«Es bleibt ein Katz-und-Maus-Spiel»

Im Herbst 2024 beginnt an der BFH wiederum der Studiengang Master of Science in Engineering (MSE), der von allen Schweizer Fachhochschulen gemeinsam angeboten wird. Er beinhaltet neu eine Vertiefungsrichtung in Cyber Security. Die Schweiz sei überdurchschnittlich gut gegen Cyber-Kriminalität gerüstet, sagt BFH-Professor Bruce Nikkel. «Aber es bleibt ein Katz-und-Maus-Spiel mit den Kriminellen.» Peter Bader

Vor Ihrem Engagement an der BFH waren Sie während über 20 Jahren für die Cyber-Sicherheit einer Bank tätig. Wie hat sich die Bedrohung verändert?

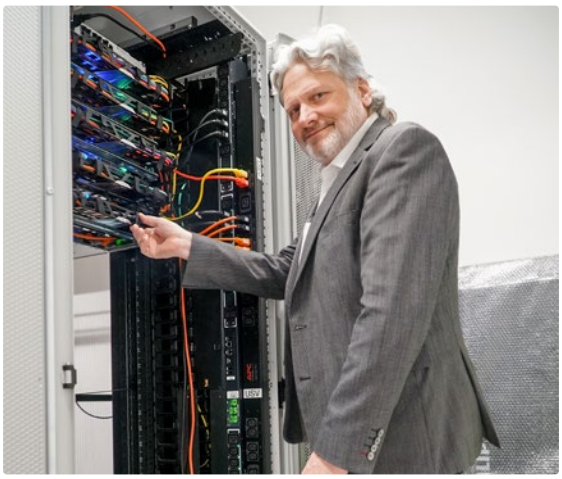
Bruce Nikkel: Vor 15, 20 Jahren waren die Kriminellen im Vergleich zu heute noch Amateur*innen. Damals war das E-Banking grossen Cyber-Angriffen ausgesetzt: Kriminelle versuchten, sich mit Trojaner-Programmen Zugriff auf Konten zu verschaffen. Heute ist dies für sie schwieriger: Banken sind besser in der Lage, infizierte Kunden-Computer zu entdecken und Cyber-Angriffe frühzeitig abzuwehren. Dafür haben wir es mit Ransomware zu tun, also mit Schadprogrammen, die den Zugriff auf Daten und Systeme einschränken oder unterbinden. Für die Freigabe wird dann ein Lösegeld verlangt. Die Fahndung nach den Tätern, die zumeist aus dem Ausland operieren, ist aufwändig und selten erfolgreich. Ransomware kam mit der Einführung der Bitcoin-Währung immer mehr zum Einsatz: Damit lassen sich Lösegeld-Transaktionen anonym und zuverlässig durchführen, ohne dass viele Menschen konkret daran beteiligt sind.

Gibt es weitere Gefahren?

Auch das «Industrial internet of things», also zum Beispiel die Vernetzung von smart-Gebäuden oder industrielle Steuerungssysteme, kann zum Problem werden: Die Technik ist oft unsicher oder veraltet und wird nicht schnell genug aktualisiert. Industrie-Betriebe lassen sich so leichter hacken und stören. Ein Problem ist zudem das fehlende Bewusstsein der Menschen: Sie sind nach wie vor das grösste Einfallstor für Ransomware, weil sie zum Beispiel gegenüber Mails mit unbekanntem Absender zu wenig skeptisch sind und schnell einmal auf einen verdächtigen Link klicken.

Welche Rolle spielt die künstliche Intelligenz (KI)?

Im Moment noch keine entscheidende. Kriminelle nutzen sie etwa, um Malware zu schreiben. Mittels KI gefälschte Anrufe von Familienangehörigen, die Hilfe benötigen, werden in Zukunft ein Problem werden. Im Moment weisen solche Deepfakes immer noch kleine Fehler auf, an denen man sie erkennen kann. Aber auch Polizei oder Sicherheitsunternehmen werden KI nützen, um vor deren kriminellem Einsatz zu schützen. Es bleibt ein Katz-und-Maus-Spiel: Angreifer*innen und Verteidiger*innen liefern sich ein permanentes Wettrüsten mit wechselnden Vorteilen für die eine oder andere Seite. Cyberkriminelle sind meistens Opportunist*innen: Wenn der Widerstand zu stark ist, suchen sie sich andere Opfer oder andere Schlupflöcher aus.



Bruce Nikkel: «Als Hochschule für angewandte Wissenschaften konzentrieren wir uns auf eine praxisnahe Ausbildung.» (Foto: Peter Bader)

Im Herbst 2024 beginnt an allen Schweizer Fachhochschulen wiederum der Studiengang Master of Science in Engineering (MSE). An der BFH wird neu die Vertiefungsrichtung Information und Cyber Security angeboten. (Foto: iStock)

Ist die Schweiz gut gerüstet?

Im Vergleich zu anderen Ländern überdurchschnittlich gut, ja. Das Nationale Zentrum für Cybersicherheit (NCSC) ist eine wichtige Anlaufstelle für Unternehmen und kritische Infrastrukturen wie Energieversorger oder Spitäler und bietet Unterstützung an. Die Schweiz nimmt das Thema Cybercrime sehr ernst, das ist gut so. Viele Unternehmen und Institutionen haben denn auch in den vergangenen Jahren gelernt, mit der Cyber-Kriminalität umzugehen. Das Bewusstsein, dass man jederzeit Zielscheibe eines Angriffs werden kann, ist gestiegen. Bei der Planung von Vorsorgemassnahmen stellt sich natürlich dennoch die Frage nach dem richtigen Verhältnis zwischen Aufwand und Nutzen. Hochstehende Technologien bieten einen guten Schutz, kosten aber auch viel Geld. Und absolute Sicherheit können auch sie nicht bieten. Der IKT-Minimalstandard des Bundes kann dabei helfen, den Handlungsbedarf im eigenen KMU zu ermitteln und Abwehrmassnahmen zu planen.

Gerade im Bereich der Cyber-Sicherheit wird es inskünftig immer mehr Fachkräfte brauchen. Welche bildet die BFH aus?

Als Hochschule für angewandte Wissenschaften konzentrieren wir uns auf eine praxisnahe Ausbildung, die ein breites Spektrum an Themen abdeckt. Wir bilden also sicherheitsbewusste Ingenieur*innen, Architekt*innen, Entwickler*innen, IT-Administrator*innen und -Operator*innen sowie Manager*innen aus. Sie werden in der Industrie dringend gebraucht.

Heute gibt es an der BFH die beiden Masterstudiengänge MAS Digital Forensics & Cyber Investigation und MAS Cyber Security. Welches sind die wichtigsten Inhalte?

Sie decken eine sehr breite Palette ab. In der Forensik werden jene Arbeitsgebiete zusammengefasst, in denen systematisch kriminelle Handlungen identifiziert, analysiert und rekonstruiert werden. Zu den Ausbildungsinhalten der beiden Studiengänge gehören etwa Malware-Analyse, digitale Forensik, Fintech-Sicherheit, industrielle Sicherheit oder das Internet der Dinge (IoT). Grundsätzlich geht es um die allgemeine Sensibilisierung und Aufklärung, die Erkennung von Vorfällen und eine angemessene Reaktion darauf, um Risikomanagement, sichere IT-Architektur und -Programmierung. Zu den Inhalten gehören auch cyberbezogene Vorschriften und Gesetze oder Bedrohungen durch Insider und Dritte.

Ab Herbst 2024 wird an der BFH wiederum der Studiengang Master of Science in Engineering (MSE) angeboten. Was ist das Besondere daran?

Dass er von den acht Fachhochschulen der Schweiz gemeinsam angeboten wird. Das heisst, dass die Studierenden von einem schweizweiten Netzwerk aus Fachspezialist*innen profitieren. Die ersten beiden Jahre sind für alle Studierenden gleich, danach gibt es 16 mögliche Vertiefungsrichtungen. Neu ist jene zu Information und Cyber Security, die unter anderem bei uns an der BFH angeboten wird.

Weitere Infos

Kontakt:
Prof. Dr. Bruce Nikkel, Co-Leiter Institut ICE
bruce.nikkel@bfh.ch