

## Millions of accounts protected from criminals

Criminals steal billions of Euros every year using stolen login data - consumers and providers alike bear the damage. From a research project on identity theft, Dr. Matthias Wübbeling as CEO founded the Identeco GmbH & Co. KG. The goal is clear: protect consumers, platform providers and companies from fraud through criminal account takeovers.

### Stolen login data on the dark web

The threat is real: 80% of cyber attacks are based on stolen login data. Hackers not only take over accounts from online shops or social networks, they also penetrate companies. Together with his colleagues, Wübbeling collects stolen identity data on the dark web. All data is anonymized in the first step. "This way we don't become the target of hackers ourselves, because we only have encrypted data in our database," says Wübbeling. However, this data can be used by companies to determine valid login data. In addition to fraud prevention, this also reduces the volume of SPAM in interactive online services. Affected accounts can be restricted before criminals get access. These measures secure a company's infrastructure and increases the trust of users.

### Learn from the past

"The horse has to leave the barn first" says Wübbeling. Login data does not have to be lost from your own service, according to Identeco more than 50% of users use the same password several times for different services. If a single account is in the hands of criminals, the risk to all other online accounts is dramatically increased. However, an affected provider is just as unaware of the increased risk as the user. Once offered for exchange on the dark web, stolen login data are then used for attacks. Wübbeling and his colleagues protect against these attacks.

### Only true positives!

Identeco customers subscribe to access the continuously updated leak database. This content is used to protect employee and customer accounts: "We have already protected several million accounts from hostile takeovers," says Wübbeling proudly. "With us, all hits are true positives", the only thing that helps is immediate blocking, or at least restricting the account. "With us, there are no false alarms or uncertainties in the assessment" Wübbeling says.

### Bonn as good location

As the former federal capital, Bonn is now also the capital of IT security in North Rhine-Westphalia - maybe even all over Germany. This is due to the branches of large companies in Bonn, the Federal Office for Information Security, research institutions such as the local Fraunhofer institutes and the offer of the university with its cyber security course. Identeco GmbH & Co. KG was founded in 2020 out of the research project "Effective information after digital identity theft". "Our customers are platform operators like New Work SE or Payback who want to protect their own customers." explains Wübbeling. Businesses large and small across all industries can also assess their account security risk through a management report for their employee accounts.

### Lockout criminals in the long term

The continuous collection of leak data, GDPR-compliant processing and prompt provision to protect user accounts, that is what Identeco GmbH & Co. KG offers. "All together, we already protect more than 100 million user accounts for our customers today," says Wübbeling and adds: "In 5 years we want to be the leader for GDPR-compliant security products in Europe and protect companies worldwide from identity fraud and cyber attacks".

### Contact:

Identeco GmbH & Co. KG  
Frank Zickenheimer  
Mail: [presse@identeco.de](mailto:presse@identeco.de)  
Tel.: +49 (0) 228 286 285 81  
[www.identeco.de](http://www.identeco.de)

