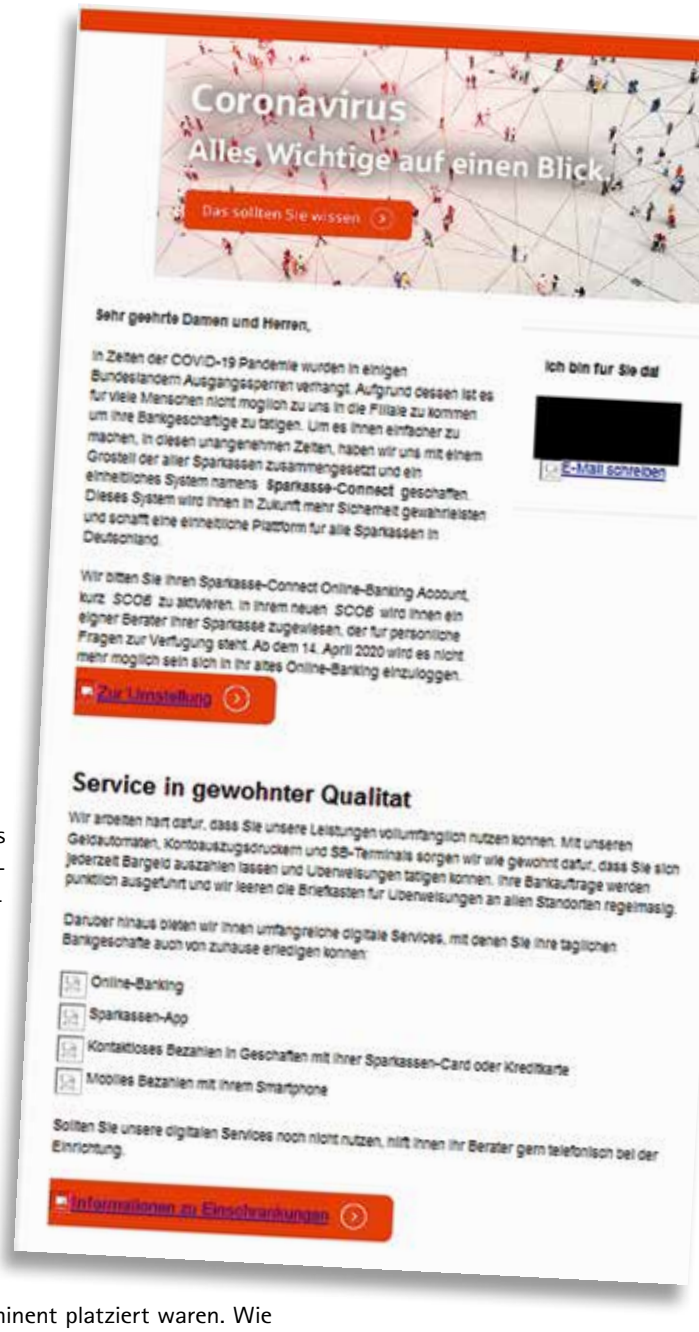
IT-Sicherheit

Virtuelle Bedrohungen – ganz real!

Mitte März wies das Bonner Bundesamt für Sicherheit in der Informationstechnik (BSI) darauf hin, dass mit der Corona-Pandemie Auswirkungen auf die IT-Sicherheit zu erwarten seien. Nur wenige Tage später wurde bekannt, dass in NRW mit gefälschten Formularen zur Beantragung von Corona-Soforthilfen Daten abgefischt wurden. Inzwischen sind viele weitere Betrugsversuche bekannt geworden. Das Thema Cybersicherheit ist also aktueller denn je, wie unsere Titelgeschichte zeigt. Dank des neuen „Cyber Security Clusters Bonn" ist die Region in Sachen IT-Sicherheit bestens aufgestellt. Zudem reifen hier die Cyberexperten von morgen heran.

Cyber Security



Wer gehofft hatte, dass mit der Corona-Pandemie andere Probleme – zum Beispiel Cyberkriminalität – in den Hintergrund treten würden, musste sich schon bald eines Besseren belehren lassen.

Ein aktuelles Beispiel – und leider eines von vielen: Die Verbraucherzentrale NRW warnte im März vor einer aktuellen Betrugsmasche. „Dass Geschäfte durch die Corona-Krise schließen, nutzen Betrüger für neue Phishing-E-Mails", heißt es auf der Website der Verbraucherzentrale (siehe dazu auch Infokasten Seite 10). „Sie behaupten zum Beispiel, dass Banken und Sparkassen nur per Telefon oder E-Mail weiterhelfen könnten, wenn Kunden ihre Daten abglichen. Doch Vorsicht: Die würden direkt an die Betrüger gehen!"

Am Beispiel eines gefälschten Sparkassenanschreibens zeigen die Verbraucherzentrale und auch das Bonner Bundesamt für Sicherheit in der Informationstechnik (BSI) auf ihren Websites die Masche der Betrüger: „Ihre Sicherheit und Gesundheit und auch die unserer Mitarbeiter liegt uns sehr am Herzen", heißt es in der Mail mit Sparkassenlogo. Und weiter: „Vor diesem Hintergrund haben wir uns dafür entschieden, unsere kleineren Filialen bis auf weiteres zu schließen." Sodann folgt der Hinweis, man stehe natürlich weiterhin telefonisch, per Mail und per Onlinebanking persönlich zur Verfügung. So weit, so realistisch.

Nun jedoch sollte sich die Empfänger der Mail zwei Minuten Zeit nehmen, um ihre Adresse, Telefonnummer und Mailadresse zu überprüfen und unter Umständen zu aktualisieren. „Über einen Link werden Betroffene auf eine authentisch aussehende Eingabemaske geleitet, die die Daten nach der Eingabe direkt an Betrüger sendet", warnt das BSI.

Wer nun denkt, solche Betrugsmaschen richten sich vor allem an Endverbraucher, irrt. Dies zeigt ein Beispiel aus der Woche vor Ostern, das bundesweit Schlagzeilen machte: Am 9. April stoppte das Land NRW vorerst die Zahlung der Corona-Soforthilfe, auf die viele Betriebe dringend warteten. Der Grund: Hinweise auf Fake-Webseiten, die in Suchergebnissen prominent platziert waren. Wie das NRW-Wirtschaftsministerium mitteilte, hatten Betreiber mit gefälschten Antragsformularen Daten von Antrag stellenden Unternehmen abgefischt und diese mutmaßlich für kriminelle Machenschaften genutzt.

Möglichkeiten für Cyberkriminelle haben sich vervielfacht

Gefälschte Websites, Datenklau und Erpresser-Software: In der Coronakrise nimmt die Cyberkriminalität nach Erkenntnissen der europäischen Polizeibehörde Europol stark zu. „Angesichts einer Rekordzahl potenzieller Opfer in der Europäischen Union, die wegen der Pandemie zu Hause bleiben und dort Online-Dienste nutzen, haben sich Möglichkeiten für Cyberkriminelle vervielfacht, Schwachstellen und neue Gelegenheiten auszunutzen", mahnte Europol Anfang April.

In der Tat: Das BSI teilte zum gleichen Zeitpunkt mit, bereits eine Zunahme von Cyber-Angriffen mit

Hunderttausende ArbeitnehmerInnen arbeiteten während der Corona-Pandemie auf einmal im Homeoffice. Oft kam dabei eine Sicherheitsprüfung zu kurz.

Bezug zum Coronavirus auf Unternehmen und Bürger zu beobachten. Eine Variante ist die soeben geschilderte: Die Täter fordern per E-Mail Betriebe auf, persönliche oder unternehmensbezogene Daten auf gefälschten Webseiten preiszugeben. Die betrügerisch erlangten Daten werden anschließend für kriminelle Aktivitäten missbraucht.

Das Informationsbedürfnis vieler Bürgerinnen und Bürger würden Cyber-Kriminelle ebenfalls ausnutzen. Das BSI konnte etwa eine exponentielle Zunahme an Registrierungen von Domainnamen mit Schlagwörtern wie ‚corona' oder ‚covid' beobachten. Neben der Nutzung für legitime Informationsangebote würden viele dieser Domainnamen für kriminelle Aktivitäten missbraucht. Nutzer würden auf solchen Webseiten zu Download und anschließender Installation vermeintlicher Software-Updates aufgefordert. Tatsächlich jedoch würden die Systeme der Nutzer dadurch mit Schadprogrammen infiziert. Auch würden Spam-Mails mit vermeintlichen Informationen in Bezug auf Corona im Dateianhang zur Verbreitung von Schadprogrammen versendet. „Nach einer erfolgreichen Infektion mit diesen Schadprogrammen", warnte das BSI Anfang April, „können die Angreifer unter anderem Betrug beim Online-Banking der Nutzer durchführen oder Zugriff auf Unternehmensnetzwerke erlangen, um sensible Informationen auszuspähen oder Daten zu verschlüsseln und dann die Opfer anschließend zu erpressen."

Einfallstor für Cyberkriminalität: das Homeoffice

Ein besonderes Problem in diesen Zeiten: Hunderttausende Arbeitnehmerinnen und Arbeitnehmer gehen ihrer Tätigkeit ganz oder phasenweise aus dem Homeoffice nach (siehe auch Bericht Seite 17). Viele Firmen waren technisch und organisatorisch einigermaßen vorbereitet, weil sie auch vor der Krise schon Homeoffice anboten. Viele andere traf die Entwicklung mehr oder weniger unvorbereitet.

Checkliste zum Schutz vor Phishing-Fallen

- Achten Sie auf Absender, Anrede und Betreff. Häufig können lange Absenderadressen oder allgemeine Anreden ein Indiz sein.
- Banken und andere Unternehmen fordern niemals per E-Mail dazu auf, persönliche Angaben zu machen. Sollten Sie in einer E-Mail darum gebeten werden, klicken Sie keinesfalls Links an. Wenn Sie unsicher sind, rufen Sie Ihre Bank oder das Unternehmen an.
- Fragen Sie sich, ob Sie die betreffende E-Mail erwartet haben. Sind Sie kein Kunde beim angeblichen Absender oder handelt es sich nicht um eine Ihnen bekannte Person, sollten Sie skeptisch werden.
- Gewinne werden nicht per E-Mail ausgeschüttet. Sollten Sie eine Gewinnbenachrichtigung erhalten, die verlangt, dass Sie einen Link anklicken oder Nutzerdaten angeben, handelt es sich wahrscheinlich um einen Betrugsversuch.
- Falls Sie Zweifel an der Echtheit eines Absenders haben, recherchieren Sie über eine weitere Quelle, beispielsweise eine Suchmaschine, eine Telefonnummer, bei der Sie nach der Echtheit der Nachricht fragen können. Nutzen Sie dazu nie die Kontaktdaten, die in der E-Mail enthalten sind.
- Auch Erpressungsversuche per E-Mail sind eine Straftat und sollten zur Anzeige gebracht werden.

Quelle: www.bsi-fuer-buerger.de

*Ein Blick ins BSI-Lagezentrum. „Cyber-Angriffe können jeden treffen", so **Arne Schönbohm**, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in Bonn.*

„Häufig mussten Heimarbeitsplätze innerhalb weniger Tage ans Firmennetz angebunden werden, oft kam dabei eine Sicherheitsprüfung zu kurz", berichtet Heiko Oberlies, IT-Experte der IHK Bonn/Rhein-Sieg, „Tatsache ist jedoch: Cloud-Anwendungen, Chats, Videokonferenzen und Filesharing mit Kolleginnen und Kollegen erleichtern die Zusammenarbeit während der Corona-Pandemie enorm – aber sind auch ein erstklassiges Einfallstor für Cyberkriminalität." Er mahnt deshalb zur Vorsicht – und verweist auf entsprechende Sicherheitstipps etwa der IHK oder des BSI (siehe www.ihk-bonn.de | Webcode @3532).

Cyberangriffe in Deutschland nehmen stetig zu

Damit kein falscher Eindruck entsteht: Zwar fördert die Corona-Pandemie die Cyberkriminalität. Ein massives Problem für die Wirtschaft war sie aber auch vorher schon, vor allem wegen der zunehmenden Digitalisierung.

Laut Bundeskriminalamt (BKA) stieg die Anzahl der Cyberangriffe in Deutschland auch im Jahr 2018 weiter an. Rund 87.000 Fälle von Cybercrime seien von der Polizei erfasst worden, ein Prozent mehr als im Jahr davor. In über 270.000 Straftaten sei 2018 das Internet als Tatmittel genutzt worden – ein Plus von rund fünf Prozent gegenüber 2017. Das zeigt das im November 2019 veröffentlichte „Lagebild Cybercrime" des BKA.

Der durch Cyberkriminalität 2018 verursachte Schaden: über 60 Millionen Euro. Diese Zahl bildet aber nur ab, was der Polizei bekannt geworden ist. Tatsächlich könnte sich der Schaden für Unternehmen auf über 100 Milliarden Euro belaufen, informierte das BKA mit Blick auf Schätzungen aus der Wirtschaft im Betrachtungszeitraum 2018/2019. Die enorme Differenz erkläre sich auch durch das hohe Dunkelfeld in diesem Bereich. „Insbesondere Unternehmen zeigen Fälle von Cybercrime und damit verbundene materielle Schäden nach wie vor vergleichsweise selten an", weiß das BKA. Die Furcht vor einem Vertrauensverlust bei Partnern und Kunden stehe dabei dem Interesse, die Tat strafrechtlich verfolgen zu lassen, entgegen.

Zum 1. April 2020 richtete das BKA die „Abteilung Cybercrime" ein, um Kompetenzen zur Bekämpfung dieses Phänomens zu bündeln und die erforderliche Spezialisierung seiner Mitarbeiterinnen und Mitarbeiter in diesem Bereich voranzutreiben. Sie soll im nächsten Jahr schrittweise auf rund 280 Personen anwachsen.

*„Die Abhängigkeit unserer Gesellschaft von einer funktionsfähigen technischen Infrastruktur nimmt stetig zu", sagte BKA-Präsident **Holger Münch** aus Anlass der Einrichtung der Abteilung. „Zugleich haben Straftäter es noch immer vergleichsweise einfach, sich im Netz kriminelle Kompetenz einzukaufen, um ohne umfängliche technische Kenntnisse etwa die Webpräsenzen ganzer Unternehmen zu blockieren oder die Informationstechnik in Krankenhäusern und Verwaltungen anzugreifen."*

*„Die Cyberattacken nehmen zu", konstatiert **Dirk Backofen** (r.), Leiter Telekom Security. 2020 rechnen die Experten mit 71 Millionen - pro Tag.*

Echtzeitüberwachung der Systeme – weil der Angreifer bereits im System ist

Auch das Landeskriminalamt NRW in Düsseldorf unterhält ein Cybercrime-Kompetenzzentrum. Außerdem hat das Polizeipräsidium Bonn einen eigenen Bereich Cybercrime. Ein großes Team sorgt dort dafür, das Bewusstsein für Cybercrime und Cybersicherheit zu schärfen. „Die Cybercrime-Prävention informiert alle Interessengruppen über Erscheinungsformen der Kriminalität, polizeiliche Bekämpfungsziele, Gefährdungseinschätzungen und Opferrisiken", erklärt Pascal Bergmeier vom Polizeipräsidium Bonn im Interview mit „Die Wirtschaft" (siehe Seite 15). Sowohl Bürgerinnen und Bürer als auch Unternehmen können sich an das Team von Bergmeier wenden, wenn sie Fragen zur Cybersicherheit und -kriminalität haben.

Ein weiterer wichtiger Bonner Akteur in Sachen Cybersicherheit ist die „Telekom Security", die ihre Firmenzentrale an der Reuterstraße hat und dort 320 Mitarbeiter beschäftigt. Für viele fast unsichtbar betreibt die Telekom dort ein integriertes „Cyber Defence and Security Operation Center" – eines von weltweit 17 Zentren in 13 Ländern. Das in Bonn ist das größte seiner Art in Europa. Insgesamt kommen so 1,2 Milliarden Anwender/innen weltweit in den Genuss von IT-Sicherheitsdienstleistungen.

Nach eigenen Angaben zählt jedes zweite Dax-Unternehmen zu den Kunden, aber auch viele größere Mittelständler und öffentliche Verwaltungen. Weltweit sorgen 1.600 Telekom-Security-Mitarbeiter für den Schutz digitaler Infrastrukturen, rund ein Drittel davon machen das für die Telekom selbst, die anderen sind für den externen Markt zuständig. Dabei kommen für die externen Kunden immer nur die professionellen Tools und das Expertenwissen zum Einsatz, mit denen sich die Telekom auch selbst schützt.

„Die Cyberattacken nehmen zu", konstatiert Dirk Backofen, Leiter Telekom Security. Um das zu messen, stellt T-Systems sozusagen Honigtöpfe auf, platziert also sogenannte „Honeypots", die Cyberangreifer anlocken sollen. 2018 zählte die Telekom zwölf Millionen Cyberangriffe täglich, 2019 waren es bereits 42 Millionen. 2020 rechnen die Experten mit 71 Millionen. Pro Tag wie gesagt.

Für den Schutz der digitalen Infrastrukturen des eigenen Konzerns und der vielen Kunden hat T-Systems den „Magenta Security Shield" entwickelt. Eine Plug-&-Play-Lösung, wie das Unternehmen verspricht, mit direkter Anbindung an das „Cyber Defence and Security Operation Center".

Backofen und seine Mannschaft verlassen sich längst nicht mehr auf gute Firewalls. Stattdessen nähern sie sich dem Phänomen Cyberkriminalität mit dem von Backofen so genannten „Zero Trust Approach". „Das heißt, wir trauen nichts und niemandem, sondern gehen grundsätzlich davon aus, dass der Angreifer bereits drinnen ist in den Systemen." Um ihm dort auf die Spur zu kommen, setzen die Expertinnen und Experten der Telekom auf – noch so ein IT-Fachwort – „Real Time Monitoring", also die Überwachung in Echtzeit.

Laufend wird nach Anomalien in den Netzwerkbewegungen und Datenströmen gesucht, Auffälligkeiten also, die bestimmte Muster erkennen lassen, die wiederum auf Angriffe schließen lassen. Auf diese kann dann rasch reagiert werden.

CYBER SECURITY CLUSTER BONN

Das „Cyber Security Cluster Bonn" wurde 2018 gegründet. Es bündelt alle in der Region Bonn/Rhein-Sieg ansässigen Security-Einrichtungen aus Wissenschaft, Forschung und Lehre, Wirtschaft, Behörden und öffentlichen Institutionen. Vorsitzender des Vorstandes ist ***Dirk Backofen*** *(l.), ebenfalls im Vorstand engagiert sich* ***Dr. Hubertus Hille*** *(M.), Hauptgeschäftsführer der IHK Bonn/Rhein-Sieg. Clustermanager ist* ***Christian Schmickler*** *(r.).*

Cyber-Knowhow: Nachwuchs aus Bonn für Bonn

Dafür ist enormes Fachwissen erforderlich. Da trifft es sich gut, dass „das Herz der Cybersicherheit in Europa" in Bonn schlägt. So steht es auf der Website des „Cyber Security Clusters Bonn" zu lesen. Dieses wurde im Oktober 2018 gegründet. Es bündelt alle in der Region Bonn/Rhein-Sieg ansässigen Security-Einrichtungen aus Wissenschaft, Forschung und Lehre, Wirtschaft, Behörden und öffentlichen Institutionen. Ziel der Initiative ist es, dazu beizutragen, die Region Bonn/Rhein-Sieg zu einem international beachteten Cyber-Security Standort auszubauen. Vorsitzender des Vorstandes ist Dirk Backofen, ebenfalls im Vorstand engagiert sich Dr. Hubertus Hille, Hauptgeschäftsführer der IHK Bonn/Rhein-Sieg.

„Das IT-Security-Potenzial in unserer Region ist enorm", findet Hille. „Wir haben hier zum Beispiel das BSI, das Kommando Cyber- und Informationsraum der Bundeswehr, die Telekom, die Universität Bonn, die Hochschule Bonn-Rhein-Sieg und das Fraunhofer Institut FKIE, aber auch Polizei NRW, Deutsche Post DHL Group und weitere Unternehmen. Mit dem Cyber Security Cluster Bonn wird deren Zusammenarbeit noch enger!"

Clustermanager Christian Schmickler findet, dass gerade diese Heterogenität der Mitglieder das Cluster zu einer wichtigen Austauschplattform für alle Beteiligte mache. „Die Bündelung der unterschiedlichen Kompetenzen erlaubt es uns", sagt Schmickler, „hochkarätige Konsortien zur Durchführung zukunftsweisender Projekte zu bilden oder auch interessante Events zur Sensibilisierung von Unternehmen und Gesellschaft für die Herausforderungen der Cybersicherheit zu veranstalten."

Einer der Schwerpunkte des Clusters sind der Transfer von Cybersecurity-Wissen in die Praxis und die Aus- und Weiterbildung von Spezialisten durch Kooperationen mit verschiedenen Instituten im Bereich Cybersecurity. „Es gibt einen enormen Bedarf an Expertinnen und Experten für Cybersicherheit", betont Heiko Oberlies von der IHK, „dem wir aber schon bald durch vielfältige Bildungsanstrengungen in der eigenen Region begegnen können."

T-Systems beispielsweise benötigt zahlreiche Fachleute für seine 17 „Cyber Defence and Security Operation Center". Deshalb bildet das Unternehmen seit 2014 jedes Jahr anfangs zehn, inzwischen fast 20 Nachwuchsprofis aus dem eigenen Haus zu „Cyber Security Professionals" weiter. Der firmeninterne Lehrgang schließt mit einer IHK-Prüfung ab.




Bilden IT-Spezialisten auf dem Gebiet Cybersicherheit aus: ***Prof. Dr. Elmar Padilla*** *und* ***Prof. Dr. Luigi Lo Iacono*** *an der Hochschule Bonn-Rhein-Sieg sowie* ***Prof. Dr. Michael Meier*** *und* ***Prof. Dr. Matthew Smith*** *(v.l.) an der Universität Bonn.*

Die Hochschulen Bonn-Rhein-Sieg (H-BRS) und Niederrhein (HSNR) starteten ein gemeinsames Pilotprojekt „Cybersecurity-Campus NRW". Ausgehend von einem steigenden Bedarf an IT-Spezialisten auf dem Gebiet der Cybersicherheit zum Schutz kritischer Infrastrukturen begann die HSNR im Herbst mit dem Studiengang „Cyber Security Management", die H-BRS weitet ihr vorhandenes Studienprogramm „Cyber Security" aus. Dazu schuf sie unter anderem die Professur „Cybersicherheit: Analyse und Bekämpfung von Malware". Besetzt wurde sie mit Prof. Dr. Elmar Padilla, Leiter der Abteilung „Cyber Analysis & Defense" am Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE in Wachtberg.

„Ich möchte den Studierenden tiefe technische Expertise vermitteln, wie sie notwendig ist, um die Herausforderungen im Bereich der Cybersicherheit im Zuge der fortschreitenden Digitalisierung erfolgreich meistern zu können", sagte Padilla bei der Übergabe der Ernennungsurkunde Anfang März. Studieninhalte werden unter anderem sichere digitale Transformation, sicheres E-Government, digitale Forensik und Cybercrime sein.

Neu an der Hochschule Bonn-Rhein-Sieg ist seit 1. April zudem Prof. Dr. Luigi Lo Iacono. Mit seiner Berufung erweitert der Fachbereich Informatik den bestehenden Schwerpunkt. Zuvor lehrte und forschte Lo Iacono rund zehn Jahre lang an der TH Köln an Technologien zur Gewährleistung der Sicherheit und Privatheit in verteilten Systemen.

Auch die Universität Bonn hat ihr Angebot erweitert. Vergangenen Herbst startete der neue Bachelor-Studiengang „Cyber Security" mit 60 Studierenden. Daran anschließen soll sich zudem ein Master-Studiengang. „Die Studieninhalte umfassen fundierte technische Informatik- und breite Cyber-Security-Kompetenzen, ergänzt um eine Nebenfachausbildung der Rechtswissenschaften und der Psychologie zur Vermittlung grundlegender Kompetenzen zur Gestaltung rechtskonformer und menschengerechter IT- und Cyber-Security-Systeme", heißt es auf der Website der Uni. Projektpartner sind unter anderem das BSI und das Fraunhofer FKIE.

Initiiert hat ihn Prof. Dr. Michael Meier, Inhaber des Lehrstuhls für IT-Sicherheit am Institut für Informatik der Universität Bonn und Leiter der Abteilung Cyber Security bei Fraunhofer FKIE. Seine Motivation für die Initiative: „Digitalisierung berührt nahezu alle Bereiche unseres Lebens, gleichzeitig ist es sehr schwierig, IT-Systeme und deren Nutzung sicher zu gestalten. Zudem fehlt es an Fachkräften zur Lösung offener Herausforderungen. Mit dem Studiengang wollen wir die erforderlichen Fachkräfte ausbilden, sowohl für die Praxis als auch für unsere Forschung."

Mit ins Leben gerufen hat den Studiengang Informatik-Professor Dr. Matthew Smith. Sein Ansatz: „Der Faktor Mensch ist sehr wichtig, wenn wir sichere Systeme entwickeln wollen. In dem ‚Cyber Security'-Studiengang wird deswegen nicht nur die technische Seite von IT-Sicherheit unterrichtet."

Der Faktor Mensch spielt in der Tat eine riesige Rolle. Jeder Experte, mit dem wir sprachen, legt Wert auf die Feststellung, dass das größte IT-Sicherheitsrisiko vor dem Computer sitzt. „Deshalb spielt ‚Security Awareness' in unserem Tun eine so wichtige Rolle", betont Dirk Backofen. Und Pascal Bergmeier vom Polizeipräsidium Bonn sagt: „Der Hauptfokus unserer Aufgabe liegt auf der Empfehlung zu tatreduzierenden Verhaltensweisen." Das BSI empfiehlt: „Ganz grundsätzlich vermeiden Sie großen Ärger, indem Sie unbekannte Dateien nicht öffnen, den Ursprung von E-Mails überprüfen und sowohl Absender als auch enthaltene Verlinkungen gründlich hinterfragen." Der Faktor Mensch eben.

Lothar Schmitz,
Wirtschaftsjournalist, Bonn

Ihr ITK-Spezialist in der IHK Bonn/Rhein-Sieg

Heiko Oberlies
Telefon 0228 2284 -138,
E-Mail: oberlies@bonn.ihk.de