Bosch Security Systems B.V.
P.O. Box 80002
5600 JB Eindhoven
Besucher:
Torenallee 49
5617 BA, Eindhoven
Telefon +31 4025 77-174
Telefax +31 4025 77-119
www.boschsecurity.nl

19.03.2021

Cybersecurity

Important information about the Cybersecurity of your Access Control System (ACS)

Dear customer,

You have chosen an access control system from Bosch Building Technologies. As many other building solutions, this access control system is based on connected IT-components.

Our access control systems meet relevant norms and standards and are protected against unauthorized access by various security measures.

In order to maintain IT security over the entire operating period your help is indispensable.

We kindly ask you to take the following notes into account in your own interest and to implement the measures mentioned there.

1. **General Measures**

    1. Minimize access: Take appropriate measures to prevent unauthorized physical access to the IT components of the access control system (e.g. access controller AMC2). You should apply the "principle of least privilege", which grants stakeholders and components only the privileges necessary for executing its role.

2. Administrative privileges: you should run the host system without administrative privileges. The host system runs without administrative privileges, but they will be required for configuration purposes.

3. Passwords: Re-assign all passwords immediately after the installation of the access control system to protect them from misuse. This also includes the access controller AMC2. See, for instance, NIST Special Publication 800-63B "Digital Identity Guidelines. Authentication and Lifecycle Management". Sect. 5.1.1 covers passwords.

4. Hardening: apply general hardening recommendations for your operating system. This includes, for instance, installing anti-virus and anti-spyware software, keep software up to date, disable USB ports and external hard drive. The exact measures depend on the situation and should be discussed with an IT security responsible person of your organization.

2. Software

1. Operating System: Use supported operating system for your host system (BIS/AMS). You find this information in the product documentation of the respective product: Product catalogue

2. Browser: Use recommended browsers on any client computer. That is Internet Explorer 9, 10 or 11 in compatibility mode. Please check the respective data sheet for BIS or AMS

3. Use .NET in the version recommended for your system. You find this information in the data sheets.

4. Latest updates: Ensure that all components of the access control system do have latest software and firmware updates. You find updates of Bosch Access products here.

5. Checksum: Bosch creates checksums of each binary package of its software products. Please reach out to Bosch Building Technologies, if you want to compare the checksums of your binaries with the one computed and approved by Bosch.

3. Network

1. Dedicated network: Use a separate network for the IT components of the access control system. The AMC communicates via UDP, so your router configuration should limit UDP broadcasts to the dedicated access control network.

2. Network transitions and firewalls: Protect any network transitions between the access control system and other IT systems with a firewall. Configure the firewall in a way that only necessary connections are allowed. Also, the host system (BIS/AMS) should be protected by an application-level firewall. The guide **BIS_Firewall_Configuration.docx**, which you'll find in the installation folder, provides information to successfully setup the BIS system in a firewall-protected environment. Herein you will find the relevant settings concerning the Windows 8.1, Windows 10, Windows Server 2012 R2, Windows Server 2016 Firewall, but also the appropriate settings for third-party firewalls.

3. Encryption: If applicable, use only encrypted protocols for communication between the access control system and other IT systems. Examples are SSL and HTTPS.

4. Data Security: The installation folder of your host system (BIS/AMS) contains a guide that describes ways to improve data security for a BIS installation. Its focus is on configuring a secure network environment for the Building Integration System using IPSec on Windows. The file name is **BIS_Data_Security.pdf**.

4. Access Control

1. Decommissioning of unused components: Reset components of the access control system (e.g. access controller AMC2) that are not used any longer to factory defaults; delete all personal data and security information.

2. Monitoring of alarms:

    1. Monitor alarms that are triggered if a device goes offline (e.g. access controller AMC2) as this indicates potential misuse.

    2. Monitor alarms that are triggered if tampering on the readers is detected, e.g. when readers are opened.

For maintaining a secure system, it is essential that trained personnel look at all alarms and takes them seriously.

3. Encryption: Use encrypted communication between access reader and access controller, i.e. OSDPv2 using Secure Channel.

4. Reader and Cards Technologies: Choice of secure card technologies and the respective readers is highly recommended. Today, secure choices are MIFARE DESFire EV1, MIFARE DESFire EV2, and Legic Advant.

Kind regards

Bosch Security Systems B.V.