



# Our supplier has been hit! What do we do now?

Gregor Wegberg | Swiss Cyber Storm, October 24, 2023

# Gregor Wegberg

**Head of Digital Forensics & Incident Response**

Member of the Management Board

Lecturer at Eastern Switzerland University of Applied Sciences



# Attackers could have cut power

TLP: CLEAR

Wayback Machine | https://www.kisters.de/en/ | 245 captures | 15 Jun 2018 - 6 Apr 2023

KISTERS | Current contact details | Press releases | Notification Data Protection

Official communication from KISTERS AG

## IT security incident

🇩🇪 Deutsche Version | 🇪🇸 Versión en español | 🇫🇷 Version française

- Current contact details
- Notification Data Protection
- Press releases

At this point we will give you updates on our current situation:

After that, the release will take place step by step in the following days and weeks. Your KISTERS contact person will then get in touch with you.

Parallel to this, the forensic analyses will continue.

2021-11-22

According to the forensic analyses carried out so far, there are currently no indications that our delivered software products have been compromised.

We will be happy to talk to you and pass on information verbally. Please contact your sales representative directly by telephone or use the [contact details on this website](#).



# Attackers could have **remote access** to your warehouse

TLP: CLEAR

## *IT infrastructure of SSI Schaefer shut down as a precautionary measure*

*For security reasons, SSI Schaefer Group's global IT network has been shut down as a precaution during the night of April 13 to 14, 2023. **The shutdown is a proactive measure.** It was taken down immediately after the company's Security Operations Center detected irregularities in its own IT network.*

*With the support of external specialists, extensive analyses and security scans are currently underway to determine what the exact cause was. In addition, corresponding task forces have been set up and are working at full speed to restore the complete working capability.*

*"The colleagues from our IT are working tirelessly to record the effects and to remedy the impairments. At SSI Schaefer, the security of products, services and data is of the utmost highest priority. That is why we suspended all systems immediately after the irregularities were discovered," explains Steffen Bersch, CEO of SSI Schaefer.*

**Based on current knowledge, customer data is not affected.**

Source: <https://www.borncity.com/blog/2023/04/24/cybersicherheit-ssi-schaefer-shop-nachwehen-post-und-dhl-portal-offline-greenbone-mit-problemen-etc/>  
Original statement (offline, removed): <https://www.ssi-schaefer.com/en-au/company/news/it-infrastructure-of-ssi-schaefer-shut-down-as-a-precautionary-measure-1474128>



# What services and products do we use that they supply? What **access** do their employees have?

TLP: CLEAR



# Sounds familiar. Doesn't it?

Remember to consider attacks against your partners **in your own security efforts**

- ▶ Their targeted security posture does not have to match or exceed yours
- ▶ Know the assets managed or accessed by external entities
- ▶ Only part of your security measures have an impact on the external party



# What can we do today to increase the likelihood of transparency?

TLP: CLEAR



# Form a **community** of affected organizations

TLP: CLEAR





# At what point can we **trust** them again? Do we want to?

TLP: CLEAR



# Understand and act accordingly

TLP: CLEAR



# How bad is it really? Okay **so far.**

TLP: CLEAR



# Let's connect



[www.oneconsult.com](http://www.oneconsult.com)



[/oneconsult-ag](https://www.linkedin.com/company/oneconsult-ag)



[/OneconsultAG](https://twitter.com/OneconsultAG)



[/oneconsult](https://www.youtube.com/channel/UC...)

