Persbericht – 30 januari 2024 –11u

Update cyberaanval

Limburg.net informeert over cyberaanval: maatregelen en oproep tot waakzaamheid

Naar aanleiding van de recente cyberaanval waarvan Limburg.net het slachtoffer is geworden, wil Limburg.net haar gebruikers en het publiek uitgebreid informeren over de huidige stand van zaken en de genomen maatregelen. Er vertrekt een brief naar de gezinshoofden die in 2014 en 2015 geregistreerd stonden en van wie de data zijn gestolen. 61 personen die in schuldbemiddeling zaten, werden al gecontacteerd. Daarnaast roept Limburg.net op tot waakzaamheid. Een gedetailleerde lijst maken van alle gestolen data per individu blijkt niet aangewezen. De Vlaamse Toezichtcommissie raadt dat uitdrukkelijk af. Limburg.net wacht de officiële richtlijn hieromtrent af.

Chronologie van de gebeurtenissen

Limburg.net wil volledige inzage geven in wat er precies gebeurd is. In bijlage vindt u een tijdslijn, hieronder enkele belangrijke data:

- Op 13/12 stelden we vast dat hackers de systemen van Limburg.net aanvielen. Uit veiligheidsoverwegingen legde Limburg.net zelf haar systemen direct stil. Dankzij goede backups kon Limburg.net haar dienstverlening snel terug opstarten, recyclageparken bleven open, afvalophalingen gingen door. Onderzoek wees inmiddels uit dat de *date of entry* op 17/11 was.
- Op 19/12 kregen we de eerste indicaties dat er ook bestanden waren gedownload. De dataspecialisten stelden vast dat het ging om een zeer geavanceerde vorm van hacking. De hackers hadden hun sporen gewist en files geëncrypteerd, met als doel de reconstructie door dataspecialisten te bemoeilijken.
- Op 21/12 stuurde Limburg.net een interne mail naar haar medewerkers met het *worst case scenario*, met daarin een oplijsting van mogelijke gegevens die waarschijnlijk waren gestolen. Op dat moment was het reconstructie-onderzoek volop bezig. Het was nog niet duidelijk welke files effectief gekopieerd waren.
- Op 11/01 verscheen het bericht van hackersorganisatie Medusa op het dark web met aftelklok, en inzage in wat ze in handen hadden. Vanaf dat moment kon er gerichter worden gezocht.
- Op 15/1 kreeg Limburg.net van de data-experten een gecontroleerde en geverifieerde lijst om mee aan de slag te gaan.
- Tijdens de bijzondere raad van bestuur op 17/01 werd beslist om niet in te gaan op de afpersing.
- Op 19/1 communiceerde Limburg.net over het datalek met de kennis die ze op dat moment had. Het ging om lijsten met naam, adres en rijksregisternummer van referentiepersonen uit 2014 en 2015 en een lijst van personen in schuldbemiddeling.
- Op 20/1 verstreek de deadline van het hackerscollectief. Alle data werden openbaar gemaakt. Snel bleek dat er meer data waren gelekt dan oorspronkelijk was vastgesteld.

Communicatie en veiligheidsmaatregelen

Limburg.net heeft steeds open gecommuniceerd over de cyberaanval en de gevolgen voor burgers, met de kennis waarover zij op dat moment beschikte. Dit via haar eigen kanalen en de media. Van bij aanvang is Limburg.net in nauw contact met alle bevoegde autoriteiten (Computer Emergency Response Team, de Gegevensbeschermingsautoriteit , de Vlaamse Toezichtcommissie en de politie). Limburg.net nam meteen extra beveiligingsmaatregelen en zal de beveiliging verder aanscherpen naar de toekomstige Europese beveiligingsnormen (NIS-2 richtlijn). Via haar raad van bestuur en gerichte communicatie, heeft Limburg.net ook de gemeenten op de hoogte gehouden. Op 31 januari volgt een extra infomoment om de burgemeesters en de gemeentelijke algemeen directeurs te informeren over de huidige stand van zaken.

Vlaamse Toezichtcommissie adviseert focus op veiligheid

De Vlaamse Toezichtcommissie raadt Limburg.net aan om geen kruisanalyses te doen op de gelekte data met als doel om aan elke burger exact te laten weten welke gegevens er van hem of haar zijn gestolen. In een schriftelijk advies meldt de Vlaamse Toezichtcommissie aan Limburg.net:

"***De begeleiding van burgers is belangrijker dan de concrete opsomming van de gegevens in de gegevensdiefstal.*** *Het is de prioriteit om na te gaan wat er gebeurd is. Zo kan, waar nodig, de beveiliging opgeschroefd worden. Het is beter om hier tijd en mensen voor aan te wenden, dan als slachtoffer van een cyberaanval bezig te zijn met het documenteren van gegevens per persoon.* ***De sensibilisering over cyberveiligheid en bewustmaking van de gevaren van digitale identiteitsdiefstal moeten nu collectief opgestart worden, zeker naar kwetsbare doelgroepen.*** *Limburg.net engageert zich om de gemeentebesturen en alle inwoners van Limburg en Diest hierin te begeleiden. Het is ook een verantwoordelijkheid van scholen, de media, het middenveld en de overheden in dit land. Het is niet de vraag of, maar wel wanneer en wie het volgende slachtoffer is.* ***Het is onze plicht als samenleving iedereen hiertegen te wapenen****"*

Limburg.net wacht de officiële richtlijn hieromtrent af.

Oproep tot waakzaamheid:

Het lekken van rijksregisternummers brengt het risico met zich mee dat criminelen deze gebruiken voor frauduleuze doeleinden. Fraudeurs kunnen met persoonlijke gegevens die ze van burgers hebben, hun vertrouwen proberen te winnen en hen te overtuigen om extra gegevens (zoals een pincode of wachtwoorden) door te geven of om geld over te schrijven op een rekening. We vragen iedereen om alert te blijven voor mails, brieven of telefoons. Zeker als burgers boodschappen ontvangen van bedrijven of overheidsorganisaties die ze niet verwachten. We roepen iedereen op om in dat geval eerst contact op te nemen met die instanties om misverstanden te vermijden.

> Mensen die vermoeden dat ze het slachtoffer zijn van identiteitsfraude, kunnen best aangifte doen bij de politie of via meldpunt.belgie.be. Wie verdachte mails of berichten ziet, stuurt ze best door naar verdacht@safeonweb.be.
>
> Op www.Safeonweb.be staan heel wat tips rond cyberveiligheid. We raden iedereen aan deze tips toe te passen en zo de beveiliging van persoonlijke gegevens te verbeteren, ook wanneer er geen gegevens gestolen zijn.

Limburg.net zal alle vragen beantwoorden

Limburg.net erkent de ernst van de gegevensdiefstal en begrijpt de ongerustheid. De organisatie zal antwoorden op vragen, maar gezien de omvang van de aanval kan dit enige tijd vergen. Antwoorden op veelgestelde vragen en de laatste stand van zaken zijn te vinden op de website. Specifieke vragen kunnen worden gesteld via mijn.limburg.net.

Expliciete dank voor inzet personeelsleden

Limburg.net heeft ook oog voor zijn medewerkers die zich plichtsbewust en vol toewijding hebben ingezet. Dit is ook een zware periode voor onze medewerkers en we willen hen bedanken voor hun inzet.

Dit bericht is met de visuele tijdslijn als bijlage verstuurd.
Via limburg.net/persmededelingen is er ook een tekstuele versie beschikbaar.

Perscontact:
Hans Roggen – woordvoerder Limburg.net – 0486 33 90 51
limburg.net/persmededelingen