GOVCERT.NL

TELEWERKEN

Veilig werken op afstand

WWW.GOVCERT.NL

POSTADRES
Postbus 84011
2508 AA Den Haag
BEZOEKADRES
Wilhelmina van Pruisenweg 104
2595 AN DEN HAAG
TELEFOON
070 888 75 55
FAX
070 888 75 50
E-MAIL
info@govcert.nl

Auteur(s) : GOVCERT.NL
Versie : 1.1
30.06.2006
Den Haag : Publieke uitgave: 04.02.2009

GOVCERT.NL
is het Computer Emergency Response
Team van en voor de Nederlandse overheid.
Zij ondersteunt overheidsorganisaties in het
Voorkomen en afhandelen van ICT-gerelateerde
veiligheidsincidenten, 24 uur per dag, 7 dagen
per week. Advies en preventie, waarschuwing,
incidentafhandeling en kennisdeling
zijn hierbij sleutelwoorden.

GBO.OVERHEID
is de Gemeenschappelijke Beheer Organisatie
waar GOVCERT.NL sinds 1 januari 2006 deel
van uit maakt. Zij is verantwoordelijk voor
beheer en verdere ontwikkeling van een aantal
overheidsbrede ICT-voorzieningen.

GOV  CERT.NL

MANAGEMENTSAMENVATTING

Binnen de overheid worden medewerkers steeds mobieler. Ze werken vaker in wisselende teams of op locaties buiten de organisatie. Ook worden hogere eisen gesteld aan de bereikbaarheid van de medewerker buiten kantoortijden. Telewerken is voor veel medewerkers een oplossing om flexibel te kunnen werken.
Telewerken brengt echter ook nieuwe risico's met zich mee en kan niet los gezien worden van informatiebeveiliging. Iedereen kent de berichten in de media over beveiligingsincidenten waarbij als gevolg van telewerken gevoelige informatie uitgelekt is.

Invoeren van telewerken begint dan ook met de vraag:
Waarom wil men telewerken invoeren en welke medewerkers komen hiervoor in aanmerking?

Met de beantwoording van deze vraag komt men automatisch tot de volgende vragen, die ook moeten worden beantwoord:

- Over welke informatie moet de medewerker op zijn telewerkplek kunnen beschikken?
- Welke risico's loopt de bedrijfsvoering van de organisatie door telwerken?

De risico's van telewerken kan men indelen naar de schakels van de telewerkketen tussen medewerker en organisatie, namelijk:

1. De telewerklocatie;
2. Het werkstation;
3. De verbinding tussen werkstation en organisatie;
4. De informatie die aan de telewerker beschikbaar wordt gesteld;
5. De telewerker zelf.

De eigenaar van de informatie heeft met een risicoanalyse een goed instrument in huis om de kosten van de voorgestelde beveiligingsmaatregelen in verhouding te laten zijn met de mogelijke schade voor de bedrijfsvoering van de organisatie.

In deze white paper worden een aantal organisatorische en technische maatregelen aangegeven, afhankelijk van de schakel in de keten van telewerken.

Daarnaast wordt aandacht geschonken aan het creëren van beveiligingsbewustzijn van de telewerker. Door de telewerker in een vroegtijdig stadium te betrekken in het project en hem/haar bewust te maken van de risico's die telewerken met zich meebrengt, krijgt de telewerker inzicht in de achtergrond van de beveiligingsmaatregelen. Dit mes snijdt dan aan twee kanten. Enerzijds zal de telewerker de beperkingen, die deze maatregelen met zich meebrengen eerder accepteren. Anderzijds zal hij bewuster omgaan met informatiebeveiliging bij het telewerken.

Abstract

Voor veel organisaties is telewerken een onlosmakelijk onderdeel geworden van de bedrijfsvoering. Door de 7*24 uurs economie dienen medewerkers te beschikken over een mobiele werkplek die hen in staat stelt om op de plaats en tijd die hen het best uitkomt te kunnen werken. Hierdoor kan de medewerker niet alleen de files vermijden, maar ook buiten het kantoor over de meest actuele informatie van bijvoorbeeld een samenwerkingsproject beschikken. Een speciale vorm van telewerken is thuiswerken, waarbij een werkplek thuis is ingericht. Telewerken geschiedt in het algemeen op een door de werkgever verstrekte laptop. Thuiswerken wordt soms met de privé-PC gedaan. In de media zijn al verscheidene beveiligingsincidenten gemeld, waarbij als gevolg van telewerken gevoelige informatie uitgelekt is. Beveiliging van een telewerkplek (en thuiswerkplek) is dan ook van groot belang.

Deze white paper gaat in op de principes van veilig telewerken. Het levert op basis van best practices een handreiking aan de proceseigenaar, de IT-manager en de Informatie Beveiligingsfunctionaris (IB'er) hoe telewerken op een veilige manier binnen een organisatie ingevoerd en geborgd kan worden. De paper start met een beschrijving van trends in telewerken en de belangrijkste risico's. Vervolgens wordt een stappenplan voor invoer van telewerken aangegeven. Tot slot worden mogelijke organisatorische en technische beveiligingsmaatregelen beschreven voor verschillende vormen van telewerken.

Leeswijzer

Deze white paper is in 2006 geschreven en gepubliceerd voor de GOVCERT.NL deelnemers. Nu, in februari 2009, wordt het white paper volledig publiek gemaakt. Voor deze publieke uitgave is het document licht herzien: waar nodig is achterhaalde informatie verwijderd en zijn kleine verbeteringen doorgevoerd.

GOV  CERT.NL

1 TELEWERKEN

1.1 Trends

Voor veel organisaties is telewerken onlosmakelijk verbonden met de bedrijfsvoering. Medewerkers zijn mobieler geworden en werken regelmatig op andere locaties. Telewerken is de oplossing om de medewerkers een flexibele werkplek aan te bieden. Zo is het mogelijk bij een partner of klant over de meest actuele informatie te beschikken of files te vermijden. Daarnaast biedt telewerken de medewerker de mogelijkheid om thuis te werken en daarmee zijn werktijden flexibel in te delen of de steeds grotere files te vermijden. Ook de beschikbaarheid van een webserver wordt steeds belangrijker, wat eisen stelt aan de beheerorganisatie. Telewerken stelt beheerders in staat om 7*24 uurs beheer vanuit thuis hiervan uit te voeren en zo de gewenste beschikbaarheid van de diensten te kunnen realiseren.

1.2 Telewerklocatie

De meest voor de hand liggende locatie voor telewerken is thuis. De werkplek thuis kan variëren van een speciaal ingerichte werkomgeving met een door de werkgever beheerd werkstation inclusief internetaansluiting tot een privé-PC met eigen internetaansluiting, waarmee men bijvoorbeeld via webmail thuis zijn e-mail kan afhandelen. Maar telewerken kan ook vanaf een werkplek bij een partner of klant waar de medewerker via een daar aanwezig werkstation verbinding maakt met zijn eigen kantooromgeving. Nu er steeds meer draadloze hotspots worden aangelegd in openbare ruimten, zoals stations, luchthavens of internetcafés, kan telewerken ook vanuit zo'n openbare ruimte, waar de medewerker met de mobiele telefoon of laptop een draadloze verbinding kan maken met de kantooromgeving.

1.3 Telewerkvoorzieningen

Een organisatie kan op verschillende manieren telewerken faciliteren. De meest voorkomende, en beperkte, vorm is het beschikbaar stellen van een mobiele telefoon, waarmee de medewerker overal bereikbaar is.
De werkgever kan ook e-mail via een webinterface beschikbaar stellen zodat de medewerker vanaf in principe ieder werkstation, bijvoorbeeld zijn privé-PC, zijn e-mail kan afhandelen.

Aan de andere zijde van het voorzieningenpalet stelt de werkgever een laptop beschikbaar met een VPN-client om een beveiligde verbinding te kunnen maken met het kantoornetwerk. Tussen deze uitersten zijn nog veel andere varianten mogelijk, afhankelijk van de behoefte aan telewerken, de gewenste beschikbare functionaliteit voor de medewerkers en het beveiligingsbeleid van de organisatie.

1.4 Mogelijke risico's van thuiswerken

Men kan zich voorstellen dat er, afhankelijk van de telewerklocatie en de beschikbare telewerkvoorziening, verschillende risico's bestaan. Als we kijken naar de risico's van telewerken, dan kunnen we die indelen per schakel van de 'telewerkketen' van medewerker naar organisatie, namelijk:

1. De telewerklocatie;
2. Het werkstation;
3. De verbinding tussen werkstation en organisatie;
4. De wijze van toegang tot informatie die men vanaf de telewerkplek kan benaderen;
5. De mens als telewerker.

1.4.1 De telewerklocatie

Indien een medewerker op een openbare locatie telewerkt, bestaat de kans dat een buitenstaander gevoelige informatie vanaf het beeldscherm leest of een telefoongesprek afluistert. Daarnaast kan de laptop, PDA of mobiele telefoon van de telewerker gestolen worden en de daarop opgeslagen informatie in handen komen van een buitenstaander.

Gebruikt een telewerker een internetcafé, dan kan in bepaalde gevallen de volgende gebruiker van deze computer de in cache opgeslagen informatie van de vorige sessie inzien.

In een enkel geval kan men verleid worden om op een valse hotspot in te loggen, waardoor het mogelijk is dat men naar een verkeerde server wordt geleid.

1.4.2 Het werkstation

Indien de telewerker een laptop of werkstation van de organisatie ter beschikking heeft, kan de organisatie zelf bepalen welke beveiligingsmaatregelen zij hierop aanbrengt. Daarmee kan een organisatie de risico's voor de laptop of het werkstation grotendeels afdekken (een speciale versie van een door de organisatie beheerd werkstation is een thin client). Hetzelfde geldt in principe voor een PDA of smartphone die door de organisatie ter beschikking wordt gesteld.
Voor de privé-PC of PC in (bijvoorbeeld) een internetcafé is dat anders. Deze PC is niet in beheer bij de organisatie en daardoor kunnen de risico's aanmerkelijk groter zijn dan bij een door de organisatie beheerd systeem.
Vooral de computer in een internetcafé loopt grote risico's. Deze kan voorzien zijn van malware zoals keyloggers waardoor kwaadwillende gebruikers wachtwoorden en gevoelige informatie kunnen achterhalen.
Meestal heeft de telewerker op zijn thuis-PC alle rechten en kan hierop willekeurige software installeren. Dit kan tot gevolg hebben dat er bijvoorbeeld peer2peer software is geïnstalleerd, waarbij alle informatie opgeslagen op de thuis-PC (en daarmee de informatie van de organisatie) gedeeld wordt met andere peer2peer gebruikers. Ook kunnen kwaadwillende buitenstaanders via malware (zoals virussen, trojan horses en spyware) informatie op de thuis-PC inzien of het netwerk

van de organisatie inloggen als de telewerker geen of niet up-to-date anti malware software gebruikt.

Ook kunnen huisgenoten de op de thuis-PC opgeslagen informatie inzien, indien deze PC niet voorzien is van een aparte toegangscontrole per gebruiker.
Als laatste kan de opgeslagen informatie bij derden terecht komen indien de telewerker zijn thuis-PC afdankt en deze zonder de data te wissen bij het huisvuil zet of verkoopt. Op deze manier is gevoelige informatie van organisaties zelfs in de media terechtgekomen, waardoor organisaties imagoschade leden.

1.4.3 De verbinding tussen werkstation en organisatie

De verbinding tussen het werkstation en de organisatie kan op vele manieren tot stand worden gebracht. Via een wireless verbinding, een inbelverbinding of een ADSL-verbinding over internet.

Deze verbindingen kunnen door kwaadwillenden worden afgeluisterd, waardoor deze inzage kunnen krijgen in de informatie die tussen de telewerker en de organisatie wordt uitgewisseld. Gebruikersnaam en wachtwoord kunnen zo worden bemachtigd, waardoor een kwaadwillende zich toegang kan verschaffen tot de bedrijfsinformatie van de organisatie. Zie ook referentie [3].

Ook als een beveiligde verbinding tussen het telewerkstation en de organisatie uitvalt, is het telewerkstation vanuit internet te bereiken en bestaat de mogelijkheid dat een kwaadwillende toegang krijgt tot de daarin opgeslagen informatie.

1.4.4 Toegang tot informatie

In veel gevallen heeft een organisatie een webserver in gebruik waarmee aan iedereen algemene informatie over de organisatie en zijn producten of diensten wordt gegeven. Indien deze website niet goed beveiligd is, kan een kwaadwillende inbreken op deze site. Als een buitenstaander eenmaal binnen is kan deze de informatie op de website wijzigen (defacement, waardoor de organisatie imagoschade lijdt) of de bedrijfsinformatie achter de website benaderen.

Een organisatie kan via een webserver e-mail beschikbaar stellen aan de telewerker. De telewerker kan dan via de browser zijn e-mail behandelen.
Soms worden zelfs interne applicaties met bedrijfsinformatie via het internet beschikbaar gesteld aan de telewerker. Indien men alleen gebruikersnaam en wachtwoord toepast om deze toegang te beveiliging, loopt men het risico dat dit wachtwoord wordt gekraakt. Op internet zijn legio password recovery tools beschikbaar, die hiervoor kunnen worden ingezet. Hiermee krijgt een hacker 'gemakkelijk' toegang tot de voor de telewerker beschikbare interne bedrijfsinformatie van de organisatie.

1.4.5 De mens als telewerker

De mens is vaak de zwakste schakel in de telewerkketen. Zeker wanneer deze zich niet bewust is van de mogelijke risico's die verbonden zijn aan telewerken:

- Het werkstation wordt onbeheerd achtergelaten in een ruimte waar derden toegang tot hebben, wat derden meer mogelijkheden geeft om in te kunnen breken;
- Men heeft (vaak) niet in de gaten heeft dat men het slachtoffer is van 'social engineering'. Een hacker probeert dan persoonlijke gegevens te achterhalen, waaronder wachtwoorden, met alle gevolgen van dien;
- Privé-PC's thuis worden niet goed beheerd en kunnen besmet raken met malware. Bijvoorbeeld na infectering met een 'trojan horse' kunnen derden remote toegang krijgen tot de informatie die op de privé-PC is opgeslagen of kan er meegelezen worden met webmail.

De introductie van telewerken kan echter ook risico's wegnemen:

- Voorkomen dat medewerkers (heel) gevoelige informatie doorsturen naar hun privé mailadres;
- Voorkomen dat medewerkers op een mobiele datadrager (bijv. een USB-stick) informatie plaatsen, waardoor deze informatie buiten de controle van de organisatie komt met alle mogelijke gevolgen van dien.

2 INVOEREN TELEWERKEN

In het vorige hoofdstuk zagen we dat telewerken voor veel organisaties niet meer weg te denken is, maar dat telewerken ook risico's met zich meebrengt. In dit hoofdstuk geven we in een aantal stappen aan hoe men telewerken op een veilige manier kan inrichten.

2.1 Beleid organisatie

De uitgangspunten voor telewerken zijn voor elke organisatie anders. Heeft een organisatie veel functies die buiten de deur zijn, zoals een sales functie, die behoefte hebben aan telewerken of is er slechts behoefte aan een incidentele telewerkplek voor een medewerker, die zijn e-mail thuis leest of een vergadering voorbereidt?

De eerste vraag die een organisatie zich moet stellen is dan ook:
Waarom wil men telewerken invoeren en welke medewerkers komen hiervoor in aanmerking?

2.2 Beveiligingsbeleid

De volgende vraag is dan ook: welke informatie moet op de telewerkplek beschikbaar zijn?

Men kan zich voorstellen dat voor een sales functie gegevens beschikbaar moeten zijn om zijn het werk te kunnen doen. Denk hierbij aan bijvoorbeeld informatie over de actuele voorraad, levertijden en prijzen. Heeft deze medewerker dan toegang op afstand nodig tot alle relevante bedrijfsinformatie die binnen de organisatie beschikbaar is, met een mogelijk risico dat deze gevoelige gegevens in handen van derden terecht kunnen komen?

In het informatiebeveiligingsbeleid kan een organisatie kaders aangeven voor beveiliging van interne informatie en daarmee richtlijnen aanreiken welke informatie via telewerken beschikbaar mag zijn voor de verschillende functies/rollen.

2.3 Risicoanalyse

Via telewerken wordt interne informatie aan medewerkers op afstand beschikbaar gesteld. In het vorige hoofdstuk is een reeks van hiermee gepaard gaande risico's genoemd. Door eerst de dreigingen te inventariseren en de bijbehorende maatregelen te bepalen, krijgt men inzicht in de restrisico's die de organisatie loopt bij telewerken. Dit betekent dus het uitvoeren van een Afhankelijkheid- & Kwetsbaarheidanalyse.

Volgens het VIR is de eigenaar van de informatie (meestal de lijnmanager) verantwoordelijk voor de beveiliging van deze informatie. De eigenaar is uiteindelijk verantwoordelijk voor het besluit om al of niet telewerken met de voorgestelde maatregelen toe te staan. Een honderd procent beveiligde telewerkomgeving bestaat niet, maar de eigenaar van de informatie heeft met een risicoanalyse een instrument om de kosten van de voorgestelde maatregelen in verhouding te laten zijn met de mogelijke schade voor de organisatie.
Hierbij moet men niet alleen denken aan technische, maar ook aan organisatorische maatregelen.

Vergeet in deze stap niet de telewerker te betrekken bij het invoeren van deze maatregelen. Door de telewerker in een vroeg stadium te betrekken in het project en hem bewust te maken van de risico's die telewerken met zich meebrengt, krijgt de telewerker inzicht in de achtergrond van de beveiligingsmaatregelen. Dit mes snijdt dan aan twee kanten. Enerzijds zal de telewerker de beperkingen die deze maatregelen met zich meebrengen eerder accepteren, anderzijds zal hij bewuster omgaan met informatiebeveiliging bij het telewerken. Dit heeft dan ook als voordeel dat de telewerker eerder aan de bel zal trekken indien men iets verdacht tegenkomt, waardoor de organisatie sneller actie kan ondernemen om de gevolgen van een incident te beperken.

In de volgende hoofdstukken worden voor elke schakel in de keten tussen de telwerker en de organisatie maatregelen beschreven, die men kan treffen om telewerken veilig te implementeren.

2.4 Implementatie en test telewerkvoorzieningen

Als de risico's van telewerken met de voorgestelde maatregelen acceptabel zijn, kan men starten met de volgende stap in het traject: het inrichten van de telewerkomgeving. In deze fase worden de voorzieningen geïnstalleerd en getest. Tevens worden in deze fase de technische en organisatorische beveiligingsmaatregelen getroffen en wordt het in beheer nemen van de telewerkvoorziening voorbereid.

2.5 Beheer telewerkomgeving

Invoer bij telewerken stopt niet bij de implementatie hiervan. Goed beheer van de telewerkomgeving is van essentieel belang om deze omgeving veilig te houden. Beheer omvat minimaal het updaten van virusdefinities en patches om bekende kwetsbaarheden te repareren.
De telewerkers en apparatuur met software vormen natuurlijk ook een onderdeel van beheer. Denk hierbij aan het intrekken van toegangsrechten en inleveren van apparatuur bij vertrek van een medewerker.
Als laatste dient de beheerorganisatie monitoring in te voeren om afwijkingen of incidenten te kunnen onderkennen en daarop actie te kunnen ondernemen.

3 ORGANISATORISCHE MAATREGELEN

Telewerken vindt altijd plaats vanaf een locatie buiten de organisatie. Deze omgeving valt voor een deel buiten de invloedssfeer van de organisatie, daarom zijn voor de beveiliging van een telewerkplek naast technische maatregelen ook organisatorische maatregelen nodig. Dit hoofdstuk gaat in op de organisatorische beveiligingsmaatregelen voor de telewerkomgeving.

3.1 Telewerklocatie

Een organisatie kan weinig invloed uitoefenen op de omgeving van een telewerklocatie. Een telewerklocatie is nu eenmaal per definitie een werkplek buiten de organisatie en daarmee buiten bereik van de directe beheerorganisatie.

Wel is het mogelijk om via een 'Gedragscode', waarin de voorwaarden voor telewerken staan, aan te geven op welke locaties de telewerker mag telewerken. Zo kan men bijvoorbeeld verbieden om vanuit een internetcafé of via een onbeveiligde draadloze verbinding te telewerken.

3.2 Werkstation

Het werkstation dat gebruikt wordt voor telewerken kan de privé-PC zijn van de telewerker of een door de organisatie beheerd werkstation (in veel gevallen een laptop). De organisatie kan op het beheerde werkstation veel zaken technisch afdwingen (zie hiervoor paragraaf 4.3), maar op de privé-PC in principe niet, omdat deze door de telewerker zelf wordt beheerd.

3.2.1 Privé-PC

Wanner er gebruik gemaakt wordt van privé-PC 's om telewerken te faciliteren, spreekt men ook wel van thuiswerken.

Ook hier kan men in de 'Gebruiksvoorwaarden voor telewerken' aangeven, dat de telewerker zijn privé-PC moet voorzien van een:

- Up to date virusscanner;
- Personall firewall;
- Anti-spyware tool;
- Gepatched Operating System en applicaties.

De organisatie doet er dan wel verstandig aan om de medewerkers te faciliteren zodat zij hun privé-PC kunnen beveiligen. Ook kan men de telewerker via 'Gebruiksvoorwaarden voor telewerken' verbieden om informatie lokaal op de privé-PC op te slaan, om zo de kans te beperken dat het via spywareprogramma's uitgelezen kan worden.

3.2.2 Werkstation of laptop beheerd door de werkgever.

Dit werkstation kan de organisatie zelf inrichten en voorzien van adequate technische beveiligingsmaatregelen.
Als organisatorische maatregel kan in de 'Gebruiksvoorwaarden voor telewerken' de zinsnede worden opgenomen dat de telewerker als een goed huisvader zorgt voor de aan hem beschikbaar gestelde apparatuur en zelf geen applicaties installeert, zonder toestemming van de beheerorganisatie.

3.3 Verbinding

De organisatie zorgt voor een beveiligde verbinding, zie hiervoor 4.3. De beveiliging hiervan wordt technisch afgedwongen.

3.4 Toegang tot informatie

Voor toegang van de telewerker tot de informatie op het bedrijfsnetwerk van de organisatie wordt aanbevolen strong authentication toe te passen. Strong authentication is gedefinieerd als iets wat men heeft (bijvoorbeeld een token) en iets wat men weet (bijvoorbeeld een PIN of een One time password).
In de 'Gebruiksvoorwaarden voor telewerken' kan men dan voorwaarden voor gebruik van het token opnemen en beheer voor de lifecycle van het token inrichten.
In 4.4 staan een aantal vormen van strong authentication beschreven.

3.5 Medewerker

De medewerker moet beveiligingsbewust zijn en weten welke risico's gepaard gaan met telewerken. Dit beveiligingsbewustzijn kan men versterken door gebruik te maken van presentaties of posters over beveiliging. Ook via een intranetsite is het mogelijk om de (informatie)beveiliging onder de aandacht van de medewerkers te brengen. Belangrijk is wel dat dit vanuit een duidelijke visie wordt aangepakt, waarbij een onderbouwing wordt gegeven waarom een bepaalde manier van telewerken noodzakelijk is.

Verder wordt aanbevolen om afspraken te maken over de rechten en plichten van de medewerker, alsook de mogelijke gevolgen bij een geconstateerde overtreding duidelijk te communiceren. De bepalingen kan men in de 'Gebruiksvoorwaarden voor telewerken' opnemen.

3.6 Beheer

Beheer van telewerken omvat:

- Het uitgeven van het recht tot telewerken;
- Het gebruik en onderhoud van de telewerkplek;
- Het innemen van het recht tot telewerken;
- Het intrekken van het recht tot telewerken.

3.6.1 Uitgeven van het recht tot telewerken

Vaak geeft een lijnmanager toestemming aan een van zijn medewerkers voor telewerken. Dit is de start van een proces waarbij een medewerker middelen ontvangt om te kunnen telewerken. Hierbij krijgt de medewerker niet alleen technische middelen (zoals een laptop of een token) om te kunnen telewerken uitgereikt, maar worden tevens zijn telewerkrechten geactiveerd en geregistreerd. Ook dient de medewerker een gedragscode te ondertekenen waarin alle rechten en plichten ten aanzien van telewerken zijn opgenomen (zie ook referentie [4]). Dit proces wordt meestel ondergebracht bij de ICT-beheerorganisatie.

3.6.2 Het gebruik en onderhoud van de telewerkomgeving

De medewerker zal behoefte hebben aan ondersteuning bij telewerken. Daarvoor kan de organisatie een helpdesk inrichten, die de telewerker kan ondersteunen bij beantwoorden van vragen en daarnaast beveiligingsincidenten kan afhandelen.
Onder onderhoud wordt niet alleen het technisch beheer van de telewerkomgeving verstaan, waarbij de technische beveiligingsmaatregelen van de omgeving (zowel aan de gebruikerskant als in het netwerk) up-to-date worden gehouden, maar ook het bijhouden van wijzigingen in (de configuratie van) de telewerkomgeving.

3.6.3 Het innemen van het recht tot telewerken

De telewerker kan van baan veranderen (interne verandering of overgang naar een andere organisatie) waardoor de behoefte tot gebruik van de telewerkomgeving verdwijnt. Op dat moment moet het recht tot telewerken worden ingenomen.

De telewerker moet dan de middelen tot telewerken inleveren (laptop of werkstation, eventueel token). Ook dient het recht tot telewerken te worden ingetrokken.
Een goede koppeling met de personeelsafdeling kan hierbij helpen. Iedereen kent de verhalen wel waarbij een medewerker al enige tijd niet meer werkzaam is bij een organisatie, maar nog steeds zijn e-mail kan lezen.

3.6.4 Het intrekken van het recht tot telewerken

Een telewerker kan misbruik maken van zijn telewerkomgeving. Indien vooraf duidelijk in de 'Gebruiksvoorwaarden voor telewerken' is aangegeven wanneer er sprake is van misbruik, kan de organisatie het recht tot telewerken intrekken door bijvoorbeeld per direct de remote access tot het bedrijfsnetwerk in te trekken.

Ook bij een (algemeen) beveiligingsincident kan men (tijdelijk) het recht tot telewerken intrekken, om daarmee tijd te kopen teneinde de vereiste aanvullende maatregelen in te kunnen voeren.

3.6.5 Monitoring

Om in een vroeg stadium te detecteren of er iets mis gaat is een adequate monitoring van de telewerkomgeving nodig. Logging levert de noodzakelijke informatie om de oorzaak hiervan te kunnen achterhalen, maar zal ook op reguliere basis bestudeerd moeten worden op eventuele afwijkingen.

4 TECHNISCHE MAATREGELEN

Dit hoofdstuk gaat in op de technische beveiligingsmaatregelen die een organisatie kan nemen in de telewerkomgeving.

4.1 Telewerklocatie

Aangezien een telewerklocatie buiten de invloedssfeer van een organisatie valt, is het meestal niet mogelijk technische beveiligingsmaatregelen op de locatie aan te brengen. Wel kan de organisatie op een, in eigen beheer, geleverde laptop een screensaver installeren die het werkstation afsluit na een bepaalde tijd van inactiviteit van de telewerker. Daarnaast kan een organisatie de harde schijf vercijferen om te voorkomen dat een derde de informatie op een gestolen laptop kan inzien en publiceren.

4.2 Werkstation

De organisatorische maatregelen zijn al aangegeven in het vorige hoofdstuk. Hier zal verder ingegaan worden op de technische maatregelen.

4.2.1 Privé-PC

Sinds kort hebben enkele bedrijven beveiligingsapplicaties geïntroduceerd, waarmee vanuit het netwerk kan worden gecontroleerd of een werkstation dat wordt men wil aansluiten op het netwerk voorzien is van een up-to-date virusscanner en een firewall. Indien de virusdefinities niet up-to-date zijn, kan men toegang tot het netwerk weigeren. Vaak wordt dan via een quarantaine netwerk de laatste virusdefinities aangeboden om de telewerker de gelegenheid te bieden deze te installeren en daarna, op een veilige manier, aan te sluiten op het bedrijfsnetwerk.

4.2.2 Werkstation of laptop beheerd door de werkgever

Op een door de organisatie beheerde laptop zijn beveiligingsmaatregelen technisch af te dwingen door de organisatie. Deze maatregelen omvatten:

- Up to date virusscanner;
- Personall firewall;
- Anti spyware tool;
- Gepatched Operating System en applicaties;
- Vercijferde harde schijf;
- Toegangscontrole d.m.v. een wachtwoord en beperkte gebruikersrechten.

De organisatie kan op een eigen werkstation bepalen welke rechten de telewerker op het werkstation krijgt,alsook welke software op de laptop geïnstalleerd wordt, inclusief beveiligingssoftware zoals een virusscanner en een firewall. Ook kan de organisatie afdwingen dat de telewerker met een gebruikersnaam en wachtwoord

inlogt, waarmee voorkomen wordt dat een derde ongemerkt toegang krijgt tot de informatie die op deze laptop aanwezig is.

4.2.3 Thin client uitvoering

Een speciale versie van een door de werkgever beheerd werkstation is de thin client. Dit is een compact werkstation zonder eigen dataopslag, zoals een windows based terminal voorzien van een browser of andere thin client. Alle bewerkingen worden op de server binnen het bedrijfsnetwerk uitgevoerd. Deze vorm wordt ook wel server based computing genoemd.
Hiermee wordt voorkomen dat de telewerker gevoelige informatie lokaal opslaat of uitprint en daarmee dat deze informatie onbedoeld in verkeerde handen terechtkomt.

4.2.4 Smart phone of PDA

Een in populariteit winnende vorm van telewerken is het gebruik van handhelds, zoals smartphones en Personal Digital Assistants (PDA). De toepassing en beveiliging van deze handhelds is beschreven in de white paper beveiliging van mobiele apparatuur [3]. Hierop zal in dit document niet verder worden ingegaan.

4.3 Verbindingen: ontsluiten van applicaties

Internet is goedkoop en bovendien 'overal' beschikbaar. Het is daarmee de ideale infrastructuur voor telewerken. Internet is echter geen vertrouwde omgeving. Daarom dient er serieus over beveiliging te worden nagedacht. In dit hoofdstuk worden een aantal telewerksituaties beschreven en waarbij wordt aangegeven welke technologieën geschikt zijn om informatie op een veilige manier over internet te transporteren.

4.3.1 Telewerksituaties

Webmail / Webapplicatie

De meest gebruikte vorm van telewerken is webmail of een web enabled applicatie, waarbij gevoelige informatie over het internet wordt verzonden. Een groot voordeel is, dat deze vorm van telewerken overal kan worden gebruikt. Thuis, bij vrienden, familie of in een internetcafé. Tijdens het verzenden moet de informatie worden beveiligd, zodat deze niet door derden gelezen en/of gewijzigd kan worden.

Door middel van SSL (Secure Sockets Layer) kan de informatie worden versleuteld, waardoor de informatie tijdens het transport onleesbaar is en niet kan worden gewijzigd. Aangezien de meest gebruikte webbrowsers standaard SSL ondersteunen, vraagt deze oplossing geen investering van de telewerker.

Toegang op afstand tot bedrijfsinformatie

Webmail is voor telewerkers niet altijd voldoende. In een aantal gevallen moet hij kunnen beschikken over bedrijfsinformatie op het interne netwerk. De technologie om deze interne informatie op een veilige manier via het internet te benaderen via een IPSec (IP Security) VPN (Virtual Private Network). Deze VPN bestaat uit twee componenten. Een IPSec VPN concentrator die tussen het bedrijfsnetwerk en het internet zit en een IPSec VPN client die op de laptop van de telewerker wordt geïnstalleerd. Tussen deze componenten wordt een beveiligde tunnel opgezet waarbinnen versleuteling en authenticatie plaatsvinden. Op deze manier heeft de telewerker op een veilige manier de informatie tot zijn beschikking, zoals hij die ook heeft als hij op het interne bedrijfsnetwerk is aangesloten.

Deze vorm van telewerken vergt wel een investering in laptops en VPN software. Bedenk dat het niet altijd mogelijk is om een VPN verbinding op te zetten, omdat tussenliggende firewalls IPSec verkeer kunnen tegenhouden (bijvoorbeeld hotels).

Server Based Computing

Een trend in kantoor automatisering is Server Based Computing (SBC). Veel organisaties voeren Server Based Computing, omdat het minder eisen stelt aan het werkstation en het beheer hiervan. Bij SBC werkt de medewerker in een sessie op de server en alleen de invoer (muis, toetsenbord) en uitvoer (scherm) worden van/naar het werkstation van de telewerker gestuurd. Dit kan zowel via een SBC client als via een standaard webbrowser. Hierdoor zijn de eisen aan de PC van de telewerker gering.

Server Based Computing is standaard niet geschikt voor telewerken, vanwege gebrek aan beveiliging. Echter door toepassing van Server Based Computing in combinatie met een SSL VPN is dit beveiligingsprobleem op te lossen. Er zijn meerdere producten op de markt die deze functionaliteit kunnen leveren. Deze producten combineren de voordelen van traditionele VPN's, SSL en Server Based Computing.

Beheer op afstand

Onze 7*24 uurs economie vergt tegenwoordig ook 7*24 uurs beheer van systemen. Vaak is het voor organisaties niet haalbaar om hiervoor een ploegendienst in te richten en bestaat de behoefte om een beheerder vanaf thuis een systeem te laten bedienen. Er zijn vele manieren om het beheerconsole van een computer op afstand te bedienen. Dit kan met Secure Shell (SSH). SSH is een tunnel protocol waarmee het verkeer tussen de remote client en de server kan worden versleuteld en authenticatie kan worden toegepast. Op het telewerkstation moet een SSH client worden geïnstalleerd en op de server moet SSH aangezet en geconfigureerd worden. Sterke authenticatie kan worden gerealiseerd in de vorm van server en client certificaten. Omdat de tunnel tussen de client en de server wordt opgezet, is het verkeer dat door de tunnel gaat niet zichtbaar voor de firewall. In de firewall dient dus voorzichtig te worden omgegaan met het toestaan van SSH ver-

keer, bijvoorbeeld door dit alleen van vooraf gedefinieerde IP-adressen (van de beheerders) toe te staan.

4.3.2 Virtual Private Network

Een Virtual Private Network (VPN) is een privé datanetwerk, dat gebruik maakt van een publieke telecommunicatie infrastructuur. Privacy wordt hierbij gerealiseerd door gebruik te maken van een tunneling-protocol en beveiligingsprocedures.

Men onderscheidt drie vormen van VPN's, te weten trusted VPN's, secure VPN's en hybride VPN's:

- Een Trusted VPN is opgebouwd uit gehuurde verbindingen die via het netwerk van een netwerk- of internet provider lopen. Exclusiviteit staat of valt bij de belofte van de provider dat niemand anders gebruik maakt van dezelfde verbinding. Hierdoor kunnen eigen IP adressering en beveiligingsprocedures worden gebruikt. De klant vertrouwt erop dat de provider de integriteit van de verbinding bewaakt, vandaar trusted.

- Een Secure VPN wordt gerealiseerd door het verkeer tussen twee computers te versleutelen. Hierdoor is het mogelijk om een verbinding via een publieke telecommunicatie infrastructuur, zoals het internet, op te zetten zonder dat de oorspronkelijke data door derden kan worden gelezen. Dit biedt grotendeels de functionaliteit van private huurlijnen tegen veel lagere kosten, door gebruik te maken van de gedeelde publieke, niet vertrouwde infrastructuur.

- Een Hybride VPN is een combinatie van de twee eerder genoemde, waarbij er een secure VPN over een trusted VPN wordt gerealiseerd.

Toepassingen

Secure VPN's worden gebruikt wanneer men gevoelige data via het internet wil versturen. De versleuteling zorgt er voor dat de data tijdens het transport niet leesbaar is en niet kan worden gewijzigd. Secure VPN's zijn met name waardevol voor telewerkers die gevoelige informatie over een niet vertrouwde verbinding willen uitwisselen.

Trusted VPN's worden gebruikt door bedrijven die willen weten over welke verbindingen de data wordt getransporteerd. Hierbij kan het bedrijf zijn eigen IP adressering gebruiken en eventueel zelf de routering bepalen.

Trusted en secure VPN's verschillen wezenlijk. Zo biedt een secure VPN beveiliging, maar geen garantie van netwerkverbindingen. Trusted VPN's bieden deze garantie wel, inclusief eventueel Quality of Service (QoS), maar zijn niet beveiligd. Door deze technieken te combineren in een hybride VPN worden de voordelen van beide gecombineerd. Hybride VPN's worden voornamelijk gebruikt indien een or-

ganisatie al een trusted VPN heeft en (een gedeelte van) de verbinding wil beveiligen.

In het kader van telewerken zal verder op Secure VPN's worden ingegaan.

Eisen voor telewerken aan een VPN

Voor secure VPN's geldt het volgende:

- Alle verkeer moet worden versleuteld en geauthenticeerd;
- De beveiligingseigenschappen van de VPN moeten met alle betrokken partijen worden overeengekomen;
- Buiten de VPN is niemand in staat de beveiligingseigenschappen te beïnvloeden. Een 'aanvaller' mag nimmer in staat zijn in te breken of deze eigenschappen te wijzigen.

Beveiligde protocollen geschikt voor telewerken

Voor het creëren van Secure VPN's worden veelal de volgende protocollen gebruikt:

- SSL 3.0 of TLS;
- IPSec;
- SSH.

Deze protocollen zullen hierna beschreven worden.

4.3.3 SSL

Secure Sockets Layer (SSL) en de opvolger hiervan, Transport Layer Security (TLS), zijn protocollen die communicatie over het internet beveiligen. Beide protocollen leveren door middel van versleuteling zowel authenticatie als een beveiligde verbinding over het internet. SSL en TLS zitten in het OSI model tussen applicatieprotocollen zoals HTTP, SMTP en Usenet en het transportprotocol TCP, dat deel uitmaakt van de protocolsuite TCP/IP. Ondanks dat zowel SSL als TLS veiligheid kan bieden aan elk protocol dat gebruik maakt van TCP, wordt SSL het meest gebruikt voor HTTPS, bijvoorbeeld ter beveiliging van gevoelige gegevens. De server bepaalt de sterkte van de vercijfering. Gezien de huidige stand van de techniek wordt hiervoor minimaal 3DES of AES-128 aanbevolen.

Toepassingen voor SSL

Webapplicaties
De meest gebruikte toepassing van SSL is het beveiligen van websites. In plaats van de website te openen via http (poort 80) wordt de website via een beveiligde connectie geopend via https (port 443). Ook e-mail kan vaak via HTTP of HTTPS in de internetbrowser worden geopend, beter bekend als webmail.

E-mail client
Een methode om met een e-mail client veilig e-mail te behandelen is 'pop3 over SSL/TLS' of 'imap4 protocol over SSL/TLS'. Er wordt dan over respectievelijk poort 995 (pop3s) en poort 993 (imaps) gecommuniceerd. De meeste e-mail clients ondersteunen tegenwoordig SSL/TLS.

SSL VPN
Een speciale vorm van een Virtual Private Network (VPN) is de SSL VPN. Deze vorm van VPN's wordt geïmplementeerd in OSI laag 7, de applicatie laag. Alle communicatie gaat via HTTPS. Deze oplossing wordt daarom ook wel 'HTTPS VPN' of 'HTTP over SSL VPN' genoemd.

Met de webbrowser wordt een beveiligde tunnel opgezet tussen de client en de webportal, waar de gebruiker in een keuzemenu (Portal) de applicaties te zien krijgt, waartoe hij gerechtigd is. Het grote voordeel is dat aan de gebruikerzijde geen installatie hoeft plaats te vinden, aangezien een webbrowser vrijwel altijd standaard aanwezig is.

Applicaties die niet geëmuleerd kunnen worden via HTTP, worden niet ondersteund. Deze applicaties gebruiken protocollen die parallel zijn aan HTTPS in de applicatie laag, waardoor de HTTPS tunnel het netwerkverkeer niet 'ziet'. Er zijn twee methodes om dit probleem aan de client zijde te omzeilen, 'Port Forwarding' en 'Network Drivers'.

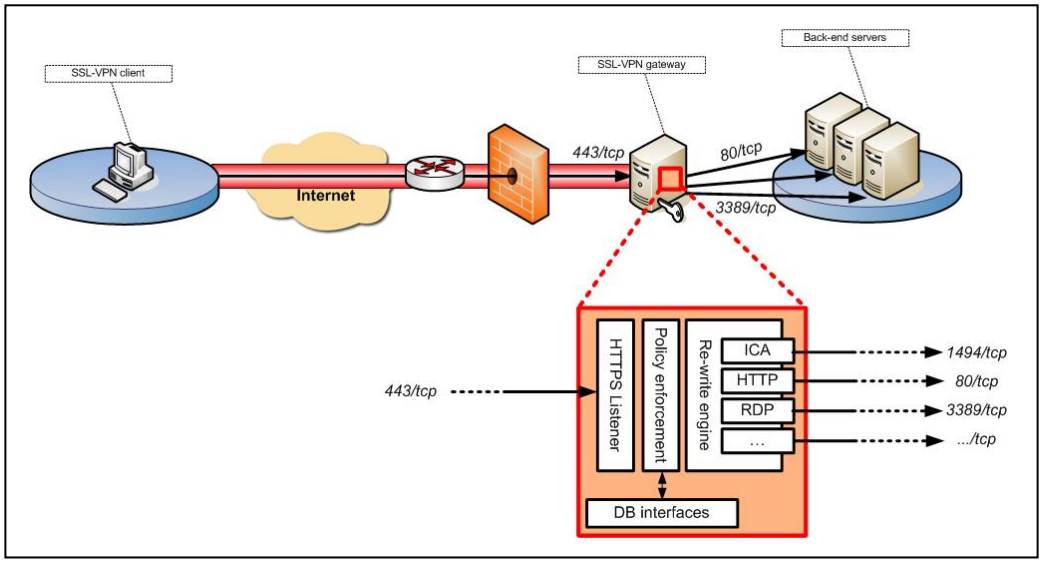
Port Forwarding
Dit is een 'Thin Client' benadering. Een 'agent' wordt gedownload en geïnstalleerd wanneer er een non-web applicatie wordt opgestart vanuit de Portal. Deze agent zorgt ervoor dat het verkeer van de applicatie doorgestuurd wordt naar de HTTPS tunnel. Er zijn echter een aantal nadelen aan 'Port Forwarding':

- Agents hebben vaak administratieve rechten nodig op het werkstation en dat is niet altijd het geval.
- Port Forwarding werkt alleen bij applicaties die gebruik maken van statische poorten. Applicaties met dynamische poorten kunnen dus niet ontsloten worden.
- Port Forwarding kan niet worden gedeeld. Er kunnen dus niet meerdere non-web applicaties tegelijk worden ontsloten.

Netwerk Drivers
Om applicaties te ontsluiten die via een SSL VPN gebruik maken van dynamische poorten, is een laag 3 of 4 netwerkdriver nodig. Dit vereist weer de installatie van

thick client software en administratieve rechten. Als de netwerkdriver eenmaal is geïnstalleerd, dan wordt het verkeer van de non-web applicatie doorgestuurd naar de HTTPS tunnel. Voor deze situatie gelden dezelfde nadelen als beschreven in de paragraaf over VPN's.
Aan de server zijde kunnen server-side plug-ins worden geïnstalleerd die applicaties via HTTP(S) aanbieden, waardoor op de client alleen de webbrowser nodig is.

Onderstaande figuur geeft een voorbeeld van een SSL VPN infrastructuur.



Producten
Er zijn een aantal producten op de markt, die gebruik maken van SSL VPN technologie. Deze bieden allen applicaties aan via een webinterface (thin client) en via client applicaties op het werkstation (fat of thick client).

Conclusie voor SSL
SSL is uitermate geschikt voor het veilig verbinden naar websites en pop3/imap servers. Het is minder geschikt voor applicaties die standaard geen SSL ondersteuning bieden. Hieronder worden de voor- en nadelen beschreven.

Voordelen
- Standaard functionaliteit. Er hoeft geen extra software geïnstalleerd te worden. Zowel webbrowsers als andere client software ondersteunen vaak SSL.
- Firewall toegang. Over het algemeen wordt HTTPS door firewalls toegestaan.
- Stringente beveiligingspolicies. De beheerder kan bepalen welke gebruikers recht hebben op het gebruik van de applicaties (autorisaties).

Nadelen

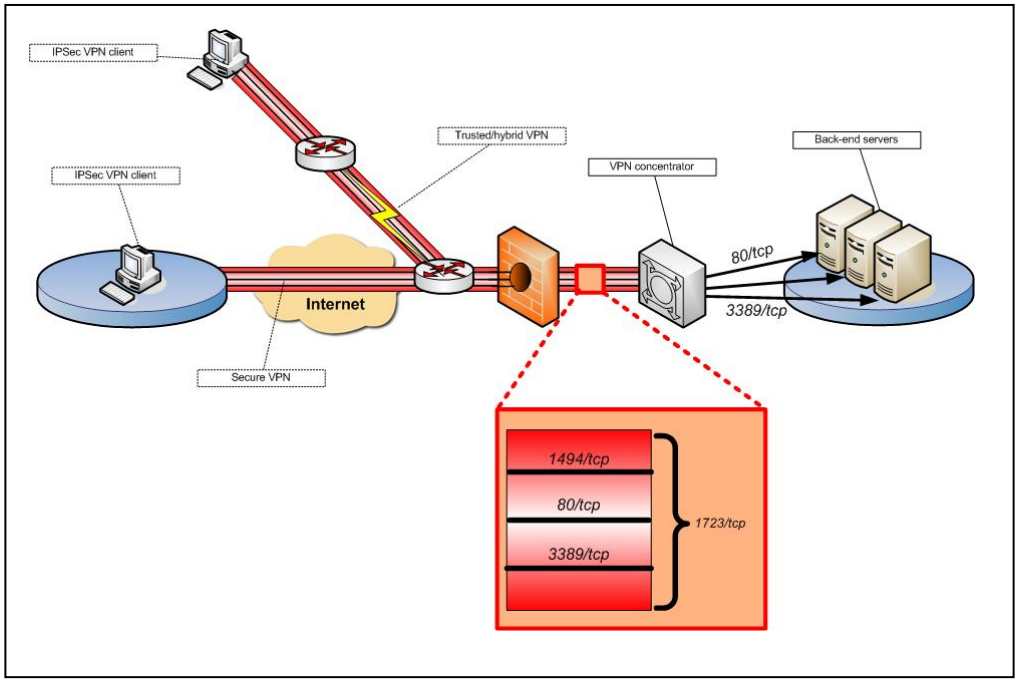
- De meeste non-web applicaties bieden standaard geen SSL ondersteuning.
- Webversies van applicaties hebben vaak een andere 'look en feel' dan de desktop versie. Dit doet een beroep op het aanpassingsvermogen van de gebruiker.

In de volgende paragraaf, IPSec, wordt een overzicht gegeven van SSL VPN versus IPSec VPN.

4.3.4 IPSec

IPSec is een versleutelingmechanisme voor IP-netwerken dat end-to-end beveiliging levert op de netwerklaag (laag 3) van het OSI model. Het biedt vertrouwelijkheid, integriteit van de data en authenticiteit van de afzender van de data door het toepassen van verscheidene protocollen en encryptie technieken. IPSec wordt vaak gebruikt in combinatie met een tunneling protocol, zoals L2TP (Layer 2 Tunnel Protocol), om trusted VPN's beter te beveiligen. Bij het opzetten van een IPSec verbinding, worden de beveiligingsparameters vastgesteld. Deze kunnen handmatig worden ingesteld of door middel van Internet Key Exchange (IKE) protocol met certificaten of 'preshared secrets'.

Onderstaande figuur geeft een voorbeeld van een IPSec VPN infrastructuur.



IPSec kent twee protocollen, dit zijn:

- Authentication Header (AH). AH zorgt voor data integriteit en authenticiteit van de afzender van IP packets. Deze vorm van IPSec versleutelt de in-

formatie niet en wordt afgeraden voor een telewerkverbinding over een niet vertrouwd netwerk.
- Encapsulation Security Payload (ESP). ESP zorgt, naast integriteit en authenticiteit, ook voor vertrouwelijkheid. Dit kan door alleen de data van één IP packet te versleutelen of door het hele IP packet te versleutelen.

IPSec kan in twee modes opereren, in transport mode of in tunnel mode. In transport mode wordt alleen de data van één IP packet beschermd. In tunnel mode wordt het hele IP packet beschermd.

Deze protocollen en modes maken de volgende configuraties mogelijk:

	Transport mode	**Tunnel mode**
AH	Integriteit en authenticiteit van de data van één IP packet	Integriteit en authenticiteit van het hele IP packet inclusief de header
ESP	Vertrouwelijkheid van de data van één IP packet	Vertrouwelijkheid van het hele IP packet inclusief de header

IPSec VPN oplossingen worden, zoals genoemd, geïmplementeerd in de netwerklaag (layer 3) van het OSI model. Hierdoor is een thick-client netwerk driver nodig om direct IP packets te kunnen manipuleren. Deze driver onderschept netwerk packets, versleutelt ze en stuurt ze vervolgens via het internet naar de VPN gateway. Dit levert de volgende voor- en nadelen op.

Voordelen:
- Brede applicatie ondersteuning. De applicaties merken niet dat er via VPN gecommuniceerd wordt.
- 'Op kantoor' gebruikers ervaring voor de telewerker. Op de snelheid na waant de gebruiker zich alsof hij direct aan het LAN op het kantoor is aangesloten.

Nadelen:
- Thick-client software. Dit betekent dat er een component (VPN Client) geïnstalleerd dient te worden op het telewerkstation. IT beheerders van een organisatie hebben geen controle over privé PC's, computers in hotels of in internet cafés. Deze oplossing is dus meestal beperkt tot werkstations en laptops van de organisatie.
- Hoge onderhoudskosten. Beheerinspanning van de Helpdesk voor beantwoorden vragen en voor update/upgrade inspanningen zijn hoog.
- Firewall toegang. VPN protocollen zijn veelal niet toegestaan op firewalls. Dit kan connectie problemen opleveren in niet door het bedrijf beheerde omgevingen, zoals klantnetwerken en hotels.
- Weinig controle over het verkeer.

Het is raadzaam om split tunneling uit te zetten op het eindpunt van de VPN tunnel van de telewerker. Door middel van 'split tunneling' is het mogelijk om, naast de VPN sessie, een tweede verbinding met het internet op te zetten. Dit levert het risico op dat derden via deze tweede sessie misbruik kunnen maken van de VPN

en zo toegang zouden kunnen krijgen tot het netwerk aan de andere kant van de tunnel.

Onderstaande tabel geeft de kenmerken van IPSec VPN en SSL VPN weer.

	IPSec VPN	**SSL-VPN**
Client	IPSec VPN Client	Webbrowser
OSI-laag	Netwerk (laag 3)	Applicatie (laag 7)
Toegangsbeveiliging	Basis (host- en poortniveau)	Uitgebreid (URL/URI gebaseerd)
Doelgroep	Interne medewerkers	Interne medewerkers en klanten (extranetten)
Voordelen	• Toegang tot alle applicaties is mogelijk door koppeling op netwerkniveau.	• Vereist alleen een web browser op de client; • Granulaire toegangsrechten zijn mogelijk; • Werkt via standaard HTTPS-verkeer waardoor geen veranderingen in de infrastructuur benodigd zijn.
Nadelen	• Aparte software is vereist op de client; • Kan alleen benaderd worden vanaf specifieke clients; • Complex beheer; • Vereist een infrastructuur die VPN-verkeer toestaat.	• Alleen web-enabled applicaties kunnen eenvoudig beschikbaar worden gesteld; • Voor niet web-enabled applicaties moet alsnog software op de client worden geïnstalleerd; • Er kan informatie op de client achterblijven.

4.3.5 SSH

Secure Shell (SSH) is ontwikkeld als veilig alternatief voor de onveilige beheerprotocollen zoals Telnet, rlogin, rsh en ftp. In tegenstelling tot deze protocollen biedt SSH versleuteling en 'strong authentication'. Met SSH wordt een beveiligde tunnel opgezet tussen client en server, waardoor het veilig is om gevoelige data, zoals login gegevens, versleuteld te transporteren. SSH2 is een verbeterde versie van SSH en is een standaard geworden. SSH2 heeft voorkeur boven versie 1.

Kenmerken van SSH2 zijn:

- Sterke encryptie
  SSH2 ondersteunt de sterke encryptie algoritmes zoals 3DES. waardoor het aftappen van bijvoorbeeld wachtwoorden niet mogelijk is.

- Strong Message Authentication (SHA-1)
  SSH2 ondersteunt ook public-key authenticatie met X.509 en andere certificaten.
- Remote command execution
  SSH2 heeft de functionaliteit om commando's op afstand uit te voeren en daarbij informatie uit te wisselen zonder dat er een interactieve sessie voor moet worden opgestart.
- Tunneling
  SSH2 kan hiermee worden gebruikt als een Virtual Private Network (VPN) waardoor het mogelijk wordt om onveilige netwerkprotocollen op een veilige manier binnen het netwerk op te nemen.
- Ondersteuning van Digital Signature Algorithm (DSA)
- Periodieke vervanging van sessiesleutels door middel van Diffie-Hellman

4.3.6 Server Based Computing

Om SBC geschikt te maken voor telewerken, kan gebruik gemaakt worden van SSL VPN. Hierbij wordt een beveiligde SSL tunnel opgezet tussen webbrowser van de telewerker en de SSL VPN gateway die tussen de SBC server en het internet 'staat'. Net als een IPSec VPN heeft deze telewerkvorm het voordeel dat de telewerker over de informatie kan beschikken die hij op het kantoor ook heeft. Het voordeel ten opzichte van IPSec VPN is dat SSL VPN verkeer (HTTPS) meestal wel door firewalls wordt toegelaten. Net als bij webmail, heeft de telewerker alleen een webbrowser nodig. Deze kan dus op elke willekeurige internet PC terecht. Dit heeft weer als nadeel dat er informatie op vreemde computers achter kan blijven.

4.4 Toegang tot informatie

4.4.1 Strong authentication

Binnen bedrijfsnetwerken krijgt de medewerker meestal toegang tot het netwerk en de gegevens door middel van het opgeven van een gebruikersnaam en een wachtwoord. Binnen een bedrijfspand kan door fysieke controle bij de ingang van het pand op relatief eenvoudige wijze het risico op misbruik van gebruikersnaam en wachtwoord door derden worden verminderd.

Met de toename van telewerken, externe toegang tot bedrijfsnetwerken en dergelijke is deze controle op wie toegang heeft tot bepaalde informatie een stuk lastiger. Aangezien de informatie die op deze manier toegankelijk is vaak bedrijfskritisch is, is het belang van authenticatie van de gebruiker groter geworden. Hiervoor is het gebruik van slechts een gebruikersnaam en wachtwoord niet voldoende.

Bij gevoelige informatie zijn sterke maatregelen nodig voor de toegang tot netwerken, applicaties en systemen. Om in hogere mate zeker te kunnen zijn dat de gebruiker die zich aanmeldt ook echt deze gebruiker is, kan er gebruik gemaakt worden van strong authentication. Strong authentication maakt gebruik van het principe dat je kunt aantonen dat je daadwerkelijk degene bent, die je zegt dat je bent door iets *wat je weet* en door iets *wat je bezit* of *wat je bent*.

1. *Wat je weet* (bijvoorbeeld: password / PIN code)
2. *Wat je bezit* (bijvoorbeeld: token)
3. *Wat je bent* (bijvoorbeeld: biometrisch kenmerk)

Op deze manier kan op basis van twee (ook wel twee factor authenticatie genoemd) of meerdere factoren worden aangetoond dat je daadwerkelijk bent wie je zegt dat je bent.

Er zijn een groot aantal vormen van strong authentication beschikbaar. In deze paragraaf worden zes gangbare oplossingen aangegeven:

1. Certificaten (software, op smart card of USB token)
2. One Time Password token
3. PINpad tokens
4. SMS authenticatie
5. Authenticatie m.b.v. software op PDA of smartphone
6. Niegebach authenticatie

Certificaten
Certificaten zijn gebaseerd op public key technologie. Hierbij worden twee cryptografische sleutels gegenereerd, een private key en een public key. Deze sleutelparen zijn aan elkaar gekoppeld en zijn uniek voor elk individu. De public key wordt ondertekend door een Certificate Service Provider (CSP) met als resultaat een X.509-certificaat. De CSP verklaart daarmee, dat deze public key toebehoort aan het betreffende individu. Dit certificaat ondersteunt een geavanceerde digitale handtekening. Grofweg bestaan er twee varianten van certificaten, de software certificaten en certificaten op een token.

1. *Software certificaten:* certificaten zoals die in webbrowser omgevingen geïnstalleerd worden.
2. *Certificaten op smart card:* certificaten die worden opgeslagen op een smart card.

One time password token
Met het One-Time Password (OTP) token wordt een wachtwoord van 6 tot 8 cijfers gegenereerd en weergegeven op de display van het persoonsgebonden OTP token. Met een OTP token wordt het wachtwoord voor toegang tot een afgeschermde bron continu gewijzigd.

PINpad token
Een PINpad Token is voorzien van een display en een toetsenbord om een PIN in te kunnen voeren. Met behulp van dit PINpad Token wordt na invoeren van een PIN code op het token zelf een One-Time Password gegenereerd.
Naast het genereren van OTP's is het op enkele PINpad Tokens mogelijk om op basis van een aantal input criteria ook een digitale handtekening te genereren (op basis van Message Authentication Code).

SMS Authenticatie
Gebruikers die willen inloggen met behulp van SMS authenticatie vullen naast hun gebruikersnaam en wachtwoord een extra transactiecode in, die de betreffende gebruiker ontvangt per SMS op zijn/haar mobiele telefoon.

Authenticatie met behulp van PDA of smartphone
Bij deze vorm van strong authentication wordt de PDA of smartphone gebruikt als platform voor de software waarmee een OTP wordt gegenereerd.

Niegebach authenticatie
Niegebach staat voor **Nie**t **ge**koppelde **ba**ncaire **ch**ipkaartlezer. Niegebach is een authenticatie methode waarbij gebruik wordt gemaakt van de chipkaart die door banken wordt verstrekt. Authenticatie vindt plaats door middel van gebruikersnaam en wachtwoord, aangevuld met het gebruik van een bancaire chipkaart, PIN code en kaartlezer die ook gebruikt wordt bij het internetbankieren.

4.4.2 *Autorisatie*

Nadat de telewerker zich heeft geauthenticeerd kan hij, afhankelijk van de functie, geautoriseerd worden voor toegang tot bepaalde applicaties en informatie. Dit wordt ook wel policy enforcement genoemd. Meestal heeft een organisatie al een tool in gebruik voor autorisatie van medewerkers tot applicaties en informatie. Deze kan uitgebreid worden met autorisaties voor medewerkers vanaf een telewerkplek.

4.4.3 *Compartimentering netwerk*

Binnen het bedrijfsnetwerk is informatie vaak verspreid over een aantal systemen opgeslagen. Met een goede configuratie van de externe firewall en toepassing van een DeMilitarized Zone (DMZ) kan de toegang van de telewerker tot die informatie, die op een telewerkplek kan worden benaderd, worden beperkt.

4.5 Beheermaatregelen

Telewerken houdt in dat (een deel van) het interne netwerk benaderbaar wordt vanaf locaties buiten de organisatie via onveilige infrastructuren zoals het internet. De genoemde technologieën hebben extra beveiligingsvoorzieningen zoals authenticatie en versleuteling. Deze paragraaf beschrijft waarop gelet moet worden bij het beheren van een telewerkomgeving.

4.5.1 *Opsomming van beheermaatregelen*

Maatregelen die getroffen kunnen worden om een veilige en beheer(s)bare telewerkomgeving te creëren, zijn:

- Logging monitoren
- Beheer goed inregelen (up-to-date houden van software)
- Beheer certificaten
- Client checks instellen
- Autorisatie op functionaliteit interne netwerk (Policy Enforcement)

Deze zullen hierna beschreven worden.

4.5.2 *Logging monitoren*

Een ander belangrijk punt is logging. Logging wordt gebruikt om na te gaan of remote toegang niet misbruikt wordt. Informatie die minimaal gelogd moet worden, is:

- Welke werkstations maken een VPN verbinding en welke pogingen mislukken;
- Welke credentials worden gebruikt of misbruikt voor toegang tot het netwerk van de organisatie;
- Welk verkeer is er tussen het telewerkstation en het interne netwerk.

4.5.3 Beheer goed inregelen (up-to-date houden van software)

De genoemde beveiligingsprotocollen maken gebruik van clients. Dit betekent dat deze software op het werkstation van de telewerker staat, die up-to-date moet worden gehouden. Voor laptops die regelmatig op het bedrijfsLAN worden aangesloten is dit centraal te regelen. Vaste thuis PC's worden echter niet op het bedrijfsLAN aangesloten en hiervoor moeten dus duidelijke procedures en richtlijnen worden opgesteld.

Daarnaast worden IPSec clients geconfigureerd met beveiligingsparameters, zoals 'preshared secrets' of certificaten. Ook deze parameters dienen beheerd en, indien vereist, regelmatig gewijzigd te worden. Ook de software die gebruikt wordt voor SSL of SSH moet up-to-date gehouden te worden, bijvoorbeeld de webbrowser of de e-mail client.

4.5.4 Beheer certificaten

Zowel bij SSL als SSH worden certificaten toegepast. Als de server en de client voorzien zijn van certificaten kan men wederzijdse authenticatie uitvoeren van zowel de server als de client en zo een beveiligde verbinding met de server opzetten. Dit houdt wel in dat deze client certificaten beheerd moeten worden om misbruik te voorkomen of tijdig waar te nemen.

4.5.5 Client checks instellen

Het is mogelijk om, voordat een VPN wordt opgezet, te controleren of het telewerkstation is voorzien van de laatste security patches, virus definities, etc. Door het uitvoeren van dit soort controles wordt voorkomen dat het netwerk geïnfecteerd raakt met malware

4.5.6 Autorisatie op functionaliteit interne netwerk

Voor alle soorten VPN geldt dat goed moet worden nagedacht over de mate van openstelling van het interne netwerk aan telewerkers. Meestal krijgt men via een VPN niet direct toegang tot het interne LAN, maar tot een 'demilitarized zone' (DMZ), die van het interne LAN is gescheiden door middel van een firewall. In deze firewall wordt vervolgens bepaald over welke functionaliteiten de telewerker kan beschikken. De telewerken dient geautoriseerd te worden voor alleen die functionaliteit waartoe hij gerechtigd is en die hij ook nodig heeft voor het uitvoeren van zijn taak.

BIJLAGE A: VOORBEELDEN TELEWERKOMGEVING

Zoals we gelezen hebben in dit document bestaat een telewerkomgeving uit een aantal schakels die elk hun eigen risico's kennen. Afhankelijk van de gewenste functionaliteit en de acceptabele risico's kan een organisatie kiezen voor verschillende oplossingen. In deze bijlage zijn een tweetal mogelijke telewerkomgevingen omschreven op basis van de gewenste functionaliteit voor de medewerkers.

A.1 Raadplegen e-mail en agenda

Een veel gebruikte oplossing voor het inzien van e-mail en agenda, is het gebruik van webmail. Met deze omgeving kan de telewerker vanaf elke willekeurige werkplek, met behulp van de daarop geïnstalleerde browser, zijn e-mail raadplegen. Wel wordt aanbevolen om de telewerker te voorzien van een token voor strong authentication, omdat de combinatie van alleen username en wachtwoord in het algemeen niet meer als voldoende veilig wordt beschouwd.

Dit is een voor telewerkers flexibele oplossing, die echter de volgende risico's kent:

- Inzien informatie door een buitenstaander (shoulder surfen: het over de schouder meekijken);
- Het, in de cache van de browser, achterblijven van informatie;
- Malware besmetting van e-mail vanaf een niet vertrouwd werkstation.

Indien de organisatie een risicoanalyse heeft uitgevoerd, is het duidelijk welke risico's de organisatie accepteert voor het ontsluiten van de desbetreffende informatie via deze telewerkomgeving. Hierbij moet men niet vergeten de medewerkers hiervan op de hoogte te stellen, om deze zo ook bewust te maken van de risico's die de organisatie loopt.

Deze omgeving vergt niet meer dan de aanschaf en installatie van een webserver die een SSL-verbinding (met minimaal AES-128 of vergelijkbaar) ondersteunt. Daarnaast dienen de tokens voor strong authentication beheerd te worden.

Deze omgeving kan met behulp van een SSL-VPN worden uitgebreid met toegang tot andere web enabled applicaties, zoals bijvoorbeeld een HRM-applicatie.

A.2 Toegang tot het bedrijfsnetwerk van de organisatie

Voor een andere organisatie kan webmail onvoldoende zijn en heeft de telewerker volledige toegang tot het bedrijfsnetwerk van de organisatie nodig. Bijvoorbeeld toegang tot de HRM-applicaties of verkoop gegevens. Ook in deze situatie moet de organisatie een risicoanalyse uitvoeren om de juiste maatregelen te bepalen voor het gewenste beveiligingsniveau. De kans dat bij deze vorm van telewerken gevoelige informatie uitlekt en dat de organisatie hierdoor schade lijdt, is aanmerkelijk groter dan bij A.1.

De beveiligingsmaatregelen voor deze telewerkomgeving omvatten onder andere:

- Een door de organisatie beheerde laptop of computer met daarop:
  - Een up-to-date virusscanner;
  - Actuele patches;
  - Gehardend OS en applicaties;
  - Een vercijferde harde schijf met daarop opgeslagen data;
  - De IPSec client, geconfigureerd voor de tunnelmode waarbij split-tunneling niet is toegestaan;
- Een IPSec verbinding tussen telewerker en het bedrijfsnetwerk;
- Een token voor strong authentication;
- Een DMZ waarin de VPN-concentrator is geplaatst;
- Eventueel is de firewall zodanig geconfigureerd dat toegang alleen mogelijk is vanaf vooraf gedefinieerde IP-adressen met goede logging.

Bovenstaande telewerkomgeving vergt een investering van de organisatie in laptops, IPSec apparatuur en software en extra beheer van werkstations en tokens.

BIJLAGE B: WOORDENLIJST

Begrip	Omschrijving
FTP	File Transfer Protocol
CSP	Certificate Service Provider
DMZ	Demilitarized Zone
FTP	File Transfer Protocol
HRM	Human Resource Management
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IPSec	IP Secure
OSI	Open Systems Interconnection
OTP	One Time Password
PDAVPN	Personal Digital AssistentVirtual Private Network
SBC	Server Based Computing
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
Telewerken	Telewerken is het vanaf een locatie buiten de organisatie door middel van (data) communicatie middelen deelnemen aan het arbeidsproces.
Thuiswerken	Een vorm van telewerken waarbij de privé-PC van de medewerker wordt gebruikt (vaak voor webmail).
TLS	Transport Layer Security
VIR	Voorschrift Informatiebeveiliging Rijksoverheid
VPN	Virtual Private Network

GOVCERT.NL

BIJLAGE C: REFERENTIES

[1]	Voorschrift Informatiebeveiliging Rijksdienst, 1994
[2]	Handboek A&K analyse (ACIB)
[3]	White paper GOVCERT.NL: Beveiliging mobiele apparatuur en datadragers. Dit paper is momenteel alleen beschikbaar voor deelnemers van GOVCERT.NL
[4]	Voorbeeld gedragscode E-werken (VNO/NCW)