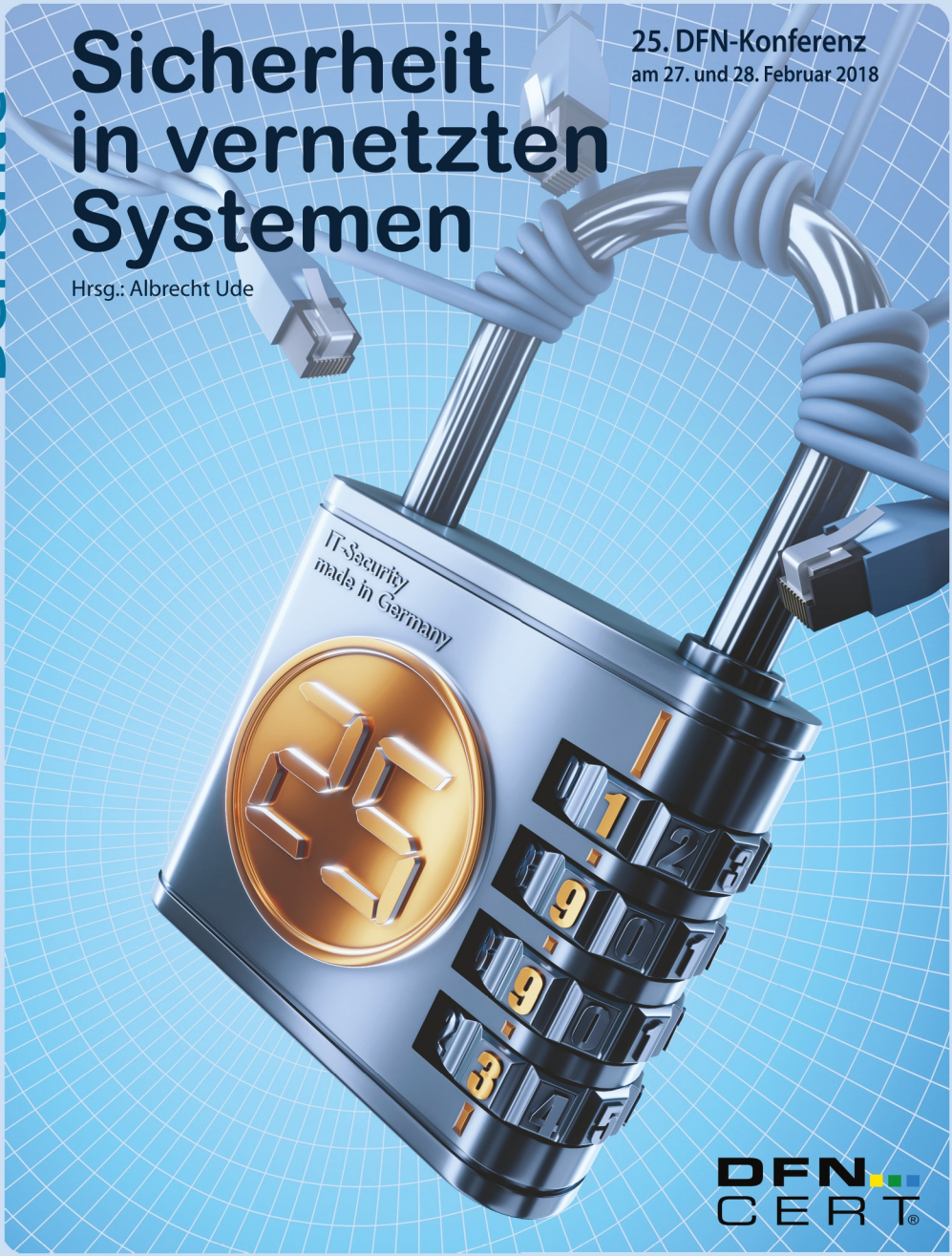
DFN
DEUTSCHES FORSCHUNGSNETZ

Berichte

Sicherheit in vernetzten Systemen

25. DFN-Konferenz
am 27. und 28. Februar 2018

Hrsg.: Albrecht Ude



DFN CERT®

Albrecht Ude (Hrsg.)

25. DFN-Konferenz

Sicherheit in vernetzten Systemen

27. / 28. Februar 2018
in Hamburg

Impressum:

25. DFN-Konferenz
„Sicherheit in vernetzten Systemen“

Hamburg, Februar 2018, ISBN: 978-3-7460-8637-8

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Herausgeber:
Albrecht Ude, Journalist | Researcher (albrecht@ude.de)
im Auftrag der
DFN-CERT Services GmbH
Sachsenstraße 5, D-20097 Hamburg

Organisation der Veranstaltung durch:
Cristiane Goldbach
Melanie Kumbischinski

Coverdesign:
Matthias Stümpke, Graphiker (matthias@stuempke.de)

Herstellung und Verlag:
BoD – Books on Demand, Norderstedt
ISBN 978-3-7460-8985-0

Organisation

Im Namen des DFN-Vereins, dem DFN-CERT und des Programm-Komitees präsentieren wir Ihnen den Konferenzband zur 25. DFN-Konferenz "Sicherheit in vernetzten Systemen" in Hamburg. Seit 1993 jährlich stattfindend, hat sich diese Konferenz mit seiner betont technischen und wissenschaftlichen Ausrichtung als eine der größten deutschen Sicherheitstagungen etabliert.

Programmkomitee

- Ingmar Camphausen, Freie Universität Berlin
- Ulrich Flegel, Infineon Technologies
- Rainer W. Gerling, Max-Planck-Gesellschaft
- Oliver Göbel, RUS-CERT
- Ralf Gröper, DFN-Verein
- Peter Gutmann, University of Auckland
- Jens Hektor, RZ RWTH Aachen
- Marc Heuse, Baseline Security Consulting
- Wolfgang Hommel, Universität der Bundeswehr München
- Stefan Kelm, DFN-CERT
- Klaus-Peter Kossakowski, HAW Hamburg
- Achim Leitner, Linux Information Systems AG
- Michael Meier, GI FB Sicherheit
- Christian Paulsen, DFN-CERT
- Helmut Reiser, Leibniz-Rechenzentrum
- Rüdiger Riediger, Bombardier Transportation
- Stefan Ritter, Bundesamt für Sicherheit in der Informationstechnik
- Andreas Schuster, BFK edv-consulting GmbH
- Thomas Schreck, Siemens CERT
- Udo Schweigert, Siemens CERT
- Gerd Sokolies, Internet Society German Chapter e.V.
- Marco Thorbrügge, Security-Experte

Veranstaltungsleitung

Klaus-Peter Kossakowski, DFN-CERT & HAW Hamburg
Christian Paulsen, DFN-CERT (Programmkomiteevorsitzender)

Hinweis

Für den Inhalt der Beiträge sind die genannten Autoren verantwortlich. Die DFN-CERT Services GmbH wählt mit Unterstützung des Programm-Komitees geeignete Einreichungen für die Veranstaltung bzw. den Konferenzband aus. Die Beiträge werden dann in diesem Konferenzband veröffentlicht, ohne die Inhalte zu verändern.

Die Vortragsfolien zu den Beiträgen werden auf der Website des DFN-CERT veröffentlicht:
http://www.dfn-cert.de/

Inhaltsverzeichnis

1 Vorwort zur 25. DFN-Konferenz

DFN-CERT: Seit mehr als 25 Jahren, vom 2. Januar 1993 an, gibt es das Computer Emergency and Response Team (CERT) im Deutschen Forschungsnetz (DFN). Es entstand aus der Erkenntnis, dass auch ein Netz wie das DFN, damals fast das einzige und ebenso wie heute das schnellste Internet in Deutschland, ein eigenes Sicherheitsteam haben sollte. Damals wie heute steht dieses Team den Anwendern und Betroffenen bei Sicherheitsproblemen zur Seite, leistet Unterstützung, koordiniert Aktivitäten und sorgt für Nachsorge bei kritischen Hinweisen auf befallene Rechner oder gestohlenen digitalen Identitäten.

Ein Netz wie das DFN mit seinen angeschlossenen Anwendern ist damals wie heute ein attraktives Ziel. Es gibt interessante Dinge zu holen, und wenn es eben nur ist, dass für Angreifer relevante Forschungsergebnisse ein paar Jahre früher als vor der offiziellen Veröffentlichung, verfügbar sind. Oder Angreifer möchten die schnelleren Leitungen mit ihren viel größeren Kapazitäten für DDoS-Angriffe nutzen. Und ja, auch in Forschungsnetzen werden manchmal Festplatten so verschlüsselt, dass niemand sie wieder entschlüsseln kann, selbst wenn die Bitcoins eingezahlt werden. Warum sollte es auch anders sein als im restlichen Internet, oder Lehrende und Forscher „immun“ gegen allgemeine Bedrohungen sein?

Die maßgebliche Ausschreibung, erarbeitet von Dr. Marcus Pattloch, war im Sommer 1992 herausgegeben worden. Dies geschah zeitgleich mit Gründung der ersten europäischen CERTs in Skandinavien (NORDUnet CERT) und den Niederlanden (heute SURFcert). In jedem größeren Netz erkannten die Verantwortlichen, das Un-Sicherheit nicht nur ein Ärgernis ist, sondern vor allem die offene, von Vertrauen geprägte Kultur von Wertschätzung und Kooperation in der Wissenschaft und in der Ausbildung gefährden würde.

Es sollte sich zeigen, dass es Not tat, etwas Sinnvolles und Konstruktives zu tun. Mit der Ausschreibung, der unermüdlichen Unterstützung und ständigen Auseinandersetzung durch und mit Dr.

Pattloch als Projekt- und Dienstverantwortlicher sowie den damaligen Geschäftsführern Klaus Ullmann und Dr. Klaus-Eckhart Maass wurde dies möglich. Natürlich gibt es viel mehr Menschen, denen wir als DFN-CERT – und ich sehr persönlich – viel zu verdanken haben. Aber diese drei seien namentlich herausgehoben, stellvertretend für alle, aber nicht zuletzt auch aufgrund ihres bis heute prägenden Einflusses, ihrer Kreativität und dem Willen, zusammen den DFN, sein Netz und die DFN-Anwenderer sicherer zu machen!

Für viele, die sich heute mit Cyber Security befassen, gehört „Incident Management" zu den ganz elementaren Aufgaben: Die Fähigkeit, zugesagte Dienste auch bei und trotz Angriffen aufrecht zu erhalten. Die Vertraulichkeit sensitiver Informationen sicherzustellen und zu verhindern, das Manipulationen an Daten oder Systemen die Reputation oder auch Leib und Leben von Menschen gefährden, ist anerkannte – quasi lebensnotwendige – Voraussetzung für jedwede Digitalisierung unserer Gesellschaft. Das DFN-CERT ist mit dieser kritischen Funktion unverzichtbar. Damals war das aber keine Selbstverständlichkeit, sondern eine Pioniertat.

Zwar war bereits fünf Jahre vorher, am 2. November 1988, den Benutzern des Internets sehr drastisch aufgezeigt worden, was ein relativ simpler Computer-Wurm (eine sich selbständig im Netzwerk durch Kopieren und Remote Execution verbreitende Art der Malware) bewirken kann. 10% der damals weltweit ca. 70.000 Rechner wurden lahmgelegt. Vor allem die E-Mail-Server waren betroffen, so dass E-Mail als primäre Basiskommunikation nicht mehr zur Verfügung stand, und zwar im gesamten Internet. Computer-Viren gab es damals schon seit Mitte der achtziger Jahre, das Konzept eines selbstreplizierenden Programms ist jedoch sehr viel älter und beschäftigte schon früh Forscher und Netzwerker (und wird es in der Zukunft im Zeitalter von maschinellem Lernen und Artificial Intelligence wohl noch sehr viel mehr, als uns allen lieb sein dürfte). John Brunner hatte das u.a. als „Tapeworms" (ca. 1977) in seinem Roman „Der Schockwellenreiter" beschrieben. Woher er diese Idee hat, entzieht sich leider meiner Kenntnis. Als ich ihm Mitte der 80er Jahre über-

raschend in Hamburg begegnete, konnte ich in dem Science Fiction Antiquariat zwar noch schnell eine deutsche Version des Romans für ein Autogramm kaufen, aber ihn danach zu fragen? Ich war ich wohl zu überrascht, ihn zu fragen … leider!

Schon einen Monat nach dem Internet-Wurm wurde durch DARPA an der Carnegie Mellon University (Pittsburgh, PA, USA) „das“ CERT gegründet, das sich in allererster Linie um das Internet und die damit vernetzten Rechner kümmerte, und damit auch weltweit seine Hilfe anbot. Mit der steten Zunahme von Internet-Anschlüssen in anderen Ländern erkannten die ersten nationalen Forschungsnetze, aber auch Regierungseinrichtungen wie die NASA oder das US Department of Energy die Notwendigkeit, eigene Ressourcen für den Fall der Fälle vorzuhalten. Wichtig war vor allem dafür zu sorgen, dass Sicherheitslücken geschlossen werden. Man bedenke, dass es die ersten Firewalls erst Anfang der neunziger Jahre gab. Wenn Sie sich heute vielleicht fragen, warum das so lange gedauert hat – überlegen Sie mal, wie lange es Autos ohne Sicherheitsgurte gab …

1992 gab es dann in Deutschland selbst ca. 70.000 Rechner im „deutschen“ Internet, doch nach dem Internet-Wurm und ähnlichen Aktionen im DECnet (WANK/OILZ, Namen, die man wahrscheinlich nur noch irgendwo auf verstaubten Internet-Seiten findet) war es relativ ruhig geworden – allerdings nicht sicherer. Und deswegen musste was passieren!

Das DFN-CERT war das erste Computer-Notfallteam für den deutschen Teil des Internets, doch gab es bereits vorher deutsche, studentische Arbeitsgruppen, die sich rund um Prof. Dr. Klaus Brunnstein in Hamburg und Christoph Fischer in Karlsruhe gesammelt hatten, um der steigenden Bedrohung durch Computer-Viren etwas entgegenzusetzen. Diese arbeiteten eng mit dem BSI zusammen, das sich mit einem eigenen Referat dieses Themas annahm und darauf aufbauend z.B. die ersten Anforderungen an Firewall-Systeme im Behördenumfeld erarbeitete.

Aber warum kam das DFN-CERT nach Hamburg? Hier gab es wie bereits angesprochen eine kritische Masse. Uns, damit meine ich eine ganze Generation von Studierenden ab April 1988, hatten die Vorlesungen von Prof. Brunnstein, der als einer der ersten deutschen Professoren einen ganzen Zyklus von mehreren Semestern zu IT-Sicherheitsthemen anbot, mit einer guten Grundausbildung versehen. Parallel gab es mit dem Virus-Test-Center eine Gruppe von Studierenden, die sich konkret mit den praktischen Auswirkungen von Unsicherheit auseinandersetzten. Einige bekamen sogar, unter strengsten Auflagen, lokal vernetzte Workstations, um Malware auseinander zu nehmen. Andere beantworteten säckeweise Post, als Professor Brunnstein über die Tagesschau zusicherte, alle, die einen frankierten Rückumschlag an das VTC schicken würden, bekäme eine Diskette mit einem selbst entwickelten Melissa-Anti-Virus. Und ja, er musste direkt nach dem Interview zu einer Konferenz ins Ausland, aber dadurch haben wir viel gelernt, glauben Sie mir.

Viele von uns sind bis heute überall in Sicherheitsfirmen zu finden, und allen gemein ist, dass wir mit diesem Thema gleichsam „infiziert“ wurden, und man uns – wenn auch nach strenger Vergatterung – viel anvertraute. Aber damit ist die eigentliche Frage noch nicht beantwortet. Denn ohne eine weitere Person, Dr. Hans-Joachim Mück, den ersten Leiter des DFN-CERTs, hätte es niemals einen „Hamburger“ Angebot gegeben. Er interessierte sich bereits damals für das Thema, wenn auch nicht ganz uneigennützig, weil es ihn damals schon umtrieb, was so mit seinen Systemen passierte, wenn er gerade nicht da war oder doch mal Feierabend machte. Und deswegen war es wohl kein Zufall, dass er die Zweitbetreuung meiner Diplomarbeit übernahm, die übrigens Computer-Würmer behandelte, was sonst?

Als Leiter des Rechenzentrums der Informatik an der Universität Hamburg und starker Verfechter der zunehmenden Vernetzung im DFN und in Hamburg erkannte Dr. Mück intuitiv die Bedeutung eines DFN-CERTs, als er die Ausschreibung sah. Er glaubte, dass es für den Verein von langfristiger, strategischer Bedeutung sein würde, sich

nicht nur selbst gegen Angreifer wehren zu können, in dem Sicherheitsinformationen schnell und zielgerichtet an die richtigen Ansprechpartnerinnen und -partner als Hilfe zur Selbsthilfe verteilt werden. Sondern auch die Experten zur Verfügung zu haben, und die Chancen, die sich daraus ergeben, nutzen zu können, würde viel Gutes bewirken. Zurückblickend weiß ich bis heute nicht, was an dem im Herbst 1992 abgegebenem Angebot für mich schwerer war: Dr. Mück zufriedenzustellen, parallel mit der Diplomarbeit fertig zu werden – oder eben das Angebot abzugeben, das ausgewählt wurde.

Für mich war es jedenfalls ein großen Glück, direkt nach Abschluss meines Diploms beim Start des DFN-CERTs dabei sein zu dürfen. Dessen erste Aktion war dann allerdings ganz profan, einen mit alten, ausrangierten Möbeln gefüllten Kellerraum unter dem RZ zu leeren und aufzumöbeln – für die nächsten acht Jahre blieben die CERTlinge die Kellerkinder im Haus D.

Und während die Forschungsaufgabe war, den Stand der Technik zu erfassen, den Bedarf abzufragen, mögliche Aufgaben zu identifizieren und Lösungsansätze zu entwickeln, geschah parallel etwas, was in dieser Form – glaube ich – keiner vorhergesehen hatte: Wir wurden gebraucht!

Schon bevor das erste Jahr zu Ende war, waren wir im „Service-Modus“. Das hat sehr viel verändert und die genannten Initiativen und vieles mehr erst möglich gemacht. Die ersten richtigen „Incident Handler“ waren dann ab Sommer 1994 Uwe Ellermann und Stefan Kelm, beide wie ich aus dem VTC kommend, sowie Wolfgang Ley, der von der TU Clausthal nach Hamburg kam. Zusammen starteten wir dann auch die DFN-PKI (1996) und das Hochgeschwindigkeits-Firewall-Labor (1997). Das Konzept ging auf!

Wir haben aber immer auch investiert und Lösungen gefunden, die man so nicht einkaufen konnte: entweder weil sie zu teuer waren, oder weil sie im DFN nicht skalierten. Lieber suchten wir nach einer intelligenten und cleveren Lösung, die unter dem Strich auch viel

Geld spart. Heute sind wir mit ca. fünfzig Mitarbeiterinnen und Mitarbeitern fünfundzwanzig mal so viele wie am Anfang. Wir arbeiten immer noch sehr eng mit allen Hamburger Hochschulen zusammen, denn wir brauchen immer Nachschub an guten Leuten! Aber zum Glück haben wir heute auch viele Kolleginnen und Kollegen, die eben nicht aus dem VTC oder aus Hamburg kommen und ihre Perspektiven und Expertisen einbringen und uns bereichern!

Über all die Jahre sind wir uns selbst, unserer besonderen Rolle und unseren Zielen im Kern treu geblieben:
Wir sind ein wertorientierter Dienstleister mit eingespielten Teams und viel individuellem Know-How, der sich immer wieder neu orientiert, um Trends aufzunehmen oder auf Herausforderungen zu reagieren. Für den DFN-Verein, die DFN-Anwender und unsere weiteren Kunden sind wir *der* verlässliche Partner für mehr Sicherheit und Datenschutz.

Danke an die, die das alles möglich gemacht haben!
Danke an die, die das durch Ihre Arbeit jeden Tag möglich machen!

Ihr Klaus-Peter Kossakowski

2 Grußwort des Vorstandes des DFN-Vereins

Was für ein bemerkenswertes Jubiläum: Das DFN-CERT veranstaltet seit 25 Jahren die DFN-Konferenzen „Sicherheit in vernetzten Systemen“! Dies ist eine wunderbare Gelegenheit, einmal aus der weitgehend stillen Rolle als Auftraggeber aus dem Hintergrund auf die Bühne zu treten und kurz das lobende Wort zu ergreifen. Als Vorsitzender des Vorstandes und damit im Namen aller Mitglieder des DFN-Vereins: Liebes DFN-CERT, unsere Hochachtung und Anerkennung für die großartige Arbeit, die in der Organisation dieser Konferenz, aber auch in den anderen Tätigkeiten des DFN-CERT ihren Ausdruck findet. Wir gratulieren ganz herzlich und schließen in diesen Dank ausdrücklich alle Mitarbeiterinnen und Mitarbeiter, das Programmkomitee sowie die vielen Referenten ein, die über die vielen Jahre zum Erfolg dieser Konferenz beigetragen haben.

Eine wissenschaftliche Konferenz wird 25! Neben den lobenden Worten auch eine gute Gelegenheit, um einen Moment innezuhalten und den Blick sowohl zurück als auch nach vorne zu richten. Dem Rückblick hat sich Klaus-Peter Kossakowski in seinem Vorwort zu diesem Konferenzband schon gewidmet. Ich möchte dies aus der Perspektive des Vorstands des DFN-Vereins auf einer etwas anderen Ebene und eher nach vorne ausgerichtet ergänzen. Ich frage mich: Sind wir als DFN-Verein im wissenschaftlichen Umfeld mit solch einer Konferenz richtig aufgestellt? Bedienen wir die Bedarfe, die uns letztendlich unsere Mitglieder mit auf den Weg geben? Lassen Sie es mich hier ausdrücklich festhalten: Ich bin davon überzeugt und sehe dafür – mindestens – zwei wesentliche Anhaltspunkte.

Zum einen sehen wir seit vielen Jahren eine hohe Anzahl von registrierten Teilnehmerinnen und Teilnehmern. In einem Umfeld von zahlreichen Konferenzen, die um Aufmerksamkeit buhlen, ist dies ein sehr zuverlässiger Indikator. Kaum eine Woche, in der nicht im Posteingang unserer E-Mail-Konten eine Einladung zu einer Konferenz auftaucht. Und dieser Wettbewerb ist in höchstem Maße von globaler Natur und wird durchaus auch mit allen Mitteln der Kunst

ausgefochten. So ist Hamburg sicherlich eine attraktive Stadt, auch im Winter. So manch eine Konkurrenz glänzt jedoch durchaus mit Luft- und Wassertemperaturen, die auf den ersten Blick als einladender erscheinen mögen.

Zum anderen steht im Mittelpunkt einer solchen Betrachtung, neben der Teilnehmerzahl die Frage nach der Relevanz des Themas. Gibt es einen Indikator, um hier einen Trend festzumachen? Offenkundig gibt es ein andauerndes Getöse um das Thema „Sicherheit in vernetzten Systemen", das ja letztendlich eine dem DFN-Verein angemessene, spezifische Sichtweise auf das Mega-Thema „Informationssicherheit" darstellt. Aber dieses Getöse wird durchaus durch Interessen beflügelt, die nicht unbedingt sachbezogen sein müssen. So mag manch ein Protagonist „Sicherheit, Sicherheit" rufen und dabei entweder mahnend den Finger heben oder hektisch mit den Armen fuchteln, um damit letztendlich in kalkulierter Weise seiner möglicherweise ganz anders gearteten Agenda Vorschub zu leisten. So wäre „Sicherheit" mitnichten das erste „Buzzword", das umgangssprachlich als „Sau durchs Dorf getrieben" wird. Ist also dieses Getöse ein zuverlässiger Maßstab? Eher nur ein Indikator. Aber wo liegt ein Maßstab, dem wir insoweit vertrauen, dass wir Informationssicherheit mit zunehmendem Einsatz von Ressourcen begegnen müssen? Nach meiner Auffassung ist er unter anderem in einer vergleichenden Bewertung der Informationssicherheit für die Prozesse in Forschung und Lehre zu finden. Schaut man 25 Jahre zurück, so waren die Leistungs-fähigkeit und Verfügbarkeit eines Wissenschaftsnetzes durchaus erwünscht, aber für viele wissenschaftliche Disziplinen kein zentraler Aspekt bei ihrer Arbeit. Wie ist das mit der heutigen Situation zu vergleichen? Ist das immer noch so? Ein ganz klares Nein! Ausgehend von den eher IT-affinen Disziplinen wie der Hochenergie-Physik sehen wir heute eine nahezu unüberschaubare Vielfalt von verteilten, netzgestützten Prozessen in Forschung und Lehre: Anmeldung zum Seminar? Videokonferenzgestützte Lehrveranstaltung? Entfernte Steuerung von astronomischen Beobachtungen? Auswertungen von Petabytes von Experimentdaten mit entfernten Höchstleistungsrechnern? Überall sehen wir den Einsatz von IT-gestützten Verfahren, in denen der

DFN-Verein mit seinen Diensten oft eine vordergründig kaum sichtbare, aber tragende Rolle spielt.

Und wir stehen hier erst am Anfang. „Welchen Beitrag wird die Seefischerei im Jahre 2050 für die globale Ernährung spielen?“ Lehnen Sie sich einen Moment zurück und denken darüber nach, wie viele wissenschaftliche Disziplinen an der Beantwortung solch einer Frage zusammenwirken müssen: „Wie viele Menschen werden wir 2050 sein? Welche Bestände werden wir in den Meeren vorfinden? Welche Rolle werden Aquakulturen spielen? Wie wird der Fischfang international geregelt sein?“. Diese Aufzählung könnte man jetzt viel weiter ausdifferenzieren. Nun, sind es eine, zwei, fünf Disziplinen? Und wie kommen wir dann an deren Forschungsdaten, die heute kaum recherchierbar in irgendwelchen Silos schlummern? Einfach mal im Web danach suchen? Eher nicht. Die Beantwortung solcher Fragen wird ein disziplinübergreifendes Management von Forschungsdaten erfordern, ein aus meiner Sicht zentrales Zukunftsthema für unsere Wissensgesellschaft, das ohne den Einsatz von verteilten, netzgestützten Prozessen in Forschung und Lehre gar nicht denkbar ist. Und wie dies ohne eine adäquate „Sicherheit in vernetzten Systemen“ zuverlässig und integer funktionieren soll, kann ich mir beim besten Willen nicht vorstellen.

Liebe Leserin, lieber Leser, lassen Sie mich nach diesem Ausflug in die etwas übergeordneten Fragen des DFN-Vereins zurückkommen zum schönen Anlass dieses Grußwortes und dies mit einem Wunsch verbinden: Wo auch immer wir persönlich in 25 Jahren sein mögen, ich wünsche dem DFN-CERT, dass es dann eine erfolgreiche 50. DFN-Konferenz „Sicherheit in vernetzten Systemen“ veranstalten wird. Es sei denn, alle Fragen sind bis dahin gelöst. Aber da mag ich nicht so recht daran glauben.

Ihr Hans-Joachim Bungartz

3 Kurzbiographien der Autoren

Ralf Spenneberg

Ralf Spenneberg berät mit seinen beiden Unternehmen OpenSource Training und OpenSource Security seit 1999 Unternehmen und Behörden bei dem Einsatz von OpenSource Sicherheitslösungen. Als Autor hat er zahlreiche Bücher zu den Themen Firewalling, VPN, Intrusion Detection, KVM-Virtualisierung, SELinux und AppArmor veröffentlicht. Er bietet seinen Kunden maßgeschneiderte Sicherheitslösungen mit OpenSource-Software und Widerstandsanalysen von Softwareprodukten und Embedded Devices. Neben Industriesteuerungen beschäftigt er sich auch mit elektronischen Zutrittsregelungen, Schließanlagen und RFID-Technologien.

Paul Schäfer

Paul Schaefer arbeitet seit 2016 als IT-Sicherheitsspezialist für OpenSource Security Ralf Spenneberg. Zu seinen Aufgabengebieten gehören neben der sicherheitstechnischen Analyse von OpenSource-Software die Untersuchung Mobile Devices. Zeitgleich studiert er an der Fachhochschule Münster und erwarb dort im Jahr 2016 einen Abschluss zum Bachelor of Science im Studiengang Angewandte Informatik.

Hans-Joachim Knobloch

Hans-Joachim Knobloch erwarb Ende 1989 sein Diplom in Informatik an der Universität Karlsruhe. Er arbeitete seit 1988 am Europäischen Institut für Systemsicherheit. Zu Beginn des Jahres 1996 wechselte er zur NTG Netzwerk und Telematik GmbH, nachmals Xlink und KPNQwest Germany. Bei Xlink/KPNQwest war er als Security Engineer und Senior Consultant am Aufbau des Bereichs Security-Services beteiligt. Seit Oktober 2000 ist er als Security Consultant bei der Secorvo Security Consulting GmbH tätig.
Hans-Joachim Knobloch verfügt über langjährige Erfahrung in den Bereichen Kryptologie, Public Key Infrastrukturen, Smartcard-Software, Netzwerk- und E-Mail-Sicherheit. Er ist Autor bzw.