Beveiliging bij EBLINC (https://eb.arbeidsvoorwaarden.com **)**

Loginnaam

Deze is verbonden aan het e-mail adres van de werkgever. Bij dienstverlating is het voor de ex-werknemer niet meer mogelijk om in te loggen.

Password

De wachtwoorden worden automatisch door het systeem gegenereerd. Het wachtwoord is een combinatie van cijfers, letters en aantal posities . Degene die inlogt heeft zelf de mogelijkheid om een nieuwe code aan te maken.

SSL key van Comodo

Voor alle specificaties van de SSL key verwijzen wij naar de website van Comodo www.comodo.com.

Daarnaast is de “arbeidsvoorwaarden” website beveiligd tegen:

1. In principe kun je nu wel een deep link maken naar een pagina ergens in het systeem, je kunt hiermee alleen niet de beveiliging omzeilen omdat voor alle pagina’s autorisatie vereist is.
2. SQL injection attacks (beveiliging tegen het invoeren en uitvoeren van SQL code in de internetpagina’s om zo ongeautoriseerde wijzigingen in de database te maken).
3. De querystring wordt nu wel gebruikt maar er wordt op bijna alle plekken gebruik gemaakt van dynamische parameters waardoor een aanval via de querystring niet mogelijk is. Daarnaast zit er nog een extra beveiliging in dat aanpassing van de querystring niet geaccepteerd wordt door de applicatie.
4. Het is niet mogelijk om javascript in te voeren middels velden in de applicatie.
5. Applicatie is geprogrammeerd rekening houdende met de OWASP standaard.

Security vanuit de provider

Arbeidsvoorwaarden is veilig en betrouwbaar in gebruik en op de diverse niveaus beschermd tegen onbevoegden en verlies van informatie:

Voor veiligheid en betrouwbaarheid werkt Arbeidsvoorwaarden met:

- Https verbinding (een beveiligde SSL lijn (Secured Soccer Layer)
- Login door middel van wachtwoorden en administratieve naam
- Dagelijkse Back-ups
- Professioneel datacenter met 24/7 beheer

De servers waarop Arbeidsvoorwaarden draait en die voor alle gebruikers via een browser vanuit elke plaats bereikbaar zijn, zijn ondergebracht bij Alpina Group.

SSL Certificaat met Extended Validation

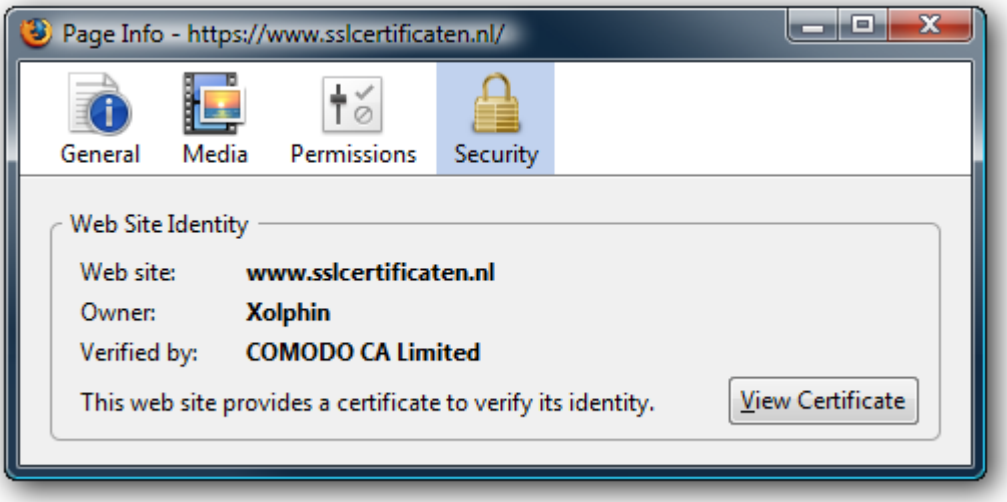
Bij certificaten met een validatie procedure waarbij de bedrijfsgegevens gecontroleerd worden, worden deze bedrijfsgegevens ook in het certificaat opgenomen. Met behulp van deze bedrijfsgegevens kunnen bezoekers van een website de eigenaar eenvoudig controleren. Klanten kunnen er van uit gaan dat de identiteit van de eigenaar correct is, de identiteit van de eigenaar wordt volgens de procedures van de uitgever van het certificaat immers vastgesteld.

Klanten lopen bij certificaten zonder bedrijfsgegevens het risico dat de website van een andere eigenaar is dan dat zij verwachten. Dit kan bijvoorbeeld gebeuren indien een domeinnaam gebruikt wordt die sterk lijkt op de domeinnaam van een andere website. Indien bedrijfsgegevens in het certificaat ontbreken, zijn klanten niet in staat de eigenaar van een website vast te stellen, waardoor het vertrouwen in een website afneemt.

Certificaat met Bedrijfsgegevens

Certificaten met bedrijfsgegevens tonen aan door welk bedrijf het certificaat is verstrekt. Bezoekers zien de bedrijfsnaam en adresgegevens van de eigenaar van het certificaat staan, wat meer vertrouwen geeft.

De bedrijfsgegevens worden alleen bij een certificaat met Extended Validation in de adresbalk weergegeven.



Voorbeeld van een Comodo EV certificaat

Alpina Group

In de bijlages (Security measures Alpina Group) geven we u meer achtergrond informatie mbt de veiligheidsmaatregelen bij Alpina Group.

PEN-Test

De klant heeft het recht om een Pen-test uit te voeren op EBlinC, uiteraard in overleg met EBlinC, de kosten zijn voor de opdrachtgever (klant).

SSL test

De klant heeft het recht op het opvragen van een grondige analyse (test) ten aanzien van de configuratie van onze SSL-webserver, de kosten zijn voor de opdrachtgever (klant).

GDPR (“State of the Art”)

Wij houden rekening met de stand van de techniek, de uitvoeringskosten en de aard, reikwijdte, context en doeleinden van de verwerking, alsmede het risico van uiteenlopende waarschijnlijkheid en ernst voor de rechten en vrijheden van natuurlijke personen en spannen ons in om passende technische en organisatorische maatregelen te treffen om het beveiligingsniveau te waarborgen. Bijvoorbeeld:

- de pseudonimisering en codering van persoonlijke gegevens;
- het vermogen om de voortdurende vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van verwerkingssystemen en -diensten te waarborgen;
- de mogelijkheid om de beschikbaarheid en toegang tot persoonlijke gegevens tijdig te herstellen in geval van een fysiek of technisch incident;

- een proces voor het regelmatig testen, beoordelen en evalueren van de effectiviteit van technische en organisatorische maatregelen om de beveiliging van de verwerking te waarborgen.
- bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de risico's die door de verwerking worden veroorzaakt, met name door accidentele of onwettige vernietiging, verlies, wijziging, ongeautoriseerde openbaarmaking van of toegang tot persoonsgegevens die worden doorgegeven, opgeslagen of anderszins verwerkt.

Overweging (Recital 78)

Bij het ontwikkelen, ontwerpen, selecteren en gebruiken van toepassingen, diensten en producten die zijn gebaseerd op de verwerking van persoonsgegevens of het verwerken van persoonsgegevens om hun taak te vervullen, moeten producenten van producten, diensten en toepassingen worden aangemoedigd rekening te houden met het recht op gegevens bescherming bij het ontwikkelen en ontwerpen van dergelijke producten, diensten en toepassingen en, met inachtneming van de “stand van de techniek”, om ervoor te zorgen dat controllers en verwerkers in staat zijn om hun verplichtingen inzake gegevensbescherming na te komen.

Tot zover de opmaak en informatieverstrekking inzake de beveiligingsmaatregelen van EBlinC.

Security measures Alpina group

Fire protection data center:

De datacenterlocaties zijn voorzien van brandmelders en automatisch werkende blusvoorzieningen. Deze voorzieningen worden jaarlijks gekeurd.

Cooling data center:

De datacenterlocaties zijn voorzien van passende koelinstallaties. Serverkasten worden zo ingericht (plaatsing apparatuur en/of afdekplaten) dat warmte op de juiste wijze wordt afgevoerd.

Power supply data center:

De datacenterlocaties zijn voorzien van backup-stroom en een noodstroomvoorziening. Apparatuur wordt via twee gescheiden voedingen aangesloten binnen de geldende aansluitwaarden.

Periodiek wordt de werking van de noodstroom getest en worden belastingmetingen uitgevoerd.

Data security

Backup procedure:

Data wordt opgeslagen op redundante storage en gerepliceerd tussen beide datacenterlocaties.

Er is daarnaast een backupprocedure in werking waarbij data op speciaal daarvoor (gescheiden) storage wordt weggeschreven. De backup procedure voorziet ook in het opslaan van backups op een “off-line omgeving”/archief.

De werking van de backupprocedure wordt dagelijks gemonitord. Periodiek wordt via een beperkte restore vastgesteld dat de backup succesvol kan worden teruggezet.

Updates and patches:

De systemen worden conform het patch- update beleid voorzien van benodigde updates. Dit vindt veelal via een geautomatiseerd proces plaats.

Er is een proces voor het identificeren van kwetsbaarheden ingericht. Vanuit zowel de tooling voor updates als vanuit het Security Information & Eventmanagement systeem (SIEM). Daarnaast worden de relevante informatiekanalen gevolgd. Zonodig wordt een proces gestart om een ontdekte kwetsbaarheid direct weg te nemen of om andere risicobeperkende maatregelen te treffen.

Security management for the network:

Beveiliging van het netwerkverkeer is ingericht via de toepassing van diverse technieken.

- Netwerk segmentering is toegepast waardoor kritische gegevens in een afgeschermde zone zijn geplaatst welke via firewalls bewaakt worden.
- Gebruik wordt gemaakt van de secure-protocollen.
- Op datacenterlocaties en kantoorlocaties is toegang tot netwerkapparatuur beperkt tot geautoriseerde personen.
- Er wordt gebruik gemaakt van poort-security.
- Netwerkverkeer wordt gemonitord vanuit het SIEM
- Verbindingen met externe partijen worden ingericht via VPN.

System monitoring:

Er is een proces van systeemmonitoring ingericht waarmee fouten, defecten en relevante (security) events worden gemeld.

- Er is een 24/7 storingsdienst ingericht.
  Protection against malware
- Apparatuur is voorzien van endpoint protectie
- Mailverkeer wordt gescand op de aanwezigheid van onveilige bijlages, malware, en onveilige (phising-) links.
- Er zijn policies ingericht ter voorkoming van misbruik van de domeinen/afzender adressen welke beheerd worden.

Overige maatregelen:

- Wachtwoorden dienen te voldoen aan het wachtwoordbeleid (sterke wachtwoorden) en deze moeten periodiek worden gewijzigd.
- Voor alle accounts wordt multi-factor-authenticatie afgedwongen.
- Risicovolle / verdachte loginpogingen worden gedetecteerd; afhankelijk van de situatie zal gevraagd worden om een extra login, zal de login geweigerd worden of zal het account geblokkeerd worden.
- Er zijn policies ingericht op basis van geografische locatie.
- Verdachte inlogevente worden gemeld vanuit het SIEM en van daaruit geanalyseerd en zonodig opgevolgd.