Responsible Disclosure

Kwetsbaarheid ontdekt? Laat het ons zo snel mogelijk weten.

Bij Korton vinden wij de veiligheid van onze systemen, ons netwerk en onze producten erg belangrijk. Wij besteden dan ook veel aandacht aan hoge beveiliging. Toch kan het voorkomen dat er een zwakke plek of kwetsbaarheid aanwezig is.

Indien u een dergelijke zwakke plek of kwetsbaarheid in één van onze systemen treft, stellen wij het zeer op prijs dat u ons hiervan op de hoogte brengt, zodat wij zo spoedig mogelijk passende maatregelen kunnen treffen.

Wij hanteren voor meldingen de zogenaamde 'Responsible Disclosure' principes. Dit heeft tot gevolg dat bij het verantwoord handelen met betrekking tot de getroffen kwetsbaarheid, wij dit zullen belonen als teken van waardering.

Korton vraagt van u als melder:

- Uw bevindingen te mailen naar security@korton.nl;
- De melding zo spoedig mogelijk na ontdekking van de kwetsbaarheid te doen;
- De juiste contactgegevens achter te laten, zodat wij met u in contact kunnen treden om samen te werken aan een veilig resultaat. Laat minimaal uw naam, een emailadres en telefoonnummer achter;
- Schriftelijk te bevestigen dat u conform deze "Responsible Disclosure" heeft gehandeld en zult blijven handelen;
- Voldoende informatie te geven om het probleem te reproduceren, zodat wij adequaat kunnen reageren en het probleem zo snel mogelijk kunnen oplossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende;
- Het probleem niet met anderen te delen;
- Verantwoordelijk om te gaan met de kennis over het beveiligingsprobleem door geen handelingen te verrichten die verder gaan dan noodzakelijk zijn om het beveiligingsprobleem aan te tonen. Wij nemen uw melding altijd serieus en zullen bij elk vermoeden van een kwetsbaarheid onderzoek verrichten.

Vermijd daarom de volgende handelingen:

- Het plaatsen van malware;
- Het kopiëren, wijzigen of verwijderen van gegevens in een systeem;
- Het aanbrengen van veranderingen in het systeem;
- Het herhaaldelijk toegang tot het systeem verkrijgen of de toegang delen met anderen;
- Het gebruikmaken van geautomatiseerde scantools;
- Het gebruik maken van het zogeheten "bruteforcen" van toegang tot systemen;
- Het gebruik maken denial-of-service of social engineering.

Wat mag u van Korton verwachten?

- Indien u bij de melding van een door u geconstateerde kwetsbaarheid aan bovenstaande voorwaarden voldoet, zal Korton geen juridische consequenties verbinden aan deze melding.
- Korton behandelt een melding vertrouwelijk en deelt persoonlijke gegevens niet zonder toestemming van de melder met derden, tenzij dit wettelijk of uit hoofde van een rechterlijke uitspraak verplicht is. Melden onder een pseudoniem is ook mogelijk.
- Korton vraagt u schriftelijk te bevestigingen dat u conform deze 'Responsible Disclosure' heeft gehandeld en zult blijven handelen (en vraagt om uw contactgegevens voor zover die nog niet bekend waren).
- Korton houdt u op de hoogte over de beoordeling van de melding en de status van het oplossen van het probleem.
- Korton lost het door u geconstateerde beveiligingsprobleem in een systeem zo snel mogelijk op.

Korton biedt een beloning als dank voor de hulp. Afhankelijk van de ernst van het beveiligingsprobleem en de kwaliteit van de melding, kan die beloning variëren. Passend bij de wensen van de melder, en op basis van redelijkheid, zullen we de beloning, na melding en onderzoek, verder met u afstemmen. Als voorwaarde geldt wel dat het een voor Korton een nog onbekend en serieus beveiligingsprobleem betreft.