unv®
Unlimited New View

Network Security Advisory

Netwerk Beveiligingsadvies

Met de populariteit van netwerkvideobewaking worden steeds meer netwerkproducten gebruikt in openbare netwerken, zoals netwerkvideorecorders en netwerkcamera's. Maar de publieke netwerkomgeving is kwetsbaarder dan het interne netwerk. Uw apparaten kunnen worden aangevallen door verschillende virussen. Neem alle nodige maatregelen om de netwerkbeveiliging van je apparaat te verbeteren.

De volgende maatregelen zijn nodig voor de netwerkbeveiliging van uw apparaat:

- Wijzig het standaard wachtwoord en stel een sterk wachtwoord in: U wordt sterk aangeraden om het standaard wachtwoord te wijzigen voordat u voor het eerst inlogt en een sterk wachtwoord in te stellen van ten minste negen tekens met alle drie de elementen: cijfers, letters en speciale tekens.
- Houd de firmware up-to-date: Het wordt aanbevolen om uw apparaat altijd te upgraden naar de nieuwste versie voor de nieuwste functies en betere beveiliging. Bezoek de officiële website van Uniview of neem contact op met uw plaatselijke dealer voor de nieuwste firmware.

Hieronder volgen aanbevelingen voor het verbeteren van de netwerkbeveiliging van uw apparaat:

- ✓ Wijzig het wachtwoord regelmatig: Wijzig het wachtwoord van uw apparaat regelmatig en bewaar het wachtwoord veilig. Zorg ervoor dat alleen de geautoriseerde gebruiker kan inloggen op het apparaat.
- ✓ HTTPS/SSL inschakelen: SSL-certificaat gebruiken om HTTP-communicatie te versleutelen en gegevensbeveiliging te garanderen. Filteren op IP-adressen inschakelen: Alleen toegang toestaan vanaf de opgegeven IP-adressen in de witte lijst.
- ✓ Minimale poorttoewijzing: Configureer je router of firewall om een minimale set poorten naar het WAN te openen en alleen de noodzakelijke poorttoewijzingen te behouden.
- ✓ Schakel de functies Automatisch aanmelden en Wachtwoord opslaan uit: Als meerdere gebruikers toegang hebben tot je computer, is het aan te raden om deze functies uit te schakelen om ongeautoriseerde toegang te voorkomen.

- ✓ Kies een discrete gebruikersnaam en wachtwoord: Vermijd het gebruik van de gebruikersnaam en het wachtwoord van je sociale media, bank, e-mailaccount, enz. als de gebruikersnaam en het wachtwoord van je apparaat, voor het geval de gegevens van je sociale media, bank en e-mailaccount uitlekken.
- ✓ Beperk gebruikersrechten: Als meer dan één gebruiker toegang tot je systeem nodig heeft, zorg er dan voor dat elke gebruiker alleen de benodigde rechten krijgt.
- ✓ UPnP uitschakelen: Wanneer UPnP is ingeschakeld, zal de router automatisch interne poorten in kaart brengen en zal het systeem automatisch poortgegevens doorsturen, wat resulteert in het risico op gegevenslekken. Wij stellen voor UPnP uit te schakelen en de Uniview EZView te gebruiken om via het internet toegang te krijgen tot het UNV-apparaat ter vervanging van UPnP.
- ✓ SNMP: Schakel SNMP uit als u het niet gebruikt. Als u het wel gebruikt, wordt SNMPv3 aanbevolen.
- ✓ Multicast is bedoeld om video naar meerdere apparaten te verzenden. Als je deze functie niet gebruikt, is het aanbevolen om multicast op je netwerk uit te schakelen.
- ✓ Controleer logs: Controleer de logs van je apparaat regelmatig om ongeautoriseerde toegang of abnormale handelingen te detecteren.
- ✓ Fysieke bescherming: Bewaar het apparaat in een afgesloten kamer of kast om onbevoegde fysieke toegang te voorkomen.
- ✓ Videobewakingsnetwerk isoleren: Het isoleren van uw videobewakingsnetwerk met andere servicenetwerken helpt onbevoegde toegang tot apparaten in uw beveiligingssysteem vanuit andere servicenetwerken te voorkomen.

Opmerking:

1) Dit document is uitsluitend bedoeld als leidraad. Alle verklaringen, informatie en aanbevelingen in dit document vormen geen expliciete of impliciete garanties. Raadpleeg de daadwerkelijke software voor de juiste werking van het product.

2) De inhoud van dit document zal periodiek worden bijgewerkt als gevolg van upgrades van productversies of vereisten van toepasselijke wet- en regelgeving in specifieke regio's. De bijgewerkte inhoud zal worden weergegeven in nieuwe versies van dit document. De bijgewerkte inhoud wordt weergegeven in nieuwe versies.

Je kunt ook beveiligingsinformatie (engels) vinden in het Security Response Center op de officiële website van Uniview. https://global.uniview.com/Support/Cybersecurity/