Internet-Sicherheitsstatement

- Sie sind für die Risiken verantwortlich, die auf die Verbindung Ihres Produkts mit dem Internet zurückgehen, einschließlich, jedoch nicht darauf beschränkt, Cyberattacken, Hackerattacken, Computerviren, Schadprogramme usw. Schützen Sie Ihre Daten und persönlichen Informationen, indem Sie die notwendigen Schritte unternehmen, wie beispielsweise das Ändern des Standard-Passworts und Verwendung einer starken Kombination, regelmäßige Änderung Ihres Passworts, regelmäßige Aktualisierung Ihrer Firmware usw. LUPUS ist nicht für Fehlfunktionen, Informationslecks oder andere Problem aufgrund der Nichtbeachtung der Sicherheitshinweise Ihrer Geräte verantwortlich.
- Soweit nicht durch geltendes Recht untersagt, sind LUPUS und seine Mitarbeiter, Lizenznehmer und Partner nicht für Verletzungen, beiläufige, besondere, mittelbare oder unmittelbare Schäden haftbar, einschließlich, jedoch nicht darauf beschränkt, Schäden für Gewinnverlust, Beschädigung oder Verlust von Daten, Unmöglichkeit der Übertragung oder des Empfangs von Daten, Geschäftsunterbrechung oder jegliche sonstige wirtschaftliche Schäden oder Verluste aufgrund oder in Verbindung mit der Verwendung oder der Unmöglichkeit der Verwendung unserer Produkte oder Dienste, wie auch immer verursacht, unabhängig von der Haftungstheorie (Vertrag, unerlaubte Handlung oder anderweitig), selbst wenn wir auf die Möglichkeit derartiger Schäden hingewiesen wurden. Da einige Gerichtsbarkeiten den Ausschluss oder die Begrenzung der Haftung für Folgeschäden nicht zulassen, trifft die obige Einschränkung für Sie möglicherweise nicht zu.
- Auf keinen Fall übersteigt die Haftung für alle Schäden den für die Produkte oder Dienste bezahlten Betrag (außer wenn durch geltendes Recht im Fall von Verletzungen gefordert).

Obligatorische Maßnahmen zur Internetsicherheit

1.Ändern Sie Passwörter und verwenden Sie starke Passwörter

- Der wichtigste Grund, warum Systeme „gehackt werden, liegt in schwachen oder Standard-Passwörtern. LUPUS empfiehlt das sofortige Ändern der Standard-Passwörter und die Wahl eines starken Passworts, wann immer dies möglich ist. Ein starkes Passwort besteht aus
- mindestens 8 Schriftzeichen und einer Kombination aus Sonderzeichen, Ziffern, Groß- und Kleinbuchstaben.

2. Aktualisieren Sie die Firmware

- Als standardmäßigen Vorgang in der Tech-Branche empfehlen wir, NVR-, DVR- und IP-Kamera-Firmware auf dem neuesten Stand zu halten, damit das System mit den neuesten Sicherheits-Patches und Fixes aktualisiert ist. Überprüfen Sie die Firmware-Version Ihrer laufenden Geräte. Ist die Firmware-Version älter als 18 Monate, so wenden Sie sich zwecks verfügbarer Update-Versionen an Ihren örtlichen autorisierten LUPUS-Fachhändler oder an den technischen Support von LUPUS.

„Nice to have - Empfehlungen zur Verbesserung Ihrer Netzwerksicherheit

1. Ändern Sie Passwörter regelmäßig

- Ändern Sie die Zugangsdaten zu Ihren Geräten regelmäßig, um zu gewährleisten, dass nur befugte Anwender Zugriff auf Ihr System haben.

2. Ändern Sie Standard-HTTP- und TCP-Ports

- Ändern Sie Standard-HTTP- und TCP-Ports für LUPUS-Systeme. Dies sind die beiden Ports, die zur Remote-Kommunikation und Anzeige von Video-Streams verwendet werden.
- Diese Ports können zu jedem beliebigen Nummer-Set zwischen 1025 und 65535 geändert werden. Eine Vermeidung der Standard-Ports verringert das Risiko, dass Außenseiter erraten können, welche Ports Sie verwenden.

3. Aktivieren Sie HTTPS/SSL

- Richten Sie ein SSL-Zertifikat ein, um HTTPS zu aktivieren. Dies verschlüsselt die gesamte Kommunikation zwischen Ihren Geräten und dem Rekorder.

4. Aktivieren Sie den IP-Filter

- Die Aktivierung Ihres IP-Filters hindert jeden, außer jenen mit spezifizierten IP-Adressen, am Zugriff auf das System.

5. Ändern Sie das ONVIF-Passwort

- Auf älterer IP-Kamera-Firmware ändert sich das ONVIF-Passwort nicht, wenn Sie die Zugangsdaten zum System ändern. Sie müssen entweder die Kamera-Firmware zur neuesten Version aktualisieren oder das ONVIF-Passwort manuell ändern.

6. Leiten Sie nur Ports weiter, die Sie benötigen

- Leiten Sie nur die HTTP- und TCP-Ports weiter, die Sie verwenden. Leiten Sie keinen riesigen Nummernbereich an das Gerät weiter. Setzen Sie die IP-Adresse des Geräts nicht in die DMZ.

<u>Internet-Sicherheitsstatement und Empfehlungen:</u>
Sie müssen keine Ports für individuelle Kameras weiterleiten, wenn sie alle an einem Rekorder vor Ort angeschlossen sind; es wird nur der NVR benötigt.

7. Deaktivieren Sie Auto-Login auf SmartPSS

- Verwenden Sie SmartPSS zur Anzeige des Systems auf einem Computer, der von mehreren Personen genutzt wird, dann sollten Sie die automatische Anmeldung deaktivieren. Dies fügt eine weitere Sicherheitsebene hinzu, um Anwender ohne die entsprechenden Zugangsdaten am Zugriff auf das System zu hindern.

8. Verwenden Sie einen unterschiedlichen Benutzernamen und Passwort für SmartPSS

- Für den Fall, dass Ihr soziale Medien-, Bank- oder E-Mail-Konto gehackt wurde, wünschen Sie wohl kaum, dass jemand diese Passwörter auf Ihrem Videoüberwachungssystem versucht. Die Verwendung eines unterschiedlichen

Benutzernamens und Passworts für Ihr Sicherheitssystem erschwert es Unbefugten, ihren Weg in Ihr System zu erraten.

9. Begrenzen Sie die Funktionen von Gästekonten

- Ist Ihr System für mehrere Anwender eingerichtet, dann gewährleisten Sie, dass jeder Anwender nur die Rechte zu Funktionen hat, die für die Durchführung seiner Arbeiten benötigt werden.

10. UPnP

- UPnP versucht automatisch, Ports in Ihren Router oder Modem weiterzuleiten. Normalerweise ist das eine gute Sache. Leitet Ihr System jedoch die Ports automatisch weiter und Sie ändern die Standard-Zugangsdaten nicht, müssen Sie möglicherweise mit unerwünschten Besuchern rechnen.
- Leiten Sie die HTTP- und TCP-Ports in Ihrem Router/Modem manuell weiter, dann sollte diese Funktion trotzdem ausgeschaltet sein. UPnP-Deaktivierung wird empfohlen, wenn die Funktion in realen Anwendungen nicht verwendet wird.

11. SNMP

- Deaktivieren Sie SNMP, wenn Sie es nicht verwenden. Verwenden Sie SNMP, so sollten Sie das nur vorübergehend tun, und nur für Verfolgungs- und Testzwecke.

12. Multicast

- Multicast dient der Freigabe von Video-Streams zwischen zwei Rekordern. Derzeit gibt es keine bekannten Probleme mit Multicast, aber wenn Sie die Funktion nicht verwenden, kann die Deaktivierung Ihre Netzwerksicherheit erhöhen.

13. Überprüfen Sie das Protokoll

- Wenn Sie vermuten, dass sich jemand unbefugten Zugriff auf Ihr System verschafft hat, können Sie das Systemprotokoll überprüfen. Das Systemprotokoll zeigt Ihnen, welche IP-Adressen zur Anmeldung bei Ihrem System verwendet wurden und worauf zugegriffen wurde.

14. Schließen Sie das Gerät effektiv ab

- Idealerweise wollen Sie jeglichen unbefugten effektiven Zugriff auf Ihr System vermeiden. Der beste Weg, dies zu erreichen, ist den Rekorder in einem verschließbaren Fach, Server-Baugruppenträger oder in einem verschlossenen Raum zu installieren.

15. Schließen Sie IP-Kameras an den PoE-Ports auf der Rückseite eines NVR an

- Kameras, die an den PoE-Ports auf der Rückseite eines NVR angeschlossen sind, sind von der Außenwelt isoliert und es kann nicht direkt auf sie zugegriffen werden.

16. Isolieren Sie NVR und IP-Kameranetzwerk

- Das Netzwerk, auf dem sich Ihr NVR und Ihre IP-Kamera befinden, sollten nicht das gleiche Netzwerk wie Ihr öffentliches Computernetzwerk sein. Dies verhindert, dass Besucher oder unerwünschte Gäste Zugang zu dem gleichen Netzwerk erhalten, welches das Sicherheitssystem für ordnungsgemäße Funktion benötigt.