HACKHELPDESK

Eerste hulp bij cybercrime voor ondernemers

HACKHELPDESK.NL

RANSOMWARE

Wat is ransomware?

Ransomware is software waarmee een computersysteem wordt 'gegijzeld'. Je kunt dan niet meer bij je persoonlijke bestanden.

Hoe gebeurt het?

Bij het opstarten van je device verschijnt een melding dat een bedrag betaald moet worden om weer toegang te krijgen tot je bestanden.

Wat is het doel?

Het doel van ransomware is om bitcoins of een andere cryptomunt te ontvangen. Dit kan gepaard gaan met afpersing.

Wat is de oplossing?

In veel gevallen is er echter maar één oplossing: de back-up terugzetten. Het is dan ook essentieel om altijd een goede back-up te hebben van de bestanden. Zonder een back-up is de kans op het terugkrijgen van bestanden klein.

Verder raden wij het betalen van losgeld sterk af! Naast dat je het criminelensysteem in stand houdt, geeft het ook géén garantie dat je bestanden weer vrij worden gegeven.

Kijk op NoMoreRansom.org voor een overzicht van alle ransomware die je zelf kunt ontsleutelen.

REPRESSIE

Wat je vooral niet moet doen.

Stap 1

Zet niet de computer uit, zo blijft bewijsmateriaal bewaard.

Wat je vooral wel moet doen.

Stap 1

Sluit direct je systemen af van het internet. Dit kan door de WiFi verbinding uit te schakelen of door de internetkabel los te koppelen.

Stap 2

Bewaar screenshots of foto's en doe aangifte bij de politie.

Stap 3

Heb je zelf weinig technische kennis, overweeg dan om een IT-security specialist in te schakelen. Deze kan je begeleiden in het proces met als doel de ransomware grondig te verwijderen en het systeem te herstellen.

HACKHELPDESK

Eerste hulp bij cybercrime voor ondernemers

HACKHELPDESK.NL

Wil je zelf aan de slag? Lees dan onderstaande tips:

Tip 1

Het kan zijn dat de makers van de ransomware al zijn opgepakt of de politie de ontsleutelings-gegevens heeft weten te bemachtigen. Voor een overzicht van alle ransomware die je zelf kunt ontsleutelen, kan je naar NoMoreRansom.org gaan. Niet voor iedere vorm van ransomware is een oplossing.

Tip 2

Een andere optie is het terugplaatsen van bestanden via een back-up. De ransomware moet wel eerst worden verwijderd voordat je de bestanden terugplaatst, bijvoorbeeld door de computer opnieuw te installeren.

Tip 3

Heb je zelf geen back up gemaakt? Dan is er een kans dat Windows dit automatisch heeft gedaan via schaduwkopieën:
→ Klik met je rechtermuisknop op een bestand of map → Selecteer Eigenschappen > tabblad 'Vorige versies' → Kijk of er een oudere versie staat die hersteld kan worden.

Tip 4

Scan je systeem met een virussoftware en malware scanner, zoals malwarebytes.

Tip 5

Het is ook de moeite waard om data herstelsoftware te proberen. Een voorbeeld is het programma Recuva.

Let op! Het betalen van losgeld bij ransomware raden we sterk af. Het geeft namelijk géén garantie dat je bestanden vrij worden gegeven. Daarnaast houd je het systeem van criminelen in stand door te betalen.

PREVENTIE

Tip 1

Houd alle software up-to-date, waaronder het besturingssysteem, de internetbrowser, internetaanvullingen en programma's, zoals Adobe Reader. Met Scan Circle zie je snel hoe je pc ervoor staat. Scan Circle controleert automatisch, gratis en snel je computer op de meest voorkomende problemen.

Tip 2

Installeer een goede virusscanner. Kijk op consumentenbond.nl/virusscanner welke virus-scanner voor jou geschikt is.

Tip 3

Klik niet op bijlagen en links in e-mails, tenzij je zeker weet dat het vertrouwd is.

Tip 4

Schakel geen macro's in bij Office-documenten van derden, zeker niet als daar in het document om wordt gevraagd.

Tip 5

Ransomware is vaak een uitvoerbaar .exe-bestand, vermomd als een ander soort bestand, zoals een pdf-document. Schakel bestandsextensies weergeven in, zodat je de vermomming kunt doorzien.

Tip 6

Maak back-ups! Dat is sowieso verstandig, maar bij ransomware-besmetting vaak het enige redmiddel om verlies van al je gegevens te voorkomen.