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 Missing Piece.

Indien u meer wilt weten over Missing Piece, kunt u daarover informatie vinden via https://missingpiece.nl/

SSL Certificaat met Extended Validation

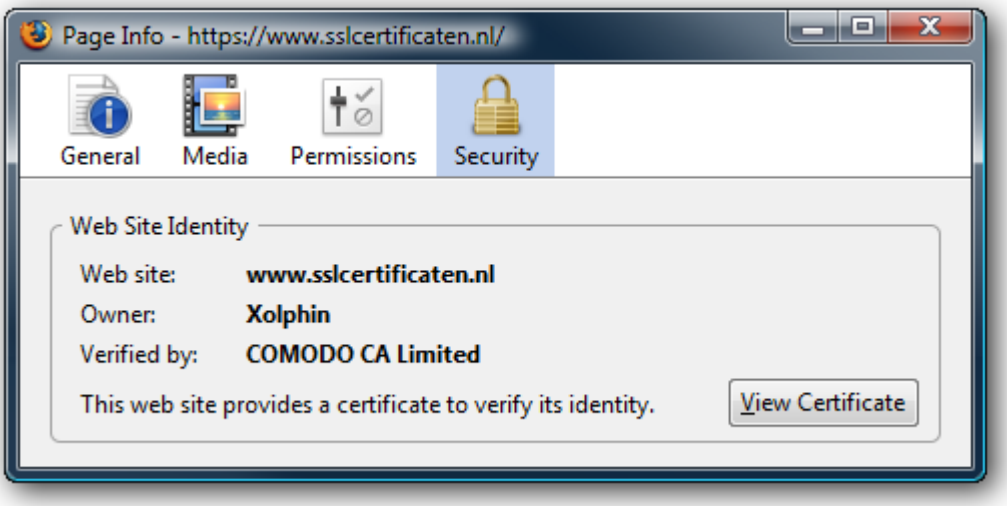
Bij certificaten met een validatie procedure waarbij de bedrijfsgegevens gecontroleerd worden, worden deze bedrijfsgegevens ook in het certificaat opgenomen. Met behulp van deze bedrijfsgegevens kunnen bezoekers van een website de eigenaar eenvoudig controleren. Klanten kunnen er van uit gaan dat de 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

Missing Piece

In de bijlages (Security measures Missing Piece BV) geven we u meer achtergrond informatie mbt de veiligheidsmaatregelen bij Missing Piece.
Missing Piece hecht grote waarde aan informatiebeveiliging en is ISO 27001 gecertificeerd. De scope van deze certificering betreft de gehele organisatie.

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 Missing Piece BV

- 2 independent surveillance services;

- Redundant connection to the emergency room;

- Double authentication with RFID access cards and iris scanners;

- VEB certified, security class 4;

- ISO / IEC 27001 and NEN 7510 certified.

Fire protection data center:

The server rooms at BIT are equipped with an independent, certified very early warning system with automatic reporting to the fire department. When a fire breaks out, the oxygen concentration in the room is lowered by gas extinguishing so that the fire is extinguished quickly. A gas mixture of Argon and nitrogen is used for this (Argonite). By fighting the fire in this way, there is no (water) damage to the equipment.

Cooling data center:

BIT's data centers are full of servers that produce a lot of heat. With more computer activity, this means that more heat is also released, and that requires specialized, scalable and reliable heat management. Inadequate cooling can cause expensive interruptions.

The cooling installation in combination with the closed cold corridors ensures optimum cooling of all equipment. The installation is redundant at all points, including pumps and pipework. In addition, the installation is as energy efficient as possible, which saves both the environment and costs.

Power supply data center:

For companies, organizations and governments, a good power supply is one of the most important reasons for placing their IT equipment in a data center. To guarantee the reliability of that power supply, the emergency power supplies are tested on a monthly basis.

BIT-2BCD has 2 direct connections to the distribution station of the network operator. The power and emergency power supply are fully doubled up to the racks.

Data security

Backup procedure:

The production data is continuously written to production (hard) disks. These production disks are multiple (redundant). This data is then copied to backup disks and the data is additionally copied to backup disks, off-site, in a separate data center. The backup disks are also multiple in both cases.

The backup is made six (6) nights per week (Monday to Saturday) and is available for a period of 90 days.

Six (6) nights per week (Monday to Saturday) an extra backup is made of the production data to the backup disks, off-site, in a separate data center. This backup is available for a period of 5 days and serves as disaster recovery.

All backup processes are provided with verification as standard, with this written data is read again and it is made plausible that the data has not only been successfully written, but that it can also be read. If an error is found here, a visual notification will be made of this in the network monitoring tool PRTG, and the backup record in the IT Service Management system will also show the failed backup. This backup record is also visible to the customer in the Missing Piece Service Portal.

Every working day, a check is made on the statuses of the backup (independently of the above reports). If a backup is not successful, the cause of the failure will be resolved and the backup will be restarted manually.

Restore test procedure:

Every Saturday the restore test procedure is carried out automatically, a restore test takes place for all available backup jobs (= all customers who have stored their data in our data centers).

The procedure is only performed for the data at the primary data center (BIT, Ede).

The restore takes place randomly for each backup job, so there is no full restore. The following method is used for the sample.

- minimum file size is 10kb, the maximum file size is 1mb

- the file is older than 100 days

- the number of files to be restored is a maximum of 100 pieces

- the maximum number of retries on the servers is 10 (is a server accessible)

- the maximum number of retries on the files is 100

If an error is found in the restore, this will be visually visible in the PRTG monitoring tool, and the restore test record in the IT Service Management system will also show the failed restore test. This is also visible to the customer in the Missing Piece Service Portal.

Updates and patches:

Microsoft updates

- The updates are automatically downloaded several times a day

- The PRTG monitoring tool gives a notification that updates have been retrieved

- These updates are automatically installed daily (at night) on the workstations (fat clients, only if they are connected to the network) and the Web servers

- The updates are automatically installed weekly on a number of selected XAPs (Citrix servers), these are the Missing Piece servers and the Missing Piece test environment

- If there are updates (PRTG notification), these are installed manually every week by the system administrator on 10 selected INFRA servers

- On the last Friday of the month a (Senior) system administrator gives a manual approval for performing the updates on all XAP servers, all ASK servers and all INFRA servers

- Following the aforementioned approval, the updates on all XAP servers are carried out automatically in the night from Friday to Saturday

- Same for the ASK and INFRA servers in the night from Sunday to Monday

A reboot is automatically performed for each server that is updated. It may be decided not to perform certain updates if there are signals from third parties that report problems as a result of an update.

Updates thin clients

Thin clients are updated by the System Administration department when found necessary, this is assessed at least every quarter.

Updates other software

Other updates are carried out if there are signals from third parties that there is, for example, a security breach. In addition, a schedule has been made with which frequency at least to check for updates.

Security management for the network:

- The data passing through the public network are protected in various ways.

  - Connections from customer locations to the data center are secured through site to site VPN (Virtual Private Network).
  - Connections that are established by telecommuting are secured by means of SSL VPN (Secure Socket Layer VPN).

- For e-mail traffic, the 'preferred' option for encryption (TLS) is enabled in the mail server.

- The data passing through the wireless network is secured by encrypting (delivered) Wifi by means of WPA2PSK.

- The equipment connected to the network from external locations is protected by the requirement to log in with an RSA token.

- The availability of network services is guaranteed because everything in the SAN, UCS system and network equipment is redundant. In addition, the production equipment has 24/7/4 support contracts.

System monitoring:

Missing Piece uses the network monitoring tool PRTG

Through PRTG, more than 11000 sensors monitor a lot such as: the network, back-up / restore test, power consumption, updates, certificates, etc. Alerts have been set for certain problems. The alert can consist of:

- an e-mail message to the Service Desk

- a message on the monitoring screen in the System Administration department (these messages are also displayed on the smartphones of the employees of this department)

Protection against malware

Measures against malware have been taken at different levels:

- Incoming and outgoing email traffic is scanned by means of ESA (email security appliance).

- The exchange server scans emails using Trendmicro Scanmail.

- All Windows machines contain anti-virus software (Microsoft System Center Endpoint Protection)

Alerts are sent to the service desk and a selective group based on file masks of cryptoware extensions. In addition, the user is automatically logged out with certain extensions.

In addition, Windows firewall rules block traffic between customers so that malware cannot spread between customers.

Other:

The following password policy applies within the Missing Piece environment:

- a password must meet the following conditions (this is enforced by the system):

- use at least seven characters (preferably create a password with 12 positions or more)
- the previous 24 passwords cannot be reused
- the login, first name and last name may not be part of the password
- a password must contain one or more characters from three of the following four categories:
- capital letters
- lowercase letters
- numbers
- non-alphanumeric characters such as punctuation marks

- if you enter a wrong password 5 times, the account will be "locked" for half an hour, after which a login attempt can be made again, a request can also be made to the Service Desk for a password reset.

- passwords must be changed every 120 days, the user will be notified by e-mail; logging in is only possible after the password has been changed.

Screensaver settings within the environment:

Automatically switched on after 30 minutes of inactivity.