Net2 - Nätverkssäkerhetsrekommendationer

Översikt

För att ditt Paxton Net2-system ska vara så säkert som möjligt i din anläggning rekommenderar Paxton att installatören (eller IT-avdelningen) följer bästa praxis för IT-säkerhet gällande vart och ett av de sju lagren i nätverkets Open Systems Interconnection-modell (OSI).

Vidta starka fysiska säkerhetsåtgärder

Vidta starka fysiska säkerhetsåtgärder i företagets anläggningar, till exempel genom att använda biometrik, autentisering med passerbricka etc. så att det går att hindra obehöriga innan de kommer in i byggnader med företagsnätverk.

Följ standarder för åtkomststyrning på nätverk, såsom IEEE 802.1X-autentisering, för att säkra LAN- och WLAN-nätverk

Denna standard upprätthåller säkerhetspolicyer genom att endast ge enheter som uppfyller säkerhetspolicyer och säkerhetsstandarder åtkomst till nätverksresurser när enheterna i fråga är anslutna till en fysisk LAN-port eller WLAN SSID. Denna standard hanterar inte bara åtkomstauktorisering och behörighetsfunktioner, utan styr även de data som specifika användare kommer åt genom att känna igen dem samt deras enheter och nätverksroller. Alla Windows-, Mac- och Linux-maskiner har inbyggt stöd för IEE 802.1X.

Använd nästa generationens brandväggar för att hindra externa och interna angrepp

Använd nästa generationens brandvägg som, förutom att genomföra traditionell paket- och tillståndsbaserad inspektion, också genomför inspektioner i applikationslagret, förhindrar och identifierar intrång samt säkrar webbtrafik etc.

Flytta dessutom potentiellt osäkra interna VLAN-nätverk på lager 2 till brandväggen och skydda mot åtkomst till andra betrodda/säkra VLAN-nätverk från dessa VLAN-nätverk genom att använda konfigurerbara säkerhetspolicyer.

Använd VLAN-nätverk (Virtual Local Area Networks) för att säkra och dela upp nätverket

VLAN-nätverk gör att vi kan behålla datapaket från flera nätverk (såsom avdelningsnätverk, kritiska servernätverk etc). separerade. Nätverkssegmentering med VLAN-nätverk skapar en samling med isolerade nätverk inom ett företagsnätverk och minskar angreppsytorna eftersom även om utomstående får åtkomst till ett litet logiskt nätverk kan de inte se eller direkt angripa enheter på andra VLAN-nätverk.

Använd starka lösenord i Net2-serverns applikationsautentisering och tillhörande databaser. Se applikationsanteckning AN1162 för information om hur man gör detta.

Använd en separat maskin som Net2-server

Använd en separat maskin som Net-2server och installera inte någon annan programvara än nätverksövervakningsverktyg (om det behövs).

Den fysiska Net2-servern ska begränsas så att den endast användas av behörig personal.

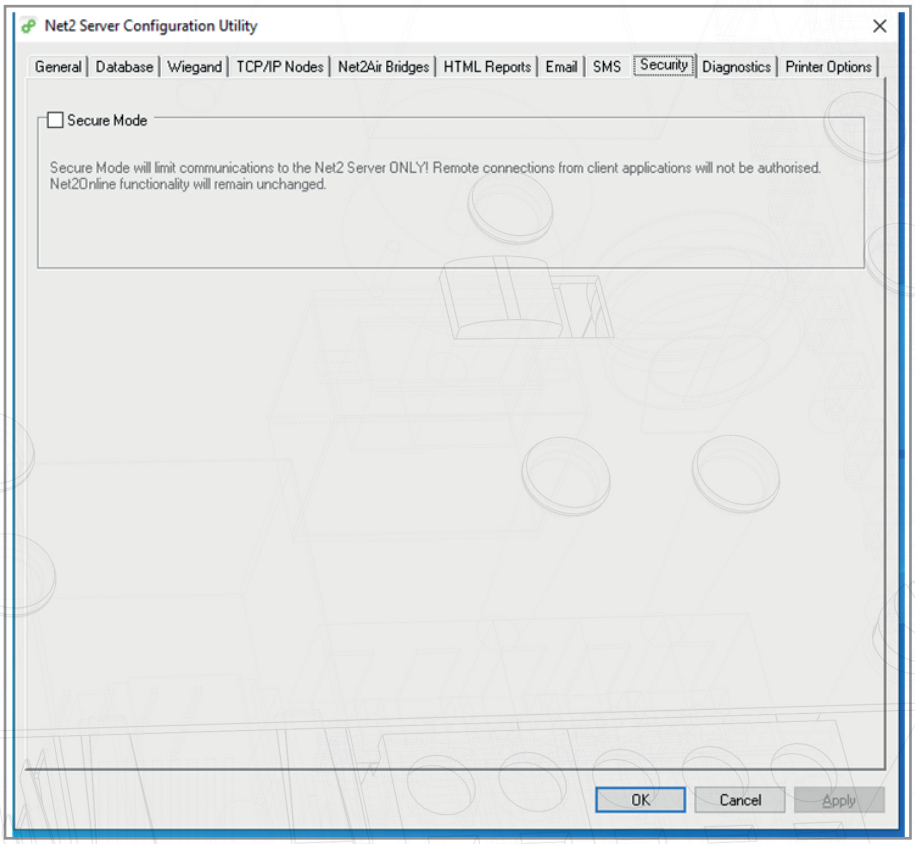
Maskinsäkerhet

Håll server- och klientmaskiner uppdaterade med de senaste kritiska uppdateringarna och se till att det finns virusskydd på klientmaskinerna.

Net2-klienter bör installeras på maskiner som inte har några e-post- och chattklienter för att undvika att skadlig kod körs oavsiktligen via bilagor.

Net2 – säkert läge

För högsta möjliga säkerhet, överväg att köra både server- och klientprogramvara på samma maskin och blockera inkommande anslutningar på TCP SQL-serverport 1433. Detta går att göra genom att aktivera "säkert läge" via Net2:s säkerhetsflik.



Alternativt, för att dra nytta av samtliga klientfunktioner, använd virtualiserade applikationsprogram, såsom VMware Horizon för att distribuera begränsade Net2-klientapplikationer som är anslutna till en Net2-server på ett separat LAN- eller VLAN-nätverk.

För att göra det möjligt att registrera passerbrickor, använd antingen en befintlig läsare eller en som är ansluten till ett trådlöst Net2 Nano-nätverk om det inte går att använda sladd. Denna lösning gör det också möjligt att isolera SDK (Software Development Kit) och videoapplikationer i det virtuella skrivbordet samt driftsätta dem på enkelt sätt och administrera dem helt och hållet i datacentret.

Vad är VMware Horizon? | VDI-program | VMware | Storbritannien

OBS: VMware Horizon har inte USB-passthrough, utan prestandan avgörs av nätverkshastigheter och behöver testas. Detta gör att vanliga skrivbordsläsare och webbkameror kan användas.

Ytterligare säkerhetsåtgärder

1. Använd MAC-adressfiltrering på dataväxeln

Använd MAC-adressfiltrering på Entry-porten. När en okänd enhet ansluter till en port inaktiveras porten och en varning skickas.

2. Isolera VLAN-nätverket

Se till att alla Paxton-enheter med IP-funktionalitet är anslutna till ett separat VLAN-nätverk. Isolera detta nätverk från företagsnätverket så att åtkomsten till andra områden förutom åtkomststyrningsenheterna begränsas.