Cyber Security Incident Response Team (CSIRT) Policy der PROFIBUS Nutzerorganisation e. V.

Version 1.0 – Datum August 2020

Order No.: 8.721

File name : PNO_CSIRT_Policy_8721_V10_Aug20.docx

Comments to be submitted to the Editor of the Document Karl-Heinz@Niemann-on-line.de
.

Prepared by PI Working Group PG10 “Security” in Committee B “PROFINET”.

In this specification the following key words (in **bold** text) will be used:

may: indicates flexibility of choice with no implied preference.

should: indicates flexibility of choice with a strongly preferred implementation.

shall: indicates a mandatory requirement. Designers **shall** implement such mandatory requirements to ensure interoperability and to claim conformance with this specification.

Publisher:
PROFIBUS Nutzerorganisation e.V.
Haid-und-Neu-Str. 7
76131 Karlsruhe
Germany
Phone : +49 721 / 96 58 590
Fax: +49 721 / 96 58 589
E-mail: info@profibus.com
Web site: www.profibus.com

Content

Revision Log

Version	Ersteller	Datum	Kommentar
0.4	Niemann	05. Juni 2020	Version zur Veröffentlichung
0.5	Niemann	23. Juli 2020	Kapitel 4 (Advisories) gestrichen, kleinere Änderungen
1.0	Niemann	20 August 2020	Erste veröffentlichte Version

1 Einleitung

Durch die zunehmende Vernetzung von Produktionsanlagen steigt das Risiko von Cyber-Angriffen. Diesem Risiko sind auch die Kommunikationstechnologien ausgesetzt, welche durch die PROFIBUS und PROFINET International (PI) spezifiziert und unterstützt werden. Um diesem Risiko Rechnung zu tragen, betreibt PROFIBUS und PROFINET International ein Cyber Security Incident und Response Team (CSIRT).

- Das PNO-CSIRT bietet Informationen und Unterstützung für Mitgliedsunternehmen von PI und Nutzern der Technologien von PI. Dies umfasst die Unterstützung bei der Umsetzung proaktiver Maßnahmen zur Verringerung der Risiken von Computersicherheitsverletzungen sowie bei der Reaktion auf derartige Verletzungen bzw. Vorfälle, sobald diese eintreten. Das PNO-CSIRT soll dabei auch den regionalen PROFIBUS und PROFINET Organisationen (RPAs) als Ansprechpartner dienen.
- Das PNO-CSIRT sieht sich dabei als Mittler zwischen Technologielieferanten, Komponentenherstellern, Systemherstellern und Nutzern der Technologien der PROFIBUS Nutzerorganisation (PI).
- Das PNO-CSIRT dient als Ansprechpartner für andere CSIRTs / CERTs sowie andere nationale und internationale Institutionen (z. B. BSI, ENISA) in Fragen der Technologien der PROFIBUS Nutzerorganisation (PI) und pflegt entsprechende Kontakte zu diesen Institutionen.

Die besondere Rolle der PNO als Herstellervereinigung bedeutet, dass das PNO-CSIRT seinen Fokus auf der Bearbeitung von Schwachstellen in den Spezifikationen der Technologien der PROFIBUS Nutzerorganisation (PI) sieht und dass die Bearbeitung produktabhängiger Schwachstellen in der Verantwortung der jeweiligen Technologie-, Komponenten- oder Systemlieferanten liegt. Das PNO-CIRT wird in diesem Fall die erforderliche Unterstützung leisten, um eingehende Schwachstellenmeldungen an die entsprechenden Adressaten weiterzuleiten und eine entsprechende Rückmeldung an die meldende Person / das meldende Unternehmen zu geben.

2 Policy

Für die Arbeit des CSIRT gelten die folgenden Regeln:

- PI ist einem vertrauensvollen Umgang mit Herstellern und Nutzern verpflichtet. Daher werden Schwachstellenmeldungen während der Bearbeitung nur in dem zuständigen Personenkreis zugänglich gemacht und sicher gespeichert.
- PI praktiziert eine verantwortliche Offenlegungspolitik. Herstellern wird vor der Veröffentlichung einer Schwachstelle, die möglicherweise ihre Produkte betreffen, die Gelegenheit gegeben, eine Lösung zur Behebung der Schwachstelle oder eine Mitigation in angemessener Zeit zu erarbeiten.
- PI veröffentlicht nach einer angemessenen Zeit Advisories über ihr bekannte Schwachstellen und die zugehörigen Behebungen bzw. Mitigationen.
- Technische Experten aus Mitgliedsunternehmen, welche PI bei der Analyse von Schwachstellen unterstützen, werden zur Vertraulichkeit -auch innerhalb des eigenen Unternehmens– verpflichtet.
- PI wird Schwachstellenmeldungen, welche Produkte eines Unternehmens betreffen, zusammen mit Informationen über die meldende Person an dieses Unternehmen zur Problemlösung weiterleiten. Die Weitergabe der Kontaktinformation der meldenden Person soll die Problemlösung beschleunigen. Sofern eine anonyme Weiterleitung gewünscht ist, kann das im Meldeformular angegeben werden.

3 Meldung von Schwachstellen

Bei der Meldung von Schwachstellen, welche Produkte betreffen, wenden Sie sich bitte an den Hersteller des jeweiligen Produktes.

Schwachstellen bei denen davon auszugehen ist, dass Kommunikationsprotokolle der PI ursächlich sind, können Sie hier melden. Sofern die Ursache unklar oder nicht bekannt ist, kann ebenfalls hier eine Meldung erfolgen. PI wird die Meldung dann bewerten und ggf. and den betroffenen Hersteller zur Problemlösung weiterleiten.

Die Meldung von Schwachstellen in Bezug auf Protokolle der PI kann wie folgt erfolgen:

- PI nimmt Meldungen von Schwachstellen über ein Online-Formular auf www.profinet.com/security oder die E-Mail-Adresse security@profinet.com entgegen.
- Sofern gewünscht kann eine verschlüsselte E-Mail-Kommunikation erfolgen. Den öffentlichen PGP-Schlüssel des CSIRT finden Sie auf www.profibus.com/security.
- Es wird vorzugsweise darum gebeten, das online-ausfüllbare Meldeformular auf dieser Webseite zu verwenden.
- Der Eingang der Meldung wird von PI bestätigt. Die meldende Person wird über den Stand der Bearbeitung informiert.
- Sofern Sie sich für eine vollständig anonyme Meldung entscheiden, werden Sie keine Bestätigung und auch keine Informationen über den weiteren Verlauf der Bearbeitung Ihrer Meldung erhalten.
- Sofern Sie sich für eine teilweise anonyme Meldung entscheiden, werden Ihre Kontaktdaten erfasst und in der Geschäftsstelle verarbeitet. Jedoch erhalten die mit der Bearbeitung befassten technischen Spezialisten keine Information über Ihre Identität.

Hinweis: Bei der Feststellung oder Meldung einer Schwachstelle müssen Gesetze oder andere Verpflichtungen, insbesondere Vertraulichkeitsverpflichtungen und/oder Exportkontrollregelungen beachtet werden.

PI wird zur Abklärung der Schwachstellenmeldung in vielen Fällen Kontakt mit dem Hersteller der Komponente oder dem Hersteller evtl. verwendeter Technologiekomponenten (z. B. Protokoll-Stacks) aufnehmen.

4 Haftungsbeschränkung

PI wird übermittelte Schwachstellenmeldungen unentgeltlich mit angemessener Sorgfalt bearbeiten.

PI übernimmt keine Haftung jeglicher Art, weder ausdrücklich noch stillschweigend, für die Richtigkeit, Fehlerfreiheit, Freiheit von Schutz- und Urheberrechten Dritter, Vollständigkeit und/oder Verwendbarkeit der angebotenen Informationen in Zusammenhang mit Schwachstellenmeldungen und deren Bearbeitung und Behebung. – außer bei Vorsatz oder Arglist.

Für Schäden materieller oder immaterieller Art, die in Zusammenhang mit den Schwachstellenmeldungen und deren Bearbeitung und Behebung unmittelbar oder mittelbar verursacht werden, haftet PI nicht, sofern ihr nicht nachweislich vorsätzliches oder grob fahrlässiges Verschulden zur Last fällt. Für Schäden aus der Verletzung von Leben, Körper oder der Gesundheit haftet PI nach den gesetzlichen Bestimmungen.

PROFIBUS Nutzerorganisation e. V. (PNO)
PROFIBUS & PROFINET International (PI)
Haid-und-Neu-Str. 7 ● 76131 Karlsruhe ● Germany
Phone +49 721 96 58 590 ● Fax +49 721 96 58 589
E-mail info@profibus.com
www.profibus.com ● www.profinet.com