# North Korea's hackers target Diehl Defence

## "Kimsuky" cyber attacks: North Korea's hackers: Diehl Defence in the crosshairs

by Hakan Tanriverdi

27.09.2024 | 13:00

Fake job offers and a fake website: Hackers from "Kimsuky" have apparently tried to steal sensitive data on military technology from the arms company Diehl Defence.


Military technology from Diehl Defence: North Korea apparently allows hackers to obtain data.

Source: Reuters

---

Anti-aircraft missiles from the Baden-Württemberg company Diehl Defence are protecting the Ukrainian capital from Russian attacks - apparently quite successfully. "Every shot is a hit," said Kyiv Mayor Vitali Klitschko in March 2023, commenting on German military technology in the defensive war against Russia .

The German government is also planning to use Diehl technology. Three new government aircraft are to be equipped with a missile defense system.

## "Kimsuky" hackers on behalf of North Korea

According to research by ZDF frontal and "Spiegel", North Korean hackers attempted to steal information about the German arms company's military technology in a months-long operation.
The hackers sent out fake job offers containing spyware, tried to steal passwords and cleverly disguised their actions. The hacker group is known in security circles as "Kimsuky" and works for North Korea's military intelligence service. They are supposed to obtain sensitive information on behalf of the government.

---

## IT experts have been observing "Kimsuky" for some time

As early as the first quarter of 2024, IT security experts from Mandiant were able to observe the "Kimsuky" hackers. They were interested in "certain zip codes" and were looking for information "on how to register phone numbers in Germany," says Michael Barnhart, an IT security expert at the company, which is owned by Google .

Research shows that the hackers set up a website in mid-April that allows conclusions to be drawn about who "Kimsuky" was targeting. The website used the name of the defense company, but misspelled: Dihl Defence - one "e" is missing.

---

## Spy software via fake job offers

The hackers sent out fake job offers: As a security officer in Berlin, you could earn up to 100,000 US dollars, with a working time of "five to seven hours." Anyone who opened the document fell into a trap and ended up on the hackers' server. From there, spy software was downloaded onto the computer without anyone noticing.

The hackers' server had Überlingen in its website name. Diehl Defence has its headquarters in Überlingen. The spy software can, among other things, take screenshots, display all files and download additional software.

---

The hackers also set up a login portal on this "Überlingen" site, supposedly from Deutsche Telekom. Anyone who tried to log in there with their Telekom data unknowingly passed this information on to the hackers. This is how the "Kimsuky" hackers wanted to get hold of user names and passwords.

## Diehl Defence does not comment

When asked, Diehl Defence declined to comment. A spokesperson said that they were "generally preparing themselves against all threats". The company did not comment on details. When asked, the Federal Office for Information Security confirmed that it was aware of a hacker "Germany campaign" that has been running since May 2024.

Back in February, ZDF, "Spiegel" and the Austrian "Standard" reported that the "Kimsuky" hackers were targeting nuclear weapons researchers, the Berlin Institute for International and Security Affairs and also arms companies. These new activities show that North Korea still needs sensitive information, and "Kimsuky" is supposed to get it.