Beveiliging mijn.loondossier.nl

Inleiding

Dit document behandelt de beveiligingsmaatregelen die genomen zijn om de gegevens die opgeslagen zijn op mijn.loondossier.nl te beschermen tegen toegang door onbevoegden. Deze maatregelen zijn onder te verdelen in vier groepen:

1. Organisatorisch
2. Fysiek
3. Virtueel
4. Softwarematig

Hieronder volgt voor elke groep een toelichting.

Organisatorisch

Beheer van de ICT-architectuur en de beveiliging daarvan is strikt gescheiden. De inrichting van het datacentrum is verzorgd door een externe partij, die deze tevens beheert. Ontwerp, implementatie en beheer van de beveiliging (lees: de firewalls) zijn in handen van een tweede externe partij. Elke wijziging in de beveiliging moet bij deze partij worden aangevraagd en wordt vervolgens - indien goedgekeurd - ook door deze partij uitgevoerd.

Fysiek

Er zijn twee datacentra: het hoofd-datacentrum HDC en het backup-datacentrum BDC. Alle voorzieningen in het HDC (web-, opslag-, databaseservers) zijn daar dubbel uitgevoerd. Alle relevante gegevens worden periodiek gekopieerd naar het BDC, waar deze voorzieningen enkelvoudig zijn uitgevoerd. Bij falen van het HDC wordt handmatig overgeschakeld naar het BDC.

Het HDC bevindt zich in een datacentrum van een grote hosting-partij in Amsterdam. Toegang tot dit datacentrum is alleen mogelijk indien vooraf aangemeld en na identificatie. Het BDC is virtueel en in het geheel niet fysiek toegankelijk.

Virtueel

In het HDC is het publiek toegankelijke deel - waar zich de webservers bevinden - virtueel gescheiden van het interne deel, waar zich de overige servers bevinden (database, opslag, management). De twee delen hebben gescheiden netwerksegmenten en de toegang tussen de twee segmenten wordt ook weer geregeld door een firewall - die weer beheerd wordt door de externe partij.

Het publieke deel heeft geen toegang tot Internet, maar kan vanaf het hele internet bereikt worden - dit is nodig voor de webservers. Het interne deel is alleen toegankelijk vanaf specifieke IP-adressen, alweer geregeld door een firewall, en heeft evenmin toegang tot internet. Beheer van het datacentrum kan alleen door vanaf een van de specifieke IP-adressen toegang te krijgen tot de management-server, die de toegang tot de overige servers regelt. Het wachtwoord voor deze server is automatisch gegenereerd en bestaat uit minstens 16 willekeurige tekens.

Ook het BDC is alleen toegankelijk vanaf specifieke IP-adressen, ook weer met een gegenereerd wachtwoord. De webserver in het BDC is normaal gesproken zelfs niet publiek toegankelijk: dit wordt pas zo bij handmatige overschakeling van het HDC naar het BDC.

Softwarematig

Zoals aangegeven zijn de webservers de enige servers die publiek toegankelijk zijn. Toegang tot mijn.loondossier.nl verloopt over https, waardoor de verbinding altijd versleuteld is. Gebruikers krijgen toegang tot de website via een combinatie van gebruikersnaam en wachtwoord. Wachtwoorden worden niet opgeslagen: wel de van een random salt voorziene hash van het wachtwoord (voorziening tegen dictionary attacks).

Voor toegang door externe services (o.a. de mobiele apps, maar ook Loon zelf) geldt hetzelfde: de verbinding loopt allereerst over https. Ten tweede vraagt de service een zogenaamd token aan via een procedure met een combinatie van gebruikersnaam, wachtwoord en random seed (voorziening tegen replay attacks) waarmee voor een bepaalde periode toegang wordt gekregen tot de gegevens op mijn.loondossier.nl (doorgaans een uur, eveneens tegen replay attacks). Het wachtwoord gaat in die procedure nooit ongehasht over de lijn en die hash hangt weer af van de random seed.

De web site is architectonisch gescheiden in losse delen voor elke rol (klant, werkgever, werknemer) waardoor op een centrale plek ingericht kan worden hoe de toegang tot de gegevens verloopt. Werknemers hebben daardoor geen toegang tot werkgevergegevens, werkgevers alleen tot de gegevens van hun eigen werknemers, enzovoort.

Om XSS-aanvallen te voorkomen wordt invoer van de website nooit gebruikt voor weergave op het scherm dan wel als parameter voor SQL-queries.

Disclaimer

De hierboven beschreven veiligheidsmaatregelen bieden uiteraard & helaas geen waterdichte garantie tegen onbevoegde toegang. Een dergelijk garantie is nu eenmaal niet te geven, omdat:

1. hardware en software van derden beveiligingslekken kunnen vertonen waar deze partijen zelf nog geen weet van hebben
2. menselijke fouten niet uit te sluiten zijn

Voor beide punten geldt echter wel, dat er ‘best practices’ zijn om de risico’s te minimaliseren.

Ad 1: Veel beveiligingsmaatregelen worden geleverd door gespecialiseerde firewalls gebaseerd op Linux. Deze vervullen slechts één taak, namelijk toegangsbeveiliging, waardoor er weinig complexe software op draait, die bovendien open source is en ook nog eens al lang stabiel is. Kwetsbaarheden zijn in deze firewalls al jaren niet meer gevonden. Door middel van deze firewalls is de ‘attack surface’ van de datacentra bovendien beperkt tot het absolute minimum: enkele poorten op enkele IP-adressen, en (afgezien van https-verkeer) alleen vanaf specifieke IP-adressen.

Ad 2: Het gescheiden beheer van de firewalls garandeert de betrokkenheid van twee partijen bij alle beslissingen over en de uitvoering van beveiligingsmaatregelen, waardoor menselijke fouten zo veel mogelijk worden uitgesloten.