Campus

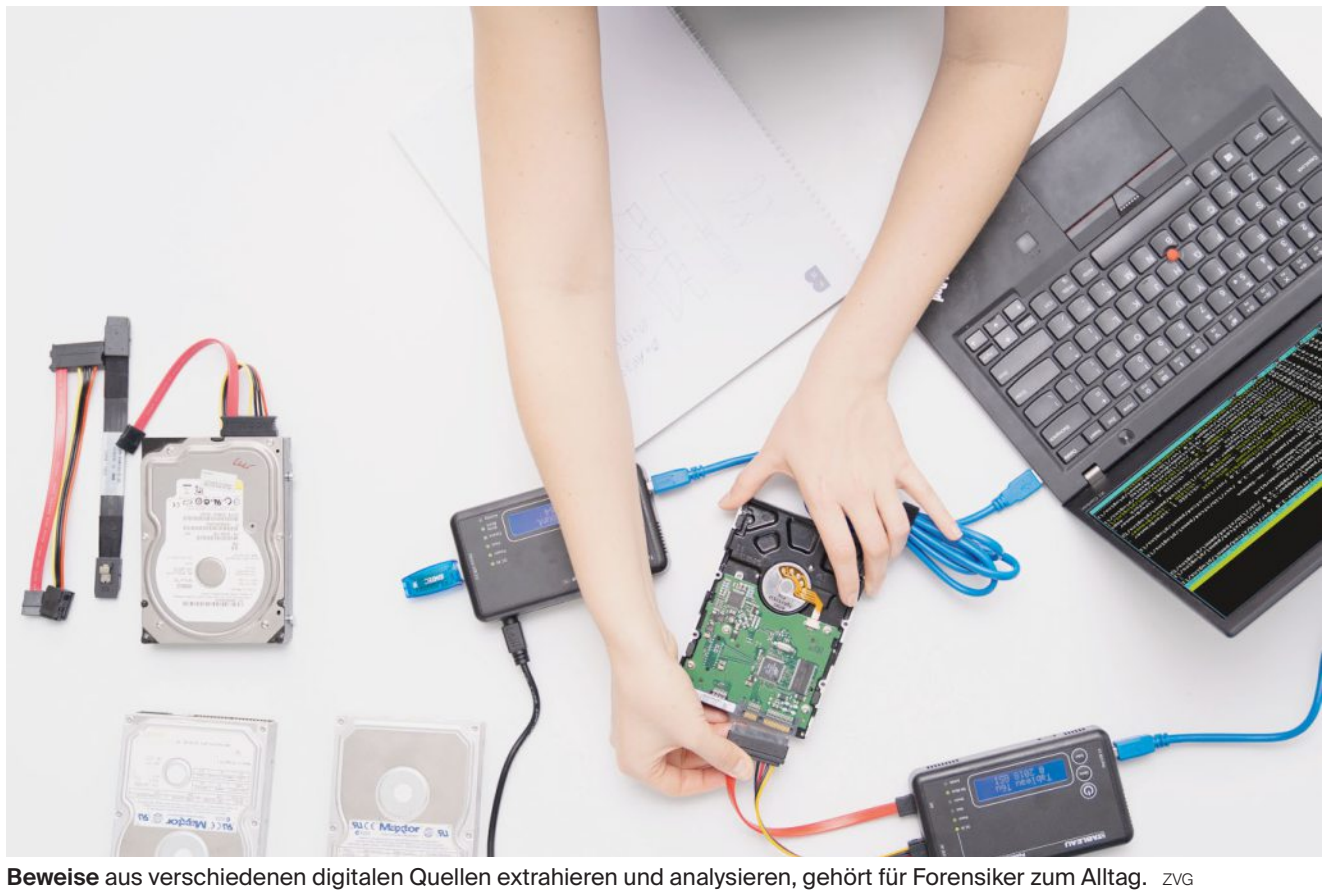
Spurensuche am digitalen Tatort

Cyberkriminalität Kriminelle Kräfte finden im Internet immer ausgeklügeltere Methoden, um an fremdes Eigentum zu kommen. Mit einem neuen Studiengang reagiert die Berner Fachhochschule auf Bedürfnisse aus Wirtschaft, Militär und Behörden.

Marc Schiess

Bankräuber alter Schule stehen vor einem Problem: Geld wird immer mehr digital. Der Serverraum löst den Banktresor ab. Die gute Nachricht: Gewalt oder Fachwissen, wie man einen Tunnel gräbt, reichen nicht mehr, um fette Beute zu machen. Die schlechte Nachricht: Nun bestehlen findige Kriminelle neben Banken vor allem kleine Fische wie Sie und ich – digital, ohne sich die Finger schmutzig zu machen. Hatten vor zehn Jahren die Cyberkriminellen noch vornehmlich die «technological Exploitation», das Aufspüren von Schwachstellen bei Geräten im Fokus, ist es heute die Schwachstelle Mensch.

Kaum jemand weiss dies besser als Bruce Nikkel. Der Kanadier arbeitet seit über 20 Jahren als Cybersicherheitsexperte bei einer Schweizer Bank. Die von ihm gegründete Forensik-Abteilung feierte bereits ihr 15-jähriges Bestehen. Nikkel ist von der Wucht, mit der das Internet in den letzten Jahrzehnten die Welt veränderte, beeindruckt: «Der digitale Wandel ist fundamental und riesig – es braucht ganz neue Skills für die Verbrechensbekämpfung.» Seine weitere Tätigkeit als Dozent am Departement Technik und Informatik der Berner Fachhochschule (BFH) und sein internationales Netzwerk öffneten dem Professor Tür und Tor: Im April 2020 startet an der BFH der von Nikkel initiierte Masterstudiengang im Bereich Digitale Forensik und Cyber Investigation.



Beweise aus verschiedenen digitalen Quellen extrahieren und analysieren, gehört für Forensiker zum Alltag. ZVG

Studenten aus ganz Europa erwartet

Als Dozenten verpflichtete Nikkel internationale Top-Shots der Fachbereiche. Diese halten ihre Vorlesungen jeweils kompakt in einer Woche ab. Vorlesungsort ist Bern, gesprochen wird englisch. Nikkel ortet denn das Zielpublikum auch im gesamteuropäischen Raum, nicht zuletzt wegen der Einzigartigkeit des Gebotenen: «In der europäischen Universitätslandschaft gibt es diese Art von stark fokussiertem Forensikprogramm bisher nicht.» Ein Polizeiausbildungszentrum werde es jedoch nicht werden, betont der Professor: «Die Polizei hat heute schon Ressourcen und Trainings für Cyberkriminalität.» Bedürfnis angemeldet haben vor allem international tätige Unternehmen im Finanz- und Versicherungssektor, aber auch Militär und Strafverfolgungsbehörden. Sie lernen im Master, wie man kriminelle Handlungen im Cyberraum wissenschaftlich und systematisch aufspürt, analysiert, untersucht und rekonstruiert. Nach Ermittlung und Analyse folgt bei kriminellen Sachverhalten die Meldung an die Polizei.

Katz- und Mausspiel

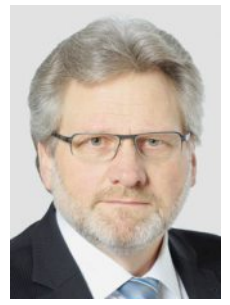
Das Fachgebiet der digitalen Forensik ist hochkomplex. Nur IT-Spezialisten verstehen, was sich hinter Begriffen wie Anti-Forensics, Hashing, Super-Timelines oder Rekall verbirgt. «Vereinfacht gesagt lernt man im Masterstudiengang, wie man im Internet zum Beispiel mit Open Source Intelligence ermittelt, wie man Beweismittel sichert oder wie man ein Smartphone oder eine Festplatte analysiert», sagt Bruce Nikkel.

Selber bezeichnet er sich mit einem Schmunzeln als «klassischen Computernerd», dem es 1983 mit dem Film «WarGames» den Ärmel reingezogen hat. Die intellektuelle Herausforderung fasziniert ihn noch heute: «Die Cyberkriminellen sind clever, es ist ein Katz- und Mausspiel, das jeden Tag Rätsel zu lösen erfordert.» Der Schwierigkeitsgrad dieses ernsten «Spiels» sei oft «extrem schwierig», wenn man berücksichtigt, dass im Gegensatz zur analogen Straftat ein physischer Tatort fehlt.

Berufssparte mit guten Aussichten

Die weltweite Zusammenarbeit zwischen den Strafverfolgungsbehörden hat denn auch in den letzten Jahrzehnten stark zugenommen. Europol und Interpol sowie in der Schweiz das Nationale Zentrum für Cybersicherheit (Vorgängerin: Melani) sind wichtige Kooperationspartner der Cyberermittler geworden: «Der öffentliche Sektor hat gemerkt, dass der Support des privaten Sektors bei der Bekämpfung der Kriminalität hilft», so Nikkel.

Die Zukunftsaussichten der noch relativ jungen Berufssparte präsentieren sich rosig. Mit den technologischen Entwicklungen erhalten Kriminelle neue Werkzeuge, die selbst sehr kritische Menschen narren könnte. Als grösste Herausforderung sieht Nikkel die «Social-Engineering»-Attacken, insbesondere die «Deep-Fake»-Technologie. Diese ermöglicht mittels künstlicher Intelligenz das Herstellen von täuschend echt wirkenden Videos einer Person. Dazu notwendig ist nur Fotomaterial jener Person. Sogar die Stimme lässt sich auf diese Art imitieren, wenn genügend Tonmaterial vorhanden ist. Falls Sie also beim Anruf einer nahe stehenden Person aufgefordert werden, Geld zu überweisen, könnte es sich lohnen, mit detaillierten Gegenfragen zur Vergangenheit abzuklären, ob wirklich die eigene Partnerin oder der Enkel am Apparat sind.



Bruce Nikkel, Leiter MAS Digital Forensics und Cyber Investigation

Der Studiengang im Detail

Der im April 2020 startende **Masterstudiengang in Digital Forensics** und **Cyber Investigation** beinhaltet vier CAS-Semester mit Vorlesungen und einer finalen Master Thesis. In jedem Semester sind vier einwöchige Module zu besuchen. Ein Teil davon ist individuell wählbar. Der Studiengang umfasst 60 ECTS-Punkte und kostet 34 000 Franken. Zielgruppen sind Forensikerinnen und Forensiker, die ihre technischen Fähigkeiten in digitaler Forensik und Cyber Investigation erweitern wollen sowie erfahrene Ingenieure und Techniker, die in den Bereich der digitalen Forensik und Cyber Investigations wechseln wollen. *msc*