Mikrodarlehen sind gefragt

START-UPS Wirtschafts- und Infrastrukturbank Hessen fördert Gründer durch unkomplizierten Kredit

DARMSTADT (tm). Wer ein Unternehmen gründet, ist auf Kapital angewiesen. Und wer gerade keinen gönnerhaften Großinvestor an der Hand hat, muss früher oder später bei der Bank anklopfen. Eine interessante Alternative ist die Wirtschafts- und Infrastrukturbank Hessen (WIBank), die Förderbank des Landes Hessen.

Dort wird Firmen das „Hessen-Mikrodarlehen" angeboten. „Diese Darlehen können Gründer für Investitionen und Betriebsmittel zum Aufbau ihres Unternehmens einsetzen", erklärt Clemens Schäfer, Finanzierungsexperte der Industrie- und Handelskammer (IHK) Darmstadt. „Wir beraten Gründer im Vorfeld und begleiten sie bei der Antragstellung."

In diesem Jahr sind bereits 18 Existenzgründer und junge Unternehmen aus der Region darauf eingegangen und haben Darlehen in Höhe von 386 000 Euro beantragt. Im gesamten Vorjahr waren es lediglich 14 Gründer und 218 000 Euro, wie die IHK als Kooperationspartner der Bank berichtet.

Das Darlehen in Höhe von maximal 25 000 Euro wird dabei ohne Sicherheiten vereinbart – auch ein Mindesteigenkapital ist nicht gefordert. Zudem kann es vorzeitig ohne Entschädigungszahlung getilgt werden. „Gerade für Unternehmen in der Startphase ist das attraktiv", weiß der IHK-Experte. „Diese Finanzierungsform interessiert zunehmend auch technologieorientierte Gründer."

Die Abwicklung ist vergleichsweise unkompliziert: „Wenn der Businessplan schlüssig ist und alle Unterlagen vorliegen, leiten wir den Antrag mit unserem Votum an die WIBank weiter", so Schäfer. Die Förderbank entscheide dann relativ schnell über eine Bewilligung – oft innerhalb von ein bis zwei Wochen und mit einer Zusagequote von über 80 Prozent.

Integration fördern

FREUDENBERG Zuliefer-Spezialist ermöglicht geflüchteten Menschen einen beruflichen Neustart

Ausbilder Hagen Braun vermittelt Abdul-Hakim Alekozai (vorne), Ahmed Al-Hlewaa (hinten links) und Nwachukwu „Samuel" Ifeanyichukwu wichtige Fertigkeiten in der Lehrwerkstatt. Foto: Freudenberg

WEINHEIM (tm). Die Integration von Flüchtlingen in den Arbeitsmarkt ist eine zentrale Aufgabe für Politik, Wirtschaft und Gesellschaft. Auch der Weinheimer Zuliefer-Spezialist Freudenberg nimmt diese Verantwortung ernst.

„Unser Ziel ist es, Geflüchteten mit einer fundierten Berufsausbildung langfristige Perspektiven aufzuzeigen", erklärt Ausbildungsleiter Dr. Rainer Kuntz. „Andererseits lernen auch wir sehr viel." Der Austausch erweitere den Horizont und ermögliche das Sammeln wertvoller Erfahrungen.

Insgesamt sollen zwölf bis 15 Geflüchtete in den kommenden drei Jahren bei Freudenberg eine Ausbildung beginnen. Aktuell absolvieren fünf geflüchtete junge Männer ein berufsvorbereitendes Praktikum am Standort in Weinheim. Im September werden sie dann eine technische Ausbildung für Metallberufe beginnen.

„Es ist mir wichtig, meinen Lebensunterhalt selbst zu verdienen", sagt Abdul-Hakim Alekozai. Dem stimmt sein Kollege Samuel Ifeanyichukwu zu: „Mit der Ausbildung bekommen wir die Möglichkeit, für uns selbst zu sorgen – und ich habe zum ersten Mal in meinem Leben das Gefühl, mir eine Zukunft aufbauen zu können."

Telefontarife

Die günstigsten Tarife im Inland von Mo - Fr

Ferngespräche Zeit	Vorwahl	Tarif	Ortsgespräche Zeit	Vorwahl	Tarif
0-7	01028	0,10	0-7	01028	0,10
	01070	0,49		01052	0,58
7-8	01011	0,52		01070	0,59
	01078	0,62	7-9	01097	0,64
8-9	01019	0,58		01019	0,74
	01078	0,62		01028	1,69
9-10	01078	0,62	9-19	01097	0,64
	01098	0,63		01028	1,69
10-12	010012	0,55		01038	1,79
	01078	0,62	19-20	01038	0,79
12-14	01078	0,62		01070	0,89
	01098	0,63		01013	0,94
14-18	010012	0,55	20-22	01038	0,79
	01078	0,62		01019	0,87
18-19	01011	0,52		01070	0,89
	01078	0,62	22-24	01038	0,79
19-24	01078	0,62		01070	0,89
	01068	0,65		01013	0,94

Festnetz zu dt. Mobilfunk: Mo - So, 0 - 24h

0-24	01078	1,89		010012	2,05

Alle Anbieter mit kostenloser Tarifansage; kurzfristige Änderungen möglich. Nutzung nur von einem Festnetzanschluss der Dt. Telekom mögl..
Internet: **www.echo-online/ratgeber**
Stand: 07. 08. 2017 Quelle: biallo.de

— AUF EINEN BLICK —

Sparda-Bank mit neuem Vorstand

FRANKFURT (tm). Die Sparda-Bank Hessen eG hat die Nachfolge ihrer Führungsspitze geregelt. Denn der Vorstandsvorsitzende Professor Jürgen Weber (64) und sein Stellvertreter Hans-Joachim Hellhake (63) hatten ihr Ausscheiden bereits im vergangenen Jahr angekündigt. Seit 14 Jahren lenken sie die Geschicke des Frankfurter Kreditinstituts – nun verabschieden sie sich in den Ruhestand. Ab dem 1. Oktober wird Markus Müller (52) den Vorstandsvorsitz übernehmen. Er ist seit 2015 im Vorstand für Finanzen und Steuerung zuständig. Im als Stellvertreter zur Seite steht künftig Vorstandskollege Michael Weidmann (43), der den Vertrieb und das Treasury verantwortet.

„Gegen viele Angreifer kann man sich wehren"

MICHAEL WAIDNER Der Leiter des Fraunhofer SIT über Risiken und Schutzmaßnahmen in einer zunehmend digitalisierten Welt

Foto: Andreas Kelm

DARMSTADT. Die Digitalisierung verändert die Welt – und hebt die Bedeutung sicherer Strukturen im Netz auf ein neues Niveau. Vor allem nach den letzten Hackerangriffen auf Unternehmen. Das rückt Darmstadt als bundesdeutsche Hauptstadt für IT-Sicherheitsforschung verstärkt in den Blickpunkt. Wir haben mit Professor Dr. Michael Waidner, Leiter des Fraunhofer-Instituts für Sichere Informationstechnologie SIT, über die Risikolage und die Antworten der Wissenschaft gesprochen.

INTERVIEW

Herr Professor Waidner, sind Sie eigentlich schon einmal persönlich Opfer einer Cyber-Attacke geworden?

Das ist eine gute Frage. Natürlich werde ich genauso angegriffen wie jeder andere Internetnutzer, etwa mit Phishing-Nachrichten oder durch E-Mails mit infizierten Anhängen. Bislang habe ich aber noch keinen Schaden erlitten, zumindest nicht wissentlich.

Ist das der springende Punkt?

Zu wissen, ob man erfolgreich angegriffen wurde, ist tatsächlich eines der großen Probleme in der Cybersicherheit. Im Durchschnitt brauchen Unternehmen mehr als 140 Tage, bis sie entdecken, dass ein Angreifer erfolgreich in ihre Systeme eingedrungen ist. Das dauert noch deutlich zu lange und gibt dem Angreifer viel zu viel Zeit, unbemerkt Daten abzugreifen und Schaden anzurichten. Das ist eine der großen Herausforderungen für die Forschung.

Der Branchenverband Bitkom hat mitgeteilt, dass jedes zweite Unternehmen angegriffen wird und dabei jährlich ein Schaden von 55 Milliarden Euro entsteht. Der Discounter Lidl und andere bauen nun spezielle Abteilungen dagegen auf. Wie schätzen Sie die gesamte Entwicklung ein?

Angegriffen werden tatsächlich alle Unternehmen in Deutschland. Das ist kein Wunder, denn Kriminelle haben die Digitalisierung für sich entdeckt wie alle anderen auch. Und Angriffe im Internet kann man vergleichsweise einfach und ohne viel Aufwand durchführen. Die Frage ist, wie oft diese Angriffe tatsächlich erfolgreich sind und was die Unternehmen, die erfolgreich angegriffen wurden, besser machen sollten. Etwa die Hälfte der Firmen wissen, dass sie erfolgreich angegriffen wurden, das heißt dort ist Schaden entstanden. In Wirtschaft und Politik hat deshalb das Bewusstsein sehr stark zugenommen, dass etwas getan werden muss. Gerade bei den großen Unternehmen ist inzwischen sehr viel investiert und aufgebaut worden. Aber kleine und mittlere Unternehmen haben nach wie vor das Problem, dass es an geeigneten Angeboten für sie fehlt.

Was meinen Sie konkret?

Große Unternehmen können einen eigenen Apparat aufbauen, mit eigenen Sicherheitsexperten, eigens auf die Bedürfnisse der Firma zugeschnittenen Lösungen und Ausbildungsprogrammen für die Mitarbeiter. Kleinere Firmen, sagen wir bis 100 oder 500 Mitarbeiter, können sich das kaum leisten. Sie sind angewiesen auf fertig konfektionierte, leicht einsetzbare Lösungen und erschwingliche Beratung. In diesem Marktsegment ist deutlich mehr zu tun, auch für die angewandte Forschung.

Zumal der Mittelstand ja hierzulande besonders innovativ ist und damit das ideale Einfallstor für böse Buben...

Richtig, der Mittelstand ist ein besonders attraktives Ziel für Cyberspione. Aber es braucht eben, wie gesagt, entsprechende Werkzeuge für den Mittelstand, um dort einen wirkungsvolleren Schutz zu bieten.

DIGITALSTADT DARMSTADT

Zum Verbraucher: Jeder Zweite macht kein Online-Banking, weil er Bedenken hat. Die Schadsoftware WannaCry haben viele am Bahnsteig miterlebt. Wie groß sind die Gefahren für wirklich kritische Infrastrukturen wie Kommunikations- oder Stromnetze?

Für die Betreiber kritischer Infrastrukturen gilt dasselbe wie für alle Unternehmen: Mit hinreichend großem Aufwand kann ein Angreifer überall einbrechen, und er wird dies tun, wenn es sich für ihn lohnt und das Risiko, dabei gefasst zu werden, gering ist. Das ist nicht anders als bei Hauseinbrüchen. Umgekehrt bedeutet dies, je kritischer eine Infrastruktur und je höher das Risiko, desto mehr Aufwand sollte man betreiben, Angreifer abzuwehren. Gegen viele Angreifer kann man sich wehren. WannaCry ist ein gutes Beispiel: Dieser Angriff nutzte Schwachstellen aus, die bereits bekannt und vom Hersteller geschlossen waren. Erfolgreich war der Angriff nur, weil eben viele Systeme nicht auf dem aktuellen Stand waren und den Angriff nicht schnell genug entdecken konnten. Wenn man die heutigen Standard-Sicherungsmaßnahmen umsetzt, könnte man die Großzahl der Angriffe abwehren.

Noch mal zurück zu den Infrastrukturen. Ist dort das Thema Sicherheit angekommen?

Bei den kritischen, großen Infrastrukturen ist das ganz bestimmt der Fall. Dort sorgt auch das IT-Sicherheitsgesetz für Mindeststandards, und die Betreiber sind üblicherweise auch gut in der Lage, diese umzusetzen. Die kleineren und mittleren Infrastrukturbetreiber, etwa kommunale Wasserwerke, haben aber dasselbe Problem wie alle kleineren und mittleren Unternehmen. Das Bewusstsein ist auch dort vorhanden, aber es fehlt an leicht und ohne viel Personalaufwand einsetzbaren Lösungen.

Gleichwohl dominiert der Eindruck, dass man aktuell mehr reaktiv unterwegs ist als proaktiv – was täuscht?

Das täuscht. In der Öffentlichkeit ist der reaktive Teil einfach sehr viel sichtbarer, weil eher über Angriffe und die Reaktion darauf berichtet wird als über proaktive Maßnahmen. Tatsächlich ist beides wichtig, und in beiden Bereichen passiert auch sehr viel in der Anwendung und in der Forschung, natürlich auch hier in Darmstadt. Wir haben Projekte, in denen wir weltweit Angriffe auf die Internet-Infrastruktur erkennen können. Wir können sogar statistische Aussagen dazu machen, wie groß die Verwundbarkeit gegen bestimmte Arten von Angriffen ist, und daraus leiten wir dann wiederum Verbesserungsvorschläge ab. Das ist ein eher reaktiver, empirischer Ansatz.

Und was passiert proaktiv?

Auf der proaktiven Seite verfolgen wir den Ansatz von „Security by Design". Wir entwerfen Systeme so, dass schon in der Konzeptionsphase an die IT-Sicherheit und mögliche Schwachstellen gedacht wird. Schwachstellen sind ja schlicht Fehler, die von Menschen gemacht werden. Und die kann man versuchen zu vermeiden. Es lässt sich da sehr viel erreichen zum Beispiel durch spezielle Sicherheitswerkzeuge für Entwickler.

Das Interview führte Achim Preu.

ZUR PERSON

- **Michael Waidner** ist Institutsleiter des Fraunhofer SIT, des führenden Instituts für angewandte Cybersicherheitsforschung in Deutschland.
- Zudem ist er Professor für Sicherheit in der Informationstechnologie an der Technischen Universität Darmstadt und seit 2017 **Chief Digital Officer der Wissenschaftsstadt Darmstadt**.
- Michael Waidner ist der Erfinder von **mehr als 20 Patenten** und Autor von mehr als 190 Papieren. (red)

Das Fraunhofer SIT in der Darmstädter Rheinstraße entwickelt Lösungen für IT-Sicherhheit. Foto: Andreas Kelm

TIPPS FÜR PRIVATE INTERNETNNUTZER

- Das Internet bestimmt vielerorts unseren Alltag – auch im Privatleben. **Professor Dr. Michael Waidner vom Fraunhofer-Institut** in Darmstadt fasst die wichtigsten Tipps für private Internetnutzer noch mal zusammen:
- **Risiken im Privatbereich minimieren** – „Man sollte Vorsorge treffen, also Back-ups seiner Daten haben, seine Systeme aktuell halten und die Angebote der Hersteller für automatische Updates wahrnehmen. Zudem sollte man Antiviren-Software installieren und aktuell halten sowie Passwörter hin und wieder ändern und für verschiedene Dienste auch verschiedene Passwörter verwenden. Im digitalen Leben gilt ebenso wie im analogen: Bevor man etwas tut, sollte man sich der Risiken bewusst sein. Zum Beispiel sollte man seine persönlichen Daten nicht unüberlegt hergeben, und man sollte Software und Apps aus dubiosen Quellen nicht einfach so installieren. Es gibt zu diesem Thema auch sehr gute Empfehlungen, etwa auf **www.bsi-fuer-buerger.de."**
- **Und bei E-Mails** – „E-Mails an sich bieten keinerlei Sicherheit. Es ist recht einfach, den Absender einer E-Mail zu fälschen, und wer eine E-Mail schreibt und einfach so abschickt, muss wissen, dass diese E-Mail auf ihrem Weg durch das Internet viele Server durchläuft – auf all diesen Servern kann man die E-Mail mitlesen. Die Lösung dieses Problems ist seit Jahrzehnten bekannt und heißt Ende-zu-Ende-Verschlüsselung, hat sich aber in der Praxis noch nicht durchgesetzt. Umfragen zeigen, dass höchstens 15 Prozent der Internetnutzer ihre E-Mails schützen, und das obwohl eigentlich alle E-Mail-Programme Ende-zu-Ende-Verschlüsselung unterstützen. Dass Verschlüsselung kaum eingesetzt wird, liegt zum größten Teil an der schlechten Benutzbarkeit. Aus diesem Grund haben wir am Fraunhofer SIT die „Volksverschlüsselung" gestartet, die für eine sehr benutzerfreundliche Ende-zu-Ende-Verschlüsselung in der E-Mail-Kommunikation sorgt. Die Software kann auf **www.volksverschluesselung.de** kostenlos runtergeladen werden." (red)