# Net2 - Aanbevelingen voor netwerkbeveiliging

Om ervoor te zorgen dat uw Net2 toegangscontrole systeem zo veilig mogelijk is, dient u mogelijk uw netwerk te beveiligen. Uw installateur of IT afdeling kan u adviseren om de juiste netwerkbeveiliging toe te passen. Hieronder vindt u aanbevelingen die helpen u om uw netwerk optimaal te beveiligen tegen interne en externe bedreigingen.

## Fysieke beveiliging

Wanneer je een gebouw of ruimte zomaar kunt betreden en eenvoudig bij netwerk infrastructuur kunt komen zonder dat dit tijdig opgemerkt wordt dan zit daar een security risico.

Het toepassen van een online toegangscontrole systeem kan dit voorkomen en is daarom de perfecte vorm van fysieke beveiliging. Daarnaast kan een toegangscontrole systeem een organisatie helpen aantoonbaar te maken wie wanneer toegang heeft gekregen tot een gebouw of ruimte zoals een serverruimte.

Het kan nodig zijn om bijvoorbeeld deurcontacten toe te passen op een deur die toegang geeft tot een server ruimte. Om te monitoren of een deur ongeautoriseerd wordt geopend. Door gebruik te maken van triggers en acties is het mogelijk om een e-mail te sturen als iemand toegang heeft gekregen tot de deur. Zodat toegang tot een serverruimte actief gemonitord kan worden.

Controleer ook of het type deur geschikt is voor de situatie en kies goede kwaliteit elektrische sluitplaten.

Meer informatie vindt u via: https://www.paxton-access.com/nl/technische-support/veiligere-toegangscontrole/

## Gebruik netwerk authenticatie standaarden zoals IEEE 802.1X om uw LAN en WLAN te beveiligen

Deze beveiligingsstandaard laat alleen LAN en WLAN netwerkapparatuur op uw netwerk toe die voldoen aan de IEEE802.1X beveiligingsstandaard.
Deze standaard behandelt niet alleen toegangsauthenticatie- en autorisatiefuncties, maar beheert zelfs de gegevens die door die specifieke gebruikers en apparaten geraadpleegd worden. IEEE802.1.x wordt standaard ondersteund door alle Windows, Mac en Linux machines, en wordt veel toegepast in sectoren zoals overheid, zorg en onderwijs.

Niet ieder apparaat ondersteund IEEE 802.1X waardoor het gebruikelijk is om apparaten die 802.1x niet ondersteunen alsnog toegang te geven tot het netwerk. Dit is vaak het geval voor printers, ip telefoons etc. Bij 802.1X is het mogelijk om MAB te gebruiken (MAC Authentication Bypass). Dit betekent dat er een White list gemaakt wordt van MAC adressen die alsnog toegang krijgen tot het netwerk terwijl deze 802.1X niet ondersteunen. Enkel en alleen deze apparaten die op de White list staan krijgen dan toegang.

**Ondersteund Paxton IEEE 802.1X?**
Zowel Net2, Paxton10 als Entry bieden geen ondersteuning voor de 802.1X standaard.

Hoewel Net2, Paxton10 en Entry geen directe ondersteuning bieden voor 802.1X, kunnen ze via MAB toch veilig worden geïntegreerd.

## Gebruik de nieuwe generatie firewalls (NGFW) om externe en interne aanvallen te voorkomen

Gebruik Next-Generation Firewalls (NGFW) om uw netwerk te beschermen tegen geavanceerde bedreigingen. NGFW's combineren traditionele firewallfuncties met geavanceerde technieken zoals Deep Packet Inspection (DPI), Intrusion Prevention Systems (IPS) en malwaredetectie.

Segmenteer uw netwerk met VLAN's om verschillende systemen (zoals camera's, toegangscontrole en werkstations) van elkaar te scheiden.

## Gebruik VLAN's (Virtual Local Area Networks) voor netwerk beveiliging en scheiding

Met VLAN's kunt u op één fysiek netwerk uw netwerken scheiden van elkaar, zo kunt u een netwerk hebben voor bijvoorbeeld uw camera's, toegangscontrole of computers.

Met netwerk segmentatie via VLAN's creëert u losstaande netwerken. Wanneer een iemand ongeoorloofde toegang heeft tot één VLAN kan er vanuit daar geen aanval gedaan worden op de overige VLAN's. Hiermee beperkt u een aanval op uw netwerk tot één VLAN.

## Wachtwoordbeleid en software updates

Gebruik sterke, unieke wachtwoorden voor de Net2 software applicaties en bijbehorende databases. Het is mogelijk om een sterk wachtwoord binnen de software te verplichten waardoor het wachtwoord dat gebruikt wordt voor Net2 minimaal 7 karakters lang moet zijn.

Ook adviseren we om regelmatig de Net2 software te updaten, niet alleen voor nieuwe functionaliteiten maar ook voor beveiligingsupdates. Regelmatig wordt Net2 voorzien van security updates die de beveiliging van Net2 nog verder verbeteren. Daarnaast maken we gebruik van externe software componenten die regelmatig bijgewerkt worden.

## Implementeer een back-up en herstelprocedures

Net2 maakt standaard elke nacht een back-up op de lokale schijf. Zorg voor een strategie waarbij deze back-up ook extern wordt opgeslagen, bijvoorbeeld op een netwerkschijf of USB-stick
Hiermee zorgt u ervoor dat in het geval dat de PC faalt u altijd toegang heeft tot een back-up en het Net2 systeem eenvoudig kunt herstellen.