|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Benämning** | OVB - 180705 | Ansvarig | Claes Gyllhamn | Skapat | 2018-07-05 10:42 |
| **Projekt** | Omvärldsbevakning | | | Senast sparat | 2018-07-05 10:42 |
| **Revision** | 0.1 | Filnamn | TEST.docx | | |

Omvärldsbevakning

(kund)

Innehåll

[1 Halvårskontroller 4](#_Toc518550533)

[1.1 Switchar / Routrar 4](#_Toc518550534)

[1.1.1 Komponentstatus 4](#_Toc518550535)

[1.1.2 Patchstatus 4](#_Toc518550536)

[1.1.3 Supportavtal 5](#_Toc518550537)

[1.1.4 Trendanalys 5](#_Toc518550538)

[1.1.5 Loggar 5](#_Toc518550539)

[2 Summering 5](#_Toc518550540)

[3 Beskrivning av kontroller 5](#_Toc518550541)

[3.1 Switchar / Routrar 5](#_Toc518550542)

# Veckovis kontroll

Då det inte kommer ut CVE eller andra definitioner av sårbarhet lika ofta som till t.ex. mjukvara så blir det desto mer manuellt arbete för att få fram den information som önskas för hårdvara. När det gäller mjukvara finns det ofta definitioner på sidor så som <https://www.cvedetails.com/index.php> vilket gör att information är lite mer lättillgänglig.

## Tillverkare / Modell

### Versionsnivå

**Åtgärd behöver vidtas.**

Det finns 109 switchar och 4 routrar som är ”End of Support” och som starkt rekommenderas att byta ut. Inom 18 månader går ytterligare 22 switchar in i ”End of Support”. En plan för att byta ut dem bör tas

### Sårbarhet

**Åtgärd behöver vidtas.**

I princip hela switch och router plattformen behöver uppgraderas. Den primära anledningen är att det har upptäckts säkerhetshål i många av mjukvarorna som används idag. Vissa komponenter har släpat uppgraderingsmässigt och ligger långt efter dagens rekommenderade versioner vilket inte är bra vid ex öppnande av supportärenden. Ytterligare en anledning till att uppgradera är att få tillgång till nya funktioner.

Följande komponenter behöver uppgraderas:

* N7K-C7010 CORE 6.2(10) -> 6.2(16)
* Nexus 5500 CORE 5.X.X.X -> 7.2(1)N1(1)

\*Ser ut som en av Nexus 5600 switcharna (n5k4n11) inte ligger på samma version som övriga Nexus 5600 switchar.

För fullständig rapport hur många säkerhetshål det finns i respektive mjukvara se ” 2016-12-05\_consolidated\_report.xls” flik ”Device List (All Devices)”

## Leverantör / produkt / Version

### Versionsnivå

**Åtgärd behöver vidtas.**

Det finns 109 switchar och 4 routrar som är ”End of Support” och som starkt rekommenderas att byta ut. Inom 18 månader går ytterligare 22 switchar in i ”End of Support”. En plan för att byta ut dem bör tas fram för att inte hamna i ett läge där det kan bli problem att få support p.g.a. gammal utrustning.

Följande komponenter bör bytas ut:

Router:

2st 2612 EoS 2011-07-31

2st 878 EoS 2016-05-31

Switch:

1st WS-C2912-XL-EN EoS 2006-11-01

För fullständig ”End of Support” rapport se ” 2016-12-05\_consolidated\_report.xls” flik ”Device List (Hardware - EOL)”

### Sårbarheter

**Åtgärd behöver vidtas.**

I princip hela switch och router plattformen behöver uppgraderas. Den primära anledningen är att det har upptäckts säkerhetshål i många av mjukvarorna som används idag. Vissa komponenter har släpat uppgraderingsmässigt och ligger långt efter dagens rekommenderade versioner vilket inte är bra vid ex öppnande av supportärenden. Ytterligare en anledning till att uppgradera är att få tillgång till nya funktioner.

Följande komponenter behöver uppgraderas:

* N7K-C7010 CORE 6.2(10) -> 6.2(16)
* Nexus 5500 CORE 5.X.X.X -> 7.2(1)N1(1)
* Nexus 5600 CORE 7.2(1)N1(1)\* -> Ligger på rekommenderad version
* Catalyst 6500 DIST 12.2(33)SXH -> 12.2.33 SXI14

# Summering

Det stora jobbet som behöver göras är att uppgradera befintlig kommunikationsutrustning så att den kommer upp i rekommenderad och enhetlig nivå. Uppgraderingarna har släpat en del och omtag behöver göras för att komma i fas. Det finns även en hel del switchar och routrar som behöver bytas ut pga att de har gått eller kommer att gå ”End of Support” i närtid. I det stora hela har Landstinget ett väl fungerade nät men det kräver kontinuerligt underhåll för att fungera så optimalt som möjligt.

# Beskrivning av kontroller

## Switchar / Routrar

|  |  |  |
| --- | --- | --- |
| **Funktion** | **Kontroll** | **Verktyg** |
| Switching / Routing | **Komponentstatus**, kontrollera End-of-Life, End-of-Sale, End of SW Maintenance, End of Service Contract Renewal, Lats Day of Support. | Cisco Active Advisor (rapport) |
| Switching / Routing | **Patchstatus**, kontrollera om nuvarande version har några kritiska buggar, ge förslag på nästkommande stabila version som är lämplig att uppgradera till för att inte släpa efter för mycket. | Cisco Active Advisor (rapport) + manuellt arbete som infogas som kommentarer till rapporten |
| Switching / Routing | **Supportavtal**, kontrollera att giltiga avtal finns på kritiska komponenter och ge förslag vad som bör läggas till alt tas bort. | Cisco Active Advisor (rapport) |
| Switching / Routing | **Trendanalys**, kontrollera CPU, flash och minnesutnyttjande samt bandbreddsutnyttjande på kritiska länkar. | Cisco Prime Infrastructure (rapport) |
| Switching / Routing | **Loggar**  Veckokontroll, sammanställa alla meddelande i alarmloggen sen senaste veckkontrollen och kommentera nya händelser + eventuella åtgärder som bör vidtas.  Halvårskontroll, sammanställa alla händelser sen senaste halvårskontrollen + veckokontroller och kommentera händelser och trender + eventuella åtgärder som bör vidtas. |  |