2016

Scriptie

VEILIGE TOEPASSING VAN HET “BRING YOUR OWN DEVICE” PRINCIPE

Auteur:	Dion Kruijswijk
Studentennummer:	1632504
Studierichting:	System- and Network Engineering
Bedrijf:	SURFsara te Amsterdam
Examinatoren:	Lex Borger en Bart Bosma

Versiebeheer

Datum	Versie	Reviewer	Beschrijving
24-02-16	0.1	Dion Kruijswijk	Opzet scriptie, invulling hoofdstuk 2,3,4,5 en 6
26-02-16	0.2	Dion Kruijswijk	Invulling hoofdstuk 7 en hoofdstuk 8
29-02-16	0.3	Dion Kruijswijk	Aanpassing hoofdstuk 5, aanpassing hoofdstuk 7
03-03-16	0.4	Dion Kruijswijk	Toevoeging informatie interviews, aanpassing hoofdvraag en methoden
07-03-16	0.5	Dion Kruijswijk	Aanpassing hoofdstuk 5, 6 en 7.
09-03-16	0.6	Dion Kruijswijk	Aanpassing hoofdstuk 8, invulling hoofdstuk 9
15-03-16	0.7	Dion Kruijswijk	Aanpassing hoofdstuk 5,6,7,8 en 9
23-03-16	0.7	Leonieke Mevius	Feedback op versie 0.7
24-03-16	0.8	Dion Kruijswijk	Feedback op versie 0.7 verwerkt
04-04-16	0.8	Bart Bosma	Feedback op versie 0.8
31-03-16	0.9	Dion Kruijswijk	Aanvulling hoofdstuk 8 en 9
05-04-16	0.10	Dion Kruijswijk	Feedback op versie 0.8 verwerkt
07-04-16	0.11	Dion Kruijswijk	Aanpassingen op hoofdstuk 6, 7, 8 en 9
12-04-16	0.12	Dion Kruijswijk	Aanpassing hoofdstuk 9, invulling hoofdstuk 10
13-04-16	0.12	Leonieke Mevius	Feedback op versie 0.12
14-04-16	0.13	Dion Kruijswijk	Feedback op versie 0.12 verwerkt
21-04-16	0.13	Bart Bosma	Feedback op versie 0.13
22-04-16	0.14	Dion Kruijswijk	Feedback op versie 0.13 deels verwerkt
29-04-16	0.15	Dion Kruijswijk	Feedback op versie 0.13 verwerkt
02-05-16	0.16	Dion Kruijswijk	Toevoeging Proof of Concept resultaten
03-05-16	0.17	Dion Kruijswijk	Aanpassing hoofdstuk 8
06-05-16	0.18	Dion Kruijswijk	Toevoeging bijlages, aanpassing hoofdstuk 6, 9 en 10
09-05-16	0.18	Leonieke Mevius	Feedback op versie 0.18
10-05-16	0.19	Dion Kruijswijk	Feedback op versie 0.18 deels verwerkt
11-05-16	0.20	Dion Kruijswijk	Feedback op versie 0.18 verwerkt
12-05-16	0.21	Dion Kruijswijk	Toevoeging management samenvatting, conclusie en evaluatie
14-05-16	0.21	Jaap Dijkshoorn	Feedback op versie 0.21
17-05-16	0.21	Paul Reemeijer	Feedback op versie 0.21
19-05-16	0.21	Bart Bosma	Feedback op versie 0.21
20-05-16	0.22	Dion Kruijswijk	Feedback op versie 0.21 verwerkt
23-05-16	0.22	Leonieke Mevius	Feedback op versie 0.22
23-05-16	0.23	Dion Kruijswijk	Feedback op versie 0.22 verwerkt
25-05-16	0.23	Jeroen Engelberts	Feedback op versie 0.23
25-05-16	1.0	Dion Kruijswijk	Feedback verwerkt, definitieve versie van de scriptie gemaakt

Managementsamenvatting

Voor SURFsara is er onderzoek gedaan naar het veilig toepassen van het “Bring Your Own Device” (BYOD) principe. SURFsara heeft aangegeven BYOD toe te willen passen, omdat externe ingehuurde medewerkers gebruik maken van eigen hardware.

Om werkzaamheden uit te voeren is er vaak toegang tot data en applicaties binnen de organisatie vereist. Externe medewerkers maken gebruik van eigen laptops, maar ook van telefoons en tablets. Deze hardware moet veilig toegelaten kunnen worden tot het netwerk van SURFsara. Om te bepalen wat voor oplossing het beste voldoet voor SURFsara, is de volgende hoofdvraag opgesteld: “*Welke methode is het meest geschikt om het “Bring Your Own Device” principe op een veilige en goed te beheren wijze toe te passen bij SURFsara, zodat de integriteit en de vertrouwelijkheid van SURFsara data en privédata gewaarborgd zijn?*”. Deze hoofdvraag wordt beantwoord aan de hand van de deelvragen.

Voor SURFsara is bepaald dat BYOD inhoudt dat externe medewerkers hun eigen hardware meenemen en gebruiken. Deze hardware is dus geen eigendom van SURFsara en wordt om die reden niet door SURFsara beheerd. Het is niet bekend welke hard- en software gebruikt wordt, maar het is wel gewenst inzicht te krijgen in het gebruik van hard- en software. Om BYOD toe te kunnen passen moet er een beleid geschreven worden om onder andere de aansprakelijkheid, aanbevolen software en eventuele beperkingen te beschrijven. Voor het beleid wordt de huidige (AS-IS) situatie beschreven.

Er wordt eerst naar de huidige situatie gekeken en op basis daarvan wordt het gewenste beleid opgesteld. Momenteel is er een “Choose Your Own Device” (CYOD) beleid, waarbij er voor interne medewerkers de keuze is uit een beperkt aantal laptops of desktops. Voor het gebruik van CYOD hardware zijn regels en richtlijnen opgesteld, waaronder de Acceptable Use Policy. Externe medewerkers gebruiken echter eigen hardware of krijgen een leenlaptop van SURFsara. Met deze hardware is in sommige gevallen toegang tot het netwerk van SURFsara mogelijk. Via Wi-Fi of een externe locatie worden data en applicaties met een VPN-verbinding benaderd. Omdat er geen controle is op de hardware en het niet bekend is of deze hardware besmet is met malware, is het gewenst dat er een aanpassing wordt doorgevoerd om risico’s te beperken. In de huidige situatie is de enige extra beveiliging, naast het gebruik van een login en wachtwoord, een token die vereist is om de VPN verbinding tot stand te brengen.

Om de risico’s te beperken moet er voor BYOD een beleid bepaald en geschreven worden. Dit beleid wordt dan naast het CYOD beleid toegepast. In het BYOD beleid moeten regels en richtlijnen opgenomen worden, zodat externe medewerkers de aanbevolen applicaties gebruiken en zich bewust zijn van de schade door besmette BYOD hardware. In het beleid worden onderdelen van de ISO27001:2013 norm opgenomen. Het beleid moet gecontroleerd en ondersteund worden door een technische oplossing. De oplossing wordt bepaald aan de hand van een toepassingsselectie en een “Proof of Concept”. In de toepassingsselectie is bekeken welke producten aan de eisen en wensen van SURFsara in theorie voldoen. De beste producten uit de toepassingsselectie worden in de “Proof of Concept” getest op basis van de eisen, wensen en doelstellingen. Het product dat het beste aansluit op de gestelde eisen, wensen en doelstellingen kan het beleid ondersteunen.

De technische oplossing kan niet alle risico's beperken, daarom moeten er preventieve maatregelen genomen worden om besmettingen en dataverlies te voorkomen. Een aantal preventieve maatregelen zijn medewerkers bewust maken van malware, het toepassen van virusscanners, het toepassen van een anti-spam product en het gebruik van opslagmedia zoals USB-sticks beperken. Daarnaast moet data beschermd worden, zodat de integriteit en vertrouwelijkheid hiervan gewaarborgd is. Dit kan gerealiseerd worden door op meerdere plaatsen virusscanners te installeren (Defense in Depth) en software van verschillende leveranciers te gebruiken. Andere mogelijkheden, zoals een afgeschermde omgeving, data encryptie en applicatie streaming, zorgen ook voor de waarborging van de integriteit en vertrouwelijkheid.

De technische oplossing moet beheerd en gemonitord worden door de afdeling Interne Automatisering. Voor het beheer wordt er gebruik gemaakt van portals en command-line interfaces via een terminal op verschillende besturingssystemen. Zo kunnen aanpassingen en updates uitgevoerd worden. Een deel van het monitoren van de technische oplossing zit in het gekozen product, maar er kan ook voor gekozen worden om een externe tool te gebruiken. Door deze tool te gebruiken worden alle statussen en meldingen gemaild, zodat er actie ondernomen kan worden door de beheerder.

Wanneer het beleid met de technische oplossing geïmplementeerd wordt, kan bij SURFsara het BYOD principe worden toegepast. De risico's worden beperkt als het principe op een veilige en goed te beheren manier wordt toegepast, waarbij de vertrouwelijkheid en integriteit van data gewaarborgd is.

Inhoudsopgave

1. Inleiding

Mijn afstudeeronderzoek naar het veilig toepassen van het Bring Your Own Device (BYOD) principe bij SURFsara wordt in deze scriptie beschreven.

BYOD houdt in dat medewerkers hun eigen (privé) hardware meenemen om daarop vervolgens voor het bedrijf hun werkzaamheden te doen. Het is niet bekend wat precies op deze hardware staat waardoor data mogelijk besmet of beschadigd kan worden. Omdat de vraag naar BYOD stijgt en dit een aantal problemen zou kunnen oplossen, heeft SURFsara hiervoor een onderzoek gestart. In het onderzoek worden de toepassingsmogelijkheden bekeken en onderzocht. Het uiteindelijke doel is onderzoeken of BYOD een werkbare oplossing is voor SURFsara.

Het is niet de bedoeling dat BYOD hardware aangesloten wordt op het kantoornetwerk van SURFsara. Nu komt dit wel vaak voor, omdat er geen beleid voor is. Het enige beleid op dit moment is dat externe medewerker geen gebruik mogen maken van Virtual Private Network (VPN) software die normaal voor interne medewerker wel geïnstalleerd wordt. Voor interne medewerkers wordt voorkomen dat besmettingen het netwerk op komen. Externe medewerkers moeten ook op afstand kunnen werken, hierdoor is het gewenst dat zij ook van een VPN oplossing gebruik kunnen maken. Een onderdeel van het onderzoek is hierdoor hoe deze VPN mogelijkheid veilig toegepast kan worden op diverse besturingssystemen van externe medewerkers.

In deze scriptie wordt het bedrijf SURFsara toegelicht, waarbij de werkplek en de rolverdeling beschreven worden. Daarna wordt de aanleiding van het onderzoek bij SURFsara beschreven. Vervolgens wordt de opdracht beschreven met de doelstellingen die behaald moeten worden en de eindproducten. Hierna wordt de aanpak beschreven waarin de hoofd- en deelvragen behandeld worden en de methoden die gebruikt zijn om deze te beantwoorden. De veranderingen in de methoden worden tevens in de aanpak vermeld.

De deelvragen zijn stuk voor stuk uitgewerkt en dienen als basis voor de conclusie. In de conclusie wordt de hoofdvraag beantwoord: “Welke methode is het meest geschikt om het “Bring Your Own Device” principe op een veilige en goed te beheren wijze toe te passen bij SURFsara, zodat de integriteit en de vertrouwelijkheid van SURFsara data en privédata gewaarborgd zijn?”.

2. Context

In dit hoofdstuk wordt de organisatie toegelicht waarvoor er onderzoek gedaan wordt. Tevens worden de rollen toegelicht.

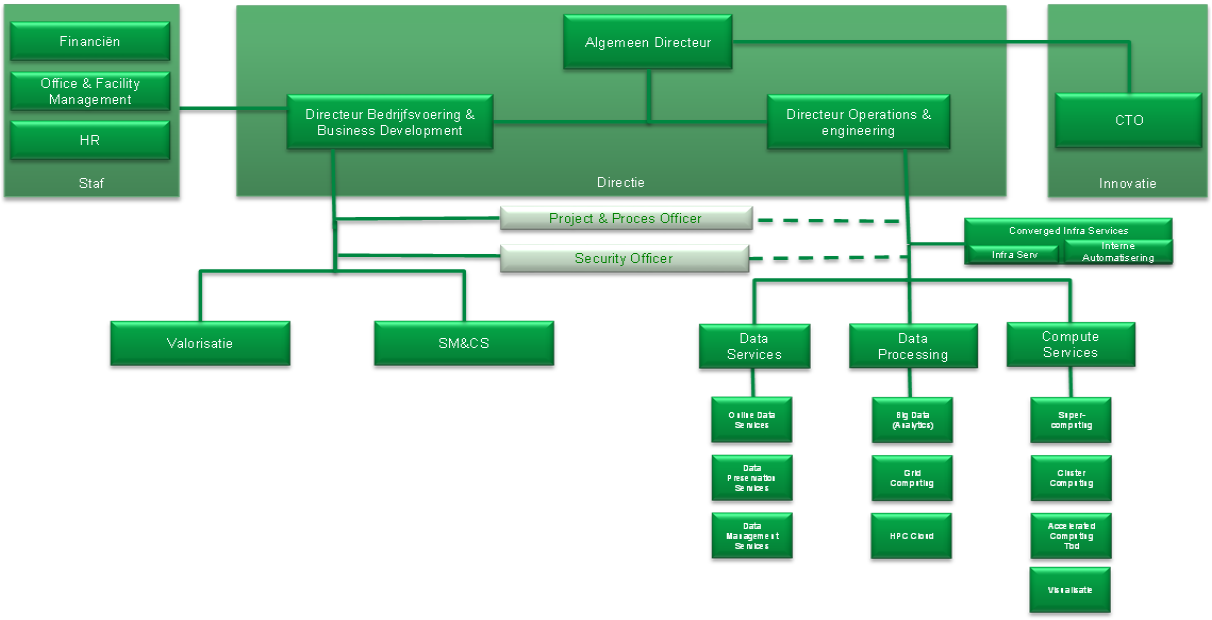
2.1. Organisatie

SURFsara is het nationale high-performance computing en e-science support center. SURFsara werd in 1971 opgericht door de Universiteit van Amsterdam, de Vrije Universiteit Amsterdam en de stichting Mathematisch Centrum. De werkzaamheden van de stichting waren destijds gericht op dataverwerking voor de drie stichters. SARA (Stichting Academisch Rekencentrum Amsterdam) maakt sinds 1 januari 2013 deel uit van de Coöperatie SURF U.A. Sindsdien wordt de naam SURFsara gebruikt. De SURF coöperatie helpt instellingen voor onderwijs en onderzoek bij het vormgeven van veranderingen tijdens ICT-trajecten.

Door de jaren heen is de dienstverlening van SURFsara uitgebreid en wordt van de voorzieningen van SURFsara gebruik gemaakt door andere onderzoeksinstituten en universiteiten. Sindsdien is de dienstverlening niet meer beperkt tot slechts dataverwerking, maar bevat ook rekentijd op supercomputers, dataopslag, visualisatie en netwerken. De rekentijd op supercomputers wordt gefaciliteerd voor wetenschappelijk onderzoek en onderwijs in Nederland. Steeds grotere en complexere modellen worden gebruikt tijdens wetenschappelijk onderzoek, waardoor de behoefte aan rekenkracht blijft toenemen. De rekenkracht wordt onder andere gebruikt voor onderzoeken in de natuurkunde, wiskunde en scheikunde, maar ook voor projecten zoals schone energie, klimaatverandering, watermanagement, geluidshinder en medische behandelingen.

Tegenwoordig biedt SURFsara een compleet pakket aan diensten, expertise en ondersteuning op het gebied van high-performance computing (HPC), data services, visualisatie, e-science support, clouddiensten en networking. SURFsara is gevestigd op het Amsterdam Science Park. (SURFsara, 2016)

SURFsara heeft verschillende afdelingen. Hoe de organisatie opgebouwd is en de samenhang tussen de verschillende afdelingen is te zien in Figuur 1: Organogram SURFsara.



FIGUUR 1: ORGANOGRAM SURFSARA

2.2. Werkplek

De werkplek voor het uitvoeren van de afstudeeropdracht is op de afdeling Interne Automatisering (IA). Deze afdeling is verantwoordelijk voor de kantoorautomatisering (KA) en voor de interne services (diensten ter ondersteuning van de externe dienstverlening). De afdeling bestaat uit zes medewerkers. Het hoofd van deze afdeling heeft de taak van stagebegeleider.

2.3. Rolverdeling

Tijdens het project zijn er rollen toegewezen aan diverse betrokkenen. Deze rollen zijn: een projectmedewerker, een projectmanager en controleurs. De rollen worden in Tabel 1: Rol verdeling toegelicht.

Rol	Beschrijving
Projectmedewerker	De projectmedewerker is de persoon die het onderzoek uitvoert voor het bedrijf SURFsara. De projectmedewerker rapporteert periodiek aan de projectmanager over de voortgang.
Projectmanager / stagebegeleider	De projectmanager, tevens de opdrachtgever en stagebegeleider, begeleidt de projectmedewerker tijdens het uitvoeren van het onderzoek.
Controleur	De controleur bekijkt opgeleverde documenten waarbij er gekeken wordt naar de vastgestelde eisen voor de documentatie.

TABEL 1: ROL VERDELING

Elke rol kent een persoon die verantwoordelijk is voor de invulling van deze rol. In Tabel 2: Rol context zijn de personen beschreven die deze rollen vervullen en wordt de bijbehorende context vermeld.

Rol	Naam	Context
Projectmedewerker	Dion Kruijswijk	Stagiair bij SURFsara en student bij de Hogeschool Utrecht.
Projectmanager / stagebegeleider	Leonieke Mevius	Hoofd van de afdeling Interne Automatisering van SURFsara en tevens de opdrachtgever.
Controleur		
Controleur	Bart Bosma	Docent van de Hogeschool Utrecht en tevens de docentenbegeleider.

TABEL 2: ROL CONTEXT

3. Aanleiding

SURFsara is een organisatie die zowel interne- als externe medewerkers in dienst heeft. Het onderzoek is in eerste instantie gericht op externe medewerkers. De externe medewerkers maken vaak gebruik van eigen hardware (afhankelijk van de periode en intensiteit van hun inzet). Vaak vereisen de werkzaamheden die zij uitvoeren toegang tot de data en/of applicaties binnen de SURFsara organisatie. In 2015 zijn er totaal 21 externe medewerkers ingehuurd. De verwachting is dat het aantal extern ingehuurde medewerkers voor 2016 zal stijgen. Als externe medewerkers een laptop of tablet en een telefoon gebruiken, betekent dit dat zij gemiddeld 42 apparaten per jaar gebruiken waarvoor een veilige oplossing gevonden moet worden.

Omdat de organisatie zelf geen enkele controle heeft over de hardware waarmee externe medewerkers werken, kan niet gegarandeerd worden dat deze machines veilig op het netwerk aangesloten worden. Zo is er onder andere geen controle op de virusscanners, updates en de aanwezigheid van disk-encryptie op deze machines.

Op dit moment wordt er gewerkt met een VPN oplossing voor zowel interne als externe medewerkers. Via het VPN is het gehele netwerk voor iedereen bereikbaar. Het is de bedoeling dat externe medewerkers niet zomaar deze VPN kunnen gebruiken. Het is niet bekend wat er op de eigen hardware geïnstalleerd is en of er virussen via het VPN verspreid kunnen worden.

Gezien het groeiende aantal medewerkers bij SURFsara en het aantal mensen dat met mobiele devices gaat werken, moet er een oplossing gezocht worden voor het veilig toepassing van het BYOD principe. Voor interne medewerkers wordt ook bekeken of het mogelijk is dat zij, in plaats van hardware van SURFsara gebruiken, een budget krijgen zodat zij zelf (niet-standaard) hardware aan kunnen schaffen (Mevius, 2015).

4. De opdracht

In dit hoofdstuk wordt de opdracht: BYOD veilig toepassen behandeld en de doelstellingen vermeld.

4.1. BYOD veilig toepassen

Voor SURFsara wordt onderzocht hoe het BYOD-principe veilig toegepast kan worden. Hierbij wordt voor BYOD beleid opgesteld. Het beleid wordt ondersteund door een toepassing, waarbij rekening gehouden worden met de eisen en wensen van SURFsara. Het beleid en de toepassing zorgen ervoor dat het BYOD principe veilig toegepast kan worden.

4.2. Doelstellingen

In het adviesrapport wordt de hoofdvraag beantwoord, onderbouwd met de deelvragen. Voor het onderzoek zijn de volgende doelstellingen bepaald:

- Verschillende mogelijkheden onderzoeken om BYOD veilig toe te passen,
- Een Proof of Concept uit te voeren,
- Een advies te geven over de mogelijke oplossing(en).

Aan het eind van het onderzoek moet een passend advies gegeven worden over welke toepassing/oplossing het beste ingezet kan worden voor het veilig toepassen van het BYOD principe. Tijdens het onderzoek wordt er rekening gehouden met de volgende eisen:

- De veiligheid binnen het interne netwerk van SURFsara moet gewaarborgd zijn, waarbij de vraag gesteld wordt: “Hoe kan gegarandeerd worden dat geen besmetting van bedrijfsdata plaatsvindt vanuit bijvoorbeeld een geïnfecteerd werkstation?”.
- Bedrijfsdata mag niet in handen vallen van mensen waarvoor deze informatie niet bestemd is in geval van verlies van data, een werkstation of mobiel apparaat.
- Privédata, inclusief eventuele bedrijfsmail van externe bedrijven, van de gebruiker die eigen hardware gebruikt moet beschermd/afgeschermd worden.
- Externe medewerkers moeten gebruik kunnen maken van “Het nieuwe werken” (HNW, remote thuis werken). Dit is voor de interne medewerkers al mogelijk doormiddel van een VPN verbinding vanaf hun, door SURFsara verstrekte, hardware. Externe medewerkers die niet in bezit zijn van SURFsara hardware moeten ook extern kunnen werken zonder in te leveren op het gebied van veiligheid. Daarnaast moeten zij ook via het draadloos netwerk kunnen werken.
- De oplossing(en) moet geschikt zijn voor verschillende besturingssystemen, waaronder Windows, Linux en Mac OS.
- De BYOD oplossing moet beheerd en bijgewerkt kunnen worden.
- Om te kunnen controleren of op de eigen hardware van externe medewerkers onder andere een virusscanner geïnstalleerd is, moet er gemonitord kunnen worden.
- Het BYOD-beleid en -principes dienen te voldoen aan de principes en richtlijnen van het SURFsara informatiebeveiligingsbeleid. Het Informatiebeveiligingsbeleid en de principes van SURFsara zijn opgesteld volgens de ISO standaard voor informatiebeveiliging ISO/IEC 27001:2013. De security maatregelen zijn gebaseerd op Annex A van ISO 27001:2013. Voor de implementatie van de maatregelen wordt gebruikt gemaakt van de norm ISO/IEC 27002:2013. Deze norm beschrijft implementatierichtlijnen voor de security controls.

Aan het eind van het onderzoek zijn deze eisen behandeld.

4.3. Op te leveren producten

Eindproduct	Beschrijving
Adviesrapport	Document waarin advies gegeven wordt over welk(e) product(en) gebruikt zou(den) kunnen worden om het probleem op te lossen en wat er gedaan moet worden om het product toe te kunnen passen.
Scriptie	Document waarin het traject beschreven wordt vanaf het begin van het onderzoek tot aan hoe er aan het eindresultaat gekomen is, waarbij tevens de hoofd- en deelvragen beantwoord worden. Een deel uit het adviesrapport komt hierin voor.
Presentatie SURFsara	Presentatie voor SURFsara waarbij het onderzoek en één of meerdere producten toegelicht worden. Delen uit het adviesrapport komen hierin voor.
Presentatie Hogeschool Utrecht	Presentatie voor de Hogeschool Utrecht, waarbij het onderzoek toegelicht wordt vanaf de aanleiding van het onderzoek tot aan het eindresultaat. Delen van de scriptie komen hierin voor.

TABEL 3: PRODUCTEN

5. Aanpak

In dit hoofdstuk wordt de aanpak beschreven, waarbij de hoofd- en deelvragen behandeld worden. Per deelvraag worden de verwachtte en de gebruikte methoden ten opzichte van het PvA beschreven.

5.1. Hoofd- en deelvragen

De hoofdvraag voor het onderzoek is: “Welke methode is het meest geschikt om het “Bring Your Own Device” principe op een veilige en goed te beheren wijze toe te passen bij SURFsara, zodat de integriteit en de vertrouwelijkheid van SURFsara data en privédata gewaarborgd zijn?”.

Ter ondersteuning en beantwoording van de hoofdvraag zijn de volgende deelvragen opgesteld en worden deze beantwoord in de komende hoofdstukken:

I. Wat houdt het “Bring Your Own Device” principe voor SURFsara in?
II. Wat is het huidige beleid betreffende het “Bring Your Own Device” principe bij SURFsara?
III. Wat moet er veranderd worden aan het huidige beleid om het “Bring Your Own Device” principe toe te kunnen passen bij SURFsara?
IV. Hoe kan voorkomen worden dat door geïnfecteerde “Bring Your Own Device” hardware bedrijfsdata besmet wordt?
V. Hoe kan de bedrijfsgevoelige of privédata van externe werknemers beschermd worden op hun eigen hardware?
VI. Op welke manier kan de “Bring Your Own Device” hardware het best gemonitord worden?

5.2. Verwachtte methoden

Om de deelvragen te beantwoorden worden er methoden gebruikt. In dit hoofdstuk worden per deelvraag de verwachte methoden uit het Plan van Aanpak beschreven.

I. Wat houdt het “Bring Your Own Device” principe voor SURFsara in?

Ter verduidelijking van het onderzoek wordt beschreven wat het BYOD principe precies is. Hiervoor wordt er literatuuronderzoek gedaan, om te onderzoeken wat de definitie en de mogelijkheden van BYOD zijn. Bij de mogelijkheden worden tevens kort de alternatieven voor BYOD vermeld en de afweging hiervoor. De afweging wordt beschreven aan de hand van een interview met de opdrachtgever.

II. Wat is het huidige beleid betreffende het “Bring Your Own Device” principe?

Om het huidige beleid in kaart te brengen worden diverse interviews gehouden. Deze interviews worden met de opdrachtgever, de security officer, externe medewerkers en beheerders gehouden. Aan deze personen wordt gevraagd welke applicaties en data toegankelijk zijn en hoe momenteel het beleid voor BYOD is. De informatie uit de interviews wordt gebruikt ter vergelijking met de gevonden oplossing, waarbij een “AS-IS” analyse (Bridging the Gap, 2015) wordt gedaan. In de AS-IS situatie wordt de huidige situatie beschreven, met het beleid en de manier waarop gewerkt wordt.

III. Wat moet er veranderd worden aan het huidige beleid om het “Bring Your Own Device” principe toe te kunnen passen bij SURFsara?

De veranderingen die plaats moeten vinden om het BYOD principe toe te kunnen passen, worden beschreven aan de hand van de “TO-BE” analyse (Bridging the Gap, 2015). In de TO-BE situatie wordt de gewenste situatie beschreven, waarvoor de eisen en wensen in kaart gebracht worden. Hierin wordt het nieuwe beleid beschreven die conform de ISO27001 standaard is. De transitie van AS-IS naar TO-BE wordt ook beschreven, met eventuele aanpassingen die benodigd zijn om naar de gewenste situatie over te gaan. Voor de beantwoording van deze deelvraag wordt een enquête opgesteld en worden er interviews gehouden waarbij prioriteiten worden gegeven aan gewenste functies. Deze interviews en enquêtes worden gehouden met de opdrachtgever, de security officer en daarnaast een netwerkbeheerder om informatie te vergaren. Alle informatie wordt verwerkt in een Analyse van Eisen en kan vervolgens gebruikt worden als onderdeel van de KPMG pakketselectie (KPMG, 2010). Onderdelen van de KPMG pakketselectie worden in een toepassingsselectie gebruikt, waarbij als eerste een longlist gemaakt wordt waarin een aantal mogelijke oplossingen bekeken wordt. Aan de hand van de eisen en wensen wordt vervolgens van de longlist een shortlist gemaakt met minimaal drie en maximaal vijf producten die voldoen. De producten in de shortlist worden getest in een Proof of Concept (Techopedia, 2016). In de Proof of Concept wordt er in een testomgeving bekeken of de producten voldoen aan de eisen, wensen en doelstellingen van SURFsara.

IV. *Hoe kan voorkomen worden dat door geïnfecteerde “Bring Your Own Device” hardware bedrijfsdata besmet wordt?*

Om te kunnen garanderen dat virussen, malware of andere besmettingen geen bedrijfsdata besmetten, wordt door middel van deskresearch gezocht naar manieren om BYOD veilig toe te passen. Deskresearch omvat het zoeken naar relevante soft- en hardware hiervoor en het bekijken van Best Practices. Hierbij wordt er rekening gehouden met de ISO27001 certificering die SURFsara wil behalen. In het Proof of Concept wordt bekeken wat voor impact er op de hardware en het netwerkverkeer is wanneer een toepassing gebruikt wordt.

V. *Hoe kan de bedrijfsgevoelige of privédata van externe werknemers beschermd worden op hun eigen hardware?*

Om bedrijfsgevoelige data en/of privédata te beschermen, wordt gezocht welke regelingen omtrent bescherming van de gegevens van toepassing zijn. Hierbij wordt deskresearch gedaan waarbij bekeken wordt hoe de data beschermd kan worden. Er wordt tevens onderzocht wat gedaan kan worden om te voorkomen dat bedrijfsdata in handen valt van personen waarvoor deze informatie niet bestemd is, in geval van verlies of diefstal. Daarnaast wordt onderzocht wat gedaan kan worden indien dit al gebeurd is. Hiervoor wordt deskresearch gedaan en een referentieonderzoek waarbij gekeken wordt hoe andere bedrijven hier mee omgaan. In het Proof of Concept wordt bekeken wat gedaan kan worden in deze situatie.

VI. *Op welke manier kan de “Bring Your Own Device” hardware het best gemonitord worden?*

Om te zorgen dat geïnfecteerde hardware niet zomaar het netwerk van SURFsara opkomt, wordt onderzocht hoe de BYOD hardware beheerd en gemonitord kan worden. Hiervoor wordt deskresearch gedaan waarbij tevens Best Practices bekeken worden. Daarnaast worden er interviews gehouden met de opdrachtgever en beheerders, zodat het bekend is wat gewenst is om te kunnen monitoren en te beheren. Hierbij wordt rekening gehouden met de wetgeving en wordt er advies

gegeven over hoe dit het beste aangepakt kan worden wanneer iemand BYOD hardware wil gebruiken. Welke monitoring- en beheer mogelijkheden er zijn worden tijdens de Proof of Concept bekeken.

Interviews die vermeld zijn als methode voor de beantwoording van de deelvragen worden uitgewerkt in een interviewverslag. In een interviewverslag staat wie geïnterviewd wordt, wanneer het interview gehouden is, de vragen en de antwoorden op de vragen. De interviewverslagen worden na afloop van het interviews gemaild naar de betrokkenen, zodat de informatie gecontroleerd wordt. Hierna worden de interviewverslagen eventueel aan de opdrachtgever aangeboden, zodat de informatie geverifieerd kan worden.

5.3. Gebruikte methoden

Tijdens het onderzoek is één van de methoden om deelvraag V: "*Op welke manier kan de "Bring Your Own Device" hardware het best gemonitord worden?"* te beantwoorden, aangepast. In plaats van een interview is er gekozen voor een enquête. Bij een enquête zijn de antwoorden bijna altijd objectief. Bij een interview is het risico aanwezig dat er indien er wordt doorgevraagd dat de antwoorden niet objectief zijn.

De enquête is naar de afdeling IA gestuurd, omdat zij de BYOD oplossing gaan beheren en monitoren als deze geïmplementeerd wordt. De enquête is opgesteld om te bepalen welke functies gewenst zijn. Omdat bij monitoring de meest gewenste functies het belangrijkste zijn, is er gekozen om de gebruikte methode voor deze deelvraag te veranderen.

In Tabel 4: Deelvraagmethoden worden de verwachte en gebruikte methoden per deelvraag nogmaals opgesomd.

Deelvraag	Verwachtte Methoden	Gebruikte methoden
Wat houdt het "Bring Your Own Device" principe voor SURFsara in?	Literatuur onderzoek, interviews	Literatuur onderzoek, interviews
Wat is het huidige beleid betreffende het "Bring Your Own Device" principe?	Interviews	Interviews
Wat moet er veranderd worden aan het huidige beleid om het "Bring Your Own Device" principe toe te kunnen passen bij SURFsara?	Enquête, interviews, toepassingsselectie	Enquête, Interviews, toepassingsselectie
Hoe kan voorkomen worden dat door geïnfecteerde "Bring Your Own Device" hardware bedrijfsdata besmet wordt?	Deskresearch, Proof of Concept	Deskresearch, Proof of Concept
Hoe kan de bedrijfsgevoelige of privédata van externe werknemers beschermd worden op hun eigen hardware?	Deskresearch, referentie onderzoek, Proof of Concept	Deskresearch, referentie onderzoek, Proof of Concept
Op welke manier kan de "Bring Your Own Device" hardware het best gemonitord worden?	Deskresearch, interviews, Proof of Concept	Deskresearch, enquête, Proof of Concept

TABEL 4: DEELVRAAGMETHODEN

6. Wat is Bring Your Own Device

Voor het onderzoek naar het veilig toepassen van het BYOD principe, is de eerste deelvraag “Wat houdt het “Bring Your Own Device” principe voor SURFsara in?”. Deze deelvraag wordt beantwoord door het perspectief van SURFsara te beschrijven. Hiervoor wordt de algemene definitie van BYOD beschreven en wordt er beschreven wat SURFsara moet aanpassen om BYOD mogelijk te maken.

SURFsara heeft aangegeven dat het gewenst is om te kijken naar mogelijkheden van het gebruik van hardware door externe medewerkers. De volgende mogelijkheden zijn onderzocht waarbij een passend beleid voor hardware toegepast wordt: “Bring Your Own Device”, “On Your Own Device”, “Choose Your Own Device” en “Here Is Your Own Device” (Stedehouder, 2012). Bij deze mogelijkheden wordt de mate van vrijheid en controle vergeleken.

- Bring Your Own Device (BYOD)

BYOD is een beleid waarbij verschillende partijen, zoals medewerkers, zakelijke partners en eventuele andere gebruikers, eigen hardware uitzoeken en gebruiken voor toegang tot bedrijfsapplicaties en data (Gartner, 2015). Hierin is de werknemer of partij vrij in de keuze van hardware, maar moet zij zich wel aan vastgestelde afspraken en eventueel gebruikte applicaties houden.

- On Your Own Device (OYOD)

OYOD houdt in dat er gewerkt wordt op eigen hardware. Bij OYOD kan er weinig controle plaatsvinden, doordat de hardware van de medewerker zelf is en hij/zij zelf bepaalt wat er geïnstalleerd wordt. Er wordt geen beleid toegepast bij OYOD. Echter kunnen medewerkers zelf bepalen welke hardware zij willen, waardoor er een hoge mate van vrijheid is. (Stedehouder, 2012)

- Choose Your Own Device (CYOD)

Bij CYOD kan er door de werknemer gekozen worden uit een beperkt aantal apparaten. Op deze apparaten zit support vanuit het bedrijf. Dit zorgt voor een redelijk hoge mate van controle, echter zijn de medewerkers niet geheel vrij in de keuze doordat zij uit beperkte hardware kunnen kiezen. (Stedehouder, 2012)

- Here Is Your Own Device (HIYOD)

HIYOD betekent dat medewerkers hardware krijgen waarbij er geen keuze is. Daarnaast kunnen medewerkers zelf geen software installeren. Dit zorgt voor een hoge mate van controle, doordat de hardware beheerd wordt door het bedrijf. Doordat er geen keuze in hard- en software is, is de mate van vrijheid erg laag. (Stedehouder, 2012)

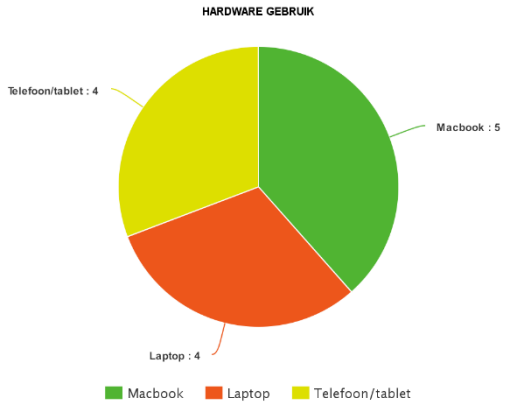
De verschillende mogelijkheden zijn in Figuur 2: Controle Own Device weergegeven waarbij de mate van controle weergegeven wordt en in Figuur 3: Vrijheid Own Device de mate van vrijheid. De afbeeldingen geven weer hoeveel controle en vrijheid er mogelijk is per mogelijkheid van “Your Own Device”.

FIGUUR 2: CONTROLE OWN DEVICE

FIGUUR 3: VRIJHEID OWN DEVICE

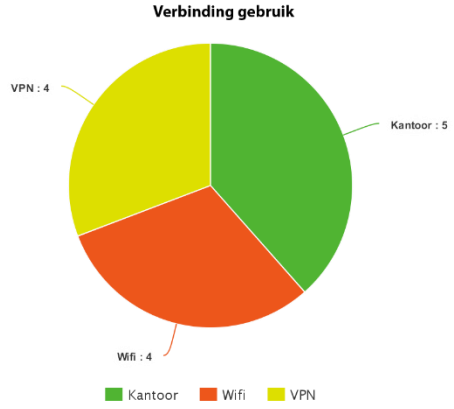
SURFsara heeft aangegeven BYOD toe te willen passen. Voor SURFsara betekent BYOD dat externe medewerkers hun eigen hardware en software meenemen. Deze hard- en software is geen eigendom van SURFsara en wordt daardoor niet beheerd door de organisatie. Onder externe hardware vallen alle telefoons, tablets, laptops en eventuele overige hardware waarop voor SURFsara gewerkt wordt. Omdat niet bekend is welke hardware en software precies gebruikt wordt, moet een beleid opgesteld worden voor het gebruik van BYOD hardware. Om BYOD toe te staan moet er onderzoek gedaan worden naar welke beleidsaanpassingen bij SURFsara gemaakt moeten worden. In het nieuwe beleid moet onder andere de aansprakelijkheid, de aanbevolen software en eventuele beperkingen beschreven worden. Het beleid moet ondersteund worden met een technische oplossing om te voorkomen dat besmettingen van onder andere bedrijfsdata plaats kunnen vinden.

Onder de externe medewerkers is een enquête verspreid om te kijken op welke manier zij op dit moment diensten gebruiken. De enquête is door acht externe medewerkers ingevuld, zie Bijlage 4: Enquêtes. Uit de enquête blijkt dat medewerkers in bepaalde gevallen meerdere apparaten gebruiken om op te werken. Zo worden er Windows laptops, Macbooks en telefoon of tablets gebruikt. Het gebruik van hardware is weergegeven in Figuur 4: Gebruik hardware.



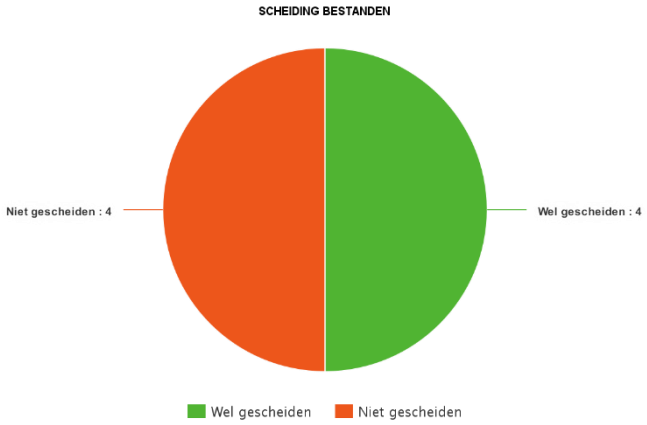
FIGUUR 4: GEBRUIK HARDWARE

Het verbinden met de BYOD hardware gebeurt tevens op verschillende manieren. Een aantal externe medewerkers maakt verbinding met het bedrade kantoornetwerk, anderen gebruiken Wi-Fi of VPN. Het gebruik van de verbindingen is weergegeven in Figuur 5: Verbinding gebruik.



FIGUUR 5: VERBINDING GEBRUIK

In de enquête is gevraagd of de gebruikers SURFsara data en privédata kunnen scheiden, hierbij is er aangegeven of dit wel of niet lukt. Dit is weergegeven in Figuur 6: Scheiding bestanden.



FIGUUR 6: SCHEIDING BESTANDEN

Met de gegevens uit de enquête moet rekening gehouden worden als er een BYOD oplossing toegepast gaat worden. De oplossing moet namelijk gebruiksvriendelijk zijn voor de externe medewerkers.

7. Huidig beleid

Voor SURFsara wordt het huidige beleid in kaart gebracht, zodat er een uitgangspunt is voor de transitie naar de gewenste situatie. Hiervoor wordt de tweede deelvraag "*Wat is het huidige beleid betreffende het "Bring Your Own Device" principe bij SURFsara?*" beantwoord.

Een deel van het "Choose Your Own Device" principe wordt momenteel (AS-IS) bij SURFsara toegepast, waarbij interne medewerkers uit een beperkt aantal laptops of desktops kunnen kiezen. Voor CYOD is er een beperkt beleid opgesteld met regels waar medewerkers zich aan moeten houden, de Acceptable Use Policy (AUP). In deze AUP (SURFsara, 2015) staat onder andere beschreven wat er wel en niet gedaan mag worden op de hardware. Bij het CYOD principe kan er gekozen worden uit een beperkt aantal laptops, waarmee medewerkers ook thuis kunnen werken. Bij het kiezen van een laptop moet er gekozen worden wat voor besturingssysteem geïnstalleerd wordt. In geval van een Windows laptop wordt deze deels beheerd door de tool CFEngine. CFEngine is een configuratiemanagement en automatiseringsframework waarmee de IT infrastructuur beheerd kan worden (CFEngine, 2016). Door het gebruik van deze tool, worden instellingen en applicaties regelmatig automatisch gecontroleerd, geconfigureerd en geïnstalleerd. Het is momenteel echter ook mogelijk om zelf applicaties te installeren op de hardware, doordat gebruikers administratorrechten hebben. De mate van controle is hierdoor niet optimaal en er wordt overwogen om gebruikers geen administratorrechten meer te geven. Hardware met Mac OS en Linux worden nog niet beheerd. Voor zowel Mac (SURFsara, 2016) als Linux (SURFsara, 2015) systemen zijn de volgende richtlijnen voor het gebruik opgesteld:

- Gebruik van disk encryptie.
- Gebruik van een virusscanner.
- Inloggen met een wachtwoord.
- Na tien minuten inactiviteit automatisch de screensaver met wachtwoordbeveiliging inschakelen.

Deze richtlijnen zijn bedoeld voor de CYOD hardware.

Het is de bedoeling dat BYOD hardware niet zomaar toegelaten wordt tot het netwerk van SURFsara. BYOD hardware kan verbinding maken met drie Wi-Fi netwerken. De drie Wi-Fi netwerken zijn het SURFsara gastenlan Wi-Fi netwerk, het Amsterdam Science Park Wi-Fi en het Eduroam Wi-Fi netwerk. Alle drie de netwerken zijn bruikbaar voor bezoekers. Eduroam is een veilig draadloos netwerk dat gebruikt wordt door medewerkers en studenten van onderwijs- of onderzoeksinstellingen. Indien leveranciers toegelaten moeten worden tot het netwerk van de supercomputer, wordt hiervoor een oplossing bedacht. Deze oplossing is meestal het opzetten van een nieuw netwerksegment of VLAN. In het aparte netwerksegment gelden strikte en beperkte toegangsregels. In alle andere gevallen is het alleen toegestaan dat BYOD hardware gekoppeld wordt met de Wi-Fi netwerken en niet met het kantoornetwerk.

Indien bestanden of applicaties toegankelijk moeten zijn via het Wi-Fi netwerk, kan een VPN opgezet worden. Zowel interne als een aantal externe medewerkers maken gebruik van een VPN-verbinding via de Wi-Fi netwerken om te verbinden met een netwerk van SURFsara. Via de VPN verbinding is het ook mogelijk om op afstand te werken.

Momenteel worden er geen controles uitgevoerd op BYOD hardware, waardoor het niet bekend is wanneer hardware besmet is met malware. Indien de hardware besmet is, kan vervolgens bedrijfsdata van SURFsara besmet worden. Het is gewenst dat hier verandering in komt, zodat risico's beperkt worden.

8. Gewenst beleid

Nadat het huidige beleid beschreven is, wordt de derde deelvraag "*Wat moet er veranderd worden aan het huidige beleid om het "Bring Your Own Device" principe toe te kunnen passen bij SURFsara?*" beantwoord. Hiervoor wordt eerst het gewenste beleid beschreven en daarna de transitie naar het gewenste beleid.

Het is de bedoeling dat het BYOD principe naast het CYOD principe toegepast wordt. Delen van de AS-IS situatie worden hergebruikt voor het gewenste beleid, zoals het gebruik van CFEngine. Het BYOD principe is voornamelijk van toepassing op externe medewerkers. Vanwege de vraag naar BYOD door interne medewerkers, wordt het mogelijk dat zij kunnen kiezen tussen CYOD of BYOD. Bij het kiezen van CYOD verandert er ten opzichte van het huidige beleid niets, er kan dan gekozen worden uit hardware die SURFsara aanbiedt.

Indien BYOD toegepast wordt, kan er gekozen worden om een budget vast te stellen per medewerker waardoor deze de mogelijkheid krijgt om zelf hardware aan te schaffen. Indien medewerkers zelf al hardware hebben, kunnen zij die hardware gebruiken. Deze hardware moet veilig toegelaten worden tot het netwerk van SURFsara, zodat er vanaf de BYOD hardware gewerkt kan worden. Externe medewerkers maken altijd gebruik van BYOD hardware, waarbij zij zelf of de ingehuurde bedrijven hardware aangeschaft hebben.

Het is gewenst dat er een BYOD beleid wordt geschreven dat toepasbaar is op zowel de interne als de externe medewerkers. In het beleid zijn regels opgenomen waaraan voldaan moet worden bij het gebruik van BYOD hardware. Bij het BYOD principe zijn er een aantal beleidsregels van toepassing:

- Welke toegangsmanieren mogen gebruikers gebruiken om toegang te krijgen tot SURFsara data?

Slechts bepaalde toegangsmanieren mogen gebruikt worden op BYOD hardware. Deze manieren worden in het beleid opgenomen, zodat bekend is wat wel en niet toegestaan is. In het geval van SURFsara is het de bedoeling dat BYOD hardware slechts via het VPN verbonden kan worden met het netwerk van SURFsara. Dan pas kan er verbonden worden met een virtuele omgeving en worden data en applicaties beschikbaar.

- Wat moet de gebruiker doen om te voorkomen dat de veiligheid van SURFsara data en privédata in gevaar komt?

In het beleid wordt opgenomen wat de gebruiker wel en niet mag doen op de hardware, zodat de kans op besmetting minimaal is. Hiervoor moeten regels en richtlijnen opgesteld worden waar gebruikers zich aan moeten houden.

- Wie is er verantwoordelijk voor de BYOD apparatuur en in welke gevallen?

In bepaalde situaties moeten de verantwoordelijkheden duidelijk zijn, zoals in situaties waarin hardware gestolen of besmet is. In het beleid moet opgenomen worden wanneer het bedrijf of de werknemer verantwoordelijk is.

- Waar kunnen BYOD gebruikers terecht indien zij problemen of vragen hebben met of over de BYOD hardware?

Voor het gebruik van BYOD moet er ook support gegeven worden, zodat als medewerkers problemen hebben zij vragen kunnen stellen. Hiervoor moet er bekeken worden wat precies het probleem is, als het probleem bijvoorbeeld bij de hardware zelf ligt kan SURFsara geen support geven. In het beleid moet aangegeven worden welke specifieke applicaties en VPN toegangsmogelijkheden ondersteund worden, zodat het voor iedereen duidelijk is wat wel en niet aangeraden wordt.

Indien medewerkers BYOD hardware willen gebruiken, moeten zij akkoord gaan met het opgestelde beleid voor het gebruik van BYOD hardware. Mochten medewerkers het beleid niet willen ondertekenen, kan er gekozen worden om deze medewerkers geen toegang met BYOD hardware te verlenen of er wordt een andere medewerker ingehuurd.

In het beleid moet opgenomen worden op welke manier het mogelijk is om lokale bestanden op de BYOD hardware te wissen indien de hardware gestolen wordt. Om dit beleid passend te maken op een technische oplossing, is er een toepassingsselectie gedaan. In de toepassingsselectie is bekeken welke producten een oplossingen kunnen bieden. Hiervoor zijn diverse eisen en wensen geïnventariseerd in de Analyse van Eisen. Een aantal producten die geschikt lijken zijn in een Proof of Concept getest. Ten behoeve van het opstellen van het BYOD-beleid en de implementatie ervan is rekening gehouden met de relevante controls uit Annex A van de ISO27001 norm en de ISO27002:2013 standaard. Een aantal van deze controls zijn (NEN, 2013):

- Reviewen van het beleid om ontwikkelingen en significante veranderingen te beoordelen (ISO27001 Annex A.5.1.2 Review of the policies for information security.)
- Beleid voor het werken met mobiele apparatuur en telewerken. Het in kaart brengen van risico's van het gebruik van BYOD inclusief audits en monitoring om te controleren of de oplossing nog voldoet, waarin opgenomen is hoe vaak en hoe de audits plaatsvinden (ISO27001 Annex A.6.2.1 Mobile devices and teleworking)
- Het beleid integreren in de processen van het bedrijf. (ISO27001 Annex A.12.1.2 Change management)
- Wat er gemonitord wordt en op welke manier. (ISO27001 Annex A.12.4.1 Event logging)

8.1. Technische ondersteuning

Wanneer de ISO27001 controls verwerkt zijn in het beleid, kan het BYOD principe toegepast worden door één van de oplossingen te gebruiken uit de toepassingsselectie ter ondersteuning van het beleid. In de toepassingsselectie zijn drie verschillende toepassingen bekeken, namelijk:

- Gebruik van Virtual Desktop Infrastructure (VDI) software

VDI is het draaien van desktop omgevingen als virtuele machines (VM's) op een virtuele omgeving. Hierbij wordt een gecontroleerde omgeving gecreëerd waarbij gebruikers toch alle mogelijkheden kunnen hebben van een normale desktop (Gartner, 2015).

- Gebruik van Network Access Control (NAC) software

NAC is het toepassen van beleidsregels in het netwerk voor de toegangscontrole van hardware en gebruikers (Gartner, 2015).

- Implementatie van SSL VPN

Een SSL VPN is een versleutelde VPN waarbij netwerk verkeer veilig getransporteerd wordt tussen twee locaties (TechTarget, 2015).

Voor de toepassingen zijn er producten gevonden. Deze producten zijn in een tabel gezet samen met de eisen en wensen. In deze toepassingsselectie hebben de eisen en wensen een waarde gekregen door interviews te houden met de opdrachtgever en de security officer (Interviewverslag BYOD eisen en wensen Sedat Capkin, Interviewverslag BYOD eisen en wensen Leonieke Mevius). Tijdens de interviews is bepaald dat een wens een optionele functie is die minder belangrijk is dan een eis. De toepassingsselectie is toegevoegd in Bijlage 2: Toepassingsselectie. In de interviews zijn de volgende eisen bepaald:

- Open Source
- Ondersteuning verschillende besturingssystemen (o.a. Windows, Linux en Mac OS)
- Eenvoudig in gebruik (snel en duidelijk toegang voor eindgebruikers)
- Passend binnen de beheeromgeving (gebruik maken van de huidige server OS-en en virtualisatie platformen)
- Bedrijfsdata niet lokaal op externe hardware
- Besmettingsgevaar minimaliseren / virusscanners
- Back-up van data
- Netwerkbeveiliging (toegang beveiligd)
- Continuïteit (geen hinder in gebruik)

Er was maar één wens voor het gewenste beleid; er mogen offline mogelijkheden zijn zodat medewerkers overal kunnen werken. De producten, eisen en de wens zijn in een longlist verwerkt, dit is te zien in Tabel 5: Longlist. In de tabel zijn aan de linkerkant de producten opgesomd die vergeleken worden. Bovenin zijn de eisen en wensen geplaatst om per product te bekijken of er voldaan wordt aan de eis of niet. Een V in de tabel betekent dat het product voldoet aan de eis of wens.

Product	Offline mogelijkheden	Open Source	Ondersteuning besturingssystemen	Eenvoudig in gebruik	Passend binnen de beheer omgeving	Bedrijfsdata niet lokaal	Besmettingsgevaar minimaliseren	Back-up van data	Netwerkbeveiliging	Waarborging continuïteit
Ulteo Open Virtual Desktop		V	V	V	V	V	V	V	V	V
Dell vWorkspace	V		V	V	V	V	V	V	V	V
VMWare Horizon View + Flex	V*		V	V		V	V	V	V	V
Citrix Workspace Suite			V	V		V	V	V	V	V
OpenVPN python intergratie	V	V	V	V	V		V		V	V
Juniper firewall VPN instellingen	V		V	V			V		V	V
Cisco ASA VPN instellingen	V		V	V			V		V	V
Packetfence	V	V	V	V	V		V		V	
OpenNAC	V	V	V	V	V		V		V	
Cortado Corparate Server	V		V	V	V		V		V	
ForeScout CounterACT	V		V	V			V		V	

TABEL 5: LONGLIST

In de tabel heeft VMware bij Offline mogelijkheden een V*. Het is namelijk vereist dat indien bij VMWare Horizon gebruik gemaakt wordt van offline mogelijkheden, een tweede pakket geïnstalleerd moet worden. VMWare Horizon View zorgt dat de VM omgeving op afstand beschikbaar is. Met VMWare Horizon Flex is het mogelijk om een VM offline beschikbaar te maken waarvan op elk moment wanneer er internet verbinding een back-up gemaakt kan worden naar de Horizon View server. VMWare voldoet zodoende niet als slechts Horizon View gebruikt wordt. VMWare wijkt hiermee als enige af van de andere oplossingen.

Uit de tabel valt op te maken dat er twee producten bijna volledig voldoen. Bij de twee producten wordt slechts op één wens of eis niet voldaan. Andere producten voldoen minder goed, waardoor Ulteo Open Virtual Desktop en Dell vWorkspace in de shortlist opgenomen worden.

De opdrachtgever heeft echter aangegeven dat een NAC product in de vergelijking meegenomen moet worden om te bekijken of dit als alternatief ingezet kan worden. Het NAC pakket is gekozen door gebruik te maken van een onafhankelijke bron, IJcaonline. IJcaonline onderzoekt en schrijft reviews over diverse producten, waaronder informatiesystemen, software en embedded systemen. De reviews worden door diverse personen bekeken, waardoor zij objectief blijven. Dit bedrijf heeft een vergelijking gemaakt tussen drie producten, waarvan twee in de longlist opgenomen zijn. De drie producten zijn OpenNAC, Packetfence en FreeNAC. PacketFence scoort in hun vergelijking (IJcaonline, 2014) iets beter, waardoor PacketFence opgenomen wordt in de shortlist. Hierdoor worden er uiteindelijk drie producten in de shortlist opgenomen.

Product	Offline mogelijkheden (2)	Open Source (3)	Ondersteuning besturingssystemen (4)	Eenvoudig in gebruik (4)	Passend binnen de beheer omgeving (4)	Bedrijfsdata niet lokaal (5)	Besmettingsgevaar minimaliseren (5)	Back-up van data (5)	Netwerkbeveiliging (5)	Waarborging continuïteit (5)
Ulteo Open Virtual Desktop	0	2	2	2	2	2	2	2	2	2
Dell vWorkspace	2	0	2	2	2	2/0*	2	2/0**	2	2
PacketFence	2	2	2	2	2	0	2	0	2	1

TABEL 6: SHORTLIST

In de Tabel 6: Shortlist zijn getallen opgenomen. Als eerste zijn de eisen opgenomen waaraan een weging is toegekend. Deze eisen en wensen zijn boven verticaal weergegeven. Vervolgens zijn de waardes toegekend aan de eisen per product met een waarde van nul, één of twee. Nul betekent voldoet niet, één deels en twee volledig. * in de tabel betekent dat indien er gebruik gemaakt wordt van offline mogelijkheden, staat de bedrijfsdata lokaal, waardoor het product niet voldoet. ** in de tabel betekent dat indien er gebruik gemaakt wordt van offline mogelijkheden, er geen back-up gemaakt wordt. Om te bepalen hoe goed elk product voldoet, worden de waardes vermenigvuldigd met de weging van de eisen en wensen.

Product	Offline mogelijkheden (2)	Open Source (3)	Ondersteuning besturingssystemen (4)	Eenvoudig in gebruik (4)	Passend binnen de beheer omgeving (4)	Bedrijfsdata niet lokaal (5)	Besmettingsgevaar minimaliseren (5)	Back-up van data (5)	Netwerkbeveiliging (5)	Waarborging continuïteit (5)	Totaal
Ulteo Open Virtual Desktop	0	6	8	8	8	10	10	10	10	10	80
Dell vWorkspace	4	0	8	8	8	10/0	10	10/0	10	10	78/58
Packetfence	4	6	8	8	8	0	10	0	10	5	59

TABEL 7: SHORTLIST VERMENIGVULDIGD

In Tabel 7: Shortlist vermenigvuldigd wijkt Dell vWorkspace af met de waardes 10/0. Indien er geen offline mogelijkheden gebruikt worden is de waarde 10 van toepassing op de eis 'Bedrijfsdata niet lokaal' en 'Back-up van data'. Echter, als er wel offline mogelijkheden gebruikt worden, wordt de waarde 0, omdat het product dan niet voldoet. Hierdoor heeft de totaalscore ook twee waardes.

Om de gewenste situatie mogelijk te maken moet de gekozen oplossing aansluiten op het beleid. De technische oplossing dwingt gebruikers om gebruik te maken van de richtlijnen in het beleid. Uit de tabel valt op te maken dat Ulteo Open Virtual Desktop in principe het beste voldoet.

Om de gewenste situatie mogelijk te maken, moet er een transitie plaatsvinden van het huidige naar het gewenste beleid. Tijdens deze transitie worden de richtlijnen en de controls van de ISO norm aangepast en verder gedefinieerd. De medewerkers waarvoor het beleid bedoeld is worden ingelicht over de aanpassingen die plaats gaan vinden. Er wordt vermeld wanneer er volledig overgegaan wordt naar de nieuwe omgeving. De omgeving wordt ingericht met de applicaties die de medewerkers gebruiken. Voor niet standaard applicaties wordt per gebruikers overlegd welke applicaties benodigd zijn en of deze geïnstalleerd worden. Hierna kan het gewenste beleid in werking treden.

9. Besmetting voorkomen

Wanneer het BYOD principe ingevoerd wordt, moet bedrijfsdata beschermd worden tegen besmettingen. Hiervoor wordt de vierde deelvraag beantwoord: *"Hoe kan voorkomen worden dat door geïnfecteerde "Bring Your Own Device" hardware bedrijfsdata besmet wordt?".*

Het is gewenst dat bedrijfsdata niet besmet wordt. Om dit mogelijk te maken kunnen best-practices ((Faronics, 2014), (Sophos, 2015)) gebruikt worden om besmettingen te verminderen of helemaal te voorkomen. De volgende preventieve maatregelingen zijn mogelijk:

- Medewerkers bewust maken van malware

Om te voorkomen dat medewerkers malware op hun hardware krijgen, is het noodzakelijk dat medewerkers zich bewust worden van de schade die malware kan aanrichten. Ter bewustwording kunnen er tips en trainingen worden gegeven waarin onderwerpen zoals downloaden van bestanden, spammails herkennen en internetgedrag/het gebruik van internet aan bod komen. Wanneer deze tips en trainingen gegeven worden, wordt de kans kleiner dat medewerkers malware binnenhalen. Eventueel kunnen er audits plaatsvinden om te toetsen of medewerkers zich aan de tips houden.

- Virusscanners

Omdat het niet helemaal voorkomen kan worden dat medewerkers, ondanks tips en trainingen, virussen binnen krijgen zijn virusscanners noodzakelijk om de kans op besmettingen nog kleiner te maken. Er moet een virusscanner op de BYOD hardware geïnstalleerd zijn, zodat indien er een virus gedownload wordt, dit tegengehouden kan worden. De keuze hiervoor is aan de gebruiker. Het is mogelijk om een 'leaders' virusscanner uit de Magic Quadrant van Gartner te gebruiken (Gartner, 2016). Deze 'leaders' virusscanners zijn gebalanceerd en vooruitstrevend, waardoor deze de meeste kans hebben om besmettingen te verkleinen. Daarnaast is er de mogelijkheid om virusscanners te integreren met de uiteindelijk gekozen oplossing. Indien de virusscanner ook een browser-plugin heeft, kan tevens hiermee de toegang tot onveilige websites voorkomen worden. Het voorkomen van besmettingen met virusscanners is niet altijd mogelijk, maar de kans op besmetting kan wel verkleind worden. Daarnaast moeten er op de servers waar bestanden op staan ook virusscanners geïnstalleerd worden. Indien er verschillende virusscanners gebruikt worden, is de kans op besmetting kleiner.

- Mail filteren

Veel virussen worden per mail verstuurd. In de bijlage is dan een besmet bestand toegevoegd en wanneer dit uitgevoerd wordt kan het schadelijk zijn. Veel van deze mails worden bijgehouden in databases van Anti-spam producten. Door het gebruik van anti-spam producten wordt de kans op besmetting kleiner. Met Anti-spam producten is het nog steeds mogelijk dat een virus niet gefilterd wordt vanwege hetzelfde probleem als bij virusscanners; er is nog geen update waarin het bestand daadwerkelijk als spam/virus gezien wordt. Er moet namelijk eerst informatie vergaard worden van de spam mail of het virus, waarbij er een handtekening gegenereerd wordt (Computable, 2004). Deze handtekening is benodigd om herkenpatronen in de database van zowel anti-spam als antivirussoftware te plaatsen. Hierdoor kan het enige tijd duren voordat de patronen herkend

worden. Er moeten zodoende meer maatregelen genomen worden om de kans op besmetting te verkleinen. Indien de spam filters nog strakker afgesteld worden, wordt de kans nog kleiner op besmetting. Er wordt namelijk meer geblokkeerd door de tools die het anti-spam filter gebruiken, door bijvoorbeeld een blacklist. Een blacklist wordt toegepast in een anti-spam product om bekende bronnen te blokkeren die vaak spam versturen. Zowel het spam filter als het gebruik maken van blacklists kunnen er voor zorgen dat er veel geblokkeerd wordt. In sommige gevallen kan dit ongewenst zijn.

- Opslag mediamogelijkheden beperken

Opslagmedia zoals USB-sticks en CD's vormen één van de manieren waarop besmettingen verspreid worden. Indien alleen de door KA geleverde USB sticks toegestaan worden, wordt de kans op een (on)bewuste besmetting kleiner.

- Advertenties blokkeren

Het is bekend dat zelfs advertenties op websites tot besmetting kunnen leiden (AD, 2016). Indien advertenties geblokkeerd worden in de browser, wordt de kans kleiner dat er een besmetting plaatsvindt via internet.

In de Proof of Concept zijn er twee extra mogelijkheden naar voren gekomen om de kans op een besmetting te verkleinen. Bij het gebruik van PacketFence kan de toegang tot het netwerk geblokkeerd worden. Bij gebruik van Ulteo Open Virtual Desktop of Dell vWorkspace is het mogelijk om in een afgeschermde externe omgeving te werken.

- Blokkeren van de toegang tot het netwerk

Indien nodig kan hardware geblokkeerd worden zodat deze geen toegang heeft tot het netwerk. Er zijn programma's waarbij er beleidsregels ingesteld kunnen worden waardoor onder andere gecontroleerd kan worden of de firewall op de hardware aan staat of dat de hardware gescand wordt op virussen voordat er verbinding gemaakt wordt. Wanneer er niet voldaan wordt aan deze beleidsregels, als de firewall staat uit staat of er een virus is gevonden, wordt er geen toegang gegeven tot het netwerk en is de hardware geblokkeerd. Op de hardware moet in dat geval eerst het probleem opgelost worden, waarna het programma nogmaals controleert of de hardware voldoet aan de beleidsregels. Indien het probleem opgelost is, wordt de hardware weer toegelaten tot het netwerk.

- Externe omgeving

Om een extra laag aan beveiliging te verzorgen, is het mogelijk om met een externe omgeving te werken. Deze externe omgeving wordt wel via BYOD hardware benaderd, maar indien alles correct ingesteld wordt kan een besmetting van de BYOD hardware niet de omgeving besmetten. Hiervoor kan een terminal server gebruikt worden, mits er geen shares over de verbinding toegevoegd worden. Daarnaast zijn er ook VDI mogelijkheden waarbij er een volledig geïsoleerde omgeving gemaakt kan worden, waar gebruikers niet de optie hebben om shares toe te voegen van de BYOD hardware. De gebruiker kan hierdoor geen virussen bewust of onbewust verspreiden vanaf de BYOD hardware.

10. Data beschermen

Zowel privédata als bedrijfsdata moet beschermd worden op de BYOD hardware. Hiervoor wordt aan de hand van deskresearch, een referentie onderzoek en een Proof of Concept het volgende onderzocht: "*Hoe kan de bedrijfsgevoelige of privédata van externe werknemers beschermd worden op hun eigen hardware?*". Hiermee wordt deelvraag vijf beantwoord.

Het is mogelijk dat externe medewerkers privé- of bedrijfsdata op hun hardware hebben staan. Omdat zij verbinding maken met het netwerk van SURFsara door diensten te gebruiken, is het gewenst om de data van de externe werknemer te beschermen. Het kan namelijk voor komen dat SURFsara data besmet is ondanks alle maatregelen, waardoor hun hardware op dit moment ook besmet kan worden. Om de data te beschermen zijn er mogelijkheden die SURFsara kan implementeren:

- Defense in Depth

Het beschermen van bedrijfsinformatie met diverse beveiligingsmaatregelingen heet Defense in Depth (TechTarget, 2007). Bij Defense in Depth kan bijvoorbeeld gebruik gemaakt worden van encryptie, firewalls, hashing en two-way authentication. In het geval van BYOD kan op verschillende plaatsen virusscannersoftware geïnstalleerd worden. Deze software kan op (file)servers en op de BYOD hardware geïnstalleerd worden. Door het gebruik van Defense in Depth is het lastiger voor malware om bestanden te besmetten. Wanneer naast verschillende implementatie mogelijkheden ook verschillende leveranciers van software gebruikt worden, is er een betere bescherming mogelijk. Dit komt doordat leveranciers beveiliging meestal op verschillende manieren aanpakken. Mocht er een zwakke plek in de software van één leverancier zijn, is het mogelijk dat een andere de zwakke plek niet heeft. Uit referentie onderzoek, Enquête Bring Your Own Device Gemeente Utrecht, is gebleken dat de Gemeente Utrecht ook gebruik maakt van Defense in Depth (Gemeente Utrecht, 2016). De Gemeente Utrecht gebruikt op verschillende plaatsen virusscanners om besmettingen tegen te gaan.

- Gebruik van een afgeschermde omgeving

Het is mogelijk om een aantal VM's in te zetten om naar toe te verbinden. Dit wordt gedaan in een VDI omgeving, waardoor medewerkers een afgeschermde omgeving hebben. In deze afgeschermde omgeving kan slechts de data van SURFsara benaderd worden en is er geen verkeer mogelijk tussen de VM en de BYOD hardware. Doordat een VM met een software cliënt benaderd wordt, is uitwisseling van data niet mogelijk. VM's kunnen indien gewenst met elkaar communiceren, externe hardware niet. Alleen geautoriseerde medewerkers kunnen op deze VM's inloggen. Een virusscanner op deze VDI omgeving waar de VM's op draaien kan de Defense in Depth mogelijkheid aanvullen. De integriteit wordt hierdoor gewaarborgd.

- Dataencryptie

Wanneer hardware encryptie toegepast wordt, kan de data op de hardware niet uitgelezen worden indien deze gestolen wordt. Hierdoor kan de data niet in verkeerde handen vallen. Op deze manier wordt de vertrouwelijkheid van data gewaarborgd.

- Netwerk detectie en infectie monitoring

Het is mogelijk om in het netwerk een Intrusion Detection System (IDS) en een Intrusion Prevention System (IPS) te plaatsen. Een IDS bekijkt de data die over het netwerk gaat en bepaalt of het verdacht verkeer is. Hiervoor worden patronen herkend, waardoor als er verdacht verkeer plaatsvindt er een melding gegenereerd kan worden. Hierop kan, en in veel gevallen moet, actie ondernomen worden. Een IPS zorgt ervoor dat dreigingen zoveel mogelijk geblokkeerd worden door (vooringestelde) beleidsregels te gebruiken. Een IPS kan ook op de meldingen van een IDS reageren door dat verkeer te blokkeren. Uit een referentieonderzoek bij de Hogeschool van Amsterdam (HvA), Enquête Bring Your Own Device Hogeschool van Amsterdam, blijkt dat de HvA een Quarantaine netwerk gebruikt om hardware waarop misbruik plaatsvindt te isoleren om verdere besmetting te voorkomen. Bij misbruik kan er gedacht worden aan illegale programma's of een besmet apparaat dat verkeer genereert. Indien dit naast IDS en IPS toegepast wordt, is de kans op besmetting kleiner.

- Applicatie streaming

Zowel in Dell vWorkspace als in Ulteo Open Virtual Desktop is het mogelijk om applicaties te streamen naar een cliënt. Hiermee kan een geautoriseerde gebruiker werken zonder de applicaties te installeren. Het opslaan van bestanden wordt gedaan op een server of VM van SURFsara, waardoor er geen data lokaal staat. Deze applicaties zijn zodoende afgeschermd voor de data van de externe medewerker, waardoor de integriteit gewaarborgd wordt.

Wanneer Defense in Depth gebruikt wordt, is de kans op een besmetting kleiner. Het gebruik van een afgeschermde omgeving zorgt ervoor dat SURFsara data en bedrijfs- of privédata gescheiden blijven, waardoor hier tussen geen besmetting kan plaatsvinden. Door dataencryptie te gebruiken, is de lokale data beveiligd tegen uitlezing tijdens een diefstal. Het detecteren en blokkeren van dreigingen zorgt ervoor dat er preventief en actief dreigingen voorkomen of opgelost kunnen worden. Door applicaties te streamen, staat er geen data lokaal en kan de gebruiker zonder alle benodigde applicaties te installeren toch SURFsara data en privédata scheiden. Indien alle bovenstaande mogelijkheden geïmplementeerd zijn, wordt de data van externe medewerkers zo goed mogelijk beschermd en blijft de integriteit en vertrouwelijkheid van de data gewaarborgd.

11. Monitoring BYOD hardware

Naast de bestaande manieren om gebruik te monitoren, moet het mogelijk zijn om de BYOD hardware te monitoren. Hiervoor wordt deelvraag zes beantwoord, namelijk "*Op welke manier kan de "Bring Your Own Device" hardware het best gemonitord worden?*".

Omdat de BYOD hardware op een andere manier gebruikt wordt dan reguliere hardware, is het noodzakelijk dat ook deze hardware gemonitord wordt. Wanneer er gemonitord wordt kan er sneller ingesprongen worden op problemen en is het beheer van de omgeving die BYOD mogelijk maakt makkelijker. Om te bepalen wat er gemonitord moet worden, is een enquête rondgestuurd op de afdeling IA. Aan de hand van de enquêteresultaten is er bekeken welke oplossing het beste voldoet.

In de enquête, Bijlage 6: Enquête monitoring, is gevraagd welke hardware er gemonitord moet worden, welke onderdelen (zoals de processor) op de hardware, hoe de alerts gestuurd moeten worden en of de monitoring tool in het pakket moet zitten of dat dit een aparte tool mag zijn. Er is aangegeven dat in ieder geval de Servers en de VM's die geïnstalleerd zijn gemonitord moeten worden. Voornamelijk gaat het om de connectiviteit, services, performance, opslag, geheugen gebruik, processor gebruik en de problemen. Indien er problemen zijn met deze onderdelen van de servers en VM's, moeten er alerts gestuurd worden. Het is gewenst dat dit via de e-mail gaat, alternatieven hiervoor zijn alerts via de portal, via sms of een extra monitoring tool genaamd Nagios mag. Het is gewenst dat de betreffende monitoring tool in de BYOD oplossing zit. Er is aangegeven dat als alternatief voor de ingebouwde monitoring tools ook andere tools gebruikt kunnen worden.

In de Proof of Concept zijn de drie producten uit de shortlist vergeleken met de resultaten uit de enquête. Ulteo Open Virtual Desktop heeft een ingebouwde monitoring tool, maar is beperkt. Het is slechts mogelijk om een email te versturen indien er services niet draaien of veranderd zijn van status. Deze meldingen zijn alleen van toepassing op de Linux server en niet op de Windows server die voor Windows applicaties zorgt. De mogelijkheden bij Dell vWorkspace zijn groter. Hierin zijn namelijk rapporten en alerts beschikbaar, waarin status van de server en de VM's gemeld worden. Daarnaast is er ook de mogelijkheid om een rapportage te laten mailen met het gebruik van geheugen, opslag, de login's die gedaan zijn en de processen die gestart zijn. Packetfence heeft echter weer minder mogelijkheden, waarbij slechts de schendingen van de vooringestelde regels (malware infectie gevonden, Windows niet up-to-date) vermeld worden via de email.

Bij Ulteo Open Virtual Desktop en Packetfence kan het best gemonitord worden door een extra monitoring tool te gebruiken om meer informatie per mail te ontvangen. Monitoring tool Nagios (Nagios, 2016) of PRTG (Paessler, 2016) vult de standaard mogelijkheden aan. Bij beide producten worden er sensoren aangemaakt die statussen uit kunnen lezen op de besturingssystemen en daarmee een rapportage kunnen maken. Dell vWorkspace heeft zelf een uitgebreide monitoring tool in het pakket verwerkt waarmee het best gemonitord kan worden. Met behulp van CFEngine of een extra monitoring tool zoals Nagios of PRTG, kunnen de mogelijkheden voor monitoring aangevuld worden.

12. Onderzoeksresultaat

De drie producten uit de shortlist van de toepassingsselectie zijn in een Proof of Concept, Bijlage 7: Proof of Concept, getest. In de Proof of Concept zijn de producten bekeken en vergeleken met de eisen, wensen en de doelstellingen. De resultaten van de Proof of Concept zijn hieronder weergegeven.

12.1. Ulteo Open Virtual Desktop

Ulteo Open Virtual Desktop wordt getest en er wordt bekeken of aan de eisen, wensen en doelstellingen wordt voldaan. Hieronder worden de resultaten uit de Proof of Concept weergegeven.

Eisen en wensen	Voldoet?	Toelichting
Open Source	Ja	Source Code is beschikbaar voor de community editie.
Ondersteuning verschillende besturingssystemen	Ja	Mac, Windows en Linux worden ondersteund.
Eenvoudig in gebruik	Ja	Keuze tussen applicaties en desktop bij login, ook mogelijk om deze in een browser omgeving te starten.
Passend binnen de beheeromgeving	Ja	Windows en Linux (CentOS) kunnen gebruikt worden, deze besturingssystemen worden nu ook gebruikt.
Bedrijfsdata niet lokaal op externe hardware	Ja	Desktop omgeving mogelijk waar alle data opgeslagen wordt, waardoor de data niet lokaal staat.
Besmettingsgevaar minimaliseren / virusscanners	Ja	Scan's kunnen gedaan worden en upload's geblokkeerd worden op de applicatieserver.
Back-up van data	Ja	De userfolders op de servers kunnen geback-upt worden.
Netwerkbeveiliging	Ja	Authenticatie en beveiligde verbinding (SSL) zijn mogelijk.
Continuïteit	Matig	De Remote Desktop Service werkt niet altijd door verkeerde browser cookies. Wanneer deze gewist worden werkt de omgeving meestal wel tot er een aanpassing op de server gedaan wordt.

TABEL 8: EISEN EN WENSEN ULTEO

Doelstelling	Voldoet?	Toelichting
Besmetting van bedrijfsdata voorkomen	Ja	Er is een afgeschermde omgeving waar naartoe verbonden kan worden via de browser op de BYOD hardware.
Verlies van data gewaarborgd	Ja	Data staat op de server, waardoor dit niet lokaal staat.
Privédata beschermd/afgeschermd	Ja	Data staat op de server, waardoor dit niet lokaal staat.
Remote werken mogelijk	Matig	Van afstand via VPN kan er verbonden worden naar de omgeving. Echter is slechts voor

		Windows een Windows Server omgeving mogelijk.
Ondersteuning meerdere besturingssystem	Ja	Mac, Windows en Linux
Beheer en up-to-date houden	Ja	Beheer kan via een admin portal, het updaten kan eenvoudig via de command-line gedaan worden.
Monitoring mogelijk	Matig	Er zijn wel status updates van services etc. Geen mogelijkheid om het gebruik van resources te monitoren.
Conform de ISO27001 norm en de richtlijnen van SURFsara	Ja	Er kan een beveiligde verbinding opgezet worden naar het systeem, door gebruik te maken van SSL certificaten.

TABEL 9: DOELSTELLINGEN ULTEO

Ulteo Open Virtual Desktop streamt alle Windows applicaties via een Windows Terminal Server omgeving. De Remote Desktop die hierdoor mogelijk is, maakt direct verbinding op de Windows server. Hierdoor is er geen cliënt omgeving en kan dit mogelijk schadelijk zijn voor de server. Door de server omgeving zijn er beperkte mogelijkheden om extra of minder beveiligingsregels toe te passen, omdat dit dan voor iedereen geldt die verbinding maakt met de server. Het is een aantal keer voorgekomen dat de Remote Desktop service tijdelijk niet werkte of dat de server een verkeerde omgeving toewees door browser cookies. Daarnaast kan niet alles gemonitord worden wat wel gewenst is, zoals de status van het gebruik van resource op de server. Ulteo Open Virtual Desktop voldoet niet volledig aan de eisen, wensen en doelstellingen van SURFsara.

12.2. Dell vWorkspace

De BYOD oplossing Dell vWorkspace wordt ook getest en er wordt bekeken of aan de eisen, wensen en doelstellingen voldaan wordt. Hieronder de resultaten van de Proof of Concept.

Eisen en wensen	**Voldoet?**	**Toelichting**
Open Source	Nee	Het is een commercieel product.
Ondersteuning verschillende besturingssystemen	Ja	Mac, Windows en Linux worden ondersteund.
Eenvoudig in gebruik	Ja	Er is een keuze tussen applicaties en een desktop omgeving bij login, ook mogelijk om in een browser omgeving applicaties en de desktop te starten.
Passend binnen de beheeromgeving	Ja	Windows wordt gebruikt, dit besturingssysteem wordt nu ook gebruikt.
Bedrijfsdata niet lokaal op externe hardware	Ja	Data staat op de server, waardoor dit niet lokaal staat.
Besmettingsgevaar minimaliseren / virusscanners	Ja	Virusscanners op verschillende platformen zijn mogelijk, tevens kunnen USB apparaten en netwerk shares geblokkeerd worden.
Back-up van data	Ja	De userfolders op de servers kunnen geback-upt worden.
Netwerkbeveiliging	Ja	Authenticatie en beveiligde verbinding (SSL) zijn mogelijk.

Continuïteit	Ja	Geen problemen ondervonden tijdens het testen.

TABEL 10: EISEN EN WENSEN DELL VWORKSPACE

Doelstelling	Voldoet?	Toelichting
Besmetting van bedrijfsdata voorkomen	Ja	Er is een afgeschermde omgeving waar naartoe verbonden kan worden via de cliënt of via de browser op de BYOD hardware.
Verlies van hardware en data gewaarborgd	Ja	Data staat op de server, waardoor dit niet lokaal staat.
Privédata beschermd/afgeschermd	Ja	Data staat op de server, waardoor dit niet lokaal staat.
Remote werken mogelijk	Ja	Van afstand via VPN kan er verbonden worden naar de omgeving.
Ondersteuning meerdere besturingssystem	Ja	Mac, Windows, Linux worden ondersteund.
Beheer en up-to-date houden	Ja	Via de management console kan de BYOD oplossing beheerd worden. Tevens zijn de nieuwste updates die direct te downloaden zijn in de management console beschikbaar.
Monitoring mogelijk	Ja	Interne mogelijkheden om te monitoren en rapporten te genereren.
Conform de ISO27001 norm en de richtlijnen van SURFsara	Ja	Er kan een beveiligde verbinding opgezet worden naar het systeem, door gebruik te maken van SSL certificaten.

TABEL 11: DOELSTELLINGEN DELL VWORKSPACE

Dell vWorkspace streamt alle applicaties via een Remote Desktop Sessie. Indien er gebruik gemaakt wordt van VM's, kan er verbonden worden met een cliënt omgeving. In eerste instantie kon er alleen verbonden worden met een cliënt, voor het mogelijk maken van in-browser streaming is er een extra BYOD server geïnstalleerd met Windows Server 2012 R2. De VM's worden meestal gekoppeld via een VDI pool van een andere hypervisor, zoals VMWare of Citrix, maar dit is niet noodzakelijk. VM's kunnen ook los toegevoegd worden, waardoor deze persoonlijk ingericht kunnen worden. Beveiliging kan zodoende per VM toegepast worden. In Dell vWorkspace zitten uitgebreide opties om te monitoren. Dell vWorkspace voldoet alleen niet aan de open-source wens.

12.3. PacketFence

Als laatste product wordt PacketFence getest en wordt tevens bekeken of aan de eisen, wensen en doelstellingen voldaan wordt. De resultaten zijn als volgt:

Eisen en wensen	Voldoet?	Toelichting
Open Source	Ja	De source code is beschikbaar.
Ondersteuning verschillende besturingssystemen	Matig	Besturingssystemen worden ondersteund, echter de scan engines zijn slechts bedoeld voor Mac OS en Windows, maar niet voor Linux.

Eenvoudig in gebruik	Matig	Indien er geblokkeerd wordt, kan het lastig zijn voor de gebruiker doordat zij niets meer kunnen doen.
Passend binnen de beheeromgeving	Ja	Windows en Linux (CentOS) kunnen gebruikt worden, deze besturingssystemen worden nu ook gebruikt.
Bedrijfsdata niet lokaal op externe hardware	Nee	De data staat nog steeds lokaal op de BYOD hardware.
Besmettingsgevaar minimaliseren / virusscanners	Matig	Besmette hardware zou niet toegang tot het netwerk moeten krijgen. Echter als er iets niet gedetecteerd wordt is besmetting mogelijk.
Back-up van data	Nee	Gebruikers zijn in dit geval zelf verantwoordelijk voor een back-up van de data, omdat dit lokaal staat.
Netwerkbeveiliging	Ja	Authenticatie en beveiligde verbinding (SSL) zijn mogelijk. Daarnaast kan er gescand worden tijdens of voor het inloggen op de portal.
Continuïteit	Matig	Als het pakket cliënts blokkeert kan dit hinder veroorzaken, doordat al het verkeer dan geblokkeerd wordt.

TABEL 12: EISEN EN WENSEN PACKETFENCE

Doelstelling	**Voldoet?**	**Toelichting**
Besmetting van bedrijfsdata voorkomen	Matig	Besmette hardware zou niet in het netwerk toegang moeten krijgen. Echter als er iets niet gedetecteerd wordt is besmetting nog mogelijk.
Verlies van hardware en data gewaarborgd	Nee	Extra maatregelen moeten genomen worden, het pakket zelf doet dit niet omdat de data lokaal staat. In dit geval moet er een oplossing gevonden worden om van afstand data te verwijderen.
Privédata beschermd/afgeschermd	Nee	Extra maatregelen moeten genomen worden, het pakket zelf doet dit niet. Er zijn zelfs mogelijkheden in het pakket om juist de privédata ook te scannen waardoor er mogelijk privacy issues kunnen ontstaan.
Remote werken mogelijk	Ja	Van afstand via VPN kan er verbonden worden naar de omgeving.
Ondersteuning meerdere besturingssystem	Ja	Mac, Linux, Windows worden ondersteund.
Beheer en up-to-date houden	Ja	Beheer is mogelijk via de admin portal. Het pakket is eenvoudig te updaten via command-line.

Monitoring mogelijk	Matig	Via de portal zijn logs uit te lezen. Via de email kunnen de schendingen (malware gevonden en dergelijke) gestuurd worden. Andere opties zijn niet mogelijk.
Conform de ISO27001 norm en de richtlijnen van SURFsara	Ja	Er kan een beveiligde verbinding opgezet worden naar het systeem, door gebruik te maken van SSL certificaten.

TABEL 13: DOELSTELLINGEN PACKETFENCE

PacketFence voldoet niet geheel aan de eisen en doelstellingen. Dit was bij de pakketselectie al bekend, maar zou in de praktijk anders kunnen zijn. In de praktijk blijkt dat het product alsnog niet voldoet, omdat het product direct achter de VPN-verbinding geplaatst moet worden. Al het verkeer van de VPN-verbinding moet dan ook via de PacketFence server. Hierdoor kan er een single-point of failure voor alle gebruikers ontstaan. Daarnaast kan dit tot ongewenste effecten leiden op BYOD hardware, doordat gebruikers moeten registreren en voldoen aan de voorwaardes van PacketFence om verder te kunnen. Hoewel het de bedoeling is dat gebruikers geblokkeerd worden, kan hierdoor de continuïteit gehinderd worden. Een ander ongewenst effect kan zijn dat al het verkeer gescand wordt en opgeslagen wordt in logfiles. Dit kan tot privacy issues leiden.

Uit de Proof of Concept blijkt dat er één product voldoet als oplossing voor het veilig toepassen van het BYOD-principe. Dell vWorkspace voldoet namelijk aan de meeste eisen, wensen en doelstellingen. In de praktijk werkt Dell vWorkspace snel en gemakkelijk, waardoor deze oplossing het best gebruikt kan worden ter ondersteuning van het beleid dat geschreven moet worden.

12.4. Aanbevelingen

Wanneer de gekozen oplossing toegepast wordt, zijn er een aantal extra aanbevelingen. De aanbevelingen zijn beschreven om het toepassen van het beleid en de oplossing zo goed mogelijk te laten verlopen. De onderstaande aanbevelingen zijn tevens in het adviesrapport, Bijlage 8: Adviesrapport, opgenomen.

- Externe medewerkers geen hardware meer van SURFsara.

Momenteel worden laptops gebruikt van SURFsara door externe medewerkers. Deze hardware wordt nu gekozen door het CYOD beleid, maar het is gewenst dat alle externe medewerkers de BYOD oplossing gebruiken.

Externe medewerkers kunnen toegang krijgen tot de BYOD oplossing. Mijn aanbeveling is om de betreffende medewerkers over te laten gaan op de BYOD oplossing. Als momenteel een overtreding plaatsvindt en er gekozen wordt om de laptop in te nemen, kan de gebruiker nog lokaal bestanden aanpassen of verspreiden. Met de BYOD oplossing kan indien nodig de toegang tot services en data ontzegd worden, zodat er niets meer aangepast of verspreid kan worden. Daarnaast blijft het beleid uniform als iedereen over gaat naar de BYOD oplossing, in plaats van dat er voor specifieke personen een uitzondering gemaakt wordt.

- VM's per gebruiker

In de oplossing is het mogelijk om gebruik te maken van een VDI omgeving waar dynamische of statische VM's toegewezen worden. Het voordeel van een dynamische VM ten opzichte van een

statische is dat de VM's uit gaan als deze niet gebruikt worden. Hierdoor wordt er minder gebruik gemaakt van het netwerk, de processorkracht en het geheugen van de server. In een dynamische omgeving zijn de VM's allemaal hetzelfde. Het nadeel van dynamische VM's is dat indien er persoonlijke instellingen gemaakt moeten worden, deze losgekoppeld moeten worden. Hierdoor wordt het alsnog een statische VM. Bij dynamische VM's moet ook alle software geïnstalleerd worden die gebruikers gebruiken. Hierdoor krijgen sommige gebruikers applicaties in hun omgeving die zij nooit gebruiken.

Mijn aanbeveling is om VM's per gebruiker in te richten. Deze VM's staan wel altijd aan maar kunnen gepersonaliseerd worden. Applicaties kunnen per gebruiker bepaald worden en er kunnen eventuele restricties op gebruikers ingesteld worden. Een restricties kan bijvoorbeeld zijn dat gebruikers geen administrator rechten hebben, waardoor zij zelf geen extra applicaties kunnen installeren.

- Ondertekening beleid in verband met aansprakelijkheid

Voor het gebruik van BYOD hardware wordt een beleid opgesteld. In dit beleid worden de richtlijnen en aansprakelijkheid opgenomen. De richtlijnen omvatten het gebruik van de BYOD oplossing en de aansprakelijkheid omvat wie er verantwoordelijk is.

Mijn aanbeveling is om externe medewerkers het BYOD beleid te laten ondertekenen. Doordat in het beleid opgenomen is wie er verantwoordelijk is, kan er later geen aanspraak gemaakt worden dat het niet bekend was. Dit voorkomt problemen indien er ongewenste situaties voor komen waarin het anders niet bekend zou zijn wie er verantwoordelijk is. Het beleid kan in de indiensttredingsprocedure verwerkt worden als interne medewerkers ook BYOD hardware willen gebruiken.

- Beheerder toewijzen

Indien een BYOD oplossing toegepast wordt, moet de oplossing bijgehouden worden. Onder het bijhouden valt het monitoren van services, het monitoren van het gebruik van VM's en het monitoren van de applicaties. Wanneer een nieuwe externe medewerker een VM nodig heeft, moet deze aangemaakt worden, de toegang tot de VM ingeregeld worden en de VM geconfigureerd worden. Daarnaast moet het mogelijk zijn om de toegang te ontheffen.

Het is raadzaam om een beheerder toe te wijzen aan de BYOD oplossing indien deze geïmplementeerd wordt, zodat de continuïteit gewaarborgd wordt.

- Gebruik van VM templates

Wanneer de BYOD oplossing gebruikt wordt, moeten er voor externe medewerkers VM's aangemaakt worden. Het is ook mogelijk dat het aantal externe medewerkers groeit, waardoor meerdere VM's later aangemaakt moeten worden. Het aanmaken, configureren en updaten van een VM kan tijdrovend zijn.

Om tijd te besparen is het raadzaam dat er gebruik gemaakt wordt van templates om VM's snel aan te maken. Deze VM's kunnen in eerste instantie een clone zijn, waarbij er daarna instellingen aangepast worden. Door het gebruik van een template die periodiek bijgewerkt wordt betreft updates, zijn nieuwe VM's altijd up-to-date.

- Support

Wanneer gebruikers de BYOD oplossing gebruiken, is het bijna onvermijdelijk dat er problemen optreden of dat gebruikers vragen hebben.

Mijn aanbeveling is om in het beleid een apart hoofdstuk te wijden aan het onderdeel support. In het hoofdstuk support zouden de contact gegevens van de afdeling waarbij gebruikers terecht kunnen bekend en benoemd moeten zijn. Met vragen, problemen of opmerkingen kunnen gebruikers bij deze afdeling terecht.

- Toepassing Defense in Depth

Op cliënts en servers in het kantoornetwerk zijn virusscanners geïnstalleerd. Op de firewall is er IDS en IPS ingericht. Het is mogelijk dat er op cliënts en servers dezelfde virusscanners staan, waardoor er exploits gebruikt kunnen worden.

Mijn aanbeveling is om verschillende virusscanners op de cliënts en servers te installeren. Hierdoor is het mogelijk dat als de virusscanner malware op de cliënts niet detecteren, de servers de malware mogelijk wel detecteren. Daarnaast kan er voor gekozen worden om ook op de BYOD server een andere virusscanner te installeren. Indien F-secure op de cliënts gebruikt wordt, moet er op de servers en de BYOD server een andere virusscanner geïnstalleerd worden.

- Audits op het beleid en de technische oplossing

Naar mate het beleid toegepast wordt en de technische oplossing gebruikt wordt, kan het zijn dat het beleid niet meer voldoet. Indien dit zo is, dient het beleid aangepast te worden.

Het is hierdoor raadzaam om periodiek audits plaats te laten vinden, zowel om de beveiliging als gebruik van applicaties en bestanden te controleren. Hierdoor blijft het beleid up-to-date en de technische oplossing zo optimaal mogelijk.

- Apart netwerk voor de BYOD oplossing

Indien BYOD gebruikers verbinding moeten maken met de huidige VPN-verbinding, hebben zij meestal ook toegang tot het kantoornetwerk. Het is echter niet altijd gewenst dat gebruikers bij applicaties of data van SURFsara kunnen.

Het is hierdoor aanbevolen om de BYOD oplossing in een apart netwerk te plaatsen of in ieder geval op een andere manier toegankelijk. Hiervoor zou een tweede VPN-verbinding voor gebruikt kunnen worden. Specifieke VM’s die gekoppeld zijn via de BYOD oplossing kunnen toegelaten worden tot het kantoornetwerk van SURFsara of specifieke file-shares door firewall regels te maken.

- PacketFence als VPN beveiliging

Hoewel het product PacketFence niet voldoet voor het toepassen van het BYOD principe, kan het wel gebruikt worden als extra beveiliging op de VPN verbinding. Gebruikers moeten hierna één keer extra inloggen voordat zij toegang krijgen tot het netwerk. De hardware kan dan gescand worden op virussen en hardware blokkeren indien er virussen gevonden zijn.

De afweging moet gemaakt worden of PacketFence geschikt is om de VPN verbinding extra te beveiligen. Al het VPN verkeer moet via PacketFence, waardoor het een single-point of failure is. Om dit op te lossen zou er een loadbalancer geplaatst moeten worden, waardoor de kosten hoger worden. Daarnaast is er geen mogelijkheid om Linux distributies te scannen tijdens het verkrijgen van toegang tot het netwerk. Hierdoor is PacketFence beperkt inzetbaar.

- Wet bescherming persoonsgegevens (Wbp)

Vanaf begin 2016 is de Wbp (Overheid.nl, 2015) van toepassing. In deze wet wordt de verplichting om datalekken te melden behandeld. Bij het gebruik van de BYOD oplossing, is het mogelijk dat gebruikers referenties opslaan om gemakkelijk in te loggen. Wanneer de hardware van de gebruiker gestolen of gehackt wordt, kan hierdoor een datalek ontstaan. Vanaf 2018 kan de boete die opgelegd wordt erg hoog zijn.

Het is niet geheel bekend of de Wbp van toepassing is op het BYOD principe en wie er aansprakelijk zijn. Hoewel in het beleid beschreven staat dat gebruikers voorzichtig om moeten gaan met data, kan het voorkomen dat een datalek toch voorkomt. Indien de BYOD oplossing toegepast wordt, moet er uitgezocht worden of de Wbp van toepassing is op BYOD en welke extra maatregelen genomen moeten worden.

13. Conclusie

Voor SURFsara is er onderzoek gedaan naar het implementeren van het Bring Your Own Device principe. De hoofdvraag in het onderzoek: "*Welke methode is het meest geschikt om het Bring Your Own Device principe op een veilige en goed te beheren wijze toe te passen bij SURFsara, zodat de integriteit en de vertrouwelijkheid van SURFsara data en privédata gewaarborgd zijn?*" wordt beantwoord. De beantwoording wordt ondersteund door de antwoorden op deelvragen.

Momenteel kunnen externe medewerkers van SURFsara toegang krijgen tot het kantoornetwerk, waardoor zij diverse gegevens en applicaties ongecontroleerd kunnen gebruiken. Het is ongewenst, omdat dit besmettingen en misbruik van data mogelijk maakt. Om het BYOD principe veilig en op goed beheerde wijze toe te kunnen passen, moet er een beleid geschreven worden. In het beleid staan regels en richtlijnen waar externe medewerkers zich aan moeten houden. De beleidsregels en richtlijnen hebben betrekking op de toegang tot de data en applicaties van SURFsara, hoe de gebruiker zelf kan voorkomen dat bedrijfs- en privédata in gevaar komt, wie in bepaalde situaties verantwoordelijk is en waar problemen gemeld en/of vragen gesteld kunnen worden. Het beleid is gebaseerd op de ISO27001:2013 richtlijnen voor informatiebeveiliging.

Het beleid kan niet garanderen dat externe medewerkers zich aan de regels en richtlijnen houden. Met een technisch ondersteuning worden externe medewerkers gedwongen om zich aan de regels en richtlijnen te houden, waardoor het BYOD principe zo veilig mogelijk wordt toegepast. Om te bepalen welke technische ondersteuning het beleid kan aanvullen, zijn de eisen en wensen van SURFsara in kaart gebracht door interviews af te nemen met de opdrachtgever en de security officer. Deze eisen en wensen zijn in een toepassingsselectie verwerkt samen met potentiële producten die als technische ondersteuning gebruikt kunnen worden. Per product is bekeken of deze in theorie voldoen aan de eisen en wensen. In de toepassingsselectie zijn uiteindelijk drie producten gekozen en deze zijn getest in een Proof of Concept. Deze drie producten zijn: Ulteo Open Virtual desktop, Dell vWorkspace en PacketFence. De producten zijn in de praktijk getest of deze voldoen aan de eisen, wensen en doelstellingen. Slechts één van de drie producten voldoet bijna volledig hieraan. Dell vWorkspace voldoet alleen niet aan de eis Open Source.

Er moeten preventieve maatregelen genomen worden om de kans op besmettingen te verkleinen of geheel voorkomen worden. Dit moet door het gekozen product ondersteund worden. Medewerkers kunnen trainingen krijgen om bewuster te worden van malware en de schade hiervan. Ook virusscanners kunnen geïmplementeerd worden op diverse niveaus, zoals op de servers, op de BYOD oplossing en op de BYOD cliënts. Om de kans op besmetting nog kleiner te maken, moet er gebruik gemaakt worden van een anti-spam product dat schadelijke mails tegenhoudt. Een bekende bron van besmetting zijn opslagmediums zoals USB-sticks en advertenties op websites. Wanneer er slechts door de kantoorautomatisering geleverde beveiligde USB-sticks toegelaten worden en advertenties geblokkeerd worden, ondersteund dit de technische oplossing. Hierdoor wordt de integriteit van data gewaarborgd.

Om verder bedrijfsgevoelige en privédata van externe medewerkers te beschermen, kan er gebruik gemaakt worden van een afgeschermde omgeving. In deze omgeving draaien Virtuele Machines waarop gewerkt wordt, in plaats van dat data lokaal staat. Privédata blijft hierdoor gescheiden van bedrijfsdata. Om verdere datascheiding mogelijk te maken, kan gekozen worden om applicatie te streamen. Applicaties wordt hierbij niet geïnstalleerd, maar in een separate omgeving weergegeven.

Ook kunnen de externe medewerkers gebruik maken van data encryptie, om te zorgen dat de hardware niet uitgelezen kan worden indien deze in verkeerde handen valt. Verdacht netwerkverkeer kan geblokkeerd worden door een Intrusion Detection System en een Intrusion Prevention System. Deze systemen herkennen patronen, genereren meldingen en kunnen verkeer blokkeren. Door het toepassen van deze systemen wordt de vertrouwelijkheid van data gewaarborgd.

In de technische oplossing maken rapportages en alerts deel uit van het beheer. Tijdens de Proof of Concept is gekeken welke mogelijkheden in de producten aanwezig waren. Ulteo Open Virtual Desktop en PacketFence bezitten uit zichzelf niet de gewenste mogelijkheden die uit de monitoring enquête is gekomen. Deze twee producten moeten hierin ondersteund worden door gebruik te maken van een extra monitoring tool. Ulteo Open Virtual Desktop en PacketFence kunnen via de portal en de Command-line beheerd worden. Dell vWorkspace bezit wel de gewenste mogelijkheden uit de monitoring enquête, maar er kan alsnog gekozen worden om een extra monitoring tool te gebruiken. Dell vWorkspace wordt beheerd door gebruik te maken van de management-console.

In de Proof of Concept is Dell vWorkspace als beste uit de test gekomen. Het product is niet open-source, maar voldoet wel aan de eisen, wensen en doelstellingen. Hierdoor is Dell vWorkspace de meest geschikte technische oplossing voor het toepassen van het BYOD-principe. Door het beleid en de technische oplossing op elkaar af te stemmen, kan het Bring Your Own Device principe veilig toegepast worden bij SURFsara. De integriteit en vertrouwelijkheid van SURFsara data en privédata zijn gewaarborgd als alle preventieve maatregelen gebruikt worden. De combinatie van het beleid, de technische oplossing en de ondersteuning van de maatregelen, is de meest geschikte methode om het Bring Your Own Device principe op een veilige en goed te beheren wijze toe te passen.

14. Evaluatie

Door de beantwoording van de hoofdvraag, is het onderzoek naar het veilig toepassen van het BYOD principe afgerond. In deze evaluatie wordt de procesgang van het project bekeken.

Op 1 februari 2016 is het afstudeeronderzoek van start gegaan. Hierbij is er direct begonnen aan het opstellen van een Plan van Aanpak. Voor de invulling van het onderzoek is overlegd met de opdrachtgever in welke richting er gegaan moest worden. Hierdoor is het duidelijk geworden wat de eisen en wensen voor de toepassing van het BYOD principe waren en wat er niet gewenst was. Doordat er wekelijks overlegd werd vanaf het begin, was er controle op de werkzaamheden en sturing mogelijk. Hierdoor kon het project snel van start gaan zonder tegenvallers.

In het afstudeercontract en het Plan van Aanpak is er een planning gemaakt. Deze planning bestond uit fases waarin aan diverse producten gewerkt zou worden. Vrij snel is er afgeweken van deze planning, door parallel aan diverse (deel)producten te werken. Zo werd er al aan de scriptie en het adviesrapport gewerkt direct na het afronden van het Plan van Aanpak. Hierdoor werden documenten eerder opgeleverd dan de einddatums en deadlines. Hierdoor kon er eerder feedback gegeven worden, waardoor de feedback met de opdrachtgever besproken kon worden.

Doordat er documenten eerder opgeleverd werden, kon er meer tijd besteed worden aan het zoeken naar producten die mogelijk voldoen. Om te bepalen wat de eisen en wensen zijn voor het product, hebben er interviews met de opdrachtgever en de security officer plaatsgevonden. De producten zijn vervolgens in een toepassingsselectie met eisen en wensen vergeleken. Na een aantal producten gevonden te hebben, is de top drie van de toepassingsselectie in de Proof of Concept getest. De Proof of Concept is van de planning afgeweken, omdat de omgeving ingericht moest worden. Het inrichten duurde langer dan verwacht, omdat een andere afdeling hiervoor het een en het ander moest aanpassen. De deadline van de Proof of Concept werd hierdoor niet behaald, echter omdat er veel producten al af waren was dit geen probleem voor de voortgang van het onderzoek.

De producten die getest zijn in de Proof of Concept zijn door meerdere personen van de afdeling bekeken. Hierbij kwamen nog een aantal functionele wensen naar boven, waardoor één omgeving aangepast werd. Deze aanpassing was niet veel werk, waardoor de planning niet in gevaar kwam. De functionele wensen zorgden ervoor dat naast de vooraf bepaalde eisen, wensen en doelstellingen de producten beter getest konden worden of deze in de praktijk voldoen.

Als laatst is het adviesrapport beschreven. Hierin staat een beknopte samenvatting van de scriptie. Doordat tijdens de Proof of Concept functionele wensen naar boven gekomen waren, is hier in het adviesrapport op in gespeeld.

Al met al is het onderzoek soepel verlopen zonder dat er erg van de planning afgeweken is. De hoofdvraag is naar tevredenheid beantwoord, waardoor SURFsara gebruik kan gaan maken van de aangedragen oplossing.

15. Afkortingenlijst

Afkorting	Betekenis
AS-IS	Afkorting voor de huidige situatie
AvE	Analyse van Eisen
BYOD	Bring Your Own Device, waarbij medewerkers eigen hardware gebruiken en onderworpen zijn aan regels van het bedrijf.
CYOD	Choose Your Own Device, waarbij medewerkers een keuze krijgen uit beperkte hardware vanuit het bedrijf en onderworpen zijn aan regels van het bedrijf.
HIYOD	Here Is Your Own Device, waarbij medewerkers hardware van het bedrijf krijgen en onderworpen zijn aan strenge regels van het bedrijf.
HNW	Het nieuwe werken, waarbij er remote gewerkt wordt.
HPC	High-performance computing
HU	Hogeschool Utrecht
IA	Afkorting voor de afdeling Interne Automatisering
IDS	Afkorting voor Intrusion Detection System
IPS	Afkorting voor Intrusion Prevention System
KA	Afkorting voor Kantoorautomatisering
NAC	Afkorting voor Network Access Control
OYOD	On Your Own Device, waarbij medewerkers eigen hardware gebruiken en niet onderworpen zijn aan regels van het bedrijf.
PvA	Plan van Aanpak
SARA	Stichting Academisch Rekencentrum Amsterdam
SSL VPN	Afkorting voor Secure Socket Layer Virtual Private Network
TO-BE	Afkorting voor de gewenste situatie
UAP	Afkorting voor Acceptable Use Policy
VDI	Afkorting voor Virtual Desktop Infrastructure
VM	Afkorting voor Virtual Machine
VPN	Afkorting voor Virtual Private Network

16. Figuren en tabellen

17. Bibliografie

AD. (2016, 04 11). *Advertenties op honderden grote sites kort tijd besmet*. Opgehaald van AD.nl: http://www.ad.nl/ad/nl/38261/Nieuws/article/detail/4279992/2016/04/11/Advertenties-op-honderden-grote-sites-korte-tijd-besmet.dhtml

Bridging the Gap. (2015, 03 17). *As-is Business process*. Opgehaald van Bridging-the-gap.com: http://www.bridging-the-gap.com/as-is-business-process/

Bridging the Gap. (2015, 10 10). *To-be Business process*. Opgehaald van Bridging the Gap.com: http://www.bridging-the-gap.com/to-be-business-process/

CFEngine. (2016, 02 23). *Product*. Opgehaald van CFEngine: https://cfengine.com/product/

Computable. (2004, 04 16). *Traditionele antivirus-oplossingen voldoen niet meer*. Opgehaald van Computable.nl: https://www.computable.nl/artikel/achtergrond/security/1384342/1444691/traditionele-antivirus-oplossingen-voldoen-niet-meer.html

Faronics. (2014, 10 01). *Best practices malware protection prevention*. Opgehaald van Faronics.com: http://www.faronics.com/news/blog/best-practices-malware-protection-prevention/

Gartner. (2015, 07 23). *bring-your-own-device*. Opgehaald van Gartner.com: http://www.gartner.com/it-glossary/bring-your-own-device-byod

Gartner. (2015, 09 08). *Mobile Device Management mdm*. Opgehaald van Gartner.com: http://www.gartner.com/it-glossary/mobile-device-management-mdm

Gartner. (2015, 10 02). *Network Access Control (NAC)*. Opgehaald van Gartner.com: http://www.gartner.com/it-glossary/network-access-control-na

Gartner. (2015, 11 23). *virtual-desktop-infrastructure-vdi*. Opgehaald van Gartner.com: http://www.gartner.com/it-glossary/virtual-desktop-infrastructure-vdi

Gartner. (2016, 02 01). *Magic Quadrant for Endpoint Protection Platforms*. Opgehaald van Gartner: https://www.gartner.com/doc/reprints?id=1-2XU816T&ct=160203

Gemeente Utrecht. (2016, 03 30). Enquête Bring Your Own Device Gemeente Utrecht - Richardo Theben Tervile.

Ijcaonline. (2014, 11). *A review of Opensource Network Access COntrol*. Opgehaald van research.ijcaonline.org: http://research.ijcaonline.org/volume106/number6/pxc3899721.pdf

IJcaonline. (2014, 11). *A review of Opensource Network Access COntrol*. Opgehaald van research.ijcaonline.org: http://research.ijcaonline.org/volume106/number6/pxc3899721.pdf

International Organization for Standardization. (2016, 02 08). *iso27001*. Opgehaald van iso.org: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

KPMG. (2010, 12 31). *0208_KPMG.* Opgehaald van itinbedrijf: http://itinbedrijf.info/0208_KPMG.pdf

Mevius, L. (2015, 11 02). Veilige toepassing van BYOD.

Nagios. (2016, 05 05). *Nagios*. Opgehaald van Nagios.org: https://www.nagios.org/

NEN. (2013). NEN-ISO/IEC 27001. *Ionformation technology - Security techniques - Information secuirty management systems - Requirements (ISO/IEC 27001:2013,IDT)*, 1-23.

Paessler. (2016, 04 23). *PRTG*. Opgehaald van passler.com/prtg: https://www.paessler.com/prtg

Sophos. (2015, 05 10). *Top 5 threat protection best practices*. Opgehaald van Sophos.com: https://www.sophos.com/en-us/security-news-trends/security-trends/top-5-threat-protection-best-practices.aspx

Stedehouder, J. (2012, 09 02). *byod-een-balans-tussen-controle-en-vrijheid*. Opgehaald van bringyourowndevice.wordpress: https://bringyourowndevice.wordpress.com/2012/09/02/byod-een-balans-tussen-controle-en-vrijheid/

Steehouder, M., Jansen, C., Mulder, J., van der Pool, E., & Zeijl, W. (2011). *Leren communiceren.* Noordhoff Uitgevers.

SURFsara. (2015, 11 11). *AUP SURF v1 def.* Opgehaald van intranet.surfsara.nl: https://intranet.surfsara.nl/argos/attachment/wiki/Beleid/AUP%20SURF%20V1%20def.pdf

SURFsara. (2015, 12 16). *Manual Linux Tips Tricks*. Opgehaald van intranet.surfsara.nl: https://intranet.surfsara.nl/ka/wiki/ManualLinuxTipsTricks

SURFsara. (2016, 03 23). *ManualMac*. Opgehaald van intranet.surfsara.nl: https://intranet.surfsara.nl/ka/wiki/ManualMac

SURFsara. (2016). *over-surfsara*. Opgehaald van surf.nl: https://www.surf.nl/over-surf/werkmaatschappijen/surfsara/over-surfsara/index.html

Techopedia. (2016, 01 28). *Proof of concept poc.* Opgehaald van techopedia: https://www.techopedia.com/definition/4066/proof-of-concept-poc

TechTarget. (2007, 06). *Defense in depth*. Opgehaald van searchsecurity.techtarget.com: http://searchsecurity.techtarget.com/definition/defense-in-depth

TechTarget. (2015, 04). *Comparing the top SSL VPN products*. Opgehaald van searchsecurity.techtarget.com: http://searchsecurity.techtarget.com/feature/Comparing-the-top-SSL-VPN-products

Utrecht, H. (2015, 11 04). *Afstuderen.* Opgehaald van sharepoint.hu.nl: https://onderwijsteams.sharepoint.hu.nl/fnt/Cluster_ICT/afstuderen/Belangrijke%20documenten1/Afstudeerleidraad%20Instituut%20voor%20ICT%20cursus%202015-2016.pdf

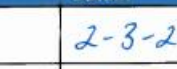
Bijlage 1: Plan van Aanpak

Versiebeheer

Datum	Versie	Reviewer	Beschrijving
02-02-16	0.1	Dion Kruijswijk	Opzet Plan van Aanpak
03-02-16	0.2	Dion Kruijswijk	Invulling hoofdstukken 4, 5.1, 6, 7 en 8
05-02-16	0.3	Dion Kruijswijk	Invulling hoofdstukken 2, 3, 5.2 en 9
09-02-16	0.3	Leonieke Mevius	Feedback op versie 0.3
09-02-16	0.4	Dion Kruijswijk	Feedback op versie 0.3 deels verwerkt
11-02-16	0.5	Dion Kruijswijk	Resterende feedback verwerkt en uitbreiding aanpak
12-02-16	0.6	Dion Kruijswijk	Aanpassing deelvragen, uitbreiding hoofdstuk 2, 4, 5 en 7
17-02-16	0.6	Leonieke Mevius	Feedback op versie 0.6
18-02-16	0.6	Lucas Slim	Feedback op versie 0.6
18-02-16	0.7	Dion Kruijswijk	Feedback op versie 0.6 verwerkt
21-02-16	0.7	Bart Bosma	Feedback op versie 0.7
22-02-16	0.8	Dion Kruijswijk	Feedback op versie 0.7 verwerkt
23-02-16	0.8	Leonieke Mevius	Feedback op versie 0.8
23-02-16	0.8	Lucas Slim	Feedback op versie 0.8
23-02-16	0.9	Dion Kruijswijk	Feedback op versie 0.8 verwerkt
29-02-16	0.9	Bart Bosma	Feedback op versie 0.9
29-02-16	1.0	Dion Kruijswijk	Feedback op versie 0.9 verwerkt

Goedkeuring

Onderstaande personen zijn akkoord gegaan met het Plan van Aanpak.

Naam	Datum	Handtekening
Bart Bosma	2-3-2016	
Leonieke Mevius	2-3-2016	
Dion Kruijswijk	2-3-2016	

Inhoudsopgave

1.Inleiding

In dit Plan van Aanpak (PvA) wordt het afstudeeronderzoek naar het veilig toepassen van het Bring Your Own Device (BYOD) principe bij SURFsara beschreven. BYOD houdt in dat medewerkers hun eigen (privé) hardware meenemen om daarop vervolgens voor het bedrijf hun werkzaamheden te doen. Vaak is het niet bekend wat er precies op deze hardware staat waardoor data van SURFsara mogelijk besmet of beschadigd kan worden. Omdat BYOD steeds meer aangevraagd wordt en dit een aantal problemen zou kunnen oplossen, heeft SURFsara hiervoor een onderzoek gestart.

Voor BYOD is op dit moment de policy dat externe werknemers geen gebruik mogen maken van Virtual Private Network (VPN) software die normaal wel geïnstalleerd wordt. Dit is om te voorkomen dat besmettingen het netwerk opkomen. Echter, omdat de externe werknemers ook op afstand moeten kunnen werken, is het gewenst dat het wel mogelijk is om het VPN te gebruiken. Een onderdeel van het onderzoek is hoe dit veilig ingesteld kan worden op diverse besturingssystemen.

In dit PvA wordt het bedrijf SURFsara toegelicht, waarbij de werkplek en de rolverdeling vermeld worden. Daarna wordt de aanleiding van de opdracht beschreven waarin vermeld wordt waarom SURFsara het onderzoek heeft gestart. Vervolgens wordt de opdracht beschreven met de doelstellingen die behaald moeten worden, de scope van het project, de relatie met andere projecten, de randvoorwaarden en de grenzen van het onderzoek. Hierna wordt de aanpak beschreven waarin de hoofd- en deelvragen behandeld worden en de methoden die gebruikt worden om deze te beantwoorden. De producten die gemaakt worden, worden vermeld als deel- en eindproducten. Hieronder valt onder andere de Proof of Concept, het adviesrapport en de scriptie. Voor het project is tevens een planning gemaakt, waarin per product of tussenresultaat een begin-, einddatum en deadline voor beschreven is.

Om ervoor te zorgen dat het document alle eisen van de Hogeschool Utrecht (HU) bevat, is de waarborging van de kwaliteit beschreven. Hierna zijn de kosten beschreven van het onderzoek en als laatste welke risico’s er zijn tijdens het uitvoeren van het onderzoek.

2. Context

In dit hoofdstuk wordt de organisatie toegelicht waarvoor er onderzoek gedaan wordt. Tevens worden de rollen toegelicht.

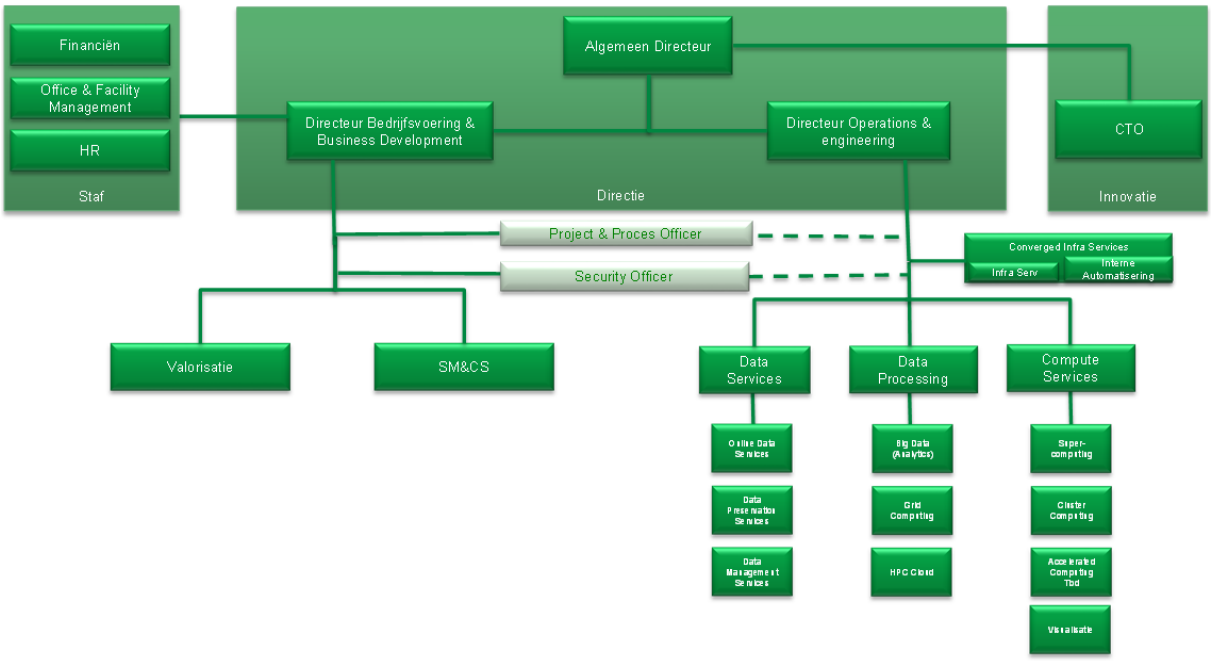
2.1 Organisatie

SURFsara is het nationale high-performance computing en e-science support center. SURFsara werd in 1971 opgericht door de Universiteit van Amsterdam, de Vrije Universiteit Amsterdam en de stichting Mathematisch Centrum als stichting Academisch Rekencentrum Amsterdam (SARA). De werkzaamheden van de stichting waren destijds gericht op dataverwerking voor de drie stichters. SARA maakt sinds 1 januari 2013 deel uit van de Coöperatie SURF U.A. en wordt sindsdien SURFsara genoemd. De SURF coöperatie helpt instellingen voor onderwijs en onderzoek bij het vormgeven van veranderingen tijdens ICT-trajecten.

Door de jaren heen is de dienstverlening van SURFsara uitgebreid en wordt van de voorzieningen van SURFsara gebruik gemaakt door andere onderzoeksinstituten en universiteiten. Sindsdien is de dienstverlening niet meer beperkt tot slechts dataverwerking, maar bevat ook rekentijd op supercomputers, dataopslag, visualisatie en netwerken. De rekentijd op supercomputers wordt gefaciliteerd voor wetenschappelijk onderzoek en onderwijs in Nederland. Steeds grotere en complexere modellen worden gebruikt tijdens wetenschappelijk onderzoek, waardoor er veel rekenkracht gebruikt wordt. De rekenkracht is vaak benodigd voor onderzoeken naar schone energie, klimaatverandering, watermanagement, geluidshinder en medische behandelingen.

Tegenwoordig biedt SURFsara een compleet pakket aan diensten, expertise en ondersteuning op het gebied van high-performance computing (HPC), data services, visualisatie, e-science support, clouddiensten en networking. SURFsara is gevestigd op het Amsterdam Science Park. (SURFsara, 2016)

SURFsara heeft verschillende afdelingen. Hoe de organisatie opgebouwd is en de samenhang tussen de verschillende afdelingen is te zien in Figuur 1: Organogram SURFsara.



FIGUUR 1: ORGANOGRAM SURFSARA

2.2 Werkplek

De stageplek is op de afdeling Interne Automatisering (IA). Deze afdeling is verantwoordelijk voor de kantoorautomatisering en voor de interne services (diensten ten behoeve van de externe dienstverlening). De afdeling bestaat uit zes medewerkers. Het hoofd van deze afdeling zal de taak van stagebegeleider op zich nemen.

2.3 Rolverdeling

Tijdens het project zijn er een aantal rollen die aangenomen worden. Deze rollen zijn: een projectmedewerker, een projectmanager en controleurs. De rollen worden in Tabel 1: Rol verdeling toegelicht.

Rol	Beschrijving
Projectmedewerker	De projectmedewerker is de persoon die het onderzoek uitvoert voor het bedrijf SURFsara. De projectmedewerker rapporteert periodiek aan de projectmanager over de voortgang.
Projectmanager / stagebegeleider	De projectmanager, tevens de opdrachtgever en stagebegeleider, begeleidt de projectmedewerker tijdens het uitvoeren van het onderzoek.
Controleur	De controleur bekijkt opgeleverde documenten waarbij er gekeken wordt naar de vastgestelde eisen voor de documentatie.

TABEL 1: ROL VERDELING

Elke rol kent een persoon die verantwoordelijk is voor de invulling van deze rol. In Tabel 2: Rol context zijn de personen beschreven die deze rollen vervullen en de bijbehorende context.

Rol	Naam	Context
Projectmedewerker	Dion Kruijswijk	Stagiair bij SURFsara en student bij de Hogeschool Utrecht.
Projectmanager / stagebegeleider	Leonieke Mevius	Hoofd van de afdeling Interne Automatisering van SURFsara en tevens de opdrachtgever.

Controleur	Leonieke Mevius	Hoofd van de afdeling Interne Automatisering van SURFsara en tevens de opdrachtgever.
Controleur	Bart Bosma	Docent van de Hogeschool Utrecht en tevens de docentenbegeleider.

TABEL 2: ROL CONTEXT

3. Aanleiding

SURFsara is een organisatie die zowel interne- als externe werknemers in dienst heeft. De externe werknemers maken vaak gebruik van eigen hardware (afhankelijk van de periode en intensiteit van hun inzet), maar vaak vereisen de werkzaamheden die zij uitvoeren toegang tot de data en/of applicaties binnen de organisatie. In 2015 zijn er 21 externe werknemers ingehuurd. Indien externe werknemers een laptop of tablet en een telefoon gebruiken, betekent dit dat zij 42 apparaten per jaar gebruiken waarvoor een veilige oplossing gevonden moet worden. Interne medewerkers nemen ook eigen hardware, zoals telefoons, mee. Deze apparaten moeten veilig toegelaten kunnen worden tot het netwerk van SURFsara.

Omdat de organisatie zelf geen enkele controle heeft over de hardware waarmee externe werknemers werken, kan niet gegarandeerd worden dat deze machines veilig op het netwerk aangesloten kunnen worden. Zo is er bijvoorbeeld geen controle op de virusscanners, updates en de aanwezigheid van disk-encryptie op deze machines.

Op dit moment wordt er gewerkt met VPN's voor zowel interne als externe werknemers. Via het VPN is het gehele netwerk bereikbaar. Het is de bedoeling dat externe werknemers niet zomaar deze VPN's kunnen gebruiken, omdat het niet bekend is wat er op de hardware geïnstalleerd is en virussen via het VPN verspreid kunnen worden. Momenteel zijn er geen controles op de hardware van de externe medewerkers. Gezien het groeiende aantal werknemers bij SURFsara en het aantal mensen dat met mobiele devices gaat werken, dient een oplossing gezocht te worden voor het veilig toepassing van het BYOD principe. Voor interne werknemers wordt bekeken of het mogelijk is dat in plaats van dat zij hardware van SURFsara krijgen, een budget vrijgemaakt wordt zodat werknemers zelf (niet-standaard) hardware aan kunnen schaffen. (Mevius, 2015)

4. De opdracht

In dit hoofdstuk wordt de opdracht behandeld waarbij de doelstellingen vermeld worden, de scope gedefinieerd wordt, de randvoorwaarden en grenzen beschreven worden en eventuele andere betrokken projecten vermeld worden.

4.1 BYOD veilig toepassen

Vanwege het toenemende aantal externe werknemers en de vraag naar BYOD door interne medewerkers, wordt voor SURFsara onderzocht hoe het BYOD-principe veilig toegepast kan worden. Hierbij wordt er rekening gehouden met de eisen en wensen van SURFsara. Aan de hand hiervan wordt een toepassingsselectie uitgevoerd. De toepassingsselectie bevat onderdelen van een pakketselectie, maar richt zich zowel op hard- en software als op aanpassingen in de huidige ICT-infrastructuur, zoals het toevoegen van VPN functies aan de bestaande VPN oplossing.

De toepassingsselectie wordt gedaan zodat in theorie bekend wordt welke programma's zouden moeten voldoen aan de eisen en wensen. Vervolgens wordt een Proof of Concept gedaan, waarin een aantal programma's getest worden in de praktijk.

4.2 Doelstellingen

De doelstellingen tijdens het onderzoek zijn: verschillende mogelijkheden onderzoeken om BYOD veilig toe te passen, een Proof of Concept uit te voeren en een advies te geven over de mogelijke oplossing(en). In het adviesrapport wordt de hoofdvraag beantwoord, onderbouwd met de deelvragen. Aan het eind van het onderzoek moet een passend advies gegeven worden over welke toepassing/oplossing het beste ingezet kan worden voor het veilig toepassen van het BYOD-principe. Tijdens het onderzoek wordt er rekening gehouden met de volgende eisen:

- De veiligheid binnen het interne netwerk van SURFsara moet gewaarborgd zijn, waarbij de vraag gesteld wordt: "Hoe kan gegarandeerd worden dat geen besmetting van bedrijfsdata plaats vindt vanuit bijvoorbeeld een geïnfecteerd werkstation?".
- Bedrijfsdata mag niet in handen vallen van mensen waarvoor deze informatie niet bestemd is in geval van verlies van data, een werkstation of mobiel apparaat.
- Privédata, inclusief eventuele bedrijfsmail van externe bedrijven, van de gebruiker die eigen hardware gebruikt moet beschermd/afgeschermd worden.
- Externe werknemers moeten gebruik kunnen maken van "Het nieuwe werken" (HNW, remote werken). Dit is in principe al mogelijk gemaakt voor de interne werknemers doormiddel van een VPN verbinding vanaf hun, door SURFsara verstrekte, hardware. Externe werknemers die niet in bezit zijn van SURFsara hardware moeten ook extern kunnen werken zonder in te leveren op het gebied van veiligheid. Daarnaast moeten zij ook via het draadloos netwerk kunnen werken.
- De oplossing(en) moet geschikt zijn voor verschillende besturingssystemen, waaronder Windows, Linux en Mac OS.
- De BYOD oplossing moet beheerd en bijgewerkt kunnen worden.
- Om te kunnen controleren of op de eigen hardware van externe medewerkers onder andere een virusscanner geïnstalleerd is, moet er gemonitord kunnen worden.
- Het BYOD principe moet conform de richtlijnen van de ISO27001 norm zijn.

Aan het eind van het onderzoek zijn deze eisen behandeld.

4.3 Scope

Voor het onderzoek is een scope gedefinieerd. Binnen de scope valt alles wat tijdens het onderzoek gedaan wordt in de periode van 1 februari 2016 tot en met 31 mei 2016. Buiten de scope bevat alles wat niet tijdens het onderzoek gedaan wordt.

Binnen de scope:

- De verschillende oplossingen voor het BYOD probleem onderzoeken.
- Het testen van de gevonden mogelijkheden met laptops, tablets en smartphones.
- Advies geven over de gevonden oplossing en de eventuele veranderingen of extra installaties die plaats moeten vinden indien de oplossing geïmplementeerd wordt.

Buiten de scope:

- Implementeren van een gevonden oplossing.
- Het testen van alle applicaties die gebruikt worden door externe werknemers, in combinatie met de gevonden oplossing.

4.4 Relatie met andere projecten

SURFsara is bezig om zich te certificeren voor ISO27001 (International Organization for Standardization, 2016). Dit is de internationale ISO standaard voor informatiebeveiliging. In deze ISO standaard komt onder andere gegevensbeveiliging aan bod. Tijdens het project wordt er rekening gehouden met deze ISO standaard.

4.5 Randvoorwaarden

Tijdens het onderzoek zijn er verschillende randvoorwaarden. De volgende randvoorwaarden zijn van toepassing tijdens het onderzoek:

- Vanuit SURFsara is voldoende begeleiding en informatie beschikbaar.
- De stagiair heeft een werkplek op het kantoor en kan door de weeks werken vanaf 8:00-18:00.
- De werkweek van de stagiair bedraagt 40 uur.
- De stagiair heeft toegang tot het gebouw en de werkplek.
- Er wordt periodiek overlegd met de docentenbegeleider over concepten van documentatie.
- Ingeleverde documentatie bij de docentenbegeleider wordt binnen zeven dagen nagekeken en feedback op gegeven.
- Overleg met de opdrachtgever is wekelijks of om de week mogelijk.
- Er moet rekening gehouden worden met de ISO27001 certificering.
- Er moet rekening gehouden worden met de volgende vertrouwelijkheids- en geheimhoudingsaspecten:
    - De Nederlandse wetgeving.
    - Het bedrijfs- en personeelsregelement van SURFsara.

Indien er wijzigingen aan de bovenstaande randvoorwaarden zijn, wordt er overlegd met de opdrachtgever over de alternatieven.

5. Aanpak

In dit hoofdstuk wordt de aanpak beschreven, waarbij de hoofd- en deelvragen behandeld worden. Voor deze vragen worden voorlopige methoden beschreven die gebruikt kunnen worden voor de beantwoording van deze vragen.

5.1 Hoofd- en deelvragen

De hoofdvraag voor het onderzoek is: “Welke methode is het meest geschikt om het Bring Your Own Device principe op een veilige en goed te beheren wijze toe te passen bij SURFsara, zodat de integriteit en de vertrouwelijkheid van SURFsara data en privédata gewaarborgd is?”. Deze hoofdvraag wordt tijdens het onderzoek beantwoord.

Ter ondersteuning en beantwoording van de hoofdvraag zijn de volgende deelvragen opgesteld:

Wat houdt het Bring Your Own Device principe voor SURFsara in?

Wat is het huidige beleid betreffende het Bring Your Own Device principe bij SURFsara?

Wat moet er veranderd worden aan het huidige beleid om het Bring Your Own Device principe toe te kunnen passen bij SURFsara?

Hoe kan voorkomen worden dat door geïnfecteerde Bring Your Own Device hardware bedrijfsdata besmet wordt?

Hoe kan de bedrijfsgevoelige of privédata van externe werknemers beschermd worden op hun eigen hardware?

Op welke manier kan de Bring Your Own Device hardware het best gemonitord worden?

5.2 Methoden

Om de deelvragen te beantwoorden worden methoden gebruikt. Een methode is een werkwijze waarmee informatie vergaard wordt. Deze informatie is benodigd om adequaat de vraag te beantwoorden. In dit hoofdstuk wordt per deelvraag de methoden beschreven die gebruikt worden.

Wat houdt het Bring Your Own Device principe voor SURFsara in?

Ter verduidelijking van het onderzoek wordt beschreven wat het Bring Your Own Device principe precies is. Hiervoor wordt er literatuur onderzoek gedaan, om te onderzoeken wat de definitie en de mogelijkheden van Bring Your Own Device zijn. Bij de mogelijkheden worden tevens kort de alternatieven voor BYOD vermeld en de afweging hiervoor. De afweging wordt beschreven aan de hand van een interview met de opdrachtgever.

Wat is het huidige beleid betreffende het Bring Your Own Device principe?

Om het huidige beleid in kaart te brengen worden diverse interviews gehouden. Deze interviews worden met de opdrachtgever, de security officer, externe werknemers en beheerders gehouden. Aan deze personen wordt gevraagd welke applicaties en data toegankelijk zijn en hoe momenteel het beleid voor BYOD is. De informatie uit de interviews wordt gebruikt ter vergelijking met de gevonden oplossing, waarbij een “AS-IS” analyse (Bridging the Gap, 2015) wordt gedaan. In de AS-IS situatie wordt de huidige situatie beschreven, met het beleid en de manier waarop gewerkt wordt.

Wat moet er veranderd worden aan het huidige beleid om het Bring Your Own Device principe toe te kunnen passen bij SURFsara?

De veranderingen die plaats moeten vinden om het BYOD principe toe te kunnen passen, worden beschreven aan de hand van de "TO-BE" analyse (Bridging the Gap, 2015). In de TO-BE situatie wordt de gewenste situatie beschreven, waarvoor de eisen en wensen in kaart gebracht worden. Hierin wordt het nieuwe beleid beschreven die conform de ISO27001 standaard is. De transitie van AS-IS naar TO-BE wordt ook beschreven, met eventuele aanpassingen die benodigd zijn om naar de gewenste situatie over te gaan. Voor de beantwoording van deze deelvraag wordt een enquête opgesteld en worden er interviews gehouden waarbij prioriteiten worden gegeven aan gewenste functies. Deze interviews en enquêtes worden gehouden met de opdrachtgever, de security officer en daarnaast een netwerkbeheerder om (extra) informatie te vergaren. Alle informatie wordt verwerkt in een Analyse van Eisen en kan vervolgens gebruikt worden delen van de KPMG pakketselectie (KPMG, 2010) voor de toepassingsselectie gebruikt. In de toepassingsselectie wordt als eerste een longlist gemaakt, waarbij een aantal mogelijke oplossingen bekeken worden. Aan de hand van de eisen en wensen wordt vervolgens een shortlist gemaakt van de producten die voldoen. De producten in de shortlist worden getest in een Proof of Concept (Techopedia, 2016).

Hoe kan voorkomen worden dat door geïnfecteerde Bring Your Own Device hardware bedrijfsdata besmet wordt?

Om te kunnen garanderen dat virussen, malware of andere besmettingen geen bedrijfsdata besmetten, wordt door middel van deskresearch gezocht naar manieren om BYOD veilig toe te passen. Deskresearch bevat het zoeken naar relevante soft- en hardware hiervoor en het bekijken van Best Practices. Hierbij wordt er rekening gehouden met de ISO27001 certificering die SURFsara wil behalen. In het Proof of Concept wordt bekeken wat voor impact er op de hardware en het netwerkverkeer is wanneer een toepassing gebruikt wordt.

Hoe kan de bedrijfsgevoelige of privédata van externe werknemers beschermd worden op hun eigen hardware?

Om bedrijfsgevoelige data van het externe ingehuurde bedrijf en/of privédata te beschermen, wordt gezocht welke regelingen omtrent bescherming van de gegevens van toepassing zijn. Hierbij wordt deskresearch gedaan waarbij bekeken wordt hoe de data beschermd kan worden.

Er wordt tevens onderzocht wat gedaan kan worden om te voorkomen dat bedrijfsdata in handen valt van personen waarvoor deze informatie niet bestemd is, in geval van verlies of diefstal. Daarnaast wordt onderzocht wat gedaan kan worden indien dit al gebeurd is. Hiervoor wordt deskresearch gedaan en een referentie-onderzoek waarbij gekeken wordt hoe andere bedrijven hier mee omgaan. In het Proof of Concept wordt bekeken wat gedaan kan worden in deze situatie.

Op welke manier kan de Bring Your Own Device hardware het best gemonitord worden?

Om te zorgen dat geïnfecteerde hardware niet zomaar het netwerk van SURFsara opkomt, wordt onderzocht hoe de BYOD hardware beheerd en gemonitord kan worden. Hiervoor wordt deskresearch gedaan waarbij tevens Best Practices bekeken worden. Daarnaast worden er interviews gehouden met de opdrachtgever en beheerders, zodat het bekend is wat gewenst is om te kunnen monitoren en te beheren. Hierbij wordt rekening gehouden met de wetgeving en wordt er advies gegeven over hoe dit het beste aangepakt kan worden wanneer iemand BYOD hardware wilt gebruiken. Welke monitoring en beheer mogelijkheden er zijn worden tijdens de Proof of Concept bekeken.

Interviews die vermeld zijn als methode voor de beantwoording van de deelvragen worden uitgewerkt in een interviewverslag. In een interviewverslag staat wie geïnterviewd wordt, wanneer het interview gehouden wordt, de vragen en de antwoorden op de vragen. De interviewverslagen worden na afloop van het interviews gemaild naar de betrokkenen, zodat de informatie gecontroleerd wordt. Hierna worden de interviewverslagen aan de opdrachtgever aangeboden, zodat deze de interviewverslagen kan controleren en eventueel op- en/of aanmerkingen erop kan geven.

In Tabel 4: Deelvraagmethoden worden de methoden per deelvraag nogmaals opgesomd.

Deelvraag	Methode
Wat houdt het Bring Your Own Device principe voor SURFsara in?	Literatuur onderzoek, interviews
Wat is het huidige beleid betreffende het Bring Your Own Device principe?	Interviews
Wat moet er veranderd worden aan het huidige beleid om het Bring Your Own Device principe toe te kunnen passen bij SURFsara?	Enquête, interviews, toepassingsselectie
Hoe kan voorkomen worden dat door geïnfecteerde Bring Your Own Device hardware bedrijfsdata besmet wordt?	Deskresearch, Proof of Concept
Hoe kan de bedrijfsgevoelige of privédata van externe werknemers beschermd worden op hun eigen hardware?	Deskresearch, referentie onderzoek, Proof of Concept
Op welke manier kan de Bring Your Own Device hardware het best gemonitord worden?	Deskresearch, interviews, Proof of Concept

TABEL 4: DEELVRAAGMETHODEN

6. Producten

Tijdens het onderzoek worden diverse producten gemaakt. Deze producten worden verdeeld in deel- en eindproducten. De deelproducten zijn ter ondersteuning van de eindproducten. Per product wordt een indicatie gegeven van hoeveel tijd er benodigd is voor het opstellen van de documenten, inclusief informatie verzamelen, en het verwerken van de informatie. Alle documenten worden ter review aangeboden aan de opdrachtgever zodat de kwaliteit gewaarborgd is. De producten zijn op volgorde weergegeven en zijn van elkaar afhankelijk.

6.1 Deelproducten

De deelproducten die tijdens het onderzoek gemaakt worden, zijn in Tabel 5: Deelproducten weergegeven:

Product of tussenresultaat	Beschrijving	Benodigde uren
Analyse van Eisen	De AS-IS en TO-BE situaties worden beschreven waarbij de eisen en wensen geïnventariseerd worden ter voorbereiding van de toepassingsselectie. Er worden waardes toegewezen aan de eisen en wensen zodat deze in de toepassingsselectie gebruikt kunnen worden.	30
Toepassingsselectie	Pakketselectie waarbij zowel hard- en software als extensies onderzocht worden. Hieruit wordt duidelijk welke producten in theorie geschikt zijn voor SURFsara, rekening houdend met de eisen en wensen. Een long- en shortlist worden opgezet van de gevonden oplossingen. Dit is het vooronderzoek voor de Proof of Concept.	30
Proof of Concept	In een testomgeving de shortlist van de toepassingsselectie testen om te bevestigen of deze aan de eisen en wensen voldoen in de praktijk.	40

TABEL 5: DEELPRODUCTEN

6.2 Eindproducten

De producten die aan het eind van het onderzoek opgeleverd worden, zijn in Tabel 6: Eindproducten beschreven.

Eindproduct	Beschrijving	Benodigde uren
Adviesrapport	Document waarin advies gegeven wordt over welk(e) product(en) gebruikt zou kunnen worden om het probleem op te lossen en wat gedaan moet worden om het product toe te kunnen passen.	40
Scriptie	Document waarin het traject beschreven wordt vanaf het begin van het onderzoek tot aan hoe er aan het eindresultaat gekomen is, waarbij tevens de hoofd- en deelvragen beantwoord worden. Een deel uit het adviesrapport komt hierin voor.	40
Presentatie SURFsara	Presentatie voor SURFsara waarbij het onderzoek en één of meerdere producten toegelicht worden. Delen uit het adviesrapport komen hierin voor.	10
Presentatie Hogeschool Utrecht	Presentatie voor de Hogeschool Utrecht, waarbij het onderzoek toegelicht wordt vanaf de aanleiding van het onderzoek tot aan het eindresultaat. Delen van de scriptie komen hierin voor.	10

TABEL 6: EINDPRODUCTEN

7. Planning

Voor het onderzoek naar het toepassen van het BYOD-principe, wordt een planning gehanteerd. Deze planning bestaat uit de op te leveren producten of tussenresultaat en een tijdsindicatie wanneer er hieraan gewerkt wordt. Deze tijdsindicatie bestaat uit een begin- en einddatum. Het is mogelijk dat een product of eindresultaat uitloopt, hiervoor is een deadline gesteld. Het streven is dat de deadline behaald wordt, zodat er geen vertraging opgelopen wordt. Voor de opzet van de planning is gebruikt gemaakt van de afstudeerleidraad (Utrecht, 2015).

De producten of tussenresultaten worden verdeeld in drie fases. Deze fases zijn verdeeld in: de initiatiefase, de definitiefase en de uitwerkingsfase. In de initiatiefase worden de mogelijkheden onderzocht, waarbij het Plan van Aanpak beschreven en afgerond wordt en gewerkt wordt aan de scriptie. Hierna begint de definitiefase waarbij de producten getest worden in een Proof of Concept en de scriptie verder uitgewerkt wordt. Als laatste is de uitwerkingsfase, hierin wordt het project afgerond met een adviesrapport, een definitieve scriptie en de afstudeerzitting. Een aantal producten zijn mijlpalen tijdens het project, deze zijn; de definitieve versie van het Plan van Aanpak, de uitwerkingen van de Proof of Concept en de definitieve scriptie. De planning wordt in Tabel 7: Planning weergegeven.

Fase / mijlpalen	Product of tussenresultaat	Begindatum	Einddatum	Deadline
Fase 1: Initiatie	Inventarisatie probleemstelling	1 februari 2016	12 februari 2016	19 februari 2016
	Concept Plan van Aanpak	8 februari 2016	19 februari 2016	26 februari 2016
	Onderzoek oplossing BYOD-principe (pakketselectie)	22 februari 2016	4 maart 2016	11 maart 2016
	Feedback verwerken Plan van Aanpak	7 maart 2016	11 maart 2016	18 maart 2016
Mijlpaal	Inleveren definitieve Plan van Aanpak	14 maart 2016	18 maart 2016	18 maart 2016
	1e concept scriptie	21 maart 2016	1 april 2016	8 april 2016
Fase 2: Definitie	Testen pakketten in een Proof of Concept	4 april 2016	15 april 2016	22 april 2016
Mijlpaal	Uitwerken resultaten Proof of Concept	11 april 2016	22 april 2016	29 april 2016
	2e concept scriptie	25 april 2016	6 mei 2016	13 mei 2016
Fase 3: Uitwerking	Adviesrapport	2 mei 2016	13 mei 2016	20 mei 2016
	Feedback verwerken scriptie	16 mei 2016	20 mei 2016	27 mei 2016
Mijlpaal	Inleveren definitieve scriptie	23 mei 2016	27 mei 2016	27 mei 2016
	Voorbereiden afstudeerzitting	30 mei 2016	7 juni 2016	17 juni 2016
	Afstudeerzitting	7 juni 2016	17 juni 2016	17 juni 2016

TABEL 7: PLANNING

Wanneer het blijkt dat een product of tussenresultaat eerder voltooid wordt dan de einddatum, wordt er aan het volgende product of tussenresultaat gewerkt.

8. Kwaliteit

Om de kwaliteit van het onderzoek te waarborgen, worden diverse controles gebruikt. Deze controles zijn:

- Gebruik van het boek “leren communiceren”

Tijdens het opstellen van producten zoals het Plan van Aanpak en de scriptie, wordt gebruik gemaakt van de richtlijnen uit het boek “Leren communiceren”. Deze richtlijnen zijn van toepassing op onder andere documenten en presentaties. (Steehouder, Jansen, Mulder, van der Pool, & Zeijl, 2011)

- Periodiek overleg met de opdrachtgever

Om te controleren of tijdens het project naar de correcte oplossing voor het probleem gezocht wordt, wordt er periodiek overlegd met de opdrachtgever. Er vindt wekelijks overlegd plaats, waarbij over de voortgang van het onderzoek gesproken wordt. Indien gewenst kan er op andere moment vragen gesteld worden of overleg plaats vinden.

- Controle van het Plan van Aanpak en de scriptie door de Hogeschool Utrecht

Om de kwaliteit van het Plan van Aanpak en de scriptie te waarborgen, worden er voor de deadline concepten opgesteld. Deze concepten worden gecontroleerd door de HU of deze volgens de richtlijnen zijn. Hierbij wordt tevens door de HU gecontroleerd of het PvA alle eisen bevat en wat er nog ontbreekt.

- Controle van interviewverslagen

Wanneer interviewverslagen geschreven worden, worden deze eerst opgestuurd naar de geïnterviewde om te controleren of de informatie die verkregen is op de correcte manier geïnterpreteerd is. Wanneer de informatie correct blijkt, wordt daarna het interviewverslag naar de opdrachtgever gestuurd en wordt het besproken. Hierdoor wordt gecontroleerd of de informatie relevant is voor het onderzoek, zodat deze informatie gebruikt kan worden.

9. Kosten

De stagevergoeding bedraagt €500,- per maand. Naar verwachting zijn er verder geen kosten tijdens het onderzoek voor de opdrachtgever. De kosten van eventuele software bedraagt €0,-, omdat er gebruik gemaakt wordt van een evaluatie of open source licenties wanneer een product getest moet worden. Indien blijkt dat er extra kosten gemaakt moeten worden, wordt dit eerst besproken met de stagebegeleider.

De stage loopt van 1 februari 2016 tot en met 31 mei 2016, een periode van vier maanden.

10. Risico's

Tijdens het onderzoek kunnen er zich omstandigheden voordoen die tot vertraging kunnen leiden. Dit brengt een zeker risico met zich mee. Een aantal risico's zijn bekend en daar kan preventief actie op worden ondernomen. Deze risico's zijn in Tabel 8: Risico's weergegeven:

Risico	Preventieve actie
Het beeld van de opdracht is bij de opdrachtgever en de stagiair verschillend.	Er vinden wekelijkse vergaderingen plaats waarbij de opdracht en de voortgang besproken wordt. De gemaakte documentatie wordt ter review aangeboden.
Het onderzoek, of onderdelen hiervan, wordt niet afgerond voor de deadline.	In de planning worden de deadlines duidelijk beschreven. Vertraging wordt hierdoor voorkomen.
Benodigde informatie voor het project wordt niet bekend of verstrekt.	Om problemen te voorkomen of op te lossen wordt dit tijdig aangegeven bij de betrokkenen. Eventueel wordt de projectleider geïnformeerd.
De projectscope is onduidelijk.	De projectscope wordt afgebakend in overleg met de opdrachtgever. Tevens wordt het PvA ondertekend, waardoor misverstanden beperkt worden.
Het Plan van Aanpak wordt niet goedgekeurd.	Van te voren met de docentbegeleider en de stagebegeleider concepten doornemen, zodat het PvA alle vastgestelde eisen bevat. Daarnaast kan gebruik gemaakt worden van de richtlijnen in de afstudeerleidraad.
De onderzochte oplossing blijkt niet aan te sluiten bij de eisen en wensen van de organisatie.	Tijdens het onderzoek met betrokkenen bespreken waaraan de oplossing moet voldoen en eventuele wensen in kaart brengen.
De onderzochte oplossing kan niet toegepast worden in de huidige infrastructuur.	Onderzoek doen naar de huidige infrastructuur en dit meenemen in de afweging tijdens de toepassingsselectie. Eventueel advies doen voor aanpassingen aan de infrastructuur.
Het testen van een oplossing voor het BYOD-principe is niet mogelijk of niet representatief, vanwege te weinig hard- of software.	Er moet verschillende hard- en software (o.a. diverse laptops met besturingssystemen) zijn. Bespreken met de opdrachtgever welke hard- en software tijdens de Proof of Concept getest kan worden.
Evaluatie-licenties zijn niet beschikbaar voor producten of bezitten niet de gewenste functies die getest moeten worden voor het onderzoek in de Proof of Concept.	Tijdens de toepassingsselectie bekijken wat de mogelijkheden zijn, indien nodig contact opnemen met de leverancier. Anders een alternatief zoeken voor het product.
Referentieonderzoek is niet mogelijk of het is niet bekend waar dit gedaan kan worden.	Met de opdrachtgever de mogelijkheden bekijken om het referentieonderzoek uit te voeren. Indien nodig slechts contact per mail

	met bedrijven die het BYOD-principe hebben toegepast.
De gevonden oplossing is beperkt in het aantal gebruikers, waardoor deze slechts voor een selecte groep gebruikt kan worden.	Tijdens het onderzoek overleggen over een indicatie van hoeveel gebruikers ondersteund moeten worden. Daarnaast wordt er rekening gehouden met eventuele groei en interne medewerkers die ook gebruik willen maken van dezelfde oplossing.
Wekelijkse opdrachtgeversgesprekken gaan niet door.	Van te voren overleggen op welke dag het overleg plaats vindt. Indien de afspraak verplaatst moet worden, wordt er overlegd of dit nog in dezelfde week kan. In ieder geval elke twee weken vind er overleg plaats. Daarnaast een tweede contactpersoon aanwijzen die in geval van nood tijdelijk de rol van opdrachtgever aan kan nemen.
De docentbegeleider of de bedrijfsbegeleider kunnen het PvA niet ondertekenen.	Van te voren wordt besproken dat het PvA ondertekend moet worden. Hiervoor wordt er voor de deadline een afspraak ingepland.

TABEL 8: RISICO'S

11. Contactgegevens

11.1 SURFsara

Naam:	Leonieke Mevius
Functie:	Opdrachtgever / Bedrijfsbegeleider
E-mail adres:	leonieke.mevius@surfsara.nl
Telefoonnummer:	020-8001300

Naam:	Sedat Capkin
Functie:	Security Manager

Naam:	Lucas Slim
Functie:	Systeem Programmeur Afdeling IA

Naam:	Paul Reemeijer
Functie:	Tweede contactpersoon in geval van afwezigheid bedrijfsbegeleider

11.2 Hogeschool Utrecht

Naam:	Bart Bosma
Functie:	Docentenbegeleider / Tweede examinator
E-mail adres:	bart.bosma@hu.nl
Telefoonnummer:	06-45488356

Naam:	Lex Borger
Functie:	Eerste examinator
E-mail adres:	lex.borger@hu.nl
Telefoonnummer:	N.v.t.

Naam:	Dion Kruijswijk
Functie:	Stagiair
E-mail adres:	dion.kruijswijk@student.hu.nl
Telefoonnummer:	06-47918260

12. Afkortingenlijst

Afkorting	Betekenis
AS-IS	Methode afkorting voor de huidige situatie
BYOD	Bring Your Own Device, waarbij werknemers eigen hardware gebruiken om op te werken.
HNW	Het nieuwe werken, waarbij er remote gewerkt wordt.
HPC	High-performance computing
HU	Hogeschool Utrecht
IA	Afkoring voor de afdeling Interne Automatisering
PvA	Plan van Aanpak
SARA	Stichting Academisch Rekencentrum Amsterdam
TO-BE	Methode afkorting voor de gewenste situatie
VPN	Afkorting voor Virtual Private Network

13. Literatuurlijst

Diogenes, Y., Gilbert, J. (2015) Enterprise Mobility Suite – Managing BYOD and Company-Owned Devices. Microsoft Press.

In het boek “Enterprise Mobility Suite – Managing BYOD and Company-Owned Devices” wordt de Microsoft manier beschreven waarop BYOD toegepast kan worden. Hierin wordt het principe BYOD uitgelegd met de uitdagingen die kunnen plaatsvinden bij het implementeren hiervan. Het pakket dat Microsoft gebruikt, de Enterprise Mobility Suite, wordt als leidraad gebruikt om verschillende voorbeelden aan te halen en uit te leggen hoe het BYOD-principe door een Microsoft oplossing geïmplementeerd kan worden.

Nicol, D. (2013) Mobile Strategy – How your company can win by embracing Mobile Technologies. IBM Press.

De uitdagingen en veiligheidsaspecten van onder andere het BYOD-principe worden in het boek “Mobile Strategy – How your company can win by embracing Mobile Technologies” beschreven. Hierin wordt onder andere Mobile Device Management, Mobile Network Management en Mobile Application Management beschreven inclusief de beveiliging hiervan. In het boek wordt ook behandeld waar er op gelet kan worden voor de toepassing van het BYOD-principe.

BCS (2015) Bring Your Own Device – The mobile computing challenge. BCS, The Chartered Institue for IT.

In het boek “Bring Your Own Device – The mobile computing challenge” worden de voordelen van het toepassing van BYOD beschreven, waarbij er advies gegeven wordt om de risico’s te minimaliseren.

14. Bibliografie

AD. (2016, 04 11). *Advertenties op honderden grote sites kort tijd besmet*. Opgehaald van AD.nl: http://www.ad.nl/ad/nl/38261/Nieuws/article/detail/4279992/2016/04/11/Advertenties-op-honderden-grote-sites-korte-tijd-besmet.dhtml

Bridging the Gap. (2015, 03 17). *As-is Business process*. Opgehaald van Bridging-the-gap.com: http://www.bridging-the-gap.com/as-is-business-process/

Bridging the Gap. (2015, 10 10). *To-be Business process*. Opgehaald van Bridging the Gap.com: http://www.bridging-the-gap.com/to-be-business-process/

CFEngine. (2016, 02 23). *Product*. Opgehaald van CFEngine: https://cfengine.com/product/

Computable. (2004, 04 16). *Traditionele antivirus-oplossingen voldoen niet meer*. Opgehaald van Computable.nl: https://www.computable.nl/artikel/achtergrond/security/1384342/1444691/traditionele-antivirus-oplossingen-voldoen-niet-meer.html

Faronics. (2014, 10 01). *Best practices malware protection prevention*. Opgehaald van Faronics.com: http://www.faronics.com/news/blog/best-practices-malware-protection-prevention/

Gartner. (2015, 07 23). *bring-your-own-device*. Opgehaald van Gartner.com: http://www.gartner.com/it-glossary/bring-your-own-device-byod

Gartner. (2015, 09 08). *Mobile Device Management mdm*. Opgehaald van Gartner.com: http://www.gartner.com/it-glossary/mobile-device-management-mdm

Gartner. (2015, 10 02). *Network Access Control (NAC)*. Opgehaald van Gartner.com: http://www.gartner.com/it-glossary/network-access-control-na

Gartner. (2015, 11 23). *virtual-desktop-infrastructure-vdi*. Opgehaald van Gartner.com: http://www.gartner.com/it-glossary/virtual-desktop-infrastructure-vdi

Gartner. (2016, 02 01). *Magic Quadrant for Endpoint Protection Platforms*. Opgehaald van Gartner: https://www.gartner.com/doc/reprints?id=1-2XU816T&ct=160203

Gemeente Utrecht. (2016, 03 30). Enquête Bring Your Own Device Gemeente Utrecht - Richardo Theben Tervile.

Ijcaonline. (2014, 11). *A review of Opensource Network Access COntrol*. Opgehaald van research.ijcaonline.org: http://research.ijcaonline.org/volume106/number6/pxc3899721.pdf

IJcaonline. (2014, 11). *A review of Opensource Network Access COntrol*. Opgehaald van research.ijcaonline.org: http://research.ijcaonline.org/volume106/number6/pxc3899721.pdf

International Organization for Standardization. (2016, 02 08). *iso27001*. Opgehaald van iso.org: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

KPMG. (2010, 12 31). *0208_KPMG.* Opgehaald van itinbedrijf: http://itinbedrijf.info/0208_KPMG.pdf

Mevius, L. (2015, 11 02). Veilige toepassing van BYOD.

Nagios. (2016, 05 05). *Nagios*. Opgehaald van Nagios.org: https://www.nagios.org/

NEN. (2013). NEN-ISO/IEC 27001. *Ionformation technology - Security techniques - Information secuirty management systems - Requirements (ISO/IEC 27001:2013,IDT)*, 1-23.

Paessler. (2016, 04 23). *PRTG*. Opgehaald van passler.com/prtg: https://www.paessler.com/prtg

Sophos. (2015, 05 10). *Top 5 threat protection best practices*. Opgehaald van Sophos.com: https://www.sophos.com/en-us/security-news-trends/security-trends/top-5-threat-protection-best-practices.aspx

Stedehouder, J. (2012, 09 02). *byod-een-balans-tussen-controle-en-vrijheid*. Opgehaald van bringyourowndevice.wordpress: https://bringyourowndevice.wordpress.com/2012/09/02/byod-een-balans-tussen-controle-en-vrijheid/

Steehouder, M., Jansen, C., Mulder, J., van der Pool, E., & Zeijl, W. (2011). *Leren communiceren.* Noordhoff Uitgevers.

SURFsara. (2015, 11 11). *AUP SURF v1 def.* Opgehaald van intranet.surfsara.nl: https://intranet.surfsara.nl/argos/attachment/wiki/Beleid/AUP%20SURF%20V1%20def.pdf

SURFsara. (2015, 12 16). *Manual Linux Tips Tricks*. Opgehaald van intranet.surfsara.nl: https://intranet.surfsara.nl/ka/wiki/ManualLinuxTipsTricks

SURFsara. (2016, 03 23). *ManualMac*. Opgehaald van intranet.surfsara.nl: https://intranet.surfsara.nl/ka/wiki/ManualMac

SURFsara. (2016). *over-surfsara*. Opgehaald van surf.nl: https://www.surf.nl/over-surf/werkmaatschappijen/surfsara/over-surfsara/index.html

Techopedia. (2016, 01 28). *Proof of concept poc.* Opgehaald van techopedia: https://www.techopedia.com/definition/4066/proof-of-concept-poc

TechTarget. (2007, 06). *Defense in depth*. Opgehaald van searchsecurity.techtarget.com: http://searchsecurity.techtarget.com/definition/defense-in-depth

TechTarget. (2015, 04). *Comparing the top SSL VPN products*. Opgehaald van searchsecurity.techtarget.com: http://searchsecurity.techtarget.com/feature/Comparing-the-top-SSL-VPN-products

Utrecht, H. (2015, 11 04). *Afstuderen.* Opgehaald van sharepoint.hu.nl: https://onderwijsteams.sharepoint.hu.nl/fnt/Cluster_ICT/afstuderen/Belangrijke%20documenten1/Afstudeerleidraad%20Instituut%20voor%20ICT%20cursus%202015-2016.pdf

Bijlage 2: Toepassingsselectie

Analyse van Eisen

In dit hoofdstuk worden de huidige situatie (AS-IS) en de gewenste situatie (TO-BE) beschreven. In de AS-IS wordt de huidige situatie met het beleid beschreven. Voor de TO-BE situatie worden de eisen en wensen van SURFsara geanalyseerd zodat bekend is wat er aan het eind van het onderzoek behaald moet worden. Daarnaast wordt de transitie tussen de AS-IS en TO-BE situatie beschreven. De eisen en wensen zijn verkregen door overleg met de opdrachtgever en interviews met eventuele belanghebbende (beheerders, gebruikers etc.). De eisen en wensen worden gebruikt in de toepassingsselectie om te onderzoeken welke producten het BYOD-principe veilig toe kunnen passen.

Huidige situatie (AS-IS)

Een deel van het “Choose Your Own Device” principe wordt momenteel (AS-IS) bij SURFsara toegepast, waarbij interne medewerkers uit een beperkt aantal laptops of desktops kunnen kiezen. Voor CYOD is er geen beleid opgesteld met regels waar werknemers zich aan moeten houden. Bij het CYOD principe kan er gekozen worden uit een beperkt aantal laptops, waarmee werknemers ook thuis kunnen werken. Hierbij wordt er een keuze gemaakt tussen het besturingssysteem dat op de laptop of desktop wordt geïnstalleerd. In geval van een Windows laptops wordt de laptop deels beheerd door de tool CFEngine. CFEngine is een configuratie management en automatiseringsframework waarmee de IT infrastructuur beheerd kan worden (CFEngine, 2016). Door het gebruik van deze tool, worden instellingen en applicaties regelmatig automatisch gecontroleerd en indien deze niet ingesteld zijn geïnstalleerd. Hierdoor is er een hoge mate van controle door de beheerders. Het is mogelijk om zelf applicaties te installeren op de hardware, doordat gebruikers administrator rechten hebben. Mac en Linux systemen worden niet beheerd. Voor zowel Mac (SURFsara, 2016) als Linux (SURFsara, 2015) systemen zijn de volgende richtlijnen voor het gebruik opgesteld:

- Gebruik van disk encryptie.
- Gebruik van een virusscanner.
- Inloggen met een wachtwoord.
- Na tien minuten inactiviteit automatisch de screensaver met wachtwoordbeveiliging inschakelen.

Deze richtlijnen zijn bedoeld voor de CYOD hardware.

Het is de bedoeling dat deze BYOD hardware niet zomaar toegelaten wordt tot het netwerk van SURFsara. Hiervoor zijn twee uitzonderingen gemaakt voor het toelaten van BYOD hardware, namelijk het gebruik van twee voor BYOD hardware bedoelde Wi-Fi netwerken. Er is een SURFsara gastenlan en Eduroam waar bezoekers eventueel gebruik van kunnen maken. Werknemers maken van beide draadloze netwerken ook gebruik. Eduroam is een veilig draadloos netwerk dat gebruikt kan worden door werknemers en studenten van onderwijs- of onderzoeksinstellingen. Indien bijvoorbeeld leveranciers toegelaten moeten worden tot het netwerk van de supercomputer, wordt hiervoor een oplossing bedacht. Deze oplossing is meestal het opzetten van een nieuw netwerksegment of vlan. In het aparte netwerk gelden strikte en beperkte toegangsregels. In alle andere gevallen is het alleen toegestaan dat BYOD hardware gekoppeld wordt met de daarvoor bedoelde Wi-Fi netwerken.

Zowel interne als een aantal externe werknemers maken gebruik van VPN mogelijkheden om van afstand te verbinden met een netwerk van SURFsara. Momenteel worden er geen controles uitgevoerd, waardoor het niet bekend is wanneer hardware besmet is. Indien de hardware besmet is, kan zodoende bedrijfsdata van SURFsara besmet worden. Het is gewenst dat hier verandering in komt, zodat risico's beperkt worden.

Gewenste situatie (TO-BE)

Om te bepalen wat de gewenste situatie (TO-BE) wordt voor het toepassen van het BYOD-principe, worden de eisen en wensen geïnventariseerd. Aan de hand hiervan moet er een beleid opgesteld worden. Slechts met beleid kan het BYOD principe niet opgelost worden, waardoor er een technische oplossing (product) moet komen om het beleid te ondersteunen. De eisen zijn functies waaraan het product moet voldoen. De wensen zijn functies waarbij het optioneel is dat ze in het pakket inbegrepen zijn. De wensen kunnen een waarde hebben van één of twee, waarbij één '*niet erg belangrijk*' is en twee '*matig belangrijk*' is. De eisen hebben standaard een hogere waarde dan de wensen. De eisen kunnen een waarde hebben van drie, vier of vijf, waarbij drie '*redelijk belangrijk*' is, vier '*belangrijk*' is en vijf '*erg belangrijk*' is. Deze waardes zijn bepaald in overleg met de opdrachtgever en worden vermenigvuldigd aan het eind van de toepassingsselectie om te bepalen welke producten het beste voldoen. De eisen en wensen zijn in twee opsommingen weergegeven. De eisen zijn als volgt bepaald met de waardes:

- Open Source – Waarde 3
- Ondersteuning verschillende besturingssystemen – Waarde 4 (o.a. Windows, Linux en Mac OS)
- Eenvoudig in gebruik – Waarde 4 (Snel en duidelijk toegang voor eind gebruikers)
- Passend binnen de beheeromgeving – Waarde 4 (Gebruik maken van de huidige OS-en)
- Bedrijfsdata niet lokaal op externe hardware – waarde 5
- Besmettingsgevaar minimaliseren / virusscanners - Waarde 5
- Back-up van data – Waarde 5
- Netwerkbeveiliging – Waarde 5
- Continuïteit – Waarde 5

Naast de eisen, zijn de wensen:

- Offline mogelijkheden – Waarde 2

Transitie tussen AS-IS en TO-BE

Om de transitie mogelijk te maken van de AS-IS situatie naar de TO-BE situatie, wordt er gekeken wat er gedaan moet worden om de gewenste situatie mogelijk te maken. Hierbij voor wordt als eerst bekeken welke producten aan de eisen en wensen voldoen. Wanneer dit bekend is, kan er bekeken worden wat er veranderd moet worden in het beleid ten opzichte van de huidige situatie. Welke producten precies gebruikt zouden kunnen worden, wordt in de toepassingsselectie beschreven. Voor het beleid moet er rekening gehouden wordt met de ISO27001 standaard. Het beleid moet bevatten wat de gebruikers die BYOD willen gebruiken kunnen verwachten en waarvoor hun wel of niet aansprakelijk zijn.

Toepassingsselectie

In dit hoofdstuk wordt de toepassingsselectie voor het veilig toepassen van het BYOD-principe weergegeven. De toepassingsselectie is een toepassingsselectie waarbij zowel hard- en software als extensies bekeken worden die mogelijk het BYOD-principe veilig toe kunnen passen.

Tijdens het onderzoek zijn er een aantal producten gevonden die voor SURFsara geschikt kunnen zijn. De producten zijn uit de volgende categorieën:

- Virtual Desktop Infrastructure (VDI)
- Secure Sockets Layer (SSL) Virtual Private Network (VPN)
- Network Access Control (NAC)

VDI is het draaien van desktop omgevingen als virtuele machines op een virtuele omgeving. Hierbij is er een omgeving waarbij gebruikers toch alle mogelijkheden kunnen hebben van een normale desktop (Gartner, 2015). Een SSL VPN is een VPN waarbij versleuteling wordt toegepast om netwerk verkeer veilig te transporteren tussen twee locaties (TechTarget, 2015). NAC is het toepassen van beleidsregels in het netwerk voor de toegangscontrole van hardware en gebruikers. (Gartner, 2015) NAC wordt vaak gebruikt in combinatie met Mobile Device Management (MDM), sommige producten hebben MDM in het NAC pakket zitten en anderen moeten door MDM aangevuld worden. MDM is het gebruik maken van software distributie, policy management, security management en service management voor smartphones en tablets. (Gartner, 2015)

Deze producten worden als eerst in een tabel uiteengezet waarin gekeken wordt welke functies het product uit de Analyse van Eisen bevat. Indien hieruit blijkt dat het product voldoet aan de eisen en wensen, wordt het product vervolgens nogmaals in een tabel uitgezet. Wanneer er te veel functies niet ondersteund worden, valt het product af. Het is mogelijk dat wanneer een combinatie van producten gemaakt kan worden waardoor wel alles ondersteund wordt, dit met de opdrachtgever overlegd wordt. De tabel waarin de functies bekeken worden, wordt de longlist genoemd. Het is mogelijk dat de opdrachtgever een bepaald product zou willen testen ook al voldoet deze niet, indien dit zo is wordt dit aangegeven.

Naast de longlist, is er ook een shortlist. Hierin wordt er in een tabel bekeken welke prioriteit een functie heeft (hoe erg het gewenst is) en hoe goed het product deze functies ondersteund. De beste producten worden vervolgens getest in de Proof of Concept.

De volgende producten worden in deze toepassingsselectie uiteengezet:

- VDI
  1. Ulteo Open Virtual Desktop
  2. Dell vWorkspace
  3. VMWare Horizon View + Flex
  4. Citrix Workspace Suite
- SSL VPN
  5. OpenVPN python integratie
  6. Juniper firewall VPN instellingen
  7. Cisco ASA VPN instellingen
- NAC
  8. PacketFence
  9. OpenNAC
  10. Cortado Corparate Server

11. ForeScout CounterACT

Longlist

Om te bekijken welke pakketten de functies bevatten die gewenst zijn en beschreven zijn in de gewenste situatie van de Analyse van Eisen, wordt dit in een tabel gezet. Voor de producten worden bekeken of ze de functie (V) bezitten. De longlist wordt hieronder weergegeven.

Product	Offline mogelijkheden (2)	Open Source (3)	Ondersteuning besturingssystemen (4)	Eenvoudig in gebruik (4)	Passend binnen de beheer omgeving (4)	Bedrijfsdata niet lokaal (5)	Besmettingsgevaar minimaliseren (5)	Back-up van data (5)	Netwerkbeveiliging (5)	Waarborging continuïteit (5)
Ulteo Open Virtual Desktop		V	V	V	V	V	V	V	V	V
Dell vWorkspace	V		V	V	V	V	V	V	V	V
VMWare Horizon View + Flex	V*		V	V		V	V	V	V	V
Citrix Workspace Suite			V	V		V	V	V	V	V
OpenVPN python intergratie	V	V	V	V	V		V		V	V
Juniper firewall VPN instellingen	V		V	V			V		V	V
Cisco ASA VPN instellingen	V		V	V			V		V	V
Packetfence	V	V	V	V	V		V		V	
OpenNAC	V	V	V	V	V		V		V	
Cortado Corparate Server	V		V	V	V		V		V	
ForeScout CounterACT	V		V	V			V		V	

V*) Offline mogelijkheden zijn alleen mogelijk als er naast VMWare Horizon View ook VMWare Horizon Flex gebruikt wordt om offline/local desktops mogelijk te maken.

Uit de longlist valt op te maken dat geen producten zijn die volledig voldoen. Echter is dit vaak op het vlak een eis of wens op het gebied van waarde twee en drie. De producten die één van de twee lage waardes hebben, worden in de shortlist nader onderzocht. De producten die het beste uit de vergelijking zijn gekomen zijn:

- Ulteo Open Virtual Desktop
- Dell vWorkspace

De opdrachtgever heeft aangegeven interesse te hebben in een NAC pakket. PacketFence en OpenNAC scoren beide het beste uit de vier mogelijkheden. Om hier één keuze uit te maken, is er gekozen om gebruik te maken van een onafhankelijke bron. Deze bron, ijcaonline, heeft een vergelijking gemaakt tussen drie producten. Twee van de drie producten zijn PacketFence en OpenNAC.

Features	**OpenNAC**	**PacketFence**	**FreeNAC**
Posture Analysis	Fairly	Yes	Not inherent
Contrivance Authentication	Yes	Yes	Yes
Bandwidth Management	No	Yes	No
Network vendor	Multivendor	Multivendor	Multivendor

support			
Wired and wireless support	Yes	Yes	Yes
Software Integration	Yes	Yes	Commercial
Community Support	Active	Active	Fairly active
Administrative Interface	Web interface	Web interface	Mainly window based
Reporting	Yes	Yes	Yes

Vergelijking tussen OpenNAC, PacketFence en FreeNAC (Ijcaonline, 2014)

In deze vergelijking is PacketFence op het gebied van Posture Analysis beter en bied PacketFence één extra functie ten opzichte van OpenNAC. Hierdoor is ervoor gekozen om PacketFence verder in de vergelijking mee te nemen.

Shortlist

In de shortlist worden de beste producten uit de longlist vergeleken door de functies een waarde te geven. Deze waarde geeft weer hoe goed het product voldoet aan de eisen en wensen. Het voldoen bevat waardes van nul, één en twee, waarbij nul '*voldoet niet*' betekend, één '*voldoet deels*' betekend en twee '*voldoet*' betekend. Dit is de eerste vergelijking van de shortlist. Wanneer deze waardes gegeven zijn aan de functies, wordt de waarde van de prioriteiten in een tweede tabel vermenigvuldig met de waarde van de eisen en wensen. In deze tabel worden de eind waardes (na de vermenigvuldigingen) bij elkaar opgeteld, zodat het bekend is welke producten de beste zijn en getest gaan worden in de Proof of Concept. De eerste vergelijkingstabel is hieronder in de tabel weergegeven.

Product	Offline mogelijkheden (2)	Open Source (3)	Ondersteuning besturingssystemen (4)	Eenvoudig in gebruik (4)	Passend binnen de beheer omgeving (4)	Bedrijfsdata niet lokaal (5)	Besmettingsgevaar minimaliseren (5)	Back-up van data (5)	Netwerkbeveiliging (5)	Waarborging continuïteit (5)
Ulteo Open Virtual Desktop	0	2	2	2	2	2	2	2	2	2
Dell vWorkspace	2	0	2	2	2	2/0*	2	2/0**	2	2
PacketFence	2	2	2	2	2	0	2	0	2	1

*) Indien er gebruik gemaakt wordt van offline mogelijkheden, staat bedrijfsdata wel lokaal en voldoet het product niet.
**) Indien er gebruik gemaakt wordt van offline mogelijkheden, kan het zijn dat er geen back-up gemaakt wordt.

De tweede vergelijkingstabel gebruikt de waardes van de eerste tabel en vermenigvuldigd deze met elkaar.

Product	Offline mogelijkheden (2)	Open Source (3)	Ondersteuning besturingssystemen (4)	Eenvoudig in gebruik (4)	Passend binnen de beheer omgeving (4)	Bedrijfsdata niet lokaal (5)	Besmettingsgevaar minimaliseren (5)	Back-up van data (5)	Netwerkbeveiliging (5)	Waarborging continuïteit (5)	Totaal

Ulteo Open Virtual Desktop	0	6	8	8	8	10	10	10	10	10	80
Dell vWorkspace	4	0	8	8	8	10/0	10	10/0	10	10	78/58
Packetfence	4	6	8	8	8	0	10	0	10	10	59

Uit deze tabel kan opgemaakt worden dat Ulteo Open Virtual Desktop het beste zou moeten voldoen, gevolgd door Dell vWorkspace en daarna Packetfence. Indien er een combinatie gemaakt wordt met offline mogelijkheden, voldoet PacketFence eerder dan Dell.

Bijlage 3: Interviewverslagen

Interviewverslag BYOD eisen en wensen Sedat Capkin

Datum	18-02-2016
Tijd	10:30-11:10
Geïnterviewde(n)	Sedat Capkin
Functie geïnterviwde	Security Officer
Interviewer	Dion Kruijswijk
Onderwerp	BYOD + Eisen en Wensen

Wat is volgens u het Bring Your Own Device principe?
Het BYOD-principe is wanneer iemand eigen apparatuur meeneemt dat niet SURFsara eigendom is en niet door SURFsara beheerd wordt. Op dit moment heeft SURFsara een beperkt "Choose Your Own Device" beleid waarbij een medewerker kan uitzoeken wat voor machine hij/zij wil hebben. Hij/zij kan een keuze maken uit een door de werkgever bepaalde set aan mogelijkheden.

Wat is het huidige beleid betreffend het meenemen van eigen hardware?
Het beleid is dat BYOD hardware in principe niet (zomaar) toegelaten wordt tot het SURFsara netwerk. Een uitzondering hierop zijn tweetal wifi netwerken, het SURFsara gastenlan en Eduroam voor bezoekers. Algemeen geformuleerde BYOD-apparatuur mag alleen op de daarvoor bedoelde netwerken aangesloten worden. Er zijn specifieke gevallen waarvoor uitzonderingen gemaakt kunnen worden. Voor deze uitzonderingen wordt er een oplossing bedacht zodat er toegang mogelijk is voor bepaalde personen of bedrijven, leveranciers bijvoorbeeld. Hiervoor kan er een nieuw netwerksegment/vlan ingesteld worden, waar bepaalde strikte en beperkte toegangsregels aan gekoppeld worden. Ten behoeve van het beheer van de supercomputer door Bull-engineers, is er bijvoorbeeld een dergelijk vlan opgezet. Dit vlan geeft toegang tot het management netwerk van de supercomputer, maar niet tot de rest van het SURFsara netwerk. Wanneer er eigen hardware meegenomen wordt, kan er verbonden worden met het gasten netwerk, waarbij geen toegang is tot het SURFsara netwerk maar er wel internettoegang mogelijk is.

Bied het huidige beleid voldoende veiligheid volgens u?
Het huidige beleid biedt op zich voldoende veiligheid. Het is momenteel echter nog wel mogelijk dat iemand fysiek hardware aan het netwerk aansluit. Hiervoor wordt een ander project opgestart met als doel om (hardware) authenticatie in te voeren om toegang tot het netwerk te krijgen. Alternatieven zullen daarbij ook aan de orde komen zoals bijvoorbeeld het gelijktrekken van de wired en wireless netwerken, waarbij deze netwerken standaard als onveilig zullen worden beschouwd. Om bij bedrijfsdata van SURFsara te komen, moet er eerst een VPN verbinding opgezet worden. Verder is het nodig dat bij wired- en wireless kantoornetwerken private vlan feature wordt gebruikt. Hiermee wordt verhinderd dat machines in hetzelfde netwerk elkaar kunnen aanvallen en/of besmetten.
Een ander zorgpunt in geval van BYOD is dat er zich SURFsara data op de machines van anderen kunnen bevinden. Dat kan gemitigeerd worden door middel van (harddisk) encryptie. Bij deze encryptie-eis is BYOD lastig te controleren, bij centraal beheerde machines is het beter te controleren.

Zou u iets veranderd willen zien aan het huidige beleid? En zo ja, wat dan?
Het huidige beleid willen wij voorlopig blijven hanteren. Het huidige beleid kan wellicht in een aantal gevallen ervoor zorgen dat er minder flexibel gewerkt kan worden. Bijvoorbeeld wanneer externen

tijdelijk voor ons moeten werken of wanneer je informatie met anderen/externen wilt delen. Wanneer er meer beveiliging is of beter beveiligde oplossingen worden bedacht zoals VDI of application portals, kan het beleid wat minder streng / anders geformuleerd worden en kan het BYOD principe dus toegepast worden. Als we het gaan toestaan moet beveiliging van lokale data op BYOD devices speciale aandacht krijgen, bijvoorbeeld gëencrypte opslag.

Moet het beleid voor interne en externe medewerkers hetzelfde of verschillend zijn als er een BYOD oplossing toegepast zou worden?
Als je BYOD toestaat dan kan het beleid in principe gelijkgetrokken worden, deze groepen kunnen op dezelfde manier worden behandeld omdat het externe apparaten betreft die niet zomaar toegang mogen hebben. Er wordt hiervoor dus geen verschil gemaakt tussen interne of externe werknemers. Beide categorieën worden als even veilig/onveilig beschouwd. Let wel, het gaat hier dan met name om de technische afspraken. Uiteraard zal er verschil zijn tussen de groepen als het om de organisatorische afspraken gaat. Een andere lastig punt dat uitgezocht moet worden is in hoeverre je eisen kan stellen aan de eigen/privé apparatuur van de BYOD-gebruiker.

Welke eisen zou een BYOD oplossing moeten bevatten als deze geïmplementeerd zou worden?
De BYOD oplossing zou op de eerste plaats voor de veiligheid van de data moeten zorgen, waarbij er bij voorkeur geen bedrijfsdata lokaal op BYOD hardware staat. In de praktijk is het haast onmogelijk om geen opslag van data te hebben, hetgeen betekent dat encryptie een vereiste is. Daarnaast moet het besmettingsgevaar geminimaliseerd worden en de continuïteit mag niet onder de BYOD oplossing lijden. Het mag niet zo zijn dat werknemers tijden zonder laptop zitten, omdat er geen support gegeven wordt op de BYOD hardware. Hiervoor zou het beleid aangepast moeten worden en mogelijk praktisch een aantal zaken geregeld moeten worden. Bijvoorbeeld reserve leen laptops en terminal servers waar de mensen op terecht kunnen. Samengevat kunnen we de volgende eisen op een rijtje zetten:

- Goede/betrouwbare back-ups.
- Encryptie.
- Centrale ondersteuning vanuit KA, minimaal in de vorm van centrale faciliteiten zoals leenlaptops, en/of terminal/VDI servers, geschikte (verplicht, aangeraden, etc.) software.
- Gebruik van aparte logins voor werk en privé.
- Virus scanner / firewall faciliteiten zoals F-secure
- OS en applicaties moeten up-to-date gehouden worden, met name patches voor kwetsbaarheden moeten zo snel mogelijk aangebracht worden.

Als we BYOD zouden invoeren moet er een duidelijk BYOD-beleid worden gedefinieerd met regels, richtlijnen, eisen, controle etc.

Welke wensen zou een BYOD oplossing moeten bevatten als deze geïmplementeerd zou worden?
De oplossing zou bij voorkeur een Open Source oplossing moeten zijn, waarbij gebruik wordt gemaakt van open protocollen. Als er door de markt betere en veiligere oplossingen worden geboden, dan mag de keuze beargumenteerd op deze commerciële producten vallen. Let wel, deze wens geldt met name voor de centraal aangeboden faciliteiten. Het is anders lastig om wensen te hebben met betrekking tot privé apparatuur van de werknemers.

Welke waardes zou u geven aan de door u opgegeven eisen om de prioriteit te bepalen van ondersteunde functies, waarbij drie redelijk belangrijk betekend, vier belangrijk betekend en vijf erg belangrijk betekend?
Veiligheid van de data – 5
Back-up van data – 5
Bedrijfsdata op externe hardware – 5 (ligt aan de BYOD toepassing, de data op de externe apparaten dient te worden geëncrypt)
Besmettingsgevaar minimaliseren / virusscanners– 5
Netwerkbeveiliging – 5
Continuïteit – 5

Welke waardes zou u geven aan de door u opgegeven wensen om de prioriteit te bepalen van ondersteunde functies, waarbij één niet erg belangrijk betekend en twee matig belangrijk betekend?

Open-Source – 2

Indien het BYOD principe geïmplementeerd zou worden, welke risico's voorziet u tijdens of na de implementatie?
Het BYOD principe zou voor een grote diversiteit aan hardware kunnen zorgen. Werknemers mogen hun eigen hardware kiezen, waardoor er veel apparaten gebruikt worden. Deze apparaten zorgen ervoor dat het niet meer overzichtelijk kan zijn, waardoor er geen volledige controle meer mogelijk is. Het BYOD principe zorgt er ook voor dat werknemers met vragen kunnen gaan komen over de hardware en software. (Technische) problemen met de apparatuur kan voor discontinuïteit in het werken van de persoon in kwestie betekenen. Licentie moeten ook in de gaten worden gehouden. Hoe wordt omgegaan met persoonlijke licenties van apparatuur/applicaties die wellicht voor het werk worden ingezet?

Interviewverslag BYOD eisen en wensen Leonieke Mevius

Datum	01-03-2016
Tijd	10:15-10:45
Geïnterviewde(n)	Leonieke Mevius
Functie geïnterviewde	Opdrachtgever
Interviewer	Dion Kruijswijk
Onderwerp	BYOD

Wat is volgens u het Bring Your Own Device principe:

Het BYOD principe houdt in dat werknemers met hardware die niet van de organisatie is voor de organisatie werkzaamheden uitvoeren.

Wat is het huidige beleid betreffend het meenemen van eigen hardware?:

BYOD wordt op dit moment wel toegelaten, maar het is niet de bedoeling dat de apparatuur aan het netwerk gekoppeld wordt. Op dit moment kunnen werknemers wel gewoon de apparatuur aansluiten op het netwerk. In principe krijgen alle werknemers de mogelijkheid voor een laptop, maar er is momenteel geen controle of ze daarnaast eigen hardware aansluiten. Voor de laptop is op dit moment een CYOD beleid, waarbij werknemers een beperkte keuze hebben in merk en besturingssysteem.

Bied het huidige beleid voldoende veiligheid volgens u?

Nee, want er is geen officieel beleid en geen maatregelingen omtrent het meenemen van eigen hardware en het aansluiten hiervan. De applicatie die nu wordt gebruikt om externen toegang te geven tot de server, LogMeIn, is niet 100% veilig, maar er is geen alternatief voorhanden. Momenteel is het ook mogelijk om administrator te zijn op de hardware, waardoor niet alles gecontroleerd kan worden.

Zou u iets veranderd willen zien aan het huidige beleid? En zo ja, wat dan?

Het BYOD principe zou als toevoeging zijn aan het huidige beleid. Bij het CYOD beleid zou er meer controle op Mac systemen moeten zijn of deze systemen zien als BYOD hardware. Er moet een echt beleid komen voor BYOD hardware met vaste regels, zodat het voor iedereen duidelijk is wat wel en niet de bedoeling is. Externe medewerkers moeten ook iets ondertekenen waar deze regels in staan.

Moet het beleid voor interne en externe medewerkers hetzelfde of verschillend zijn als er een BYOD oplossing toegepast zou worden?

Het beleid is voor beide hetzelfde, omdat het externe/niet beheerde hardware is.

Wanneer het BYOD principe toegepast wordt, wie gaat de omgeving beheren?

Voor de regelgeving is Sedat Capkin verantwoordelijk en verder voor het beheer de Interne Automatisering en netwerken.

Wordt BYOD naast het huidige beleid toegepast of is het als vervanging voor het huidige beleid?

BYOD is als toevoeging op het CYOD beleid en niet als vervanging. Externe werknemers worden altijd gezien als BYOD gebruikers als ze hun eigen hardware gebruiken. Interne werknemers hebben de mogelijkheid in de toekomst om te kiezen tussen BYOD en CYOD.

Welke eisen zou een BYOD oplossing moeten bevatten als deze geïmplementeerd zou worden?

Ondersteuning van besturingssystemen / flexibiliteit
Eenvoudig in gebruik
Veiligheid van het systeem
Passend binnen de beheeromgeving

Welke wensen zou een BYOD oplossing moeten bevatten als deze geïmplementeerd zou worden?

N.v.t.

Welke waardes zou u geven aan de door u opgegeven eisen om de prioriteit te bepalen van ondersteunde functies, waarbij drie redelijk belangrijk betekend, vier belangrijk betekend en vijf erg belangrijk betekend?

Ondersteuning van besturingssystemen / flexibiliteit - 4
Eenvoudig in gebruik - 4
Veiligheid van het systeem - 5
Passend binnen de beheeromgeving - 4

Welke waardes zou u geven aan de door u opgegeven wensen om de prioriteit te bepalen van ondersteunde functies, waarbij één niet erg belangrijk betekend en twee matig belangrijk betekend?

N.v.t.

Indien het BYOD principe geïmplementeerd zou worden, welke risico's voorziet u tijdens of na de implementatie?

Werknemers kunnen hun werk niet doen dat ze zouden moeten doen, de continuïteit moet behouden worden. Er kunnen te veel support vragen komen. De oplossing moet goed overzichtelijk zijn om te kunnen beheren.

Bijlage 4: Enquêtes externe medewerkers

Enquête BYOD Menno Hiemstra

Ten behoeve van onderzoek naar het veilig toepassen van het BYOD principe bij SURFsara

Voor en achternaam: Menno Hiemstra
Datum: 5 april 2016
1. Is de hardware die u gebruikt om op te werken van u, van SURFsara of een ander bedrijf waarbij u werkt?
Van mij
2. Met wat voor hard- en software (laptop, tablet etc. en besturingssysteem) maakt u verbinding met het netwerk van SURFsara om gebruik te maken van SURFsara diensten of bestanden?
Dell XPS 13 / Windows 10 Motorola Moto-G / Android 5.1
3. Op welke manier benaderd u het netwerk van SURFsara of maakt u helemaal geen gebruik hiervan? (Bijvoorbeeld via het kantoor netwerk van SURFsara, Eduroam WiFi of via VPN)
Eduroam
4. Van welke diensten of bestanden van SURFsara maakt u gebruik? (Bijvoorbeeld SURFdrive)
SURFdrive / Zimbra e-mail
5a. Werkt u wel eens 'offline' met bestanden of diensten van SURFsara en op welke manier doet u dit (bijvoorbeeld bestanden lokaal plaatsen en gebruiken)?
SURFdrive-client mapping naar SSD sync
5b. Indien u met 'offline' bestanden werkt, kunt u volledig privé en/of bedrijfsdata scheiden? Zo ja, op welke manier doet u dit?
Voor SURFdrive 100% gescheiden Zimbra attachements niet 100%
6. Indien er door gebruik te maken van een virtuele desktop waar naartoe verbonden kan worden, meer hardware gebruikt kan worden (diverse tablets, laptops en dergelijke) zou u hiervan gebruik willen maken? Ook als er dan geen 'offline' mogelijkheden meer zijn?
Als virtuele desktop verbinding maakt met intranet ja, anders niet

Enquête BYOD anoniem

Ten behoeve van onderzoek naar het veilig toepassen van het BYOD principe bij SURFsara

Voor en achternaam: Anoniem
Datum: 06 april 2016
1. Is de hardware die u gebruikt om op te werken van u, van SURFsara of een ander bedrijf waarbij u werkt?
SURFsara

2. Met wat voor hard- en software (laptop, tablet etc. en besturingssysteem) maakt u verbinding met het netwerk van SURFsara om gebruik te maken van SURFsara diensten of bestanden?
Macbook Pro
3. Op welke manier benaderd u het netwerk van SURFsara of maakt u helemaal geen gebruik hiervan? (Bijvoorbeeld via het kantoor netwerk van SURFsara, Eduroam WiFi of via VPN)
Kantoor en VPN
4. Van welke diensten of bestanden van SURFsara maakt u gebruik? (Bijvoorbeeld SURFdrive)
SURFdrive, netwerkopslag, back-up, mail, intranet
5a. Werkt u wel eens 'offline' met bestanden of diensten van SURFsara en op welke manier doet u dit (bijvoorbeeld bestanden lokaal plaatsen en gebruiken)?
Lokaal plaatsen bij uitzondering, meestal werk ik via VPN.
5b. Indien u met 'offline' bestanden werkt, kunt u volledig privé en/of bedrijfsdata scheiden? Zo ja, op welke manier doet u dit?
Op mijn laptop staat alleen maar bedrijfsdata. Privé gebruik ik andere apparaten.
6. Indien er door gebruik te maken van een virtuele desktop waar naartoe verbonden kan worden, meer hardware gebruikt kan worden (diverse tablets, laptops en dergelijke) zou u hiervan gebruik willen maken? Ook als er dan geen 'offline' mogelijkheden meer zijn?
Ja, dat denk ik wel. Ik gebruik dit nu al om MS Project en MS Visio te kunnen gebruiken.

Enquête BYOD Jeroen Harmse

Ten behoeve van onderzoek naar het veilig toepassen van het BYOD principe bij SURFsara

Voor en achternaam: Jeroen Harmse
Datum: 6 april 2016
1. Is de hardware die u gebruikt om op te werken van u, van SURFsara of een ander bedrijf waarbij u werkt?
Laptop van SURFsara, ik gebruik mijn eigen telefoon.
2. Met wat voor hard- en software (laptop, tablet etc. en besturingssysteem) maakt u verbinding met het netwerk van SURFsara om gebruik te maken van SURFsara diensten of bestanden?
Macbook Air, OS X Yosemite
3. Op welke manier benaderd u het netwerk van SURFsara of maakt u helemaal geen gebruik hiervan? (Bijvoorbeeld via het kantoor netwerk van SURFsara, Eduroam WiFi of via VPN)
Ik maak een verbinding via VPN met Entrust Soft Token, als ik niet op mijn werkplek zit. Bij SURF in Utrecht of bij instellingen over het algemeen Eduroam WiFi. Op mijn werkplek heb ik een netwerkkabel aangesloten op mijn laptop.
4. Van welke diensten of bestanden van SURFsara maakt u gebruik? (Bijvoorbeeld SURFdrive)
SURFdrive
5a. Werkt u wel eens 'offline' met bestanden of diensten van SURFsara en op welke manier doet u dit (bijvoorbeeld bestanden lokaal plaatsen en gebruiken)?
Ik sla vaak bestanden op de laptop op, daar kan ik dan offline (bijvoorbeeld in de trein) mee werken.
5b. Indien u met 'offline' bestanden werkt, kunt u volledig privé en/of bedrijfsdata scheiden? Zo ja, op welke manier doet u dit?
Ik heb een paar privézaken op deze laptop staan, die bewaar ik in een aparte map.

6. Indien er door gebruik te maken van een virtuele desktop waar naartoe verbonden kan worden, meer hardware gebruikt kan worden (diverse tablets, laptops en dergelijke) zou u hiervan gebruik willen maken? Ook als er dan geen 'offline' mogelijkheden meer zijn?
Ik zou het nu niet nodig hebben.

Enquête BYOD anoniem

Ten behoeve van onderzoek naar het veilig toepassen van het BYOD principe bij SURFsara

Voor en achternaam: Anoniem
Datum: 14 april 2016
1. Is de hardware die u gebruikt om op te werken van u, van SURFsara of een ander bedrijf waarbij u werkt?
Een ander bedrijf
2. Met wat voor hard- en software (laptop, tablet etc. en besturingssysteem) maakt u verbinding met het netwerk van SURFsara om gebruik te maken van SURFsara diensten of bestanden?
MacBook Air Ipad 2 Huawei Ascend P8
3. Op welke manier benaderd u het netwerk van SURFsara of maakt u helemaal geen gebruik hiervan? (Bijvoorbeeld via het kantoor netwerk van SURFsara, Eduroam WiFi of via VPN)
Voor alle devices: WIFI 'Amsterdam Science Park'.
4. Van welke diensten of bestanden van SURFsara maakt u gebruik? (Bijvoorbeeld SURFdrive)
Surfdrive. Verder niets.
5a. Werkt u wel eens 'offline' met bestanden of diensten van SURFsara en op welke manier doet u dit (bijvoorbeeld bestanden lokaal plaatsen en gebruiken)?
Lokaal plaatsen inderdaad; eventueel bewerken en weer uploaden naar surfdrive
5b. Indien u met 'offline' bestanden werkt, kunt u volledig privé en/of bedrijfsdata scheiden? Zo ja, op welke manier doet u dit?
100% bedrijfsdata. Op mijn devices staan geen privedata.
6. Indien er door gebruik te maken van een virtuele desktop waar naartoe verbonden kan worden, meer hardware gebruikt kan worden (diverse tablets, laptops en dergelijke) zou u hiervan gebruik willen maken? Ook als er dan geen 'offline' mogelijkheden meer zijn?
Ja!

Enquête BYOD anoniem

Ten behoeve van onderzoek naar het veilig toepassen van het BYOD principe bij SURFsara

Voor en achternaam: Anoniem
Datum: 14-4-2016

1. Is de hardware die u gebruikt om op te werken van u, van SURFsara of een ander bedrijf waarbij u werkt?
Eigen hardware
2. Met wat voor hard- en software (laptop, tablet etc. en besturingssysteem) maakt u verbinding met het netwerk van SURFsara om gebruik te maken van SURFsara diensten of bestanden?
Laptop met W10; Samsung telefoon
3. Op welke manier benaderd u het netwerk van SURFsara of maakt u helemaal geen gebruik hiervan? (Bijvoorbeeld via het kantoor netwerk van SURFsara, Eduroam WiFi of via VPN)
Niet; ik werk niet op locatie bij SURsara.
4. Van welke diensten of bestanden van SURFsara maakt u gebruik? (Bijvoorbeeld SURFdrive)
E-Mail & agenda (laptop en telefoon), SURFdrive (laptop)
5a. Werkt u wel eens 'offline' met bestanden of diensten van SURFsara en op welke manier doet u dit (bijvoorbeeld bestanden lokaal plaatsen en gebruiken)?
Ja, via SURFdrive windows applicatie (ownCloud) worden de bestanden van SURFdrive gesynchroniseerd met mijn laptop.
5b. Indien u met 'offline' bestanden werkt, kunt u volledig privé en/of bedrijfsdata scheiden? Zo ja, op welke manier doet u dit?
Ik gebruik voor SURFsara alleen bedrijfsdata.
6. Indien er door gebruik te maken van een virtuele desktop waar naartoe verbonden kan worden, meer hardware gebruikt kan worden (diverse tablets, laptops en dergelijke) zou u hiervan gebruik willen maken? Ook als er dan geen 'offline' mogelijkheden meer zijn?
Nee, alleen de eigen laptop is prima.

Enquête BYOD anoniem

Ten behoeve van onderzoek naar het veilig toepassen van het BYOD principe bij SURFsara

Voor en achternaam: Anoniem
Datum: 15-04-2016
1. Is de hardware die u gebruikt om op te werken van u, van SURFsara of een ander bedrijf waarbij u werkt?
Van mij / van sara
2. Met wat voor hard- en software (laptop, tablet etc. en besturingssysteem) maakt u verbinding met het netwerk van SURFsara om gebruik te maken van SURFsara diensten of bestanden?
Laptop Linux
3. Op welke manier benaderd u het netwerk van SURFsara of maakt u helemaal geen gebruik hiervan? (Bijvoorbeeld via het kantoor netwerk van SURFsara, Eduroam WiFi of via VPN)
Wifi-Eduroam, ethernet
4. Van welke diensten of bestanden van SURFsara maakt u gebruik? (Bijvoorbeeld SURFdrive)
Surfdrive
5a. Werkt u wel eens 'offline' met bestanden of diensten van SURFsara en op welke manier doet u dit (bijvoorbeeld bestanden lokaal plaatsen en gebruiken)?

Nee
5b. Indien u met 'offline' bestanden werkt, kunt u volledig privé en/of bedrijfsdata scheiden? Zo ja, op welke manier doet u dit?
N/A
6. Indien er door gebruik te maken van een virtuele desktop waar naartoe verbonden kan worden, meer hardware gebruikt kan worden (diverse tablets, laptops en dergelijke) zou u hiervan gebruik willen maken? Ook als er dan geen 'offline' mogelijkheden meer zijn?
N/A

Enquête BYOD Mark Hoevers

Ten behoeve van onderzoek naar het veilig toepassen van het BYOD principe bij SURFsara

Voor en achternaam: Mark Hoevers
Datum: 17 april 2016
1. Is de hardware die u gebruikt om op te werken van u, van SURFsara of een ander bedrijf waarbij u werkt?
Van mij.
2. Met wat voor hard- en software (laptop, tablet etc. en besturingssysteem) maakt u verbinding met het netwerk van SURFsara om gebruik te maken van SURFsara diensten of bestanden?
MacBook Pro (Apple iOS) en Dell (MS Windows 7 professional)
3. Op welke manier benaderd u het netwerk van SURFsara of maakt u helemaal geen gebruik hiervan? (Bijvoorbeeld via het kantoor netwerk van SURFsara, Eduroam WiFi of via VPN)
Via de SURF DRIVE website in het kader van een tijdelijke opdracht
4. Van welke diensten of bestanden van SURFsara maakt u gebruik? (Bijvoorbeeld SURFdrive)
Uitsluitend SURFdrive
5a. Werkt u wel eens 'offline' met bestanden of diensten van SURFsara en op welke manier doet u dit (bijvoorbeeld bestanden lokaal plaatsen en gebruiken)?
Meestal schrijf ik zelf iets en plaats dat op SURFDRIVE ter deling met 3 andere personen
5b. Indien u met 'offline' bestanden werkt, kunt u volledig privé en/of bedrijfsdata scheiden? Zo ja, op welke manier doet u dit?
Op beide laptops zijn privé en bedrijfsdata niet gescheiden
6. Indien er door gebruik te maken van een virtuele desktop waar naartoe verbonden kan worden, meer hardware gebruikt kan worden (diverse tablets, laptops en dergelijke) zou u hiervan gebruik willen maken? Ook als er dan geen 'offline' mogelijkheden meer zijn?
Neen

Enquête BYOD anoniem

Ten behoeve van onderzoek naar het veilig toepassen van het BYOD principe bij SURFsara

Voor en achternaam: Anoniem
Datum: 18 april 2016
1. Is de hardware die u gebruikt om op te werken van u, van SURFsara of een ander bedrijf waarbij u werkt?
Van SURFsara
2. Met wat voor hard- en software (laptop, tablet etc. en besturingssysteem) maakt u verbinding met het netwerk van SURFsara om gebruik te maken van SURFsara diensten of bestanden?
MacBook Pro uit begin 2015, met MacOS 10.10.5 (Yosemite)
3. Op welke manier benaderd u het netwerk van SURFsara of maakt u helemaal geen gebruik hiervan? (Bijvoorbeeld via het kantoor netwerk van SURFsara, Eduroam WiFi of via VPN)
Via het kantoornetwerk van SURFsara en VPN
4. Van welke diensten of bestanden van SURFsara maakt u gebruik? (Bijvoorbeeld SURFdrive)
SURFdrive
5a. Werkt u wel eens 'offline' met bestanden of diensten van SURFsara en op welke manier doet u dit (bijvoorbeeld bestanden lokaal plaatsen en gebruiken)?
Ja, middels Git
5b. Indien u met 'offline' bestanden werkt, kunt u volledig privé en/of bedrijfsdata scheiden? Zo ja, op welke manier doet u dit?
Ja, ik sla geen prive data op
6. Indien er door gebruik te maken van een virtuele desktop waar naartoe verbonden kan worden, meer hardware gebruikt kan worden (diverse tablets, laptops en dergelijke) zou u hiervan gebruik willen maken? Ook als er dan geen 'offline' mogelijkheden meer zijn?
Nee

Bijlage 5: Referentie onderzoek

Enquête Bring Your Own Device Gemeente Utrecht

Ten behoeve van onderzoek naar het veilig toepassen van het BYOD principe bij SURFsara.

Voor en achternaam: Richardo Theben Tervile
Datum: 29-03-16
Wat wordt er verstaan onder Bring Your Own Device (BYOD; gebruik van eigen hardware) binnen de Gemeente Utrecht?
Het gebruik van privé apparaten door werknemers (in- en externe medewerkers) waarmee werk activiteiten uitgevoerd (zoals mail lezen of inloggen op het werk) worden.
Hoe wordt er met BYOD verbonden met het netwerk van de Gemeente Utrecht en op welke manier wordt er authenticatie op de verbinding uitgevoerd (Active directory en dergelijke)?
Op dit moment kunnen mensen gebruik maken van OMA (Outlook Mobile Access) . Er loopt een project om de applicatie Good te gebruiken. Met deze applicatie kan data veilig opgeslagen worden op apparaten en wordt versleuteld. Daarnaast kunnen gebruikers gebruik maken van de VMware client. Gebruikers met deze software op afstand inloggen op hun standaard werkplek.
Welke BYOD hard- en software (laptops, tablets etc. en de besturingssystemen op de hardware) wordt er gebruikt door personeel om toegang te krijgen tot het netwerk?
De gebruikers gebruiken alle mogelijkheden. Alle hardware kan gebruik maken van de infrastructuur. Maar GU ondersteund alleen hardware met Android systeembesturing voor de OMA oplossing . Voor de VMware client worden geen tablets ondersteund.
Zijn er beleidsregels en richtlijnen geschreven voor het gebruik van BYOD? Zo ja, zijn hier een aantal voorbeelden van (richtlijnen, gebruikswijzers en dergelijke)?
- Gebruikers zijn zelf verantwoordelijk voor hun eigen apparaat. - Indien een medewerker in dienst komt dient hij/zij een gebruik verklaring te ondertekenen. - Indien een apparaat met bedrijfsgegevens gestolen of kwijt is dient de gebruiker een data lek te melden. - Gebruikers krijgen geen support op gebruikersvragen. - Niet alle hardware en besturingssystemen worden ondersteund
Hoe wordt er voorkomen dat virussen op de BYOD hardware bedrijfsdata van de Gemeente Utrecht, servers of andere hardware besmet?
De systemen van GU zijn uitgerust met virusscanners op elk niveau . Elk bestand die gedownload of geüpload wordt naar de interne systemen wordt gescand door meerdere virusscanners.
Wordt privédata en bedrijfsdata gescheiden op de BYOD hardware? Zo ja, hoe wordt deze data van elkaar gescheiden?
De data wordt op dit moment niet gescheiden. Als de applicatie GOOD in productie zal dit wel gescheiden en versleuteld worden.

Zijn er beperkingen opgetreden door het gebruik van BYOD (zoals niet meer offline kunnen werken)? Zo ja welke?
Er zijn geen beperkingen bij mij bekend.

Enquête Bring Your Own Device Hogeschool van Amsterdam

Ten behoeve van onderzoek naar het veilig toepassen van het BYOD principe bij SURFsara.

Voor en achternaam: Eric Kamsma
Datum: 18-04-2016
Wat wordt er verstaan onder Bring Your Own Device (BYOD; gebruik van eigen hardware) bij de HVA?
Er wordt min of meer een knip gemaakt wb werkplek tussen hardware en software. Voor studenten en medewerkers is het mogelijk om eigen apparaten mee te nemen, en te gebruiken binnen het netwerk van de HvA. Medewerkers mogen niet de aanschaf van eigen apparaten declareren. Ze moeten uit de catalogus kiezen, en mogen daarna het apparaten als BYO beschouwen: ander OS, zelf zaken installeren noem maar op. Hardware blijft van de HvA, inclusief service-contract. Medewerkers en studenten kunnen binnen het netwerk schijven koppelen. Verder kunnen binnen en buiten de HvA ze naar een virtuele werkplek gebaseerd op Citrix, waarna ze alle mogelijkheden hebben die specifiek voor hun gebruikersgroep zijn geregeld.
Hoe wordt er met BYOD verbonden met het netwerk van de HVA en op welke manier wordt er authenticatie op de verbinding uitgevoerd (Active directory en dergelijke)?
Dit doen we met het 802.nx protocol, voor bedraad en draadloos. Userbased, authenticatie via Radius.
Welke BYOD hard- en software (laptops, tablets etc. en de besturingssystemen op de hardware) wordt er gebruikt door personeel of studenten om toegang te krijgen tot het netwerk?
Voor medewerkers via CYO vanuit catalogus, met eigen keuze voor OS. En via een citrix-portal kunnen ze gebruik maken van een HVA-eigen applicaties. Voor studenten is de keuze vrij, en hebben ook de (beperkte aantal applicaties) toegang tot dit portal
Zijn er beleidsregels en richtlijnen geschreven voor het gebruik van BYOD? Zo ja, zijn hier een aantal voorbeelden van (richtlijnen, gebruikswijzers en dergelijke)?
Nee.
Hoe wordt er voorkomen dat virussen op de BYOD hardware bedrijfsdata van de HVA, servers of andere hardware besmet?
De servers zijn beveiligd met anti-virus software. En er zijn richtlijnen voor gebruik van eigen devices. We maken gebruik van een Quarantaine netwerk om misbruik te isoleren.
Wordt privédata en bedrijfsdata gescheiden op de BYOD hardware? Zo ja, hoe wordt deze data van elkaar gescheiden?
Nee, maar de gebruiker is gehouden aan veilig gebruik van gegevens, en heeft daar ook de middelen voor.

ICT-GEDRAGSREGELS HvA

Iedereen aan wie toegang is verleend tot het HvA-netwerk is gehouden aan de hieronder beschreven en goedgekeurde ICT-gedragsregels, die integraal deel uitmaken van het Reglement HvA-netwerk.

Bij overtreding van één of meer van de gedragsregels kan de overtreder de toegang tot het HvA-netwerk worden ontzegd voor een door of namens het College van Bestuur te bepalen periode. Deze periode bedraagt ten hoogste één jaar. Bij recidive kan deze periode verlengd worden.

1. GA VERTROUWELIJK MET JE TOEGANGSCODES OM. LEEN ZE NIET UIT.

- Toegangscodes uitlenen is niet toegestaan. Ze zijn strikt persoonlijk.
- Systeembeheerders mogen nooit om jouw toegangscodes (wachtwoord) vragen.
- Toegangscodes uitlenen aan derden is verboden. SURFnet, waar het HvA-netwerk deel vanuit maakt, staat gebruik van het netwerk door derden niet toe. Uitlenen aan een medestudent of collega is hoe dan ook niet nodig. Zij beschikken zelf over toegangscodes.

2. KIES ALLEEN NIET-VANZELFSPREKENDE WACHTWOORDEN EN VERANDER JE WACHTWOORD REGELMATIG.

Gebruik voor je wachtwoord bijvoorbeeld de eerste letters van een gemakkelijk te onthouden zin en verander een of twee letters in tekens. ‘Spruitjes eet ik echt niet meer hoor’ wordt dan bijvoorbeeld Se!enmh. Er is programmatuur dat viapassword guessing jouw wachtwoord kan achterhalen indien dat te voor de hand liggend is. Gebruikersnaam en wachtwoord moeten altijd verschillend zijn.

3. BEWAAR JE GEGEVENS ZO VEEL MOGELIJK OP DE SERVER EN NIET OP JE PC.

Als je je gegevens op de server bewaart, blijft de schade aan je bestanden bij calamiteiten beperkt: van de bestanden op de server wordt een back-up gemaakt en de servers zijn beter beveiligd tegen onder andere virussen.

4. GEEF GEEN AANLEIDING OF GELEGENHEID TOT HET KRAKEN VAN COMPUTERS.

- Stel op je computer een screensaver met wachtwoordbeveiliging in.
- Gebruik als het even kan op de thuis-pc een firewall en installeer met regelmaat updates van je besturingssysteem.
- Installeer of activeer geen overbodige programmatuur.
- Houd jezelf verre van hacking, cracking, spoofing, defacing, cross-site scripting, portscans, sniffing en denial of service attacks.

5. VERRICHT GEEN ACTIVITEITEN IN STRIJD MET ENIGE WET, WAARONDER AUTEURSRECHTWETGEVING.

Medewerkers en/of studenten van de HvA mogen via het HvA-netwerk geen activiteiten verrichten die in strijd zijn met enige wet.

Voor HvA-medewerkers geldt dat zij een arbeidsrechtelijke relatie hebben met de HvA waardoor ook vanuit de CAO kaders kunnen worden opgelegd.

6. VERSPREID GEEN DISCRIMINEREND, LASTERLIJK EN/OF BELEDIGEND MATERIAAL.

Ondanks de vrijheid van meningsuiting zijn er grenzen aan het toelaatbare. Neem de goede omgangsvormen in acht. Hierbij geldt tevens ‘wat gij niet wilt dat u geschiedt, doe dat ook een ander niet’.

7. INSTALLEER EN/OF GEBRUIK GEEN ILLEGALE EN/OF ONGEWENSTE SOFTWARE.

Hieronder valt software waarvoor geen licentierechten zijn betaald terwijl dat wel moet en software die de werking van de computer en/of het HvA-netwerk verstoort. Programmatuur als bijvoorbeeld KAZAA is niet illegaal maar de gevolgen van het gebruik ervan zijn dat vrijwel altijd wel.

8. VERSPREID GEEN COMPUTERVIRUSSEN EN DERGELIJKE.

Onder computervirussen wordt in dit geval ook wormen en Trojaanse paarden begrepen. Installeer op de thuis-pc minimaal een antivirusprogramma en zorg dat je de meest actuele antivirusbestanden hebt. Wees behoedzaam bij het openen van bijlagen (attachments) en programma’s op internet.

9. VERSTUUR GEEN ONGEVRAAGDE E-MAIL: VEROORZAAK NIET ONNODIG VEEL NETWERKVERKEER.

- Doe niet mee aan ‘kettingmail’, hoe zinnig de boodschap ook mag lijken. Vrede op aarde bereik je niet door een e-mailbombardement.

- Het is niet toegestaan om anonieme e-mail of e-mails met een fout afzenderadres (spam) te versturen of een e-mail aan een willekeurige groep medewerkers uit het adresboek (om bijvoorbeeld mee te doen aan een enqute).

10. GEBRUIK JE HVA-NETAANSLUITING NIET VOOR COMMERCIËLE DOELEINDEN.

Het HvA-netwerk is eigendom van de HvA. In geval van misbruik kan de toegang tot ICT-diensten, waaronder het HvA-net, worden ontzegd. Bij medewerkers kan misbruik reden zijn voor ontslag.

Gepubliceerd door ICTS 3 juni 2015

Bijlage 6: Enquête monitoring

Enquête BYOD monitoring Paul Reemeijer

Ten behoeve van onderzoek naar het veilig toepassen van het BYOD principe bij SURFsara.

Voor en achternaam: Paul Reemeijer
Datum: 6 mei 2016
Welke hardware moet gemonitord kunnen worden? (Server, VM's, BYOD hardware?)
Vanuit de BYOD software een BYOD check of dat alles up-to-date is op bijvoorbeeld aanwezige patches, firewall en virusscanner
Welke onderdelen moeten er gemonitord kunnen worden? (Services, gebruik cliënts etc.?)
Niet noodzakelijk; keuzes maken welke BYOD worden ondersteunt
Hoe moeten alerts gemeld worden? (Email, portal, beide of iets anders?)
Beide
Moet er een monitoring tool in de BYOD oplossing zitten of mag/moet dit een aparte tool zijn?
Het lijkt me persoonlijk praktisch als het 1 oplossing is

Enquête BYOD monitoring Remy Bien

Ten behoeve van onderzoek naar het veilig toepassen van het BYOD principe bij SURFsara.

Voor en achternaam: Remy Bien
Datum: 09-05-16
Welke hardware moet gemonitord kunnen worden? (Server, VM's, BYOD hardware?)
In geval van een gevirtualiseerde omgeving wil je de server en de VM's monitoren, de BYOD hardware is de verantwoordelijkheid van de gebruiker dus niet interessant.
Welke onderdelen moeten er gemonitord kunnen worden? (Services, gebruik cliënts etc.?)
De server uiteraard, en daarnaast misschien de status van de VM's, niet teveel ivm. privacy
Hoe moeten alerts gemeld worden? (Email, portal, beide of iets anders?)
e-mail is een eis, alles daar bij is extra
Moet er een monitoring tool in de BYOD oplossing zitten of mag/moet dit een aparte tool zijn?
We hebben op dit moment meerdere monitoringtools, bijvoorbeeld ganglia maar ook cf-engine monitort dingen. Zo lang de tool kan mailen is er mee te werken

Enquête BYOD monitoring Dennis Stam

Ten behoeve van onderzoek naar het veilig toepassen van het BYOD principe bij SURFsara.

Voor en achternaam: Dennis Stam
Datum: 09-05-2015

Welke hardware moet gemonitord kunnen worden? (Server, VM's, BYOD hardware?)
Alle facetten moeten gemonitord worden, hierdoor ben je altijd on control
Welke onderdelen moeten er gemonitord kunnen worden? (Services, gebruik cliënts etc.?)
Eigenlijk beetje hetzelfde als hierboven, alle zaken die nodig zijn voor het aanbieden van een BYOD oplossing moeten gemonitord worden. Dat is inclusief zaken die vantui het Operating Systeem komen.
Hoe moeten alerts gemeld worden? (Email, portal, beide of iets anders?)
Errors die voorkomen moeten gemaild worden, waarshuwingen kunnen verzameld worden en 1x gemaild worden.
Moet er een monitoring tool in de BYOD oplossing zitten of mag/moet dit een aparte tool zijn?
Dit kan ook een aparte tool zijn, maar heeft altijd meerwaarde als deze word meegeleverd met de BYOD oplossing.

Enquête BYOD monitoring Leonieke Mevius

Ten behoeve van onderzoek naar het veilig toepassen van het BYOD principe bij SURFsara.

Voor en achternaam: Leonieke Mevius
Datum: 9-5-2016
Welke hardware moet gemonitord kunnen worden? (Server, VM's, BYOD hardware?)
De servers/VM's
Welke onderdelen moeten er gemonitord kunnen worden? (Services, gebruik cliënts etc.?)
Services, Perfomance, Resources, Problemen
Hoe moeten alerts gemeld worden? (Email, portal, beide of iets anders?)
Problemen via E-mail (dus ook problemen met services, resources)
Moet er een monitoring tool in de BYOD oplossing zitten of mag/moet dit een aparte tool zijn?
Mag apart

Enquête BYOD monitoring Bas van der Vlies

Ten behoeve van onderzoek naar het veilig toepassen van het BYOD principe bij SURFsara.

Voor en achternaam: Bas van der Vlies
Datum: 09-05-16
Welke hardware moet gemonitord kunnen worden? (Server, VM's, BYOD hardware?)
Alles zodat je kan zien wat er aan de hand is. Voor een BYOD zal dat lastig zijn. Want je weet niet welke software er op draait, je zou wel een BYOD kunnen scannen
Welke onderdelen moeten er gemonitord kunnen worden? (Services, gebruik cliënts etc.?)
Heb je hier over de servers of BYOD. Servers/VM's moeten zo en zo gemonitord worden of alles nog werkt. Als je de servers monitort weet je ook welke clients worden gebruikt., is handig om te weten. Voor BYOD is het lastig je bent afhankelijk of de software wordt geinstalleerd.
Hoe moeten alerts gemeld worden? (Email, portal, beide of iets anders?)
Je hebt verschillende type alerts. Voor ek type kan je andere instelllingen hebben,bv Critical is misschien een SMS wel handig. Het liefst heb je een flexibel systeem. Een dashboard voor een handig overzicht en makkelijk voor de helpdesk, email, sms, …
Moet er een monitoring tool in de BYOD oplossing zitten of mag/moet dit een aparte tool zijn?
Het is handig als het erin zit, dan sluit het goed op elkaar aan. Het zou ook heel handig zijn als er een API inzit, dan zou je het ook in een andere monitor tool kunnen laten zien. Anders zijn er genoeg monitor tools, alleen zal je zelf veel moeten programmeren/configureren om de informatie in de tool te krijgen.

Enquête BYOD monitoring Jaap Dijkshoorn

Ten behoeve van onderzoek naar het veilig toepassen van het BYOD principe bij SURFsara.

Voor en achternaam: Jaap Dijkshoorn
Datum: 10-05-2016
Welke hardware moet gemonitord kunnen worden? (Server, VM's, BYOD hardware?)
Servers en VM's. Byod zullen ieder geval in een separaat netwerk gezet moeten worden.
Welke onderdelen moeten er gemonitord kunnen worden? (Services, gebruik cliënts etc.?)
Netwerk verkeer/connectiviteit.
Hoe moeten alerts gemeld worden? (Email, portal, beide of iets anders?)
Via Email en/of Nagios. Via een portal kan, maar de vraag is of daar vaak naar gekeken wordt.
Moet er een monitoring tool in de BYOD oplossing zitten of mag/moet dit een aparte tool zijn?
Dit kan apart geregeld worden, maar er moet wel aangegeven worden waarmee gemonitord moet gaan worden.

Enquête BYOD monitoring Paulus Smit

Ten behoeve van onderzoek naar het veilig toepassen van het BYOD principe bij SURFsara.

Voor en achternaam: Paulus
Datum: 10-05-2016
Welke hardware moet gemonitord kunnen worden? (Server, VM's, BYOD hardware?)
De hardware die mensen in het netwerk pluggen.
Welke onderdelen moeten er gemonitord kunnen worden? (Services, gebruik cliënts etc.?)
Update status "hardware die mensen in het netwerk pluggen", services die draaien, status virus scanner. Patch lvl.
Hoe moeten alerts gemeld worden? (Email, portal, beide of iets anders?)
E-mail
Moet er een monitoring tool in de BYOD oplossing zitten of mag/moet dit een aparte tool zijn?
Kan wel apart maar lijkt me handig alles in een te houden

Enquête BYOD monitoring Lucas Slim

Ten behoeve van onderzoek naar het veilig toepassen van het BYOD principe bij SURFsara.

Voor en achternaam: Lucas Slim
Datum: 10-05-2016
Welke hardware moet gemonitord kunnen worden? (Server, VM's, BYOD hardware?)
Server/vms Voor BYOD wellicht alleen of deze wel aan bepaalde veiligheidseisen voldoen (zoals een actuele virusscanner etc., want ook wanneer iemand vertrouwelijke informatie via een streamed app opent kan het zijn dat er iemand remote op het scherm mee kijkt.)
Welke onderdelen moeten er gemonitord kunnen worden? (Services, gebruik cliënts etc.?)
Load voor de servers en het netwerk, controle of meerdere clients met dezelfde credentials verbinden Zie ook BYOD comment van de vraag hierboven Ook zouden BYOD clients in een apart netwerk moeten komen, denk hierbij bijvoorbeeld aan een oplossing met 802.1X in combinatie met een aparte groep voor de gebruikers die geen SURFsara hardware hebben. Die kunnen dan wanneer zij inloggen in een apart VLAN geplaatst worden. Dit zou ook gedaan kunnen worden met mac adres registratie. Het probleem blijft echter dan nog wel wanneer een gebruiker die ook SURFsara hardware alsnog een eigen device meeneemt en het mac adres hiervan spooft naar het adres van de surfsara hardware die hem is toebedeeld
Hoe moeten alerts gemeld worden? (Email, portal, beide of iets anders?)
In principe zoals dit nu ook gedaan wordt, namelijk doormiddel van mail, maar het zou ook mooi zijn wanneer dit bijvoorbeeld op de ganglia pagina's op de monitors in het kantoor getoond zou kunnen worden.
Moet er een monitoring tool in de BYOD oplossing zitten of mag/moet dit een aparte tool zijn?
Dit maakt in principe geen verschil, zolang deze qua methodieken maar niet teveel af zou wijken van de huidige monitoring. Het zou eigenlijk ideaal zijn wanneer dit met de huidige monitoring zou kunnen zodat dit eenvoudig te integreren is.

Bijlage 7: Proof of Concept

In de Proof of Concept worden de producten uit de shortlist van de Analyse van Eisen getest. De producten worden als VM's op drie Dell geïnstalleerd. De servers zijn ingericht met CentOS 7 waar KVM op draait. KVM is de hypervisor waardoor het mogelijk is om VM's te installeren. Op de drie KVM server worden tevens drie VM's per server geïnstalleerd. De KVM servers hebben allemaal 64GB geheugen en 15TB schijven tot hun beschikking. De VM's op de hypervisors krijgen allemaal 8 van de 48 mogelijke logische cores. Deze geïnstalleerde VM's per hypervisor zijn:

- Een Active Directory (AD) server; die voor de authenticatie zorgt

Elke AD server wordt ingericht met Windows Server 2008, Server 2008 wordt algemeen ondersteund en 2012 nog niet altijd.

- Een BYOD server; waar het product op geïnstalleerd wordt

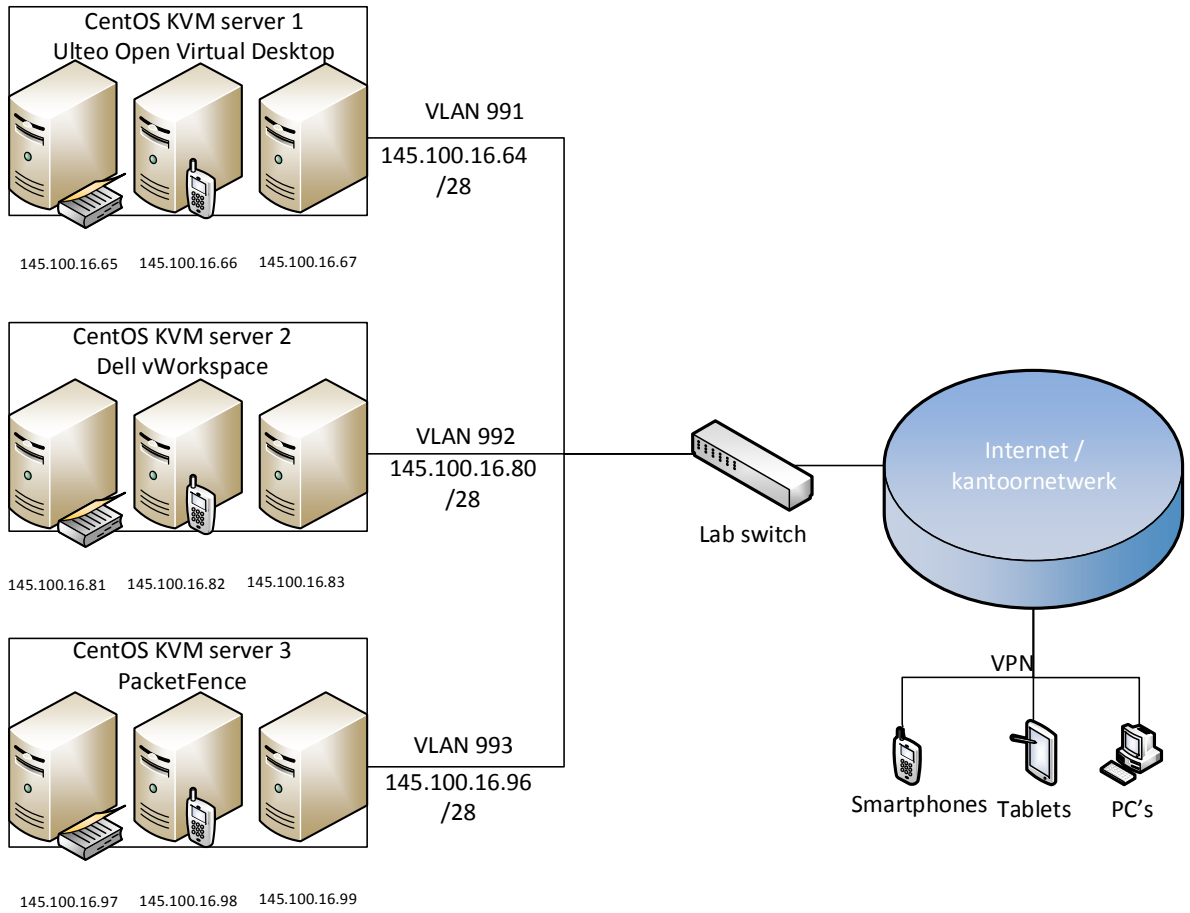
Per product is het verschillend wat het OS wordt voor de BYOD server. Dit kan CentOS of Windows server 2008 zijn.

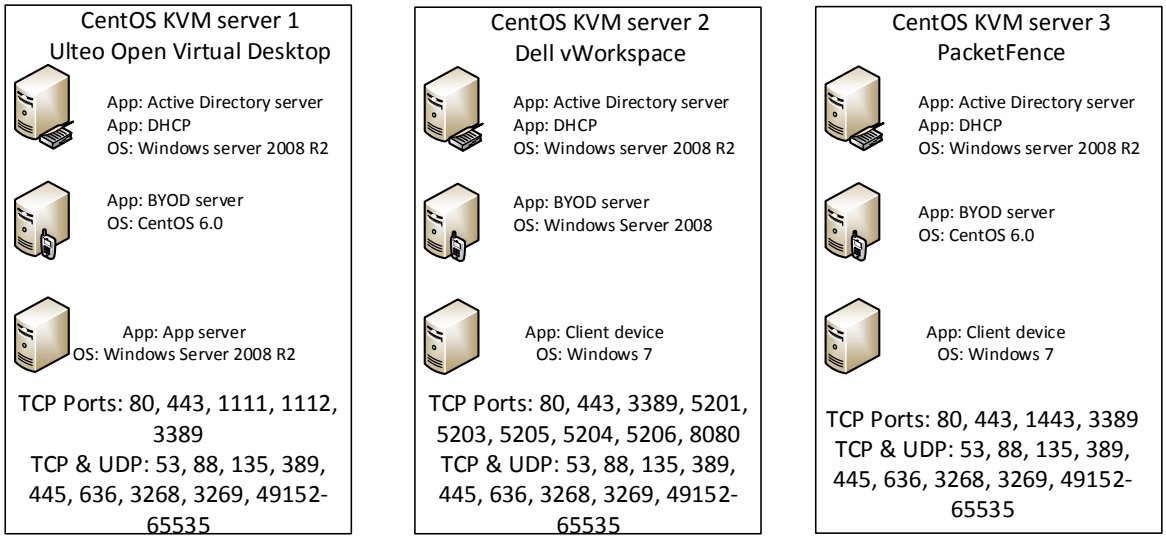
- Een cliënt of applicatie server; waarmee verbinding gemaakt kan worden met de BYOD server

Elke cliënt wordt ingericht met Windows 7 indien deze benodigd is. De cliënt kan ook vervangen worden voor Server 2008 in het geval van een applicatie server.

Mogelijk wordt er nog één extra cliënt of server geïnstalleerd indien dit nodig blijkt.

De opstelling van de Proof of Concept ziet er als volgt uit:





Door deze Proof of Concept opstelling kunnen de producten tegelijk getest worden en is de omgeving toegankelijk van zowel het kantoornetwerk als via VPN. In de Proof of Concept worden de eisen en wensen getest om te bekijken of ze hier aan voldoen. De eisen en wensen zijn:

- Offline mogelijkheden

- Open Source
- Ondersteuning verschillende besturingssystemen (o.a. Windows, Linux en Mac OS)
- Eenvoudig in gebruik (snel en duidelijk toegang voor eind gebruikers)
- Passend binnen de beheeromgeving (gebruik maken van de huidige server OS-en)
- Bedrijfsdata niet lokaal op externe hardware
- Besmettingsgevaar minimaliseren / virusscanners
- Back-up van data
- Netwerkbeveiliging (toegang beveiligd)
- Continuïteit (geen hinder in gebruik)

Tevens wordt er rekening gehouden met de volgende doelstellingen:

- De veiligheid binnen het interne netwerk van SURFsara moet gewaarborgd zijn, waarbij de vraag gesteld wordt: “Hoe kan gegarandeerd worden dat geen besmetting van bedrijfsdata plaatsvindt vanuit bijvoorbeeld een geïnfecteerd werkstation?”.
- Bedrijfsdata mag niet in handen vallen van mensen waarvoor deze informatie niet bestemd is in geval van verlies van data, een werkstation of mobiel apparaat.
- Privédata, inclusief eventuele bedrijfsmail van externe bedrijven, van de gebruiker die eigen hardware gebruikt moet beschermd/afgeschermd worden.
- Externe werknemers moeten gebruik kunnen maken van “Het nieuwe werken” (HNW, remote werken). Dit is in principe al mogelijk gemaakt voor de interne werknemers doormiddel van een VPN verbinding vanaf hun, door SURFsara verstrekte, hardware. Externe werknemers die niet in bezit zijn van SURFsara hardware moeten ook extern kunnen werken zonder in te leveren op het gebied van veiligheid. Daarnaast moeten zij ook via het draadloos netwerk kunnen werken.
- De oplossing(en) moet geschikt zijn voor verschillende besturingssystemen, waaronder Windows, Linux en Mac OS.
- De BYOD oplossing moet beheerd en bijgewerkt kunnen worden.
- Om te kunnen controleren of op de eigen hardware van externe medewerkers onder andere een virusscanner geïnstalleerd is, moet er gemonitord kunnen worden.
- Het BYOD-beleid en -principes dienen te voldoen aan de principes en richtlijnen van het SURFsara informatiebeveiligingsbeleid. Het Informatiebeveiligingsbeleid en de principes van SURFsara zijn opgesteld volgens de ISO standaard voor informatiebeveiliging ISO/IEC 27001:2013. De security maatregelen zijn gebaseerd op Annex A van ISO 27001:2013. Voor de implementatie van de maatregelen wordt gebruikt gemaakt van de norm ISO/IEC 27002:2013. Deze norm beschrijft implementatierichtlijnen voor de security controls.

Naast de eisen, wensen en doelstellingen, worden de functies bekeken om te kijken of er gemakkelijk met het product gewerkt kan worden.

Stappenplan:

De Proof of Concept wordt als volgt per pakket opgebouwd en getest:

1. Installatie CentOS op de Dell hardware
2. Configuratie KVM ten behoeve van VM's
3. Installatie en configuratie Active Directory server VM
4. Installatie BYOD server
5. Installatie cliënt of appserver
6. Configuratie en koppeling BYOD met AD
7. Configuratie en koppeling cliënt met BYOD server
8. Testen van de BYOD software waarbij er rekening gehouden wordt met eisen, wensen en doelstellingen
9. Met de opdrachtgever het pakket doornemen

Nadat het stappenplan uitgevoerd is, is het volgende bekend geworden:

Ulteo Open Virtual Desktop

Ulteo OVD wordt getest en bekeken of de eisen, wensen en doelstellingen voldoen. Hieronder worden de resultaten uit de Proof of Concept weergegeven.

Eisen en wensen	**Voldoet?**	**Toelichting**
Open Source	Ja	Source Code is beschikbaar voor de community editie.
Ondersteuning verschillende besturingssystemen	Ja	Mac, Windows en Linux worden ondersteund.
Eenvoudig in gebruik	Ja	Keuze tussen applicaties en desktop bij login, ook mogelijk om deze in een browser omgeving te starten.
Passend binnen de beheeromgeving	Ja	Windows en Linux (CentOS) kunnen gebruikt worden, deze besturingssystemen worden nu ook gebruikt.
Bedrijfsdata niet lokaal op externe hardware	Ja	Desktop omgeving mogelijk waar alle data opgeslagen wordt, waardoor de data niet lokaal staat.
Besmettingsgevaar minimaliseren / virusscanners	Ja	Scan's kunnen gedaan worden en upload's geblokkeerd worden op de applicatieserver.
Back-up van data	Ja	De userfolders op de servers kunnen geback-upt worden.
Netwerkbeveiliging	Ja	Authenticatie en beveiligde verbinding (SSL) zijn mogelijk.
Continuïteit	Matig	De Remote Desktop Service werkt niet altijd door verkeerde browser cookies. Wanneer deze gewist worden werkt de omgeving meestal wel tot er een aanpassing op de server gedaan wordt.

Doelstelling	Voldoet?	Toelichting
Garantie geen besmetting bedrijfsdata	Ja	Er is een afgeschermde omgeving waar naartoe verbonden kan worden via de browser op de BYOD hardware.
Verlies van data gewaarborgd	Ja	Data staat op de server, waardoor dit niet lokaal staat.
Privédata beschermd/afgeschermd	Ja	Data staat op de server, waardoor dit niet lokaal staat.
Remote werken mogelijk	Matig	Van afstand via VPN kan er verbonden worden naar de omgeving. Echter is slechts voor Windows een Windows Server omgeving mogelijk.
Ondersteuning meerdere besturingssystem	Ja	Mac, Windows en Linux
Beheer en up-to-date houden	Ja	Beheer kan via een admin portal, het updaten kan eenvoudig via de command-line gedaan worden.
Monitoring mogelijk	Matig	Er zijn wel status updates van services etc. Geen mogelijkheid om het gebruik van resources te monitoren.
Conform de ISO27001 norm en de richtlijnen van SURFsara	Ja	Er kan een beveiligde verbinding opgezet worden naar het systeem, door gebruik te maken van SSL certificaten.

Ulteo Open Virtual Desktop streamt alle Windows applicaties via een Windows Terminal Server omgeving. De Remote Desktop die hierdoor mogelijk is, maakt direct verbinding op de Windows server. Hierdoor is er geen cliënt omgeving en kan dit mogelijk schadelijk zijn voor de server. Door de server omgeving zijn er beperkte mogelijkheden om extra of minder beveiligingsregels toe te passen, omdat dit dan voor iedereen geld die verbinding maakt met de server. Het is een aantal keer voorgekomen dat de Remote Desktop service tijdelijk niet werkte of dat de server een verkeerde omgeving toewees door browser cookies. Daarnaast kan niet alles gemonitord worden wat wel gewenst is, zoals de status van het gebruik van resource op de server. In de praktijk voldoet Ulteo Open Virtual Desktop niet helemaal aan de eisen, wensen en doelstellingen van SURFsara.

Dell vWorkspace

De BYOD oplossing van Dell, vWorkspace, wordt ook getest en bekeken aan de hand van eisen, wensen en doelstellingen. Hieronder de resultaten van de Proof of Concept.

Eisen en wensen	Voldoet?	Toelichting
Open Source	Nee	Het is een commercieel product.
Ondersteuning verschillende besturingssystemen	Ja	Mac, Windows en Linux worden ondersteund.
Eenvoudig in gebruik	Ja	Er is een keuze tussen applicaties en een desktop omgeving bij login, ook mogelijk om in een browser omgeving applicaties en de desktop te starten.

Passend binnen de beheeromgeving	Ja	Windows wordt gebruikt, dit besturingssysteem wordt nu ook gebruikt.
Bedrijfsdata niet lokaal op externe hardware	Ja	Data staat op de server, waardoor dit niet lokaal staat.
Besmettingsgevaar minimaliseren / virusscanners	Ja	Virusscanners op verschillende platformen zijn mogelijk, tevens kunnen USB apparaten en netwerk shares geblokkeerd worden.
Back-up van data	Ja	De userfolders op de servers kunnen geback-upt worden.
Netwerkbeveiliging	Ja	Authenticatie en beveiligde verbinding (SSL) zijn mogelijk.
Continuïteit	Ja	Geen problemen ondervonden tijdens het testen.

Doelstelling	**Voldoet?**	**Toelichting**
Garantie geen besmetting bedrijfsdata	Ja	Er is een afgeschermde omgeving waar naartoe verbonden kan worden via de cliënt of via de browser op de BYOD hardware.
Verlies van hardware en data gewaarborgd	Ja	Data staat op de server, waardoor dit niet lokaal staat.
Privédata beschermd/afgeschermd	Ja	Data staat op de server, waardoor dit niet lokaal staat.
Remote werken mogelijk	Ja	Van afstand via VPN kan er verbonden worden naar de omgeving.
Ondersteuning meerdere besturingssystem	Ja	Mac, Windows, Linux worden ondersteund.
Beheer en up-to-date houden	Ja	Via de management console kan de BYOD oplossing beheerd worden. Tevens zijn de nieuwste updates die direct te downloaden zijn in de management console beschikbaar.
Monitoring mogelijk	Ja	Interne mogelijkheden om te monitoren en rapporten te genereren.
Conform de ISO27001 norm en de richtlijnen van SURFsara	Ja	Er kan een beveiligde verbinding opgezet worden naar het systeem, door gebruik te maken van SSL certificaten.

Dell vWorkspace streamt alle applicaties via een Remote Desktop Sessie. Indien er gebruik gemaakt wordt van VM's, kan er verbonden worden met een cliënt omgeving. In eerste instantie kon er alleen verbonden worden met een cliënt, voor het mogelijk maken van in-browser streaming is er een extra BYOD server geïnstalleerd met Server 2012 R2. De VM's worden meestal gekoppeld via een VDI pool van een andere hypervisor, zoals VMWare of Citrix, maar dit is niet noodzakelijk. VM's kunnen ook los toegevoegd worden, waardoor deze persoonlijk ingericht kunnen worden. Beveiliging kan zodoende per VM toegepast worden. In Dell vWorkspace zitten uitgebreide opties om te monitoren. In de praktijk voldoet Dell vWorkspace alleen niet aan de open-source wens.

PacketFence

Als laatste product wordt PacketFence getest en tevens bekeken aan de hand van eisen, wensen en doelstellingen. De resultaten zijn als volgt:

Eisen en wensen	Voldoet?	Toelichting
Open Source	Ja	De source code is beschikbaar.
Ondersteuning verschillende besturingssystemen	Matig	Besturingssystemen worden ondersteund, echter de scan engines zijn slechts bedoeld voor IOS en Windows, maar niet voor Linux.
Eenvoudig in gebruik	Matig	Indien er geblokkeerd wordt, kan het lastig zijn voor de gebruiker doordat zij niets meer kunnen doen.
Passend binnen de beheeromgeving	Ja	Windows en Linux (CentOS) kunnen gebruikt worden, deze besturingssystemen worden nu ook gebruikt.
Bedrijfsdata niet lokaal op externe hardware	Nee	De data staat nog steeds lokaal op de hardware.
Besmettingsgevaar minimaliseren / virusscanners	Matig	Besmette hardware zou niet toegang tot het netwerk moeten krijgen. Echter als er iets niet gedetecteerd wordt is besmetting mogelijk.
Back-up van data	Nee	Gebruikers zijn in dit geval zelf verantwoordelijk voor een back-up van de data, omdat dit lokaal kan staan.
Netwerkbeveiliging	Ja	Authenticatie en beveiligde verbinding (SSL) zijn mogelijk. Daarnaast kan er gescand worden tijdens of voor het inloggen op de portal.
Continuïteit	Matig	Als het pakket cliënts blokkeert kan dit hinder veroorzaken, doordat al het verkeer dan geblokkeerd wordt.

Doelstelling	Voldoet?	Toelichting
Garantie geen besmetting bedrijfsdata	Matig	Besmette hardware zou niet in het netwerk toegang moeten krijgen. Echter als er iets niet gedetecteerd wordt is besmetting nog mogelijk.
Verlies van hardware en data gewaarborgd	Nee	Extra maatregelen moeten genomen worden, het pakket zelf doet dit niet omdat de data lokaal staat. In dit geval moet er een oplossing gevonden worden om van afstand data te verwijderen.
Privédata beschermd/afgeschermd	Nee	Extra maatregelen moeten genomen worden, het pakket zelf doet dit niet. Er zijn zelfs

		mogelijkheden in het pakket om juist de privédata ook te scannen waardoor er mogelijk privacy issues kunnen ontstaan.
Remote werken mogelijk	Ja	Van afstand via VPN kan er verbonden worden naar de omgeving.
Ondersteuning meerdere besturingssystem	Ja	Mac, Linux, Windows worden ondersteund.
Beheer en up-to-date houden	Ja	Beheer is mogelijk via de admin portal. Het pakket is eenvoudig te updaten via command-line.
Monitoring mogelijk	Matig	Via de portal zijn logs uit te lezen. Via de email kunnen de schendingen (malware gevonden en dergelijke) gestuurd worden. Andere opties zijn niet mogelijk.
Conform de ISO27001 norm en de richtlijnen van SURFsara	Ja	Er kan een beveiligde verbinding opgezet worden naar het systeem, door gebruik te maken van SSL certificaten.

Packetfence voldoet niet geheel aan de eisen en doelstellingen. Dit was bij de pakketselectie al bekend, echter zou het in de praktijk anders kunnen zijn. In de praktijk blijkt dat het product alsnog niet voldoet, omdat het product direct achter de VPN-verbinding geplaatst moet worden. Al het verkeer van de VPN-verbinding moet dan ook via de Packetfence server. Hierdoor kan er een single-point of failure voor alle gebruikers ontstaan. Daarnaast kan dit tot ongewenste effecten leiden op BYOD hardware, doordat gebruikers moeten registreren en voldoen aan de voorwaardes van Packetfence om verder te kunnen. Een ongewenst effect kan zijn dat al het verkeer gescand wordt en opgeslagen wordt in logfiles. Dit kan tot privacy issues leiden.

Bijlage 8: Adviesrapport

Versiebeheer

Datum	Versie	Reviewer	Beschrijving
19-04-2016	0.1	Dion Kruijswijk	Opzet adviesrapport
02-05-2016	0.2	Dion Kruijswijk	Toevoeging aanbevelingen
04-05-2016	0.3	Dion Kruijswijk	Toevoeging beleidsregels
06-05-2016	0.4	Dion Kruijswijk	Aanpassing aanbevelingen
09-05-2016	0.5	Dion Kruijswijk	Toevoeging aanbevelingen
10-05-2016	0.6	Dion Kruijswijk	Toevoeging technische oplossing, aanpassing aanbevelingen
13-05-2016	0.7	Dion Kruijswijk	Aanpassing aanbevelingen
17-05-2016	0.8	Dion Kruijswijk	Toevoeging conclusie
18-05-2016	0.9	Dion Kruijswijk	Aanpassing beleid en technische oplossing
23-05-2016	0.9	Leonieke Mevius	Feedback op versie 0.9
24-05-2016	1.0	Dion Kruijswijk	Feedback op versie 0.9 verwerkt, definitieve versie gemaakt

Inhoudsopgave

1.Inleiding

Voor SURFsara is er onderzoek gedaan naar het veilig toepassen van het Bring Your Own Device principe. SURFsara wil dat externe werknemers gebruik kunnen maken van hun eigen hardware, maar dit op een veilige manier gebeurt. Per jaar worden er ongeveer 21 medewerkers ingehuurd, die soms eigen hardware gebruiken. Deze BYOD hardware wordt gebruik voor het uitvoeren van de werkzaamheden, maar ook voor toegang tot data en/of diensten van SURFsara.

Op de BYOD hardware wordt geen controle uitgevoerd. Hierdoor kan het niet gegarandeerd worden dat de het veilig is dat BYOD aangesloten is op het netwerk. Als externe medewerkers een besmetting hebben, kan dit mogelijk ook schadelijk zijn voor de bedrijfsdata van SURFsara of andere systemen. Om dit te voorkomen moet er een beleid opgesteld worden. In het beleid wordt onder andere de richtlijnen, de aanbevolen applicaties, de aansprakelijkheid en de maatregelingen beschreven. Het beleid en de bijbehorende doelstellingen worden in het hoofdstuk “Beleid opstellen” beschreven.

Een beleid kan niet zonder een technische oplossing. De technische oplossing zorgt er voor dat eventuele besmettingen verminderd of voorkomen worden. De technische oplossing is gekozen door gebruik te maken van een toepassingsselectie, waarin diverse producten in theorie bekeken zijn. Vervolgens zijn deze in een Proof of Concept getest. De uitwerking hiervan is beschreven in het hoofdstuk “Technische ondersteuning”.

Het beantwoorden van de hoofdvraag van het onderzoek wordt beschreven in het hoofdstuk Conclusie. Om een ideale situatie te bereiken, zouden er aanpassingen plaats moeten vinden in het bedrijf om het BYOD principe veilig toe te kunnen staan. Deze aanpassingen worden in het hoofdstuk Aanbevelingen beschreven.

2.Beleid opstellen

In dit hoofdstuk wordt de inhoud van het BYOD beleid beschreven, zodat deze gebruikt kan worden door SURFsara. In het beleid zijn de Annex controls van de ISO27001 norm opgenomen. Deze worden per onderdeel indien nodig benoemd.

2.2.Richtlijnen

Voor externe werknemers moet een beleid opgesteld worden, waar zij akkoord mee moeten gaan indien zij BYOD hardware willen gebruiken. Het beleid bevat de richtlijnen voor het gebruik van de BYOD hardware. Deze richtlijnen kunnen het volgende bevatten:

- Gebruik van een virusscanner

Besmettingen worden voorkomen of verwijderd door een virusscanner op de BYOD hardware te installeren. F-secure kan als virusscanner gebruikt worden op cliënts.

- Geen illegale programma's gebruiken

Veel besmettingen komen van illegale programma's. Wanneer het gebruik van dergelijke programma's verboden is, is de kans op besmetting kleiner.

- Hoe kan SURFsara data of een dienst benaderd worden

Data of een dienst kan benaderd worden door gebruik te maken van Wi-Fi (Eduroam of het gasten netwerk) binnen het kantoorpand van SURFsara en daarna te verbinden met de VPN of vanaf elke externe locatie via VPN. De cliënt hiervoor is OpenVPN, andere VPN cliënts worden niet ondersteund. Hierna kan verbinding gemaakt worden met de BYOD oplossing via de cliënt of de webbrowser.

- Gebruik van complexe wachtwoorden

Om toegang te krijgen met BYOD hardware, moet er het wachtwoord dat gebruikt wordt voor data en/of diensten 'complex' zijn. Complex houdt in dat het wachtwoord minstens één hoofdletter, één kleine letter, één cijfer, één symbool bevat en de lengte heeft van minimaal 8 tekens.

- Periodiek een nieuw wachtwoord kiezen

Om te voorkomen dat wachtwoorden in handen vallen van personen waar deze niet voor bedoeld zijn, worden wachtwoorden periodiek veranderd. Hierbij kan er gekozen worden om dit elke maand te doen of in ieder geval elke twee maanden.

- Data opslag

Externe data opslag moet in het beleid opgenomen worden. Vanwege het gemakkelijk kwijtraken van USB-sticks en dergelijke, is het niet gewenst dat deze gebruikt worden. Het koppelen van shares aan de BYOD oplossing is niet toegestaan, vanwege de verspreiding van malware.

- Beveiligde of geen lokale data

Wanneer SURFsara data lokaal staat, mag dit slechts data als de hardware beveiligd is door middel van encryptie. In alle andere gevallen mag er geen SURFsara data lokaal staan op de BYOD hardware.

- Support en training

Indien er problemen zijn met het gebruik van de BYOD oplossing, moet er support gegeven kunnen worden. Een handleiding voor het gebruik van de BYOD oplossing wordt gedocumenteerd. Hierdoor kunnen gebruikers direct van start. Indien gewenst kunnen er trainingssessies plaatsvinden.

- Periodieke audits

Om te bekijken of het beleid gehanteerd wordt en voldoet, worden periodieke audits uitgevoerd. In deze audits wordt een steekproef gedaan waarbij het gebruik van de BYOD apparatuur bekeken wordt en of alles nog voldoet aan de richtlijnen.

- Kosten, vergoeding of leenapparatuur

Werknemers krijgen in plaats van hardware van SURFsara mogelijk een vergoeding. Deze vergoeding wordt in het beleid vermeld en moet aantoonbaar besteed zijn aan hardware door middel van een bon/rekening van de aanschaf. Als alternatief zou er gekozen kunnen worden om 'verouderde' hardware in te zetten. Deze hardware is al afgeschreven, maar kan gebruikt worden voor de BYOD oplossing. Indien werknemers al eigen hardware hebben en die willen gebruiken, mogen zij die gebruiken maar kunnen zij geen aanspraak doen op een vergoeding.

- Werkplek bepaling

In het beleid moet opgenomen worden waar (externe) werknemers kunnen werken. Deze werkplekbepaling bevat het thuis/extern werken en in specifieke gevallen het werken op de SURFsara locatie.

- Niet mailen naar de virtuele omgeving

De makkelijkste manier om vanaf de BYOD hardware bestanden over te zetten naar de VM bedoeld voor de BYOD hardware, is om de bestanden te mailen. Dit blijft altijd mogelijk, echter moet in het beleid opgenomen worden dat dit niet toegestaan is.

2.2.Aansprakelijkheid

Naast de richtlijnen zijn er momenten waarin bepaalde partijen aansprakelijk kunnen zijn, deze zijn SURFsara of de medewerker. De volgende aansprakelijkheidsafspraken moeten gemaakt worden:

- Eigenaar hardware

In het beleid moet opgenomen worden van wie de hardware is die voor werkzaamheden gebruikt wordt. Indien er een vergoeding gegeven wordt, moet er vermeld worden of de hardware uiteindelijk van SURFsara of van de externe werknemers is. In het geval van leenapparatuur is de hardware altijd van SURFsara. Wanneer eigen hardware gebruikt wordt, is dit van de werknemer.

- Gebruik van applicaties

Vanuit SURFsara worden er applicaties aangeboden waarmee gewerkt kan worden. Indien de werknemer zelf extra applicaties installeert welke besmettingen of schade kunnen veroorzaken, is de werknemer verantwoordelijk. Illegale programma's zijn nooit toegestaan. Bij het installeren moeten werknemers altijd melden dat zij deze gebruiken. Als alternatief kan er gekozen worden om geen rechten te verlenen waarmee applicaties geïnstalleerd kunnen worden.

- Diefstal

Wanneer eigen hardware gestolen wordt, is de werknemer hier zelf aansprakelijk voor. De werknemer kan hier zelf preventieve maatregelingen voor nemen. Indien data lokaal staat, moet er encryptie toegepast worden zodat in het geval van diefstal de data niet in verkeerde handen kan vallen.

- Verlies van data

Voor het verlies van privédata is de werknemer zelf aansprakelijk. Indien het om bedrijfsdata gaat is SURFsara verantwoordelijk voor een back-up hiervan mits deze op de servers opgeslagen worden. In het beleid moet opgenomen worden hoe vaak er geback-upt wordt, wanneer deze gecontroleerd wordt en waarop. De werknemer is verantwoordelijk bij verlies of diefstal dit zo snel mogelijk te laten weten aan Argos, zodat zij actie kunnen ondernemen.

- Meldingen maken van bugs en dergelijke

Mochten de gebruikers van BYOD hardware bugs, backdoors, foutief ingestelde poorten of andere 'vreemde' problemen tegen komen tijdens hun werk, zijn zij verantwoordelijk dit direct te melden. SURFsara is vervolgens verantwoordelijk om de problemen op te lossen als de problemen mogelijk werkzaamheden in gevaar kunnen brengen.

2.3.Risico's

Door het implementeren van het BYOD beleid en de oplossing, kunnen eventueel risico's voorkomen of bekend worden die daarvoor er niet waren. Deze risico's moeten in het beleid opgenomen worden om aan de ISO27001:20013 norm te voldoen. Een aantal van deze risico's zijn in Tabel 14: Risico's BYOD benoemd.

Risico	Preventieve actie
BYOD gebruikers houden zich niet aan het beleid.	Periodieke audits om te achterhalen wie zich niet aan het beleid houdt. Indien nodig een waarschuwing geven of in extreme gevallen een (tijdelijke) blokkering op het systeem voor de specifieke gebruiker(s).
De BYOD oplossing is niet veilig genoeg.	Verkeer kan standaard geëncrypt worden, bijvoorbeeld met SSL. Daarnaast kan er gebruik gemaakt worden van 2-way authentication.
De externe werknemers maken niet verbinding met Wi-Fi netwerken en vervolgens met de VPN, maar met het kantoornetwerk.	Het kantoornetwerk niet toegankelijk maken voor BYOD hardware. Er kan gekozen worden om het kantoornetwerk om te zetten naar een gasten netwerk, waarna er alsnog een VPN verbinding opgezet moet worden voordat data benaderd kan worden.
Data wordt lokaal opgeslagen, op USB-stick of op de BYOD hardware zelf.	Opslag media niet toe staan en eventuele audits om te bekijken of gebruikers lokale data hebben staan.
Gebruikers verliezen de BYOD hardware en hebben logins lokaal opgeslagen, maar geen beveiliging of encryptie.	Bij verlies van hardware moet dit direct gemeld worden. Hierdoor kunnen account tijdelijk geblokkeerd worden.

TABEL 14: RISICO'S BYOD

2.4.Maatregelen

Om te zorgen dat het beleid nageleefd wordt, moeten maatregelen genomen kunnen worden als dit niet zo is. Het kan namelijk zijn dat werknemers handelingen verrichten die in strijd zijn met het beleid. De volgende maatregelingen kunnen toegepast worden:

- Waarschuwing

Indien een handeling in strijd is met het beleid, kan er gekozen worden om een waarschuwing te geven aan het persoon die de handeling uit voert. Na een aantal, bijvoorbeeld 2 of 3, foutieve handelingen kan er een andere maatregel toegepast worden.

- Tijdelijk de toegang ontzeggen

Een gebruiker kan tijdelijk de toegang tot diensten en data ontzegd worden, in het geval van diefstal, herhaaldelijk foutief handelen of in andere nader te bepalen gevallen.

- Permanent de toegang ontzeggen

Indien een gebruiker echt foutieve handelingen verricht of herhaaldelijk dit doet, kan er gekozen worden om permanent de toegang te ontzeggen. Dit wordt in uitzonderlijke gevallen gedaan.

3.Technische ondersteuning

Om externe medewerkers toegang te geven tot data en applicaties van SURFsara, moet er een technische oplossing geïmplementeerd worden. Deze oplossing is gekozen naar aanleiding van een toepassingsselectie. In de toepassingsselectie zijn drie producten getest, Ulteo Open Virtual Desktop, PacketFence en Dell vWorkspace.

Ulteo Open Virtual Desktop voldoet niet, omdat er slechts verbinding gemaakt kan worden met een server omgeving. Hierbij zijn er beperkte mogelijkheden en is het mogelijk dat de server zelf besmet wordt, doordat er lokaal opgeslagen wordt. De continuïteit kan ook in gevaar komen, doordat de Remote Desktop service niet altijd goed werkt. De monitoring mogelijkheden zijn matig, er moet een extra tool gebruikt worden. Hierdoor voldoet Ulteo niet, maar zou voor app streaming wel gebruikt kunnen worden vanwege de Open-source.

PacketFence voldoet ook niet, omdat besmettingen eventueel wel door kunnen komen en de continuïteit mogelijk beperkt kan worden. PacketFence moet zo ingesteld zijn dat alles geredirect wordt zolang er niet ingelogd is, waardoor er mogelijk niet met de BYOD hardware te werken is als er iets fout gaat. Verlies van data is nog steeds mogelijk en privédata kan niet beschermd worden. Niet alles kan gemonitord worden vanuit de portal, waardoor er een extra tool gebruikt moet worden. Wel kan er gekozen worden om PacketFence achter de VPN te implementeren als extra beveiliging. Hierbij wordt de cliënt gescand, bekeken of de cliënt up-to-date is en of een virusscanner geïnstalleerd is. Indien er virussen gevonden zijn, de cliënt niet up-to-date is of er geen virusscanner geïnstalleerd is wordt de toegang geblokkeerd tot het netwerk.

Ter ondersteuning van het beleid, kan het beste de oplossing Dell vWorkspace gebruikt worden. Met Dell vWorkspace kunnen diverse besturingssystemen verbinding maken via een cliënt applicatie. Op de VM’s kunnen bestanden via de cliënt applicatie opgeslagen worden. Daarnaast is het ook mogelijk om vanuit de browser applicaties te streamen, waardoor een cliënt installatie niet benodigd is. Het toewijzen van de toegang tot een VM kan gedaan worden via de Active Directory en indien nodig kan hierdoor de toegang eenvoudig ontzegt worden. De VM’s kunnen opgebouwd worden via een VDI pool op VMWare of Citrix, echter is het ook mogelijk om ‘losse’ VM’s te koppelen zonder een extra omgeving. Door deze losse VM’s te gebruiken, kan er per VM een gebruiker toegewezen worden en kunnen er persoonlijke instellingen gemaakt worden. De VM’s kunnen beheerd worden zoals een normale cliënt met bijvoorbeeld CFEngine. Bij het gebruik van Dell vWorkspace wordt er aan alle eisen voldaan.

4.Conclusie

Om het BYOD principe veilig toe te kunnen passen, moet er een beleid geschreven worden. In dit beleid staan richtlijnen waar externe werknemers zich aan moeten houden. De richtlijnen zijn er voor bedoel om de omgeving zo veilig mogelijk te houden en ervoor te zorgen dat het duidelijk is voor externe werknemers wat zij wel en niet mogen.

In het beleid moet ook een hoofdstuk gewijd worden aan aansprakelijkheid, waarin beschreven wordt in welke situaties iemand aansprakelijk is. Zodra deze aansprakelijkheden beschreven zijn, is het duidelijk voor zowel de gebruiker als SURFsara wie de probleem eigenaar is. Beide partijen moeten zich aan het beleid houden.

Voor de ISO27001 norm zijn er risico's opgesteld voor het gebruik van BYOD hardware. Op deze risico's kunnen preventieve maatregelen genomen worden. De risico's richten zich zowel op organisatorisch als technische gebied.

Indien externe werknemers zich niet houden aan het beleid, kan er voor gekozen worden om maatregelen te nemen. Dit kan een waarschuwing inhouden, echter bij ernstig misbruik kan de toegang ook ontzegd worden. Door hier een hoofdstuk aan te wijden, weten de externe gebruikers waar zij aan toe zijn in het geval van misbruik.

Het beleid kan echter niet zonder technische ondersteuning. De technische ondersteuning dwingt gebruikers zich aan het beleid te houden. Dell vWorkspace voldoet het best als technische ondersteuning, omdat het voldoet aan bijna alle eisen, wensen en doelstellingen. De andere twee pakketten voldoen minder goed, echter kunnen deze wel gebruikt worden voor andere doeleinden binnen SURFsara.

Het beleid en de technische oplossing kunnen er voor zorgen dat het BYOD veilig en op een goed te beheren wijze toegepast kan worden, waarbij de integriteit en vertrouwelijkheid van SURFsara data en privédata gewaarborgd worden.

5.Aanbevelingen

Externe medewerkers geen hardware meer van SURFsara.

Momenteel worden laptops gebruikt van SURFsara door externe werknemers. Deze hardware wordt nu gekozen door het CYOD beleid, maar het is gewenst dat alle externe medewerkers de BYOD oplossing gebruiken.

Externe medewerkers kunnen toegang krijgen tot de BYOD oplossing. Mijn aanbeveling is om de betreffende medewerkers over te laten gaan op de BYOD oplossing. Als momenteel een overtreding plaatsvindt en er gekozen wordt om de laptop in te nemen, kan de gebruiker nog lokaal bestanden aanpassen of verspreiden. Met de BYOD oplossing kan indien nodig de toegang tot services en data ontzegd worden, zodat er niets meer aangepast of verspreid kan worden. Daarnaast blijft het beleid uniform als iedereen over gaat naar de BYOD oplossing, in plaats van dat er voor specifieke personen een uitzondering gemaakt wordt.

VM's per gebruiker

In de oplossing is het mogelijk om gebruik te maken van een VDI omgeving waar dynamische of statische VM's toegewezen worden. Het voordeel van een dynamische VM ten opzichte van een statische is dat de VM's uit gaan als deze niet gebruikt worden. Hierdoor wordt er minder gebruik gemaakt van het netwerk, de processorkracht en het geheugen van de server. In een dynamische omgeving zijn de VM's allemaal hetzelfde. Het nadeel van dynamische VM's is dat indien er persoonlijke instellingen gemaakt moeten worden, deze losgekoppeld moeten worden. Hierdoor wordt het alsnog een statische VM. Bij dynamische VM's moet ook alle software geïnstalleerd worden die gebruikers gebruiken. Hierdoor krijgen sommige gebruikers applicaties in hun omgeving die zij nooit gebruiken.

Mijn aanbeveling is om VM's per gebruiker in te richten. Deze VM's staan wel altijd aan maar kunnen gepersonaliseerd worden. Applicaties kunnen per gebruiker bepaald worden en er kunnen eventuele restricties op gebruikers ingesteld worden. Een restricties kan bijvoorbeeld zijn dat gebruikers geen administrator rechten hebben, waardoor zij zelf geen extra applicaties kunnen installeren.

Ondertekening beleid in verband met aansprakelijkheid

Voor het gebruik van BYOD hardware wordt een beleid opgesteld. In dit beleid worden de richtlijnen en aansprakelijkheid opgenomen. De richtlijnen omvatten het gebruik van de BYOD oplossing en de aansprakelijkheid omvat wie er verantwoordelijk is.

Mijn aanbeveling is om externe medewerkers het BYOD beleid te laten ondertekenen. Doordat in het beleid opgenomen is wie er verantwoordelijk is, kan later geen aanspraak gemaakt worden dat het niet bekend was. Dit voorkomt problemen indien er ongewenste situaties voorkomen waarin het anders niet bekend zou zijn wie er verantwoordelijk is. Het beleid kan in de indiensttredingsprocedure verwerkt worden als interne medewerkers ook BYOD hardware willen gebruiken.

Beheerder toewijzen

Indien een BYOD oplossing toegepast wordt, moet de oplossing bijgehouden worden. Onder het bijhouden valt het monitoren van services, het monitoren van het gebruik van VM's en het

monitoren van de applicaties. Wanneer een nieuwe externe medewerker een VM nodig heeft, moet deze aangemaakt worden, de toegang tot de VM ingeregeld worden en de VM geconfigureerd worden. Daarnaast moet het mogelijk zijn om de toegang te ontheffen.

Het is raadzaam om een beheerder toe te wijzen aan de BYOD oplossing indien deze geïmplementeerd wordt, zodat de continuïteit gewaarborgd wordt.

Gebruik van VM templates

Wanneer de BYOD oplossing gebruikt wordt, moeten er voor externe medewerkers VM's aangemaakt worden. Het is ook mogelijk dat het aantal externe medewerkers groeit, waardoor meerdere VM's later aangemaakt moeten worden. Het aanmaken, configureren en updaten van een VM kan tijdrovend zijn.

Om tijd te besparen is het raadzaam dat er gebruik gemaakt wordt van templates om VM's snel aan te maken. Deze VM's kunnen in eerste instantie een clone zijn, waarbij er daarna instellingen aangepast worden. Door het gebruik van een template die periodiek bijgewerkt wordt betreft updates, zijn nieuwe VM's altijd up-to-date.

Support

Wanneer gebruikers de BYOD oplossing gebruiken, is het bijna onoverkomelijk dat er problemen optreden of dat gebruikers vragen hebben.

Mijn aanbeveling is om een apart hoofdstuk te wijden aan support in het beleid. In dit hoofdstuk staan de contact gegevens van een afdeling waarbij gebruikers terecht kunnen indien er problemen of vragen zijn.

Toepassing Defense in Depth

Op cliënts en servers in het kantoornetwerk zijn virusscanners geïnstalleerd. Op de firewall is er IDS en IPS ingericht. Het is mogelijk dat er op cliënts en servers dezelfde virusscanners staan, waardoor er exploits gebruikt kunnen worden.

Mijn aanbeveling is om verschillende virusscanners op de cliënts en servers te installeren. Hierdoor is het mogelijk dat als de virusscanner malware op de cliënts niet detecteren, de servers de malware mogelijk wel detecteren. Daarnaast kan er voor gekozen worden om ook op de BYOD server een andere virusscanner te installeren. Indien F-secure op de cliënts gebruikt wordt, moet er op de servers en de BYOD server een andere virusscanner geïnstalleerd worden.

Audits op het beleid en de technische oplossing

Naar mate het beleid toegepast wordt en de technische oplossing gebruikt wordt, kan het zijn dat het beleid niet meer voldoet. Indien dit zo is, dient het beleid aangepast te worden.

Het is hierdoor raadzaam om periodiek audits plaats te laten vinden, zowel om de beveiliging als gebruik van applicaties en bestanden te controleren. Hierdoor blijft het beleid up-to-date en de technische oplossing zo optimaal mogelijk.

Apart netwerk voor de BYOD oplossing

Indien BYOD gebruikers verbinding moeten maken met de huidige VPN-verbinding, hebben zij meestal ook toegang tot het kantoornetwerk. Het is echter niet altijd gewenst dat gebruikers bij applicaties of data van SURFsara kunnen.

Het is hierdoor aanbevolen om de BYOD oplossing in een apart netwerk te plaatsen of in ieder geval op een andere manier toegankelijk. Hiervoor zou een tweede VPN-verbinding voor gebruikt kunnen worden. Specifieke VM's die gekoppeld zijn via de BYOD oplossing kunnen toegelaten worden tot het kantoornetwerk van SURFsara of specifieke file-shares door firewall regels te maken.

PacketFence als VPN beveiliging

Hoewel het product PacketFence niet voldoet voor het toepassen van het BYOD principe, kan het wel gebruikt worden als extra beveiliging op de VPN verbinding. Gebruikers moeten hierna één keer extra inloggen voordat zij toegang krijgen tot het netwerk. De hardware kan dan gescand worden op virussen en hardware blokkeren indien er virussen gevonden zijn.

De afweging moet gemaakt worden of PacketFence geschikt is om de VPN verbinding extra te beveiligen. Al het VPN verkeer moet via PacketFence, waardoor het een single-point of failure is. Om dit op te lossen zou er een loadbalancer geplaatst moeten worden, waardoor de kosten hoger worden. Daarnaast is er geen mogelijkheid om Linux distributies te scannen tijdens het verkrijgen van toegang tot het netwerk. Hierdoor is PacketFence beperkt inzetbaar.

Wet bescherming persoonsgegevens (Wbp)

Vanaf begin 2016 is de Wbp (Overheid.nl, 2015) van toepassing. In deze wet wordt de verplichting om datalekken te melden behandeld. Bij het gebruik van de BYOD oplossing, is het mogelijk dat gebruikers referenties opslaan om gemakkelijk in te loggen. Wanneer de hardware van de gebruiker gestolen of gehackt wordt, kan hierdoor een datalek ontstaan. Vanaf 2018 kan de boete die opgelegd wordt erg hoog zijn.

Het is niet geheel bekend of de Wbp van toepassing is op het BYOD principe en wie er aansprakelijk zijn. Hoewel in het beleid beschreven staat dat gebruikers voorzichtig om moeten gaan met data, kan het voorkomen dat een datalek toch voorkomt. Indien de BYOD oplossing toegepast wordt, moet er uitgezocht worden of de Wbp van toepassing is op BYOD en welke extra maatregelen genomen moeten worden.