Responsible Disclosure GBLT

GBLT hecht veel belang aan de beveiliging van haar systemen. Ondanks alle voorzorgsmaatregelen blijft het mogelijk dat een tijdelijke zwakke plek in deze systemen te vinden is. Wanneer u een zwakke plek in een van onze systemen heeft ontdekt, vernemen wij dit graag van u, zodat GBLT snel gepaste maatregelen kan nemen. Door het maken van een melding verklaart u zich als melder akkoord met de hierna volgende afspraken over Responsible Disclosure. GBLT zal uw melding met zorg en conform diezelfde afspraken afhandelen.

GBLT vraagt het volgende van u:

- Meld de bevinding binnen 24 uur na de ontdekking van de kwetsbaarheid.
    - Mail de bevinding naar **security@gblt.nl** versleuteld met onze publieke PGP Key die u in de bijlage aantreft op onze website.
- Geef voldoende informatie om het probleem te reproduceren, zodat we het zo snel mogelijk kunnen oplossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.
- Beperk de bevinding tot verifieerbare feitelijkheden die betrekking hebben op de door u geconstateerde kwetsbaarheid.
- Geef eventuele tips die ons kunnen helpen het probleem op te lossen door, als u daartoe bereid bent. Vermijd dat uw advies neerkomt op reclame voor specifieke (beveiligings) producten.
- Beperk de bevinding tot de buitenste schil van het netwerk.
- Laat minimaal een e-mailadres of telefoonnummer achter, zodat we met u in contact kunnen treden om samen te werken aan een veilig resultaat. Het staat u vrij om daarbij anoniem te blijven.
- Maak het probleem niet openbaar en deel het niet met anderen totdat het is opgelost.
  Ook als het niet mogelijk blijkt om het probleem adequaat op te lossen, zullen wij u vragen het niet openbaar te maken of met anderen te delen.
- Wis eventueel verkregen (vertrouwelijke) gegevens zo snel mogelijk.

De volgende handelingen zijn niet toegestaan:

- Misbruiken van het probleem. Download bijvoorbeeld niet méér gegevens dan nodig zijn om het lek te testen. Verwijder of verander daarbij ook geen gegevens, zeker niet van anderen.
- Maak geen gebruik van tooling die bij GBLT overlast kunnen veroorzaken.
- Het plaatsen van malware op onze systemen.
- Het zogeheten “Bruteforcen” van toegang tot onze systemen is niet toegestaan.
- Maak geen gebruik van Social engineering.

GBLT belooft u het volgende:

- Wij reageren binnen drie werkdagen op uw melding met onze beoordeling en voor zover nodig, de verwachte oplossingstermijn.
- Wij houden u op de hoogte van de probleemoplossing.
- Wij behandelen uw melding vertrouwelijk en verstrekken uw gegevens alleen aan anderen als dat van rechtswege verplicht is, bijvoorbeeld door vordering justitie.
- Wij besteden geen publieke aandacht aan meldingen. Alleen als er een meldplicht (datalekken)geldt en de wet GBLT dit voorschrijft. De melder kan anoniem blijven.
- Wij geven een beloning voor meldingen van ons onbekende problemen.
  De grootte van die beloning bepalen we aan de hand van de ernst van het lek en de kwaliteit van de melding. De beloning kan bijvoorbeeld bestaan uit een financiële beloning.