

BNA Fernwartung

Maßnahmen für die IT-Sicherheit

Copyright © 2015 by BN Automation AG

Alle Rechte vorbehalten. Die Weitergabe und Vervielfältigung dieses Dokuments oder von Teilen davon ist – gleich welcher Art und Weise – nur mit schriftlicher Genehmigung der BN Automation AG gestattet.

Technische Daten dienen nur der Produktbeschreibung und sind keine zugesicherten Eigenschaften im Rechtssinn.

Änderungen – auch in technischer Hinsicht – vorbehalten.

Inhaltsverzeichnis

<u>1</u>	<u>Einführung</u>	<u>3</u>
<u>2</u>	<u>Realisierte Maßnahmen für die IT-Sicherheit</u>	<u>4</u>
<u>2.1</u>	<u>Geregelte Verantwortung</u>	<u>4</u>
<u>2.2</u>	<u>Verpflichtung der Mitarbeiter</u>	<u>4</u>
<u>2.3</u>	<u>Dedizierte Fernwartungsrechner</u>	<u>4</u>
<u>2.4</u>	<u>Zugang zum Fernwartungsnetzwerk nur für berechtigte Mitarbeiter</u>	<u>4</u>
<u>2.5</u>	<u>Laufende Aktualisierung der Fernwartungsrechner</u>	<u>4</u>
<u>2.6</u>	<u>Verschlüsselte Kommunikation zu Kundennetzwerken (Standardfall: IPsec VPN)</u>	<u>4</u>
<u>2.7</u>	<u>Feste Adresse für alle Fernwartungszugriffe</u>	<u>5</u>
<u>2.8</u>	<u>Zentrale Datenhaltung</u>	<u>5</u>

1 Einführung

Immer mehr Unternehmen nehmen zur Absicherung der Produktion die Hilfe von externen Experten in Anspruch. Vielfach geschieht dies im Rahmen einer Fernwartung. Die Fernwartung ermöglicht eine schnelle Reaktion bei Bedarf, erfordert jedoch eine gleichzeitige Umsetzung von geeigneten IT-Sicherheitsmaßnahmen, um die Risiken nicht unnötig zu steigern.

Das Dokument listet die bei der Fernwartungslösung von BN Automation AG umgesetzten Maßnahmen für die IT-Sicherheit auf.

2 Realisierte Maßnahmen für die IT-Sicherheit

2.1 Geregelte Verantwortung

Die Verantwortung für die IT-Sicherheit der BNA-Fernwartungslösung ist geregelt und eine laufende Kontrolle der IT-Sicherheitsmaßnahmen sichergestellt.

BN Automation AG hat einen Mitarbeiter als Datenschutzbeauftragten berufen.

2.2 Verpflichtung der Mitarbeiter

Die Mitarbeiter der BN Automation AG sind zur Wahrung der Datengeheimnisse mit einer Verpflichtungserklärung nach § 5 des Bundesdatenschutzgesetzes verpflichtet. Diese Verpflichtung besteht auch über das Ende der Tätigkeit bei der BN Automation AG hinaus.

2.3 Dedizierte Fernwartungsrechner

Die Fernwartung erfolgt über eigens zu diesem Zweck bereitgestellte Fernwartungsrechner und nicht über die normalen Arbeitsplatzrechner der Mitarbeiter. Auf den Fernwartungsrechnern sind somit nur die für die Durchführung der Fernwartung erforderlichen Programme installiert. Die Fernwartungsrechner sind gehärtet und mit aktivierten Sicherheitsmechanismen konfiguriert. Die Benutzer der Fernwartungsrechner verfügen nicht über Administrationsrechte.

2.4 Zugang zum Fernwartungsnetzwerk nur für berechtigte Mitarbeiter

Die Fernwartungsrechner sind weitgehend vom internen BNA-Netzwerk abgeschottet und kommunizieren über ein eigenes Fernwartungsnetzwerk. Das Fernwartungsnetzwerk selbst wird durch eine separate Firewall geschützt.

Den Zugang zu den Fernwartungsrechnern haben nur berechtigte und eingewiesene Mitarbeiter. Alle An- und Abmeldungen an den Fernwartungsrechnern werden protokolliert und die Protokolle zwei Jahre aufbewahrt.

2.5 Laufende Aktualisierung der Fernwartungsrechner

Auf den Fernwartungsrechnern ist eine Sicherheitslösung aktiv, die alle Dateiaktionen überwacht, bei Verdacht den Zugriff auf die betroffene Datei verhindert und den Benutzer sowie den IT-Administrator benachrichtigt. Diese Sicherheitslösung wird mehrmals täglich mit aktuellen Daten vom Hersteller automatisch aktualisiert.

Die Fernwartungsrechner sind mit dem aktuellen Windows-Betriebssystem ausgestattet, die von Microsoft bereitgestellten Sicherheitsupdates werden automatisch verteilt und installiert. Mit dem gleichen Verfahren werden auch die Standardsoftwareprodukte weiterer Hersteller wie Adobe auf dem aktuellen Stand gehalten.

2.6 Verschlüsselte Kommunikation zu Kundennetzwerken (Standardfall: IPsec VPN)

Die Kommunikation zwischen dem Fernwartungsnetzwerk und der Anlage erfolgt über eine sichere und verschlüsselte VPN-Verbindung. Wir empfehlen die Nutzung des bewährten und verbreiteten IPsec-

Protokolls, das von allen namhaften Router- und Firewall-Herstellern unterstützt wird. Alternativ unterstützen wir auch SSL-VPN-Verbindungen nach dem OpenVPN-Standard.

2.7 Feste Adresse für alle Fernwartungszugriffe

Alle Fernwartungszugriffe erfolgen ausschließlich von einer festen IP-Adresse bzw. Telefonnummer. Das gibt Ihnen die Möglichkeit, die Zugriffe auf diese Adresse bzw. Rufnummer einzuschränken und so die IT-Sicherheit weiter zu steigern.

2.8 Zentrale Datenhaltung

Alle für die Durchführung der Fernwartung erforderlichen Daten werden zentral gehalten und täglich gesichert. Besonders sensible Daten wie Passwörter werden verschlüsselt und separat für jede Anlage abgelegt.

Impressum:

BN Automation AG
Gewerbepark „Am Wald“ 5a
98693 Ilmenau

Autor: Dr. Jan Rudorfer
Telefon: +49 3677 855-510
Telefax: +49 3677 855-599