INTERVIEW

Mirko Ross, CEO of [illegible] GmbH in Stuttgart

"The cyber mafia is always one step ahead technologically."

If you want to take on online criminals, you have to know their methods, says Mirko Ross, founder of the Stuttgart-based IT security company Asvin.

Mr. Ross, artificial intelligence is creating new opportunities in many industries. Does that also apply to criminals? Oh yes. Generative AI, for example, has taken phishing to a new level. In the past, fake emails could usually be recognized by typos or awkward style. Today, they are almost perfectly worded and can hardly be distinguished from real messages.

And where do these deceptively real sender addresses come from? Mostly from open sources. Criminals collect data on social networks or buy it on the darknet. Suddenly, emails from colleagues or business partners appear – with real addresses but fraudulent content.

How can you defend yourself against this professionalism? Above all, with alert attention. Everyone should check the subject line and sender—not just for errors, but for plausibility. Example: An email asks you to sign a contract via Docusign. You have to ask yourself: Does this process even exist? Is it ready to be finalized? And if in doubt: call and ask.

That sounds like healthy skepticism. But is it enough when the attacks are becoming increasingly sophisticated? It is undoubtedly becoming more difficult. With AI, voices can be can be imitated to sound deceptively real, even with emotion. Anyone who has

If you receive a voice message from your boss asking you to make a transfer, it is better not to act immediately, but to double-check first.

So not even a video call is secure? Unfortunately not. Recently, criminals infiltrated the video conference of an international company. They played AI-generated sequences of the CEO – perfectly timed so that employees believed their boss was speaking live. The goal was to trigger transfers in favor of the cybercriminals.

That sounds almost like science fiction. But it's reality. Such deepfake attacks are becoming more common. And they show that everyone, from interns to board members, needs to be aware of the danger.

What basic rules do you recommend? Firstly, healthy skepticism is not paranoia, but a necessary precaution. Secondly, there must be clarity about processes and responsibilities: callback numbers, dual control, and two-step approval must be standard. Thirdly, training. The better employees know the tricks, the less vulnerable they are.

And the perpetrators—do they ever reach their limits? Technically, hardly. What slows them down is effort. The more difficult an attack is to carry out, the less likely it is to happen. On the other hand, criminals are willing to invest if they expect high profits, and that makes it dangerous for individual companies. Therefore, those who know the methods can fight back. Ignorance, however, is the biggest weakness.

The interview was conducted by **WALTER BECK**
Editorial team, Wirtschaft magazine, walter.beck@stuttgart.ihk.de

EVENT TIP

Many representatives from companies and institutions are expected **to attend the 7th Baden-Württemberg Cybersecurity Forum** on Thursday, **November 27**. Lectures will be given by Prof. Jan Hesthaven, President of KIT, Prof. Dr. Christian Dörr from the Hasso Plattner Institute, Brigadier General Dr. Volker Pötzsch (Federal Office of Defense) and Nicole Matthöfer, President of the Baden-Württemberg Cybersecurity Agency.

Information and registration:
https://cybersicherheitsforum-bw.de