Abuse beleid

Bij Denit besteden wij zorg aan de beveiliging van onze systemen. Desondanks kunnen er toch zwakke plekken bestaan. Als je een zwakke plek in één van onze systemen hebt gevonden, horen wij dit graag zo snel mogelijk, zodat wij maatregelen kunnen treffen als dat nodig is. De richtlijnen zijn hieronder te lezen.

Wij vragen het volgende:

- Mail je bevindingen naar info@denit.nl. De bevindingen dienen met behulp van PGP/GPG versleuteld te zijn met de door ons beschikbaar gestelde public key om te voorkomen dat de informatie in verkeerde handen valt. Voeg je public key toe aan het mailbericht, zodat wij je ook versleutelde berichten terug kunnen sturen. Optioneel kun je ook een telefoonnummer toevoegen, zodat wij je eventueel kunnen bellen om samen te werken aan een oplossing.
- 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.
- Wij houden ons aanbevolen voor tips die ons helpen het probleem op te lossen. Beperk je daarbij wel graag tot verifieerbare feitelijkheden die betrekking hebben op de door jou geconstateerde kwetsbaarheid en vermijd dat je advies in feite neerkomt op reclame voor specifieke (beveiligings) producten.
- Dien de melding graag zo snel mogelijk na ontdekking van de kwetsbaarheid in.

De volgende handelingen zijn niet toegestaan:

- Dreigen de kwetsbaarheid te misbruiken om schade aan te richten als wij je advies niet opvolgen.
- Plaatsen van malware, noch op onze systemen noch op die van anderen.
- “Bruteforcen” van toegang tot systemen, behalve voor zover dat strikt noodzakelijk is om aan te tonen dat de beveiliging op dit vlak ernstig tekort schiet, d.w.z. als het buitengewoon eenvoudig is om met openbaar verkrijgbare en goed betaalbare hardware en software een wachtwoord te kraken waarmee het systeem ernstig kan worden gecompromitteerd.
- Gebruik maken van social engineering, behalve voor zover dat strikt noodzakelijk is om aan te tonen dat medewerkers met toegang tot gevoelige gegevens in het algemeen (ernstig) tekortschieten in hun plicht om daar zorgvuldig mee om te gaan. Dit is het geval wanneer op volkomen legale wijze (dus bijvoorbeeld niet via chantage) in het algemeen het te eenvoudig is om hen over te halen tot het verstrekken van dergelijke gegevens aan onbevoegden. Je dient daarbij alle zorg te betrachten die redelijkerwijs van je verwacht kan worden om de betreffende medewerkers zelf niet te schaden. Je bevindingen dienen uitsluitend te zijn gericht op het aantonen van kennelijke gebreken in onze procedures en werkwijzen en niet op het schaden van individuele personen die bij ons werkzaam zijn.
- Openbaar maken of aan derden verstrekken van informatie over het beveiligingsprobleem voordat het is opgelost.
- Verrichten van handelingen die verder gaan dan wat strikt noodzakelijk is om het beveiligingsprobleem aan te tonen en te melden, in het bijzonder waar het gaat om het verwerken (waaronder het inzien of kopiëren) van vertrouwelijke gegevens waar je door de kwetsbaarheid toegang toe hebt gehad. In plaats van een complete database te kopiëren, kun je normaliter volstaan met bijvoorbeeld een directory listing. Het wijzigen of verwijderen van gegevens in het systeem is nooit toegestaan.
- Gebruik maken van technieken waarmee de beschikbaarheid en/of bruikbaarheid van het systeem wordt verminderd (DoS-aanvallen).
- Op wat voor (andere) wijze dan ook misbruik maken van de kwetsbaarheid.

Wat je van ons mag verwachten als je je aan het bovenstaande houdt:

- Indien je aan alle bovenstaande voorwaarden voldoet, zullen wij geen strafrechtelijke aangifte tegen je doen en ook geen civielrechtelijke zaak tegen je aanspannen.
- Als achteraf blijkt dat je een bovenstaande voorwaarde toch hebt geschonden, kunnen wij alsnog besluiten om stappen tegen je te ondernemen.
- Wij behandelen een melding vertrouwelijk en delen persoonlijke gegevens van een melder niet zonder diens toestemming met derden, tenzij wij daar volgens de wet of een rechterlijke uitspraak toe verplicht zijn.
- Wij kunnen de ontvangen informatie over de geconstateerde kwetsbaarheid altijd delen met de relevante toeleveranciers van de door ons gebruikte systemen. Wij vragen onze toeleveranciers zich te houden aan alles wat wij in dit abuse beleid beloven.
- In onderling overleg kunnen we, indien wenst, je naam vermelden als de ontdekker van de gemelde kwetsbaarheid. In alle andere gevallen blijf je anoniem.
- Wij sturen je direct na ontvangst een automatische ontvangstbevestiging.
- Wij proberen binnen 5 werkdagen inhoudelijk te reageren op een melding met een (eerste) beoordeling en eventueel een verwachte datum voor een oplossing.
- Wij lossen het door jou gemelde beveiligingsprobleem zo snel mogelijk op en proberen daar nooit langer over te doen dan 90 dagen. Wij zijn daarbij vaak wel mede afhankelijk van toeleveranciers.
- Op jouw verzoek, kunnen wij je op de hoogte houden hoe ver we zijn met het oplossen.
- In onderling overleg kan worden bepaald of en op welke wijze over het probleem wordt gepubliceerd, nadat het is opgelost.
- Wij kunnen je een beloning bieden als dank voor de hulp. Afhankelijk van de ernst van het beveiligingsprobleem en de kwaliteit van de melding, kan die beloning variëren van een eenvoudig ‘dankjewel’ tot een bedrag van maximaal € 500,-. Het moet hierbij wel gaan om een nog onbekend en serieus beveiligingsprobleem.

Denit