MEER VEILIGHEID, MINDER FRICTIE

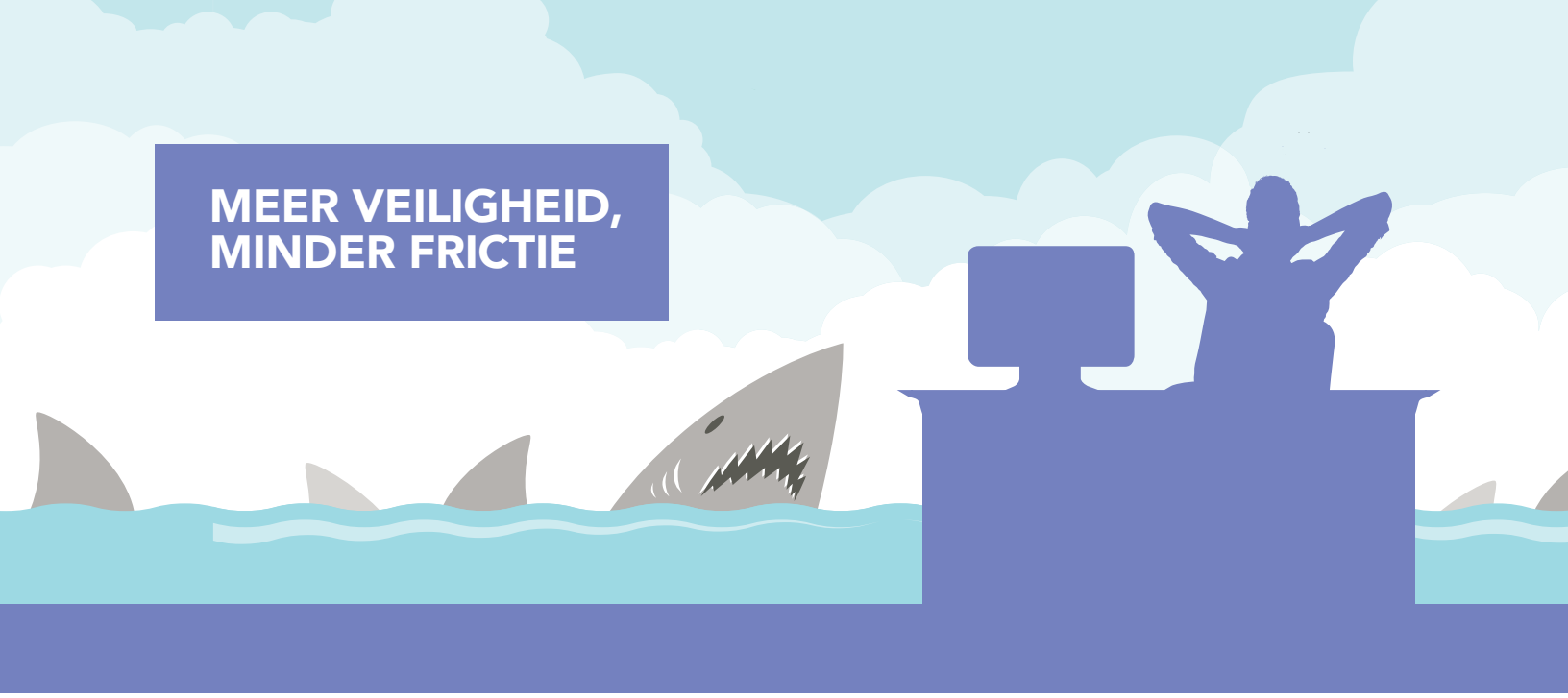
Beveilig

De Digitale Werknemer

Vijf belangrijke feiten over digitale werkplekken in een onveilige wereld

RES software

MEER VEILIGHEID, MINDER FRICTIE



Beveilig

De Digitale Werknemer

Vijf belangrijke feiten over digitale werkplekken in een onveilige wereld

RES software

THE OBJECTIVE:
MEER VEILIGHEID, MINDER FRICTIE

Steeds meer mensen werken digitaal. Voor het succes van uw bedrijf is het daarom van essentieel belang dat medewerkers altijd en overal beschikking hebben tot een goed functionerende digitale werkplek.

Helaas hebben bedrijven ook vaker te kampen met bedreigingen van de IT-veiligheid. Zeker nu steeds meer mensen steeds meer apparaten op steeds meer locaties gebruiken. Ook het verplaatsen van de IT-infrastructuur naar de cloud zorgt voor nieuwe bedreigingen. Een afschrikwekkende gedachte is wat de gevolgen kunnen zijn van een dergelijke beveiligingsfout. Denk daarbij aan het verlies van klanten, de aangetaste merkwaarde en de juridische gevolgen.

Bedrijven tasten flink in de buidel om al die bedreigingen het hoofd te bieden. Ze investeren in firewalls, antispyware- software, biometrische authenticatie en inbraakdetectiesystemen. Desondanks zijn er meer problemen rond beveiliging en compliance dan ooit.

Er zijn drie belangrijke vragen die managers en ondernemers zichzelf moeten stellen met betrekking tot beveiliging:

1. Welke extra beveiligingsmaatregelen passen het beste bij de maatregelen die mijn bedrijf al heeft genomen?

2. Welke maatregelen maken onze digitale werkplekken veiliger?

3. Hoe kan mijn bedrijf de IT-beveiliging verbeteren zonder dat dit ten koste gaat van de productiviteit van de medewerkers en de bedrijfsprestaties?

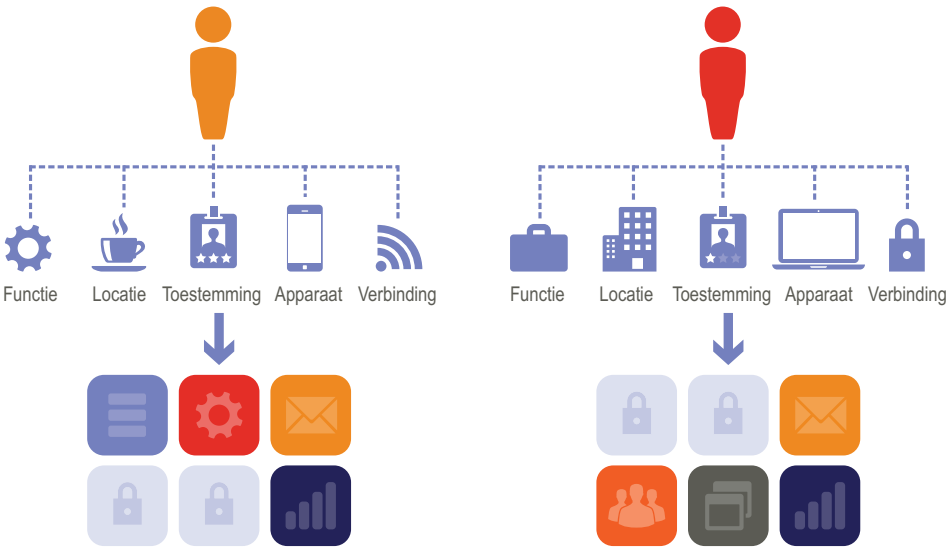
De volgende vijf feiten zijn de antwoorden op deze belangrijke vragen.

FEIT #1:
BEVEILIGING DRAAIT NIET OM DINGEN, MAAR OM MENSEN.

Zoals blijkt uit de affaire Snowden is zelfs de meest geavanceerde IT-beveiliging niet waterdicht als er geen rekening wordt gehouden met de menselijke factor. Gegevens en applicaties worden door verschillende mensen gebruikt, dus het is erg belangrijk dat de toegang tot IT-middelen efficiënt wordt geregeld op basis van bedrijfsregels en beleid.

Hiervoor is meer nodig dan alleen technologieën als Identity & Access Management (IAM) en Mobile Device Management (MDM). Natuurlijk zijn ze van belang voor de verificatie van gebruikers en apparaten op infrastructureel niveau. Maar ze kunnen er niet voor zorgen dat de regels en het beleid voor de realtime toegang van gebruikers tot apparaten worden nagekomen.

Met andere woorden: uw bedrijf heeft niet genoeg aan alleen technische mechanismen ter voorkoming van onbevoegde toegang tot bepaalde IT-middelen en data. U heeft ook een geïntegreerde beheerlaag nodig die uw IAM, MDM en andere beveiligingsmechanismen laat weten welke persoon wanneer en waar toegang mag hebben tot een digitale werkplek.



Bij de toegang tot business en IT-services moet de mens centraal staan. De werkplek zou dynamisch moeten aansluiten op de individuele context van de persoon.

FEIT #2:
BEVEILIGING MAG NIET TEN KOSTE GAAN VAN FACILITEITEN VOOR GEBRUIKERS.

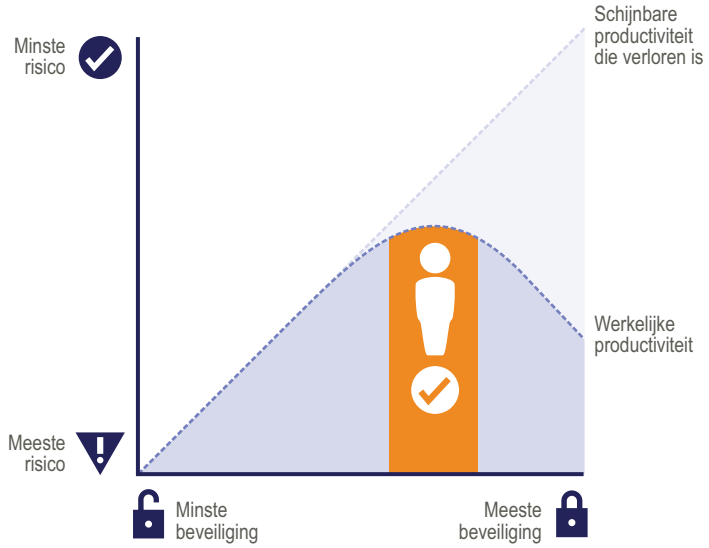
Sommige bedrijven nemen het zekere voor het onzekere en kiezen voor een rigoureuze beperking van de toegang tot IT-middelen. Dit is een onveilige aanpak, om verschillende redenen:

- **Te weinig faciliteiten voor gebruikers leidt tot minder rendement.** Wanneer gebruikers geen toegang hebben tot de middelen die ze nodig hebben, lijden de bedrijfsprestaties daaronder. Het afschermen van middelen die gebruikers willen en moeten gebruiken, heeft dus negatieve gevolgen voor de business.

- **Gefrustreerde gebruikers proberen de beperkingen te omzeilen.** De moderne medewerker is goed op de hoogte van IT. Als u hen niet op een gebruikersvriendelijkeen beheersbare manier de beschikking geeft over wat ze nodig hebben, vinden ze wel een illegale en/of onbeheersbare route (zoals bv. Dropbox). Een dergelijke "schaduw-IT" brengt nog veel meer risico's voor beveiliging en compliance met zich mee.

- **U trekt geen nieuw talent aan.** Voor personeel van de nieuwe generatie (ook wel millenials of generatie Y genoemd) is technologie als zuurstof. Als hun werkplek te verstikkend is, gaan ze met hun vaardigheden en netwerk naar een concurrent.

Onder meer om deze redenen moet u zich bij het verlenen van toegang tot uw IT concentreren op wat wel mag en voorkomen wat niet mag.



Veiligheid en gebruiksvriendelijkheid moeten hand in hand gaan. Hoewel een betere beveiliging vaak leidt tot minder risico's, zorgt een te strikte beveiliging ervoor dat medewerkers minder productief worden en dat er meer gebruik wordt gemaakt van schaduw-IT.

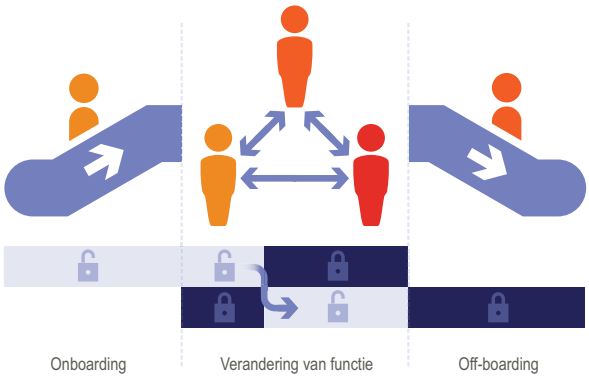
FEIT #3:
IN EEN STEEDS DYNAMISCHER WORDENDE BEDRIJFSOMGEVING IS ANTICIPEREN BETER DAN REAGEREN.

De tijd dat mensen hun hele carrière voor dezelfde baas werkten, ligt lang achter ons. In de flexibele ondernemingen van vandaag is het een komen en gaan van personeel. Ook intern veranderen medewerkers vaak van functie. Niet alleen omdat ze zich ontwikkelen, maar ook omdat werkgevers hun talenten beter willen afstemmen op de wisselende vraag van een veranderlijke en concurrerende markt.

In deze dynamische bedrijfswereld kan geen onderneming het zich veroorloven medewerkers niet tijdig en uitsluitend de juiste IT-diensten te bieden. Het te laat of onvolledig verschaffen van de juiste digitale werkplek heeft negatieve gevolgen in elke fase van de 'levenscyclus' van medewerkers:

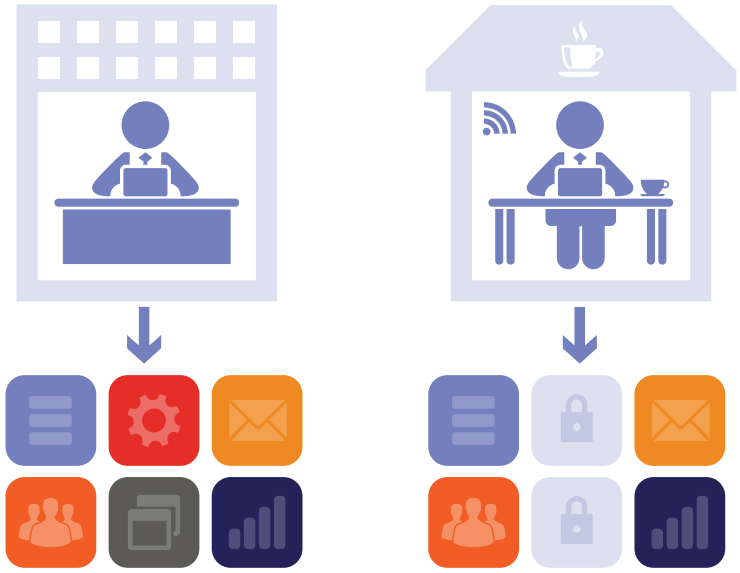
- **Trage onboarding** leidt ertoe dat nieuwe medewerkers en contractanten niet direct aan de slag kunnen. Dit heeft tot gevolg dat de productiviteit van de medewerker er dagen of zelfs weken onder lijdt, zakelijke kansen worden gemist, de integratie in de rest van het team niet optimaal verloopt en het aanvankelijke enthousiasme van de nieuwe medewerker wordt getemperd. Bovendien ontstaat zo een cultuur waarin medewerkers op eigen houtje naar oplossingen gaan zoeken.
- **Trage reacties op promoties, overplaatsingen en andere veranderingen met betrekking tot de functies en verantwoordelijkheden van medewerkers** heeft vergelijkbare consequenties. Bovendien kan dit leiden tot problemen op het gebied van beveiliging en compliance. Als medewerkers een ander takenpakket krijgen, is het immers niet de bedoeling dat ze nog steeds toegang hebben tot applicaties en gegevens uit hun vorige functies.
- **Trage offboarding** is nog wel het ergste. Dit is vooral gevaarlijk als medewerkers teleurgesteld vertrekken. Als imensen na hun vertrek nog steeds toegang hebben tot bedrijfsfaciliteiten, kan dit leiden tot ernstige beveiligings- en compliance-problemen.

Het is belangrijk om er gedurende hun gehele 'levenscyclus' voor te zorgen dat medewerkers zo snel mogelijk productief zijn.



Voor een tijdige en zorgvuldige provisioning en de-provisioning van IT-diensten is er meer nodig dan alleen het versnellen van handmatige processen. Ook dient u de digitale werkplekken van uw medewerkers op een proactieve manier te beheren. Hiervoor moet de provisioning/de-provisioning van diensten op een deugdelijke manier worden geautomatiseerd. Ook vereist dit flexibele bedrijfs- en beleidsregels en een nauwe integratie met HR, Active Directory en andere relevante administratieve systemen.

FEIT #4: IN EEN WERELD VOL MOBIELE APPARATEN EN CONSUMERIZATION IS REALTIME CONTEXTBEWUSTZIJN VAN GROOT BELANG.



Een contextbewuste digitale werkplek voorkomt dat onbevoegden toegang krijgen tot IT-middelen en data waardoor beveiligings- en compliance-problemen ontstaan.

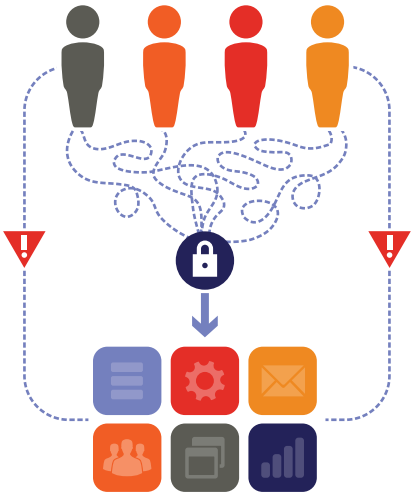
Toen medewerkers alleen aan hun bureau toegang hadden tot IT-diensten, hoefde de beveiliging alleen te voorkomen dat ze de verkeerde diensten gebruikten. Maar met de komst van mobiele apparaten en consumerization of IT moet u er ook voor zorgen dat ze de IT_middelen en data niet in de verkeerde omstandigheden gebruiken. Denk daarbij aan gebruik buiten geautoriseerde locaties, via een onveilig draadloos netwerk of op een apparaat met root access. Natuurlijk is het belangrijk dat medewerkers altijd en overal de beschikking hebben over een digitale werkplek die optimaal aansluit bij hun behoeften. Het is echter ook noodzakelijk dat deze werkplek in realtime kan worden aangepast aan de context van de medewerker.

Net als bij onboarding en offboarding vereist contextbewuste toegang goed geautomatiseerde processen en goed beheerde beleidsregels. Voor een veilig gebruik van mobiele apparaten en consumerization moet echter ook rekening worden gehouden met realtime veranderingen in de context, zoals de netwerkbeveiliging en de locatie. Hiervoor moet er gebruik kunnen worden gemaakt van beveiligingsmechanismen als geofencing (gebiedsdefiniëring).

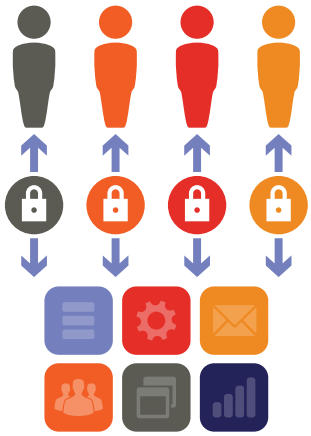
Ter bescherming van uw bedrijfsgegevens is het ook zaak dat u beleid opstelt en implementeert ten aanzien van verwijderbare media als USB-apparaten. Zo kunt u gebruikers de toegang ontzeggen, alleen-lezen-toegang geven of volledige toegang verlenen op basis van contextfactoren (zoals het serienummer van het USB-apparaat).

Bedrijven moeten echter waken voor een buitensporige beveiliging van de digitale werkplek. De best presterende mensen bepalen het succes van uw bedrijf en juist zij werken veel buiten kantoor en buiten kantooruren. Als u onnodig beperkt waar en wanneer ze mogen werken, heeft dat negatieve gevolgen voor de business. Daarom is het belangrijk dat u het toegangsbeleid voortdurend aanpast en de juiste balans zoekt tussen een deugdelijke beveiliging en een optimale productiviteit buiten kantoor en buiten kantooruren.

FEIT #5: ZORG VOOR EMPOWERMENT VAN MEDEWERKERS EN BUSINESSUNITS.



Boven: Medewerkers verliezen kostbare tijd als ze door trage handmatige processen en overbelaste IT-teams moeten wachten op IT-diensten.



Onder: Maak het minder complex en geef medewerkers hun eigen digitale werkplek met selfservice en automatisering. Dit verhoogt de productiviteit, vermindert de kosten en verlaagt de risico's.

Nu technologie steeds belangrijker wordt op de werkvloer, is het belangrijk dat medewerkers en businessunits zelf de verantwoordelijkheid voor technologie dragen.

Ze hebben immers geen tijd om te wachten tot iemand hen de benodigde middelen verschaft. Bovendien willen managers van businessunits zelf bepalen op welke manier ze hun teams van technologie voorzien.

Professionele informatiebeveiligers hebben van oudsher hun bedenkingen tegen deze empowerment, omdat het overdragen van verantwoordelijkheden aan 'leken' risico's in de hand zou werken. Maar in deze tijd van vooruitstrevende consumententechnologie en de grote rol die technologie speelt in de werkomgeving is empowerment juist veel veiliger. En wel om de volgende redenen:

Selfservice voorkomt schaduw-IT. Als gebruikers zelf kunnen kiezen wat ze nodig hebben van een goedgekeurde lijst met IT-middelen, zullen ze niet meer zo snel naar niet- ondersteunde IT-middelen grijpen. Op die manier kan content beter worden beheerd en is er minder kans op zeer kwetsbare 'blind spots'.

Door IT-taken te delegeren aan de desbetreffende business unit zijn er meer IT-professionals beschikbaar om proactief te beveiligen. Vaak zijn IT-budgetten te krap om alle bedreigingen het hoofd te bieden. Daarom moeten er prioriteiten worden gesteld. Door routinematige administratieve taken over te hevelen naar de businessunits, kunnen IT-professionals zich meer concentreren op een proactieve bescherming van de IT-omgeving.

Op regels gebaseerde automatisering is betrouwbaarder dan handmatige processen. Om ervoor te zorgen dat zakelijke gebruikers op een veilige manier werken, moet IT de regels voor autorisatie en provisioning vastleggen en automatiseren. Het vastleggen in regels dwingt IT ertoe het beheer van digitale werkplekken systematisch te benaderen. Dit maakt het betrouwbaarder en consistenter dan wanneer het te veel afhankelijk is van ad-hocacties van menselijke technici.

Voor een optimale veiligheid en compliance is dus behalve een goed beleid ook empowerment van gebruikers en businessunits aan te raden. Dit verhoogt de productiviteit en vermindert de risico's.

SAMENGEVAT

Natuurlijk moeten bedrijven zich wapenen tegen de toenemende bedreiging van hun financiële positie, intellectuele eigendommen en relaties met klanten door risico's rond gegevensbeveiliging. Toch moeten ze zich ook realiseren dat te strikte beveiligingsmaatregelen leiden tot fricties in het bedrijfsproces die zakelijk succes in de weg staan.

Tegenwoordig speelt technologie een steeds belangrijkere rol binnen organisaties. Daarom is de balans tussen een betere beveiliging en organisatorische flexibiliteit van het grootste belang.

Beide doelstellingen kunnen worden bereikt met een anticiperend, contextbewust beleid dat de beschikbaarheid van IT-diensten garandeert en selfservice voor gebruikers mogelijk maakt. Natuurlijk blijft traditionele beveiligingstechnologie een belangrijke rol spelen in de bescherming van ondernemingen. Maar voor IT-diensten die voor mensen zijn gemaakt is het essentieel te zorgen voor een productieve digitale werkplek en het beleid dat daarbij hoort. Als het goed wordt geïmplementeerd, is dit een krachtig middel om de concurrentiepositie te verbeteren.