Scada

Sie erhalten diese Nachricht, da eine IP-Adresse aus Ihrem Verantwortungsbereich einer Steuerungskomponente zugeordnet wurde, welche über das Internet verfügbar ist. Es besteht eine mögliche Gefährdung für die Systeme Ihres Kunden. Das BSI bittet Sie daher, den betroffenen Kunden mit dem beigefügten Informationsschreiben zu warnen, in dem die bestehenden Gefahren sowie mögliche Handlungsoptionen aufgezeigt werden.

Explizit möchten wir darauf hinweisen, dass keine Anzeichen dafür vorliegen, dass von der genannten IP-Adresse ausgehend ein Angriff durchgeführt wurde.

Da es sich vermutlich um eine Steuerungskomponente aus der Fabrikautomation, Prozessautomatisierung oder Gebäudesteuerung handelt, sollte diese IP-Adresse nicht blockiert oder gesperrt werden, da dies u. a. kritische Folgen für den Betreiber bzw. den gesteuerten Prozess haben kann.

```
Sie erhalten diese Nachricht, da eine Ihnen zugeordnete Steuerungskomponente
unmittelbar über das Internet erreichbar ist.

Das BSI hat von Dritten Kenntnis darüber erhalten und möchte Ihnen die damit
verbundenen Gefahren sowie mögliche Handlungsoptionen aufzeigen.

Speicher-programmierbare Steuerungen, Visualisierungsmodule oder andere Komponenten
aus dem industriellen Umfeld im Bereich Fabrikautomation, Prozessautomatisierung oder
Gebäudesteuerung werden zunehmend vernetzt.

Mit der Anbindung an das Internet werden solche Komponenten einer Reihe von
Gefährdungen ausgesetzt, die im Falle eines unberechtigten Zugriffs mitunter kritische
Folgen haben können.

Sofern eine mit dem Internet verbundene Komponente nicht hinreichend vor
unberechtigtem Zugriff geschützt ist, kann ohne die dazu erforderlichen
Authentisierungsinformationen darauf zugegriffen werden.

Auch Standardpasswörter zu solchen Komponenten sind über das Internet zu ermitteln und
bieten somit keinen Schutz.

Auch wenn eine Anmeldung mit Benutzername und Passwort erforderlich ist, schützt dies
noch nicht vor Angriffen.

Häufig werden solche Komponenten nicht mit verfügbaren Updates und Patches versorgt,
um bekannte Schwachstellen zu schließen.

In der Folge kann ein Angreifer diese Schwachstellen ausnutzen, um ggf. die
vollständige Kontrolle über die Komponente zu erlangen. In diesem Fall ist nicht nur
die Komponente selbst betroffen.

Ein Angreifer kann diese als Einfallstor in das lokale Netzwerk missbrauchen und sich
so in der gesamten Infrastruktur ausbreiten.
```

```
## Was sollten Sie tun?
* Bewerten Sie die genannten Gefährdungen und die damit verbundenen Risiken für ihren
konkreten Anwendungsfall.
* Verwenden Sie hinreichend komplexe Passwörter für den Zugriffsschutz.
* Beschränken Sie den Zugriff auf Steuerungskomponenten über eine Firewall mit
möglichst restriktivem Regelwerk.
* Minimieren Sie die von der Steuerungskomponente bereitgestellten Dienste auf das,
was unbedingt erforderlich ist (z. B. durch Deaktivieren von Diensten wie Telnet).
* Versorgen Sie Steuerungskomponenten zeitnah mit Updates und Patches des jeweiligen
Herstellers.
* Setzen Sie VPN-Lösungen ein, um die Kommunikation über das Internet über einen
kryptographisch geschützten Tunnel zu führen.

Weitere Informationen bietet das BSI kostenfrei auf der Webseite <https://
www.bsi.bund.de/ICS> <i class="fa fa-external-link"></i> an. Dort finden Sie u.a. das
Dokument "Industrial Control System Security: Top 10 Bedrohungen und Gegenmaßnahmen"
zum Download, welches über diese und weitere Gefährdungen informiert.

<https://www.bsi.bund.de/DE/Themen/weitereThemen/ICS-Security/Empfehlungen/Betreiber/
Betreiber_node.html>

Wenn Sie Fragen haben oder ein persönliches Gespräch wünschen, wenden Sie sich bitte
per E-Mail an <ics-sec@bsi.bund.de> um das Referat "Cyber-Sicherheit in kritischen IT-
Systemen, Anwendungen und Architekturen" direkt zu erreichen.
```

Quelle: https://support.belwue.de/sicherheit/sicherheitswarnungen/scada/