

Q&A ransomware-aanval

1. Hoe zijn de hackers binnengekomen?

We hebben ons beveiligd op basis van de richtlijnen Baseline informatiebeveiliging Overheid. Wij testen onze beveiliging jaarlijks. Aandachtspunten pakken wij direct op. Ondanks dat hebben ze een weg gevonden om bij ons binnen te komen. Het digitaal forensisch onderzoek naar de exacte oorzaak loopt nog. We hebben naar aanleiding van de hack extra maatregelen getroffen.

2. Waarom gaat het ook om gegevens van de gemeente Neder-Betuwe?

Gemeente Buren voert voor de Gemeente Neder-Betuwe de participatiewet uit. Denk aan bijstandsuitkeringen. Dit is de reden waarom er gegevens van inwoners uit Neder-Betuwe bij ons bekend zijn.

3. Hoe worden inwoners geïnformeerd als blijkt dat hun gegevens op het darkweb staan?

Als er gegevens zijn gestolen van een inwoner, dan nemen we persoonlijk contact op met deze inwoner om hem of haar op de hoogte te brengen.

4. Wanneer worden inwoners geïnformeerd als hun gegevens op het darkweb staan?

Zodra dit bij ons bekend is. Het uitzoekwerk is intensief en complex. Daardoor duurt het helaas lang. We zouden willen dat het sneller ging, maar om een beter beeld van de omvang van de diefstal te krijgen, hebben we nog minstens een aantal dagen nodig. Daarna gaan we alle gegevens bekijken. Dat neemt enkele weken in beslag. We informeren u zo snel mogelijk over de relevante resultaten.

5. Wat kan ik zelf doen?

Wees vooral alert! Krijgt u een telefoontje, post of een mail van de gemeente, uw bank of van andere instanties en twijfelt u of dit wel klopt? Neem dan zelf contact op met de gemeente, uw bank, of de andere instantie om het te controleren.

Krijgt u een verdacht linkje doorgestuurd via WhatsApp of per mail, check het linkje veilig via www.checkjelinke.nl.

Op www.veiliginternetten.nl leest u alles wat u kunt doen om veilig te internetten. Denk aan hoe u veilig draadloos internet, internetbankiert en hoe u veilig gebruik kan maken van uw sociale media. Ook leest u hier hoe u een phishingmail herkent en hoe u identiteitsfraude voorkomt.

6. De gemeente spreekt van 130 Gb, de hackers hebben zelf kenbaar gemaakt dat ze 5 Tb hebben, waarom praat de gemeente dan over 130 Gb?

De hackers zeggen 5 Tb aan gegevens van ons in handen te hebben. Ze hebben 130Gb aan gegevens gepubliceerd op het darkweb.

7. Klopt het dat de hackers in het slechtste geval alle 5 Tb online zal zetten?

Dat sluiten wij niet uit.

8. Heeft de gemeente de autoriteit persoonsgegevens ingelicht en aangifte gedaan bij de politie? Zo ja, wanneer?

Ja, de Autoriteit Persoonsgegevens is onmiddellijk ingelicht. Ook is er direct aangifte gedaan bij de cyberafdeling van de Politie.

9. Om wat voor persoonlijke gegevens gaat het?

Dat zijn we nu aan het onderzoeken.

10. Staat mijn identiteitsbewijs en IBAN op het darkweb?

Dat zijn we nu aan het onderzoeken. Waar nodig brengen we inwoners en/of ondernemers persoonlijk op de hoogte.

11. Waarom informeert de gemeente nu pas haar inwoners als de hack al op 1 april heeft plaatsgevonden?

We hebben direct na de aanval gecommuniceerd via allerlei kanalen. Afgelopen week is pas bekend geworden dat er gegevens van ons gestolen zijn. Op 1 april was dat nog niet bekend.

12. Waarom worden we via Facebook geïnformeerd?

We hebben direct na de aanval gecommuniceerd via allerlei kanalen, zoals via onze website, sociale media en via de pers. Vrijdag en zaterdag is er ook een brief van de gemeente bij inwoners bezorgd.

13. Worden we ook nog op andere manieren geïnformeerd?

Ja, we informeren u via allerlei kanalen, zoals via onze website, sociale media en via de pers. Zaterdag/vandaag ook per brief. Waar nodig brengen we inwoners en/of ondernemers persoonlijk op de hoogte.

14. Waarom wordt niet iedereen persoonlijk geïnformeerd?

Het uitzoekwerk is intensief en complex. Daardoor duurt het helaas lang. We zouden willen dat het sneller ging, maar om een beter beeld van de omvang van de diefstal te krijgen, hebben we nog minstens een aantal dagen nodig. Daarna gaan we alle gegevens bekijken. Dat neemt enkele weken in beslag. We informeren u zo snel mogelijk over de relevante resultaten.

15. Slaat de gemeente haar gegevens niet veilig op? Dit mag een gemeente toch niet gebeuren?

We hebben ons beveiligd op basis van de richtlijnen Baseline informatiebeveiliging Overheid. Wij testen onze beveiliging jaarlijks. Aandachtspunten pakken wij direct op. Ondanks dat hebben ze een weg gevonden om bij ons binnen te komen.

16. Zijn er regels overschreden?

We hebben ons beveiligd op basis van de richtlijnen Baseline informatiebeveiliging Overheid. Wij testen onze beveiliging jaarlijks. Het digitaal forensisch onderzoek loopt nog.

17. Hoe gaat gemeente Buren haar verantwoordelijkheid nemen?

Wij nemen onze verantwoordelijkheid door dit zeer serieus te nemen. We zijn met man en macht bezig om na te gaan welke gegevens er zijn gestolen door de criminelen. Dat doen we zodat we u daarover kunnen informeren. Daarnaast doen we dit zodat we passende maatregelen kunnen treffen om de beveiliging van onze systemen te verbeteren.