LAB-PC'S OP HET UT-NET

MARC BERENSCHOT

VERSIE: 1.0

1-4-2022

UNIVERSITY OF TWENTE.

COLOPHON

MANAGEMENT
LISA-DSM
Publiek

DATE
1-4-2022

VERSION
1.0

AUTHOR(S)
Marc Berenschot

EMAIL
m.berenschot@utwente.nl

TABLE OF CONTENT

1. INLEIDING

Dit document richt zich op de apparatuur die een netwerk-”aansluiting” gebruikt en vooral in lab-achtige situaties ingezet wordt. In dit document wordt dat de Lab-pc genoemd, maar dat is slechts een naam. Het kan ingebouwd zitten in andere apparatuur of redelijk autonoom zijn zoals bijvoorbeeld een robot of meetapparaat. Lab-pc’s die geen netwerkaansluiting gebruiken zijn niet volledig buiten scope, maar veel van de maatregelen zullen niet van toepassing zijn.

De beveiliging van aan het UT-netwerk gekoppelde apparatuur wordt steeds belangrijker. Er zijn situaties waarin de standaard beveiligingsmethodieken zoals die voor de UT-werkplek en standaard UT-servers gebruikt worden niet uitvoerbaar zijn. Dit speelt vooral op Lab-pc’s.

Systemen die persoonsgegevens verwerken vallen buiten de scope van dit document. Daar geldt specifieke wetgeving voor die veel strenger is en de voorgestelde maatregelen kunnen tegen wetgeving op dit gebied in gaan.

Allereerst wordt vastgesteld wat nodig is om een Lab-pc goed te laten functioneren. In het hoofdstuk daarna worden relevante ICT-middelen en technieken genoemd die hiervoor te gebruiken zijn. Vervolgens wordt stil gestaan bij de standaard beveiligingseisen die de UT stelt en wordt uitgewerkt wat de alternatieven zijn als dat strijdig is met de eisen die nodig zijn om de Lab-pc goed te laten functioneren.

Tot slot zullen nog extra services benoemd worden die ingezet kunnen worden om de beveiliging verder te verbeteren.

1.1 DEFINITIES

Naast de omschrijving van Lab-pc hierboven zullen de volgende termen gebruikt worden:

UT-Net	Het netwerk zoals dat op de UT aanwezig is. Hierop zitten alleen mensen met een relatie tot de UT (gasten met bijv. X-accounts vallen hier dus ook onder)
Internet	Het netwerk buiten de UT, incl. de cloud.
UT account	Het account dat iedere medewerker, student of gast krijgt en dat voor strikt persoonlijk gebruik bedoeld is.
Lab	Een verzamelplaats van apparatuur anders dan UT-werkplekken. In deze context wel apparatuur dat van het netwerk gebruikt maakt of over enige eigenschappen van een PC beschikt.
Functioneel account	Een niet-persoonlijk account. Op dit moment (eerste opzet) kan een functioneel account zowel een account in AD als een lokaal account zijn. Het is vooral een account dat door meerdere personen gedeeld wordt.
Remote Login	De lab-pc gebruiken vanaf een andere locatie/pc.

2. WENSEN VAN DE LAB-BEHEERDERS

Voor het gebruik van lab-pc's zijn een aantal zaken noodzakelijk. Niet iedere Lab-pc zal dit allemaal nodig hebben, maar over alle Lab-pc's heen gelden de volgende eisen:

1. Een Lab-pc kan niet zomaar ge-update worden en soms zelfs helemaal niet.
2. Een Lab-pc kan software/hardware nodig hebben die door een leverancier niet meer ondersteunt wordt. Bekendste voorbeeld is Windows 7 PC's.
3. Op een Lab-pc moet met een gedeeld account gewerkt kunnen worden. Soms is het zelf onwenselijk om met UT accounts te werken.
4. Een Lab-pc moet data uit kunnen wisselen. Soms met andere Lab-pc's, soms met systemen buiten het lab. Soms moet data van een gedeelde user overgezet kunnen worden naar een UT account.
5. Een Lab-pc moet het internet op kunnen, soms om bijv. updates op te halen (dus een technische reden) maar soms ook omdat de gebruiker van de Lab-pc dat nodig heeft.
6. Een Lab-pc moet soms van buiten het lab bereikbaar zijn.
7. Op een Lab-pc moet met admin-rechten gewerkt kunnen worden.
8. Een Lab-pc kan niet altijd opgenomen zijn in een domein (in de praktijk: AD).
9. Een verzwaring van administratieve lasten moet zoveel mogelijk voorkomen worden.
10. Een Lab-pc moet soms benaderbaar zijn door derden (bijv. leveranciers).
11. Een Lab-pc kan toegang tot M: , P: , U: en Software-center nodig hebben.

3. RELEVANTE TECHNIEKEN EN MIDDELEN

Er zijn een aantal technieken en middelen die ingezet kunnen worden om bovenstaande doelen op een veilige manier te bereiken. In dit hoofdstuk worden die middelen beschreven. Eis 9 geldt voor ieder punt en wordt hier verder niet behandeld.

3.1 LAB-VLANS

Relevante eisen: 1, 2, 5, 6 en 10.

Een VLAN is een virtueel netwerk om systemen die bij elkaar horen te groeperen. Voor Lab-pc's is vaak vraag naar afscherming om de systemen te beschermen en om systemen die niet volledig geüpdatet kunnen worden toch veilig in te zetten. Een VLAN kan deze afscherming bieden.

Het verkeer binnen is VLAN is ongefilterd, dus de systemen in een VLAN kunnen goed met elkaar samenwerken.

Een VLAN heeft als voordeel dat meerdere Lab-pcs eenzelfde netwerk gebruiken en er dus binnen de lab-omgeving een eigen netwerk bestaat waarin de Lab-pc's onderling eenvoudig kunnen communiceren. De beveiliging die ingericht is geldt dan direct voor het gehele VLAN, zodat hier niet per Lab-pc aandacht aan gegeven hoeft te worden en de kans op fouten kleiner wordt.

Het inprikken van je UT-werkplek in een VLAN is niet mogelijk.

3.1.1 **Standaard VLAN**

Een standaard VLAN heeft de volgende kenmerken:

- Privé IP-adressen
- Registratie op basis van MAC-adres (via netwerkgroep)
- Geregistreerde systemen krijgen een vast IP-adres
- Alleen geschikt voor 'bedrade' netwerkaansluitingen.
- Proxy: Nuttig om wel het internet op te kunnen of bijv. updates op te halen. Standaard aan. Kan op verzoek aangepast worden. Let op dat dit nog wel op de client geconfigureerd moet worden.
- Standaard alleen toegang tot cruciale infrastructuur zoals DNS/DHCP.

3.1.2 Opties

De volgende opties zijn beschikbaar:

- Toegang tot alle LISA/Vakgroep servers in datacentrum. Dit zet je oa. in als je toegang tot het AD-domein nodig hebt voor bijvoorbeeld UT accounts of toegang tot M/P:-schijf
- Aanpassingen toegang proxy (standaard aan voor alle systemen)
- Het is mogelijk om toegang van en naar geselecteerde systemen op het UT-net krijgen (als dat systeem een vast IP-adres heeft).
- Toegang tot EfficientIP om zelf MAC-adressen te registreren. Daar is nog geen handleiding voor, maar is zonder handleiding ook goed te doen.
- Remote Login

3.1.3 Remote login

Dit kan binnen een VLAN omdat het mogelijk is toegang van en naar geselecteerde systemen te krijgen. Om remote login buiten het UT-net te gebruiken moet de hele VPN-range toegevoegd worden aan de systemen die van buiten toegang krijgen. Remote Login via RDP (Windows Remote Desktop) buiten de UT zonder VPN is een te groot security risico en wordt niet aangeboden. TeamViewer in combinatie met de proxyserver werkt dan wel.

3.1.4 Updaten van Lab-pc's

In de meeste situaties is het activeren van de proxy voldoende om ervoor te zorgen dat systemen updates op kunnen halen. Afscherming hoeft dus niet te betekenen dat systemen niet meer bijgewerkt kunnen worden.

De verwachting is dat boven beschreven VLAN met opties het overgrote deel van de Lab-VLAN situaties afdekt. Maatwerk is zeker mogelijk maar buiten de scope van dit document.

3.1.5 MAC-address bepaalt plaatsing

Het MAC-address bepaalt waar een device geplaatst wordt. Een device kan in 1 VLAN geplaatst worden. Daarom kunnen in een LAB-VLAN geen 'gewone' werkplekken terecht.

3.1.6 Meerdere netwerkkaarten

Sommige devices hebben meerdere netwerkkaarten, deze ondersteunen bijv. zowel WiFi als bedraad netwerk. Let erop dat dit de afscherming van je VLAN kan verminderen, zowel naar binnen toe als naar buiten. Als op zo'n device WiFi geactiveerd wordt, wordt de VLAN bescherming omzeild. Het is technisch niet mogelijk meerdere bedrade aansluitingen naar meerdere netwerken te realiseren.

3.1.7 Aanvraag procedure

De aanvraag van een LAB-VLAN kan alleen door een labbeheerder gedaan worden in samenspraak met de ICT-Contactpersoon om te voorkomen dat binnen groepen meerdere oplossingen ontstaan. De accountmanager is de eerste gesprekspartner.

3.2 REMOTE LOGIN

Relevante eisen: 4, 6, 10

In een aantal situaties is remote login nodig. De consensus in de beveiligingswereld is echter dat RDP, het meest gebruikte protocol hiervoor, niet aan het internet aangeboden kan worden. De risico's en overlast zijn te groot.

Het advies van LISA is om RDP alleen bereikbaar te maken voor het UT-net (en liever nog kleiner). Middels het VLAN kan dat geregeld worden. Een Lab-pc zal echter vaak ook buiten het UT-net bereikbaar moeten zijn voor specifieke personen. UT-medewerkers kunnen in die situatie gebruik maken van VPN, niet UT-medewerkers kunnen van de labbeheerder een x-account krijgen dat toegang geeft tot VPN.

Een andere gebruikte methode is Teamviewer, deze is geschikt om in situaties te werken waarbij de Lab-pc afgeschermd is.

Naar VNC, SSH en dergelijke lijkt weinig vraag te zijn, maar dit is het beste te behandelen op dezelfde manier als RDP.

3.3 PROXYSERVER

Relevante eisen: 5 en 4 (in mindere mate).

De UT heeft een proxyserver die ervoor zorgt dat afgeschermde PC's toch het internet op kunnen. Dit voor de protocollen HTTP en HTTPS. Over het algemeen kan de proxy ook gebruikt worden om systemen en software te updaten. De proxy is noodzakelijk als Microsoft Endpoint Protection ingezet wordt.

3.4 UITWISSELEN VAN DATA

Relevante eis: 4, 11

Er zijn diverse mogelijkheden om data uit te wisselen indien gebruik gemaakt wordt van het LAB-VLAN. Deze lijst bevat de meest voor de hand liggende keuzes.

Een veelgenoemd protocol voor uitwisseling is FTP. FTP is echter onversleuteld, ook het password dat bij de verbinding gebruikt wordt gaat onversleuteld over de lijn. FTP is opgevolgd door SFTP, wat eigenlijk SSH is en onder die naam verder in dit document gebruikt wordt. Ook bestaat FTPS, maar dat zien we eigenlijk niet meer gebruikt worden.

M: of P:-Schijf	Kies de optie “Toegang tot alle LISA servers”
OneDrive/SURFDrive/SURFfilesender	Gebruik de proxy
Combinatie lokaal en UT account	Kies de optie “Toegang tot alle LISA servers” om ervoor te zorgen dat het gebruik van UT accounts mogelijk is.
Remote copy toegang (SMB/SSH)	Gebruik hiervoor geselecteerde systemen op het UT-net
Mobiele datadragers	Dit wordt afgeraden, let op de risico’s van verlies en diefstal. Het is technisch lastig dit te voorkomen, dus de gebruikers van de Lab-pc kunnen hier gebruik van maken. Bedenk of je dit wel wilt en zorg voor de juiste voorlichting.
De Lab-PC zelf kan de data buiten het VLAN opslaan	Gebruik hiervoor de proxy

3.5 ACCOUNTS

Relevante eisen: 3, 4, 8

3.5.1 **Functionele accounts**

Het werken met Functionele accounts is voor de beveiliging van het UT-net lastig. Dit omdat SURFnet vereist dat gedrag naar personen te herleiden is en we dan niet kunnen bepalen wie de gebruiker is (labuser1 bijvoorbeeld). Er kunnen dus situaties optreden waarbij we ongewenst gedrag zien op een Lab-pc maar dat niet verder kunnen duiden naar een persoon.

Dit betekent in de praktijk dat LISA contact op zal nemen met de persoons op wiens naam de Lab-pc geregistreerd staat en dat deze persoon mogelijk hulp zal moeten bieden om het probleem op te lossen of verder te zoeken naar de daadwerkelijke gebruiker.

Ondanks bovenstaand probleem is het een feit dat dit soort accounts in sommige situaties noodzakelijk zijn. De bijbehorende nadelen moeten bekend zijn, maar kunnen geaccepteerd worden.

Als met functionele accounts wordt gewerkt en deze accounts in grotere kring bekend zijn, is het aan te raden toegangscontrole voor de lab-ruimte in te richten.

Er kan overwogen worden om per Lab-pc of taak een apart functioneel account te gebruiken om de verspreiding van username en password te beperken.

3.5.2 Combinatie Functionele accounts en UT accounts

Relevante eis: 4

Het is mogelijk functionele accounts en UT accounts naast elkaar te gebruiken op Lab-PC's als deze onderdeel zijn van het AD-domein.

3.5.3 Admin rechten

Relevante eis: 7

De labbeheerder heeft admin-rechten op de Lab-pc. In sommige gevallen zal ook de gebruiker admin-rechten op de Lab-pc moeten hebben. Dit is in meerdere vormen mogelijk, hier is geen algemene regel voor op te stellen.

3.5.4 Derden

Relevante eis: 10

Op dit moment wordt door LISA de mogelijkheid geboden om X-accounts af te nemen voor derden. Dit zijn persoonlijke accounts, dus mogen alleen gebruikt worden door de persoon die het account gekregen heeft. Deze kan hiermee gebruik maken van VPN en evt. inloggen op systemen als dat mogelijk gemaakt is voor dat account.

De indruk is dat dat op dit moment voldoende mogelijkheden biedt.

4. BEVEILIGINGSDOELSTELLINGEN

Naast de eisen en wensen die nodig zijn om goed gebruik van de Lab-pc's te maken is er ook nog de eis dat het UT-netwerk veilig blijft.

De UT hanteert een aantal standaard beveiligingsmaatregelen, vaak uitgeschreven in beleidsstukken die in principe ook van toepassing zijn op Lab-pc's. Als een beveiligingsmaatregel niet uitvoerbaar is, kan een alternatieve maatregel ingezet worden. Het noemen van de maatregel en het beschrijven van de alternatieven is het doel van dit stuk. Bij eenvoudig inzetbaar hoort een eenvoudig aanvraag-proces, goede documentatie en een reële prijs. Eis 10 zal dus meegenomen moeten worden

Het uitgangspunt is dat het UT-beleid leidend is. Alternatieven kunnen ingezet worden als niet aan het beleid voldaan kan worden, maar beleid gaat voor.

4.1 DIRECT UPDATEN

De meest belangrijke maatregel die ingezet wordt is direct updaten. Op Lab-pc's kan dit vaak prima, maar zeker niet altijd.

4.1.1 **Alternatief 1**

Als updaten niet kan, dan zal de Lab-pc zoveel mogelijk afgeschermd moeten worden zodat kwaadwillenden er simpelweg niet bij kunnen. Deze afscherming kan bereikt worden door gebruik te maken van een LAB-VLAN.

Als er slechts sprake is van een of enkele Lab-pc's is een VLAN niet nodig en zullen de Lab-pc's losstaand beveiligd moeten worden. De beveiliging van een enkele LAB-PC is buiten scope van dit stuk. Een harde grens is niet te noemen, vermoedelijk is in de praktijk wel duidelijk of een VLAN nuttig is of niet.

4.1.2 **Alternatief 2**

Als updaten niet mogelijk is omdat een product op de Lab-pc end-of-life is, is het zinvol bij de leverancier te informeren naar "extended support". Hou er rekening mee dat dit niet altijd een bruikbaar alternatief is waardoor op alternatief 1 terug gevallen moet worden.

4.2 REGISTRATIE VAN SYSTEMEN

Door de eisen die voor SURFnet en dus ook voor de universiteiten gelden is het nodig dat we van elk gebruik van UT-IP-adressen kunnen achterhalen wie de gebruiker was. Een registratie van systemen is dus noodzakelijk. Dit zal plaatsvinden op de naam van de lab-beheerder.

5. EXTRA BEVEILIGINGSDIENSTEN

LISA biedt extra mogelijkheden de beveiliging van systemen te verbeteren die voor Lab-pc's niet standaard aan staan. De lab-beheerder kan zelf beoordelen of dit een zinvolle toevoeging is.

5.1 VULNERABILITY SCAN

LISA scant haar servers in de datacentra 1x per maand. Dit geldt ook voor de servers van faculteiten die in de datacentra (Seinhuis en Teehuis) staan. De bestaande licentie laat het toe ook buiten de datacentra te scannen. Als apparatuur **bereikbaar** is vanaf de scan-server, dan is het mogelijk dit systeem 1x per maand te laten scannen. Bij Critical of High-bevindingen zal LISA dan contact opnemen met de lab-beheerder.

Aanvragen van deze dienst kan via Marc Berenschot (m.berenschot@utwente.nl).

5.2 MICROSOFT ENDPOINT PROTECTION

Microsoft Endpoint Protection is een uitgebreide beveiliging met Microsoft Defender als basis. Op de UT-werkplekken wordt dit standaard gebruikt. Dit omvat meer dan een virus-scanner, een uitgebreide uitleg valt buiten de scope van dit stuk.

Deze dienst kan ook op Lab-PC's aangezet worden. Het is niet noodzakelijk om in het AD domein te zitten om gebruik te maken van deze dienst, een Lab-PC kan met een 'onboarding'-package aan Defender toegevoegd worden. Een Lab-PC die wel in het domein zit is mogelijk al beschermd door Endpoint Protection. Deze dienst is beschikbaar vanaf Windows 10 en is ook beschikbaar voor Linux.

De cloud-diensten van Microsoft zijn nodig voor een volledige werking van Endpoint Protection. Dat betekent dat bij deze dienst gebruik gemaakt moet worden van de Proxy-server.

Een onboarding package moet aangevraagd worden bij LISA en is slechts beperkt bruikbaar (max 1 maand). Dit is niet door LISA aan te passen. Hier is nog geen procedure voor en deze dienst is ook niet bekend bij de Service-desk. Tot die tijd kun je m.berenschot@utwente.nl mailen.

5.3 FIREWALL-DIENST

Dit levert LISA nog niet, maar een firewall op maat voor een specifiek systeem is wel een onderwerp waar over nagedacht wordt. Dus feedback is welkom.

6. OPENSTAANDE VRAGEN

6.1 TEGENHOUDEN VAN UPDATES

Dit wordt in nieuwere versies van Windows steeds moeilijker. Wat is er nog mogelijk op dit gebied?

6.2 VERSCHILLENDE ADMIN ACCOUNTS

Er bestond vroeger iets als de power-user die wel op verschillende plekken kon schrijven (program files en registry bijv.) maar geen volwaardige admin zijn. Is er nog iets tussen gewone gebruiker en admin in?

7. AANVRAAGFORMULIER VLAN VOOR LAB-PC'S

Dit formulier kan ingevuld worden als een VLAN voor Lab-PC's aangevraagd wordt.

Aanvrager:

Accountmanager LISA:

Datum:

Afdeling:

Lab-pc's in een LAB-VLAN krijgen privé-IP-adressen en worden geregistreerd op MAC-address

Mac-Adressen van LAB-PC's:

☐ Proxy mogelijkheid blokkeren (standaard: Aan)

☐ Toegang tot alle LISA-Servers aanzetten (nodig voor diensten als M:, P:, U:-schijf, software center en domein-lidmaatschap)

☐ Zelf MAC-adressen registreren (alleen bij hoog-volume veranderingen).

☐ Toegang van/naar systemen op UT-net instellen (systemen moeten een vast IP-adres hebben of krijgen dit na invullen van dit formulier)

☐ Remote Login (via VPN) open

☐ RDP (Windows Remote Login) ☐ SSH ☐ Overig (invullen poort of naam):

☐ Extra dienst Vulnerablity Scan: IP adressen:

☐ Extra dienst: Microsoft Endpoint Protection