Quelle: Polizei Bayern

Isabelle Reiff und Michael Praschma

ERMITTLERINNEN IM CYBERSPACE

Cyberkriminalität ist weiter auf dem Vormarsch. Bei der Polizei, vor Gericht und in der freien Wirtschaft werden deshalb hochspezialisierte Experten gesucht, die den Online-Gangstern Einhalt gebieten. Das berufliche Spektrum reicht vom gewieften Webpolizisten bis zum Entwickler von Forensik-Software.

Was fällt an dieser Einleitung auf? – Ganz selbstverständlich heißt es: der (!) Experte, Polizist, Entwickler. Das bildet die Realität aber immer weniger ab. Nicht nur allgemein im digitalen Bereich, sondern auch in der Exekutive und und im IT-Developing drängen zunehmend Frauen auf Stellen mit hochqualifizierten Tätigkeiten. Denn das Arbeitsfeld ist hochgradig interessant und die Herausforderungen reizen selbstverständlich nicht nur Männer. Das ist durchaus noch neu, denn gerade die IT-Branche kämpft mit einem Männerlastigkeitsproblem. Exemplarisches Schlaglicht auf das Silicon Valley: 23 % Frauen auf technischen Stellen bei Apple; nicht abreißende Sexismusvorwürfe bei Unternehmen wie Uber und Tesla, über die erst kürzlich *futurezone* berichtete.

Zurück zu Cyberattacken – sie kosten die deutsche Wirtschaft im Jahr an die 50 Mrd. Euro, so eine grobe Schätzung des Verfassungsschutzes. Zur Anzeige gebracht werden allerdings nur die wenigsten. Beim Bund Deutscher Kriminalbeamter geht man davon aus, dass rund 90 % der Fälle von Cyberkriminalität überhaupt nicht gemeldet werden. Das hat auch damit zu tun, dass schätzungsweise 66 % aller Angriffe unbemerkt bleiben, erst sehr viel später ans Licht kommen oder gar nicht in vollem Ausmaß erkannt werden. Gerade in Kleinunternehmen und bei Mittelständlern gibt es oft niemanden, der in der Lage wäre, den Zugang zurückzuverfolgen, über den eine Person das Unternehmen um Geld oder Daten erleichtert hat. Sicherheitslücken werden dann des Öfteren einfach gar nicht geschlossen. Das ist fatal, denn meistens bleibt es nicht bei einer Attacke. Entsprechend werden auch viel zu wenig solcher Fälle aufgeklärt, geschweige denn die Hintermänner identifiziert.

Doch ab Mai 2018 gilt EU-weit die neue Datenschutz-Grundverordnung (DSGVO). Dann besteht nicht nur detaillierte Meldepflicht für jeden IT-Sicherheitsvorfall. Die Datenverarbeitung im Unternehmen muss spätestens zu diesem Zeitpunkt auch entsprechend abgesichert sein. Optimal ist hierfür ein Informationssicherheitsmanagementsystem (ISMS), das nach dem Standard ISO/IEC 27001 oder nach dem BSI-Grundschutz zertifiziert ist. Die neuen Vorschriften zwingen nämlich zum Umdenken in der Risikobetrachtung: Nicht mehr der Schaden für das Unternehmen steht im Mittelpunkt, sondern die Rechte und Freiheiten aller Betroffenen – also auch die der Kunden und Geschäftspartner.

IT-Sicherheitsexperten dauerhaft gesucht

Der Bedarf an Experten und Expertinnen für IT-Sicherheit wird damit weiter wachsen. Nicht nur weil Angriffszahlen und -arten zunehmen, sondern auch weil im privaten und beruflichen Bereich immer mehr digitale Geräte im Einsatz sind: Früher besaß jeder Haushalt gerade mal einen PC. Heute sind mindestens drei, vier Smartphones und Spielekonsolen, aber auch Sprachassistenten, intelligente Stromzähler, Kfz-Steuerungssysteme usw. dazugekommen. Mit der Digitalisierung zu Hause – Stichwort: Smart Home – und erst recht mit dem Internet of Things werden mehr und mehr Dinge von außen angreifbar. Besonders brisant wird die Sache, wenn es dabei um Server und Großrechner geht, die kritische Infrastrukturen etwa in Krankenhäusern oder bei Notdiensten steuern. Angriffe können hier tausende von Menschen in Lebensgefahr bringen.

Das in Bonn angesiedelte Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt hohe Anforderungen an sogenannte Penetrationstester, die solche Netze auf Sicherheitslücken testen und zu diesem Zweck gutartige Angriffe auf Webapplikationen und IT-Systeme durchführen: Ohne einschlägiges Hochschulstudium, Programmier- und gesonderte Detailkenntnisse braucht sich weder Mann noch Frau hier zu bewerben. Ähnlich hoch sind die Erwartungen, die das BSI an Incident-Response-Analysten im neu geschaffenen Mobile Inci-

Willst du mit uns entwickeln?

[X] Ja [ ] Nein [ ] Vielleicht

careers.rohde-schwarz.com

ROHDE&SCHWARZ

dent Response Team (MIRT) richtet. Kernaufgabe ist es hier, akute Angriffe schnell zu analysieren und einzudämmen – Schwerpunkt IT-Forensik also.

Doch auch bei klassischen Verbrechen kommen zunehmend digitale Beweismittel ins Spiel: Überwachungskameras filmen möglicherweise Verdächtige, Handys speichern Bewegungsdaten, Fotokopierer prägen Papier mit einer unsichtbaren Kennung. Selbst ein vernetzter Wasserzähler kann ein hilfreicher Zeuge sein: In Arkansas lieferte solch ein Gerät jüngst der Polizei Hinweise darauf, dass ein Mörder seine Spuren buchstäblich weggewischt hatte. Nach anfänglichem Widerstand gab Amazon auch die Sprachaufzeichnungen heraus, die Echo, der vernetzte Lautsprecher, am Tag des Verbrechens gespeichert hatte.

IT-Forensik-Zertifikate

IT-Forensiker und -Forensikerinnen müssen alle möglichen Beweise auf Datenerfassungsgeräten so verarbeiten und sichern, dass sie bei einer Anhörung vor Gericht verwertbar sind. Das setzt eine strukturierte Untersuchung voraus, aus der sich eine klar dokumentierte Beweiskette ergibt. Gerichte legen großen Wert darauf, dass solche Gutachter zertifiziert sind. Zum Beispiel in Form einer Ausbildung zum Certified Cyber Forensics Professional (CCFP). Seit drei Jahren ist dieses aus den USA stammende, am weitesten verbreitete Zertifikat auch auf Deutsch verfügbar. Herausgeber ist die Fachorganisation $(ISC)^2$. Ihre Berechtigungsnachweise erfüllen die Anforderungen des ISO/IEC Standards 17024. Auch über Schulungen vom SANS-Institut erhält man anerkannte Zertifizierungen, wie die zum Certified Forensic Analyst (GCFA) oder zum Network Forensic Analyst (GNFA).

Die International Association of Computer Investigative Specialists (IACIS) bietet ebenfalls Forensik-Schulungen mit Zertifikat an. Das Besondere dabei: Die Lernenden untersuchen die Daten ohne die sonst üblichen Tools. Dies soll angehende IT-Forensiker und -Forensikerinnen in die Lage versetzen, Befunde der Analysesoftware zu erläutern und zu begründen. Erfolgreiche Absolventen tragen den Titel CFCE (Certified Forensic Computer Examiner), der insbesondere bei US-Strafverfolgern hoch angesehen ist.

Ausbildung auf höchstem Niveau

Ein besonderes, in Deutschland konzipiertes Zertifikatsprogramm bietet das Open Competence Center for Cyber Security, abgekürzt Open C^3S. Das an der Hochschule Albstadt-Sigmaringen gemeinsam mit acht weiteren Hochschulen und Universitäten entwickelte Studienangebot umfasst 35 in sich abgeschlossene Module zu den Themenschwerpunkten IT-Sicherheit, Kryptografie, IT-Compliance, IT-Forensik und IT-Recht. Jedes Modul beansprucht acht Wochen. Dabei werden schriftliche Studienmaterialien, Online-Vorlesungen, eine Online-Lernplattform und ein Präsenzwochenende mit persönlicher Studienbetreuung kombiniert. Nach dem erfolgreichen Abschluss eines Moduls gibt es neben einer Zertifikatsurkunde fünf ECTS-Punkte (European Credit Transfer and Accumulation System). Man kann auch mehrere Zertifikate kumulieren, beispielsweise zum Gesamtzertifikat Netzwerkforensiker/-in Open C^3S oder Datenträgerforensiker/-in Open C^3S.

Methodenkompetenz per Fernstudium

Das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Zertifikatsprogramm steht auch Teilnehmern ohne Abitur offen. Für Teilnehmer ohne Informatikkenntnisse oder Hochschulzugangsberechtigung haben die Tutoren spezielle Grundlagen-Module konzipiert. Darunter sind auch Forensik-Autodidakten, die sich hier den offiziellen Beleg beschaffen, damit sie mehr Gehalt verdienen, wie auch Juristen, die ein Forensik-Gutachten selbst einschätzen können wollen, statt immer eine Fremdmeinung einzuholen. Allein die Telekom lässt regelmäßig ganze Abteilungen an den Fortbildungen teilnehmen.

Digitale Forensik ist mit ein Schwerpunkt der Hochschule Albstadt-Sigmaringen. Sie und die Hochschule Mittweida sind die einzigen akademischen Einrichtungen in Deutschland, die einen Studiengang Digitale Forensik anbieten. In Albstadt-Sigmaringen steht dieser auch als berufsbegleitender Online-Fernstudiengang zur Verfügung. Der Abschluss Master of Science berechtigt anschließend zur Promotion. Die Anzahl der Plätze ist auf 30 begrenzt, um eine hohe Qualität der Betreuung sicherzustellen. Mit Frauen besetzt sind hier bereits die Studiengangskoordination und -assistenz. Im gesamten Masterstudiengang Digitale Forensik beträgt der Anteil der weiblichen Studierenden derzeit 18 %.

Inhaltlich wird hier wie auch beim Zertifikatsprogramm viel Wert auf universell anwendbares Wissen gelegt. In den dreieinhalb Jahren, die das Studium dauert, kann sich einiges auf dem Markt für Forensik-Produkte tun. Daher sind die Lehrinhalte bewusst anbieterneutral gehalten und an Methodenkompetenz orientiert. Teilnehmer lernen nachzuvollziehen, wie ein Tool funktioniert und wie es sich von anderen unterscheidet. Denn IT-Forensiker sollten ihren Werkzeugen nie unbesehen vertrauen. Der Einsatz von Antiforensik zeigt längst, dass professionalisierte Täter nur allzu genau wissen, wie sie ihre Spuren gegenüber Forensik-Tools verwischen können. Ideal ist es also, selbst programmierte Tools zu verwenden.

Training für echte Cybercops

Auch Frauen bei der Polizei nutzen die Fernstudienangebote der Hochschule Albstadt-Sigmaringen. Manche davon, um einfach ihr IT-Wissen zu erweitern, andere, um Zugang zum höheren Dienst zu erhalten. Eine von ihnen ist Kriminalkommissarin Sabrina Krüger-Voigt. Eine Lokalzeitung widmete ihr einen ausführlichen Bericht. Ihr Jobprofil und ihre Erfahrungen im Team der Kriminalinspektion 5 – zuständig für Cybercrime – in einer Kriminalpolizeidirektion in der Region Stuttgart zeigen exemplarisch, wie Frauen mit fundierter Ausbildung in diesem Bereich bereits angekommen sind.

Damit machen sie sich auch beim Bundeskriminalamt (BKA) gefragt. Hier ist nämlich eine Quick Reaction Force im Aufbau, die andere Strafverfolgungsbehörden unterstützen und bei Cyberangriffen Daten sicherstellen soll. Auch das Bundesamt für Verfassungsschutz soll so eine schnelle Eingreiftruppe erhalten. „Insgesamt", sagte BKA-Präsident Holger Münch auf der Jahreskonferenz in Berlin, „müssen wir der Fortentwicklung unseres Berufsbildes hin zu einem Cybercop Rechnung tragen." Und wohl nicht zufällig zeigt eine Anzeigenkampagne der Bayerischen Polizei zum Recruiting für die Kernbereiche IT-Kriminalistik/IT-Forensik/IT-Professional symbolstark immer eine Frau mit zwei Männern als Illustration für den Bereich IT-Terrorabwehr „mit Job-Garantie".

Doch was so ein Cybercop alles draufhaben muss, ist nicht nur in Deutschland in jedem Bundesland anders definiert. In ganz Europa arbeitet jede Polizeibehörde mit ihren eigenen Methoden. Das erschwert die Zusammenarbeit in Sachen Abwehr und Verfolgung grenzüberschreitender Netzkriminalität. Daher fördert die EU-Kommission den Aufbau einer Kompetenzmatrix, in der die nötigen Fähigkeiten aller im Bereich Cybercrime aktiven Berufe in den europäischen Strafverfolgungsbehörden erfasst werden – vom sogenannten Ersteinschreiter über den IT-Forensiker bis zum Polizeichef. Ziel der zusammen mit EUROPOL und CEPOL umgesetzten Initiative ist eine grenzüberschreitende Standardisierung der Cybercop-Ausbildung.

Europaweit einheitliche Polizeifortbildung

Das Projekt nennt sich SENTER (Strengthening European Network Centres of Excellence in Cybercrime), und auch hier ist die Hochschule Albstadt-Sigmaringen aktiv. Seit 2016 hat sie Poli-

Neue Herausforderung gesucht? Swiss Life sucht Verstärkung in Hannover.

Swiss Life verfügt über eine hochmoderne, agile IT und sucht Spezialisten für die Bereiche IT-Betriebsmanagement und Anwendungsentwicklung.

Swiss Life Deutschland ist ein führender Anbieter von Finanz- und Vorsorgelösungen mit Sitz in Garching b. München und Hannover. Unter der Marke Swiss Life stellen wir Privat- und Firmenkunden innovative Versicherungsprodukte und Dienstleistungen in den Bereichen Vorsorge und Sicherheit zur Verfügung. Unsere Vertriebsgesellschaften Swiss Life Select, tecis, HORBACH und Deutsche Proventus stehen für ganzheitliche und individuelle Finanzberatung.

Entdecken Sie unsere berufliche Vielfalt und klicken Sie sich durch unser Haus der Berufe:
www.swisslife.de/ueber-uns/karriere/haus-der-berufe/rundgang.html

Haben wir Ihr Interesse geweckt?
Weitere Informationen finden Sie unter:
www.swisslife.de/karriere

top EMPLOYER DEUTSCHLAND 2016
CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

SwissLife

In über 500 Weiterbildungsprodukten für IT-Anwender, -Profis und -Entscheider finden Sie das für Sie passende IT-Training. Profitieren Sie von unserem breitgefächerten Angebot für Ihren individuellen Weg zum Erfolg:

- Autorisierter Trainingsanbieter von Microsoft, Oracle, VMware, AWS u.v.m.
- Herstellerunabhängiges Angebot zu IT-Management und IT-Security
- Verschiedene Lernformen, wie z.B. Training on Demand
- Viele Garantietermine
- Zertifizierte Trainer

Jetzt informieren:
www.tuv.com/it-training

TÜVRheinland®
Genau. Richtig.

zisten aller Mitgliedsländer interviewt und daraus fast 300 Kompetenzkriterien abgeleitet, die in den verschiedenen Bereichen der Polizeiarbeit zum Tragen kommen – technische genauso wie psychologische und Ermittlungsfähigkeiten. Auch welche didaktischen Methoden sich für die Polizeiausbildung im Thema bewährt haben, wurde auf diese Weise ermittelt. Das daraus entwickelte Skill-Management-Portal funktioniert wie ein persönlicher Trainer: Man gibt ein, welchen Tätigkeitsschwerpunkt man hat und in welches Berufsprofil man sich entwickeln möchte. Wo die Anwendung Nachholbedarf erkennt, schlägt sie passende Online-Trainings vor.

Bei zahlreichen Polizisten taten sich Wissenslücken im Bereich Open Source Intelligence (OSINT) auf – Informationsgewinnung aus frei verfügbaren Quellen. Dazu gehören Augenzeugenberichte genauso wie Massenmedien, in zunehmendem Maße aber auch Social-Media-Portale wie Facebook, Xing, Twitter und Webseiten im Internet und Darknet. Findige Ermittler sind längst darauf gekommen, mit welchen selbst geschriebenen Scripts sie Massenabfragen auf mehreren Kanälen gleichzeitig durchführen können. Im Großen und Ganzen besteht hier aber noch viel Unwissenheit. Die Wissenschaftler an der Hochschule Albstadt-Sigmaringen haben deshalb für OSINT-Ermittler ein gezieltes Training entwickelt, das ihr Skill-Management-Portal vervollständigt.

Vom Softwareentwickler zum IT-Kriminalisten

Es kommt nicht selten vor, dass solch ein fähiger Cybercop von der Industrie abgeworben wird – und hier sehr viel mehr verdient. Doch es gibt auch die umgekehrten Fälle. Bei der Bereitschaftspolizei in Sulzbach-Rosenberg in der Oberpfalz wurden auch im sechsten Jahrgang alle Ausbildungsplätze zum Cybercop vergeben – an Bewerber mit abgeschlossenem IT-Studium und mindestens zwei Jahren Berufserfahrung, Höchstalter 44. Innerhalb von zwölf Monaten werden in Sulzbach-Rosenberg pro Jahr um die 20 IT-Fachkräfte zu richtigen Vollzugsbeamten weitergebildet. Sie bekommen die rechtlichen Grundlagen der Polizeiarbeit vermittelt, lernen schießen und üben sich in Selbstverteidigung. Wenn sie die Prüfung am Ende bestehen, werden sie zu Beamten ernannt und können sich an einem Präsidium ihrer Wahl bewerben – Einstiegsstufe A10.

Bei den Good Cops bin ich dabei

Auf solche Überzeugungstäter setzt auch die sächsische Polizei mit ihrer Kampagne „Endlich Zugang zum Polizeirechner – und damit Gutes tun!" Um qualifizierte Cyberkommissarinnen und -kommissare zu finden, warb der Freistaat Sachsen mit Plakaten und Flyern an 29 Hochschulen in Sachsen, Thüringen, Sachsen-Anhalt und Brandenburg. Interessierte können sich unter *cyber crime.verdaechtig-gute-jobs.de* über das Berufsbild und die Bewerbungsvoraussetzungen informieren. Auch die bayerische Polizei hat für Interessierte eine gut gestaltete Seite ins Netz gesetzt: *mit-sicherheit-anders.de/IT/*. Für den ein oder anderen vielleicht überraschend: Die Personen auf den Anzeigenfotos sind keine Models, sondern allesamt echte IT-Cracks, die zur Polizei gewechselt sind (s. Bild S.16)!

Das dort abgebildete „Drittel" Frauenanteil ist vielfach aber noch Zukunftsmusik. Eine aktuelle Studie, u. a. von Human Resources Information Systems der Universität Bamberg, zeigt, dass in Unternehmen nicht einmal ein Zehntel der IT-Stellen mit Frauen besetzt sind. Es sind aber auch nur gut 17 % Frauen, die sich auf offene IT-Positionen bewerben. „Wir brauchen Förderprogramme für Frauen in IT-Führungspositionen, um sie gezielt zu unterstützen. Der Fachkräftemangel wird alleine mit männlichen Kräften nicht zu decken sein", wird Ex-KPMG-Partner Michael Ruplitsch in einer Presseinformation zitiert. Und gerade in dieser smarten Art der Verbrechensbekämpfung können Frauen zeigen, dass sie ihren männlichen Kollegen allemal das Wasser reichen können.