A:

Besmetting

V: Weet u hoe en wanneer het systeem besmet is geraakt met de ransomware? Vermeld hier zoveel mogelijk informatie over.
A:

V: Heeft u een bepaalde website bezocht? Welke website was dit en waar heeft u eventueel op geklikt?
A:

V: Heeft u op een link in een e-mail geklikt? Noemt u hier dan zoveel mogelijk informatie over de e-mail en de gebruikte link. Graag ontvangen wij een digitale kopie van de e-mail.
A:

V: Update u uw software regelmatig? Wanneer was dit voor het laatst gedaan?
A:

V: Maakt uw bedrijf gebruik van Citrix, VPN, RDP of andere manier om op afstand in te loggen op het bedrijfsnetwerk?
A:

Communicatie

Leg hier duidelijk vast hoe en wat de communicatie is geweest tussen u en de criminelen:

V: Heeft u contact met de criminelen opgenomen? Hoe is dat verlopen?

A:

V: Heeft u met de criminelen onderhandeld over het losgeld? Zo ja, wat was de gevraagde prijs voor en na het onderhandelen?
A:

V: Hebben criminelen druk op u gezet door het bellen of mailen van werknemers of klanten, of hebben ze u bijvoorbeeld aangevallen met DDoS? Zo ja, hoe is dat verlopen?
A:

V: Noteer hier de beschikbare gegevens van de criminelen (e-mail, URL-link, TOR-chat, etc.).
A:

Neemt u zo veel mogelijk correspondentie mee naar de aangifte. Neemt u ook de technische details mee, zoals de e-mailheaders & logging van de webserver rondom alle contactmomenten. Op de website internetsporen.nl kunt u lezen hoe u de e-mailheaders, belangrijk voor het opsporingsonderzoek, kunt veiligstellen.

Datalek

Indien er sprake is van een datalek, vult u dan de volgende vragen in.

V: Om wat voor soort data gaat het?
A:

V: Wat is de omvang van het lek?
A:

V: Op wat voor apparaten heeft het lek plaatsgevonden?
A:

V: Om hoeveel slachtoffers gaat het?
A:

V: Zijn er steeds hetzelfde soort persoonsgegevens gelekt of verschillende combinaties?
A:

V: Indien de data online is gedeeld, van welke platformen is bekend dat de data er gedeeld is?
A:

V: Is de Autoriteit Persoonsgegevens in kennis gesteld?
A:

V: Zijn de gedupeerden allen op de hoogte van het lek?
A:

V: Zijn er aanwijzingen dat de persoonsgegevens zijn misbruikt?
A:

Betaling

Is het gevraagde losgeld betaald? Indien van toepassing:

Vul in per cryptotransactie:

Datum en tijdstip:
Aantal en valuta:
Van wallet:
Naar wallet:

Transactie hash:

V: Wat was de reden om het losgeld te betalen?
A:

V: Bent u verzekerd tegen ransomware aanvallen? Zo ja, is het losgeld verzekerd en/of ook de overige schade van de ransomware aanval?
A:

Schade en impact

Om de impact van de ransomware aanvallen op de maatschappij te volgen ontvangen we graag informatie over de schade die u heeft geleden door de ransomware aanval.

V: Welke schade ervaart u (bijv. reputatieschade, weggevallen inkomsten, betaald losgeld, inhuren van derden)? Kunt u dat kwantificeren?
A:

V: Hoeveel schade heeft u (minimaal) geleden?
Mocht u geen precieze schatting van de kosten kunnen maken, kan u wellicht vertellen of dit in de duizenden, tienduizenden, honderdduizenden of miljoenen euro's loopt?
A:

Slachtofferhulp

Heeft u behoefte aan slachtofferhulp of nazorg? (zie informatie op https://www.politie.nl/informatie/ik-ben-slachtoffer-wat-nu.html)
Deze vraag graag met **ja** of **nee** beantwoorden. A:

Blijf alert op ransomware, dit kunt u doen:

Bij de politie zijn meldingen gedaan van bedrijven die na verloop van tijd nog een tweede (en zelfs derde) ransomware aanval hebben gehad. Dit kunt u doen om het te voorkomen:

- Installeer updates van besturingssystemen en updates van programma's direct. Niet alleen omdat updates de veiligheid verbeteren, maar ook omdat nieuwe versies extra functionaliteit bieden en sneller draaien en minder snel vastlopen.
- Gebruik antivirussoftware. Deze kan ransomware namelijk detecteren en blokkeren.
- Open geen e-mails, links in e-mails en zeker geen bijlage(n) van onbekende afzenders
- Open ook geen e-mails, links in e-mails en bijlage(n) die u eigenlijk niet verwacht, ook al is de afzender bekend.
- Maak regelmatig back-ups, ofwel een kopie van de bestanden op je computer. Dit voorkomt dat je bestanden kwijt bent na een ransomwarebesmetting. U kunt automatisch back-ups instellen of handmatig een back-up maken. U bewaart een back-up bijvoorbeeld op een externe harde schijf of in de cloud. Zorg ervoor dat u ook back-ups heeft die losgekoppeld zijn van internet.
- Gebruik tweestapsverificatie voor inloggen. Dat betekent dat u naast een wachtwoord bijvoorbeeld een code van uw telefoon moet invoeren bij het inloggen.
- Verklein de gevolgen van incidenten door ook maatregelen te treffen die specifiek gericht zijn op het mitigeren van de risico's en impact als een incident toch onverhoopt plaatsvindt. Denk daarbij aan netwerksegmentatie, kroonjuwelen extra beschermen, het hebben van een Incident Responseplan, het doen van oefeningen etc.
- Wij adviseren u om nooit in te gaan op betaaleisen. Met het betalen van geld aan deze criminelen groeperingen blijft het criminele proces in stand.
- Mocht u toch betalen, dan is het extra belangrijk om de politie daarvan op de hoogte te stellen omdat betalingsinformatie van grote waarde is voor het opsporingsonderzoek.
- Voor meer informatie, ga naar www.ncsc.nl of www.digitaltrustcenter.nl.