LUMC Aansluitvoorwaarden IPS

Eigenaarsgroep (verplicht)

Deze aansluitvoorwaarden en de daaruit voortvloeiende detailleringen worden voorbereid en onderhouden door het team Security en vastgesteld door het management van Informatie Technologie & Digitale Innovatie (IT&DI) en de divisies. Wijziging of aanpassing van de voorwaarden vindt plaats zodra technische of andere ontwikkelingen dit noodzakelijk maken. In dat geval zal gevraagd en ongevraagd een voorstel worden gedaan aan het MT van IT&DI.

Inleiding (verplicht)

Binnen het LUMC netwerk worden periodiek beveiligingsupdates en virusscans uitgevoerd om zo virusinfecties en beveiligingsincidenten te voorkomen. Zie ook Computervirus op Albinusnet. De beveiligingsupdates en scans kunnen in enkele gevallen problemen opleveren bij software die specifieke apparatuur aanstuurt (bijv. laboratorium- of analyse apparaten). Indien dit het geval is dient een afdeling contact op te nemen met IT&DI. Wanneer in overleg met IT&DI en de leverancier duidelijk wordt dat het uitvoeren van deze beveiligingsupdates en scans een negatieve invloed heeft op de werking van het apparaat of de software, wordt er gekeken of plaatsing achter de IPS mogelijk is.

Afspraken standaard (verplicht)

Bij het plaatsen achter IPS zijn de volgende afspraken van toepassing:

Consequenties

Na het aansluiten van IT-apparatuur achter IPS:

- Worden de volgende acties uitgevoerd:
    - De reguliere beveiligingsupdates op de IT-apparatuur komen te vervallen. Indien gewenst kunnen er specifieke afdelingsafhankelijke updates worden uitgevoerd. De afdeling/leverancier is hier zelf verantwoordelijk voor
    - De IT-apparatuur is NIET meer voorzien van de standaard LUMC antivirus software en instellingen (zoals bijv. de Weekly Sheduled Scan).
- Is het voor gebruikers en leveranciers NIET meer toegestaan om:
    - Internet te gebruiken op de IT-apparatuur.
    - USB of andere opslagmedia te gebruiken op de IT-apparatuur.

Beide maatregelen zij om virusbesmettingen te voorkomen. Bij virusbesmetting, op achter de IPS geplaatste apparatuur, loopt alle IT-apparatuur achter de IPS het risico besmet te worden. Het LUMC netwerk is dan wel beschermd.
In geval van besmetting houdt het IT&DI zich het recht voor om IT-apparatuur zonder aankondiging van het netwerk te verwijderen. Achteraf wordt hierover verantwoording afgelegd naar de afdeling.

Verantwoordelijkheden en bevoegdheden

- De afdeling/leverancier is verantwoordelijk voor het aangeven dat een specifiek apparaat niet mee moet draaien met de beveiligingsupdates en virusscans.
- IT&DI is verantwoordelijk voor het beoordelen van de aanvraag om IT-apparatuur achter een IPS te plaatsen,
- IT&DI is verantwoordelijk voor het plaatsen achter IPS,
- IT&DI is bevoegd om IT-apparatuur te verwijderen indien er een beveiligingsrisico ontstaat.

Motivatie/reden gebruik (verplicht)

Indien een leverancier aangeeft dat de (aan het apparaat gekoppelde) IT-apparatuur niet mee kan draaien met de reguliere Windows updates en/of virusprotectie, worden de reguliere updates en de virusprotectie, na overleg met de leverancier gestopt. Als gevolg hiervan voldoet het IT-apparaat niet meer aan de standaard aansluitvoorwaarden van het LUMC en ontstaat er een risico voor beveiligingsincidenten voor zowel de onbeschermde IT-apparatuur als de rest van de IT-apparatuur in het LUMC. Het IT-apparaat kan worden beveiligd door deze achter een IPS te plaatsen. De IPS fungeert dan als een netwerkbeveiliging door het dataverkeer te controleren. Het dataverkeer wordt in beide richtingen gestopt als er misbruik van bekende kwetsbaarheden in software plaats vindt.

Toepassing (verplicht)

Dit protocol beschrijft onder welke voorwaarden IT-apparatuur achter een IPS wordt geplaatst. Tevens wordt beschreven welke consequenties dit heeft voor de IT-apparatuur.

Definities en afkortingen

IPS	Intrusion Prevention System.