

# „Ihre Daten sind das Gold der Zukunft“

Experten zeigen, wo die Abgründe des Internets lauern – und wie sich Unternehmer schützen können

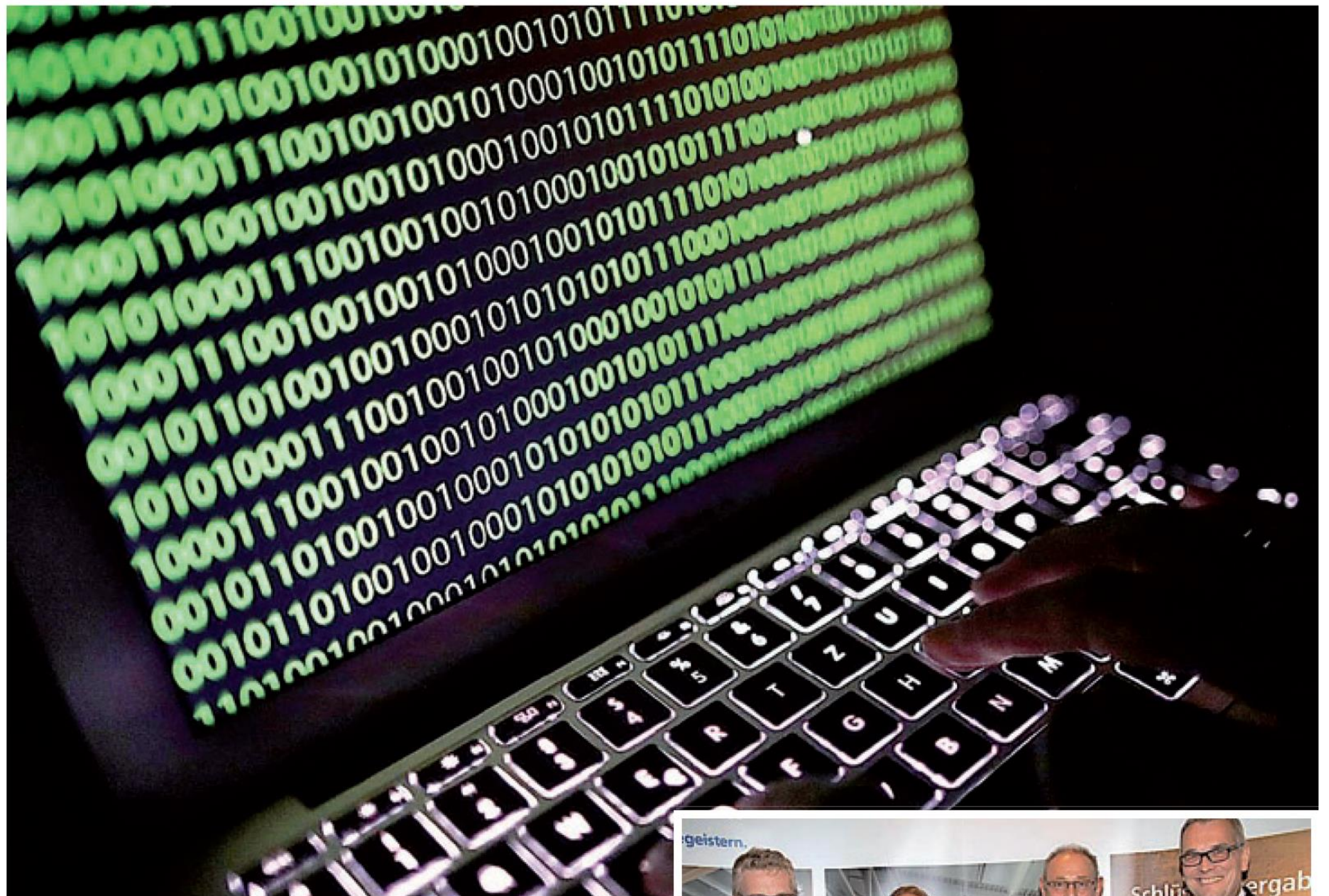
Al Capone hat die Banken noch mit der Maschinenpistole überfallen, heute werden Banken und Unternehmen so überfallen, dass sie es gar nicht merken: durch das Internet.

von Gerhard Meiser

**Frankenberg.** Um das Thema Internetkriminalität ging es jüngst bei einer spannenden Vortragsveranstaltung der Volksbank Mittelhessen im Hotel „Die Sonne“ Frankenberg für Unternehmer aus dem Raum Frankenberg/Marburg. Referenten waren der Staatsanwalt Dr. Benjamin Krause von der Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (ZIT) mit Sitz in Gießen. Zudem berichteten Jürgen Schroetter von Pharmaserv und Andreas Kötter von der Volksbank Mittelhessen von ihren Erfahrungen. „Gerade im Cybercrime ist eine ständig steigende Kriminalitätsentwicklung zu verzeichnen“, machte Bankvorstand Rolf Witezek die Gäste bei der Begrüßung auf die Brisanz des Themas aufmerksam.

„Woher können Angriffe kommen“ – um Vorsorge ging es bei dem Vortrag von Benjamin Krause von der Generalstaatsanwaltschaft in Frankfurt, er ist einer der führenden Experten für die Bekämpfung von Cybercrime. Krause ging dabei vor allem auf aktuelle Fälle ein und nahm die Zuhörer mit in die Abgründe des Internets. Vor allem machte er deutlich, dass es für einen Hackerangriff heutzutage keineswegs mehr besondere Kenntnisse erfordert. „Den passenden Virus oder Trojaner gibt es auf Bestellung gegen ein paar Euro im anonymen Darknet“, sagte Krause. „Ob Drogen, Waffen, Ausweise oder Falschgeld – für dunkle Geschäfte muss der Kriminelle nicht mal mehr das Haus verlassen. Die Ware kommt auf Bestellung per Post.“

Als einen regelrechten Trend bezeichnete Krause die so



**Hackerangriffe haben es häufig auf Firmendaten abgesehen. Rund um die Cybersicherheit informierten Andreas Kötter (Volksbank Mittelhessen, von links), Staatsanwalt Dr. Benjamin Krause, Jürgen Schroetter (Pharmaserv) und Rolf Witezek, Vorstandsmitglied der Volksbank.**

Fotos: Oliver Berg / Gerhard Meiser

genannte „Fake-President“-Masche: „Dabei geben sich die Kriminellen als Mitglied der Chefetage aus und ergaunern so mit großem manipulativen Geschick oft Millionenbeträge.“

## Auch Pharmaserv stand im Visier der Hacker

Die Dunkelziffer sei hoch, sagte der Staatsanwalt – aus Angst vor einem Reputations- und Imageverlust vermieden viele Opfer den Gang zur Polizei. „Dabei wäre die Zusammenarbeit mit den Behörden eine realistische Option zur Abwehr oder Ahndung der Straftat.“ Dass die Verfolgungsbehörden durch-

aus in der Lage sind, wirksam zu unterstützen, davon berichtete Jürgen Schroetter von Pharmaserv. Auch sein Unternehmen sei von Hackern mit umfassendem Firmenwissen und entsprechendem Sprachduktus angegriffen worden, sagte Schroetter.

Nur durch die Skepsis der sensibilisierten Mitarbeiter und mit Unterstützung durch das Landeskriminalamt habe der Angriff abgewehrt werden können. „Die Schutzmechanismen des Unternehmens und ein internes Kontrollsystem haben Schlimmeres verhindert“, so Schroetter. Er riet dazu, einen versierten IT-Security-Beauftragten



einzustellen. Es gebe auch immer wieder Angriffsversuche auf sensible Daten von Bankkunden, sagte Andreas Kötter von der Volksbank Mittelhessen. Er zeigte vor allem auf, welche Techniken die Volksbank einsetzt, um sich und ihre Kunden vor Cybercrime zu schützen. „Ihre Daten sind das Gold der Zukunft“, appellierte Kötter an die Unternehmer, dieses

Eigentum zu schützen. Gerade in unserer dynamischen Welt müsse man bewusst damit umgehen, welche Informationen man auf der Internetseite zugänglich mache.

Von den Vorträgen waren die Zuhörer „zunächst etwas geplättet“, wie es Vorstand Rolf Witezek formulierte. Trotzdem gab es anschließend noch rege Diskussionen zu dem Thema.