Der Mensch als Sicherheitsrisiko in der IT

Vorträge aus Wissenschaft und Wirtschaft anlässlich der Arbeitskreissitzung „IT-Sicherheit“ des ZKI e.V.

Christoph Becker, Stefan Brützsch

Wie können Studierende, Mitarbeitende und Führungskräfte einer Hochschule effektiv und effizient für Informationssicherheit sensibilisiert und geschult werden? Was sind die Erfolgsfaktoren für Awareness-Maßnahmen und IT-Security-Trainings für IT-Fachpersonal?

Mit diesen Fragen hatte sich der Arbeitskreis „IT-Sicherheit“ des Vereins der „Zentren für Kommunikationsverarbeitung in Forschung und Lehre“ (ZKI e. V.) am 14. und 15. März 2018 an der Universität Konstanz befasst. Im Rahmen der Zusammenarbeit zwischen IT-Servicezentren der Hochschulen und Forschungseinrichtungen in Deutschland wird in diesem Arbeitskreis unter anderem durch Austausch von Erfahrungsberichten das Thema IT-Sicherheit im Kontext hochschulspezifischer Herausforderungen adressiert. In ihm sind viele der deutschen Hochschulen mit ihren jeweiligen Informationssicherheitsbeauftragten oder Personen mit ähnlichen Funktionen vertreten. Den Rahmen des Austauschs in Konstanz bildeten Vorträge zum Thema von Referenten aus Wissenschaft und Wirtschaft.

Die Auftaktpräsentation hielt Prof. Dr. Hanno Langweg von der Hochschule für Technik, Wirtschaft und Gestaltung (HTWG) Konstanz, wo er seit 2014 eine Professur für Datensicherheit in cloudbasierten Systemen und IT-Forensik innehat. In seinem Vortrag berichtete er über die Erfahrungen mit „Capture the Flag“ (CTF) -Wettbewerben im Rahmen von Lehrveranstaltungen zur IT-Sicherheit. Bei diesem spielerischen Ansatz werden die Teilnehmenden in Teams aufgeteilt und in einem isolierten Netzwerk mit je einem Computersystem betraut. Bei diesem Spiel gewinnt, wer sowohl das eigene System erfolgreich gegen die Angriffe der gegnerischen Teams verteidigen als auch selbst mit erfolgreichen Angriffen kontern kann. An der HTWG Konstanz wurde in mehreren Projekten systematisch untersucht, wie sich CTF-Wettbewerbe sinnvoll in die Lehre integrieren lassen können. Das Fazit von Prof. Dr. Langweg ist positiv: CTF-Wettbewerbe erhöhen die Motivation Studierender im Bereich IT-Sicherheit – ein Wettbewerb als Teil einer Lehrveranstaltung, bei dem „Verlieren“ keine Nachteile für das eigene Studium bringt, so Prof. Langweg. Dabei sammeln sie erste praxisrelevante Erfahrungen, sichere Software zu schreiben, Konfigurationsfehler zu vermeiden, Angriffe frühzeitig zu erkennen und deren Auswirkungen unter Zeitdruck abzumildern.

Daran anknüpfend berichtete Florian Fankhauser, Leiter der Forschungsgruppe Establishing Security (ESSE) der Technischen Universität (TU) Wien, über seine Erkenntnisse und Erfahrungen mit unterschiedlichen Arten von CTF-Wettbewerben in der universitären Ausbildung. Nach einem kurzen Überblick über die unterschiedlichen Formen von CTF-Wettbewerben präsentierte er Erfahrungen aus der langjährigen Anwendung in der Lehre an der TU Wien sowie Impulse über den Nutzen von CTF-Wettbewerben in der Weiterbildung von IT-Personal. Auch Herr Fankhauser zieht ein positives Fazit und hebt insbesondere das durch CTF-Wettbewerbe gesteigerte Interesse der Teilnehmenden an der Materie hervor.

Dr. Marco Ghiglieri, damals noch Postdoc in der Arbeitsgruppe von Prof. Dr. Melanie Volkamer an der TU Darmstadt,[1] berichtete über seine Forschung zu effektiven Maßnahmen gegen Phishing und andere gefährliche E-Mail-Nachrichten. Im Rahmen eines vom Bundesministeriums für Wirtschaft und Energie (BMWi) geförderten Projektes hat die Arbeitsgruppe ein Konzept sowie verschiedene Umsetzungsformen zur Nutzersensibilisierung im Umgang mit gefährlichen E-Mails entwickelt, die nachweislich effektiv sind. Unter der Überschrift „SECUSO für den Bürger“[2] hat die Gruppe Materialien und Tools online veröffentlicht, die auf unterschiedliche Art und Weise helfen, sich vor Angriffen besser zu schützen. Er plädiert dafür,

dass auch die Einrichtungen selbst passende Maßnahmen (wie die Verwendung von E-Mail-Signaturen und der Verzicht auf URL-Shortener in E-Mails) ergreifen müssen, damit das Verifizieren durch E-Mail-Empfangende vereinfacht wird.

Sebastian Klipper, Gründer und Geschäftsführer der CycleSEC GmbH mit Sitz in Hamburg und Lehrbeauftragter an der Wilhelm Büchner Hochschule (Hessen), ergründete in seinem humorvollen Vortrag den veränderten Menschentyp: Einen neuen, auf hoher Risikobereitschaft, mangelnder Voraussicht und Gefährdung eigener Gewinnchancen ausgelegten „Homo Carens Securitate“ - eine attraktive Zielscheibe für Angreifer. Er verdeutlicht damit die Abhängigkeit der Institutionen vom individuellen Verhalten und Urteilsvermögen der Mitarbeitenden, die sich täglich mit menschlichem Fehlverhalten, technischem Versagen oder vorsätzlichen Handlungen wie Sabotage und Spionage konfrontiert sehen können. Herr Klipper konstatierte, dass Sicherheitstechnologien, Prozesse und organisatorische Regelungen nahezu wertlos sein können, wenn die Beschäftigten diese nicht kennen, verstehen und korrekt anwenden können.

Prof. Dr. Stefan Schwarz, Leiter des Rechenzentrums der Universität der Bundeswehr München, berichtete in seinem Vortrag am darauffolgenden Tag von Erfahrungen und Ergebnissen von Untersuchungen zum konkreten Verhalten bei Phishing-Angriffen an der Universität der Bundeswehr München aus Sicht der IT auf die Endnutzenden. Seine Erfahrungen zeigten, dass ein Großteil der Nutzenden – darunter auch vermeintlich erfahrene – durch die üblichen Maßnahmen zur Awareness nicht oder nicht zielführend erreicht werden können. Allerdings weisen auch die technischen Maßnahmen zur IT-Sicherheit klare Grenzen auf, während die Gefährdung durch gezielte Angriffe auf die Nutzenden der Endgeräte stetig ansteige. Auch eine konkrete Sensibilisierung von Betroffenen zeige in der Regel nur kurzzeitige Wirkung. Er stellte Lösungen vor, mit denen sich durch zielgruppenorientierte und sich unregelmäßig wiederholende Simulation von gezielten Angriffen die Awareness der Anwendenden steigern und diese auch auf einem Mindestlevel halten lassen.

Oliver Pyka, freiberuflicher IT-Berater mit Sitz in Giebelstadt, stellte typische Problemfälle aus seiner Berufspraxis im Hinblick auf Sensibilisierung und Compliance aus Sicht der Systemadministratoren vor. Sie seien es schließlich, die permanent mit sensiblen Informationen umgehen und Zugriff auf Daten mit teils sehr hohem Schutzbedarf haben. Er verdeutlichte die Herausforderung, dass sich die Beschäftigten die damit einhergehende Verantwortung jeden Tag erneut ins Bewusstsein rufen. Wie es gelingen kann, diese Achtsamkeit dauerhaft auf einem hohen Level zu halten und welche fatalen Folgen es mit sich bringen kann, wenn dies nicht geschieht oder die passenden Rahmenbedingungen fehlen, erläuterte er in seinem Vortrag.

Andreas Schütz, wissenschaftlicher Mitarbeiter an der Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt, thematisierte Awareness bei der Nutzung von Mobilgeräten. Er präsentierte aktuelle Forschungsergebnisse hinsichtlich des Ist-Zustandes für mobile Sicherheit und verdeutlichte, dass Nutzerawareness kein Allheilmittel, wohl aber eine wichtige Maßnahme zum sicheren Umgang mit mobilen Endgeräten ist, sofern sie gezielt und überzeugend wirkt. Er plädierte für eine ganzheitliche Betrachtung, in der durch Prinzipien eines Risikomanagementsystems auch technische und organisatorische Rahmenbedingungen geschaffen werden müssen. Herr Schütz erklärte zum Abschluss, wie Erkenntnisse der Sozialpsychologie in Unternehmen genutzt werden können, um maßgeschneiderte Kampagnen zur Erhöhung der „Mobile Security Awareness“ zu erstellen.

Im letzten Vortrag sprach Michael Sauer, Leiter der IT am Manfred Donike Institut für Dopinganalytik e. V. und am Institut für Biochemie der Deutschen Sporthochschule Köln, über die Komplexität, die Entscheidungsebene in Institutionen für das Thema IT-Sicherheit zu interessieren und zu sensibilisieren, um eine erfolgreiche Umsetzung der nötigen Maßnahmen gewährleisten zu können. Er verdeutlichte eindrücklich die Wichtigkeit von Einfühlungsvermögen für das Gegenüber und Geduld, um die scheinbar einfachen technischen Sachverhalte zur Gewährleistung der IT-Sicherheit so an die Entscheidungsebene zu adressieren, dass dort die Einsicht zur Ressourcenfreigabe erzielt wird. Schließlich wird durch das bloße Benennen von Bedrohungen, Gefahren und

Risiken noch keine Überzeugung für die Sache hervorgerufen. Den Zuhörenden bot er mögliche Strategien für die Überzeugung von Vorgesetzten an und belegte diese mit Beispielen aus seiner Praxis.

Bei der Gelegenheit möchten wir uns nochmals ganz herzlich bei allen Beteiligten bedanken, die diese Veranstaltung mitgestaltet und deren Durchführung unterstützt haben.

Unser besonderer Dank gilt den Referenten.

Fußnote:

1 Die Forschungsgruppe von Prof. Volkamer inklusive Dr. Marco Ghiglieri ist von der TU Darmstadt an das KIT gewechselt.
https://secuso.aifb.kit.edu/Team.php

2 Forschungsgruppe Security, Usability, Society (SECUSO) des Karlsruher Instituts für Technologie (KIT), https://secuso.aifb.kit.edu/642.php

Nach beendeter Sanierung der Räume inkl. neuem Serverraum im V-Gebäude wurde gefeiert - mit Pizza !