Bild: depositphotos

Zur Person

Nathalie Weiler ist seit Mai 2020 Professorin für Cybersecurity an der OST, Ostschweizer Fachhochschule, in Rapperswil (vormals HSR). Sie ist 1973 in Luxemburg geboren und dort aufgewachsen. An der ETH Zürich studierte sie ab 1992 Informatik und Ingenieurwesen (Dipl. Inf. Ing. ETH) und promovierte im Anschluss über das Thema Netzwerk-Security. Von 2004 bis 2019 war Nathalie Weiler in verschieden Unternehmen als CISO und Security Architect tätig. *(acp)*

Interview: Andrea C. Plüss

Nathalie Weiler, Sie sind Professorin für Cybersecurity an der Fachhochschule Ost in Rapperswil. Können Sie in einfachen Worten erklären, was man sich darunter vorstellen muss?
Nathalie Weiler: Digitalisierung und Vernetzung aller Lebensbereiche fordern von unseren Infrastrukturen, Systemen und Applikationen einen besseren Schutz vor Missbrauch und Angriffen aus dem Cyberspace. Die notwendigen Spezialisten auf diesem Gebiet sind stark gefragt. Im Studiengang Informatik an der OST wird Studierenden vermittelt, wie sie ihre Software und Systeme gegen die neuen und alten Bedrohungen immunisieren. Der Studiengang hat sowohl eine forschungs- als auch anwendungsorientierte Ausrichtung. Nebst einer breiten Grundausbildung in mathematischen und informationstechnischen Themen bietet er Spezialisierung an, damit künftige Software- und System Engineers sichere Software auf sicheren Systemen und Infrastrukturen entwickeln.

Sollte man, salopp formuliert, Hacker-Qualitäten haben, um wirklich gut zu sein?
Das Verständnis, wie man eine Webapplikation oder auch ein IoT-System «hackt», ist ein sehr wichtiger Aspekt der Cybersecurity, aber aus meiner Sicht bei weitem nicht der einzige und auch nicht zwingend vorausgesetzt. Hacker-Qualitäten sind wichtig, um erstellte Applikationen und Systeme zu verbessern oder überhaupt erst publizierbar zur machen. Niemand von uns möchte schliesslich gern als Versuchskaninchen missbraucht werden, weder beim Onlineshoppen noch bei der Steuerung seines Smart Homes.

Welche Fähigkeiten sind darüber hinaus wichtig?
Wir brauchen auch, und zwar viel dringender Fachkräfte, die wissen, wie sie solche Systeme überhaupt erst sicher erstellen können. Auch, damit ein potenzieller Hacker eine Challenge vorfindet, auf eine Herausforderung trifft, bei seinen professionellen Einbruchsversuchen. Salopp formuliert würde ich sagen, wir brauchen Lego-Kreative dringender als jemanden mit speziellen Hacker-Qualitäten.

> *«Blind zu glauben, man sei geschützt, ohne in die IT-Sicherheit zu investieren, ist naiv.»*

Sie waren auch als CISO in Industrieunternehmen beschäftigt. Welche Aufgaben standen dabei im Vordergrund?
Der Chief Information Security Officer wird ja häufig dargestellt als jemand mit reiner Kontrollfunktion für IT-Sicherheit in Unternehmen. Sicher gehören diese Aufgaben, wie z. B. der risikoarme Wechsel vom Büro ins Homeoffice im Pandemiefall, wie diesen Frühling, zu den sichtbarsten Events dieser Rolle. Dieser «Incident», wie er im Fachjargon bezeichnet wird, ist aber nur einer von ganzen vielen Plänen, die der CISO im Team bereitstellt und mit dem Unternehmen übt, damit klar ist, was zu tun ist, sollte ein Eindringen ins System stattfinden.

Ein anderer wesentlicher Aspekt eines CISO ist seine Beraterfunktion. Beispielsweise, wenn ein Unternehmen sich entschliesst, Teile seiner IT in eine externe Cloud-Lösung auszulagern. Dann sind die Auswirkungen auf die Risikolandschaft abzuschätzen.

Wird das Thema Cybersecurity von Unternehmen Ihrer Meinung nach gebührend beachtet?
Viele Unternehmen haben nicht erst mit der Coronakrise realisiert, dass Cyber-Sicherheit wichtig für den Unternehmenserfolg ist. Speziell die Kontrollfunktionen, die direkt sichtbar sind im operativen Betrieb (Krisenplan vorhanden oder nicht) wurden in den letzten fünf Jahren stark ausgebaut. Leider sind auf der Entwicklungsseite aber immer noch grosse Lücken. Das sieht man beispielsweise daran, dass es zwar ein Budget für Penetration Tests (also für den «Sicherheitsabnahmetest» am Schluss) gibt, aber weder Zeit noch Geld für andere, vorgelagerte Verbesserungen der Sicherheit im Software-Entwicklungsprozess eingeplant wird.

Gibt es Branchen, deren Unternehmen eher Opfer eines Hackerangriffs werden, als andere?
Ich halte es für kontraproduktiv, sollte ein Unternehmen denken, es stünde nur deshalb nicht im Fokus eines Angriffes, weil es keine Finanzdienstleistungen oder sonstigen monetären Anreize für Hacker bietet. Blind zu glauben, man sei geschützt, ohne in die Sicherheit zu investieren, ist naiv.

Haben Sie den Eindruck, dass Firmen auf die Sicherheitsrisiken durch vermehrtes Homeoffice und die Nutzung privater Geräte für Firmenbelange ausreichend reagiert haben?
Ganz ehrlich: nein. Das sieht man auch an den Meldungen, die heute schon bei Melani (Melde- und Analysestelle Informationssicherheit des Bundes, Anm. der Red.) eintreffen. Wenn man bedenkt, dass die richtig grossen Vorfälle oft erst Monate oder Jahre nach der ersten Infiltration im Unternehmen als Schaden auftreten, stehen uns wohl, sicherheitstechnisch betrachtet, spannende Zeiten bevor – leider.