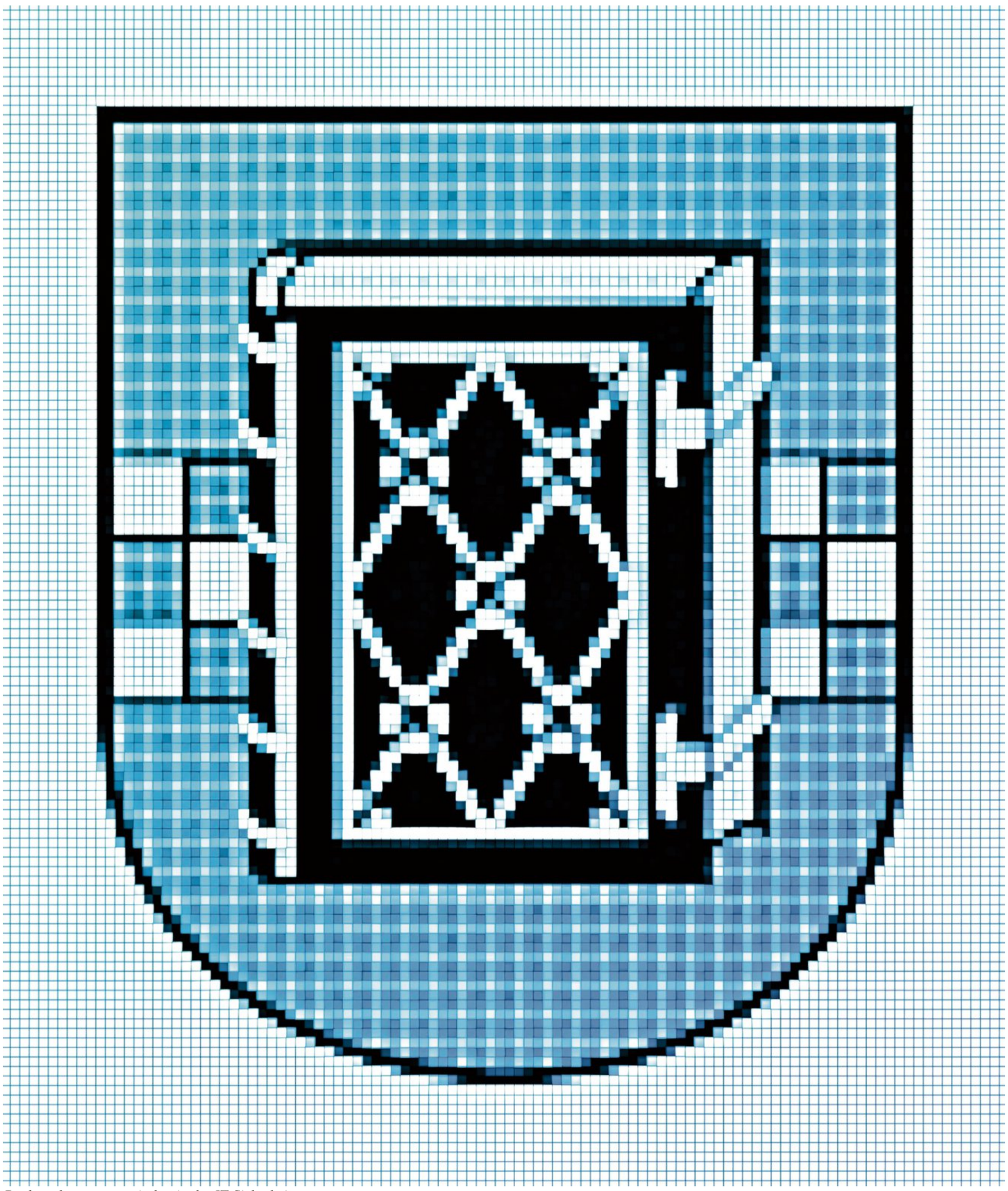

Bochum boomt – zumindest in der IT-Sicherheit. Illustration F.A.Z.

Die Cyberwächter aus dem Pott

In Bochum gibt es mehr als 1000 Studierende für IT-Sicherheit, sie gründen zahlreiche Start-ups. Ihre Vorbilder sind die eigenen Professoren.

Von Jonas Jansen

Autos müssen nicht erst autonom fahren, sie sind längst rollende Computer. Sie haben Schnittstellen durch ihre Navigationsgeräte und Fahrassistenzsysteme, selbst die Funkverbindung zum Autoschlüssel könnte für Hacker ein Einfallstor sein. Kein Wunder, dass sich Hersteller und Autozulieferer seit Jahren in der Architektur von Fahrzeugen auch mit der IT-Sicherheit beschäftigen. Als der weltgrößte Automobilzulieferer Bosch das Bochumer Unternehmen Escypt vor neun Jahren übernahm, waren dort rund 30 Leute beschäftigt. Heute arbeiten mehr als 400 Fachleute an Sicherprodukten sowohl im Auto als auch in der Cloud. Sie verkaufen auch sogenannte Managed Services, also Dienstleistungen für IT-Sicherheit. An 17 Standorten haben sich die IT-Sicherheitsfachleute inzwischen angesiedelt, meist in der Nachbarschaft der Kunden aus der Automobilindustrie wie etwa in München oder Stuttgart. Gleichwohl ist der Gründungsstandort in Bochum für Escrypt ein ganz wichtiger – denn dort gibt es ein echtes Ökosystem für IT-Sicherheit.

„Wir beobachten die Forschung der Universität und transferieren sie in wichtige Informationen für unsere Kunden“, sagt Thomas Wollinger, einer von zwei Geschäftsführern von Escrypt. „Wir beantworten damit etwa die Frage, was es für die Plattform bedeutet, die in den nächsten 20 Jahren im Auto läuft.“ Wollinger hat selbst an der Ruhr-Universität Bochum promoviert, als dritter Mitarbeiter war er praktisch von Beginn an dabei, als das Unternehmen im Jahr 2004 ins Handelsregister eingetragen wurde. Aus der Universität heraus hatte sich das Start-up entwickelt für Anfragen aus der Industrie nach sogenannter „Embedded Security“, also allen vernetzen Geräten ohne Tastatur und Bildschirm. Noch heute ist Esrcypt auch in Forschungsprojekten an der Ruhr-Universität beteiligt, wo direkt für das Unternehmen wichtige Fragestellungen behandelt werden. Der dritte, nicht zu verachtende Punkt für die Standortwahl ist das Recruiting neuer Fachkräfte: Durch die große Zahl der Absolventen kommen nicht nur aus der IT-Sicherheit, sondern auch der Informatik und den Ingenieurwissenschaften mögliche Mitarbeiter zu Escrypt.

Die Probleme, um die sie sich kümmern, werden immer drängender. Neun von zehn Unternehmen waren im vergangenen und in diesem Jahr von Hackerangriffen betroffen. Die Schadenssumme für die deutsche Wirtschaft ist nach Angaben des Digitalverbands Bitkom mit 223 Milliarden Euro heute doppelt so hoch wie noch vor zwei Jahren. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bezeichnet die Bedrohungslage im Land als „sehr angespannt“. Ziemlich genau ein Jahr ist es her, dass Unbekannte mit Ransomware die Universitätsklinik in Düsseldorf lahmlegten, die Drahtzieher sind immer noch nicht gefasst. Der Hackerangriff auf den Landkreis Anhalt-Bitterfeld in diesem Juli war der erste Cyberkatastrophenfall in der Geschichte der Bundesrepublik. Im Ausland sieht es nicht viel besser aus, bevorzugt wird die kritische Infrastruktur attackiert: In Amerika wurde vor einigen Monaten eine Pipeline angegriffen. Als das Unternehmen Solarwinds gehackt wurde, waren in der Folge Tausende Unternehmen betroffen, außerdem mehr als ein Dutzend amerikanische Behörden, wie das Heimatschutzministerium, die amerikanische Telekommunikationsaufsicht NTIA oder die Nationale Verwaltung für Nukleare Sicherheit (NNSA).

Das größte Problem ist: Alles hängt mit allem zusammen. Es gibt Tausende verschiedene Motivationen, warum Staaten, Kommunen, Unternehmen oder Privatpersonen attackiert werden von Hackern. Manche Angriffe sind hoch spezialisiert, andere versuchen, einen möglichst großflächigen Schaden anzurichten. Wieder andere sind nur Tarn-Missionen, um davon abzulenken, dass im Hintergrund an einem viel schwerwiegenderen Angriff gearbeitet wird. Gemein haben sie, dass eine ausgenutzte Sicherheitslücke sehr weitreichende Folgen haben kann: Wenn persönliche Informationen etwa von Hotelketten abfließen, wie das einst der Marriot-Gruppe passierte, sind auf einen Schlag eine halbe Milliarde Daten im Umlauf. Damit können Kriminelle etwa halb automatisiert Konten für Cloud-Dienste anlegen und dann mit sogenannten DDoS-Attacken versuchen, Netzwerke mit Anfragen zu überfluten und somit lahmzulegen. Wenn mit solchen Konten Botnetze gebaut werden, verschleiern die Täter ihre Spuren und suchen sich mit Daten von früheren Opfern neue.

Mitunter wirkt die Gefahr durch Cybercrime abstrakt, weil jede Sekunde rund um die Welt Behörden und Unternehmen angegriffen werden. Viele dieser Millionen Attacken am Tag sind zwar potentiell gefährlich, werden aber durch moderne Sicherheitstechnik abgefangen. Bedrohlicher sind Angriffe durch Geheimdienste oder von durch Regierungen finanzierte Hacker-Söldner, die versuchen, Regierungsgeheimnisse zu stehlen oder Industriespionage zu betreiben. Oder, um es wie Thomas Wollinger kurz zu sagen: „Das war eine weitsichtige Kaufentscheidung von Bosch, weil Security in allen Feldern des Unternehmens viel wichtiger wird, ob es das Auto, die Wasch- oder die Bohrmaschine ist.“

Derzeit arbeiten gut 140 Menschen in Bochum für Escrypt, auf dem ehemaligen Produktionsgelände des Autounternehmens Opel wird aber gerade ein großes Bürogebäude für das Unternehmen errichtet, damit in Zukunft mehrere Hundert Sicherheitsfachleute dort angesiedelt werden. Das alte Industriegelände, das heute als Mark 51°7 bekannt ist, ist ein Beispiel für den gelungenen Strukturwandel im Ruhrgebiet, verknüpft es dort doch die Wissenschaft mit der Wirtschaft. Zahlreiche Forschungsinstitute haben sich auf den 70 Hektar mit Unternehmen und Start-ups vernetzt.

Solche engen Verbindungen fallen jedoch nicht vom Himmel, sondern sind das Ergebnis jahrzehntelangen Austauschs und Aufbauarbeit der Lehre – und einer gehörigen Portion Unternehmertum. Bochum ist heute einer der wichtigsten Standorte für IT-Sicherheit in Deutschland. Schon Mitte der Achtziger- jahre sind dort Unternehmen wie G Data entstanden, das noch heute zu den bekanntesten Dienstleistern für IT-Sicherheit zählt. Im Jahr 2000 wurde in Bochum der bundesweit erste Studiengang „Sicherheit in der Informationstechnik“ aufgelegt mit zunächst 30 Studenten. Zwei Jahre später wurde dort das Horst-Görtz-Institut (HGI) gegründet, die Entwicklung dieses Forschungszentrums ist vielleicht der wichtigste Baustein dafür, warum Bochum heute so gut aufgestellt ist in der IT-Sicherheit.

Der Unternehmer Horst Görtz hat selbst Datensicherheitsprodukte wie etwa eine Festplattenverschlüsselung entwickelt und Mitte der Neunzigerjahre durch einen Börsengang eines seiner Unternehmen recht viel Geld eingenommen. Daher war er zum Jahrtausendwechsel auf der Suche nach einer Universität, die mit seiner Unterstützung ein Forschungs- und Ausbildungszentrum aufbauen konnte. Wegen der Gründungsspende trägt das Institut seinen Namen – von Anfang an gab es die Auflage, dass es auf drei Säulen fußt: Spitzenforschung, Ausbildung und Vernetzung mit der Wirtschaft. „Das war eine super Sache“, erinnert sich Christof Paar. Er ist einer der ersten Professoren dort gewesen, von früheren Studenten wird er ehrfürchtig als „Superstar der Krypto“ bezeichnet. 26 Professorinnen und Professoren arbeiten im Umfeld des HGI, in Arbeitsgruppen der Elektro- und Informationstechnik, Mathematik und Informatik sowie den Geisteswissenschaften – immer mit Bezug zur IT-Sicherheit. Inzwischen gibt es ungefähr 1000 Studierende in der IT-Sicherheit in Bochum, jedes Jahr kommen gut 200 Erstsemester in dem Bereich im Bachelor und Master dazu. Die Universität zählt in dem Bereich mehr als 150 Abschlüsse im Jahr, das sind mit Abstand die meisten Studienabgänger rund um IT-Security in Europa. „Das ist ein Nährboden, um das Ökosystem zu erhalten und auszubauen“, sagt Paar.

Aus der Informationstechnologie kommen so viele Impulse, dass die Ruhr-Universität das erste Mal seit Bestehen der Fakultätsstruktur aus dem Jahr 1985 eine neue Fakultät gründet, zum 1. Oktober gibt es eine eigene für Informatik. Und die Bochumer Forscher fallen auch international auf: auf der „Conference on Cryptographic Hardware and Embedded Systems“ (CHES), die Mitte September digital stattfindet, wird es 78 Fachbeiträge geben zu kryptographischer Hardware und eingebetteten Systemen. An 18 davon waren Forscher aus der Bochumer IT-Sicherheit beteiligt, zehn davon wurden von einem einzigen Professor der Universität mitverfasst. In der Branche wird in Deutschland schon von einer „Bochumer Schule“ gesprochen, weil allein durch die vielen Studienabgänger überproportional viele Professuren an anderen Universitäten von Absolventen der Ruhr-Uni besetzt sind. Gern gesehen sind sie auch beim BSI, dem BKA oder in der Forensik.

Paar leitet heute das Max-Planck-Institut für Sicherheit und Privatsphäre (MPI-SP), das vor zwei Jahren in Bochum angesiedelt wurde, womit die Spitzenforschung abermals auf ein anderes Niveau gehoben wurde. „Das ist ein Ritterschlag“, sagt Paar nicht ohne Stolz, mit so einem Namen im Rücken werden Professoren und Doktoranden dann doch noch internationaler rekrutiert. In den vergangenen Jahren kamen schon einige Professoren aus Madrid, Paris oder Wien. Wenn das Max-Planck-Institut voll aufgebaut sein wird, rechnet der Professor mit etwa 150 bis 200 Doktoranden für IT-Sicherheit. Ein Vorteil im Wettbewerb um die Auszeichnung der Max-Planck-Gesellschaft dürfte die enge Zusammenarbeit über Hierarchien hinweg in Bochum gewesen sein. An der Uni komme es immer wieder vor, dass Bachelorstudenten mit Professoren ein Start-up gründen, sagt Paar. In den vergangenen zehn Jahren haben sich aus der Uni heraus um die 20 Start-ups gebildet. „Gerade in der Cybersicherheit sind Start-ups ein super Vehikel, um Wissenstransfer zu erzielen“, sagt Paar.

Der Professor muss es wissen, er hat das selbst vorgemacht als Mitgründer von Escrypt. Und sein Gründungskompagnon aus der Zeit hilft heute anderen Start-ups dabei, Fuß zu fassen. Als Willi Mannheims vor mehr als 20 Jahren einen Professor für Kryptographie in seinem Büro an der Universität von Worcester in der Nähe von Boston besuchen wollte, um mit ihm über Cybersecurity in den Vereinigten Staaten zu sprechen, dachte er, er hätte es mit einem Amerikaner zu tun. Doch hinter ihm hing ein Bild des Kölner Doms. Das war die erste Begegnung mit Paar, daraus sollte eine enge Beziehung entstehen – und einige Jahre später eben Escrypt. Mannheims kam eher aus der unternehmerischen Ecke, der studierte Luft- und Raumfahrttechniker war schon Anfang der Neunzigerjahre an einem Risikokapitalfonds beteiligt. Später hatte er das Sicherheitsunternehmen Secunet gegründet und an die Börse geführt und sich von dem Geld danach eingekauft in eine Datensicherheitsfirma namens Eracom, die kryptographische Boxen herstellte. „Datensicherheit ist also nicht nur etwas, wo man von kleinen Firmen von 5 bis 10 Leuten redet, die aus einem universitären Umfeld kommen“, sagt Mannheims. „Das ist ein richtiger Industriefaktor.“ Heute ist Mannheims Partner in dem Münsteraner Risikokapitalfonds Ecapital. Die Investoren haben sich auf Deep Tech fokussiert, wo Datensicherheit freilich eine wichtige Rolle spielt. „Wir sitzen hier in Nordrhein-Westfalen in einem der weltweit besten Zentren“, ist Mannheims überzeugt.

Davon überzeugt hat Ecapital auch andere Geldgeber, die Risikokapitalgeber haben einen eigenen Cybersecurityfonds im Volumen von 50 Millionen Euro aufgesetzt. „Die Investitionen in Datensicherheit sind hierzulande im Verhältnis zu Israel und Amerika trotzdem noch homöopathisch“, sagt Mannheims. Israel allein hat in den vergangenen Jahren mehr investiert in den Bereich als die ganze EU. „Wir müssen noch deutlich besser werden“, sagt Mannheims.

Im Befruchten des Start-up-Ökosystems helfen Ecapital freilich die schon lange geknüpften Kontakte. Bekannte wie Paar oder der heutige Direktor des Horst-Görtz-Instituts sind Sicherheitspartner für Ecapital und bewerten die Investitionen in Jungunternehmen aus dem Blickfeld der Forschung. Davon erhoffen sich die Investoren eine Einschätzung zur globalen Marktreife für neue Cybersecurity-Ideen. So kam es, dass drei britische Investmentfonds, darunter Seraphim Capital, vor einigen Jahren auch bei Ecapital vorbeikamen, als es um eine weitere Finanzierungsrunde für ihr Start-up Ultrasoc ging. „Geld haben viele, aber wir haben einen Mehrwert für die Unternehmen, der sich in Geld nicht auszahlen lässt“, sagt Mannheims. Gekauft wurde Ultrasoc dann im vergangenen Jahr von Siemens, die Schnittstellen oder kritische Bereiche auf Computerchips werden nun für den Münchener Dax-Konzern auf ihre korrekte Funktion hin überwacht.

In drei der Start-ups aus dem Ecapital-Portfolio sitzt Hans-Christoph Quelle im Beirat. Quelle war Gründer und Chef des Düsseldorfer Unternehmens Secusmart, das alle Bundesbehörden mit Krypto-Handys beliefert hat und deshalb für das „Kanzler-Handy“ bekannt war. Das Unternehmen wurde im Jahr 2014 von Blackberry gekauft, heute ist Quelle in einige kleine Firmen privat investiert und berät zudem Regierungen, die Sicherheitslösungen bauen wollen. Als Beirat für Start-ups sieht er seine Rolle reflektiert, schließlich hat er sich selbst in seiner Zeit als Gründer immer darüber geärgert, wenn er sich rund um die Uhr den Kopf über sein Unternehmen zerbrach – und dann ein Beirat kam, der eine andere Idee hatte. „Aber es ist hilfreich, wenn man mit jemandem sprechen kann, der die Fehler alle schon mal gemacht hat“, sagt Quelle. Mit IoT Inspektor berät er gerade ein hessisches Unternehmen, das Software von Tausenden Schnittstellen analysiert, in Flughafen-Kameras, Kühlschränken oder der Kaffeemaschine. Produkten eben, die – einmal verkauft – viel zu selten geupdatet werden.

Ecapital hat freilich auch Bochumer Universitätsausgründungen im Portfolio, Vmray ist eines davon. 25 Millionen Euro hat das Unternehmen in seinen Finanzierungsrunden eingesammelt – unter anderem vom High-Tech-Gründerfonds. Die beiden Gründer Carsten Willems und Ralf Hund haben eine Technologie gegen sehr komplexe und gezielte Angriffe entwickelt, die auch unbekannte Malware erkennt und analysieren kann. Weil das so gut funktioniert, hat das Unternehmen Banken, Regierungen, Geheimdienste und Flugzeughersteller als Kunden. Willems und Hund konnten das System deshalb bauen, weil sie in ihrer Forschung diese IT-Sicherheitsnische selbst mitgestalteten. Noch heute ist das System einzigartig, mehrere Kaufversuche haben die Gründer abblitzen lassen. Es geht ihnen auch darum, Wissen nicht einfach an ein amerikanisches Tech-Unternehmen abzugeben, sondern es in der Region weiter zu entwickeln, in der sie selbst so lange forschten. So kommt es, dass Vmray inzwischen mehr als 100 Mitarbeiter hat – und Talente und Mitarbeiter nach Bochum lockt.

Dass man mit seiner Gründung aber irgendwann auch mal an Wände stoßen kann, hat Thomas Wollinger vor gut zehn Jahren mit Escrypt erfahren. Als Vertreter eines kleinen Unternehmens, das bei den großen mit seinen IT-Sicherheitslösungen anklopft, hat er häufig die Antwort zu hören bekommen: Super Technologie und Fachleute, aber woher können wir sicher sein, dass ihr morgen noch da seid? „Vor allem die Erweiterung der Mannschaft und des Portfolios ist in einem bestimmten Stadium schwierig aus eigener Kraft zu stemmen“, sagt er. Da kam die Anfrage von Bosch, eine von drei Angeboten zu der Zeit, gerade recht. Die einen bekamen Zugang zur Technologie, die anderen zum Netzwerk und der Professionalität eines Konzerns. Zusätzlich war Bosch mit seinen eigenen Anforderungen für Escrypt schon Großkunde. „Das war eine Symbiose“, erinnert sich Wollinger. Neben seinem Hauptjob für den Autozulieferer hat er inzwischen übrigens noch einmal gegründet – und zwar einen Inkubator für IT-Sicherheit namens Cube5. Der berät Studenten aus der IT-Sicherheit, die gründen wollen – und sitzt, natürlich, in Bochum.