BUILDING AND HOME AUTOMATION SOLUTION, 01/2022

Safety related Technical Bulletin

Setting or activating the BCU key by a "Cyber Attack"

Intelligent building installations, including KNX, are increasingly becoming targets of cyber attacks. However, these cyber attacks can be avoided very easily by ensuring that such installations are never directly accessible (without a VPN) via the Internet.

If a KNX installation is connected to the Internet, the use of a VPN tunnel is an absolute MUST HAVE. When using a KNX Secure Tunnel interface, it must be ensured that the strong passwords recommended by the ETS are used.

Therefore, we aren´t basically talking about a direct cyber attack on the KNX here.

What is or can be the consequence or impact of such a Cyber-Attack?

The most common report is about the unauthorized setting of a BCU key. Here, the physical individual addresses of the devices are read or scanned and afterwards – if not already done - set with a BCU key. It is noticeable that the function of the KNX devices is no longer guaranteed. This can usually only be done with a corresponding tool of the KNX "ETS version".

Within a KNX project there is always the possibility to set a BCU key for all KNX products used there. This key is then set after the first download of the application in all KNX devices that support this function.

Setting a BCU key prevents unauthorized access to the individual KNX components on the one hand, but on the other hand access to devices is no longer possible if the BCU key is lost.

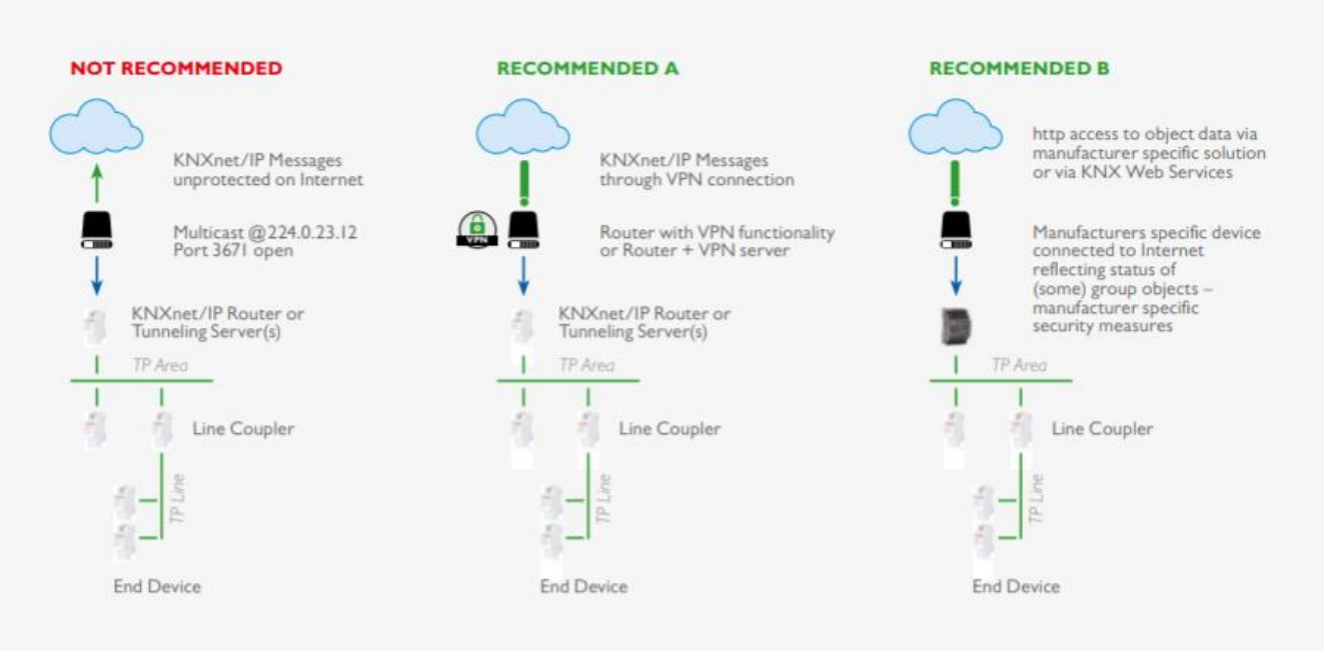
A reset of such a BCU key is currently only possible with the corresponding KNX project and its valid key, which must be identical to the key stored in the device.

KNX devices become unusable if the BCU key is lost and must be replaced.

From the KNX side we can only recommend the use of our IP KNX Secure components to prevent manipulation and unauthorized access via IP. Taking this in consideration should prevent such cyber attacks when encryption is set or activated.

BHAS Support Center – DESTO Application Engineering Team

IP Topology



Source: KNX.org

It is still the operator's or administrator's responsibility to not make such systems directly accessible or visible via the Internet.

Overview of our ABB i-bus® KNX system components with IP – Secure:

Product Type	Product ID	Additional Information
IPR/S 3.5.1	2CDG110176R0011	IP - Secure
IPS/S 3.5.1	2CDG110204R0011	IP - Secure

For more product information visit our website (link).

BUILDING AND HOME AUTOMATION SOLUTION, 01/2022

Sicherheitsrelevante technische Mitteilung

Setzen bzw. Aktivieren des BAU Passworts durch eine „Cyber-Attacke”

Intelligente Gebäudeinstallationen, dazu gehört auch KNX, werden zunehmend Ziel von Cyber-Attack Angriffen. Diese Cyber Angriffe können sehr einfach vermieden werden, indem sichergestellt wird, dass solche Installationen nie direkt (ohne einen VPN) über das Internet zugänglich sind.

Ist eine KNX Installation mit dem Internet verbunden, ist der Einsatz eines VPN-Tunnels für den Zugriff über das Internet ein absolutes MUSS. Beim Einsatz einer KNX Secure Tunnel-Schnittstelle ist also zu beachten, dass die von der ETS empfohlenen starken Passwörter verwendet werden.

Deshalb sprechen wir hier grundsätzlich nicht über einer direkten Cyber-Attacke auf den KNX.

Was ist bzw. kann die Folge bzw. Auswirkung einer solchen Cyber-Attacke sein?

Am häufigsten wird über das unberechtigte Setzen eines BAU Passwortes berichtet. Hier werden die Physikalischen Adressen der Geräte ausgelesen bzw. gescannt und danach mit einem BAU Schlüssel, falls noch nicht gesetzt, beschrieben. Auffällig dabei ist, dass die Funktionen der betroffenen KNX Geräte nicht mehr gewährleistet sind. Das kann in der Regel nur mit einem entsprechenden Tool der KNX „ETS Version“ durchgeführt werden.

Innerhalb eines KNX Projektes besteht grundsätzlich immer die Möglichkeit, gesamthaft ein BAU Passwort für alle dort verwendeten KNX Produkte zu setzen. Dieses Passwort wird dann nach dem ersten Download der Applikation in allen KNX Geräten, welche diese Funktion unterstützen, gesetzt.
Das Setzen eines BAU Schlüssels verhindert auf der einen Seite unberechtigte Zugriffe auf die einzelnen KNX Komponenten, aber auf der anderen Seite sind Zugriffe auf Geräte bei Abhandenkommen des BAU Passwortes nicht mehr möglich.

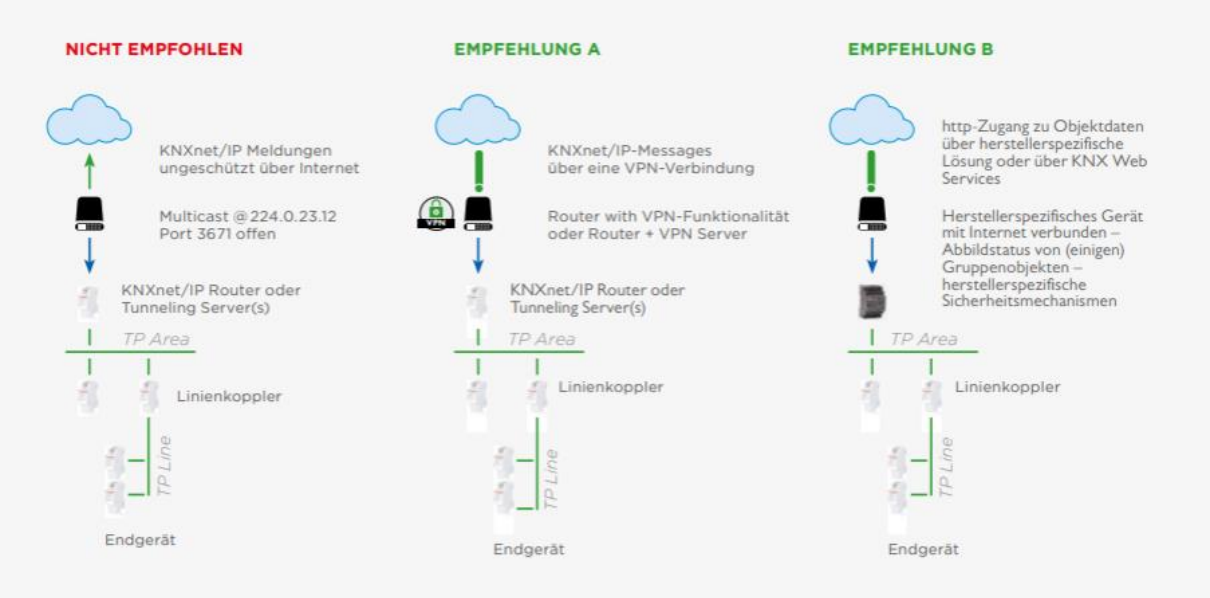
Ein Rücksetzen eines solchen BAU Schlüssels ist derzeit nur mit dem entsprechenden KNX Projekt und dessen gültigen BAU Schlüssel, welcher identisch mit dem im Gerät hinterlegten Schlüssel sein muss, möglich.

BHAS Support Center – DESTO Application Engineering Team

KNX Geräte werden bei Abhandenkommen des BAU Passwortes unbrauchbar und müssen ausgetauscht werden!

Von der KNX Seite her können wir nur die Verwendung unserer IP KNX Secure Komponenten empfehlen, um die Manipulation und den unberechtigten Zugang über IP schon mal zu verhindern. Diese Maßnahme verhindert bei gesetzter bzw. aktivierter **Verschlüsselung** solche Cyber Attacken.

IP Topology



Quelle: KNX.org

Es liegt deshalb immer noch in der Eigenverantwortung des Betreibers bzw. Administrators solche Anlagen nicht direkt über das Internet zugänglich bzw. sichtbar zu machen.

Übersicht unserer ABB i-bus® KNX Systemkomponenten mit IP - Secure:

Produkt Typ	Produkt ID	Zusätzliche Informationen
IPR/S 3.5.1	2CDG110176R0011	IP- Secure
IPS/S 3.5.1	2CDG110204R0011	IP - Secure

Für mehr Produktinformationen besuchen Sie unsere Website (Link).