GFFT

Gemeinnützige Gesellschaft zur Förderung des Forschungstransfers e.V.

GFFT Jahresbericht 2018/2019

Wir bringen innovative Technologien in die Anwendung.

Gemeinnützige Gesellschaft zur Förderung des Forschungstransfers

www.gfft-portal.de

Inhalt

Grußwort

Dr. Gerd Große
Vorstandsvorsitzender des GFFT e.V.

Sehr geehrte Damen und Herren,
liebe Freunde der GFFT,

die Welt ist unsicherer geworden und hat uns aus der Komfortzone sicherer Umsätze, Geschäftsmodelle und Mittelfristpläne hinausgeführt. Der neue amerikanische Präsident mit seinen gewöhnungsbedürftigen Ansichten, die chinesischen Anstrengungen von den KI-Investitionen bis zur neuen Seidenstraße und die ökologischen Anforderungen hinterlassen ihre Spuren.

Die einzelnen Unternehmen suchen vielerorts ihr Heil in der Gemeinschaft: Unsere süddeutschen Autobauer finden in den Zukunftsfeldern zueinander. Auch die westdeutschen Energiekonzerne strukturieren ihre Aktivitäten untereinander neu. Die Liste der Firmenkäufe und Akquisitionen ist lang. Natürlich sollte man dabei aufpassen, dass man sich nicht noch das Leben unnötig schwer macht wie so manches Unternehmen, das man inzwischen eher in der Juristerei verortet, statt in seinem Stammgeschäft.

Auch die GFFT sieht den Vorteil in einem Miteinander. Daher bilden sich unter unserem Dach für einige der wichtigsten Themenfelder einzelne Communities, die gemeinsam neue Lösungen erarbeiten möchten. Stellvertretend seien die Informationssicherheit, die IT und das Management logistischer Lieferketten genannt. Wichtig erscheint uns dabei, die verschiedenen Perspektiven von Anwendern, Technologieanbietern und Wissenschaftlern in einen produktiven Zusammenhang zu bringen. Dies sollte nicht durch einfaches Austauschen erfolgen, sondern durch strukturierte Aktivitäten wie den GFFT-Innovationsprozess. Wir werden sehen, wie sich daraus ein wirksamer Schub für den Innovationsstandort entwickeln lässt.

Aus dieser Zielsetzung heraus lässt sich auch das heutige 13. Jahrestreffen unserer Gesellschaft sehr gut verstehen. Die oben genannten Themenfelder sind in der Veranstaltung als einzelne Tracks wiederzufinden und einige der laufenden Projekte werden auch an den Ständen vorgestellt. Lassen Sie sich von den Arbeiten der vielen Vortragenden, Aussteller und Partner einfangen und inspirieren. Ich wünsche Ihnen einen „innovativen“ Tag.

Ihr

Dr. Gerd Große

Grußwort

Tarek Al-Wazir
Hessischer Minister für Wirtschaft,
Energie, Verkehr und Wohnen

Sehr geehrte Damen und Herren,

Die digitale Transformation verändert unseren Alltag und unsere Wirtschaft. Sie birgt Herausforderungen, aber auch enorme Chancen – für Bürgerinnen und Bürger wie auch für Unternehmen.

Hessen möchte, dass diese Potenziale ausgeschöpft werden. Ob die digitale Transformation gelingt, entscheidet sich auf dem Weg von der Forschung in die Anwendung. Deswegen fördern wir digitale Innovationen.

Diesem Ziel hat sich auch die GFFT verschrieben. Wir freuen uns sehr, dass ihr Jahrestreffen 2019 in Hessen stattfindet und unter anderem das wichtige Thema der IT-Sicherheit behandelt. Denn die neuen Technologien werden nur genutzt werden, wenn die Anwender darauf vertrauen können, dass ihre Daten vor unberechtigtem Zugriff geschützt sind. Wir sind sehr stolz darauf, dass sich im Raum Darmstadt ein international anerkanntes Zentrum für IT-Sicherheitsforschung entwickelt hat.

Unsere gemeinsame Aufgabe ist es, dessen Forschungsergebnisse in die breite Anwendung zu bringen.

Wir wünschen allen Teilnehmerinnen und Teilnehmern ein anregendes Treffen
Ihr

Tarek Al-Wazir

Die Arbeit der GFFT

Mit großem Enthusiasmus haben wir vor zwei Jahren mit den Ehren- und Kuratoriumsmitgliedern das „GFFT-Manifest für Technologietransfer“ geschrieben. Damals wie heute wurde der deutschen Innovationskraft eher Platz 10 als Platz 1 zugeordnet. Es ist schwer, die Korrektheit dieser Platzierung zu bestätigen. Allerdings erscheint unzweifelhaft, dass es noch andere Länder gibt, die sich anstrengen und dass wir nicht nachlassen dürfen, wenn wir weiterhin führende Produkte für den Weltmarkt entwickeln möchten.

Ausgehend von dieser Sorge haben die Autoren eine Reihe von Themenfeldern oder Maßnahmen identifiziert, in denen man Fortschritte erzielen muss:

A. Verbreitung von Erfindungen, Entwicklungsvorhaben und Lösungsbedarfen
B. Standardisierung von Verträgen und Regelung geistigen Eigentums
C. Einbindung von Wagniskapitalgebern
D. Personal als Innovationsfaktor
E. Identifikation von Zukunftsfeldern und Initiierung von übergreifenden Teams
F. Innovationsziele in den Unternehmen
G. Forschungsförderung durch Konzerne

Um Wirkung zu erzielen, muss jede dieser Maßnahmen natürlich branchen- und fachbereichsweit gedacht werden. Bspw. muss man für Punkt D den Informatik-Nachwuchs so aufstellen, dass er die digitalen Herausforderungen in allen Branchen aufnimmt. Gleiches gilt für den Maschinenbau-Nachwuchs usw. Fokussiert man bspw. auf die Logistikbranche, so muss jede einzelne Maßnahme von der Vermittlung der Innovationen (A) bis zur Förderung der Forschung (G) umgesetzt werden. Mathematiker würden dies als Raum mit den Dimensionen Maßnahme * Fachgebiet * Branche definieren.

Als Verein, der ein solches Manifest herausbringt, sollte man sich natürlich nicht vor der Antwort drücken. Allein die Größenordnung macht klar, dass die Lösung in einer übergreifenden

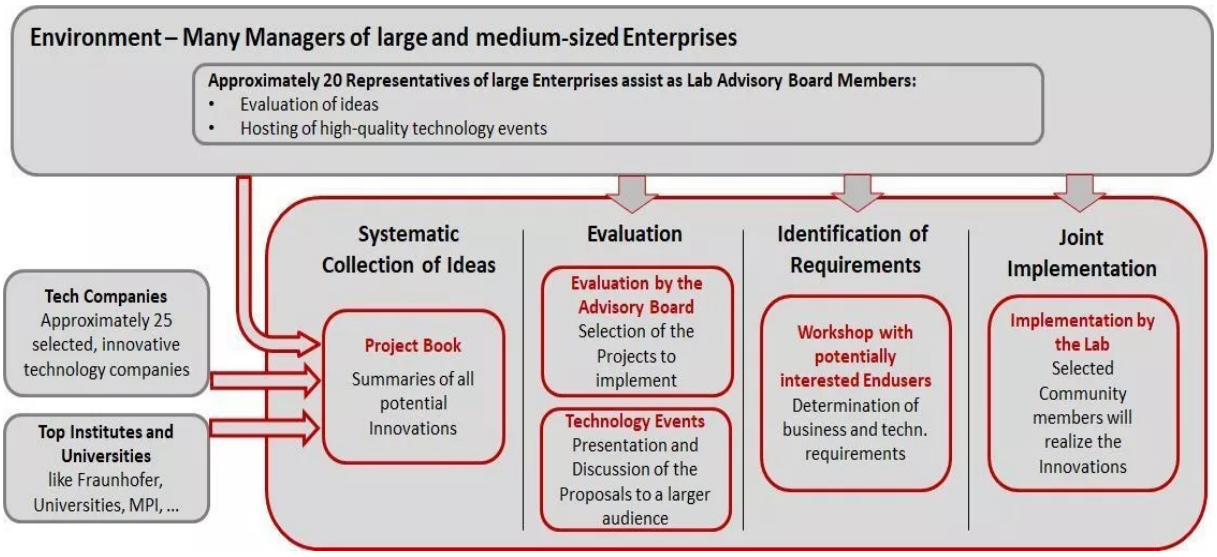
Innovationsstruktur liegt, in die die verschiedenen Stakeholder wie bspw. die Wissenschaftler, Technologieanbieter und Anwender integriert werden. Sie wird auch nur angenommen werden und wachsen, wenn jede eingebundene Gruppe direkte Vorteile aus der Zusammenarbeit ziehen kann. Es muss für sie deutlich attraktiver sein, zu kooperieren als außen vorzubleiben.

Der GFFT-Innovationsprozess

Abstrakt gesprochen benötigt man einen Innovationsprozess, der

- die systematische Entwicklung neuer Lösungen ins Zentrum der Aktivitäten rückt,
- den Stakeholdern attraktive Rollen zuordnet und
- verschiedene Fördermaßnahmen beinhaltet, die die Innovationen über ihren gesamten Lifecycle hinweg zum Erfolg schieben.

Der GFFT-Innovationsprozess ist so gestaltet worden, dass er diese Kriterien alle erfüllt. Er kann für beliebige Größen durchgeführt werden. Vom Projekt zur Effizienzsteigerung in globalen Lieferketten genauso wie für ein gesamtes Themenfeld wie die Informationssicherheit. Das nachfolgende Bild stellt ihn im Überblick dar:



Der Ablauf des Prozesses ist simpel und zielorientiert gehalten: Es werden von allen Stakeholdern die Innovationsvorschläge und -services eingeholt. In der Prüfphase sehen sich zunächst geeignete Experten der Anbieterseite den Vorschlag an, anschließend bewerten ausgewählte Anwender den überarbeiteten Text. Abhängig vom Ergebnis werden dann entweder ein Umsetzungsprojekt angestoßen oder Maßnahmen zur Verbreitung initiiert. Jede Rolle in diesem Prozess muss so gehalten werden, dass sich der Aufwand mit dem Ergebnis rechtfertigen lässt.

Die Nutzung dieses Prozesses ist für alle Mitwirkenden gleichermaßen vorteilhaft:

1. Die **Technologieanbieter** können ihre Ideen vor der letztendlichen Investitionsentscheidung von Anwendern bewerten lassen. Im Idealfall kann es sogar dazu kommen, dass einige der Anwender das Projekt als Referenzkunde unterstützen.
2. Die **Anwender** können eigene Vorschläge in den Prozess einbringen und darauf hoffen, dass eine größere Anzahl anderer Anwender diese Herausforderung gleichermaßen spürt und sich an einer Lösungsentwicklung beteiligt.
3. Die **Wissenschaftler** können gleichfalls Ideen einbringen und die Meinung der Anwender erhalten. Darüber hinaus können sie in die Lösungsfindung aller Vorschläge eingebunden werden.
4. Den **Beratern** schließlich kommt eine Katalysatorrolle zu. Sie helfen dabei, die Einsetzbarkeit der Ideen zu gewährleisten, sorgen für die professionelle Bearbeitung der Projekte und auch für die Verbreitung in den Märkten.

Auf diese Weise können gemeinschaftlich ...

- ... die Innovationsgeschwindigkeit aller Prozessteilnehmer deutlich erhöht werden, ohne dabei höhere Kosten zu verursachen,
- ... wesentlich mehr Innovationen generiert werden und
- ... Herausforderungen angegangen werden, die die Unternehmen einzeln nicht lösen könnten, bspw. der Abgleich von Lieferketten über die Unternehmen einer ganzen Branche hinweg.

Die themenbezogenen GFFT-Communities

Der Erfolg des Innovationsprozesses kann signifikant erhöht werden, wenn man die Stakeholder an der Gestaltung der Zusammenarbeit direkt beteiligt. Aus dieser Motivation heraus verbindet die GFFT die Anwender und Innovationsanbieter in einer Community, die mit Hilfe von Nutzen stiftenden Aktivitäten und Services ein aktives Miteinander fördern soll. Durch die zentrale Rolle des Innovationsprozesses entstehen innovationsgetriebene Communities, die die versprochenen wirtschaftlichen Vorteile für die einzelnen Mitglieder auch erbringen können.

Noch verstärkt wird das Innenleben dadurch, dass alle Mitglieder eigene Services vorschlagen und anbieten dürfen. Dies soll vor allen Dingen den Startups helfen, auf ihre neuen Lösungen aufmerksam zu machen.

Die GFFT Labs

Um dem Zusammenspiel aus Innovationsprozess und Community-Bildung Stabilität zu verleihen, werden entsprechende GFFT-Labs gebildet. Ihre Aufgabe ist es, als Träger der Aktivitäten zu dienen und den Erfolg zu gewährleisten. Weiterhin sorgen sie u.a. für den Ausbau der Mitgliederschaft, die

Verankerung neuer Services und die Unterstützung der Innovationen von der Ideenfindung bis zur breiten Vermarktung.

Die Labs sind so angelegt, dass sie sich auch an den Projekten selbst beteiligen bzw. eigene Ideen über den Innovationsprozess nach vorne treiben können. Hierzu werden sie sukzessive eigene Entwicklungsbereiche aufbauen, die gezielt die Nachwuchskräfte der kooperierenden Lehrstühle ansprechen und attraktive Arbeitsplätze bereitstellen. Insbesondere die Nähe zu beiden Seiten, Anwendung und Forschung, sollte es den Labs ermöglichen, ihre Ideen über das Prototypenstadium hinaus bis zu einer erfolgreichen Markteinführung zu führen.

Erste Themenfelder

In manchen Bereichen ist der beschriebene Ansatz bereits verwirklicht worden:

1. **IT-Security**: Die rapide Entwicklung der Informationstechnologie bringt jeden Tag eine Mannigfaltigkeit an neuen Diensten und Möglichkeiten, aber auch an neuen Bedrohungskanälen. Wir erleben vielerorts Hackerangriffe, die Kontrollübernahme durch Außenstehende oder Spionage und Sabotage. Um dem effektiv zu begegnen, hat die GFFT einen diesbezüglichen Innovationsprozess und eine Community ins Leben gerufen. Die ersten Projekte befassen sich mit einem KPI-Gerüst zur Messung der Informationssicherheit in den Unternehmen und mit einer Policy-Toolbox, die das Wissen für die Security-Verantwortlichen in handhabbarer Form beinhaltet, ausbaut und bereitstellt.

2. **Software-Entwicklung inkl. Test- und Projektmanagement:** Heutzutage werden bis 80 % der Prozesse in einem Unternehmen digital abgebildet oder zumindest IT-seitig stark unterstützt. Dies reicht von dem Thema Organizational Intelligence, das die GFFT im Jahr 2018 diskutiert hat, bis zu allen Haupt- und nachgelagerten Prozessen. Daher kommen der Softwareentwicklung und der fehlerfreien Qualität eine enorme Bedeutung zu. In diesem Bereich arbeitet die GFFT gemeinsam mit der Commerzbank, BearingPoint und vielen anderen Partnern an neuen Lösungen.

3. **Global Supply Chain Management:** Neben den offensichtlichen ökologischen Gründen gibt es auch eine Reihe ökonomischer Gründe, um über die Effizienz des Gütertransports in Deutschland intensiv nachzudenken. Viele LKWs sind nicht voll beladen. Sie fahren z.T. ähnliche Routen wie bspw. zwischen den großen Produktionsstandorten der Automobilhersteller. Gemeinsam mit Logistikleitern, Frachtbörsen, Beratern und wissenschaftlichen Instituten wird systematisch an Effizienzverbesserungen gearbeitet. In das Management der Community sind Vertreter von Schaeffler und der BLG Logistics Group eingebunden.

4. **Smart Products:** Mit heutiger IT und Sensortechnologie können viele Prozesse unter ständiger Kontrolle gehalten werden. Dies gilt insbesondere auch für die großen und kleinen Industriegüter, bspw. Autos, Lokomotiven, Landmaschinen, Waschmaschinen, usw. Zumeist konzentriert man sich aktuell auf die vorausschauende Wartung. Doch dabei wird es nicht bleiben. Man wird versuchen, aus dem operativen Nutzungsverhalten auf die zukünftigen Funktionalitäten zu schließen. Dieser Fragestellung geht die GFFT mit Unternehmen wie Bosch, Daimler, Bombardier, Camelot und anderen in einer Serie von Workshops nach. Der nächste Schritt wäre alsbald die Gründung eines Smart Products Labs und die gemeinschaftliche Entwicklung geeigneter Lösungen.

In der weiteren Planung befinden sich noch die Felder „Digitalisierung“, das sich mit der Prozessautomatisierung in Unternehmen beschäftigen wird, und „Industrie 4.0“, das den Fortschritt im Produktionsumfeld unterstützen soll. Insgesamt kann die GFFT damit Verbindungen zu den wichtigsten Bereichen der meisten Unternehmen aufbauen und eine breit angelegte Kontaktbasis in die hiesige Wirtschaft für den Technologietransfer bereitstellen.

Vermarktung über Technology Events

Essenziell für den Erfolg der GFFT ist es, die Neuentwicklungen den Anwendern schnell vorstellen zu können und erste Projekte zu initiieren. Ausgehend von der ständig wachsenden Kontaktbasis bietet die GFFT den Innovationsentwicklern daher die Möglichkeit an, den Anwendern ihre Ideen und kommenden Produkte in kleinen, regelmäßig stattfindenden Workshops vorzustellen.

Das Ziel der Technology Events ist es, ein Bild über den technischen Stand zu erlangen und gemeinsam über neue Lösungen nachzudenken. In der Regel werden die Events bei einem Anwenderunternehmen durchgeführt, welches aufgrund eigener Anstrengungen ein großes Interesse an der ausgewählten Thematik besitzt. Geeignete weitere Anwenderunternehmen werden dazu geladen und vergrößern damit die Chance, Projektgemeinschaften zu bilden.

Fazit und Ausblick

Die GFFT kann aufgrund ihrer Größe nicht die Innovationsmenge in Deutschland verändern. Was sie aber in den zurückliegenden Monaten erstellt hat, ist nicht weniger als eine Wegbeschreibung, wie man die Ziele des GFFT-Manifests als Gemeinschaftsprojekt erreichen kann. Wichtig hierfür ist es, dass die Anzahl der Innovationsprozesse und Communities sukzessive ausgebaut wird, dass immer mehr Unternehmen sich der Initiative anschließen und dass diese auch Verantwortung an den einzelnen Stellen für das gesamte Werk übernehmen.

Wenn die Idee des Innovationsprozesses sich als wirkungsvoll erweist, dann lassen sich auch die anderen Maßnahmen B bis E und G des GFFT-Manifests integrieren und erfüllen.

Dies wird entlang der folgenden Linie verlaufen:

B: Es werden sich aus den laufenden Projekten Standardverträge ableiten lassen. Auch das IP-Vergabeproblem wird sich sukzessive klären lassen.
C: VC-Geber können in die Communities eingebunden werden. Sie erhalten die Möglichkeit, in Projekte zu investieren, bei denen die Anwender mitentwickeln und daher die Marktrelevanz gewährleisten.
D: Der Nachwuchs wird über die Lehrstühle an die Zukunftsprojekte herangeführt und werden diese Arbeiten bei einem der Community-Mitglieder fortsetzen.
E: Innovation in der Gemeinschaft ist günstiger, weshalb die Unternehmen sich an mehr Zukunftsprojekten werden beteiligen können.
G: Wenn man es schafft, die forschenden Institute als Projektpartner zu integrieren, werden sie automatisch als IP-Besitzer an den Gewinnen der Neuentwicklungen beteiligt. Es muss das Ziel sein, mit den dadurch erzielbaren Mehreinnahmen die Grundlagenforschung zu unterstützen.

Dann wird sich auch die Frage nach der zukünftigen Rolle der GFFT stellen. Mit ihrer Arbeit könnte sie sich stark für die Innovation durch Vernetzung und strukturelle Abstimmung engagieren. Dazu sollte sie das jetzt schon weitreichende Netzwerk von Innovationspartnern weiter ausbauen und für die einzelnen Stakeholder nutzbar machen.

Über den Autor

Dr. Gerd Große

Vorstandsvorsitzender des GFFT e.V.
Geschäftsführer GFFT Technologies GmbH

Auszeichnung der GFFT-Ehrenmitglieder

Vorwort

Seit neun Jahren besteht das Gremium zur Auswahl der Ehrenmitglieder bei der GFFT. Während dieser Zeit hat das Gremium zuerst unter Leitung von Prof. Dr. Wolfgang Bibel und seit drei Jahren unter der Leitung von Dr. Harald Schöning herausragende Persönlichkeiten ausgewählt und geehrt.

Der Forschungstransfer zwischen Wissenschaft und Wirtschaft ist eines der wichtigsten Anliegen der GFFT, insbesondere die systematische Überführung von neuen Ideen und Technologien in die Wirtschaft. Eine wichtige Aktivität bei der Verfolgung dieses Zieles ist die Ehrung von Persönlichkeiten, die sich um die Förderung universitärer, institutioneller oder industrieller Forschung, deren Verzahnung oder um die daraus resultierende Entwicklung und Innovation in Deutschland besonders verdient gemacht haben.

Ihre besondere Würdigung soll dazu führen, jungen Nachwuchskräften Vorbilder aufzuzeigen und sie zu eben solchen Leistungen zu animieren. Denn gerade in der Welt der Digitalisierung wird es immer wichtiger, die Visionen und Ergebnisse aus der Forschung in die Welt der Wirtschaft zu übertragen und auch zum Erfolg zu führen. Dazu braucht es Menschen, die sich engagiert und hartnäckig für ihre Ziele einsetzen.

Über den Autor

Dr. Harald Schöning

Leiter des Gremiums zur Auswahl der GFFT-Ehrenmitglieder

Würdigung

Von Herrn Prof. Dr.-Ing. habil. Raymond Freymann

durch Prof. Dr. h.c. mult. Hartmut Raffler

Erfolgreiche Innovationen werden von kreativen, querdenkenden Menschen geschaffen, die bestehende Geschäftsmodelle hinterfragen, die den intensiven Dialog mit Forschungseinrichtungen suchen, die unkonventionelle Ideen entwickeln und fördern. Prof. Dr. Raymond Freymann ist solch ein kreativer Querdenker mit enormer fachlicher Breite.

Prof. Dr.-Ing. habil. Raymond Freymann

Wir blicken auf eine außergewöhnliche Persönlichkeit und auf eine bemerkenswerte Karriere. Beeindruckend ist die Bandbreite seiner wissenschaftlich-technischen Veröffentlichungen, die von der Flugzeug- bis zur Automobiltechnik reichen. Herr Freymann veröffentlichte mehr als 150 Beiträge, die international große Anerkennung finden. Zu seinen Publikationen gehört außerdem ein Lehrbuch. Der Hugo-Junkers Preis und mehrere Best Paper Awards wurden ihm verliehen. Außerdem meldete er rund 50 Patente national und international an.

Herr Prof. Dr. Raymond Freymann wurde 1952 in Esch-sur-Alzette (Luxemburg) geboren. Nach dem Abitur studierte er Maschinenbau mit Schwerpunkt Luft- und Raumfahrt an der TU Braunschweig. Danach begann er eine fast 10-jährige Forschungstätigkeit am Institut für Aeroelastik des Deutschen Zentrums für Luft- und Raumfahrt in Göttingen. Übrigens werden mit Aeroelastik physikalische Vorgänge beschrieben, die an umströmten, elastischen Strukturen entstehen. Während seiner Forschungstätigkeit am Institut für Aeroelastik des DLR promovierte er 1981 an der TU Braunschweig.

Danach arbeitete er als Gastwissenschaftler im Flight Dynamics Laboratory der US Air Force in Dayton, Ohio. Raymond Freymann leistete wesentliche Beiträge für die Konstruktion von Flugzeugen im

Bereich der Aeoroelastik. Außerdem trug er entscheidend zu aktiv gedämpften Flugzeugfahrwerksystemen bei.

Trotz seiner herausragenden technisch-wissenschaftlichen Erfolge, verließ er die Flugzeugtechnik und wandte sich erdgebundenen Fahrzeugen zu, nämlich dem Automobil. 1986 startete er eine Karriere bei BMW in München. Zunächst war Raymond Freymann in dem im Aufbau befindlichen Forschungszentrum verantwortlich für die Abteilung Akustik und Strukturdynamik und übernahm dann die Hauptabteilung Fahrzeugphysik mit den Aufgabengebieten Akustik, Schwingungskomfort, Aerodynamik und Wärmetechnik. Anschließend leitete er die Hauptabteilung Fahrzeugforschung. Im Jahre 2000 habilitierte sich Raymond Freymann auf dem Gebiet der Strukturdynamik am Lehrstuhl für Angewandte Mechanik der TU München. Nebenbei bemerkt, die Strukturdynamik ist ein äußerst komplexes Gebiet, das sich mit dem dynamischen Verhalten von elastischen Systemen befasst. Im Jahre 2002 wurde er an die TU München als Honorarprofessor berufen.

Die Geschäftsführung der BMW Forschungs- und Technikgesellschaft übernahm Raymond Freymann 2003. Die BMW Forschung und Technik GmbH, ein Think Tank der BMW-Group, ist eine hundertprozentige Tochter der BMW AG mit ca. 200 Mitarbeitern. Sie hat die Aufgabe, neuartige Fahrzeugkonzepte zu entwickeln, unabhängig von der aktuellen Produktpalette. Herr Freymann verantwortete damals in der Forschungs- und Technik GmbH die Themenbereiche Fahrzeugtechnik, Wasserstofftechnologien, alternative Antriebskonzepte und Energiemanagement, Fahrerassistenzsysteme und aktive Sicherheit sowie die Informations- und Kommunikationstechnologien.

Den wirkungsvollen Technologietransfer in die spätere Serienfertigung gestaltete Raymond Freymann so, dass bereits in den verschiedenen Forschungsphasen die entsprechenden Produktabteilungen eingebunden waren. Die firmenrechtliche Eigenständigkeit erlaubte maximalen Freiraum und eine hohe Flexibilität. Kooperationen mit internationalen Forschungseinrichtungen waren für Raymond Freymann essenziell. Den Zugang zu neuen Trends und Technologien erlaubte u. a. ein Netzwerk mit Stützpunkten in USA, Japan und Frankreich.

Federführend beteiligt war Raymond Freymann mit seinem Team an der Entwicklung des BMW H2R, ein Versuchsfahrzeug mit Wasserstoffantrieb. Ziel für Freymann war es, einen Antrieb zu entwickeln, der kein CO2 emittiert. Im Gegensatz zu Wettbewerbern setzte Raymond Freymann nicht auf die Brennstoffzelle, sondern auf einen modifizierten konventionellen Ottomotor, der neben Benzin auch Wasserstoff verbrennen kann. Bekannt wurde das Versuchsfahrzeug nicht nur durch den umweltfreundlicheren Wasserstoffantrieb, sondern auch durch eine Reihe von Geschwindigkeitsrekorden im Jahre 2004 auf der BMW-Teststrecke in Miramas in Südfrankreich.

Der wasserstoffbetriebene H2R erreichte eine Höchstgeschwindigkeit von 302 km/h. Freymann und sein Team bewiesen also bereits vor 15 Jahren, dass Wasserstoff eine umweltfreundliche Brennstoffquelle für Fahrzeuge sein kann und dass der Wasserstoffantrieb im Prinzip serienreif ist.

Voraussetzung für den breiten Einsatz, solcher Fahrzeuge ist allerdings die entsprechende Wasserstoffinfrastruktur. Aber auch damit beschäftigte sich Freymann.

In einer visionären Veröffentlichung 2011 zeigte er Wege auf, wie der aus Wind- und Sonnenenergie erzeugte Wasserstoff für Kraftstoffe auf der Basis von LOHC (Liquid Organic Hydrogen Carrier) genutzt werden kann. Wasserstoff wird bei diesem Verfahren an eine organische Trägerflüssigkeit gebunden und lässt sich so gefahrlos transportieren. Für LOHC - Kraftstoffe kann somit die bestehende Infrastruktur an Tankstellen verwendet werden. Übrigens wurden Forscher für den Deutschen Zukunftspreis 2018 nominiert, die das LOHC-Prinzip zur industriellen Reife weiterentwickeln.

Ein wichtiges Forschungsgebiet als CEO bei der BMW Forschungs- und Technik GmbH waren für ihn die Informations- und Kommunikationstechnologien. In diesem Kontext lernte ich Herrn Raymond Freymann im Feldafinger Kreis kennen, dessen Sprecher zu dieser Zeit Wolfgang Wahlster und ich waren. Herr Freymann erkannte sehr früh die Bedeutung der Software und des Internet der Dinge (IoT) für die Automobiltechnik. Er propagierte bereits 2008 in einer Studie des Feldafinger Kreises die Vernetzung von Fahrzeugen untereinander und mit ihrer Umgebung. Auf diese Weise lassen sich, so Raymond Freymann, Fahrerassistenzsysteme realisieren, die die Sicherheit aller Verkehrsteilnehmer signifikant erhöhen, den Verkehrsfluss verstetigen und die Umweltbelastung reduzieren. Für selbstfahrende Automobile entwickelte Freymann Technologien, die 2010 autonomes Fahren auf öffentlichen Autobahnen mit einer Geschwindigkeit von bis zu 130 km/h ermöglichten. Ungefähr 5000 km wurden auf diesen Straßen voll autonom zurückgelegt.

Freymann plädierte außerdem für eine Kommunikationsplattform, die sowohl Echtzeitübertragung von Datenpaketen für sicherheitsrelevante Anwendungen als auch den zeitunkritischen Transfer großer Datenmengen für kommerzielle Anwendungen ermöglicht. In Zusammenarbeit mit der TU München untersuchte Raymond Freymann bereits 2009 mit seinem Team die Anwendbarkeit von IP-Netzen für die Fahrzeugkommunikation, also die Kommunikation zwischen Steuergeräten und Sensoren, die höchsten Echtzeitanforderungen genügen muss. Ein weiterer Beweis seines unkonventionellen Denkens.

Raymond Freymann hat neben seiner wissenschaftlichen und beruflichen Tätigkeit den Forschungstransfer durch sein Engagement in vielen internationalen Gremien gefördert. Er war beispielsweise Mitglied der NATO Advisory Group for Aerospace Research and Development (AGARD), im American Institute of Aeronautics and Astronautics (AIAA), in der Society of Automotive Engineers (SAE), im Leitungskreis des Comite´ Superieur de la Recherche et de l´Innovation der Regierung in Luxemburg und im Feldafinger Kreis.

Seine Erfahrungen und sein breites Wissen bringt Raymod Freymann heute u.a. in das European Institute for Innovation and Technology Digital (EIT Digital) ein. Er ist in diesem Institut Vorsitzender des Aufsichtsrates. Das EIT Digital hat sich zum Ziel gesetzt, die digitale Transformation Europas zu fördern. EIT Digital unterstützt u.a. Existenzgründungen, konzipiert und begleitet europaweit

zertifizierte Master- und Doktorandenprogramme, kooperiert mit mehr als 180 Großunternehmen, KMUs, Forschungszentren und Universitäten, um ein Ökosystem zu schaffen, in dem Innovationen gedeihen.

Raymond Freymann sagte einmal: „Die Zukunft kommt alleine, der Fortschritt nicht." Sie, Herr Freymann, leisten und haben viel geleistet, um den Fortschritt zu ermöglichen. Mit Ihren Erfolgen gestalten Sie die Zukunft. Die Gesellschaft zur Förderung des Forschungstransfers ehrt Sie, Herr Prof. Dr. Raymond Freymann, für Ihre außergewöhnlichen Verdienste mit der Ernennung zum Ehrenmitglied.

Über den Autor

Prof. Dr. h.c. mult. Hartmut Raffler

GFFT-Ehrenmitglied

Würdigung

Von Frau Prof. Dr. Claudia Eckert

durch Prof. Dr. Johannes Buchmann

Prof. Dr. Claudia Eckert

Nach dem Studium der Informatik an der Universität Bonn wurde Frau Eckert 1993 an der TUM in Informatik promoviert und habilitierte sich im Jahre 1999 ebendort mit einer Arbeit zum Thema „Sichere verteilte Systeme: Modelle und System-Architekturen“. Nach Gastprofessuren an der Universitäten Kiel und an der LMU München, nahm Frau Eckert den Ruf auf eine Professur für IT-Sicherheit an der Universität Bremen an.

2001 folgte sie einem Ruf an die Technische Universität Darmstadt und baute dort den neu geschaffenen Lehrstuhl für IT-Sicherheit auf. Gleichzeit übernahm sie die Leitung des Fraunhofer Instituts für Sichere Informationstechnologie (SIT), das sie 10 Jahre lang bis 2011 verantwortlich leitete und zum führenden IT-Sicherheitsinstitut in Deutschland machte. An der TU Darmstadt gründete sie 2003 das Darmstädter Zentrum für IT Sicherheit, das durch die BMBF-Initiative Land der Ideen als Leuchtturm-Aktivität im Bereich Sicherheit ausgezeichnet wurde. 2007 gründete Claudia Eckert das hessische Exzellenz-Zentrum CASED zum Thema Sicherheit als In-Institut der TU Darmstadt.

Bis zu ihrem Wechsel nach München leitete sie das CASED Zentrum und war bis 2010 in dessen wissenschaftliche Leitung weiterhin eingebunden. Im Dezember 2008 folgte sie einem Ruf auf die W3 Professur für Sicherheit in der Informatik an der TUM, verbunden mit der Leitung einer neu aufzubauenden Fraunhofer-Projektgruppe am Standort München/Garching. Aufgrund der erfolgreichen Entwicklung wurde diese Projektgruppe 2011 bereits nach weniger als 5 Jahren zum Fraunhofer Institut für Angewandte und Integrierte Sicherheit (AISEC). Das Institut hat sich in kurzer Zeit sowohl in der wissenschaftlichen Community als auch am Standort hervorragend etabliert. Mit über 100

Mitarbeiterinnen und Mitarbeiter erforscht und entwickelt das Institut Sicherheitstechnologien, wie beispielsweise neue Technologien zum physikalischen Schutz von Komponenten (beispielsweise für den Bereich des Produktschutzes von Interesse), vertrauenswürdige Software-Bausteine, um beispielsweise Komponenten in Fahrzeugen beweisbar sicher zu schützen, oder auch neue Test- und Analyseverfahren, wie beispielsweise neuartige Fehleranalysen unter Nutzung von speziellen Lasermessplätzen. Frau Eckert hat mit dem Aufbau des Fraunhofer AISEC mit dessen sehr enger Anbindung an die TUM ein Competence Center für IT Sicherheit an der TUM etabliert und international sichtbar gemacht.

In ihrer universitären Forschung hat Claudia Eckert Beiträge zu vielen wichtigen Themen geleistet. Sie entwickelt neue Konzepte, Methoden und Technologien, um die Sicherheit und Vertrauenswürdigkeit von IT-basierten Systemen und Anwendungen zu erhöhen. Damit trägt Claudia Eckert wesentlich dazu bei, die Sicherheit im Cyber-Raum und den Schutz der kritischen Informationsinfrastrukturen zu gewährleisten, der eine existenzielle Aufgabe des 21. Jahrhunderts ist. Frau Prof. Eckert hat ihre wissenschaftlichen Arbeiten in über 140 begutachteten Konferenzen veröffentlicht. Ihr Lehrbuch IT-Sicherheit ist bereits in der 8. Auflage erschienen und gilt als deutschsprachiges Standardwerk für die Ausbildung (sowohl universitäre Ausbildung als auch betriebliche Weiterbildung).

Schwerpunkte der Forschungsarbeiten von Frau Eckert liegen derzeit in den Bereichen der Entwicklung von Konzepten und Methoden zur Erhöhung der Sicherheit von System-Architekturen, insbesondere im Bereich der eingebetteten Systeme und des Trusted Computings, der Entwicklung neuer und verbesserter Verfahren zur Erkennung von Angriffen basierend auf maschinellen Lerntechniken, der Weiterentwicklung von virtuellen Maschinen zur Erhöhung der Systemsicherheit, der Entwicklung von datenschutzgewährenden Verfahren insbesondere für den Einsatz in medizinischem Umfeld, sowie von sicheren Multiparty Protokollen, die insbesondere auch im Cloud-Computing zum Einsatz kommen werden.

Die Lehre der Studierenden liegt Frau Eckert sehr am Herzen, was diese in hohem Maße schätzen. Sie hat exzellente Beurteilungen bei ihren Hörern. An der TU München hat Frau Eckert ein umfassendes Lehrangebot entwickelt, das sowohl breit angelegte Grundlagenvorlesungen zu den Themen IT-Sicherheit, Kryptographie und mobiler Sicherheit, als auch Vertiefungsvorlesungen zu Themen wie Eingebettete Sicherheit, Sensornetzsicherheit oder auch Maschinelle Lernverfahren zur Anomalie-Erkennung umfasst. Sie bietet Sicherheits-Praktika an, die bei den Studierenden überaus nachgefragt sind und organisiert zusammen mit ihren Mitarbeitern ein Team, das an dem internationalen Capture-of-the-Flag Wettbewerb (ein internationaler Hackerwettbewerb) an dem Studierende, aber auch Mitarbeiter von Firmen mit hohen Engagement in ihrer Freizeit teilnehmen, um vertiefte Kenntnisse im Bereich IT-Sicherheit zu erarbeiten.

Das herausragende Engagement und die Fähigkeiten Prof. Eckerts als Hochschullehrerin wurden bereits zweimal mit dem Preis für die beste Lehre, einmal an der TU Darmstadt und einmal an der TU München, gewürdigt.

Die hohe Anerkennung Frau Eckert in der Wissenschaft genießt, wird zum einen durch ihre Mitgliedschaft in der Akademie der Technik-Wissenschaften (acatech) und der Bayerischen Akademie der Wissenschaften verdeutlicht. Zum anderen unterstreichen ihre Berufungen als Mitglied in zahlreiche wissenschaftliche Beiräte, die Anerkennung, die Frau Eckert als Expertin genießt. So ist sie Mitglied des Vorstandes des Münchner Kreises, Mitglied des Vorstands des Sicherheitsnetzwerks München e.V und im Kuratorium der PTB, Braunschweig. Sie ist auch Sprecherin der Plattform IT Sicherheit des Zentrums Digitalisierung, Bayern, Mitglied des Beirats des Bavarian Instituts of digital Transformation und Mitglied des Kuratoriums der Volkswagen Stiftung.

Das Engagement und der Erfolg von Frau Eckert als Wissenschaftlerin, Hochschullehrerin und Wissenschaftsmanagerin sind außergewöhnlich. Bereits in jedem einzelnen Bereich sind ihre Leistungen überdurchschnittlich, aber die Kombination ist einzigartig. Und all das tut sie in einem Bereich von so außerordentlicher gesellschaftlicher und wirtschaftlicher Bedeutung – Cybersicherheit und Privatheit. Sie deckt damit den gesamten Bereich ab: von der grundlegenden Forschung, über die Anwendungsentwicklung und die Ausbildung von Expertinnen und Experten bis zur wirtschaftlichen Verwertung und trägt damit in besonderer Weise zum Forschungstransfer bei. Ich könnte mir keine geeignetere Person für die Ehrenmitgliedschaft der GFFT vorstellen.

Über den Autor

Prof. Dr. Johannes Buchmann

GFFT-Ehrenmitglied

Security

Vorwort

Sehr geehrte Damen und Herren,

Digitalisierung ist unumstritten der größte Trend für Unternehmen. Aber: Nur wer Cybersicherheit die nötige Bedeutung beimisst, wird Digitalisierung weiterhin vorantreiben können. Wir leben in einer zunehmend vernetzten und digitalisierten Welt. Das ist gut, denn noch nie zuvor waren wir technisch so verbunden wie heute. Über Länder- und Kulturgrenzen hinaus können wir Wissen und Daten austauschen – und so Isolation durchbrechen.

Eine Vernetzung bis in den letzten Winkel ist also unabdingbar, wenn wir für jeden eine gleichberechtigte Teilhabe am gesellschaftlichen, wirtschaftlichen und kulturellen Leben ermöglichen wollen. Gleichzeitig steigt damit aber auch die Angriffsfläche und -möglichkeit für Kriminelle und staatliche Organisationen. Die ersten erfolgreichen Ransomware-Attacken auf Krankenhäuser und Wirtschaftsunternehmen haben genau das verdeutlicht. Allein in den letzten zwölf Monaten registrieren wir beispielsweise DDoS-Angriffe aus Bot-Netzwerken von bisher unbekannter Größenordnung.

Dieser Trend wird sich fortsetzen und dann ganze Wirtschaftsbereiche, hunderttausende von Privatkunden, aber auch die politische Handlungsfähigkeit eines Landes bedrohen können. Vor 20 Jahren hatten wir es lediglich mit einer Handvoll Viren und Würmern zu tun, heute wächst mit fortschreitender Vernetzung nicht nur die Angriffsfläche proportional – auch Cyberkriminelle agieren organisierter und zielgerichteter denn je.

Digitalisierung erfordert also in erster Linie neuen Formen der Unternehmensorganisation. Cyber Security spielt dabei eine zentrale Rolle. Nur wenn Unternehmen die Bedrohungen und die daraus resultierenden Anforderungen erkennen, gibt es eine Chance Prozesse umzubauen und einen wirklichen Imagewandel zu vollziehen. Nicht nur der technische Aspekt ist hier also entscheidend, vor allem auch die Sensibilität und Widerstandsfähigkeit der eigenen Mitarbeiter muss dem aktuellen

Stand der „neuen“ Bedrohungslage entsprechen. Das alles braucht seine Zeit - ist aber zwangläufig notwendig, damit Deutschland im globalen Markt zukunftsfähig bleibt. Es ist das Anliegen des Vereins - und auch mein ganz persönliches, einen Beitrag zu leisten, damit auch die nächsten Generationen die Möglichkeit haben aktiv mitzugestalten. Gelingen kann dies nur, wenn Wissenschaft, Forschung und Wirtschaft eng zusammenarbeiten.

Ich freue mich deshalb sehr von der GFFT als neues Beiratsmitglied im Security Lab ernannt worden zu sein. Allen Teilnehmerinnen und Teilnehmern einen wertvollen Austausch auf dem diesjährigen Treffen.

Ihr
Thomas Tschersich

Über den Autor

Thomas Tschersich

Senior Vice President Internal Security & Cyber Defense
T-Systems International GmbH

Security

Container Apps als Herzstück des sicheren mobilen Arbeitens

Der Einsatz mobiler Geräte ist für Unternehmen mit erheblichen Sicherheitsrisiken verbunden. Trotzdem ist es möglich, eine sichere mobile Systemumgebung aufzubauen.

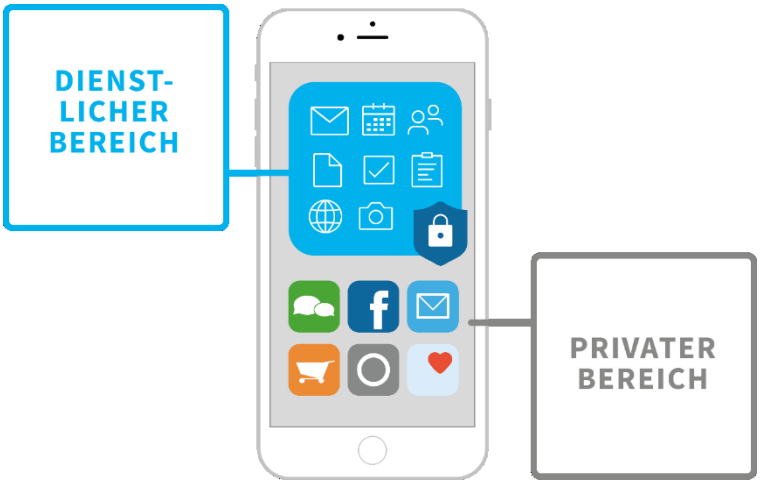
Mobile Endgeräte sind in der heutigen Arbeitswelt nicht mehr wegzudenken, da sie ein wichtiger Bestandteil für flexibles Arbeiten sind. Laut einer aktuellen Studie von bitkom setzten 2018 bereits 39% der Unternehmen auf mobiles Arbeiten im Home Office. Zum Vergleich: 2014 lag dieser Wert bei nur 22%. Rechnet man weitere Einsatzmöglichkeiten für mobiles Arbeiten, beispielsweise beim Kunden, auf Dienstreisen oder beim täglichen Pendeln mit dazu, dürfte dieser Wert noch deutlich höher liegen.

Mobiles Arbeiten und IT-Sicherheit

Als (IT-) Entscheider steht man daher immer noch vor Herausforderungen: Smartphone und Tablet werden von Nutzern in "unsicheren Umgebungen" eingesetzt, also außerhalb geschützter Systemumgebungen. Die IT hat daher mobile Systeme nur bedingt unter Kontrolle – und würde die Nutzung daher am liebsten verbieten. Noch schwieriger wird es, wenn Mitarbeiter ihre privaten Geräte für dienstliche Aufgaben nutzen. Mobile Geräte und Apps selbst werden zudem bei Cyberkriminellen immer beliebter, da sie vermehrt für den Zugriff auf Unternehmensinformationen eingesetzt werden.

Unternehmen müssen daher verschiedene Hürden überwinden, wenn sie ihren Mitarbeitern mobiles Arbeiten ermöglichen möchten. So muss eine sichere mobile Systemumgebung alle Anforderungen hinsichtlich Datensicherheit und Datenschutz erfüllen. Gleichzeitig darf diese den Mitarbeiter beim mobilen Arbeiten nicht einschränken. Am einfachsten lassen sich die genannten Herausforderungen mit der Container-Technologie meistern.

Überblick: Was ist eine Container-App?



Die Container-Technologie legt im Gegensatz zu anderen Ansätzen den Fokus auf den Schutz von Daten auf mobilen Endgeräten. Berufliche Anwendungen und Daten befinden sich in einem abgeschotteten Bereich (Container) auf dem Smartphone oder Tablet. So wird verhindert, dass Daten manipuliert werden oder abfließen können. Die Unternehmensdaten werden in der Container-App gespeichert, die durch PIN, Passwort, TouchID oder FaceID geschützt ist. Andere Apps haben keinen Zugriff auf die Daten im Container. Container-Lösungen sind für sämtliche Branchen umsetzbar und kommen sowohl im Behörden- als auch im Unternehmensumfeld zum Einsatz.

So wichtig Lösungen für MDM (Mobile Device Management), die mobile Geräte zentral verwalten, grundsätzlich sein mögen, für die Sicherung der auf mobilen Geräten befindlichen Daten und Anwendungen reichen sie keinesfalls aus. Dafür müssen unmittelbar auf dem jeweiligen mobilen Gerät die privaten und die dienstlichen Daten und Anwendungen strikt voneinander getrennt werden. Nur wenn beide Bereiche voneinander abgeschottet sind, wenn das mobile Gerät gewissermaßen aus zwei virtuellen Systemen besteht, kann es auch mit hinreichender Sicherheit betrieben werden.

Realisieren lässt sich dieses Konzept mit einer Container-Lösung. Ein solcher Container ist ein automatisch verschlüsselter Bereich, in dem Unternehmensdaten, E-Mails, Kontakte, Kalender, Notizen, Aufgaben und Dokumente gespeichert werden. Auch firmeneigene Apps lassen sich auf einfache Art und Weise „Containerisieren“. Auch im Falle von Diebstahl oder Verlust des Geräts bleiben die Daten auf diese Weise vor Missbrauch geschützt. Der Container verhindert auch, dass Mitarbeiter aus dem sicheren Unternehmensbereich auf eine private App zugreifen oder Daten etwa mit Copy-and-Paste in den privaten Bereich übernehmen. Andere Anwendungen erhalten grundsätzlich keinen Zugriff auf die Inhalte des Containers; so kann beispielsweise WhatsApp daraus keine Kontaktdaten übernehmen, was vor allem im Hinblick auf die Einhaltung der DSGVO-Vorgaben wichtig ist.

Eine Container-Lösung schützt nicht nur die Daten und Anwendungen des Unternehmens, sondern im BYOD-Fall zugleich auch die Privatsphäre der Eigentümer. IT-Administratoren haben keinen Zugang zum Gerät, sondern steuern immer nur den Container, ein MDM ist damit nicht nötig. Es ist also kein Problem die gesetzlichen Anforderungen hinsichtlich des Schutzes der Privatsphäre einzuhalten. Auf der anderen Seite können Unternehmen damit auch die rechtlichen Vorgaben für den Schutz der Unternehmensdaten einhalten, etwa bezüglich personenbezogener Daten von Kunden, Lieferanten, Geschäftspartnern und Mitarbeitern, die ja regelmäßig in E-Mails und Dokumenten

enthalten sind. Unternehmen sind gesetzlich für die Einhaltung des Datenschutzes bei der Verarbeitung personenbezogener Daten verantwortlich, was auch gilt, wenn Mitarbeiter private mobile Endgeräte dafür benutzen.

Was sind die Anforderungen an eine Container App?

Eine gute Container-App enthält alle nötigen Basisanwendungen wie E-Mail, Kontakte oder einen Kalender, Zugriff auf wichtige Systeme, die ohne großen Schulungsaufwand sofort genutzt werden können. Es darf für die Nutzer keinen Grund geben, Apps außerhalb des Containers betrieblich zu verwenden. Dabei spielt die Benutzerfreundlichkeit eine wichtige Rolle. Die User bzw. Mitarbeiter müssen wissen, wie sie die App nutzen und wie sie beispielsweise eine verschlüsselte oder signierte E-Mail versenden. Zuletzt ist das Thema Verschlüsselung zu nennen. Daten müssen dabei nicht nur im Container, sondern auch während der Kommunikation mit der Unternehmens-IT verschlüsselt sein. Mittels Ende-zu-Ende Verschlüsselung bleibt so z.B. eine E-Mail vom Absender bis zur Entschlüsselung beim Empfänger auf allen Datenstrecken vor dem Zugriff durch Dritte geschützt. Außerdem sollte kontrolliert werden, wer über welches Endgerät Zugriff auf Unternehmensressourcen erhält.

Hierfür müssen genaue Zugriffsrechte und Sicherheitsvorkehrungen definiert und spezielle Gateways eingerichtet werden. Beispielsweise sollte ein Zugriff auf den Microsoft Exchange Server mittels TLS-Verschlüsselung erfolgen, Zugriffe auf ActiveSync Server oder auf Intranet-Anwendungen durch zertifikatsbasierte Authentifizierung.

Über die Autoren

Günter Junk

CEO, Virtual Solution AG
Mitglied der GFFT Security Lab Community

Regina Hoffmann

Marketing Director, Virtual Solution AG
Mitglied der GFFT Security Lab Community

Security

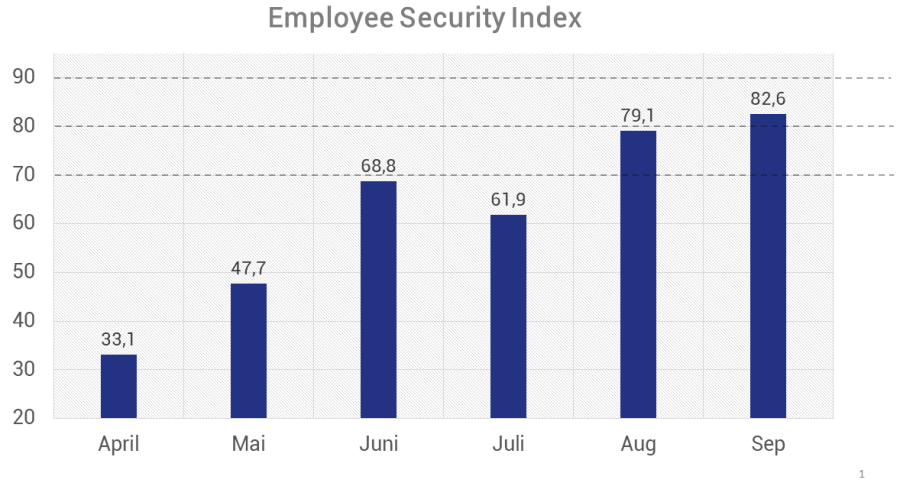
Security Awareness – Training für Mitarbeiter

Die größte Sicherheitslücke in Unternehmen sind oft die eigenen Mitarbeiter. So können Angestellte mit einem einzigen Klick auf einen manipulierten E-Mail-Link die gesamte IT-Infrastruktur lahmlegen. Gut geschulte Mitarbeiter sind ein Garant in der IT-Security Strategie jedes Unternehmens.

Diesen Lösungsansatz fokussiert das junge Technologieunternehmen IT-Seal und trainiert Mitarbeiter mit Spear-Phishing-Mails und anderen Social Engineering Simulationen passgenau, auf Ihre individuellen Bedürfnisse.

Damit diese Weiterbildung unkompliziert funktioniert hat IT-Seal ein Weiterbildungskonzept entwickelt, welches kürzlich die zweite Platzierung der Awareness Security Initiative des Jahres erhielt. Die IT-Seal Phishing Akademie ist ein "learning-by-doing"-Awareness Training, das in den Alltag von Mitarbeitern integriert ist und auf den neuesten wissenschaftlichen Erkenntnissen der Pädagogik basiert. Teilnehmer erleben selbst eine simulierte Bedrohung und lernen genau die Fähigkeiten, die sie benötigen, um in ihrer digitalen Selbstverteidigung erfolgreicher und effektiver zu werden.

Mit Ihren respektvollen Simulationen ermöglicht das Darmstädter Cybersecurity Startup ein kontinuierlich hohes IT-Sicherheitsbewusstsein bei Ihren Kunden. Der kürzlich zum Patent angemeldete Employee Security Index® - kurz ESI, ist nur ein Beispiel für die Innovationskraft, welche Ihren Start in einer Masterthesis an der TU Darmstadt hatte. Hier legte David Kelm, Best Student Award Gewinner des Bundesamts für Sicherheit in der Informationstechnik (BSI) die Grundlage für transparente und Nachhaltige IT-Sicherheit für den Faktor Mensch.



IT-Seal bietet „learning by doing“ Security Awareness Simulationen an und erhöht praxisnah das IT-Sicherheitsbewusstseins von Mitarbeitern - kontinuierlich und nachhaltig, dies ist das Leistungsversprechen. Den Mitgliedern von Hessenmetall will IT-Seal als vertrauensvoller Partner an Ihrer Seite stehen. Gemeinsam mit Ihren Mitarbeitern lässt sich eine IT-Sicherheitskultur etablieren, um die Digitalisierung erfolgreich zu begleiten.

Die Gründung erfolgte 2016, heute zählen namhafte Unternehmen aus zahlreichen Branchen - vom Mittelstand zum MDAX-Konzern - zu Kunden von IT-Seal. Es folgte die Auszeichnung TOP10 Cyber Security Startup Europa und die Auszeichnung als Best6es Cybersecurity Startup 2018.

Über den Autor

Alex Wyllie

Head of Business Development Marketing & Sales
IT-Seal GmbH

Security

Threat Intelligence: Cyber-Abwehrstrategien ganzheitlich denken

Sicherheitskomponenten, die allein auf den Schutz vor Cyber-Bedrohungen ausgelegt sind, kommen schnell an ihre Grenzen. Zentrale Bausteine für eine erfolgreiche Cyber Abwehrstrategie sind die schnelle Entdeckung und Beurteilung bekannter wie auch unbekannter Schadsoftware und Angriffsmuster.

Vor dem Hintergrund der sich wandelnden digitalen Anforderungen funktionieren klassische IT-Security-Mechanismen zum Schutz vor Angreifern und zur Abschottung des Unternehmensnetzwerks nur noch bedingt. Für den Fortbestand und Erfolg von Unternehmen ist es entscheidend, zeitnah über aktuelle Bedrohungen, die Risiken für die digitalen Geschäftsprozesse, System und Daten darstellen, Bescheid zu wissen, um schnell reagieren zu können. Aktuelle Bedrohungen verlangen daher neue Konzepte: Zentraler Bausteine für eine erfolgreiche Cyber Abwehrstrategie sind die schnelle Entdeckung und Beurteilung bekannter und unbekannter Schadsoftware und Angriffsmuster. Genau hier setzt Threat Intelligence an: Die sogenannte Threat Intelligence-Schicht entfaltet ihren Nutzen zusätzlich zu klassischen Schutzmaßnahmen in der Kombination aus Prävention und Überwachung für einen ganzheitlichen Schutz vor Cyber Bedrohungen und eine schnelle Reaktion bei Vorfällen.

Prävention: Vulnerability Managament

Kern von Threat Intelligence bildet die automatisierte Analyse und Erkennung von Schwachstellen im Firmennetz durch ein effektives Vulnerability Management. Ziel ist es dabei, rechtzeitig über aktuelle Angriffspunkte durch bekannte Schadsoftware und Schwachstellen im eigenen Firmennetz informiert zu sein, um mögliche Risiken zu entschärfen. Von schwachen Zugangsdaten, über fehlende Patches und Netzwerkfreigaben bis hin zu Fehlkonfiguration sollten Schwachstellen im eigenen Netz automatisch erfasst, gesammelt, priorisiert und im Entwicklungsverlauf dargestellt werden. Dadurch sind eine Risikobewertung sowie das Ableiten von Maßnahmen zur Beseitigung der Schwachstellen möglich.

Überwachung: Anomalie Erkennung

Gerade in kritischen Umgebungen wie Industrieanlagen oder Netzleitständen ermöglicht eine permanente Analyse des Datenverkehrs und der Kommunikationsbeziehung die Erkennung von Anomalien im Netzwerk. Sicherheitskritische Auffälligkeiten wie beispielsweise Malware-Kommunikation, ungewöhnliche oder veränderte Datenpakete, unbekannte Netzwerkteilnehmer oder Verbindungen lassen sich genauso detektieren wie Netzwerkprobleme oder sogar Anlagenfehler. Es werden so auch Gefährdungen und Kommunikationsmuster sichtbar, die bislang unbekannt sind oder schleichend agieren. Dieses ermöglicht gerade in Bereichen, die störungsfrei laufen müssen eine ganzheitliche und dabei passive, rückwirkungsfreie Störungsabwehr, ohne die kritischen Systeme zu belasten.

Intelligence: SIEM als Unterstützung im Umgang mit Sicherheitsvorfällen

Für eine gute Klassifizierung und Analyse von Events liefern Security Incident and Eventmanagement-Systeme (SIEM) als übergeordnete und intelligente Tools die erforderliche Transparenz in einer größeren Security-Landschaft und bieten so ein aktuelles Bild der Sicherheitslage. Für den erfolgreichen Einsatz ist hierbei die zur Bedrohungslage und Risikobetrachtung passende Auswahl der richtigen Usecases sowie die Aufbereitung der relevanten Daten wichtig, um effektiv reagieren und schnell Maßnahmen ableiten zu können. Ergänzende „Playbooks“ mit Handlungsanweisungen helfen die Meldungen und Events richtig einzuordnen und bieten Ablaufpläne für die schnelle Reaktion auf bekannte und unbekannte Vorfälle. Richtig aufgesetzt unterstützt ein SIEM somit zusätzlich zur Prävention und Erkennung von Schwachstellen die IT Security-Mitarbeiter.

Management: Der ganzheitliche Ansatz

Der Erfolg von Threat intelligence hängt letztendlich davon ab, wie die eintreffenden Daten verarbeitet und daraus auch die entsprechenden Maßnahmen abgeleitet werden. Das erfordert, dass Mensch und Technik bestmöglich ineinandergreifen und Nutzer nicht einer Flut von Daten gegenüberstehen, deren Relevanz für die eigenen Systeme sie nicht abschätzen können. Der Einsatz eines branchenspezifischen Information Security Management Systems (ISMS) sollte hierbei die Grundlage für die Entscheidungsfindung und das Ableiten von Maßnahmen sein. So können geregelte IT Security-Abläufe, Transparenz über die Risiken und eine geeignete, pragmatische Vorgehensweise das Risiko durch Cyber Security-Angriffe bestmöglich minimieren.

Über den Autor

Dr. Stefan Rummenhöller

Geschäftsführer IT Security
r-tec IT Security GmbH

Security

Videokommunikation so einfach wie Telefonieren

Videokonferenzen und Unified Collaboration sind die Firmenkommunikation der Zukunft. Damit kommunizieren Unternehmen nicht nur schneller und effektiver, sondern sie erhöhen gleichzeitig ihre Produktivität. Die früher gängigen Telefonkonferenzen und Geschäftsreisen verschwenden Zeit, Geld und Ressourcen. Connect4Video will dafür sorgen, dass diese Zeiten der Vergangenheit angehören.

Sicher und einfach – so muss Videokommunikation sein, denn nur so wird sie von Anwendern akzeptiert. Das mussten in der Vergangenheit etliche Anbieter von Videokonferenz-Services und -Geräten leidvoll erfahren. Die Mitarbeiter in den Unternehmen lehnten ihre Technik ab, weil sie sie nicht bedienen konnten, ganz abgesehen davon, dass Heerscharen von IT-Spezialisten bezahlt werden mussten, um die verschiedenen Systeme überhaupt erst ins Laufen zu bringen. Und selbst wenn alles funktionierte, mussten die Konferenzsysteme im Firmennetzwerk außerhalb der Firewall platziert werden, damit sie mit einer öffentliche sichtbaren IP-Adresse von außen anwählbar waren. Allein dies bedeutete für die Sicherheitschefs der Firmen Alarmstufe Rot und war ein Killer-Argument gegen Videokommunikation.

Connect4Video hat diese Problemlage von Anfang an verstanden und aktiv überwunden. Der Kundenwunsch nach sicherer und einfacher Videokommunikation war und ist der Motor unseres Handelns. Dies begann 2007 mit der Entwicklung der ersten Firewall-Traversale, durch die Konferenzsysteme im sicheren Bereich hinter der Firewall stehen, aber per Tunnel mit außen kommunizieren können. Weiterhin erkannten wir früh, dass die sehr teuren Hardware-System durch günstige Desktop-Anwendungen verdrängt werden würden. Die Nutzer wollten keine umständliche Konferenzraumbuchung, sondern ständige Verfügbarkeit und spontane Meetings. Seit etwa 2010 drängen

entsprechende Lösungen auf den Markt, allerdings mit sehr unterschiedlicher Ausstattung und Qualität. Als Experten haben wir stets die leistungsfähigsten Anbieter gewählt, um unseren Kunden jeden Wunsch zu erfüllen und die optimal passende Lösung anzubieten. Momentan leisten dies hauptsächlich zwei sehr variable, skalierbare Dienste, die für Firmen jeder Größenordnung geeignet sind. Unsere Statistiken beweisen, dass dieses Konzept aufgeht und dass die Anzahl der Nutzer sowie der Konferenzminuten stetig steigen.

Die nächste Entwicklung – die noch immer andauert – ist die steigende Mobilität der Mitarbeiter. Videokonferenz-Clients müssen auf Mobilgeräten ebenso schnell und einfach zur Verfügung stehen wie auf dem Desktop. Meetings jederzeit und überall, egal ob Laptop, Tablet oder Smartphone. Unsere Produkte bringen entsprechende Apps bereits von Hause aus mit. Last but not least: die Sicherheit. Spätestens seit der DSGVO legen vor allem deutsche Unternehmen mehr denn je höchsten Wert auf Datenschutz und -sicherheit. Auch diese Ansprüche befriedigt Conect4Video: Wir betreiben unseren Dienst nach Wunsch auf deutschen, DIN-zertifizierten Servern nach deutschem Datenschutzrecht. Verschlüsselung der Konferenzen ist selbstverständlich. Wer sich also nicht dem Patriot Act der USA ausliefern möchte, liegt bei uns richtig. Unser Service beinhaltet zudem ein Customer Success Management, das mit Schulungen dem Kunden beim Ausrollen der Konferenzlösung im Betrieb hilft. Dazu braucht der Kunde nichts außer einem Internetanschluss. Keine Investition in neue Technik und teure Geräte mehr. In wenigen Minuten steht alles bereit.

Ziel von Connect4Video ist es, Videokommunikation als das Mittel der Wahl für schnelle, effektive Unternehmenskommunikation zu etablieren. Ein Videogespräch ist immer sinnvoller als ein Telefonat, denn die menschliche Kommunikation funktioniert hauptsächlich über Körpersprache, Mimik und Gestik. Mit Screensharing und Whiteboards ist die Videokommunikation genauso effizient und produktiv wie ein persönliches Meeting. Zudem ist Videokommunikation sogar günstiger als Telefonieren und spart Reisekosten und Zeit. Der Einstieg in die Videokommunikation fällt mit den Diensten von Connect4Video umso leichter, da sie keine zusätzlichen Hardwarekosten erfordern. Sie lassen sich ganz einfach mit den bereits im Unternehmen vorhandenen Geräten nutzen, also PC, Laptop, Tablet und Smartphone. Voraussetzung sind nur Kamera, Mikrophon und eine Internetverbindung. Die Bedienung der Software ist denkbar einfach. Sowohl persönliche Video-Anrufe als auch Einwahlen in eine Videokonferenz funktionieren genauso schnell wie Telefonanrufe.

Über den Autor

Andreas Zenger

Operations Manager
Connect4Video GmbH

Security

Sichere Nutzung von Microsoft Office 365 in Unternehmen

Produkte der Microsoft Office 365 Suite werden sich in Zukunft in vielen Unternehmen etablieren, da sie den Weg zum vernetzten Arbeiten über die Microsoft Cloud ebnen. Allerdings bietet diese keine persistente Verschlüsselungsmöglichkeit. Eine sicherere Dateiverarbeitung in der Cloud sogar ohne Änderung in der User Experience kann allerdings durch die Integration einer Cloud-Verschlüsselung erreicht werden.

In vielen Unternehmen haben sich Arbeitsabläufe mit bestimmter Software über Jahre etabliert. Hierzu kommen auch Möglichkeiten, Dateien über die Cloud eines großen Softwareanbieters extern allen Mitarbeitern des Unternehmens weltweit sehr performant verfügbar zu machen. Die neu geltende EU-DSGVO und das allgemein steigende Bewusstsein für den Schutz von Unternehmens- und Kundendaten in den vergangenen Jahren führen aber zu neuen Anforderungen an die Datensicherheit. Der Wunsch vieler Unternehmen ist es dabei, diese zu erhöhen, ohne ihre Geschäftsprozesse und die User Experience ihrer Mitarbeiter mit den Software-Produkten grundlegend zu verändern. Eine vollständige Umstellung auf eine andere, verschlüsselte Cloud-Lösung ist also meistens nicht gewünscht, da diese mit einem hohen Kosten- und Zeitaufwand verbunden wäre und viele dieser Lösungen nicht die gewünschte Performance für große Unternehmen bieten. Vielmehr soll mit allen Dateien in der Cloud wie bisher gearbeitet werden können und die Verschlüsselung „on top“ oder „nebenbei“ erfolgen.

Die Produktsuite Microsoft Office 365

Laut einer Studie von Gartner nutzten im Juli 2017 61% der Unternehmen Produkte von Microsoft Office 365. Im Vergleich dazu waren es im Juli 2014 erst 35%. Die Produktsuite zählt damit zu den etabliertesten in der deutschen Unternehmenslandschaft. Besonders die folgenden sechs Softwareprodukte kommen laut der Studie in mehr als der Hälfte der Unternehmen, die Microsoft-Cloud-Kunden sind, zum Einsatz: Office Pro Plus, Exchange Online und Outlook, OneDrive for Business,

SharePoint, OneNote und Skype for Business. Sie alle bieten den Austausch über die von Microsoft bereitgestellte Cloud an.

Hier wird natürlich von einer durch TLS/SSL gesicherten Internetverbindung zur Übertragung ausgegangen. Eine zusätzliche, die Internetverbindung überdauernde, also persistente Verschlüsselung der übertragenen Dateien findet aber nicht statt. Unternehmen, die auf Grundlage ihrer Information Security Policy, der Richtlinien des BSI oder der EU-DSGVO auf die sichere Verarbeitung und den besonderen Schutz der unternehmensinternen Dateien angewiesen sind, können diese Anforderung mit Microsoft Office 365 nicht vollständig umsetzen. Gleichzeitig ist es aber auch nicht erwünscht, das Produkt komplett zu verlassen und eine neue, zunächst fremde Cloud zu verwenden, die die geforderte Verschlüsselung anbietet. Die von Microsoft bereitgestellten Funktionen sind oft bereits in den Geschäftsprozessen des Unternehmens etabliert. Darüber hinaus sind komplett verschlüsselte Cloud-Lösungen gerade für große Unternehmen oft nicht performant genug. Es muss also eine Lösung gefunden werden, wie die Dateien innerhalb und während der Kommunikation mit der Microsoft Cloud verschlüsselt werden können.

Lösung: Integration in eine Cloud-Verschlüsselung

Werden die Produkte der Microsoft Office 365 Produktsuite in der Microsoft Cloud durch ein Unternehmen genutzt, so liegen in dieser alle mithilfe der Produkte erzeugten Dateien. Dort wird von verschiedenen Mitarbeitern auf sie zugegriffen, um Veränderungen an den Dateien durchzuführen. Um nun die Verschlüsselung anzuwenden, muss der Vorgang des Bearbeitens einer Datei durch einen Mitarbeiter und dessen Verarbeitung in der Cloud betrachtet werden. Wenn der Mitarbeiter mit den Dateien aus der Cloud arbeitet, kommunizieren die Office 365 Anwendungen während der Bearbeitung eigenständig mit dem Server. Die Daten werden immer bei Bedarf vom Server heruntergeladen oder an den Server gesendet. Dabei ist zu beachten, dass nicht auf Dateiebene kommuniziert wird, sondern mit Datenpaketen unterschiedlicher Größe. Somit ist eine lokale Kopie eines Dokumentes nicht mehr nötig und sämtliche Änderungen werden direkt auf dem Server gesichert. Eine klassische Dateiverschlüsselung ist also nicht möglich. Es muss daher dazu übergegangen werden, immer nur die heruntergeladenen Daten, die nur einen Teil der gesamten Datei darstellen, zur Bearbeitung lokal in einer sicheren Umgebung zu entschlüsseln und anschließend wieder verschlüsselt in die Datei auf dem Server einzufügen. Nur so kann eine lückenlose Sicherung der Daten gewährleistet werden. Hinzu kommt, dass auf diese Weise auch mehrere Mitarbeiter gleichzeitig an derselben Datei arbeiten können, was für die Verschlüsselung eine weitere Komplexitätsebene darstellt.

Herausforderungen bei der Integration etablierter Produkte in eine Verschlüsselungslösung

Microsoft verwendet zur Übertragung der Dateien in die Cloud ein eigenes Protokoll, das eine besonders hohe Performance der Datenverarbeitung gewährleistet. Hierbei werden die Dateien, die mehrere Mega- oder Gigabyte groß sein können, nicht als ein Element verarbeitet. Sie werden stattdessen in sehr viele kleinere Dateifragmente aufgeteilt, ohne dass diese ihre Verbindung zueinander verlieren. Zum einen kann so der Upload-Prozess einer komplett neuen Datei in die Cloud besser verarbeitet werden. Viel wichtiger ist aber, dass bei Änderungen an einer bereits in der Cloud

vorhandenen Datei nicht die gesamte Datei neu aktualisiert werden muss, sondern nur die von der Änderung betroffenen Fragmente. Da oft im Vergleich zur Dateigröße nur sehr geringe Datenmengen verändert werden, dieser Vorgang aber häufig und von mitunter mehreren verschiedenen Mitarbeitern auch gleichzeitig ausgeführt wird, liefert diese Strategie die höchste mögliche Geschwindigkeit der Datenverarbeitung in der Cloud mit für den Nutzer kaum wahrnehmbaren Verzögerungen.

Abbildung: Illustration einer beispielhaften Verschlüsselung der Datenfragmente in der Microsoft-Cloud

Auf der anderen Seite stellen die Erstellung und Zuordnung der Fragmente zur Originaldatei eine komplexe Ausgangslage für einen Verschlüsselungsalgorithmus dar. Die Herausforderung bei der Integration von Microsoft Office 365 in eine Cloud-Verschlüsselungslösung besteht darin, die Verschlüsselung der Dateifragmente so zu realisieren, dass sie unabhängig genug sind, um einzeln verändert zu werden. Dennoch fügen Sie sich nach den Änderungen durch den User und die anschließende erneute Verschlüsselung wieder passend in das Puzzle ein. Die größte Schwierigkeit liegt dabei besonders darin, diejenigen Dateifragmente zu identifizieren, in denen Veränderungen stattgefunden haben, ohne diese dabei zu entschlüsseln, sodass eine Ende-zu-Ende-Verschlüsselung für das Unternehmen gewährleistet bleibt. Eine weitere besondere Herausforderung bei der Ver- und Entschlüsselung der Dateifragmente liegt in der sich variabel ändernden Größe während ihrer Verarbeitung. Hierfür soll eine nahtlos integrierbare Lösung geschaffen werden. Nach der Analyse und Bewältigung der beschriebenen Herausforderungen steht einer verschlüsselten Nutzung der Microsoft Cloud und damit der etablierten und gleichzeitig sicheren Realisierung der Geschäftsprozesse in der Cloud nichts mehr im Weg.

Über die Autoren

Pia Bauspieß

Produktmanagerin
Applied Security GmbH

Veronika Röthel

Produktmanagerin
Applied Security GmbH

Security

Phishing- und Cybersecurity Fachchinesisch entziffert.

Begriffserklärung und Beispiele realer Angriffe

Phishing, Vishing, Sextortion & Co: Wussten Sie, dass über 91% aller erfolgreichen Cyberangriffe mit Phiishing begannen? Fakt ist: Phishing und phishingähnliche Techniken sind heute DER am weitesten verbreiteten und auch der gefährlichste Typ von Cyberangriffen. Es wird gezielt auf Schwachstellen des menschlichen Geistes abgezielt und verwandelt so jeden Mitarbeiter in eine potenzielle Hintertür zu Unternehmenswerten.

Kein Wunder, dass Cyberkriminelle Tag für Tag immer ausgefeiltere Phishing-Techniken erfinden. Erfahren Sie mehr über die verschiedenen Phishing-Typen und wie diese für echte Hacks verwendet wurden.

Smishing

Smishing ist eine Art Phishing, die per SMS durchgeführt wird. Es ist sehr einfach, aber für die Cyberkriminellen profitabel. Sie können eine SMS von einem unbekannten Mädchen erhalten, das Sie zu einem Date mit einem Link zu den Fotos in ihrem Profil in einem sozialen Netzwerk einlädt. Um das Profil zu sehen, müssen Sie sich natürlich zuerst auf der Phishing-Seite anmelden, mit der der Link verbunden ist. Ein weiteres beliebtes Thema solcher SMS ist "Problem mit Bankkonto oder Kreditkarte". In diesem Fall geht der Link zu einer Bank-Phishing-Seite. Im Allgemeinen kann das Thema einer solchen SMS unterschiedlich sein, aber das Muster ist immer das gleiche: die Benutzer dazu zu bringen, auf den Link zu klicken und ihre Zugangsdaten einzugeben.

OTP Bypass Phishing

OTP (One-Time-Password) ist ein Teil der Zwei-Faktor-Authentifizierung, die viele Personen zum Schutz ihrer Konten verwenden. Neben dem Login und dem Passwort benötigen Sie einen OTP, der Ihnen in der Regel per SMS zugesandt wird. Der Prozess sieht super sicher aus, aber jetzt haben Cyberkriminelle die Methoden erfunden, um diesen Schutz mit Phishing-Tricks zu umgehen. Stellen

Sie sich vor, Sie erhalten eine E-Mail mit einem Link zu Ihrem Konto mit Zwei-Faktor-Authentifizierung und klicken darauf. Dann öffnet sich die eigentliche Login-Seite der Website, Sie erhalten das OTP und melden sich erfolgreich an. Es scheint, dass nichts Schlimmes passiert ist, oder? Falsch gedacht! Ja, die von Ihnen angemeldete Website ist kein Phishing. Aber, wenn Sie auf den Link in der E-Mail klicken, läuft der gesamte Datenverkehr über den Server des bösartigen Angreifers, der Ihr Cookie extrahiert und an den Angreifer weiterleitet. Mit diesem Cookie kann sich der Angreifer leicht als Sie ausgeben und sich in Ihrem Konto anmelden.

Attachment-basiertes Phishing

(File based Attacks) Phishing kommt bei vielen Opfern unter dem Deckmantel eines Links in einer angehängten Datei vor. Sehr oft handelt es sich um ein.pdf, das außer dem bösartigen Link nichts enthält. Wenn Sie daraufklicken, gelangen Sie zu einer Phishing-Website, die versucht, Ihre Anmeldeinformationen herauszulocken. Heutzutage sind sich viele Menschen bewusst, dass eine PDF Datei einen gefährlichen Inhalt enthalten kann. Aber was ist mit anderen Dateien, z.B. Sprachaufzeichnungen mit der Endung .eml? Können die gefährlich sein?

Stellen Sie sich vor, Sie erhalten eine Nachricht wie "Neue Sprachaufzeichnung empfangen" mit der angehängten Datei. Natürlich sind Sie gespannt, was sich darin befindet - und klicken Sie auf die Datei. Dann lädt eine Microsoft Login-Seite herunter und fordert Sie auf, die Anmeldeinformationen einzugeben. Viele Menschen finden es logisch - da Microsoft sich um ihre Sicherheit kümmert. Schlechte Nachrichten für sie: Die Referenzen fallen direkt in die Hände der Cyberkriminellen. Manchmal kann es sich um eine HTML-Datei handeln, die als Web-Formular Ihrer Bank getarnt ist, um sofort ausgefüllt zu werden. In Wirklichkeit enthält es ein Skript, um eine Phishing-Seite mit Web-Formular in Ihrem Browser zu öffnen. In allen Fällen ist die Wirkung gleich - Cyberkriminelle erhalten Ihre Zugangsdaten.

Böse KI: Maschinelles Lernen im Dienst der Cyberkriminellen

Was passiert, wenn Sie in Ihrer Inbox eine Mail von einem Bekannten erhalten. Die Nachricht ist zu einem Thema, das Sie interessiert sind und es hat ein PDF im Anhang. Viele Chancen bestehen, dass Sie auf die angehängte Datei klicken, oder? Dann öffnet sich die E-Mail-Login-Seite zum Beispiel GMX und fordert Sie auf, Ihre Zugangsdaten einzugeben. Es sieht vertrauenswürdig aus, denn es hat sogar GMX in der Adressleiste, während es ein wenig seltsam aussieht, wie: "data:text/html,https://accounts.gmx.com".

Aber in Wirklichkeit ist nichts so, wie es scheint. Die Seite ist Phishing, das.pdf ist ein Bild mit einem eingebetteten Link und dem Namen des Absenders und das Thema wurde von einem gehackten Rechner eines Ihrer Kontakte übernommen. Wie? Der bösartige Algorithmus gräbt sich in die Kontakte bereits gehackter Computer ein und erstellt und versendet automatisch neue Phishing-E-Mails mit entsprechenden Namen und Themen. So funktioniert das automatisierte hochpersonalisierte „Spear“-Phishing mit Hilfe von Machine Learning.

Vishing (Voice Pishing)

Diese Art von Phishing könnte die älteste sein - die Täuschung der Benutzer, dass sie geheime Daten per Telefon preisgeben, stammt aus den 90er Jahren. Der Punkt ist einfach: Betrüger rufen Sie von "Ihrer Bank" aus an und versuchen, Ihre Konto- und Kartendaten mit listigen Fragen herauszufordern. Aber heutzutage hat das Vishing eine neue Ebene erreicht. Nicht nur menschliche Betrüger rufen Opfer an, um ihre Zugangsdaten anzulocken, sondern auch Bots und Roboter. Dies ist ein echter technischer Sprung für Cyberkriminelle, denn so können sie eine große Anzahl potenzieller Opfer ohne großen Aufwand rund um die Uhr angreifen. Heute können Bots Menschen sehr plausibel darstellen, und diese Fähigkeit steigt mit den Fortschritten beim Machine Learning und den KI-Technologien in die Höhe.

Phishing-Kits

Es gibt viele Phishing-Tools, die auch Nicht-Techniker leicht ausführen können. Auf Darknet können Betrüger Dinge kaufen, die als "Multibrand Phishing Kit" bezeichnet werden - eine Software, mit der sie einen sehr plausiblen Klon berühmter Internet-Shops erstellen können. Für einen Betrüger reicht es aus, eine solche bösartige Website einzusetzen und sie zu bewerben, um die Website in die ersten Reihen der Suchmaschinen zu bringen. Eigentlich ist es eine Kombination mit einer anderen Art von Phishing - Search Engine Phishing. Um die Opfer zu locken, kündigen die Gauner auf ihren Seiten einen "Big Sales" mit unglaublich niedrigen Preisen für die beliebtesten Waren wie ausgefallene Smartphones und Laptops an. (Sie stehlen Bilder und Beschreibungen der Ware aus den echten Online-Shops). Um sie zu kaufen, müssen die Benutzer ihre Kreditkartennummern und andere persönliche Daten eingeben und.... Sie wissen wie die Geschichte enden wird.

Sextortion

Eines Tages werden Sie vielleicht einen Brief in Ihrer Mailbox finden, der mit dem Satz "Dein Passwort ist..." beginnt und Ihr echtes Passwort für ein Konto enthält. Dann schüchtert der Angreifer Sie mit der Aussage ein, dass er Ihren PC gehackt und ein kompromittierendes Video aufgenommen hat, in dem Sie sich eine Website für Erwachsene ansehen. Jetzt ist Ihr Computer unter seiner totalen Kontrolle, sagt er, und wenn Sie nicht sofort ein Lösegeld zahlen, wird das Video an alle Kontakte aus Ihrem Adressbuch gesendet. Aber in Wirklichkeit ist all das nichts anderes als ein Bluff. Niemand hat deine Maschine gehackt. Aber wie hatte der Gauner Ihr Passwort herausgefunden? Das ist kein Rätsel: Er hat es aus einer gestohlenen Datenbank eines Internet-Shops oder eines anderen Web-Ressource genommen, wo Sie sich irgendwann angemeldet hatten. Solche Datenbanken sind im Darknet weit verbreitet. Wir wissen das, wir von LUCY bieten ja auch Darknet Research an. Alles, was Sie tun müssen, ist, das gestohlene Passwort zu ändern - und bloß nicht auf den Bluff reinfallen.

IDN-Spoofing von Phishing-Angriffen

Auch eine Art ‚Typosquatting': IDN steht für Internationalized Domain Name - Domainnamen, die in anderen Sprachen als Englisch geschrieben wurden. Dementsprechend basiert dieser Angriff auf der Tatsache, dass einige Buchstaben in Alphabeten vieler verschiedener Sprachen ähnlich aussehen. So sieht beispielsweise das kyrillische "n" und "r" dem lateinischen "h" und "p" ähnlich. Diese

Buchstaben sind Homogramme. Wenn man also einige Buchstaben in einer URL, in die ähnlich aussehende aus einer anderen Sprache ändert, können Cyberkriminelle eine Website leicht fälschen. Wenn ein Angreifer beispielsweise das englische "p" für die russische Homographie "p" in apple.com ändert, kann er eine Web-Domain erstellen, die absolut gleich aussieht. Darüber hinaus kann der Angreifer sogar legitim ein SSL-Zertifikat für diese Website erhalten. Das bedeutet, dass Sie in der Leiste Ihres Browsers hptts://www.apple.com sehen, das genauso aussieht wie die echte URL der Apple-Website und somit Ihre Zugangsdaten an die Kriminellen weitergeben.

Subdomain-Übernahme

Cyberkriminelle können eine Subdomain einer legitimen Firmenwebsite übernehmen. Wie? Stellen Sie sich vor, Sie haben einen Service auf einer Subdomain Ihrer Firmenwebsite. Der Dienst ist auf „Amazon S3“ registriert. Nach einer Weile sind sie unzufrieden mit dem Dienst und Sie beenden ihn. Sie kümmern sich aber nicht darum, den DNS-Eintrag zu entfernen, der mit Amazon S3 Bucket verbunden ist - eine Funktion, die Subdomainnamen enthält. Und hier kommen die Cyberkriminellen ins Spiel. Sie registrieren diesen leeren S3-Eimer für sich selbst und nutzen ihn für bösartige Zwecke wie Phishing. Aber da DNS mit Ihrer Subdomain-Adresse verbunden bleibt, werden Sie vielleicht eines Tages sehr überrascht sein, wenn Sie herausfinden, dass Ihre geschlossene Subdomain lebt und für Kriminelle bestimmt ist.

Phishing durch Ausnutzung von Schwachstellen bei Webanwendungen

Viele Sicherheitslücken in Webanwendungen können für Phishing genutzt werden. Einer von ihnen verwendet eine legitime Website mit Open Redirect-Schwachstelle. In diesem Fall kann ein Angreifer der URL der Website einen externen Link hinzufügen, der auf eine Phishing-Website umgeleitet wird. Die meisten Benutzer werden nur den ersten, legitimen Teil der URL bemerken - und haben ein falsches Gefühl, dass die Website sicher ist. XSS (Cross-Site-Scripting), einer der beliebtesten Angriffe auf Webanwendungen, wird auch für Phishing eingesetzt - und das nicht nur in einer Hinsicht. So kann beispielsweise ein Angreifer der URL der Website ein bösartiges JavaScript hinzufügen, um Benutzer auf eine Phishing-Seite umzuleiten oder Ihm ein gefälschtes Webformular unterzujubeln.

Pharming

Dieser Angriff leitet legitimen Datenverkehr auf eine Phishing-Webseite direkt auf Ihrem PC um. Sie geben beispielsweise einen Browser "google.com" ein, gelangen aber stattdessen auf eine Phishing-Website. Wie ist das möglich? Durch Ändern der Datei "hosts" auf Ihrem Computer mit Malware, die Ihren Arbeitsplatz irgendwie infiziert hat. In dieser Datei stellte die Malware eine falsche Übereinstimmung zwischen IP-Adressen und einem Domänennamen ein und leitete so den Datenverkehr um. In unserem Beispiel hat die Malware die tatsächliche IP-Adresse von google.com in die IP-Adresse der Website des Angreifers geändert. Natürlich können Cyberkriminelle dies mit jedem Domainnamen tun, einschließlich Ihrer Bank oder Social Media Website. Da Sie sich dessen nicht bewusst sind, werden Sie auf die Phishing-Webseite weitergeleitet, geben Ihre Anmeldeinformationen ein - und die Probleme beginnen.

Nachahmung oder BEC-Angriffe

Business Email Compromise (BEC)-Angriffe sind Phishing-E-Mails, die keinen ‚gefährlichen Inhalt' wie eine böse URL oder Anhang enthalten. Die Angreifer haben sehr gute Kenntnisse über die Angestellten, die Unternehmensstruktur oder über gängige Transaktionen, um Mitarbeiter davon zu überzeugen, Geld oder Daten zu überweisen oder Bankkontoinformationen für ausstehende Zahlungen zu ändern. Gemäß den neuesten Zahlen des FBI haben Business Email Compromise (BEC) Programme in den letzten Jahren (insbesondere in den letzten 2 Jahren) mindestens 3,1 Milliarden Dollar an Gesamtverlusten für rund 22.000 Unternehmen auf der ganzen Welt verursacht. Seit Januar 2015 gab es einen Anstieg der anerkannten exponierten Verluste um 1.300%, was einem durchschnittlichen Verlust von 140.000 $ pro Betrug entspricht.

Phishing über Social Media

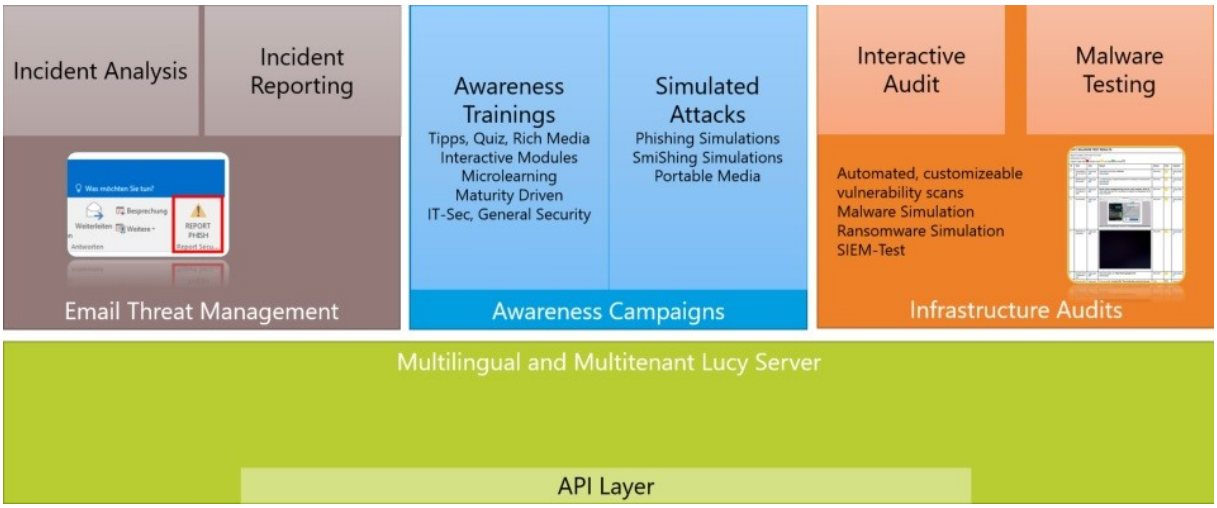
Wie beim Smishing werden diese Angriffsvektoren (z.B. bösartige Links, Nachahmungen usw.) durch die neue Art von Social Media Collaboration Apps (LinkedIn, Slack, Skype, Teams, Facebook Messenger) bereitgestellt. Während die Nutzer darauf trainiert wurden, E-Mails zu misstrauen, neigen sie dazu, bei der Verwendung dieser Tools übermäßig vertrauensvoll zu sein. 2017 offenbarte Facebook, dass bis zu 270 Millionen Konten unrechtmäßig waren, während Twitter 2018 über 70 Millionen gefälschte und verdächtige Konten identifizierte. Laut dem Bericht von Corrate wurden die meisten dieser Konten für die Verbreitung von Phishing über Social Media über die schändliche Nutzung der Plattform verwendet.

Am 24. Januar 2018 erhielt die First Business Bank (FBS) von einem CEO eines Geschäftskunden einen Antrag auf Überweisung in Höhe von 15.850,00 US-Dollar per E-Mail. Die E-Mail kam von der geschäftlichen E-Mail-Adresse des CEO, und der Buchhalter des Unternehmens wurde in die E-Mail kopiert. Der FBS Bankmitarbeiter schickte per E-Mail ein leeres Formular zur elektronischen Banküberweisung (Wire Request Form), um die Transaktion abzuschließen. Bald kam eine Antwortmail von der E-Mailadresse des CEO, die das ausgefüllte Wire Request Form und den Wire Agreement enthielt, die beide auch die authentische Unterschrift des CEO trugen.

Die Lösung heißt Mitarbeiterschulung und Phishingsimulationen

Wie Sie sehen gibt es heutzutage Phishing in verschiedenen Formen und selbst ein Computerfreak ist nicht immer in der Lage, sie alle zu erkennen. Wie können wir also diese Gefahr bekämpfen? Die beste Methode, um Sicherheit zu erhöhen, ist die Schulung der Mitarbeiter unter realitätsnahen Bedingungen. Bewährte Phishing Simulationen und Sensibilisierungstrainings der LUCY Software und Plattform helfen Ihnen dabei.

Die LUCY Security Awareness Suite wird zur Mitarbeiterschulung und zur Simulation von Social Engineering Angriffen eingesetzt und ist universell einsetzbar - vom Mittelstand bis zum Großkunden. Das DSGVO konforme Produkt kann direkt beim Kunden installiert werden, eine Cloud-Version ist ebenfalls erhältlich.



Die Schweizer Lösung bietet Hunderte von selbstständig nutzbaren, vorkonfigurierten Phishing-Vorlagen und Schulungsmodulen. Mit dem "Phishing Incident Plugin" für Microsoft Outlook etc. kann der Anwender Alarm schlagen, wenn er einen Angriff vermutet. Der "Threat Analyzer" von LUCY wertet vermutete Phishing-Angriffe automatisch aus und schätzt deren Risiko ein. Das Produkt ist auf mehr als 8000 Servern in über 60 Ländern installiert. Inzwischen wurden mehr als 7 Millionen Benutzer mit LUCY trainiert. Zertifizierte Eco-System-Partner in 12 Ländern ergänzen die LUCY-Lösung mit ihren Mehrwertdiensten.

Über den Autor

Palo Stacho

Co-Founder
LUCY Security AG

Security

Cyber Security „Made in Hessen”

Wir haben QuoScient gegründet, um unsere Expertise im Kampf gegen digitale Bedrohungen jeglicher Art für Unternehmen und Organisationen über alle Branchen hinweg zur Verfügung zu stellen. Wir sind überzeugt, dass wir unsere Kunden mit unseren ganzheitlichen oder auch modularen Sicherheitslösungen bestmöglich gegen alle Arten von Bedrohungen im Cyberraum schützen können. Unseren Ansatz nennen wir Digital Active Defense und steht für das Zusammenspiel von Intelligence Operations, Security Operations und Defense Technology, die gemeinsam arbeiten, um proaktiven Schutz vor digitalen Bedrohungen zu bieten.

Unsere Intelligence Operations warnen unsere Kunden vor aktuellen und neu auftretenden Bedrohungen, die speziell auf ihre Organisation ausgerichtet sind und unterstützen sie so aktiv. Unsere Security Operations (oder auch Managed Security) bekämpfen Angriffe aktiv und neutralisieren diese, indem sie diese Angriffe auf ihre Ursachen hin untersuchen und so sicherstellen, dass diese sich nicht wiederholen. Mit unserer Defense Technology stellen wir sicher, dass rechtzeitig geeignete Maßnahmen ergriffen werden, kritische Informationen verbreitet werden und die technischen Ressourcen voll eingesetzt werden. Im Mittelpunkt unserer Produkte und Dienstleistungen steht dabei unser Kernprodukt QuoLab, die Cyber-Sicherheitsplattform der nächsten Generation. QuoLab ist die logische und konsequente Weiterentwicklung für den operativen IT-Sicherheitsbetrieb.

QuoLab verkürzt Analyse- und Entscheidungsprozesse, in dem es relevante Funktionen in einem ganzheitlichen, kollaborativen Ökosystem vereint. Dazu gehören die administrative Verwaltung von Fakten und Fällen (Case Management) ebenso wie technisch analytische Werkzeuge (z.B. Feststellung der Schadhaftigkeit von Dokumenten) und automatisierte Verarbeitung erlangter Erkenntnisse zu technischen Bedrohungen (Threat Intelligence Platform).

Mit der automatisierten Sammlung relevanter Fakten (Threat Intelligence-Feeds, wie MISP, TAXII, OTX und mehr) lassen sich sofort Zusammenhänge zwischen Bedrohungsinformation und den Daten aus internen Sicherheitssystemen (SIEM, Firewall, IDS, etc.) aufzeigen. Ergänzend hilft QuoLab technische Artefakte zu analysieren, zu kontextualisieren und zu verfolgen. Operative Einheiten erlangen schneller eine klare Übersicht und Einschätzung der Lage. Falls nötig oder gewünscht, lassen sich die Fakten in angebundene Sicherheitsökosystem einspeisen. Medienbrüche werden vermieden und Schaden-minimierende Maßnahmen schneller ausgeführt.

QuoLab stellt sicher, dass Ihre wertvollsten Ressourcen – Zeit und Menschen – optimal genutzt werden. Sicherheitsexperten aus verschiedenen Disziplinen und mit verschiedenen operativen Hintergründen können effektiv faktisch zusammenarbeiten, um die Unternehmensinfrastruktur, Netzwerke und kritische Daten aktiv, aber effizient zu verteidigen. Mit QuoLab haben Kunden Zugang auf eine echte „Active Defense Platform“, die ihnen eine konsolidierte Kontrolle über die gesamten Sicherheitssysteme gibt. Die Zusammenarbeit wird erleichtert, der Mehrwert bestehender Sicherheitskontrollen maximiert.

Wir begreifen unseren Industriesektor Cyber Security als eine immense Chance für die lokale, regional und nationale Wirtschaft und möchten durch unser Engagement in der GFFT Lab Community aktiv unseren Beitrag für die erfolgreiche Gestaltung dessen leisten. Wir wollen Cyber Security Made in Germany zu einem Markenzeichen machen, wie es vielen anderen deutschen Firmen in ihren jeweiligen Industrien gelungen ist.

Über den Autor

Ioannis Bizimis

Mitgründer und CFO
QuoScient GmbH

Software

Warum Lasttests?

Zuerst ist hier sicherlich die Erwartungshaltung von uns allen Anwendern zu nennen: wir erwarten heute die Geschwindigkeit von Google egal wie komplex eine Anwendung ist, egal welche technischen Bedingungen herrschen, egal welche Frontendgeräte verwendet werden und egal unter welchen Konditionen auch immer. Hinzu kommt eine immer größere Verschiebung der Geschäftsvorfälle in Richtung e-Business, Mobile-Applikation oder Cloud-Service. Die persönliche Kundenbeziehung tritt immer mehr in den Hintergrund, was bedeutet, dass wir unseren Kunden und Geschäftspartnern auch immer mehr über unsere Softwarelösungen, unsere Portale und Multi-Channel-Angebote begeistern und binden müssen.

Neben der Erwartungshaltung der Anwender gibt es auch noch eine Vielzahl von technischen Bedingungen, die heute Last- und Performancetests unabdinglich machen. Die IT-Infrastruktur wird immer vielfältiger. Mit Cloud- und Mobile-Anwendungen müssen wir Bedingungen händeln, die nicht in unserer Kontrolle liegen. Und dann gibt es das große Thema Security: unter Last offenbaren viele Anwendungen ganz andere Sicherheitsrisiken, die es zu erkennen und zu eliminieren gibt. Die Migration von Anwendungen in die Cloud bedeutet andere Kommunikation: die auf TCP/IP ausgerichtete Applikationsarchitektur ist oftmals hinderlich. Ähnliches gilt für SAP Migrationen von R3 auf Hana. Der Erfolg Ihrer digitalen Strategie hängt von Ihrer Fähigkeit ab, regelmäßig schnelle und zuverlässige Software zu liefern.

Die schnelle Erstellung großartiger Software, die Verwendung eines optimierten Performanctestverfahrens ist Ihr Wettbewerbsvorteil - Agile und DevOps sind Teil der Lösung. Neotys hat über 14 Jahre Entwicklungsarbeit in NeoLoad investiert - die Performance-Test-Plattform zur Beschleunigung von Agile und DevOps-Prozessen. Das Endergebnis - bis zu 10x schnellere Testerstellung und 20x schnellere Testwartung mit NeoLoad, höchst mögliche Automatisierung und Integrationsfähigkeit.

NeoLoad ist die branchenführende Plattform für Performancetests. Schnell, kraftvoll, realistisch. NeoLoad ist die einzige Performance-Test-Plattform, die sowohl für Cloud-fähige, Microservices-Architektur-, Mobil- und IoT- als auch für Enterprise-Anwendungen geeignet ist. Im Gegensatz zu herkömmlichen Tools, die eine breite Technologieabdeckung bieten, aber nur langsam zu bedienen und teuer in der Anschaffung sind, ist NeoLoad die einzige Lösung, die sowohl Geschwindigkeit als auch breite Technologieunterstützung bietet - ohne Kompromisse. Da die Anwendungsleistung zum geschäftlichen Gebot wird, unterstützt unsere Enterprise Performance Testing-Plattform die Anforderungen des Performance Engineering während des gesamten Softwareentwicklungszyklus. NeoLoad bietet Testern, Entwicklern, Betriebsspezialisten und anderen Experten die Möglichkeiten:

- Performancetests schnell durchzuführen, ohne Kompromisse zwischen Geschwindigkeit und Qualität
- Entwickeln Sie Tests zehnmal schneller als mit herkömmlichen Tools
- Identifizieren Performanceengpässe und geben Sie praktische Einblicke in Probleme
- Führen Sie die Tests auf das Tempo von Anwendungsänderungen abgestimmt durch – agile und in die DevOps-Umgebung integriert
- NeoLoad unterstützt Sie in Ihrem bevorzugten Arbeitsstil: NeoLoad as a Code (für Entwickler), die hoch effiziente NeoLoad GUI (für Performance-Testexperten), NeoLoad Dashboards (für Entscheider), und dann lässt sich NeoLoad auch in automatisierte Prozesse einbinden.

Business Impact

- Freigaben mit Zuversicht: Mehr Testfälle abdecken, professionelle Qualität sicherstellen, Tester zu vertrauenswürdigen Partnern machen
- Support Agile: Perfornancetests zu einem Schlüsselelement Ihrer agilen Softwarelieferung machen
- DevOps erreichen: Performancetests zu einem kontinuierlichen Prozess über Dev, QA und Ops hinweg machen
- Automatisierung nutzen: Senken Sie die Kosten für die Wartung von Testskripten drastisch, indem Sie Änderungen in der Anwendung erkennen und das Testskript automatisch aktualisieren

Wir glauben fest daran, dass der Performance Engineer zum kritischen Partner für die Anwendungsperformance werden kann, der die beste Testabdeckung bietet und gleichzeitig die Kadenz des Continuous Delivery-Prozesses respektiert. Da die Performance in die Verantwortung des breiteren DevOps-Teams fällt, ist die kontinuierliche Bereitstellung einer optimierten Plattform für Performancetests der Antrieb unserer täglichen Arbeit.

"Wir haben das gleiche sechswöchige Projekt innerhalb der LoadRunner-Umgebung in weniger als zwei Wochen mit NeoLoad abgeschlossen. Wir erlebten ein 60-70% schnelleres Skriptdesign im Vergleich zu LoadRunner und konnten andere Abteilungsmitglieder schnell in die intuitive Benutzeroberfläche von NeoLoad einarbeiten. Ich bin beeindruckt von der Qualität und Unterstützung durch Neotys." **Corey Bradley, AppSystems Analyst Consultant, BlueCross/BlueShield TN**

"Mit NeoLoad haben wir die Skripting-Zeit und die Wartung von Skripttests um 66% reduziert."
Mikey Warner Leiter QA, Office Depot

"NeoLoad ermöglicht es uns, an einem Tag zu testen, was früher mit unserer vorherigen Lösung 5 Personen gekostet hat." Andreas Papadopoulos Leiter Software Delivery, Sporting Index
"Lasttests sind mit NeoLoad 6x schneller als mit unserem Legacy-Tool."
Pascal Auger, Leiter Leistungstests, Credit Agricole Technologies & Services

“Wir verwenden NeoLoad, weil es schneller, benutzerfreundlicher und mit unserem notwendigen Agile Footprint ausgestattet ist."
Steve Lampke Technology Manager, Kronos

Über den Autor

Gregor Mayer

Territory Manager DACH
Neotys Germany

Software

Rule based-testing – ein neuartiger Ansatz auf der Testplattform webmate

Voller Zugriff auf die Intuition ihrer Tester

Ihre Tester sind Ihr bestes Werkzeug im täglichen Kampf gegen Fehler, denn trotz aller Fortschritte ist das automatisierte Testen dem menschlichen Tester immer noch unterlegen: Ihre Tester haben fachliches Wissen über Ihre Anwendung, kennen die Historie Ihres Projekts und haben jahrelange Erfahrung in der Nutzung des World Wide Web. Rule-Based Testing gibt Ihnen die Möglichkeit, dieses Wissen als Regeln zu formulieren, die bei jedem Test automatisch geprüft werden. So stellen Sie mit geringem Aufwand sicher, dass Ihre Anwendung zu jedem Zeitpunkt dem mentalen Modell Ihrer Tester entspricht.

Ein deklaratives Modell Ihrer Seite.

Technisch ausgedrückt ist Rule-Based Testing ein modell-basiertes Testverfahren, das on-the-fly auf einem regelbasierten Systemmodell operiert. Das heißt, webmate prüft im Hintergrund die Eigenschaften Ihrer Anwendung auf Korrektheit, sobald die Plattform „irgendwie“, z.B. bei einem automatisierten oder manuellen Test, Daten einsammelt. Das Systemmodell erlaubt es, wichtige Eigenschaften Ihrer Seite als Regeln zu formulieren. Was wichtig ist, bestimmen Sie dabei ganz allein, zum Beispiel:

- Layout-Regeln erlauben es Ihnen, Ihre Anforderungen an das Aussehen der Seite zu formulieren. Beispiel: Links oben im Header muss immer das Firmenlogo sichtbar sein.
- Netzwerk-Regeln geben Ihnen die Möglichkeit, Anforderungen an die Art und Geschwindigkeit der Netzwerkanfragen Ihrer Seite zu stellen. Beispiel: Die Werbung muss innerhalb von 200 Millisekunden geladen werden.

Die webmate Rule Engine prüft nach jedem Testschritt, dass Ihre Seite den formulierten Regeln entspricht.

Keine Regel ohne Ausnahme.
Layout- und Netzwerkregeln beschreiben das gewünschte Verhalten Ihrer Seite. Sie haben aber mit Sicherheit auch Regeln, die nicht auf allen Seiten gelten sollen. An dieser Stelle helfen Ihnen Bedingungen : Eine Bedingung spezifiziert, wann eine Regel gelten soll. Rule-Based Testing bietet Ihnen verschiedene Möglichkeiten, um Regeln anzugeben, zum Beispiel:

- URLs: Sie können vorgeben, dass Regeln nur für bestimmte URLs gelten. Damit können Sie spezielle Regeln für Ihre Startseite festlegen.
- Sichtbare Elemente: Regeln können auch nur dann gelten, wenn bestimmte Elemente auf der Seite aktuell sichtbar sind: Ist der Login-Button sichtbar, dürfen keine Links zum Profil des Nutzers sichtbar sein.

Die Vorteile von Rule-Based Testing
Der Einsatz von regelbasiertem Testen bietet Ihnen zahlreiche Vorteile:

- Kommunizierbar: Ihre Regeln beschreiben ein Modell Ihrer Seite. Dieses Modell können Sie im Team diskutieren, analysieren und bearbeiten. Es bietet Ihnen eine Sprache, um implizites Wissen und Annahmen aller Beteiligten explizit zu formulieren.
- Deklarativ und funktional: Ihre Regeln sind von der Spezifikation der funktionalen Testskripte getrennt. Diese Trennung führt zu kürzeren Testskripten und vermeidet Wiederholungen.
- Frühe Spezifikation: Regeln können bereits sehr früh im Projektverlauf definiert werden. Am Projekt beteiligte Rollen, z.B. Business-Owner oder Designer, können Regeln natürlichsprachlich definieren. Später im Projekt können diese Rollen verfeinert und der technischen Realisierung angepasst werden.
- Immer und immer wieder testen: Aufgrund der Trennung vom Testskript können ihre Regeln in beliebigen Kontexten getestet werden: Aus einem Testskript, einem einem explorativen Agenten („Crawler") und auch im Rahmen eines manuellen Tests.

Webmate ist ein Produkt der Testfabrik AG. Die Testfabrik AG ist ein Spin-off des Lehrstuhls für Softwaretechnik der Universität des Saarlandes, wo unter der Leitung von Prof. Andreas Zeller seit vielen Jahren weltweit anerkannte Spitzenforschung in den Bereichen Testen, Debugging, und Software-Analyse betrieben wird.

Über den Autor

Bernd Pohl

Vorstand
Testfabrik AG

Organizational Intelligence

Vorwort: Das GFFT Smart Logistics Lab- gemeinsam Potenziale in der Logistik erschließen

Sehr geehrte Damen und Herren,

nach wie vor stellt die Logistik eine tragende Säule der Wertschöpfungsprozesses dar. Der reibungslose Transport von Waren ist für die produzierende Industrie und den Handel ein unverzichtbares Element. Insbesondere der straßengebundene Gütertransport wird jedoch zunehmend kontrovers diskutiert: Hier stehen soziale Aspekte – wie die Arbeitsbedingungen der Fahrer, die steigenden Unfallstatistiken und die für jedermann spürbaren Überlastungen der Straßen und Autobahnen im Vordergrund. Gleichzeitig sind es auch die ökologischen Auswirkungen und die daraus resultierenden externen Kosten, die immer deutlicher in den Vordergrund rücken.

Darüber hinaus sind diverse externe Faktoren erkennbar, wie z.B. steigende Treibstoffpreise, Maut-Gebühren sowie der Konkurrenzdruck von Logistikanbietern aus dem Ausland, die den Marktdruck für deutsche Speditionen weiter erhöhen. Logistikdienstleister kämpfen in diesem Umfeld mit steigenden Kosten und höchsten Ansprüchen der Kunden im Hinblick auf die Qualität der Transportdienstleistung. Für Versender hingegen resultiert diese Entwicklung in nicht unerheblichen Problemen, die Fracht zuverlässig und zu angemessenen Preisen zu befördern. Die Qualität der Transportdienstleistung im Hinblick auf Pünktlichkeit und den ordnungsgemäßen Zustand der Ware haben dabei deutliche Auswirkungen auf die Kundenzufriedenheit und damit die Konkurrenzfähigkeit in kundengetriebenen, globalen Märkten.

Trotz der Verfügbarkeit zuverlässiger und durchaus etablierter Technologien – insbesondere aus den Bereichen Telematik nebst diverser Softwarelösungen zur Planung und Steuerung der Logistikprozesse – darf an dieser Stelle festgehalten werden, dass nach wie vor großes Verbesserungs-

potenzial besteht, um den straßengebundenen Güterverkehr für alle Stakeholder effizienter und nachhaltiger zu gestalten.

Dieser Annahme folgend wurde das GFFT Smart Logistics Lab ins Leben gerufen. Es hat sich die Aufgabe gestellt, möglichst viele Lösungen zur Verbesserung der Lieferkette zu initiieren und mit zu entwickeln. Ziel ist die kooperative Umsetzung innovativer Lösungen, die den Anforderungen der Bedarfsträger gerecht werden und bereits kurzfristig einen nachhaltigen Nutzen stiften. Das Lab versteht sich in diesem Zusammenhang als eine Plattform, die gleichermaßen eine ständige Diskussion von aktuellen Herausforderungen und Verbesserungspotenzialen mit den Stakeholdern wie auch die Lösungsfindung unter Einbeziehung führender Technologie- und Forschungspartner unterstützt. Jedes Mitglied des Labs hat die Möglichkeit, eigene Projektvorschläge zu äußern. Im Sinne praxisrelevanter Lösungen muss jeder Vorschlag, der gemeinsam zur Realisierung kommen soll aufzeigen, inwieweit er die wichtigen Zielkriterien einer durchgängigen Lieferkette zu verbessern hilft. Hauptanliegen des GFFT Smart Logistics Labs ist die zeitnahe Erprobung und Umsetzung neuer Technologie-Ideen. Jedes Projekt wird mit Implementierungspartnern und einer Reihe von Referenzkunden umgesetzt, die auch gemeinsam die Finanzierung abstimmen.

Als einer der ersten Aktionen des GFFT Smart Logistics Labs wurde im Februar 2019 ein Workshop im Hause der Schaeffler AG organisiert, der die aktuellen Trends und daraus resultiere Probleme und Optimierungspotenziale in der Logistik von unternehmensübergreifenden Lieferketten mit besonderem Fokus auf den straßengebundenen Güterverkehr adressierte. Gemeinsam mit Versendern, Logistikunternehmen, Beratungsunternehmen und weiteren Dienstleistern aus dem Logistikumfeld wurden Probleme bzw. Anforderungen und mögliche Lösungen diskutiert.

In der Veranstaltung wurden insbesondere für die folgenden Bereichen Verbesserungs- bzw. Entwicklungsbedarfe identifiziert:

1. Verbesserung der Informationsgrundlage für die Entscheidungsfindung:
    a. Datenqualität,
    b. durchgängige Datenverfolgbarkeit über Unternehmensgrenzen hinweg,
    c. standardisierte Schnittstellen für die Informationsübergabe zwischen IT-Systemen,
    d. Digitalisierung transportbegleitender Dokumente,
    e. KPI-Dashboards zur Bewertung der Effizienz und Qualität der Logistikprozesse.
2. Senkung der manuellen Aufwände:
    a. Automatisierung von Prozessen,
    b. Reduzierung von „Last-Minute Aktionen“ bzw. Sonderfahrten, für die Disponenten erforderlich sind.
3. Optimierung zur Erhöhung von Effizienzen:
    a. Trailer- / Yard-Management,
    b. frühzeitige Auftragsvergabe,
    c. Spotmarkt-Ausschreibungen / -börsen,

d. Flexibilisierung von Zeitslots für die Be- und Entladung,
e. LKW-Sharing unter Beachtung von Volumen und Gewicht,
f. gemeinsame Transportvergabe zur besseren Ausnutzung der LKW im Sinne von Full Truck Loads (FTL),
g. neue Geschäfts- und Preismodelle.

Die oben genannten Themen wurden unter den Teilnehmern der Veranstaltung offen diskutiert. Bereits im Rahmen dieses ersten Workshops fanden sich erste Arbeitsgruppen, die sich ausgewählten Themen annehmen und diese vorantreiben.

Das in Herzogenaurach gestartete GFFT Smart Logistics Lab wird im Rahmen der am 06. Mai 2019 in Wiesbaden stattfindenden GFFT-Jahrestagung mit einem weiteren Workshop fortgesetzt. An dieser Stelle werden erste Ergebnisse präsentiert und gemeinsam das weitere Vorgehen festgelegt. Das Lab ist für weitere Partner offen. Im Sinne der Fortsetzung der offenen und vorbehaltslosen Diskussion von Bedarfen und möglicher Lösungsansätze ist für die Aufnahme weiterer Mitglieder ein Aufnahmeverfahren festgelegt worden.

Als Teilnehmer an der diesjährigen GFFT-Jahrestagung in Wiesbaden sind interessierte Unternehmen jedoch herzlich willkommen, an diesem Workshop teilzunehmen. Neben interessanten Technologien aus dem Logistikumfeld, die innerhalb der Innovationsmesse vorgestellt werden, bietet das Vortragsangebot des GFFT Smart Logistics Lab interessante Impulse für eine weiterführende Diskussion zur Verbesserung der Logistik in unternehmens-übergreifenden Lieferketten. Auch externe Gäste sind an dieser Stelle eingeladen, mitzudiskutieren und sich mit ihren Bedarfen und Lösungsvorschlägen einzubringen.

Ihr
Dr. Carl Hans

Über den Autor

Dr. Carl Hans

Geschäftsführer
OHS Engineering GmbH
GFFT e.V.

Organizational Intelligence

Digitalisierung fordert Mensch – Technik – Organisation

Das Schlagwort Digitalisierung ist seit Jahren ein Trendthema in Medien und Fachvorträgen. Für jedes Unternehmen bedeutet es aber auch etwas Anderes. Fest steht jedoch, dass der Wandel bereits in allen Branchen längst begonnen hat und dieser sich noch lange fortsetzen wird. Um aus dieser Entwicklung erfolgreich hervorzugehen, sollten Unternehmen sich nicht treiben lassen, sondern aktiv den Gestaltungsprozess auf dem Weg zur Digitalisierung angehen.

Die Zukunft der industriellen Produktion ist vor allem durch die Individualisierung der Produkte sowie der damit einhergehenden Flexibilisierung und Vernetzung der Produktion geprägt. Dieser Paradigmenwechsel ist in Fachkreisen als Industrie 4.0 und allgemein unter dem Begriff Digitalisierung bekannt. Der aktuelle Trend der steigenden Variantenvielfalt wird sich zukünftig noch weiter verstärken und zahlreiche Unternehmen vor neue Herausforderungen in der Planung und Steuerung ihrer Wertschöpfungssysteme stellen. Moderne Fertigungssysteme sind unter anderem durch globale Wertschöpfungsnetze gekennzeichnet. Ein Wertschöpfungsnetz kann als ein Ökosystem verstanden werden, das durch verschiedene Akteure mit unterschiedlichen Bedürfnissen geprägt ist. Die Akteure agieren dabei in einer dynamischen Umwelt und stehen untereinander in Interaktion. Die dadurch steigende Dynamik und Komplexität verlangt neue Lösungen in der Gestaltung von Methoden, Prozessen und Technologien, um die geläufigen Zielgrößen wie Qualität, Zeit und Kosten weiter erfüllen zu können.

Das zuverlässige Funktionieren der Wertschöpfungssysteme verlangt eine umfassende Betrachtung der Digitalisierung, also die Auseinandersetzung der Perspektiven Mensch, Technik und Organisation. Um eine effiziente und effektive Planung und Steuerung moderner Wertschöpfungsprozesse zu garantieren, werden bestens qualifizierte Mitarbeiter benötigt. Ebenfalls erfordert das Arbeiten in Netzwerken moderne Formen der Organisation, die das arbeitsprozessorientierte Lernen fördern

und unkompliziert umsetzen. Moderne Ansätze zur Qualifizierung wie z.B. das ernsthafte Spielen (Serious Gaming) oder das „spielifizierte“ Arbeiten (Gamification) ermöglichen es, komplexe Sachverhalte spielerisch zu vermitteln und damit einen wichtigen Beitrag in der Aus- und der kontinuierlichen Weiterbildung zu leisten.

Das Identifizieren zukunftsfähiger Wertschöpfungssysteme, die ganz individuell zu Ihrem Unternehmen passen, erfordert Einblicke in viele verschiedene Trends, Technologien und Erfahrungswerte. Die bundesweite Initiative Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die im Rahmen dieser Initiative geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital. Weitere Informationen finden Sie unter www.mittelstand-digital.de.

Im Mittelstand 4.0-Kompetenzzentrum Bremen werden zahlreiche Kompetenzen aus der Bremer Region zusammengeführt und gebündelt den Unternehmen zugänglich gemacht. Das Zentrum hilft dabei angesichts des diffusen Megatrends Digitalisierung zunächst die wichtigen Fragestellungen zu ermitteln, die für Unternehmen relevant sind. Die Mitarbeiter unterstützen die Unternehmen beim Aufspüren der optimalen Antworten in Sachen Digitalisierung.

Egal, wie weit sich die Unternehmen auf dem Weg der Digitalisierung befinden – das Zentrum unterstützt dabei, die nächste Stufe zu erreichen und die Marktposition zu stärken.

An wen sich das Angebot richtet

Im Fokus des Mittelstand 4.0-Kompetenzzentrums Bremen stehen kleine und mittlere Unternehmen (KMU) in den Innovationsclustern Luft- und Raumfahrt, Windenergie, Automobil sowie Nahrungs- und Genussmittel. Hinzu kommen weitere Branchen, die für die regionale Wirtschaft bedeutend sind, beispielsweise Logistik, Transport, Offshore-Industrie, Schiffbau, Meerestechnik und Meeresforschung. Die Angebote stehen allen KMU – auch über Bremen hinaus – offen. Das Bremer Zentrum ist eines von insgesamt 25 bundesweiten Mittelstand 4.0 Kompetenzzentren. www.kompetenzzentrum-bremen.digital

Wie es funktioniert

Das Kompetenzzentrum hält für interessierte KMU eine Reihe kostenfreier Unterstützungsangebote bereit, die je nach Bedarf durch Fach- und Führungskräfte in Anspruch genommen werden können. Dabei wird der gesamte Innovationsprozess abgedeckt. Er beginnt mit Informationen über Potenziale der Digitalisierung für das jeweilige Unternehmen. Weiter geht es mit der Chance, entsprechende Anwendungen in der Praxis zu erleben. Parallel erhalten die Mitarbeiter die Möglichkeit sich für die digitale Welt durch Qualifizierungen fit zu machen. Auf Wunsch begleitet das Mittelstand 4.0 Kompetenzzentrum das Unternehmen auch bei der Gestaltung eines Umsetzungsprojekts, um die direkte Wirkung der Digitalisierung im Unternehmen praxisnah zu erleben.

Das Kompetenzzentrum hält ein breites Spektrum an Themen und Formaten bereit, um für jeden Bedarf die passenden Maßnahmen anbieten zu können.

Über den Autor

Dr. Christian Gorldt

Leiter der IKAP-Abteilung Collaborative Business in Unternehmensnetzwerken
BIBA - Bremer Institut für Produktion und Logistik GmbH
Mittelstand 4.0 Kompetenzzentrum Bremen

Organizational Intelligence

Informatisierung als Vorrausetzung für datengetriebene Dienstleitungen

Die Informatisierung ist ein fortschreitender Prozess, sowohl im betrieblichen als auch im privaten Umfeld, welcher sich auf die Erzeugung und Nutzung digitaler Informationen fokussiert.

Hierbei ist die Erzeugung im Rahmen der betrieblichen Informatisierung bereits soweit vorangeschritten, dass „…Most organizations of middle to large size have hundreds or, more probable, thousands of applications, each with its own various database and other data stores….” (Reeve 2013). Der Trend zu der steigenden Anzahl an Datenquellen wird durch die zunehmende Informatisierung von Produkten, der Integration von IoT Systemen und cyber-physischen Systemen beschleunigt.

Auch der Bereich der privaten Informatisierung bereits so weit vorangeschritten, das Social Media ein anhaltender Trend ist. Hierbei veröffentlicht der Nutzer Informationen aus dem täglichen Leben im Internet. Die zunehmende Menge an Informationen beinhaltet u.a. solche, die als Rückmeldungen von Verbrauchern zu Produkten betrachtet werden können. Hierbei umfasst die verfügbare "Blogosphäre" inzwischen mehr als 100 Millionen Blogs (Kietzmann et al. 2011). Bei der Anwendung des Mikroblogging hat das führende Unternehmen Twitter mehr als 145 Millionen Nutzer erreicht, die täglich mehr als 90 Millionen Tweets mit jeweils 140 Zeichen senden (Kietzmann et al. 2011).

Ein weiterer Trend der Informatisierung ist die Initiative zu Linked Open Data im Rahmen des Semantic Webs. Damit werden Regierungen, Unternehmen und private Personen befähigt, Datenquellen im Internet bereitzustellen und für jeden Interessierten zugänglich zu machen. Dies führt zu einem weiteren Anstieg an Datenquellen. Die oben aufgeführten Trends führen zu einer Vielzahl an Datenquellen, welche von unterschiedlichen Parteien bereitgestellt und genutzt werden. Obwohl sich das Nutzungsprinzip auf den Dreiklang von „…Erfassung – Interpretation – Reaktion…“

(Bauernhansl et al. 2014) reduziert lassen kann, ergeben sich für die Erfassung und Interpretation große Herausforderungen im Hinblick die Nutzung von heterogenen Datenquellen im operativen Betrieb. Die Art und Weise, wie Daten interpretiert werden, resultiert anschließend in unterschiedlichen Nutzungsszenarien. Die eindeutige Interpretation der übertragenen Informationen kann auf verschiedenen Ebenen erreicht werden. (Ades 2007) definierte die unterschiedlichen Ebenen als

- lexikalisches Verständnis,
- syntaktisches Verständnis,
- morphologisches Verständnis,
- semantisches Verständnis und
- pragmatisches Verständnis.

Das lexikalische, syntaktische und morphologische Verständnis ermöglicht das Erkennen der Informationsstruktur und die Gruppierung relevanter Entitäten, die Bedeutung ist jedoch noch unklar. Das semantische Verständnis ist der Schlüssel, um die Bedeutung der Daten zu verstehen und die Lücke von der Datensicht zur Informationssicht schließen zu können.

Die Informationssicht ermöglicht die effiziente Nutzung der Informationen für datengetriebene Dienstleitungen. Beispiele für datengetriebene Dienstleitungen aus unterschiedlichen Domänen sind die Produktionsplanung, die Intralogistik, die Verspätungsanzeige im öffentlichen Nahverkehr oder die Integration von Nutzererfahrung in den Entwicklungsprozess. Um die Informationssicht von unterschiedlichen Datenquellen herstellen zu können, muss zum einen eine einheitliche Terminologie der Informationen aus den unterschiedlichen Datenquellen erreicht werden. Zum anderen sind die Datenintegrationskonflikte bei der Transformation der Daten in die einheitliche Terminologie aufzulösen. Die Erstellung einer einheitlichen Terminologie erfolgt heutzutage zunehmend mithilfe von Ontologien. Ontologien, wie in der Künstlichen Intelligenz erörtert, werden als formale, partielle Spezifikationen einer Vereinbarung über die Beschreibung einer Domäne verstanden (Ferrario und Kuhn 2016).

Die Handhabung der Datenintegrationskonflikte und die Transformation der Daten aus unterschiedlichen Datenquellen, welche sich sowohl in der Terminologie, der Struktur als auch der Bedeutung einzelner Datensätze unterscheiden, ist bereits möglich. Hierfür können unterschiedliche Ansätze verfolgt werden. Im Folgenden wird der Ansatz der semantischen Datenintegration mithilfe eines Mediators vorgestellt. Die Aufgabe eines Mediators ist die Vermittlung der Informationen zwischen heterogenen Datenquellen und einem Zielsystem. Hierfür definiert ein Nutzer eine Informationsanfrage und übergibt sie dem Semantischen Mediator (Franke et al. 2016). Dieser ist in der Lage zu identifizieren, welche Datenquelle welchen Teil der angeforderten Informationen bereitstellen kann. Der Zugriff auf diese Informationen erfolgt mit Wrappern. Ein Wrapper ist ein Softwaremodul, welches Daten von einem bestimmten Typ von Datenquelle abfragen und in ein Zwischenformat umwandeln kann. Nachdem der Semantische Mediator alle Zwischenergebnisse eingesammelt hat, aggregiert er alle Teilergebnisse zu einem Gesamtergebnis und löst hierbei alle Datenintegrationskonflikte auf. Das Ergebnis jeder Anfrage ist eine Informationssicht in einer datenquellen-

unabhängigen Terminologie, welche die Eingabe für datengetriebene Services sein kann. Der Mehrwert, der sich durch den Einsatz des Semantischen Mediators oder einer anderen Datenintegrationslösung ergibt, ist die strikte Trennung der Datensicht von der Informationssicht. Hierdurch werden die datengetriebenen Services unabhängig von den spezifischen Datenquellen und Datenschemas, was sie skalierbar und wartbar gestaltet. So wird beispielsweise die Robustheit gegenüber den alltäglichen Modernisierungsprozessen in der schnelllebigen IT erreicht.

Aus der Perspektive der Industrie ist der Einsatz eine Semantischen Mediators damit vor allem in solchen Bereichen interessant, in denen eine durchgehende Informationskette durch eine Vielzahl unterschiedlicher IT-Systeme und der damit verknüpften Datenquellen nur schwer oder gar nicht umzusetzen ist. Im Hinblick auf die Logistik bietet diese Technologie eine interessante Basis für innovative Geschäftsmodelle, um die Effizienz von heutigen Lieferketten weiter zu steigern, indem relevante Informationen aller Stakeholder rechtzeitig und in der notwendigen Qualität bereitgestellt werden können.

Literaturverzeichnis

Ades, Maurice J. (2007): Proceedings of the 2007 spring simulation multiconference - Volume 2. Volume 2. San Diego, CA: Society for Computer Simulation International. Online verfügbar unter http://dl.acm.org/citation.cfm?id=1404680.

Bauernhansl, Thomas; Hompel, Michael ten; Vogel-Heuser, Birgit (Hg.) (2014): Industrie 4.0 in Produktion, Automatisierung und Logistik. Anwendung, Technologien, Migration. Wiesbaden: Springer Vieweg (SpringerLink).

Ferrario, Roberta; Kuhn, Werner (Hg.) (2016): Formal ontology in information systems. Proceedings of the 9th International Conference (FOIS 2016). FOIS (Conference); IOS Press. Amsterdam, Netherlands: IOS Press (Frontiers in artificial intelligence and applications, volume 283). Online verfügbar unter http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&AN=1640432.

Franke, Marco; Klein, Konstantin; Hribernik, Karl A.; Thoben, Klaus-Dieter (2016): Semantic Data Integration Approach for the Vision of a Digital Factory. In: Kai Mertins, Ricardo Jardim-Gonçalves, Keith Popplewell und João P. Mendonça (Hg.): Enterprise Interoperability VII. Enterprise Interoperability in the Digitized and Networked Factory of the Future, Bd. 8. Cham: Springer International Publishing (Proceedings of the I-ESA Conferences, v.8), S. 77–86.

Kietzmann, Jan H.; Hermkens, Kristopher; McCarthy, Ian P.; Silvestre, Bruno S. (2011): Social media? Get serious! Understanding the functional building blocks of social media. In: Business Horizons 54 (3), S. 241–251. DOI: 10.1016/j.bushor.2011.01.005.

Reeve, April (2013): Managing Data in Motion. Data Integration Best Practice Techniques and Technologies. Burlington: Elsevier Science (The Morgan Kaufmann Series on Business Intelligence). Online verfügbar unter http://gbv.eblib.com/patron/FullRecord.aspx?p=1152636.

Über den Autor

Marco Franke

Wissenschaftlicher Mitarbeiter
BIBA - Bremer Institut für Produktion und Logistik GmbH

Organizational Intelligence

BLG Freight Quality Tracking –Der Qualität auf der Spur

Die Zukunft der digitalen Qualitätssicherung

Freight Quality Tracking (FQT) ist eine neue digitale Dienstleistung des Seehafen- und Logistikdienstleisters BLG LOGISTICS GROUP AG & Co. KG mit der die Transparenz in der Supply Chain eine neue Dimension erreicht. Der Service wurde in Zusammenarbeit mit Kunden entwickelt und nutzt die Erkenntnisse aus unterschiedlichen Innovations- und Forschungsprojekten mit Sensorbasierten Dienstleistungen. Geplant ist, die Dienstleistung ab diesen Sommer 2019 anzubieten. Doch auch darüber hinaus ist BLG LOGISTICS offen für weitere interessierte Testkunden, mit denen diese Dienstleistung partnerschaftlich weiterentwickelt werden kann. Die Supply Chain ist heute in vielen Teilen vergleichbar mit einer Black Box. Über große Teile liegen keine, oder nur wenige Daten zum Transportverlauf vor. Was während des Transports geschieht und ob sich die Ware verspätet, wird oft erst im Nachhinein oder sehr spät sichtbar. Schätzungen zufolge sind 30 Prozent aller Transporte verspätet oder beschädigt, wovon ein Fünftel der Schäden auf Feuchtigkeit zurückgeführt werden. Die jährlichen Schäden, die durch Diebstahl und Beschädigung entstehen, werden auf 60 Milliarden Dollar geschätzt.

BLG LOGISTICS hat sich das Ziel gesetzt, mit der Dienstleistung Freight Quality Tracking die Transparenz in der Supply Chain für alle beteiligten Akteure deutlich zu erhöhen. Dafür werden smarte Services zur lückenlosen Überwachung der Waren in der Supply Chain bereitgestellt. Die Entwicklung dieser digitalen Dienstleistung basiert auf der Voraussetzung, echtzeitnah Zugriff auf Positions- und Zustandsdaten der Produkte in der Lieferkette zu haben. Das ist heute in vielen Fällen noch nicht vollumfänglich gewährleistet. Oft liegen während des Transports keine Ist-Informationen über den Zustand oder die Position der Ware vor. Je früher jedoch eine Unregelmäßigkeit im Wertschöpfungsprozess erkannt wird, desto geringer sind die daraus entstehenden Aufwände. Durch die

permanente Überprüfung der Produktqualität können Sondertransporte, Nacharbeitsumfänge, Produktionsstillstände oder sogar Rückrufaktionen vermieden oder zumindest reduziert werden. Mithilfe eines Sensors, der direkt am Packstück oder am Container montiert wird, setzt BLG LOGISTICS die Vision der transparenten Supply Chain um. Der Sensor übermittelt die individuell für den Kunden nützlichen Daten. Mithilfe der BLG Software werden diese Daten dem Kunden nicht nur bereitgestellt, sondern intelligent miteinander verknüpft, ausgewertet und anschließend visualisiert. Über die BLG-eigene Cloud-basierte Plattform kann der Kunde jederzeit die Orts- und Zustandsdaten seines Frachtguts einsehen.

Der smarte Service beantwortet Fragen wie

- „Wann wurde meine Ware verladen?“
- „Wo befindet sich meine Ware?“
- „Wie ist der Zustand meiner Ware?“
- „Verändert sich mein Liefertermin?“

und erlaubt so eine Prognose von Ankunftszeiten, frühzeitige Kapazitätsplanung und dadurch optimierte Prozesse.

In Abhängigkeit von den jeweils relevanten Einflussfaktoren werden kundenspezifische Sensorlösungen eingesetzt. Diese können mit Blick auf Route, Transportmittel oder Warenart unterschiedliche Daten erheben. Entscheidend bei der Definition der Einflussfaktoren sind ihre Auswirkungen auf die Qualität und die Pünktlichkeit der Ware. Freight Quality Tracking erlaubt diese Einflussfaktoren nahezu in Echtzeit zu überwachen. Die Bandbreite erstreckt sich von reinen Trackingdaten, die die aktuelle Position und den historischen Streckenverlauf der Ware anzeigen, über Qualitätsdaten, wie Temperatur, Luftfeuchtigkeit, Luftdruck oder Erschütterung, hin zu Statusdaten, wie eine außerplanmäßige Öffnung von Containern oder Waren. Ob und in welchem Ausmaß die Faktoren relevant sind, ermittelt die BLG individuell mit dem jeweiligen Kunden. Gemeinsam wird der passgenaue Sensor ausgewählt. Anhand der präzisen Analyse und Auswertung der Daten zum Warenstatus in der Lieferkette kann bei Verspätungen, Beschädigungen oder gar Verlusten des Transportguts unmittelbar eingegriffen und die Transportkosten niedrig gehalten werden. Erreicht ein Container beispielsweise nicht rechtzeitig das Schiff, kann der Kunde schon frühzeitig eingreifen und entscheiden, mit welchen Maßnahmen aufwendige Nacharbeiten oder sogar ein Produktionsstillstand verhindert werden können. Die Daten zum Warenstatus in der Lieferkette ermöglichen aber nicht nur frühzeitig Ad-hoc–Maßnahmen zu ergreifen, sondern helfen auch dabei, aufgetretene Mängel verursachergerecht zuzuordnen oder Warenverluste gezielt zu lokalisieren und nachzuvollziehen.
Im Nachhinein können Fehlerquellen identifiziert sowie Prozesse und Routen ausgewertet und optimiert bzw. geändert werden.

Die Vorteile des Freight Quality Tracking auf einen Blick:

- Die Lieferkette wird transparenter und effizienter für alle Beteiligten
- Material- und Informationsfluss werden synchronisiert: Warenlieferungen können leichter prognostiziert und Kapazitätsplanungen frühzeitig geplant werden
- Bei Abweichungen können frühzeitig Maßnahmen ergriffen und so Zusatzkosten reduziert werden
- Zustände können dokumentiert, verursachergerecht zugeordnet und verbessert werden
- Prozessverbesserungen und Routenoptimierungen können ermittelt werden

Der Einsatz einer solchen Dienstleistung ist für die Kunden im Hinblick auf den rasant wachsenden Containerumschlag von Bedeutung. Über 90 Prozent der weltweit gehandelten Waren werden heute auf dem Seeweg abgewickelt. Gleichzeitig steigt die Komplexität der Lieferketten stetig. Die Beteiligten werden durch die wachsende Anzahl von Logistikdienstleistern, Lieferanten, Kunden, Ländern und Transportwegen vor neue Herausforderungen gestellt. Hinzu kommt die steigende Erwartungshaltung der Kunden an die Qualität, den Preis und die Zeit.

Laut einer Studie der Initiative für Global Excellence in Supply Chain Operations, betrachten Industrieunternehmen die Variantenvielfalt in zunehmendem Maße als Erfolgsfaktor. Heute sind Logistikunternehmen noch mehr denn je gefordert, intelligente Lösungen für eine kundenorientierte Logistik zu bieten. Die Digitalisierung eröffnet dafür neue Möglichkeiten und Lösungen. Der neue digitale Service Freight Quality Tracking zur lückenlosen Überwachung der Waren geht genau auf diese Erwartungen ein. Freight Quality Tracking ist Bestandteil einer umfassenden Digitalisierungs-Offensive mit der BLG LOGISTICS einer smarten Logistik der Zukunft entgegensteuert. 2018 wurde der Zentralbereich „Nachhaltigkeit und Digitalisierung“ hierfür neu aufgestellt. Er bündelt die zahlreichen Aktivitäten, die BLG LOGISTICS entwickelt und fördert, weil sie auf den Erfolg des Unternehmens sowohl heute als auch in Zukunft einzahlen. Neben Nachhaltigkeitsthemen und Forschungsprojekten zählen dazu Logistik 4.0 und 100-Tage-Projekte. In einem der 100-Tage-Projekte entstand auch die Idee zum Freight Quality Tracking.

Über den Autor

Jakub Piotrowski

Leiter Nachhaltigkeit und Digitalisierung
BLG LOGISTICS GROUP AG & Co. KG

Organizational Intelligence

Die fehlende Digitalisierung in der Lieferkette

Fehlende Fokussierung als Ausgangssituation

In der Digitalisierung der Lieferkette liegt für die Unternehmen nachwievor einer der wichtigsten Wertetreiber und Hebel für Wachstumschancen. Sie hat das Potenzial einen entscheidenden Unterschied auszumachen und Zukunftsperspektiven zu ermöglichen. Unternehmen erkennen die Bedeutung der Digitalisierung der Lieferkette. Investitionen in die Transformation und Digitalisierung der Lieferketten- sowie Logistikautomatisierung erreichten weltweit in 2018 etwa 93 Milliarden Dollar (IDC, Juni 2018).

Die Transportlogistik stellt sich aktuell einer Vielzahl von Herausforderungen und steht vor vielen noch unbeantworteten Fragen. Die Akteure müssen sich veränderten Rahmenbedingungen stellen. Thematiken wie Brexit, Schadstoffemission, Ruhezeitenregelung oder 3D-Druck sind einige von ihnen und zeugen von einer hochgradigen Komplexität und einschlägigen Veränderungen in der Branche. Die Digitalisierung der Supply Chain spielt bei den eben angesprochenen Punkten eine große Rolle. So geben laut einer Studie des Capgemini Research Institutes 50% der befragten Unternehmen an, dass das Thema der Digitalisierung der Supply Chain zu den Top drei Prioritäten der Organisationen zählt. DB Schenker 2017 (DVZ, 2019) initiierte in Frankreich ein Pilotprojekt, um zukünftig das ge-samte Bestell- und Lieferwesen im europäischen Landverkehr zu digitalisieren. Ein Vorhaben, dass exemplarisch für alle Unternehmen steht.

Die Bedeutung in eine digitale Supply Chain zu investieren wurde erkannt. Es fehlt jedoch die Fokussierung, um einen flächendeckenden Nutzen über Skaleneffekte zu erzielen (Capgemini, Dezember 2018). Unsere Studie hat herausgefunden, dass die befragten Unternehmen bis zu 30 Projekte in Ideation, PoC oder der Pilotierung haben. Lediglich 11% der Unternehmen in Deutsch-land sind in

der Lage die gestartet Initiative zu skalieren. Diese Unternehmen haben weniger als acht Vorhaben in der Umsetzung.

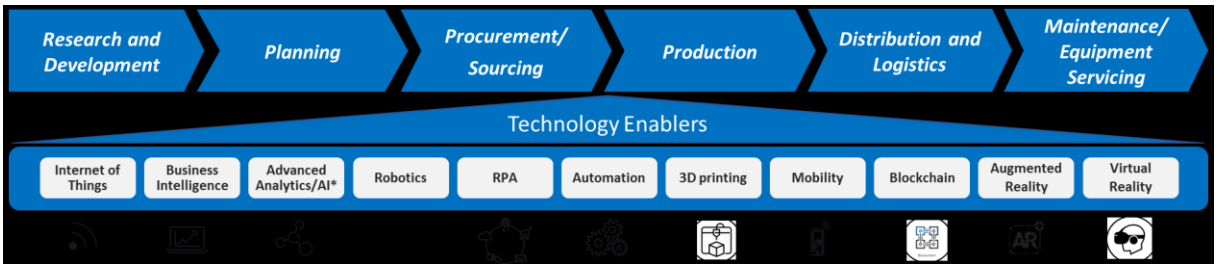
> *"Wir haben mit 200 Projektvorschlägen und 42 Proofs-of-Concept begonnen, die wir mit großer Sorgfalt überprüft haben, um zu verstehen, welcher Wert daraus gewonnen werden könnte. Von dort aus haben wir uns entschieden, uns auf fünf Hauptinitiativen zu konzentrieren.", sagt ein Top-Manager, der das Programm leitet.*

Was sind digitale Supply Chain Initiativen?

Digitale Supply Chain Initiativen nutzen digitale Technologien, um den Betrieb über die gesamte Lieferkette hinweg zu optimieren. Die Digitalisierung der Supply Chain umfasst zwei Schwerpunkte:

- Einen Prozess oder eine Aufgabe, die heute manuell oder offline ausgeführt wird, und effizienter mit digitalen Werkzeugen durchzuführen
- Digitalisierte Prozesse und Daten zu nutzen, um etwas effektiver und verbraucherorientierter zu gestalten

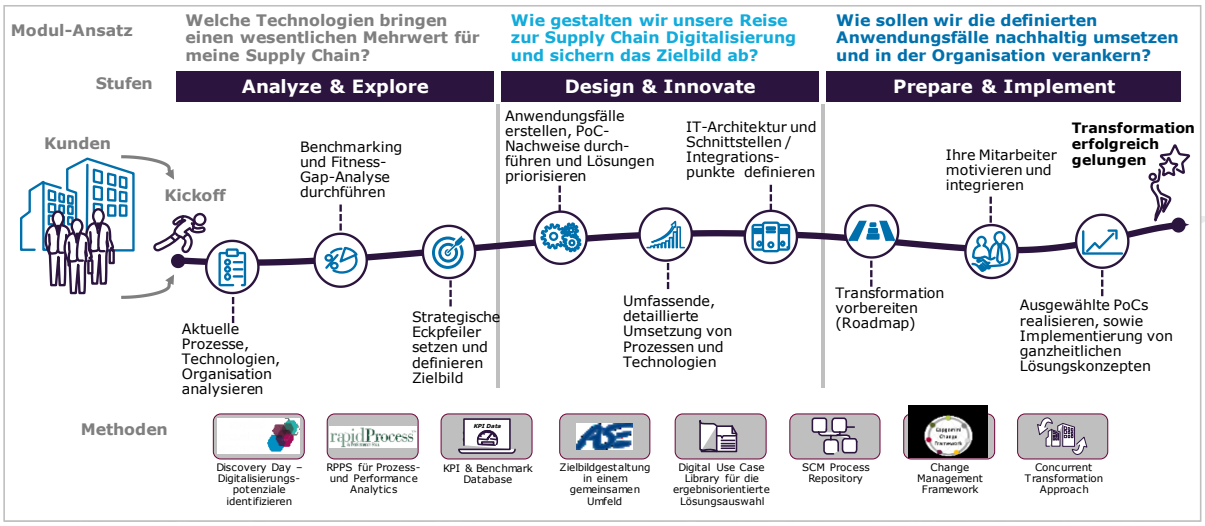
Um dies zu erreichen werden unterstützende Technologien entlang der Supply Chain eingesetzt:



Die Notwendigkeit in Technologien zu investieren ist den Beteiligten bewusst. Die von April bis Mai 2018 durchgeführten Befragung (Capgemini, Dezember 2018) von weltweit mehr als 1.000 Unternehmen unterstützt diese Sichtweise. 77% der Unternehmen sehen Kosteneinsparung als wesentlichen Treiber, gefolgt von der Absicht den Umsatz zu steigern (56%). Neue Geschäftsmodelle zu unterstützen folgt mit 53% erst an dritter Stelle. Die Begründung dafür sieht Lars Olsen, Branch Manager und Partner von NTG East und NTG Continent (Gesing, 2019), darin, dass der Fokus branchenweit auf die Reduktion von Kosten gelegt wird und nicht auf die Entwicklung bzw. Implementierung neuer Technologien.

Vorgehensweise und Lösungsansätze

Erfolgreiche Lösungsansätze einer digitalen Transformation berücksichtigen damit sowohl die anfänglich angesprochenen Problemsituationen im Markt, als auch das Kostensenkungspotential und laufen entlang eines abgestimmten modularisierten Vorgehens ab.



Als Beispiel dient das Transportmanagement System als essentielles Werkzeug, um der steigenden Komplexität und Wettbewerbssituation im Markt zu begegnen. Mit Hilfe des Systems sollen Kosten gesenkt, die Performance verbessert und die Kundenzufriedenheit gesteigert werden. Dazu ist eine abgestimmte Strategie für alle drei Aspekte zu entwickeln und in ein System zu überführen.

Ein wesentlicher Aspekt liegt in der Einbeziehung aller Beteiligten eines Unternehmens. Auf diese Weise kann auf Basis des Datenmaterials Optimierungspotential erkannt und gehoben werden. Das Transportmanagement System ist mit anderen internen Quellen wie dem ERP oder WMS eng zu koppeln. Darüberhinausgehend ist über Plattformen die Außenwelt des Unternehmens einzubeziehen, um exogene Einflüsse außerhalb des eigenen Netzwerkes entsprechend zu berücksichtigen. Dabei sind die schon genannten Einflussfaktoren zum Beispiel aus Politik oder Umwelt ebenfalls von essentieller Bedeutung.

Capgemini hat für einen Logistkdienstleister ein Transportmanagement System entwickelt, welches für Transparenz und Flexibilität in der Supply Chain sorgt. Erreicht wird dies durch eine zentrale und globale Datenbasis mit Hilfe dessen jederzeit Informationen zum aktuellen Status von Transporten geliefert werden. Die Datenbasis ermöglicht eine durchgehende Analyse der Transportkette im Hinblick auf Kosten, Erlöse sowie Prozessqualität. Der Einsatz innovativer Technologien und steigender Datenanalysefähigkeit erlaubt genauere Aussagen, z.B. hin-sichtlich der Liefer- und Ankunftszeiten.

In Zeiten von Big Data ist es darüber hinaus denkbar vorhandene Verkehrsdaten mit einfließen zu lassen und unnötige Leerfahrten zu vermeiden sowie Verkehrsflüsse effizienter auf Tageszeiten abzustimmen. Das Kapazitätsmanagement zwischen den beteiligten Partner in der Supply Chain wird somit zunehmend ein essentieller Bestandteil der Transportlogistik. Ziel ist eine optimale Auslastung, Leerfahrten zu vermeiden und so Kosten zu senken. Eine Lösung liefern die E-Marketplaces bzw. Plattformen.

Diese verbinden auf effiziente Art und Weise diejenigen, die die Dienstleistung benötigen mit den freien Transportkapazitäten und -ressourcen. Vorteilhaft wird dies jedoch nur, wenn eine einfache und intuitive Bedienung für alle Beteiligten angeboten werden kann. Der sogenannten User Experience kommt eine hohe Bedeutung zu. Diese fordert eine Konzentration auf das wesentliche und muss vom Anwender erkannt werden.

Über den Autor

Sven C. Dahlmeier

Principal, Digital Supply Chain Automotive
Capgemini invent

Die GFFT sagt DANKE!

Wir bedanken uns ebenfalls bei allen Autoren für die Bereitstellung der Beiträge und des Bildmaterials.

Das GFFT-Jahrestreffen im Schloss Biebrich

Impressum:
Gesellschaft zur Förderung des Forschungstransfers e.V.
Niddastraße 6, 61118 Bad Vilbel
Vorstand: Dr. Gerd Große,
Metin Özdiyar-Steffen,
Prof. Dr. Bernd Freisleben
Dr. Carl Hans

GFFT

Gemeinnützige Gesellschaft zur Förderung des Forschungstransfers e.V.

GFFT Jahresbericht 2018/2019

Wir bringen innovative Technologien in die Anwendung.