

readme

Bulletin der UZH Alumni Informatik | Ausgabe 47/2022



Kalender

April 2022 – Dezember 2022

DI **26.04.22**

18.30–21.00 Uhr

Vortrag von Prof. Dr. Markus Stolze und
Dr. Susanne Schmidt-Rauch, FH OST:
«Product Manager UX oder Business
Analyst: Wer «ownt» die Requirements?»

 Fachhochschule OST Rapperswil
(beim Bhf), Gebäude 4, Raum 4.006a
mit Apéro

SO **22.05.22**

10.00–16.00 Uhr

Grosse 25-Jahr-Feier & 25. Alumni
Geburtstagsbrunch

 Cafeteria Seerose Irchel
Mitglieder und die ganze Familie

MO **13.06.22**

17.30–21.00 Uhr

Wanderung auf den Uetliberg

 Treffpunkt:
Haltestelle Triemli S10

FR **02.09.22**

18.00–23.55 Uhr

Alumni Sommernachtsparty
mit Special ShowAct

 Riithalle, Zürich
Mit PartnerIn

DO **03.11.22**

19.00–21.00 Uhr

Alumni Generalversammlung

 Migros Bank Zürich
Nur Mitglieder

MI **07.12.22**

18.30–23.00 Uhr

Fondue Plausch (kein Fussballabend)

 Sorell Hotel Zürichberg,
Orellistrasse 21, 8044 Zürich
Mit PartnerIn

Inhalt

Kalender 02

Editorial

Christian Schneider 03

Aus dem Präsidium

Brigitte Bailer 04

Neues aus dem IfI

Renato Pajarola 05

Cyber Security – Schweizer KMU unter Beschuss

Hauptthema 06–13

Cybersecurity Support for SMEs

Muriel Franco, Burkhard Stiller 08

Ransomware. Rechtliche Fragen bei Lösegeldzahlung

Roland Mathys 10

Ethical Hacking und Bug-Bounties für KMU

Peter Heinrich 12

Event: Digital Detox

Brigitte Bailer 15

Event: Sommernachtsparty

Rahel Kleiner 16

17. Beitrag zum Event Fondueplausch

Franziska Schait 18

Unsere Sponsoren und Partner 19

Impressum 19

Editorial

Von Christian Schneider

Liebe Alumni

In vielen Basiskursen zu Cyber Security wird zunächst nüchtern in eine mögliche Gliederung der Thematik in die CIA vorgenommen: Confidentiality, Integrity und Availability – die altbekannte CIA-Triade, welche drei wichtige Teilbereiche der Cyber Security beschreibt. Unlängst ist vielen von uns jedoch bekannt, dass es sich dabei nicht um ein verstaubtes Thema oder ein theoretisches Konstrukt handelt. Medienberichte zeigen, wie bekannte, renommierte Unternehmen Opfer von Angriffen werden – andere kommen Angriffe teuer zu stehen. Bei grösseren Unternehmen wird Cyber Security oft sehr ernst genommen, ist längst institutionalisiert, und Teil der betrieblichen Abläufe.

Für KMU, deren Tätigkeitsschwerpunkt nicht in der Cyber Security liegt und deren Kerngeschäft die Aufmerksamkeit des Managements stark beansprucht, ist Cyber Security eine besondere Herausforderung, weil auch sie Opfer von Angriffen werden und konkrete Massnahmen Expertise benötigen. Cyber Security ist, so glaube ich, zudem kein Motivator sondern ein Hygienefaktor: Bei vielen Verantwortlichen weckt das Thema keine Freude. Jedoch umso mehr Frustration, sollte es einmal zu einem Angriff kommen.

Für die readme Redaktion ein relevantes Thema. Es freut mich deshalb, dass wir zu Cybersecurity in KMUs vielseitige Beiträge aus unserer Community zusammenstellen konnten: Prof. Dr. Burkhard Stiller und Muriel Franco zeigen Tools und Ansätze auf, an welchen sie an der Communication Systems Research Group des IfI UZH geforscht haben. Roland Mathys gibt Einblicke über rechtliche Fragen bei Lösegeldzahlungen und Dr. Peter Heinrich berichtet von Ethical Hacking sowie Bug-Bounties für KMU.

Ich wünsche euch eine gute Lektüre und verbleibe mit besten Grüssen aus der readme Redaktion
Christian



Christian Schneider

ist seit 2020 bei der LGT Bank als IT Solution Engineer tätig. Dort arbeitet er in der Parametrierung der Core Banking Plattform. Er hat mehrere Jahre Erfahrung als IT Consultant mit den Schwerpunkten Solution Design, Implementierung und Test Engineering. Christian schloss 2018 seinen Master in Wirtschaftsinformatik an der Universität Zürich ab und übernahm 2020 die Redaktion des readme im Alumni Informatik.

► christian.schneider@alumni.ch

Aus dem Präsidium

Von Dr. Brigitte Bailer

Liebe Alumna, Lieber Alumnus

Seit kurzem sind wir von Auflagen bezüglich unserer Events wieder befreit. Der Vorstand freut sich sehr auf eine organisatorisch etwas einfachere und entspanntere Zeit, gerade im 2022. Denn 2022 feiern wir unser 25-jähriges Bestehen. Die GV vom November hat aus diesem Grund einen Bezug aus unserem ansehnlichen Vereinsvermögens bewilligt. Wir werden also z.B. unseren Geburtstagsbrunch grosszügiger gestalten und auch sonst an unseren Apéros oder Events das silberne Jubiläum gebührend begehen.

Merkt euch schon mal den Sonntag, 22. Mai 2022: Dann treffen wir uns an unserem Geburtsort am Irchel. Dort, im allerersten Gebäude, in dem das Ifl am Irchel logierte, wird heute eine grosse Bar mit Umschwung betrieben. Esther Rölly (Bild), Eventmanagerin und zuständig für den Geburtstagsbrunch, hat ein grossartiges Programm zusammengestellt, dass Kinder und Erwachsene erfreuen wird. Musik, Theater, Lehrpfad, feines Essen und ein bisschen Nostalgie erwarten uns.

Unsere drei noch neueren Vorstandsmitglieder, Christian Schneider, Marc-André Pradervand und Sinja Christiani haben bereits wesentliche Pflöcke eingeschlagen. Christian ist im Profimodus für das readme angekommen. Es gelingt ihm, gehaltvolle und ansprechende readmes zu gestalten (Bild), die auch durch Dritte, etwa am WWF Jahresevent, rege gelesen werden. Marc-André hat in Zusammenarbeit mit unserem alteingessenen Strategie- und Kommunikationschef Kornél Szabó ein umfassendes Partnerprogramm für Firmen auf die Beine gestellt. Details dazu folgen. Und Sinja wickelt unsere Finanzen ohne jegliche Reibungsverluste ab. Bereits schüttelt sie mahnend den Kopf,

wenn wir geldmässig überborden. Nathan Labhart hält derweil als erfahrener Vorständler das Ifl für uns auf Trab und umgekehrt. Merkt euch schon mal den 3. September 2022. An diesem Samstag kann auch euer Nachwuchs am «Alumni & Family»-Tag das Programmieren am Ifl ausprobieren.

Und ganz aktuell wissen wir seit der letzten Vorstandssitzung, dass Nicola Fantini sein letztes Vorstands Jahr mit uns verbringt. Nach 25 Jahren und von Beginn weg im Vorstand, wird er in seiner Bündner Heimat intensiver denn je gebraucht. Wir bedauern seinen Rücktritt sehr und danken ihm herzlich für all die unvergessenen Events wie etwa unseren beliebten Fondueplausch, den er Jahr für Jahr auf die Beine gestellt hat. Es gilt also, auf die GV im November eine Nachfolge für ihn zu finden. Wer Interesse hat, spricht oder schreibt mich oder ein anderes Mitglied unseres Vorstands doch direkt an

Herzliche Grüsse
Eure Präsidentin
Brigitte



Dr. Brigitte Bailer

ist Mitinhaberin und Geschäftsführerin der Basec Software AG. Sie berät seit vielen Jahren Unternehmen in der Gestaltung ihrer Wertschöpfungskette unter optimalem Einsatz der Informatik, ist aktuell Verwaltungsrätin der Enea-Gruppe für Landschaftsarchitektur und Stiftungsrätin bei der Swiss Life. Seit 2018 präsidiert sie den UZH Alumni Informatik.

► brigitte.bailer@alumni.ch



Neues aus dem IfI

Von Prof. Dr. Renato Pajarola

Liebe Alumnae, liebe Alumni

Wir freuen uns, dass wir mit Präsenzmodus ins Frühlingssemester 2022 starten konnten. Die Normalisierung des gesellschaftlichen Lebens in der Schweiz scheint nun absehbar zu sein. Was auch immer diese Normalität dann langfristig sein wird.

Wie werden wir wohl in zehn Jahren auf die Corona-Pandemie zurückblicken, eine Zeit, in der wir uns in Geduld und Flexibilität geübt haben? Welche der erprobten Neuerungen werden sich als nachhaltig erweisen? Gehören im Jahr 2032 hybrides Arbeiten, digitale Lehre und Walking Meetings zu unserem Alltag?

Vorerst eine Rückschau auf ein paar herausragende Leistungen. Die Ehrung «Test of Time Award» wird jeweils von der ESES/FEC verliehen, der European Software Engineering Conference and Symposium on the Foundations of Software Engineering. Einflussreiche Beiträge im Bereich Software Engineering werden mit diesem Award gewürdigt, wenn sie auch noch zehn Jahre nach ihrer Veröffentlichung durch nachhaltige Wirkung hervorstechen. Wir freuen uns besonders, dass wir im letzten Herbst den «Test of Time Award» gewonnen haben. Prof. Harald Gall war Co-Autor der ausgezeichneten Studie «Don't touch my code!: examining the effects of ownership on software quality».

Ebenso erfreulich ist, dass Prof. Harald Gall und sein Postdoc Pasquale Salza einen SNF Grant erhalten haben und zwar für ihr Projekt «Melise – Machine Learning Assisted Software Development». Und ein weiterer IfI-Professor hat einen SNF Grant gewonnen! Zusammen mit zwei Forschenden der TU Delft konnte Alberto Bacchelli das Projekt «Software Engineers as Quality Experts» erfolgreich starten – mit einer Unterstützung von über CHF 762'903.

Prof. Jürgen Bernard, der schon im letzten Juni den «Young Researcher Award» der Eurographics Association erhielt, wurde an der IEEE Vis Conference mit dem Best Paper Award ausgezeichnet. Den Preis erhielt er für ein Data-Science-System, welches von BMW dazu verwendet wird, den Herstellungsprozess von elektrischen Motoren zu verbessern.

Ingo Scholtes, seit August 2018 SNF-Professor für Data Analytics am IfI, ist im Oktober einem Ruf an die Julius-Maximilians-Universität Würzburg gefolgt. Der neu eingerichtete Lehrstuhl ist innerhalb des «Center of Artificial Intelligence and Data Science» angesiedelt. Im Rahmen seiner SNF-Professur zu «Next-Generation Network Analytics for Time Series Data» bleibt uns Ingo glücklicherweise weiterhin verbunden.

Auch bei unseren Nachwuchsforschenden hat sich Erfreuliches getan. Für sein Projekt «MediaGraph» hat Luca Rossetto, Postdoc von Prof. Avi Bernstein, einen SNF Ambizione Grant erhalten. Und Anfang Jahr vergab die Digitalisierungsinitiative

der Zürcher Hochschulen (DIZH) einen Rapid Action Grant an André Meyer. André Meyer ist ehemaliger Doktorand von Prof. Thomas Fritz und verantwortet das Projekt «FlowLight».

Und zum Schluss wagen wir doch einen Blick in die Zukunft! Wir freuen uns, wenn in zehn Jahren einige Studentinnen am IfI studieren, weil sie am 11. Februar 2022 das spezielle MINT-Angebot der Universität Zürich besuchten und ihre Begeisterung für Naturwissenschaften und Technik nachhaltig geweckt wurde. Warum genau an diesem Datum? Am 11. Februar wird jeweils der «Internationale Tag von Frauen und Mädchen in der Wissenschaft» gefeiert: Ein Tag, an dem Frauen und Mädchen ermutigt werden sollen, sich für ein Studium und eine Karriere in den MINT-Fächern zu entscheiden. Anlässlich dieses Internationalen Tages der Vereinten Nationen organisierte das IfI Workshops und Führungen in Kooperation mit den drei MNF-Partnern Science Lab, Science Exploratorium und National Point of Contact for Satellite Images. Das Angebot reichte von Programmieren über Big Data und Forschung am Cern bis zu Erdbeobachtung. Insgesamt haben fast 70 Teilnehmerinnen dieses erstmalige Angebot besucht und an der Universität Zürich MINT-Luft geschnuppert.

In diesem Sinne – bleiben wir hoffnungsfroh!

Mit besten Wünschen

Euer Renato Pajarola

Wir freuen uns wenn ihr uns weiterhin auf Social Media folgt:

www.facebook.com/uzh.ifi

www.instagram.com/uzh_ifi



Prof. Dr. Renato Pajarola

studierte an der ETH Zürich Informatik und absolvierte dort auch sein Doktorat, welches er 1998 abschloss. Anschliessend war er für ein Jahr Postdoc am Georgia Institute of Technology und ab 1999 Assistenzprofessor an der University of California Irvine. Seit 2005 ist er Professor am Institut für Informatik an der Universität Zürich, wo er seit dem 1. August nun auch Institutsdirektor ist. Renato Pajarolas Forschungsinteressen liegen in den Bereichen Visual Computing, 3D Computergrafik, interaktive Datenvisualisierung und Geometry Processing.
► pajarola@ifi.uzh.ch



Cyber Security

Schweizer KMU unter Beschuss

- 08 | Cybersecurity Support for SMEs
*How SMEs can address challenges
in Cybersecurity*
Muriel Franco, Burkhard Stiller
- 11 | Ransomware
Rechtliche Fragen bei Lösegeldzahlung
Roland Mathys
- 12 | Ethical Hacking und Bug-Bounties für KMU
Im Austausch mit «freundlichen» Hackern
Peter Heinrich

Cybersecurity Support for SMEs

Von Muriel Franco und Prof. Dr. Burkhard Stiller

The Cybersecurity Landscape and The Situation of SMEs

Many of the problems plaguing cybersecurity are not only of technical nature, but of economic nature. The primary motivation (besides espionage and destruction) behind cyberattacks is making financial profits. On one hand, for example, ransomware attacks ask for money from their victims to recover their data, stolen data are sold in illegal markets, and Denial-of-Service (DoS) attacks are being used for extortion. On the other hand, companies' lack of knowledge to assess risks and potential impacts of cyberattacks trigger alerts worldwide. This problem is prevalent in companies with a small budget available to mitigate cybersecurity weaknesses, and typically they lack at the same time technical security expertise, which holds especially true for Small- and Medium-sized Enterprises (SME) and micro-companies.

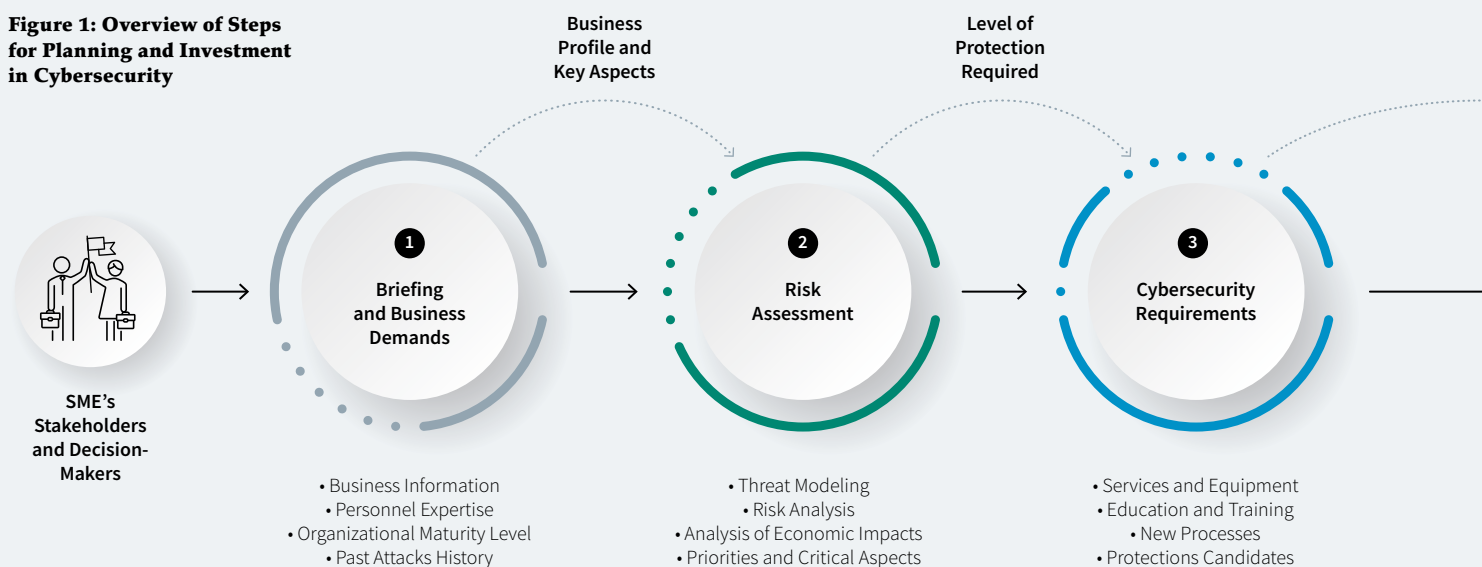
Unfortunately, SMEs frequently neglect approaches to handle cybersecurity issues, primarily due to the lack of economic and technical resources, including an insufficient budget, missing personnel skills, and minimal cybersecurity knowledge. Besides that, many SMEs falsely think that they are not a target for cybercrime. The realistic scenario is exactly the opposite, where cybercriminals tend to see SMEs as a preferred target due to a higher likelihood of success in the case of a cyberattack. Therefore, it

is highly relevant that cybersecurity initiatives, guidelines, and solutions address explicitly those challenges SMEs are facing. In the short term, education and cybersecurity awareness are also key to reducing the number of successful attacks against these companies, since expertise becomes available and applicable.

Key Steps for Cybersecurity Planning

Figure 1 exemplifies relevant steps and techniques for an efficient cybersecurity planning and deployment of effective cybersecurity strategies in SMEs. These steps and techniques are summarized and organized as a framework, starting in Phase A, where all information related to the business itself is collected, and a briefing is conducted with all stakeholders involved. Phase B is focused on the security analysis and threat modeling of this company under investigation. Different approaches can be considered, such as using well-known cybersecurity products and specific penetration tests. Also, more specific steps related to the risk assessment with economic bias can be followed, as proposed by the SEconomy framework^[1]. Lastly, with the relevant security information at hand, Phase C consists of the definition of cybersecurity requirements, the mapping of processes that must be modified or created within that company, and the

Figure 1: Overview of Steps for Planning and Investment in Cybersecurity



Example Values of Costs and Benefits Calculated by the SECAdvisor Tool

	Customers	Internal Operations	External Operations	Total	Without Segmentation	Economic Benefits of Information Segmentation
Value of Information	120'000'000	60'000'000	20'000'000	200'000'000	200'000'000	–
Calculated Vulnerability	40%	20%	10%	–	31%	–
Expected Loss Before Additional Investments	48'000'000	12'000'000	2'000'000	62'000'000	62'000'000	–
Optimal Investment	2'280'000	788'528	180'000	3'248'528	3'321'363	72'835
Expected Loss with Optimal Investment	2'400'000	848'528	200'000	3'448'528	3'521'364	72'836
Total Cybersecurity Costs	4'680'000	1'637'056	380'000	6'697'056	6'842'727	145'671

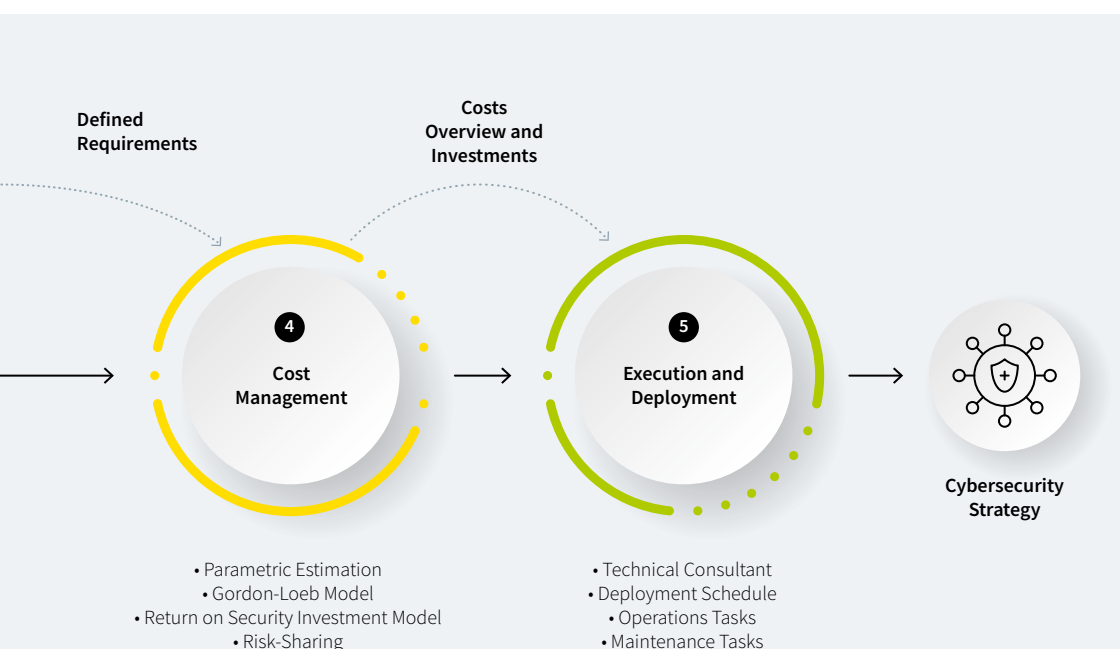
definition of training required to implement, deploy, and operate the cybersecurity strategy. After all, the information is mapped, and all relevant cybersecurity requirements are defined, e.g., the main goal, acceptable levels of protection, and risks that can be assumed.

Within the Cost Management phase (Phase D) cybersecurity costs are estimated, and the optimum investment amount is defined. For that, cybersecurity economics models can be used, such as the Gordon-Loeb model, to estimate the optimal investment in cybersecurity and the Return On Security Investment (ROSI) for calculating the payback and cost-efficiency of a given cybersecurity solution. Finally, the cybersecurity strategy can be deployed within Phase E to protect the company and its supply chain against further threats, thus, reducing the chances of business disruption and financial impacts due to cyberattacks. These steps of the framework do offer structured help to cybersecurity consultants, since it is not trivial to obtain all these information without prior experience in that field and the company.

How Much Should My Company Invest in Cybersecurity? Insights from the SECAdvisor Tool

Based on these different needs identified and current market trends, it is possible to identify a demand for approaches that simplify cybersecurity planning and to provide an intuitive way to assess risks and make cost-effective decisions, especially to support the adoption of cybersecurity measures by SMEs. This is the case with SECAdvisor^[2], a visual tool developed within the Communication Systems Research Group CSG at the Department of Informatics IfI of the University of Zurich UZH as part of Christian Omlin's Bachelor Thesis. The idea and motivation behind this tool are to consolidate the knowledge obtained along the research and discussions on this topic conducted by the CSG within the European community as part of Task 4.3 "Economics Perspective", being part of the cybersecurity project H2020 CONCORDIA.

SECAdvisor allows for the definition of information segments within a company and calculates the optimal investment for each segment, including potential losses with and without an



optimal investment in cybersecurity. This calculation uses the Gordon-Loeb model and considers security breach probability functions to estimate values as accurate as possible. After calculating an overview of the amount of funds in cybersecurity, SECAdvisor recommends protection measures. ROSI is calculated for each solution recommended to compare different protection options in terms of payback or cost-effectiveness. Table 1 overviews in an example relevant costs and investments calculated by SECAdvisor for the three determined database segments (especially "Customer", "Internal Operations", and "External Operations"). These outcomes are based on the Gordon-Loeb approach and are suggested to be used to guide precise investments in cybersecurity.

Thus, solutions like SECAdvisor can benefit SMEs around the globe in better planning and investment decisions in cybersecurity, while they also support the analysis of possible financial losses due to a successful cyberattack. Besides cybersecurity solutions, key investments have to be made to increase cybersecurity staff and promote more cybersecurity awareness for their general employees. Also, companies have to ensure that they can detect and mitigate cyberattacks effectively, with a clear cybersecurity strategy tailored for the reality of the company, e.g., targeting personnel culture, size, sector, and budget, while covering all relevant facets of cybersecurity, i.e., detection, mitigation, and recovery plans.

- [1] Bruno Rodrigues, Muriel Franco, Geetha Parangi, Burkhard Stiller: SEconomy: A Framework for the Economic Assessment of Cybersecurity; 16th Conference on the Economics of Grids, Clouds, Systems, and Services (GECON 2019), Leeds, UK, September 2019, pp 1-13. URL: http://www.gecon.info/articlesgecon2019/no13_paper31.pdf
- [2] Christian Omlin, Muriel Franco: SECAdvisor: a Visual Tool for the Support of Cybersecurity Investments; January 2022, URL: <https://gitlab.ifi.uzh.ch/franco/secadvisor>



Muriel Franco

is a Junior Researcher and PhD candidate in Informatics within the Communication Systems Group CSG of the Department of Informatics IfI. Muriel has been participating and driving cybersecurity-related projects within a team of networking, security, and economic researchers. Muriel holds a BSc and MSc in Computer Science from Brazil.

► franco@ifi.uzh.ch



Prof. Dr. Burkhard Stiller

leads the Communication Systems Group CSG since 2004 and had been with before with the University of Karlsruhe, Germany, the Computer Lab at Cambridge University, U.K., ETH Zürich, Switzerland, and the University of Federal Armed Forces Munich, Germany. His research areas include fully decentralized systems, network and service management, and communication economics.

► stiller@ifi.uzh.ch

Ransomware: Rechtliche Fragen bei Lösegeld- zahlung

Von Roland Mathys

Ransomware stellt die am meisten verbreitete Kategorie von Cyberattacken dar. Hierbei werden Daten und IT-Systeme des Opfers durch die Angreifer verschlüsselt. Für die Entschlüsselung wird ein Lösegeld (Ransom) verlangt. Bei der Frage, ob Ransom bezahlt werden soll, spielen neben grundsätzlichen auch rechtliche Überlegungen eine wichtige Rolle. Hierauf wird im Folgenden eingegangen.

Generelle Vorbehalte gegenüber der Bezahlung von Ransom

Das nationale Zentrum für Cybersicherheit (NCSC) als auch Strafverfolgungsbehörden raten von der Bezahlung von Lösegeld bei einer Ransomware-Attacke grundsätzlich ab. Begründet wird dies in erster Linie mit drei Überlegungen: Zunächst biete die Zahlung von Ransom keine Gewähr für den Erhalt der Mittel zur Datenentschlüsselung; Erfahrungswerte zeigen jedoch, dass in etwa 90 % der Fälle die Schlüssel effektiv zur Verfügung gestellt werden, womit dieses Argument nicht greift.

Stichhaltiger ist demgegenüber die Begründung, dass mit einer Lösegeldzahlung das von den Cyberkriminellen betriebene System finanziell unterhalten und gefördert



werde. Auch das Argument, dass ein Unternehmen durch Zahlung von Ransom zu einem attraktiven Zielobjekt für Wiederholungstäter und Nachahmer werde, muss ernst genommen werden, jedenfalls dann, wenn die Namen der zahlungswilligen Unternehmen (z.B. im Darknet) herumgereicht werden.

Die Qual der fehlenden Wahl

Trotz dieser Bedenken haben die von einer Ransomware-Attacke betroffenen Unternehmen oftmals kaum eine andere Wahl, als auf die Lösegeldforderung einzusteigen. Dies trifft vor allem dann zu, wenn nicht nur die produktiven Daten, sondern auch die Backups verschlüsselt wurden. Sofern in solchen Situationen eine Datenrekonstruktion überhaupt möglich wäre, wird sie häufig aufwändiger und damit teurer sein als eine Lösegeldzahlung. Selbst Unternehmen mit aktuellem und unverschlüsseltem Backup werden dann eine Zahlung von Ransom erwägen, wenn ihre Daten von den Angreifern nicht nur verschlüsselt, sondern auch exfiltriert wurden und deren Veröffentlichung (z.B. im Darknet) angedroht wird.

Muss eine Lösegeldzahlung in Betracht gezogen werden, stellen sich für das betroffene Unternehmen primär zwei Fragen: Spricht aus rechtlicher Sicht etwas gegen eine Zahlung, d.h. ist eine Zahlung unzulässig oder gar strafbar? Und kann das Unternehmen sich für die Zahlung bei seiner (Cyber)Versicherung schadlos halten, d.h. kommt diese für das Lösegeld auf?

Rechtliche Zulässigkeit von Ransom-Zahlungen

Eine Lösegeldzahlung kann zunächst gegen das Strafgesetzbuch verstossen. In Frage kommen hierbei vorab die Tatbestände der Unterstützung einer kriminellen oder terroristischen Organisation, der Terrorismusfinanzierung, der Begünstigung oder der Geldwäscherei. Obwohl eine Ransom-Zahlung bei strikter Betrachtung eine finanzielle Unterstützung darstellt, ist eine Zahlung durch das Opfer einer Cyberattacke (oder zu dessen Gunsten) nicht strafbar. Für eine Terrorismusfinanzierung fehlt es unter anderem an der hierfür erforderlichen Absicht. Auch eine Begünstigung liegt nicht vor, werden durch die Zahlung Strafverfolgung und -vollzug doch nicht vereitelt oder erschwert – im Gegenteil kann die die Spur einer Lösegeldzahlung in Kryptowährung zu den Angreifern führen. Für Geldwäscherei schliesslich müssen die fraglichen Vermögenwerte aus krimineller Tätigkeit stammen, was in Bezug auf das Opfer der Cyber-Attacke kaum der Fall sein wird.

Demgegenüber kann die Zahlung von Lösegeld an Cyberkriminelle unter die Tätigkeiten fallen, die durch Sanktions- und Embargovorschriften untersagt werden. In den meisten Fällen bleiben die Angreifer anonym, womit ein Verstoß gegen solche Vorschriften kaum dargetan werden kann und das Risiko entsprechend gering ausfällt. Ist die Identität der Cyberkriminellen (bzw. von deren Organisation oder des dahinterstehenden Staats) jedoch bekannt, sollte geprüft werden, ob der Empfänger der Ransom-Zahlung auf einer Sanktionsliste aufgeführt ist. In jedem Fall empfiehlt sich in solchen Fällen eine vorgängige Absprache mit den hierfür zuständigen Behörden.

Versicherungsdeckung

Kommt eine (Cyber)Versicherung für eine Lösegeldzahlung auf? Dies hängt von der Versicherungspolice und von den gedeckten Schadenskategorien ab. Soweit ersichtlich verfolgen die Versicherer hierbei keine einheitliche Linie, und das Spektrum reicht von gänzlichem Ausschluss bis zu vollständiger Deckung. Deckungsumfang und -voraussetzungen sollten deshalb möglichst frühzeitig geklärt werden, um keine negativen Überraschungen zu erleben.



Roland Mathys

ist Rechtsanwalt und Partner bei Schellenberg Wittmer Rechtsanwälte in Zürich, wo er das Technologie- und Datenrechtsteam leitet. Er hat an der Universität Zürich Wirtschaftsinformatik und in Basel Recht studiert. Cybersecurity zählt zu den Schlüsselgebieten seiner rechtlichen Beratung. Das Spektrum juristischer Dienstleistungen reicht dabei von präventiven Massnahmen (z.B. Vertragsprüfung hinsichtlich Mindestanforderungen an Cybersicherheit) bis hin zur Unterstützung bei Eintritt eines Cybervorfalles (z.B. Meldung von Datenschutzverletzungen an Behörden).

► roland.mathys@swlegal.ch



Ethical Hacking und Bug-Bounties für KMU

Von Dr. Peter Heinrich

Ethical Hacking oder: David für Goliath

Seit es um Sicherheit in IT-Systemen geht, wird darüber zwischen zwei philosophischen Lagern gestritten. Eine Seite sieht die grössten Erfolgsaussichten darin, sich mit immer mehr Technologie zu schützen und dabei die Spezifika möglichst geheim zu halten («Security by Obscurity»). Dies kommentierte der legendäre Bruce Schneier bereits vor über zwanzig Jahren wie folgt: «Wenn Sie glauben, Technologie könne Ihre Sicherheitsprobleme lösen, dann verstehen Sie die Probleme nicht und Sie verstehen die Technologie nicht.»

Das andere Lager erkennt an, dass Sicherheit immer nur relativ und vor allem temporär ist: man ist so lange sicher, bis man es nicht mehr ist. Die Hypothese der eigenen Unverwundbarkeit sollte daher regelmässig überprüft werden.

Aufgrund der zunehmend erfolgreichen Hackerangriffe auf sogenannte (oder so gedachte) «sichere Infrastrukturen» erstaunt es nicht, dass letztere Sichtweise immer populärer wird. Dies hängt auch mit dem wachsenden Angebot entsprechender Instrumente zusammen – insbesondere dem «Ethical Hacking».

Ethical Hacker überprüfen die Sicherheit von IT-Systemen im Auftrag der verantwortlichen Organisationen. Im Gegensatz zu ihren kriminellen Pendants, die meist auf Zerstörung, Diebstahl oder Erpressung aus sind, möchten Ethical Hacker genau dies verhindern – sie suchen und finden potenzielle Schwachstellen, damit diese geschlossen werden, bevor sie von Kriminellen ausgenutzt werden können.

Entlohnt werden Ethical Hacker oft nach Menge und Qualität der aufgespürten Schwachstellen – aber nicht nur: neben der Anerkennung in der eigenen Community steht hinter der Tätigkeit häufig auch die hohe intrinsische Motivation, Gutes zu tun. Damit geht der Ethical Hacker auch bereitwillig das Risiko ein, keine Schwachstelle zu finden und damit für seine angefallene Arbeit nicht entlohnt zu werden.

Ethical Hacking wird auch in der Schweiz seit einigen Jahren vermehrt genutzt – insbesondere Grossunternehmen lassen sich bewusst von den hochspezialisierten Davids mit Steinen bewerfen, um herauszufinden, ob sie tatsächlich getroffen werden können und wenn ja, wo es wehtun könnte und wie sehr.

Ethical Hacker und Klein(st)-Organisationen: David für David?

Während Angriffe auf die IT für Grossunternehmen Alltag geworden sind, sind zunehmend auch KMU und kleine Organisationen der öffentlichen Verwaltung betroffen. Gerade bei Gemeinden kommt dies nicht von ungefähr: sie sammeln, verarbeiten und verwalten viele sensible Daten von Bürgerinnen und Bürgern und werden daher immer öfter gezielt angegriffen.

Umgekehrt handelt es sich bei Gemeinden meist um kleine Organisationen mit entsprechend wenig IT-Ressourcen und Know-how – beides (gute) Gründe, warum sie heute noch wenig mit Ethical Hackern in Berührung kommen.

Genau das möchten wir an der ZHAW in Zusammenarbeit mit Bug Bounty Switzerland ändern. Gemeinsam erarbeiten wir in einer von Innosuisse geförderten Vorstudie derzeit die Grundlagen, um die Plattform von Bug Bounty Switzerland – einem führenden Schweizer Ökosystem für ganzheitliches Schwachstellenmanagement und für die Zusammenarbeit mit ethischen Hackern – auch für KMU und die öffentliche Verwaltung zugänglich und erschwinglich zu machen.

Das Konzept setzt dabei auf zwei Seiten auf Ausbildung: zum einen sollen kleine Organisationen über den Austausch mit freundlichen «Angreifern» mehr über ihre eigenen Sicherheitsprobleme und deren Lösung lernen. Zum anderen soll dies auch für unerfahrene Hacker eine Möglichkeit zum Lernen bieten – schliesslich ist nicht nur die insgesamt Nachfrage an «Ethical Hacks» in der Schweiz noch überschaubar, sondern auch das Angebot an fähigen Hackern.

Ein weiterer wichtiger Aspekt, der dabei ausgelotet werden soll, liegt in adäquaten Finanzierungs- und sozialen Entlohnungsmodellen, die sich zum Beispiel an der Grösse und den finanziellen Möglichkeiten der Organisationen orientieren und bei den Hackern für die richtigen Anreize sorgen.

Sie interessieren sich für Ethical Hacking und Bug Bounty? Machen Sie mit!

Egal, ob Sie eine grosse oder kleine Organisation sind (privat oder öffentlich), oder Hacker bzw. Security-Spezialist – wenn Sie bei der weiteren Entwicklung der Plattform mitmachen wollen (ob als Ideengeber, Testkunde, etc.), melden Sie sich gerne bei: peter.heinrich@zhaw.ch. Wir freuen uns auf Sie!



Dr. Peter Heinrich

leitet an der ZHAW die Fachstelle für Prozessmanagement und Informationssicherheit am Institut für Wirtschaftsinformatik. Zuvor hat er an der Universität Zürich am IFI promoviert. Primär forscht und lehrt Peter Heinrich im Bereich der Informationssicherheit insbesondere mit dem Fokus auf Klein- und Kleinstunternehmen.

► peter.heinrich@zhaw.ch

Wie finde ich die richtige Weiterbildung?

Kostenloser Ratgeber: Die richtige Weiterbildung finden

- » In 4 Schritten zur passenden Weiterbildung
- » Info-Grafik und Beschreibung zum Schweizer Bildungssystem



Ratgeber kostenlos herunterladen:
[www.ausbildung-weiterbildung.ch/
ratgeber-richtige-weiterbildung](http://www.ausbildung-weiterbildung.ch/ratgeber-richtige-weiterbildung)





Event: Digital Detox

Von Dr. Brigitte Bailer

Event 15



Event: Sommer- nachtsparty

Von Rahel Kleiner

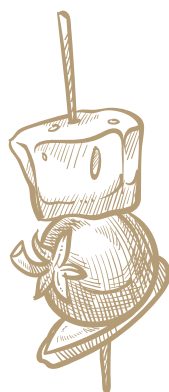
Unterhaltsamer Service

Die Maske fiel sofort auf. Sie war höchst sonderbar mit dem transparenten Einsatz in der Mitte, durch den man den rot geschminkten Mund sah. Die resolute Serviceangestellte, die sie trug, war weit weniger freundlich als die anderen Angestellten und auch beim Servieren wirkte sie weniger professionell. Wir tippten auf Notfallaushilfskraft. Doch als sie mit grosser Ernsthaftigkeit das Menu vorstellte und auch auf die speziellen Wünsche von Flexitariern und die Probleme von Peperoniunverträglichkeiten einging, dämmerte uns langsam, dass dies doch eher eine Komikerin ist. Ein Blick ins Programm, wo stand «mit Unter-

haltung», aber kein Hinweis auf die Art dieser Unterhaltung, gab uns die Gewissheit. Und sie war nicht alleine. Ihre Kollegin fiel durch ihre Grösse auf und versuchte uns im Laufe des Abends überteuerte Wochenendkurse zur Chakraöffnung zu verkaufen oder einen reichen Partner für ihre Kollegin anzuwerben. Meines Wissens beides erfolglos.

Kochkunst und anschliessender Wettbewerb

Auch der kulinarische Teil des Abends war sehr gelungen. Schon die Aperohäppchen luden zum Sattessen ein, was schade gewesen wäre um die Gazpacho (trotz eingemixter Peperoni),





den Gemüsesalat mit Gemüsesmoothie (nicht zu verwechseln mit Salatsauce), das butterzarte Rindsfilet und das Dessert mit weisser Schokoladenerde.

Das fleissige Ausfüllen des Wettbewerbs kombiniert mit gutem Raten sowie flinkem Navigieren auf der Webseite des Sponsors NSM Engineering AG wurde dieses Jahr mit vielen leckeren Spezialitäten aus dem Bündnerland und der Ostschweiz belohnt, organisiert von unseren Vorstandsmitgliedern.

Den gelungenen Abend liessen die letzten mit unsäglich süffigen, mit viel Liebe und noch mehr Zeit gemixten Amaretto Sours ausklingen.





Event Fondueplausch

Von Franziska Schait

Der Fondueplausch war trotz der damals noch angespannten Situation ein geselliger Abend, wo sich viele neue Mitglieder getroffen haben und rege Kontakt geknüpft wurde. Mit dem Fondue-Pop-Up beim Hotel Sorell am Zürichberg fand er erstmals in neuer Umgebung statt.

Schon beim kurzen Fussmarsch von der Tramstation zum Sorell-Hotel war klar, dass die marschierenden Gruppen und Einzelpersonen wohl das gleiche Ziel im Auge hatten. Informatikerinnen und Informatiker erkennen Artgenossen ja bekanntlich schon von Weitem. 😊

Im äusserst heimeligen Chalet wurden wir vom Vorstand mit einem Apéro herzlich willkommen geheissen.

Neben dem Intro-Wein konnten wir uns über eine sehr umfangreiche und schmackhafte Fleisch- und Käseplatte freuen. Obwohl der grösste Hunger danach – zumindest bei mir – gestillt war, ging es mit einem feinen Fondue weiter, begleitet von einem scheinbar nie enden wollenden Weinangebot. Ein zum Glück etwas leichteres Dessert rundete das Essen ab.

Nach diesen üppigen Runden waren wir schon fast dankbar, dass uns das Tram unserer Wahl vor der Nase abfuhr. Also legten wir, bestens gelaunt, noch einen kleinen gemeinsamen Verdauungsspaziergang zur nächsten Tramstation ein, ehe wir uns zufrieden auf den individuellen Heimweg machten. Schön, dass ein solch unterhaltsamer Anlass trotz der schwierigen Situation durchgeführt werden konnte. Bis zum nächsten Jahr!

Unsere Sponsoren und Partner

Das vielfältige Angebot der UZH Alumni Informatik wäre ohne die tatkräftige Unterstützung unserer Sponsoren und Partner nicht möglich. Ihre Unterstützung erlaubt uns, unsere Aktivitäten frühzeitig zu planen und mit attraktivem Inhalt durchzuführen. Weitere Informationen findet ihr auf www.alumni.ch («Sponsoren & Partner»).

Premiumsponsor



NSM ist ein Schweizer Software Engineering Unternehmen mit Hauptsitz in Baar und eigenen Nearshore-Entwicklungszentren in Serbien und Rumänien. Erfahrene und professionelle Solution Architects, Engineers und Projektleiter schaffen täglich Mehrwert für anspruchsvolle Kunden.

330 Mitarbeiter, verteilt auf 6 Standorte, entwickeln in optimal zusammengestellten Teams komplexe Software-Lösungen für namhafte Kunden mit hohen Anforderungen.

Kontakt: Oliver Marjanovic
www.nsm-engineering.com

Basissponsor



Das Schweizer Bildungsportal

Die Modula AG betreibt das Bildungsportal Ausbildung-Weiterbildung.ch, welches sich in den letzten Jahren zur führenden Bildungsplattform innerhalb der beruflichen Erwachsenenbildung der Schweiz entwickelt hat. Das Bildungsportal bietet zahlreiche Informations- und Entscheidungshilfen für die Wahl des richtigen Bildungsangebots und der passenden Schule.

Als Alumni findest du rasch den gewünschten Lehrgang, Kurs oder ein Angebot aus dem Bereich berufliche Neuorientierung.

Kontakt: Stefan Schmidlin
www.ausbildung-weiterbildung.ch

Partner



Die Goldwyn Partners Group AG ist ein seit über 20 Jahren etabliertes Beratungsunternehmen für die gezielte nationale Suche und Vermittlung von Fach- und Führungskräften schwerpunktmässig im IT- und Finanzumfeld. Wir sind tätig für ein hochkarätiges Portfolio führender nationaler und internationaler Unternehmenskunden. Einmal jährlich führt die Goldwyn Partners Group AG für Mitglieder der UZH Alumni Informatik ein kostenloses Video-Bewerbungstraining durch.

Kontakt: Gaby Hürlimann, gh@goldwynpartners.com
www.goldwynpartners.com

Eventpartner



Der Migros-Gründer Gottlieb Duttweiler legte der Migros Bank bereits 1958 seine einzigartige und starke Werthaltung zugrunde, den Menschen statt des Kapitals ins Zentrum des eignen Handelns zu stellen. Seitdem ist es unser Ziel und unser Auftrag, Menschen, die ideal mit ihrem Geld umgehen wollen, überzeugende Lösungen anzubieten. Die Migros Bank ist die menschliche Bank.

Die Generalversammlung zum 25-jährigen Jubiläum der UZH Alumni Informatik findet dieses Jahr bei der Migros Bank statt.

Kontakt: Patrick Wolf
www.migrosbank.ch



Als kompetenter Recruiter bringt PRO ACADEMICS Fachspezialisten und Unternehmen zusammen. Unser Fokus liegt auf Informatikern und Wirtschaftsinformatikern aus den Bereichen Technologie und Strategie. Wir unterstützen dich bei der Planung und Umsetzung deines nächsten Karriereschritts. PRO ACADEMICS bietet für Mitglieder der UZH Alumni Informatik einen professionellen CV-Check sowie ein kostenloses Standort- Karrieregespräch an.

Kontakt: Stephan Jost, stephan.jost@proacademics.ch
www.proacademics.ch

- **Hat deine Firma Interesse, Sponsor oder Partner der UZH Alumni Informatik zu werden? Gerne steht dir Marc-André Pradervand (marc.pradervand@alumni.ch) für weitere Informationen zur Verfügung.**

Impressum

Ausgabe readme Nr. 47 / 2022

Herausgeberin UZH Alumni Informatik, Schönberggasse 15 a, 8000 Zürich, www.alumni.ch

Redaktion Christian Schneider (Lead Redaktion), Brigitte Bailer, Esther Rölli, Marc-André Pradervand, Nathan Labhart, Nicola Fantini, Kornél Szabó

Redaktionsadresse readme@alumni.ch

Bildnachweise Shutterstock, Unsplash (Adi Goldstein, Bit Cloud), Porträtfotos: alumni.ch, Eventfotos: privat

Produktion und Druck brain'print, Niederhasli

Auflage 780 Exemplare

Grafikdesign Vera Grönegress

Redaktionsschluss nächste Ausgabe am 27.08.2022.



NSM
Engineering AG

connecting the world
with best sources
for over 15 years

NEARSHORING

AT ITS

BEST

nsm-engineering.com