Breng *cashflow* in je business

Cybersecurity:

Zo houden wij én jij jouw salarisadministratie veilig

Inleiding
Cybersecurity

Oktober is de Europese maand van cybersecurity. Niet voor niets wordt in deze maand aandacht gevraagd voor digitale veiligheid: maar liefst een kwart van de bedrijven in de EU, groot en klein, heeft recent te maken gehad met ICT-veiligheidsincidenten zoals datadiefstal (Eurostat, 2022). 7 op de 10 Nederlandse bedrijven schatten de risico's van een cyberaanval te laag in (AP, 2023).

Bij cyberaanvallen wordt vaak data buitgemaakt en doorverkocht. Salarisadministraties bevatten veel persoonlijke informatie over medewerkers, zoals namen, adresgegevens en bankrekeningnummers. Die data mag niet op straat komen te liggen. Dat kan, naast persoonlijk leed, tot gigantische financiële schade voor het bedrijf leiden, reputatieschade, geschaad vertrouwen van klanten en uiteindelijk zelfs tot faillissement.

Hoe houd jij de data in jouw salarisadministratie veilig? En hoe bewaakt Cash die?

In deze whitepaper geven we antwoord op deze vragen.

Maak niet de vergissing dat digitale veiligheid (alleen) een IT-aangelegenheid is. Drie kwart van de datalekken ontstaan door een menselijke fout (Verizon, 2023). Dat maakt cybersecurity een verantwoordelijkheid van elke medewerker, ook van jou, als salarisadministrateur of accountant, en van ons natuurlijk, als leverancier van jouw salarisadministratiesoftware in de cloud.

Inhoud Whitepaper

Heb belang van *cybersecurity*

Je moet er niet aan denken dat jouw salarisadministratie op straat komt te liggen. Toch gebeurt het vaak, ook in Nederland, dat persoonsgegevens in verkeerden handen komen door een cyberaanval.

Salarisadministratie achter slot en grendel

Voor je salarisadministratie gebruik je Cash Payroll. Logisch, want zo kunnen accountants, in-house-payrollprofessionals, managers en medewerkers allemaal tegelijk in dezelfde administratie werken. Thuis, op kantoor of op reis, en in realtime.

Werken in Cash Payroll is efficiënter, gemakkelijker en ook veiliger dan gevoelige informatie in losse bijlagen heen en weer e-mailen. Maar goede databeveiliging is cruciaal.

Bedrijven zijn tegenwoordig vaak doelwit van digitale aanvallen waarbij data wordt buitgemaakt. Bijna een kwart van de bedrijven in de EU, groot en klein, heeft recent te maken gehad met ICT-veiligheidsincidenten zoals datadiefstal (Eurostat, 2022). En dat zijn alleen nog maar de incidenten die gemeld zijn. Datadiefstal kan ook ongemerkt plaatsvinden, de data wordt dan vaak op het dark web te koop aangeboden.

Je moet er niet aan denken dat jouw salarisadministratie op straat komt te liggen. Toch gebeurt het vaak, ook in Nederland, dat persoonsgegevens in verkeerde handen komen door een cyberaanval.

Daarom heeft Cash de salarissoftware die jij gebruikt optimaal beveiligd. Daarover vertellen we je alles in het volgende hoofdstuk. Het is ook belangrijk dat je weet wat jij kan doen om incidenten te voorkomen. Zie daarvoor hoofdstuk 3.

Voorbeelden van grote cyberaanvallen in Nederland

- Bij de hack van een politieaccount zijn contactgegevens en functies van alle politiemensen op straat komen te liggen. (Rijksoverheid, 2024)

- Gegevens van vrijwel alle medewerkers van de HU zijn in verkeerde handen gekomen na een cyberaanval op IT-dienstverlener ID-ware. Ook de Tweede Kamer, de Technische Universiteit Eindhoven, TNO en Prorail zijn getroffen. (FD, 2022)

- Bij een aanval op software die onder meer de NS, VodafoneZiggo, CZ en ArboNed gebruiken, werden klantgegevens van zeker 2 miljoen Nederlanders buitgemaakt. (NOS, 2023)

Hoe Cash jouw data *veilig houdt*

Als jouw softwareleverancier voor HR- en salarisadministratie hebben én voelen we een grote verantwoordelijkheid om jouw data veilig te houden. Dat doen we door:

- sterke veiligheidsmuren te bouwen;
- onze servers in Europa te houden;
- data te versleutelen;
- een slimme en moderne infrastructuur te maken, met schadebeperkende maatregelen voor als gebruikers per ongeluk zelf de deur open zetten' (denk aan extra veiligheidslagen bij het inloggen en streng afgekaderde toegang voor verschillende gebruikers);
- kennis en tips over cybersecurity met onze gebruikers te delen;
- van de experts en tools gebruik te maken van de Visma Groep;
- door ons te committeren aan alle (rapportage-)verplichtingen van het Visma Security Programma.

Sterke veiligheidsmuren, tests en controles

Rondom jouw salarisadministratie staan sterke veiligheidsmuren: firewalls, in jargon. Virusscanners draaien non-stop. Onze datacenters staan bewust in Europa, waar strenge wetgeving geldt voor databeveiliging. De veiligheid van onze datacenters wordt periodiek gecontroleerd en bevestigd door onafhankelijke auditors. Alles wat we bouwen, wordt zorgvuldig getest. Intern en extern.

Schade beperken bij menselijke fouten

We hebben onze software zo ontworpen, dat de schade beperkt blijft als mensen fouten maken (zoals hun inloggegevens prijsgeven):

- In Cash Payroll stel je zelf in welke gebruiker, wat voor toegang krijgt tot de salarisadministratie. (In vaktermen: role-based access control, of RBAC.) Zie het als een gebouw, met niet alleen maar een buitendeur die toegang geeft tot de complete salarisadministratie, maar met allemaal verschillende kamers die elk een eigen deur hebben. Jij geeft gebruikers alleen de sleutel van de kamers waar ze moeten zijn.
- Data die staat opgeslagen in de salarisadministratie en de data die daar in en uit stroomt, zijn versleuteld. Mochten kwaadwillenden er onverhoopt toegang toe hebben gekregen, dan is de data niet uit te lezen.
- Omdat wachtwoorden te kraken, raden en ontfutselen zijn, hebben we het mogelijk gemaakt dat je in Cash Payroll kan inloggen met twee-factor-authenticatie (2FA, of: multifactorauthenticatie, MFA). Als je deze optie aan zet, betekent het dat jij, jouw klanten en/of jouw medewerkers het inloggen nog moeten bevestigen op hun telefoon of in hun e-mail. Zelfs met gelekte of ontfutselde inloggegevens kunnen kwaadwillenden dan de salarisadministratie nog niet in.

Let op: het is aan jou of je 2FA wil gebruiken. We raden het je wel ten zeerste aan: het is een van de gemakkelijkste maar effectiefste veiligheidsmaatregelen die je kan nemen!

Visma Security Programm

We hebben een team van toegewijde collega's die zich samen inzetten voor de beveiliging van onze software. We worden daarin bijgestaan door beveiligingsexperts van de Visma Groep, waartoe Cash behoort.

Als onderdeel van de Visma-familie is Cash gehouden aan het strenge veiligheidsbeleid van Visma. Visma deelt met haar dochterondernemingen kennis, mensen en tools om die veiligheid naar het hoogste niveau te tillen. Elk Visma-bedrijf, zo ook Cash, wordt automatisch onderdeel van het Visma Security Programma. Alle deelnemers aan Visma Security Programma committeren zich aan een bepaalde kwaliteitsstandaard voor de digitale veiligheid van hun producten. Het programma omvat onder meer:

- (verplichte) trainingen;
- rapportageverplichtingen;
- controles, tests en 24/7-monitoring;
- kennisdeling en hulp bij incidenten;
- en het gebruik van tal van state of the art veiligheidstools.

Visma's Chief Information Security Officer Cindy Wubben licht dat toe. *"Het Visma Security Programma is, ten eerste, een pakket aan veiligheidstools en -middelen. Bedrijven in onze groep maken bijvoorbeeld gebruik van de door ons ontwikkelde, goed beveiligde inlogsystemen (mét twee-factor-authenticatie), van cybersecuritytrainingen voor hun medewerkers en van tests en scans voor hun programmeercode."*

Visma heeft daarnaast een eigen Cyber Threat Intelligence team (CTI), dat non-stop onderzoek doet naar geopolitieke ontwikkelingen (die vaak verband houden met digitale aanvallen) en naar ontwikkelingen op het gebied van cybercrime en -veiligheid. Welke groepen zijn actief, hoe vallen ze aan? Ook scant dit team het dark web op gestolen inloggegevens en data die gelinkt zijn aan producten van Visma-bedrijven. Op basis van die kennis, worden tools en technieken ontwikkeld om de klanten van Visma-bedrijven nog beter te beschermen.

Wat je zelf *kan doen*

Een organisatie kan haar technische beveiliging perfect op orde hebben, de mens is de zwakste schakel. Iedereen kan weleens onzorgvuldig zijn of niet alert. Bovendien worden cyberaanvallen steeds geavanceerder. We helpen je graag de belangrijkste dreigingen te herkennen. Zodat je jouw deel doet om gevoelige informatie veilig te houden.

Phishing, spoofing, social engineering: hoe medewerkers kwetsbaar zijn

Er zijn veel verschillende, succesvolle, methodes die criminelen gebruiken om data te stelen of andere cybersecurityaanvallen te plegen. Medewerkers van bedrijven zijn vaak doelwit. Doorgaans gaat het dan om ‘social engineering’:door middel van psychologische manipulatie (een geloofwaardig, urgent klinkend verhaal) mensen verleiden persoonlijke of bedrijfsgevoelige gegevens prijs te geven. CEO-fraude is hier een goed voorbeeld van, zie de volgende pagina.

Phishing
Via nep-emails, -sms'jes of -Whatsappberichten, waarin wordt verwezen naar een nepwebsite, wordt de ontvanger (inlog)gegevens ontfutseld. Meestal gaat zo'n bericht naar duizenden tegelijk. Soms is een specifieke medewerker doelwit, zoals de CEO. Dan spreken we van Spear Phishing.

Spoofing
Het e-mailadres of de naam van de zender is gefalsificeerd, de zender doet zich voor als een bekende, als een vertrouwde collega (vaak gebruikt in combinatie met een phishing-techniek).

Malware
Ongemerkt geïnstalleerde software op jouw laptop of telefoon die data onderschept of op een andere manier schade berokkent. Die software kan geïnstalleerd zijn via een besmette e-mail, website of USB-stick.

Juice jacking
Vaak ingezet op vliegvelden, cafés of andere openbare gelegenheden: criminelen manipuleren een usb-oplaadpunt zodat wanneer je jouw laptop of telefoon daar op aansluit, niet alleen een stroomverbinding tot stand komt maar ook een dataverbinding. Op die manier wordt jouw data onderschept.

Cindy Wubben, Visma's Chief Information Security Officer, houdt alle cybersecuritytrends in de gaten: *"We zien voornamelijk die manipulatieve trucjes veel voorbij komen. Ieder mens is te manipuleren. Maar de trucs zijn ook te herkennen. Zo wordt heel vaak bij het slachtoffer een gevoel van urgentie gecreëerd. Een betaling moet zogenaamd nú gedaan worden. Zo proberen kwaadwillenden jouw vermogen om helder na te denken te omzeilen."*

Visma's hoofd Security Awareness & Training Isabel Arkvik vult aan met wat je bij twijfel zelf kan doen: *"Verifieer. Altijd. Check het verhaal en controleer of je wel echt met de afzender te maken hebt. Bel de persoon van wie het bericht afkomstig zou zijn. Geen e-mail is zo urgent dat er geen tijd meer is voor een vlugge controle. Vraag op zijn minst de collega die dichtbij je zit om een second opinion."*

CEO-fraude
In de Verenigde Staten is 'Business Email Compromise', in het Nederlands: 'CEO-fraude', financieel gezien de op een na schadelijkste vorm van criminaliteit (FBI, 2023). Ook in Nederland komt het voor.

Bij CEO-fraude wordt een medewerker van de financiële afdeling per mail gevraagd, zogenaamd door de baas, om een betaling uit te voeren. Minder bekend, maar ook veel voorkomend: frauduleuze mailtjes die uit naam van HR naar medewerkers worden gestuurd, waarin de ontvanger herinnerd wordt vakantiedagen op te geven of -ironisch genoeg - een belangrijke cybersecuritytraining te volgen. Op nepwebsites worden vervolgens belangrijke (inlog)gegevens ontfutseld.

Trainingen en bewustwording creëren: het helpt!

Isabel Arkvik, Visma's hoofd Security Awareness & Training: *"Voor elk bedrijf is het belangrijk om onder alle medewerkers bewustwording te creëren over cybersecurity en om hen kennis bij te brengen. Dan zijn ze alert en herkennen ze de schadelijkste trucs, wat ze stukken weerbaarder maakt."*

Uit onderzoek van cybersecuritybedrijf KnowBe4 blijkt dat medewerkers trainen op digitale veiligheid - bijvoorbeeld door nep-phishingmails te sturen en de respons te monitoren (zie kader) - inderdaad tot grote verbeteringen leidt. Het percentage medewerkers dat in social engineering-trucs trapt, loopt in hun onderzoek na zulke trainingen terug van ruim een derde tot slechts vijf procent (KnowBe4,2024).

Visma's Chief Information Security Officer Cindy Wubben: *"Wij organiseren intern veel digitale-veiligheidstrainingen en voorzien alle bedrijven in onze groep van trainingsmateriaal. Phishingtraining is bijvoorbeeld erg waardevol. De Visma Groep stuurt regelmatig nep-phishingmails naar alle medewerkers. We meten wie er 'in de val trappen'. Dat wordt uiteraard niet bestraft, het is immers een training, maar je kan dit opvolgen met persoonsgerichte training en met trainingen voor het hele bedrijf. Wat maakte dat er op een link geklikt is? Is het gemeld, toen het 'slachtoffer' merkte dat het hier een phishingaanval betrof? Vooral dat melden is belangrijk. Dat voorkomt (verdere) schade."*

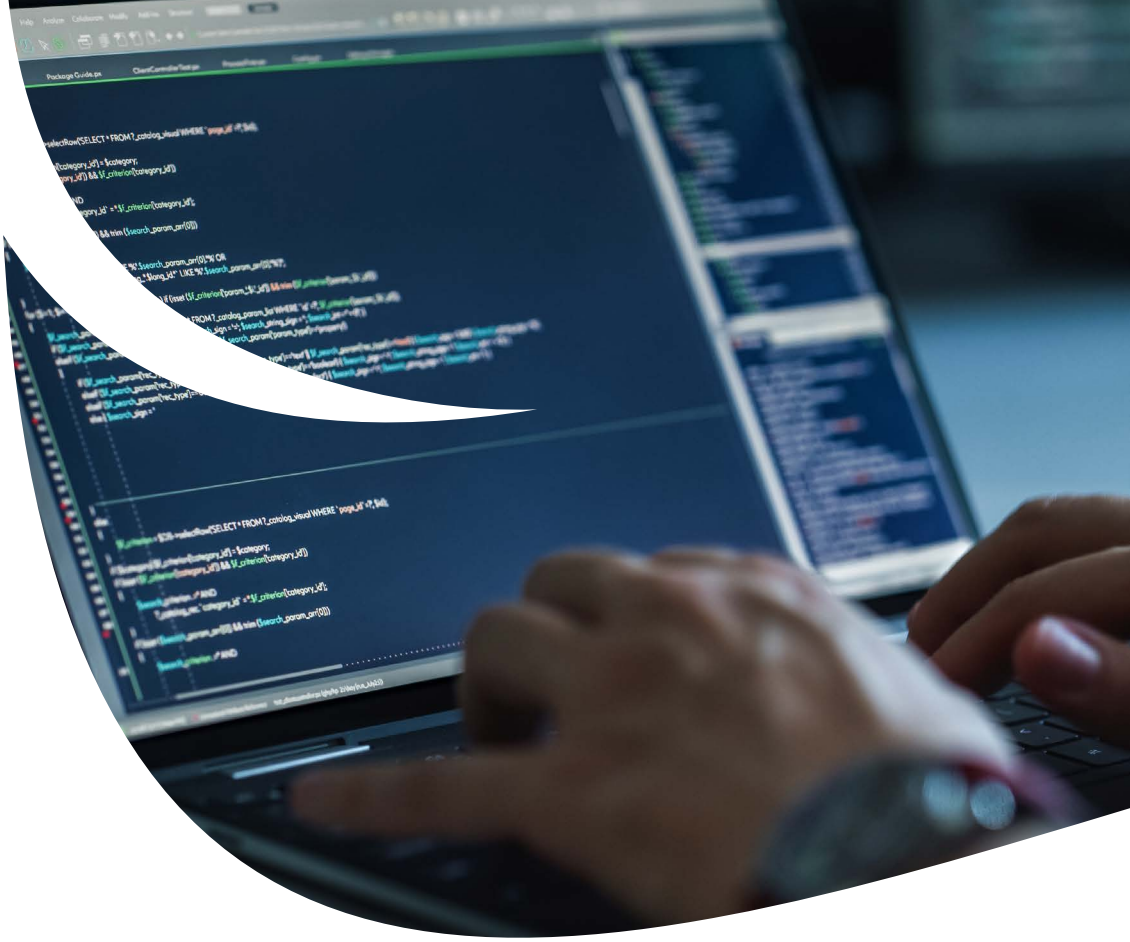
Sterke en unieke wachtwoorden en 2FA

Onze beste tip, omdat -ie zo gemakkelijk op te volgen is en toch veel bescherming biedt: zet twee-factor-authenticatie aan (2FA, of: multifactorauthenticatie, MFA). Dat betekent dat je het inloggen bevestigt op een tweede manier, zoals op je telefoon of in je e-mail of met een vingerafdruk- of gezichtscan. Zelfs met iemands inloggegevens kunnen kwaadwillenden dan de salarisadministratie nog niet in.

Belangrijk, ook: stel sterke (lange, met vreemde tekens) en unieke wachtwoorden in voor elk online account dat je hebt, dus ook voor Cash. Een wachtwoordmanager kan die wachtwoorden voor je genereren en onthouden.

Waarom is dat ook alweer zo belangrijk?

1. Korte wachtwoorden zijn te raden en te kraken.
2. Wachtwoorden kunnen op straat komen te liggen. Als je voor alles hetzelfde wachtwoord gebruikt (of allemaal varianten op één wachtwoord) heeft een kwaadwillende toegang tot al je data en bestanden, waaronder je salarisadministratie.



Tot *Slot*

Dat was een hoop informatie. Maar, zo zegt Visma's Chief Information Security Officer Cindy Wubben, wel belangrijk:

"Als informatie uit je salarisadministratie op straat komt te liggen heeft dat verstrekkende gevolgen. Naast persoonlijk leed, kan het tot gigantische financiële schade leiden voor jouw organisatie: je bedrijf staat stil, het kost veel geld om het op te lossen, er is reputatieschade, geschaad vertrouwen… We zien bedrijven soms zelfs omvallen als gevolg van een cybersecurityaanval. Digitale veiligheid kan abstract voelen. Maar nu je de potentiële gevolgen van een aanval kent, zie je vast het belang ervan. Hopelijk voel je ook de verantwoordelijkheid die we samen hebben om jouw data of die van jouw klanten veilig te houden."

Zo doen wij ons deel. Je kunt er van op vertrouwen dat we bij Cash er alles aan doen om jouw data veilig te houden.

Breng *cashflow* in je business

Ben je nieuwsgierig naar ons aanbod voor salaris- en HR-software in één? Onze adviseurs staan graag voor je klaar, per e-mail via verkoop@cash.nl of telefonisch via 070-3560570.

Alexanderstraat 3
2514 JL Den Haag

070 - 3 560 570
info@cash.nl